

Microsoft Security Best Practices

Article • 09/07/2022 • 2 minutes to read

Microsoft Security Best Practices (formerly known as the Azure Security Compass or Microsoft Security Compass) is a collection of best practices that provide clear actionable guidance for security related decisions. This is designed to help you increase your security posture and reduce risk whether your environment is cloud-only, or a hybrid enterprise spanning cloud(s) and on-premises data centers. This guidance was formerly referred to as Azure Security Compass and is now increasing in scope to encompass all Microsoft security guidance and capabilities, including Microsoft 365.

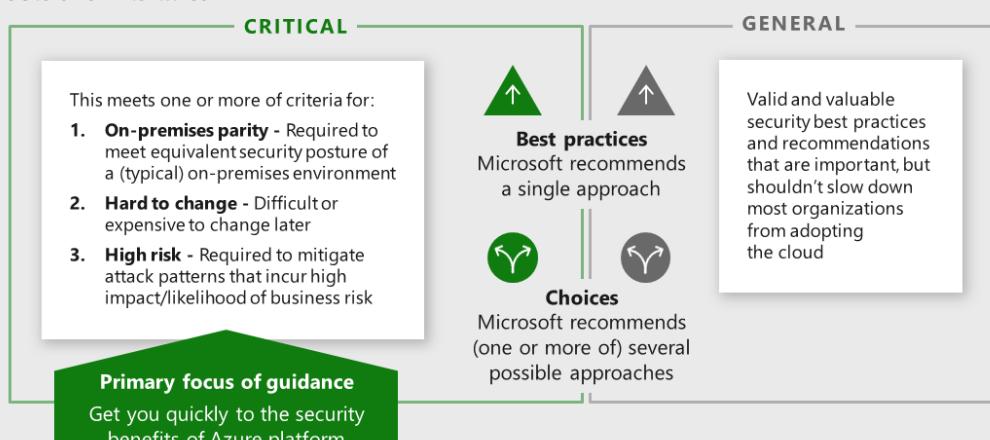
In this guidance:

- [Introduction](#)
- [Governance, risk, and compliance](#)
- [Security operations](#)
- [Identity and access management](#)
- [Network security and containment](#)
- [Information protection and storage](#)

This guidance is presented in a series of videos. To download the PowerPoint slides associated with these videos, click [download presentation slides](#).

Guidance Structure

Actionable and Prioritized



Note: These represent Microsoft's default opinion based on our experience and knowledge. Your organization may prioritize risk and mitigations differently based on your unique business needs, business risks, or other factors.

Related topics

[Security design principles for cloud architecture](#)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

What's inside Microsoft Security Best Practices?

Article • 06/08/2022 • 2 minutes to read

Microsoft Security Best Practices is a collection of best practices that provide clear actionable guidance for security related decisions. This is designed to help you increase your security posture and reduce risk whether your environment is cloud-only, or a hybrid enterprise spanning cloud(s) and on-premises data centers.

To download the PowerPoint slides associated with these videos, click [download presentation slides](#).

Introduction to Microsoft Security Best Practices (14:58)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm6i?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm6i?postJs||Msg=true)

Evolution of Threat Environment, Roles, & Digital Strategies (20:04)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9sf?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9sf?postJs||Msg=true)

Transformation of Security, Strategies, Tools, & Threats (15:13)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Ay?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Ay?postJs||Msg=true)

Azure Regions and Services (02:59)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9sk?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9sk?postJs||Msg=true)

Microsoft Security Practices (13:49)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Az?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Az?postJs||Msg=true)

Azure Components and Reference Model (21:51)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6Ft?postJsIMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6Ft?postJsIMsg=true)

Microsoft Security Best Practices workshop presentation

View the slides for this workshop.

 [Thumb image of Microsoft Security Best Practices presentation slides](#)

[PowerPoint](#) | [PDF](#)

Note

Azure Security Compass or Microsoft Security Compass is now renamed as Microsoft Security Best Practices.

Top 10 Azure Security best practices

View slides for Top 10 Azure Security best practices.

 [Thumb image of top 10 Azure Security best practices](#)

[PowerPoint](#) | [PDF](#)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Progress and role tracking worksheets

Article • 06/08/2022 • 2 minutes to read

This topic includes tracking worksheets that assist you with tracking the status of decisions and roles.

These can be used by an organization to track status for Microsoft's recommendations.

Tracking worksheet

The tracking worksheet assists with tracking status of decisions, policy, and implementation.

The screenshot shows a tracking worksheet for the Azure Security Compass Self-Assessment Guidance. It is divided into three main sections: Decisions, Policy, and Implementation. Each section has a progress bar icon (green for Decisions, blue for Policy, orange for Implementation) and a table with suggested milestones.

Decisions	Policy	Implementation
Decision made: Assign a percentage depending on what stage the decision to implement the prescribed control is, the percentages are assigned as follows: Suggested Milestones 50% Decision maker has been identified 100% Decision has been finalized.	Written in Policy: Assign a percentage based on the status of capturing decisions into written, approved, and published policy. Suggested Milestones 33% Written draft complete 66% Policy Approved 100% Policy Published	Implementation Status: This value represents the status of the implementation for each best practice and choice. Suggested Milestones 25% Planned 50% Developed 75% Tested 100% Deployed

[Excel](#)

Cloud role tracking worksheet

The cloud role tracking worksheet assists with designating the parties responsible for specific functions in Azure.

 Governance, Risk, & Compliance Clear Lines of Responsibility	
<p>Use this worksheet to designate the parties responsible for specific functions in Azure. Consistent procedures will avoid confusion that can lead to human and automation errors which increases an organization's security risk. <small>*Most organizations map these closely to current on-premises models.</small></p>	
<p>Network Security Typically existing network security team Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NGGs, ASGs, etc.</p>	
Network Management	Typically existing network operations team Enterprise-wide virtual network and subnet allocation
Server Endpoint Security	Typically IT operations, security, or jointly Monitor and remediate server security (patching, configuration, endpoint security, etc.)
Incident Monitoring and Response	Typically security operations team Investigate and remediate security incidents in SIEM or source console <ul style="list-style-type: none"> ▪ Azure Security Center ▪ Azure AD Identity Protection
Policy Management	Typically GRC team + Architecture Set direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources
Identity Security and Standards	Typically Security Team + Identity Team jointly Set direction for Azure AD directories, PIM-PAD, MFA, password/lync synchronization configuration, Application Identity Standards
<p> Tip Document and socialize this widely with all teams working on Azure</p>	

[PDF](#) | [PowerPoint](#)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

The immutable laws of security

Article • 10/27/2022 • 4 minutes to read

The original immutable laws of security (v2 updated below) identified key technical truths that busted prevalent security myths of those times. In that spirit, we're publishing a new complementary set of laws focused on busting prevalent myths in today's world of ubiquitous cybersecurity risk.

Since the original immutable laws, information security has grown from a technical discipline into a cybersecurity risk management discipline that includes cloud, IoT and OT devices. Now security is part of the fabric of our daily lives, business risk discussions, elections, and more.

As many of us in the industry followed this journey to a higher level of abstraction, we saw patterns of common myths, biases, and blind spots emerge at the risk management layer. We decided to create a new list of laws for cybersecurity risk while retaining the original laws (v2) as is (with a single slight change of "bad guy" to "bad actor" to be fully correct and inclusive).

Each set of laws deals with different aspects of cybersecurity – designing sound technical solutions vs. managing a risk profile of complex organizations in an ever-changing threat environment. The difference in the nature of these laws also illustrates the difficult nature of navigating cybersecurity in general; technical elements tend toward the absolute while risk is measured in likelihood and certainty

Because it's difficult to make predictions (especially about the future), we suspect these laws may evolve with our understanding of cybersecurity risk.

10 Laws of Cybersecurity Risk

- 1. Security success is ruining the attacker ROI** - Security can't achieve an absolutely secure state so deter them by disrupting and degrading their Return on Investment (ROI). Increase the attacker's cost and decreasing the attacker's return for your most important assets.
- 2. Not keeping up is falling behind** – Security is a continuous journey, you must keep moving forward because it will continually get cheaper and cheaper for attackers to successfully take control of your assets. You must continually update your security patches, security strategies, threat awareness, inventory, security tooling, security hygiene, security monitoring, permission models, platform coverage, and anything else that changes over time.

- 3. Productivity always wins** – If security isn't easy for users, they'll work around it to get their job done. Always make sure solutions are secure **and** usable.
- 4. Attackers don't care** - Attackers will use any available method to get into your environment and increase access to your assets including compromising a networked printer, a fish tank thermometer, a cloud service, a PC, a Server, a Mac, a mobile device, influence or trick a user, exploit a configuration mistake or insecure operational process, or just ask for passwords in a phishing email. Your job is to understand and take away the easiest and cheapest options as well as the most useful ones (for example, anything that leads to administrative privileges across many systems).
- 5. Ruthless Prioritization is a survival skill** – Nobody has enough time and resources to eliminate all risks to all resources. Always start with what is most important to your organization, most interesting to attackers, and continuously update this prioritization.
- 6. Cybersecurity is a team sport** – Nobody can do it all, so always focus on the things that only you (or your organization) can do to protect your organization's mission. For things that others can do better or cheaper, have them do it (security vendors, cloud providers, community).
- 7. Your network isn't as trustworthy as you think it is** - A security strategy that relies on passwords and trusting any intranet device is only marginally better than no security strategy at all. Attackers easily evade these defenses so the trust level of each device, user, and application must be proven and validated continuously starting with a level of zero trust.
- 8. Isolated networks aren't automatically secure** - While air-gapped networks can offer strong security when maintained correctly, successful examples are extremely rare because each node must be completely isolated from outside risk. If security is critical enough to place resources on an isolated network, you should invest in mitigations to address potential connectivity via methods such as USB media (for example, required for patches), bridges to intranet network, and external devices (for example, vendor laptops on a production line), and insider threats that could circumvent all technical controls.
- 9. Encryption alone isn't a data protection solution** - Encryption protects against out of band attacks (on network packets, files, storage, etc.), but data is only as secure as the decryption key (key strength + protections from theft/copying) and other authorized means of access.
- 10. Technology doesn't solve people and process problems** - While machine learning, artificial intelligence, and other technologies offer amazing leaps forward in security (when applied correctly), cybersecurity is a human challenge and will never be solved by technology alone.

Reference

Immutable Laws of Security v2

- **Law #1:** If a bad actor can persuade you to run their program on your computer, it's not solely your computer anymore.
- **Law #2:** If a bad actor can alter the operating system on your computer, it's not your computer anymore.
- **Law #3:** If a bad actor has unrestricted physical access to your computer, it's not your computer anymore.
- **Law #4:** If you allow a bad actor to run active content in your website, it's not your website anymore.
- **Law #5:** Weak passwords trump strong security.
- **Law #6:** A computer is only as secure as the administrator is trustworthy.
- **Law #7:** Encrypted data is only as secure as its decryption key.
- **Law #8:** An out-of-date antimalware scanner is only marginally better than no scanner at all.
- **Law #9:** Absolute anonymity isn't practically achievable, online or offline.
- **Law #10:** Technology isn't a panacea.

Microsoft Security Best Practices module: Governance, risk, and compliance

Article • 06/08/2022 • 2 minutes to read

Governance, Risk, and Compliance (GRC) activities help reduce organizational risk by ensuring policy and best practices are followed consistently over time. This section also addresses key roles and responsibilities we have found important for successfully managing cloud security.

See the [Governance, risk, and compliance](#) and [Capabilities](#) topics for more information.

The following videos provide guidance on governance, risk, and compliance. You can also download the [PowerPoint slides](#) associated with these videos.

Part 1: Introduction + Manage Connected Tenants (08:45)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qbBk?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qbBk?postJs||Msg=true)

Part 2: Clear Lines of Responsibility (02:46)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjkJ?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjkJ?postJs||Msg=true)

Part 3: Segmentation Strategy (02:11)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZi?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZi?postJs||Msg=true)

Part 4: Management Groups (04:15)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZh?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZh?postJs||Msg=true)

Part 5: Root Management Group (03:06)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZj?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qdZj?postJs||Msg=true)

Part 6: GRC Top Risks (03:31)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjkM?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjkM?postJs||Msg=true)

Part 7: Security Incident Notification (03:35)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1M?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1M?postJs||Msg=true)

Part 8: Access Reviews (02:15)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qlYf?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qlYf?postJs||Msg=true)

Part 9: Security Posture Improvement (03:30)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1N?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1N?postJs||Msg=true)

Part 10: Access for Security Personnel (03:18)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6vz?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6vz?postJs||Msg=true)

Part 11: Insecure Legacy Protocols (01:53)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3E6?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3E6?postJs||Msg=true)

Part 12: Compliance (04:29)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6vA?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6vA?postJs||Msg=true)

Part 13: Benchmarks (01:37)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3E7?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3E7?postJs||Msg=true)

Part 14: Azure Policy (02:30)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1O?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qh1O?postJs||Msg=true)

Part 15: Elevated Security Capabilities (03:43)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9wB?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9wB?postJs||Msg=true)

Part 16: General Guidance (03:01)

<https://www.microsoft.com/en-us/videoplayer/embed/RE4q3E9?postJs||Msg=true> ↗

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Governance, risk, and compliance

Article • 06/08/2022 • 20 minutes to read

Organizations of all sizes are constrained by their available resources; financial, people, and time. To achieve an effective return on investment (ROI) organizations must prioritize where they will invest. Implementation of security across the organization is also constrained by this, so to achieve an appropriate ROI on security the organization needs to first understand and define its security priorities.

Governance – How is the organization's security going to be monitored, audited, and reported? Design and implementation of security controls within an organization is only the beginning of the story. How does the organization know that things are actually working? Are they improving? Are there new requirements? Is there mandatory reporting? Similar to compliance there may be external industry, government or regulatory standards that need to be considered.

Risk – What types of risks does the organization face while trying to protect identifiable information, Intellectual Property (IP), financial information? Who may be interested or could leverage this information if stolen, including external and internal threats as well as unintentional or malicious? A commonly forgotten but extremely important consideration within risk is addressing Disaster Recovery and Business Continuity.

Compliance – Are there specific industry, government, or regulatory requirements that dictate or provide recommendation on criteria that your organization's security controls must meet? Examples of such standards, organizations, controls, and legislation are [ISO27001](#), [NIST](#), [PCI-DSS](#).

The collective role of organization(s) is to manage the security standards of the organization through their lifecycle:

- **Define** - Set organizational standards and policies for practices, technologies, and configurations based on internal factors (organizational culture, risk appetite, asset valuation, business initiatives, etc.) and external factors (benchmarks, regulatory standards, threat environment, and more)
- **Improve** – Continually push these standards incrementally forward towards the ideal state to ensure continual risk reduction.
- **Sustain** – Ensure the security posture doesn't degrade naturally over time by instituting auditing and monitoring compliance with organizational standards.

Prioritize security best practices investments

Security best practices are ideally applied proactively and completely to all systems as you build your cloud program, but this isn't reality for most enterprise organizations. Business goals, project constraints, and other factors often cause organizations to balance security risk against other risks and apply a subset of best practices at any given point.

We recommend applying as many as of the best practices as early as possible, and then working to retrofit any gaps over time as you mature your security program. We recommend evaluating the following considerations when prioritizing which to follow first:

- **High business impact and highly exposed systems** – These include systems with direct intrinsic value as well as the systems that provide attackers a path to them. For more information, see [Identify and classify business critical applications](#).
- **Easiest to implement Mitigations**– Identify quick wins by prioritizing the best practices, which your organization can execute quickly because you already have the required skills, tools, and knowledge to do it (for example, implementing a Web App Firewall (WAF) to protect a legacy application).
Be careful not to exclusively use (or overuse) this short-term prioritization method. Doing so can increase your risk by preventing your program from growing and leaving critical risks exposed for extended periods.

Microsoft has provided some prioritized lists of security initiatives to help organizations start with these decisions based on our experience with threats and mitigation initiatives in our own environments and across our customers. See [Module 4a of the Microsoft CISO Workshop](#) ↗

Manage connected tenants

Ensure your security organization is aware of all enrollments and associated subscriptions connected to your existing environment (via ExpressRoute or Site-Site VPN) and monitoring as part of the overall enterprise.

These azure resources are part of your enterprise environment and security organizations require visibility into them. Security organizations need this access to assess risk and to identify whether organizational policies and applicable regulatory requirements are being followed.

Ensure all Azure environments that connect to your production environment/network apply your organization's policy and IT governance controls for security. You can discover existing connected tenants using a [tool](#) provided by Microsoft. Guidance on permissions you may assign to security is in the [Assign privileges for managing the environment](#) section.

Clear lines of responsibility

Designate the parties responsible for specific functions in Azure

Clearly documenting and sharing the contacts responsible for each of these functions will create consistency and facilitate communication. Based on our experience with many cloud adoption projects, this will avoid confusion that can lead to human and automation errors that create security risk.

Designate groups (or individual roles) that will be responsible for these key functions:

Group or individual role	Responsibility
Network Security	<i>Typically existing network security team.</i> Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
Network Management	<i>Typically existing network operations team.</i> Enterprise-wide virtual network and subnet allocation.
Server Endpoint Security	<i>Typically IT operations, security, or jointly.</i> Monitor and remediate server security (patching, configuration, endpoint security, etc.).
Incident Monitoring and Response	<i>Typically security operations team.</i> Investigate and remediate security incidents in Security Information and Event Management (SIEM) or source console.
Policy Management	<i>Typically GRC team + Architecture.</i> Set Direction for use of Role Based Access Control (RBAC), Microsoft Defender for Cloud, Administrator protection strategy, and Azure Policy to govern Azure resources.
Identity Security and Standards	<i>Typically Security Team + Identity Team jointly.</i> Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards.

Enterprise segmentation strategy

Identify groups of resources that can be isolated from other parts of the enterprise to contain (and detect) adversary movement within your enterprise. This unified enterprise segmentation strategy will guide all technical teams to consistently segment access using networking, applications, identity, and any other access controls.

A clear and simple segmentation strategy helps contain risk while enabling productivity and business operations.

An enterprise segmentation strategy is defined higher than a traditional "*network segmentation*" security strategy. Traditional segmentation approaches for on premises environments frequently failed to achieve their goals because they were developed "bottom-up" by different technical teams and were not aligned well with business use cases and application workloads. This resulted in overwhelming complexity that generates support issues and often undermines the original purpose with broad network firewall exceptions.

Creating a unified enterprise segmentation strategy enables to guide all technical teams stakeholders (IT, Security, Applications, etc.) Business Units that is built around the business risks and needs will increase alignment to and understand and support sustainability of the security containment promises. This clarity and alignment will also reduce s the risk of human errors and automation failures that can lead to security vulnerabilities, operational downtime, or both.

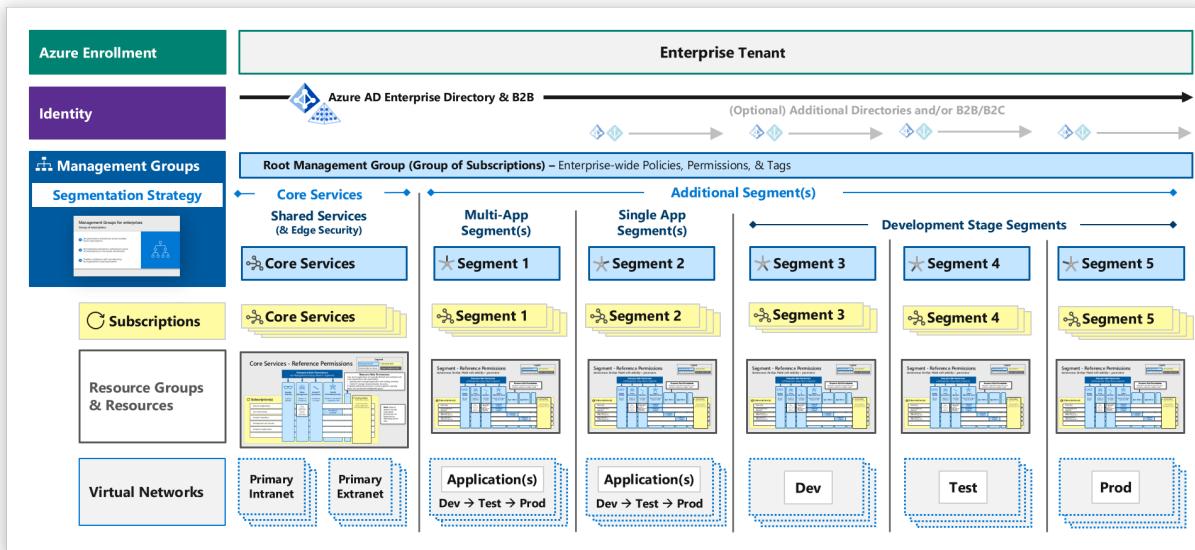
While network micro-segmentation also offers promise to reduce risk (discussed more in [Network Security and Containment](#) section), it doesn't eliminate the need to align technical teams. Micro segmentation should be considered after to and plans to ensure the ensuring technical teams are aligned so you can avoid a recurrence of the internal conflicts that plagued and confusion of the on-premises network generation segmentation strategies.

Here are Microsoft's recommendations for prioritizing initiatives on containment and segmentation (based on Zero Trust principles). These recommendations are listed in priority order by highest importance.

- Ensure alignment of technical teams to a single enterprise segmentation strategy.
- Invest in broadening containment by establishing a modern perimeter based on zero trust principles focused on identity, device, applications, and other signals (to overcome limitation of network controls to protect new resources and attack types).
- Bolster network controls for legacy applications by exploring micro segmentation strategies.

A good enterprise segmentation strategy meets these criteria:

- **Enables Operations** – Minimizes operation friction by aligning to business practices and applications
- **Contains Risk** - Adds cost and friction to attackers by
 - Isolating sensitive workloads from compromise of other assets
 - Isolating high exposure systems from being used as a pivot to other systems
- **Monitored** – Security Operations should monitor for potential violations of the integrity of the segments (account usage, unexpected traffic, etc.)



Security team visibility

Provide security teams read-only access to the security aspects of all technical resources in their purview

Security organizations require visibility into the technical environment to perform their duties of assessing and reporting on organizational risk. Without this visibility, security will have to rely on information provided from groups operating the environment who have a potential conflict of interest (and other priorities).

Note that security teams may separately be granted additional privileges if they have operational responsibilities or a requirement to enforce compliance on Azure resources.

For example in Azure, assign security teams to the **Security Readers** permission that provides access to measure security risk (without providing access to the data itself)

For enterprise security groups with broad responsibility for security of Azure, you can assign this permission using:

- *Root management group* – for teams responsible for assessing and reporting risk on all resources
- *Segment management group(s)* – for teams with limited scope of responsibility (typically required because of organizational boundaries or regulatory requirements)

Because security will have broad access to the environment (and visibility into potentially exploitable vulnerabilities), you should consider them critical impact accounts and apply the same protections as administrators. The [Administration](#) section details these controls for Azure.

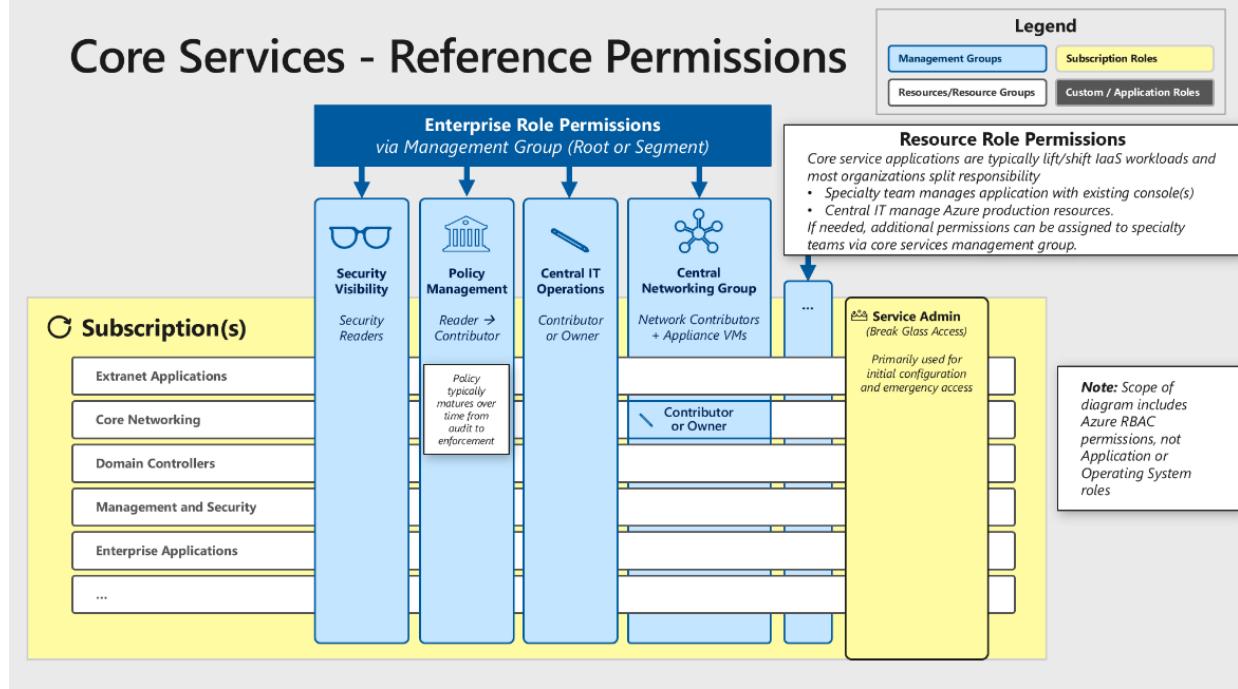
Assign privileges for managing the environment

Grant roles with operational responsibilities in Azure the appropriate permissions based on a clearly documented strategy built from the principle of least privilege and your operational needs.

Providing clear guidance that follows a reference model will reduce risk because by increasing it provides clarity for your technical teams implementing these permissions. This clarity makes it easier to detect and correct human errors like overpermissioning, reducing your overall risk.

Microsoft recommends starting from these Microsoft reference models and adapting to your organization.

Core Services - Reference Permissions



Core Services Reference Permissions

This segment hosts shared services utilized across the organization. These shared services typically include Active Directory Domain Services, DNS/DHCP, System Management Tools hosted on Azure Infrastructure as a Service (IaaS) virtual machines.

Security Visibility across all resources – For security teams, grant read-only access to security attributes for all technical environments. This access level is needed to assess risk factors, identify potential mitigations, and advise organizational stakeholders who accept the risk. See [Security Team Visibility](#) for more details.

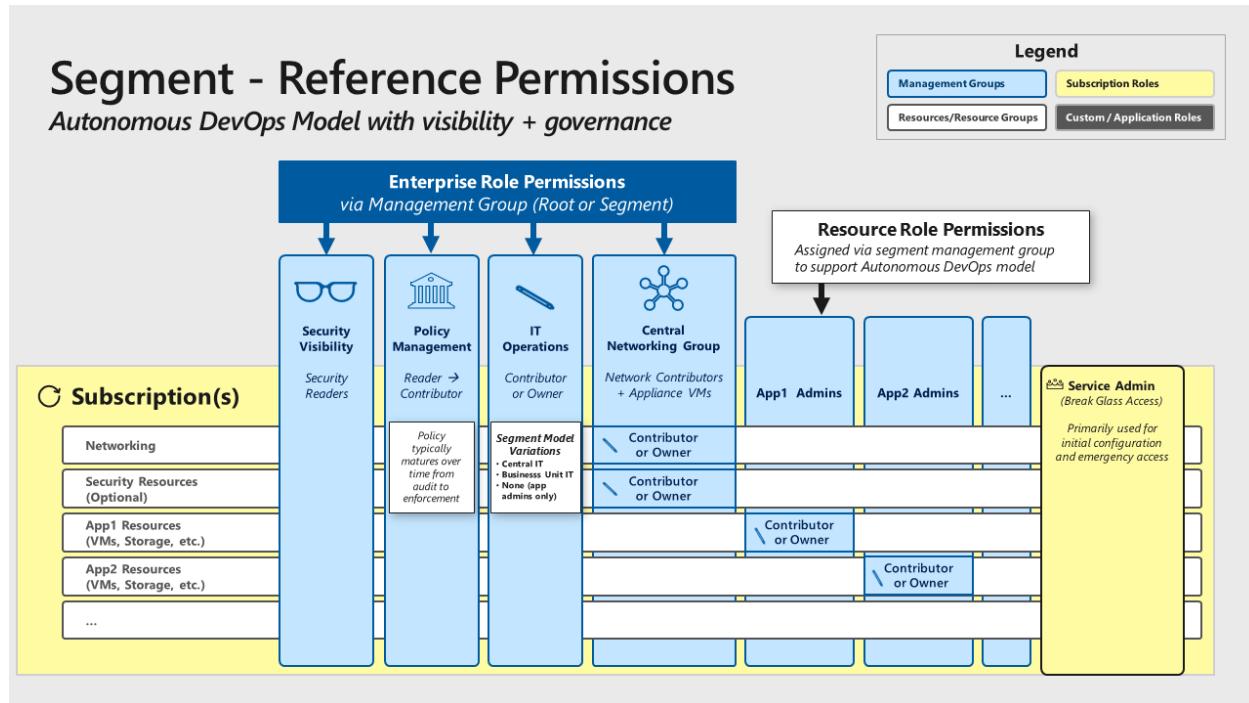
Policy management across some or all resources – To monitor and enforce compliance with external (or internal) regulations, standards, and security policy, assign appropriate permission to those roles. The roles and permissions you choose will depend on the organizational culture and expectations of the policy program. See [Microsoft Cloud Adoption Framework for Azure](#).

Central IT operations across all resources – Grant permissions to the central IT department (often the infrastructure team) to create, modify, and delete resources like virtual machines and storage.

Central networking group across network resources – To ensure consistency and avoid technical conflicts, assign network resource responsibilities to a single central networking organization. These resources should include virtual networks, subnets, Network Security Groups (NSG), and the virtual machines hosting virtual network appliances. See [Centralize Network Management And Security](#) for more details

Resource Role Permissions – For most core services, administrative privileges required to manage them are granted via the application itself (Active Directory, DNS/DHCP, System Management Tools, etc.), so no additional Azure resource permissions are required. If your organizational model requires these teams to manage their own VMs, storage, or other Azure resources, you can assign these permissions to those roles.

Service admin (Break Glass Account) – Use the service admin role only for emergencies (and initial setup if required). Do not use this role for daily tasks. See [Emergency Access \('Break Glass' Accounts\)](#) for more details.



Segment reference permissions

This segment permission design provides consistency while allowing flexibility to accommodate the range of organizational models from a single centralized IT group to mostly independent IT and DevOps teams.

Security visibility across all resources – For security teams, grant read-only access to security attributes for all technical environments. This access level is needed to assess risk factors, identify potential mitigations, and advise organizational stakeholders who accept the risk. See [Security Team Visibility](#).

Policy management across some or all resources – To monitor and enforce compliance with external (or internal) regulations, standards, and security policy assign appropriate permission to those roles. The roles and permissions you choose will depend on the organizational culture and expectations of the policy program. See [Microsoft Cloud Adoption Framework for Azure](#).

IT Operations across all resources – Grant permission to create, modify, and delete resources. The purpose of the segment (and resulting permissions) will depend on your organization structure.

- Segments with resources managed by a centralized IT organization can grant the central IT department (often the infrastructure team) permission to modify these resources.
- Segments managed by independent business units or functions (such as a Human Resources IT Team) can grant those teams permission to all resources in the segment.
- Segments with autonomous DevOps teams don't need to grant permissions across all resources because the resource role (below) grants permissions to application teams. For emergencies, use the service admin account (break-glass account).

Central networking group across network resources – To ensure consistency and avoid technical conflicts, assign network resource responsibilities to a single central networking organization. These resources should include virtual networks, subnets, Network Security Groups (NSG), and the virtual machines hosting virtual network appliances. See [Centralize Network Management And Security](#).

Resource Role Permissions – Segments with autonomous DevOps teams will manage the resources associated with each application. The actual roles and their permissions depend on the application size and complexity, the application team size and complexity, and the culture of the organization and application team.

Service Admin (Break Glass Account) – Use the service admin role only for emergencies (and initial setup if required). Do not use this role for daily tasks. See [Emergency Access \('Break Glass' Accounts\)](#) for more details.

Permission Guidance and Tips

- To drive consistency and ensure application to future subscriptions, permissions should be assigned at management group for the segment rather than the individual subscriptions. See [Avoid Granular and Custom Permissions](#) for more details.
- You should first review the built-in roles to see if one is applicable before creating a custom role to grant the appropriate permissions to VMs and other objects. See [Use Built in Roles](#) for more details

- **Security managers** group membership may be appropriate for smaller teams/organizations where security teams have extensive operational responsibilities.

Establish segmentation with management groups

Structure management groups into a simple design that guides the enterprise segmentation model.

Management groups offer the ability to consistently and efficiently manage resources (including multiple subscriptions as needed). However, because of their flexibility, it's possible to create an overly complex design. Complexity creates confusion and negatively impacts both operations and security (as illustrated by overly complex Organizational Unit (OU) and Group Policy Object (GPO) designs for Active Directory).

Microsoft recommends aligning the top level of management groups (MGs) into a simple [enterprise segmentation strategy](#) limited to 1 or 2 levels.

Use root management group carefully

Use the Root Management Group (MG) for enterprise consistency, but test changes carefully to minimize risk of operational disruption.

The root management group enables you to ensure consistency across the enterprise by applying policies, permissions, and tags across all subscriptions. Care must be taken when planning and implementing assignments to the root management group because this can affect every resource on Azure and potentially cause downtime or other negative impacts on productivity in the event of errors or unanticipated effects.

Root management group guidance:

- **Plan Carefully** - Select enterprise-wide elements to the root management group that have a clear requirement to be applied across every resource and/or low impact.

Good candidates include:

- **Regulatory requirements** with clear business risk/impact (for example, restrictions related to data sovereignty).

- Near-zero potential negative impact on operations such as policy with audit effect, Tag assignment, RBAC permissions assignments that have been carefully reviewed.
- **Test First** - Carefully test all enterprise-wide changes on the root management group before applying (policy, tags, RBAC model, etc.) using a
 - **Test Lab** - Representative lab tenant or lab segment in production tenant.
 - **Production Pilot** - Segment MG or Designated subset in subscription(s) / MG.
- **Validate Changes** – to ensure they have the desired effect.

Virtual Machine (VM) security updates and strong passwords

Ensure policy and processes enable (and require) rapid application of security updates to virtual machines.

Attackers constantly scan public cloud IP ranges for open management ports and attempt “easy” attacks like common passwords and unpatched vulnerabilities.

Enable [Microsoft Defender for Cloud](#) to identify missing security updates & apply them.

[Local Admin Password Solution \(LAPS\)](#) or a third party Privileged Access Management can set strong local admin passwords and just in time access to them.

Remove Virtual Machine (VM) direct internet connectivity

Ensure policy and processes require restricting and monitoring direct internet connectivity by virtual machines

Attackers constantly scan public cloud IP ranges for open management ports and attempt “easy” attacks like common passwords and known unpatched vulnerabilities

This can be accomplished with one or more methods in Azure:

- **Enterprise-wide prevention** - Prevent inadvertent exposure with an enterprise network and permission model such as the reference model described throughout this guidance. This significantly reduces the risk of accidental VM internet exposure by

- Ensuring that network traffic is routed through approved egress points by default
- Exceptions (for example, add a public IP address to a resource) must go through a centralized group (which can carefully evaluate exception requests to ensure appropriate controls are applied)
- **Identify and Remediate** exposed VMs using the [Microsoft Defender for Cloud](#) network visualization to quickly identify internet exposed resources.
- **Restrict management ports** (RDP, SSH) using [Just in Time access](#) in Microsoft Defender for Cloud.

Assign incident notification contact

Ensure a security contact receives Azure incident notifications from Microsoft typically a notification that your resource is compromised and/or attacking another customer.

This enables your security operations team to rapidly respond to potential security risks and remediate them.

Ensure administrator contact information in the Azure enrollment portal includes contact information that will notify security operations (directly or rapidly via an internal process)

Regularly review critical access

Regularly review roles that are assigned privileges with a business-critical impact.

Set up a recurring review pattern to ensure that accounts are removed from permissions as roles change. You can conduct the review manually or through an automated process by using tools such as [Azure AD access reviews](#).

Discover and remediate common risks

Identity well known risks for your Azure tenants, remediate those risks, and track your progress using Secure Score.

Identifying and remediating common security hygiene risks significantly reduces overall risk to your organization by increasing cost to attackers. When you remove cheap and well-established attack vectors, attackers are forced to acquire and use advanced or untested attack methods.

Azure Secure Score in Microsoft Defender for Cloud monitors the security posture of machines, networks, storage and data services, and applications to discover potential security issues (internet connected VMs, or missing security updates, missing endpoint protection or encryption, deviations from baseline security configurations, missing Web Application Firewall (WAF), and more). You should enable this capability (no additional cost), review the findings, and follow the included [recommendations](#) to plan and execute technical remediations starting with the highest priority items.

As you address risks, track progress and prioritize ongoing investments in your governance and risk reduction programs.

Increase automation with Azure Blueprints

Use Azure's native automation capabilities to increase consistency, compliance, and deployment speed for workloads.

Automation of deployment and maintenance tasks reduces security and compliance risk by limiting opportunity to introduce human errors during manual tasks. This will also allow both IT Operations teams and security teams to shift their focus from repeated manual tasks to higher value tasks like enabling developers and business initiatives, protecting information, and so on.

Utilize the Azure Blueprint service to rapidly and consistently deploy application environments that are compliant with your organization's policies and external regulations. [Azure Blueprint Service](#) automates deployment of environments including RBAC roles, policies, resources (VM/Net/Storage/etc.), and more. Azure Blueprints builds on Microsoft's significant investment into the Azure Resource Manager to standardize resource deployment in Azure and enable resource deployment and governance based on a desired-state approach. You can use built in configurations in Azure Blueprint, make your own, or just use Resource Manager scripts for smaller scope.

Several [Security and Compliance Blueprints](#) samples are available to use as a starting template.

Evaluate security using benchmarks

Use an industry standard benchmark to evaluate your organizations current security posture.

Benchmarking allows you to improve your security program by learning from external organizations. Benchmarking lets you know how your current security state compares to that of other organizations, providing both external validation for successful elements of

your current system as well as identifying gaps that serve as opportunities to enrich your team's overall security strategy. Even if your security program isn't tied to a specific benchmark or regulatory standard, you will benefit from understanding the documented ideal states by those outside and inside of your industry.

- As an example, the Center for Internet Security (CIS) has created security benchmarks for Azure that map to the CIS Control Framework. Another reference example is the MITRE ATT&CK™ framework that defines the various adversary tactics and techniques based on real-world observations. These external references control mappings help you to understand any gaps between your current strategy what you have and what other experts in the industry.

Audit and enforce policy compliance

Ensure that the security team is auditing the environment to report on compliance with the security policy of the organization. Security teams may also enforce compliance with these policies.

Organizations of all sizes will have security compliance requirements. Industry, government, and internal corporate security policies all need to be audited and enforced. Policy monitoring is critical to check that initial configurations are correct and that it continues to be compliant over time.

In Azure, you can take advantage of Azure Policy to create and manage policies that enforce compliance. Like Azure Blueprints, Azure Policies are built on the underlying Azure Resource Manager capabilities in the Azure platform (and Azure Policy can also be assigned via Azure Blueprints).

For more information on how to do this in Azure, please review [Tutorial: Create and manage policies to enforce compliance](#).

Monitor identity Risk

Monitor identity related risk events for warning on potentially compromised identities and remediate those risks.

Most security incidents take place after an attacker initially gains access using a stolen identity. These identities can often start with low privileges, but the attackers then use that identity to traverse laterally and gain access to more privileged identities. This repeats as needed until the attacker controls access to the ultimate target data or systems.

Azure Active Directory uses adaptive machine learning algorithms, heuristics, and known compromised credentials (username/password pairs) to detect suspicious actions that are related to your user accounts. These username/password pairs come from monitoring public and dark web sites (where attackers often dump compromised passwords) and by working with security researchers, law enforcement, Security teams at Microsoft, and others.

There are two places where you review reported risk events:

- **Azure AD reporting** - Risk events are part of Azure AD's security reports. For more information, see the [users at risk security report](#) and the [risky sign-ins security report](#).
- **Azure AD Identity Protection** - Risk events are also part of the reporting capabilities of [Azure Active Directory Identity Protection](#).

In addition, you can use the [Identity Protection risk events API](#) to gain programmatic access to security detections using Microsoft Graph.

Remediate these risks by manually addressing each reported account or by setting up a [user risk policy](#) to require a password change for these high risk events.

Penetration testing

Use Penetration Testing to validate security defenses.

Real world validation of security defenses is critical to validate your defense strategy and implementation. This can be accomplished by a penetration test (simulates a one time attack) or a red team program (simulates a persistent threat actor targeting your environment).

Follow the [guidance published by Microsoft](#) for planning and executing simulated attacks.

Discover & replace insecure protocols

Discover and disable the use of legacy insecure protocols SMBv1, LM/NTLMv1, wDigest, Unsigned LDAP Binds, and Weak ciphers in Kerberos.

Authentication protocols are a critical foundation of nearly all security assurances. These older versions can be exploited by attackers with access to your network and are often used extensively on legacy systems on Infrastructure as a Service (IaaS).

Here are ways to reduce your risk:

- **Discover** protocol usage by reviewing logs with Microsoft Sentinel's Insecure Protocol Dashboard or third party tools
- Restrict or Disable use of these protocols by following guidance for [SMB](#), [NTLM](#), [WDigest](#)

We recommend implementing changes using pilot or other testing method to mitigate risk of operational interruption.

Elevated security capabilities

Consider whether to utilize specialized security capabilities in your enterprise architecture.

These measures have the potential to enhance security and meet regulatory requirements, but can introduce complexity that may negatively impact your operations and efficiency.

We recommend careful consideration and judicious use of these security measures as required:

- **Dedicated Hardware Security Modules (HSMs)**
[Dedicated Hardware Security Modules \(HSMs\) may help meet regulatory or security requirements.](#)
- **Confidential Computing**
[Confidential Computing may help meet regulatory or security requirements](#).

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Governance, risk, and compliance capabilities

Article • 06/08/2022 • 2 minutes to read

This article lists capabilities that can help with governance, risk, and compliance. You can also learn more about these capabilities at [Azure governance documentation](#).

Capability	Description	More information
Microsoft 365 Defender portal	Microsoft 365 Defender portal provides security administrators and other risk management professionals with a centralized hub and specialized workspace that enables them to manage and take full advantage of Microsoft 365 intelligent security solutions for identity and access management, threat protection, information protection, and security management.	Microsoft 365 Defender portal
Microsoft Purview compliance portal	Microsoft Purview compliance portal provides easy access to the data and tools you need to manage your organization's compliance needs.	Microsoft Purview compliance portal
Microsoft Defender for Cloud	Microsoft Defender for Cloud is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.	Microsoft Defender for Cloud documentation
Management Groups	If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups.	Organize your resources with Azure management groups
Azure Policy	Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements.	Azure Policy documentation

Capability	Description	More information
Azure Blueprints	Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components -- such as networking -- to speed up development and delivery.	Azure Blueprints documentation

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Security operations

Article • 08/26/2022 • 2 minutes to read

Security operations monitor an enterprise environment to rapidly identify and remediate risk from active attack operations, sharing insights and threat intelligence from these attacks to the rest of the organization.

The following videos provide guidance on security operations.

Part 1: Introduction - SOC Learnings, Strategies, and Technical Integration (24:30 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuW?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuW?postJs||Msg=true)

Part 2: Azure Alerts (2:36 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7B?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7B?postJs||Msg=true)

Part 3: Alert and Log Ingestion (4:51 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3NI?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3NI?postJs||Msg=true)

Part 4: Journey to Cloud Analytics (6:05 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7C?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7C?postJs||Msg=true)

Part 5: Security Operations General Guidance (3:42 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qbMI?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qbMI?postJs||Msg=true)

Next steps

- See security operations [best practices](#) and [capabilities](#) for more information.
- Review the [PowerPoint slides](#) for the Microsoft Azure Security Compass Workshop.

See also

- Security operations functions from the Cloud Adoption Framework for Azure
- SOC Process Framework Workbook for Microsoft Sentinel ↗
- Additional security guidance from Microsoft

Key Microsoft security resources

Resource	Description
2021 Microsoft Digital Defense Report ↗	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic ↗ download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft cloud security for IT architects model ↗	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Microsoft security best practices for security operations

Article • 08/26/2022 • 7 minutes to read

Security operations (SecOps) maintain and restore the security assurances of the system as live adversaries attack it. The tasks of SecOps are described well by the NIST Cybersecurity Framework functions of Detect, Respond, and Recover.

- **Detect** - SecOps must detect the presence of adversaries in the system, who are incentivized to stay hidden in most cases as this allows them to achieve their objectives unimpeded. This can take the form of reacting to an alert of suspicious activity or proactively hunting for anomalous events in the enterprise activity logs.
- **Respond** – Upon detection of potential adversary action or campaign, SecOps must rapidly investigate to identify whether it is an actual attack (true positive) or a false alarm (false positive) and then enumerate the scope and goal of the adversary operation.
- **Recover** – The ultimate goal of SecOps is to preserve or restore the security assurances (confidentiality, integrity, availability) of business services during and after an attack.

The most significant security risk most organizations face is from human attack operators (of varying skill levels). This is because risk from automated/repeated attacks have been mitigated significantly for most organizations by signature and machine learning based approaches built into anti-malware (though there are notable exceptions like WannaCrypt and NotPetya, which moved faster than these defenses).

While human attack operators are challenging to face because of their adaptability (vs. automated/repeated logic), they are operating at the same “human speed” as defenders, which help level the playing field.

SecOps (sometimes referred to as a Security Operations Center (SOC)) has a critical role to play in limiting the time and access an attacker can get to valuable systems and data. Each minute that an attacker has in the environment allows them to continue to conduct attack operations and access sensitive or valuable systems.

Objective and metrics

The metrics you measure will have a significant effect on the behaviors and outcomes of SecOps. Focusing on the right measurements will help drive continuous improvement in

the right areas that meaningfully reduce risk.

To ensure that SecOps are effectively containing attackers access, the objectives should focus on:

- Reducing **time to acknowledge** an alert to ensure that detected adversaries are not ignored while defenders are spending time investigating false positives.
- Reducing **time to remediate** a discovered adversary to reduce their opportunity time to conduct and attack and reach sensitive systems
- **Prioritizing** security investments into systems that have high intrinsic value (likely targets or high business impact) and access to many systems or sensitive systems (administrator accounts and sensitive users)
- Increasing focus on **proactively hunting** for adversaries as your program matures and reactive incidents get under control. This is focused on reducing the time that a higher skilled adversary can operate in the environment (for example, skilled enough to evade reactive alerts).

For more information on how Microsoft's SOC uses these metrics, see

<https://aka.ms/ITSOC>.

Hybrid enterprise view

SecOps should ensure their tooling, processes, and analyst skill sets enable visibility across the full span of their hybrid estate.

Attackers don't restrict their actions to a particular environment when targeting an organization, they will attack resources on any platform using any method available. Enterprise organizations adopting cloud services like Azure and AWS are effectively operating a hybrid of cloud and on-premises assets.

SecOps tooling and processes should be designed for attacks on cloud and on-premises assets as well as attackers pivoting between cloud and on-premises resources using identity or other means. This enterprise-wide view will enable SecOps teams to rapidly detect, respond, and recover from attacks, reducing organizational risk.

Leverage native detections and controls

You should favor the use of security detections and controls built into the cloud platform before creating custom detections using event logs from the cloud.

Cloud platforms evolve rapidly with new features, which can make maintaining detections challenging. Native controls are maintained by the cloud provider and are typically high quality (low false positive rate).

Because many organizations may use multiple cloud platforms and need a unified view across the enterprise, you should ensure these native detections and controls feed a centralized SIEM or other tool. We don't recommend trying to substitute generalized log analysis tools and queries instead of native detections and controls. These tools can offer numerous values for proactive hunting activities but getting to a high-quality alert with these tools requires application of deep expertise and time that could be better spent on hunting and other activities.

To complement the broad visibility of a centralized SIEM (such as Microsoft Sentinel, Splunk, or QRadar), you should leverage native detections and controls such as:

- Organizations using Azure should leverage capabilities like Microsoft Defender for Cloud for alert generation on the Azure platform.
- Organizations should leverage native logging capabilities like Azure Monitor and AWS CloudTrail for pulling logs into a central view.
- Organizations using Azure should leverage Network Security Group (NSG) capabilities for visibility into network activities on the Azure platform.
- Investigation practices should leverage native tools with deep knowledge of the asset type such as an Endpoint Detection and Response (EDR) solution, identity tools, and Microsoft Sentinel.

Prioritize alert and log integration

Ensure that you are integrating critical security alerts and logs into SIEMs without introducing a high volume of low value data.

Introducing too much low-value data can increase SIEM cost, increase noise and false positives, and lower performance.

The data you collect should be focused on supporting one or more of these operations activities:

- **Alerts** (detections from existing tools or data required for generating custom alerts)
- **Investigation** of an incident (for example, required for common queries)

- Proactive **hunting** activities

Integrating more data can allow you to enrich alerts with additional context that enable rapid response and remediation (filter false positives, and elevate true positives, etc.), but collection is not detection. If you don't have a reasonable expectation that the data will provide value (for example, high volume of firewall denies events), you may deprioritize integration of these events.

SecOps resources for Microsoft security services

If you are new-to-role as a security analyst, see these resources to get you started.

Topic	Resource
SecOps planning for incident response	Incident response planning for preparing your organization for an incident.
SecOps incident response process	Incident response process for best practices on responding to an incident.
Incident response workflow	Example incident response workflow for Microsoft 365 Defender
Periodic security operations	Example periodic security operations for Microsoft 365 Defender
Investigation for Microsoft Sentinel	Incidents in Microsoft Sentinel
Investigation for Microsoft 365 Defender	Incidents in Microsoft 365 Defender

If you are an experienced security analyst, see these resources to quickly ramp up your SecOps team for Microsoft security services.

Topic	Resource
Azure Active Directory (Azure AD)	Security operations guide
Microsoft 365 Defender	Security operations guide
Microsoft Sentinel	How to investigate incidents
Microsoft 365 Defender	How to investigate incidents

Topic	Resource
Security operations establishment or modernization	Azure Cloud Adoption Framework articles for SecOps and SecOps functions
Incident response playbooks	Overview at https://aka.ms/IRplaybooks <ul style="list-style-type: none"> - Phishing - Password spray - App consent grant
SOC Process Framework	Microsoft Sentinel
MSTICPy and Jupyter Notebooks	Microsoft Sentinel

Blog series about SecOps within Microsoft

See this blog series about how the SecOps team at Microsoft works.

- [Part 1 – Organization: Mission and Culture](#)
- [Part 2a – People: Teams, Tiers, and Roles](#)
- [Part 2b – People: Careers and Readiness](#)
- [Part 3a – Technology: SOC Tooling](#)
- [Part 3b – Technology: Day in life of an analyst](#)
- [Part 3c – A day in the life part 2 - Microsoft Security](#)
- [Part 3d – Zen and the art of threat hunting](#)

Simuland

[Simuland](#) is an open-source initiative to deploy lab environments and end-to-end simulations that:

- Reproduce well-known techniques used in real attack scenarios.
- Actively test and verify the effectiveness of related Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel detections.
- Extend threat research using telemetry and forensic artifacts generated after each simulation exercise.

Simuland lab environments provide use cases from a variety of data sources including telemetry from Microsoft 365 Defender security products, Microsoft Defender for Cloud, and other integrated data sources through Microsoft Sentinel data connectors.

In the safety of a trial or paid sandbox subscription, you can:

- Understand the underlying behavior and functionality of adversary tradecraft.

- Identify mitigations and attacker paths by documenting preconditions for each attacker action.
- Expedite the design and deployment of threat research lab environments.
- Stay up to date with the latest techniques and tools used by real threat actors.
- Identify, document, and share relevant data sources to model and detect adversary actions.
- Validate and tune detection capabilities.

The learnings from Simuland lab environment scenarios can then be implemented in production.

After reading an overview of [Simuland](#), see the [Simuland GitHub repository](#).

Key Microsoft security resources

Resource	Description
2021 Microsoft Digital Defense Report	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft cloud security for IT architects model	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Next step

Review [security operations capabilities](#).

Security operations capabilities

Article • 02/01/2023 • 3 minutes to read

These are the capabilities that you can use for your security operations.

Capability	Description	More information
Microsoft Sentinel	A scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.	Microsoft Sentinel documentation
Microsoft Defender for Cloud	A unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as-on premises.	Microsoft Defender for Cloud documentation
Azure Active Directory (Azure AD) Identity Protection	Azure AD Identity Protection enables you to detect potential vulnerabilities affecting your organization's identities and configure automated remediation policy to low, medium, and high sign-in risk and user risk.	What is Azure Active Directory Identity Protection?
Microsoft Defender for Identity	A cloud-based security solution that leverages your on-premises Active Directory Domain Services signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Defender for Identity empowers SecOp analysts and security professionals to detect advanced attacks in hybrid environments.	Defender for Identity documentation
Microsoft Defender for Office 365	Safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.	Defender for Office 365 documentation
Microsoft Defender for Endpoint	An endpoint protection platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.	Defender for Endpoint documentation

Capability	Description	More information
Microsoft Defender for Cloud Apps	A cloud access security broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.	Microsoft Defender for Cloud Apps documentation
App governance add-on to Microsoft Defender for Cloud Apps	A security and policy management capability designed for OAuth-enabled apps that access Microsoft 365 data through Microsoft Graph APIs.	App governance add-on
Azure Monitor	Maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.	Azure Monitor documentation
Microsoft 365 Defender portal	Combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal. It includes information from Defender for Office 365, Defender for Endpoint, Defender for Identity, and Microsoft Defender for Cloud Apps for quick access to information, simpler layouts, and bringing related information together for easier alert detection, threat visibility, proactive hunting, and incident response.	Microsoft 365 Defender portal documentation

See also

- [Security operations functions from the Cloud Adoption Framework for Azure](#)
- [SOC Process Framework Workbook for Microsoft Sentinel ↗](#)
- [Azure AD security operations guide](#)
- [Microsoft 365 Defender security operations guide](#)

Key Microsoft security resources

Resource	Description
2021 Microsoft Digital Defense Report ↗	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.

Resource	Description
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic ↗ download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft cloud security for IT architects model ↗	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Incident response overview

Article • 02/01/2023 • 3 minutes to read

Incident response is the practice of investigating and remediating active attack campaigns on your organization. This is part of the [security operations \(SecOps\)](#) discipline and is primarily reactive in nature.

Incident response has the largest direct influence on the overall mean time to acknowledge (MTTA) and mean time to remediate (MTTR) that measure how well security operations are able to reduce organizational risk. Incident response teams heavily rely on good working relationships between threat hunting, intelligence, and incident management teams (if present) to actually reduce risk. See [SecOps metrics](#) for more information.

For more information on security operations roles and responsibilities, see [Cloud SOC functions](#).

New-to-role resources

If you're new-to-role as a security analyst, see these resources to get you started.

Topic	Resource
SecOps planning for incident response	Incident response planning for preparing your organization for an incident.
SecOps incident response process	Incident response process for best practices on responding to an incident.
Incident response workflow	Example incident response workflow for Microsoft 365 Defender
Periodic security operations	Example periodic security operations for Microsoft 365 Defender
Investigation for Microsoft Sentinel	Incidents in Microsoft Sentinel
Investigation for Microsoft 365 Defender	Incidents in Microsoft 365 Defender

Experienced security analyst resources

If you're an experienced security analyst, see these resources to quickly ramp up your SecOps team for Microsoft security services.

Topic	Resource
Microsoft Sentinel	How to investigate incidents
Microsoft Defender for Cloud (Azure resources)	How to investigate alerts
Microsoft 365 Defender	How to investigate incidents
Security operations establishment or modernization	Azure Cloud Adoption Framework articles for SecOps and SecOps functions
Microsoft security best practices	How to best use your SecOps center
Incident response playbooks	Overview at https://aka.ms/IRplaybooks - Phishing - Password spray - App consent grant
SOC Process Framework	Microsoft Sentinel
MSTICPy and Jupyter Notebooks	Microsoft Sentinel

Blog series about SecOps within Microsoft

See this blog series about how the SecOps team at Microsoft works.

- [Part 1 – Organization: Mission and Culture](#)
- [Part 2a – People: Teams, Tiers, and Roles](#)
- [Part 2b – People: Careers and Readiness](#)
- [Part 3a – Technology: SOC Tooling](#)
- [Part 3b – Technology: Day in life of an analyst](#)
- [Part 3c – A day in the life part 2 - Microsoft Security](#)
- [Part 3d – Zen and the art of threat hunting](#)

Simuland

[Simuland](#) is an open-source initiative to deploy lab environments and end-to-end simulations that:

- Reproduce well-known techniques used in real attack scenarios.

- Actively test and verify the effectiveness of related Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel detections.
- Extend threat research using telemetry and forensic artifacts generated after each simulation exercise.

Simuland lab environments provide use cases from a variety of data sources including telemetry from Microsoft 365 Defender security products, Microsoft Defender for Cloud, and other integrated data sources through Microsoft Sentinel data connectors.

In the safety of a trial or paid sandbox subscription, you can:

- Understand the underlying behavior and functionality of adversary tradecraft.
- Identify mitigations and attacker paths by documenting preconditions for each attacker action.
- Expedite the design and deployment of threat research lab environments.
- Stay up to date with the latest techniques and tools used by real threat actors.
- Identify, document, and share relevant data sources to model and detect adversary actions.
- Validate and tune detection capabilities.

The learnings from Simuland lab environment scenarios can then be implemented in your production environment and security processes.

See this overview of [Simuland](#) and the resources at the [Simuland GitHub repository](#).

Incident response resources

- [Planning](#) for your SOC
- [Process](#) for incident response process recommendations and best practices
- [Playbooks](#) for detailed guidance on responding to common attack methods
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Key Microsoft security resources

Resource	Description
2021 Microsoft Digital Defense Report	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.

Resource	Description
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic ↗ download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft security best practices for security operations	How to best use your SecOps center to move faster than the attackers targeting your organization.
Microsoft cloud security for IT architects model ↗	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Incident response planning

Article • 02/01/2023 • 7 minutes to read

Use this table as a checklist to prepare your Security Operations Center (SOC) to respond to cybersecurity incidents.

Done	Activity	Description	Benefit
<input type="checkbox"/>	Table top exercises	Conduct periodic table top exercises of foreseeable business-impacting cyber incidents that force your organization's management to contemplate difficult risk-based decisions.	Firmly establishes and illustrates cybersecurity as a business issue. Develops muscle memory and surfaces difficult decisions and decisions rights issues across the organization.

Done	Activity	Description	Benefit
<input type="checkbox"/>	Determine pre-attack decisions and decision-makers	<p>As a complement to table top exercises, determine risk-based decisions, criteria for making decisions, and who must make and execute those decisions.</p> <p>For example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Who/when/if to seek assistance from law enforcement? <input type="checkbox"/> Who/when/if to enlist incident responders? <input type="checkbox"/> Who/when/if to pay ransom? <input type="checkbox"/> Who/when/if to notify external auditors? <input type="checkbox"/> Who/when/if to notify privacy regulatory authorities? <input type="checkbox"/> Who/when/if to notify securities regulators? <input type="checkbox"/> Who/when/if to notify board of directors or audit committee? <input type="checkbox"/> Who has authority to shut down mission-critical workloads? 	Defines the initial response parameters and contacts to involve that streamline the response to an incident.
<input type="checkbox"/>	Maintaining privilege	Typically, advice can be privileged, but facts are discoverable. Train key incident leaders in communicating advice, facts and opinions under privilege so that privilege is preserved and risk is reduced.	Maintaining privilege can be a messy process when considering the multitude of communications channels, including e-mail, collaboration platforms, chats, documents, artifacts. For example, you can use Microsoft Teams Rooms . A consistent approach across incident personnel and supporting external organizations can help reduce any potential legal exposure.

Done	Activity	Description	Benefit
<input type="checkbox"/>	Insider trading considerations	Contemplate notifications to management that should be taken to reduce securities violations risk.	Boards and external auditors tend to appreciate that you have mitigations that will reduce the risk of questionable securities trades during periods of turbulence.
<input type="checkbox"/>	Incident roles and responsibilities playbook	<p>Establish basic roles and responsibilities that allow various processes to maintain focus and forward progress.</p> <p>When your response team is remote, it can require other considerations for time zones and proper handoff to investigators.</p> <p>You might have to communicate across other teams that might be involved, such as vendor teams.</p>	<p>Technical Incident Leader – Always in the incident, synthesizing inputs and findings and planning next actions.</p> <p>Communications Liaison – Removes the burden of communicating to management from the Technical Incident Leader so they can remain involved in the incident without loss of focus.</p> <p>This activity should include managing executive messaging and interactions with other third parties such as regulators.</p> <p>Incident Recorder – Removes the burden of recording findings, decisions, and actions from an incident responder and produces an accurate accounting of the incident from beginning to end.</p> <p>Forward Planner – Working with mission-critical business process owners, formulates business continuity activities and preparations that contemplate information system impairment that lasts for 24, 48, 72, 96 hours, or more.</p> <p>Public Relations – In the event of an incident that is likely to garner public attention, with Forward Planner, contemplates and drafts public communication approaches that address likely outcomes.</p>

Done	Activity	Description	Benefit
<input type="checkbox"/>	Privacy incident response playbook	To satisfy increasingly strict privacy regulations, develop a jointly owned playbook between SecOps and the privacy office. This playbook will allow rapid evaluation of potential privacy issues that might arise out of security incidents.	It's difficult to evaluate security incidents for their potential to impact privacy because most security incidents arise in a highly technical SOC. The incidents must quickly get surfaced to a privacy office (often with a 72-hour notification expectation) where regulatory risk is determined.
<input type="checkbox"/>	Penetration testing	Conduct point-in-time simulated attacks against business-critical systems, critical infrastructure, and backups to identify weaknesses in security posture. Typically, this activity is conducted by a team of external experts focused on bypassing preventative controls and surfacing key vulnerabilities.	In light of recent human-operated ransomware incidents, penetration testing should be conducted against an increased scope of infrastructure, particularly the ability to attack and control backups of mission-critical systems and data.
<input type="checkbox"/>	Red Team / Blue Team / Purple Team / Green Team	<p>Conduct continuous or periodic simulated attacks against business-critical systems, critical infrastructure, backups to identify weaknesses in security posture. Typically, this activity is conducted by internal attack teams (Red teams) who are focused on testing the effectiveness of detective controls and teams (Blue teams).</p> <p>For example, you can use Attack simulation training in Microsoft 365 Defender for Office 365 and Attack tutorials & simulations for Microsoft 365 Defender for Endpoint.</p>	<p>Red, Blue, and Purple team attack simulations, when done well, serve a multitude of purposes:</p> <ul style="list-style-type: none"> • Allows engineers from across the IT organization to simulate attacks on their own infrastructure disciplines. • Surfaces gaps in visibility and detection. • Raises the security engineering skills across the board. • Serves as a more continuous and expansive process. <p>The Green Team implements changes in IT or security configuration.</p>

Done	Activity	Description	Benefit
<input type="checkbox"/>	Business continuity planning	<p>For mission-critical business processes, design and test continuity processes that allow the minimum viable business to function during times of information systems impairment.</p> <p>For example, use an Azure backup and restore plan to protect your critical business systems during an attack to ensure a rapid recovery of your business operations.</p>	<ul style="list-style-type: none"> • Highlights the fact that there's no continuity workaround for the impairment or absence of IT systems. • Can emphasize the need and funding for sophisticated digital resilience over simpler backup and recovery.
<input type="checkbox"/>	Disaster recovery	<p>For information systems that support mission-critical business processes, you should design and test hot/cold and hot/warm backup and recovery scenarios, including staging times.</p>	<p>Organizations that conduct bare metal builds often find activities that are impossible to replicate or don't fit into the service level objectives.</p> <p>Mission-critical systems running on unsupported hardware many times can't be restored to modern hardware.</p> <p>Restore of backups is often not tested and experiences issues. Backups may be further offline such that staging times haven't been factored into recovery objectives.</p>
<input type="checkbox"/>	Out-of-band communications	<p>Prepare for how you would communicate in the the following scenarios:</p> <ul style="list-style-type: none"> • Email and collaboration service impairment • Ransom of documentation repositories • Unavailability of personnel phone numbers. 	<p>Although it's a difficult exercise, determine how to store important information immutably in off-line devices and locations for distribution at scale. For example:</p> <ul style="list-style-type: none"> • Phone numbers • Topologies • Build documents • IT restoration procedures

Done	Activity	Description	Benefit
<input type="checkbox"/>	Hardening, hygiene, and lifecycle management	In line with Center for Internet Security (CIS) Top 20 security controls, harden your infrastructure and perform thorough hygiene activities.	<p>In response to recent human-operated ransomware incidents, Microsoft has issued specific guidance for protecting every stage of the cyberattack kill chain. This guidance applies to Microsoft capabilities or the capabilities of other providers. Of particular note are:</p> <ul style="list-style-type: none"> • The creation and maintenance of immutable backup copies in the event of ransomed systems. You might also consider how to keep immutable log files that complicate the attacker's ability to cover their tracks. • Risks related to unsupported hardware for disaster recovery.
<input type="checkbox"/>	Incident response planning	<p>At the outset of the incident, decide on:</p> <ul style="list-style-type: none"> • Important organizational parameters. • Assignment of people to roles and responsibilities. • The sense-of-urgency (such as 24x7 and business hours). • Staff for sustainability for the duration. 	<p>There's a tendency to throw all available resources at an incident in the beginning, in the hope of a quick resolution. Once you recognize or anticipate that an incident will go for an extended period of time, take on a different posture that with your staff and suppliers that allows them to settle in for a longer haul.</p>

Done	Activity	Description	Benefit
<input type="checkbox"/>	Incident responders	<p>Establish clear expectations with one another. A popular format of reporting ongoing activities includes:</p> <ul style="list-style-type: none"> • What have we done (and what were the results)? • What are we doing (and what results will be produced and when)? • What do we plan to do next (and when is it realistic to expect results)? 	Incident responders come with different techniques and approaches, including dead box analysis, big data analysis, and the ability to produce incremental results. Starting with clear expectations will facilitate clear communications.

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Process](#) for incident response process recommendations and best practices
- [Playbooks](#) for detailed guidance on responding to common attack methods
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Key Microsoft security resources

Resource	Description
2021 Microsoft Digital Defense Report ↗	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic ↗ download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.

Resource	Description
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft security best practices for security operations	How to best use your SecOps center to move faster than the attackers targeting your organization.
Microsoft cloud security for IT architects model ↗	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Incident response process

Article • 02/01/2023 • 13 minutes to read

The first step is to have an incident response plan in place that encompasses both internal and external processes for responding to cybersecurity incidents. The plan should detail how your organization should:

- Address attacks that vary with the business risk and impact of the incident, which can vary from an isolated web site that is no longer available to the compromise of administrator-level credentials.
- Define the purpose of the response, such as a return to service or to handle legal or public relations aspects of the attack.
- Prioritize the work that needs to get done in terms of how many people should be working on the incident and their tasks.

See the [incident response planning article](#) for a checklist of activities you should consider including in your incident response plan. Once your incident response plan is in place, test it regularly for the most serious types of cyberattacks to ensure that your organization can respond quickly and efficiently.

Although each organization's incident response process may be different based on organizational structure and capabilities and historical experience, consider the set of recommendations and best practices in this article for responding to security incidents.

During an incident, it is critical to:

- Keep calm

Incidents are extremely disruptive and can become emotionally charged. Stay calm and focus on prioritizing your efforts on the most impactful actions first.

- Do no harm

Confirm that your response is designed and executed in a way that avoids loss of data, loss of business-critical functionality, and loss of evidence. Avoid decisions that can damage your ability to create forensic timelines, identify root cause, and learn critical lessons.

- Involve your legal department

Determine whether they plan to involve law enforcement so you can plan your investigation and recovery procedures appropriately.

- Be careful when sharing information about the incident publicly

Confirm that anything you share with your customers and the public is based on the advice of your legal department.

- Get help when needed

Tap into deep expertise and experience when investigating and responding to attacks from sophisticated attackers.

Like diagnosing and treating a medical disease, cybersecurity investigation and response for a major incident requires defending a system that is both:

- Critically important (can't be shut down to work on it).
- Complex (typically beyond the comprehension of any one person).

During an incident, you must strike these critical balances:

- Speed

Balance the need to act quickly to satisfy stakeholders with the risk of rushed decisions.

- Sharing information

Inform investigators, stakeholders, and customers based on the advice of your legal department to limit liability and avoid setting unrealistic expectations.

This article is designed to lower the risk to your organization for a cybersecurity incident by identifying common errors to avoid and providing guidance on what actions you can rapidly take that both reduce risk and meet stakeholder needs.

Note

For additional guidance on preparing your organization for ransomware and other types of multi-stage attacks, see [Prepare your recovery plan](#).

Response best practices

Responding to incidents can be done effectively from both technical and operations perspectives with these recommendations.

Note

For additional detailed industry guidance, see the [NIST Computer Security Incident Handling Guide](#).

Technical response best practices

For the technical aspects of incident response, here are some goals to consider:

- Try to identify the scope of the attack operation.

Most adversaries use multiple persistence mechanisms.

- Identify the objective of the attack, if possible.

Persistent attackers will frequently return for their objective (data/systems) in a future attack.

Here are some useful tips:

- Don't upload files to online scanners

Many adversaries monitor instance count on services like VirusTotal for discovery of targeted malware.

- Carefully consider modifications

Unless you face an imminent threat of losing business-critical data—such as deletion, encryption, and exfiltration—balance the risk of not making the modification with the projected business impact. For example, temporarily shutting down your organization's internet access may be necessary to protect business-critical assets during an active attack.

If changes are necessary where the risk of not doing an action is higher than the risk of doing it, document the action in a change log. Changes made during incident response are focused on disrupting the attacker and may impact the business adversely. You will need to roll these changes back after the recovery process.

- Don't investigate forever

You must ruthlessly prioritize your investigation efforts. For example, only perform forensic analysis on endpoints that attackers have actually used or modified. For example, in a major incident where an attacker has administrative privileges, it is practically impossible to investigate all potentially compromised resources (which may include all organization resources).

- Share information

Confirm that all investigation teams, including all internal teams and external investigators or insurance providers, are sharing their data with each other, based on the advice of your legal department.

- Access the right expertise

Confirm that you integrate people with deep knowledge of the systems into the investigation—such as internal staff or external entities like vendors—not just security generalists.

- Anticipate reduced response capability

Plan for 50% of your staff operating at 50% of normal capacity due to situational stress.

A key expectation to manage with stakeholders is that you may never be able to identify the initial attack because the data required for this may have been deleted before the investigation starts, such as an attacker covering their tracks by log rolling.

Operations response best practices

For security operations (SecOps) aspects of incident response, here are some goals to consider:

- Staying focused

Confirm you keep the focus on business-critical data, customer impact, and getting ready for remediation.

- Providing coordination and role clarity

Establish distinct roles for operations in support of the crisis team and confirm that technical, legal, and communications teams are keeping each other informed.

- Keeping your business perspective

You should always consider the impact on business operations by both adversary actions and your own response actions.

Here are some useful tips:

- Consider the [Incident Command System \(ICS\)](#) for crisis management

If you don't have a permanent organization that manages security incidents, we recommend using the ICS as a temporary organizational structure to manage the crisis.

- Keep ongoing daily operations intact

Ensure that normal SecOps are not completely sidelined to support incident investigations. This work still needs to be done.

- Avoid wasteful spending

Many major incidents result in the purchase of expensive security tools under pressure that are never deployed or used. If you can't deploy and use a tool during the investigation, which can include hiring and training for additional staff with the skill sets needed to operate the tool, defer acquisition until after you finish the investigation.

- Access deep expertise

Confirm you have the ability to escalate questions and issues to deep experts on critical platforms. This may require access to the operating system and application vendor for business-critical systems and enterprise-wide components such as desktops and servers.

- Establish information flows

Set clear guidance and expectations for the flow of information between senior incident response leaders and organization stakeholders. See [incident response planning](#) for more information.

Recovery best practices

Recovering from incidents can be done effectively from both technical and operations perspectives with these recommendations.

Technical recovery best practices

For the technical aspects of recovering from an incident, here are some goals to consider:

- Don't boil the ocean

Limit your response scope so that recovery operation can be executed within 24 hours or less. Plan a weekend to account for contingencies and corrective actions.

- Avoid distractions

Defer long-term security investments like implementing large and complex new security systems or replacing anti-malware solutions until after the recovery operation. Anything that does not have direct and immediate impact on the current recovery operation is a distraction.

Here are some helpful tips:

- Never reset all passwords at once

Password resets should focus first on known compromised accounts based on your investigation and are potentially administrator or service accounts. If warranted, user passwords should be reset only in a staged and controlled manner.

- Consolidate execution of recovery tasks

Unless you face an imminent threat of losing business-critical data, you should plan a consolidated operation to rapidly remediate all compromised resources (such as hosts and accounts) versus remediating compromised resources as you find them. Compressing this time window will make it difficult for attack operators to adapt and maintain persistence.

- Use existing tools

Research and use the capabilities of tools you have already deployed before trying to deploy and learn a new tool during a recovery.

- Avoid tipping off your adversary

As practical, you should take steps to limit the information available to adversaries about the recovery operation. Adversaries typically have access to all production data and email in a major cybersecurity incident. But in reality, most attackers don't have time to monitor all your communications.

Microsoft's Security Operations Center (SOC) has used a non-production Microsoft 365 tenant for secure communication and collaboration for members of the incident response team.

Operations recovery best practices

For the operations aspects of recovering from an incident, here are some goals to consider:

- Have a clear plan and limited scope

Work closely with your technical teams to build a clear plan with limited scope.

While plans may change based on adversary activity or new information, you should work diligently to limit scope expansion and taking on additional tasks.

- Have clear plan ownership

Recovery operations involve many people doing many different tasks at once, so designate a project lead for the operation for clear decision-making and definitive information to flow among the crisis team.

- Maintain stakeholder communications

Work with communication teams to provide timely updates and active expectation management for organizational stakeholders.

Here are some helpful tips:

- Know your capabilities and limits

Managing major security incidents is very challenging, very complex, and new to many professionals in the industry. You should consider bringing in expertise from external organizations or professional services if your teams are overwhelmed or aren't confident about what to do next.

- Capture the lessons learned

Build and continually improve role-specific handbooks for SecOps, even if it's your first incident without any written procedures.

Executive and board-level communications for incident response can be challenging if not practiced or anticipated. Make sure you have a communication plan to manage progress reporting and expectations for recovery.

Incident response process for SecOps

Consider this general guidance about the incident response process for your SecOps and staff.

1. Decide and act

After a threat detection tool such as Microsoft Sentinel or Microsoft 365 Defender detects a likely attack, it creates an incident. The Mean Time to Acknowledge (MTTA) measurement of SOC responsiveness begins with the time this attack is noticed by your security staff.

An analyst on shift is either delegated or takes ownership of the incident and performs an initial analysis. The timestamp for this is the end of the MTTA responsiveness measurement and begins the Mean Time to Remediate (MTTR) measurement.

As the analyst that owns the incident develops a high enough level of confidence that they understand the story and scope of the attack, they can quickly shift to planning and executing cleanup actions.

Depending on the nature and scope of the attack, your analysts can clean up attack artifacts as they go (such as emails, endpoints, and identities) or they may build a list of compromised resources to clean up all at once (known as a Big Bang)

- Clean as you go

For most typical incidents that are detected early in the attack operation, analysts can quickly clean up the artifacts as they find them. This puts the adversary at a disadvantage and prevents them from moving forward with the next stage of their attack.

- Prepare for a Big Bang

This approach is appropriate for a scenario where an adversary has already settled in and established redundant access mechanisms to your environment. This is frequently seen in customer incidents investigated by [Microsoft's Detection and Response Team \(DART\)](#). In this approach, analysts should avoid tipping off the adversary until full discovery of the attacker's presence, because surprise can help with fully disrupting their operation.

Microsoft has learned that partial remediation often tips off an adversary, which gives them a chance to react and rapidly make the incident worse. For example, the attacker can spread the attack further, change their access methods to evade detection, cover their tracks, and inflict data and system damage and destruction for revenge.

Cleaning up phishing and malicious emails can often be done without tipping off the attacker but cleaning up host malware and reclaiming control of accounts has a high chance of discovery.

These are not easy decisions to make and there is no substitute for experience in making these judgement calls. A collaborative work environment and culture in your SOC helps ensure that analysts can tap into each other's experience.

The specific response steps are dependent on the nature of the attack, but the most common procedures used by analysts can include:

- Client endpoints (devices)

Isolate the endpoint and contact the user or IT operations/helpdesk to initiate a reinstallation procedure.

- Server or applications

Work with IT operations and application owners to arrange rapid remediation of these resources.

- User accounts

Reclaim control by disabling the account and resetting password for compromised accounts. These procedures could evolve as your users transition to passwordless authentication using Windows Hello or another form of multi-factor authentication (MFA). A separate step is to expire all authentication tokens for the account with [Microsoft Defender for Cloud Apps](#).

Your analysts can also review the MFA method phone number and device enrollment to ensure it hasn't been hijacked by contacting the user and reset this information as needed.

- Service Accounts

Because of the high risk of service or business impact, your analysts should work with the service account owner of record, falling back on IT operations as needed, to arrange rapid remediation of these resources.

- Emails

Delete the attack or phishing email and sometimes clear them to prevent users from recovering deleted emails. Always save a copy of original email for later search for post-attack analysis, such as headers, content, and scripts or attachments.

- Other

You can execute custom actions based on the nature of the attack such as revoking application tokens and reconfiguring servers and services.

2. Post-incident cleanup

Because you don't benefit from learned lessons until you change future actions, always integrate any useful information learned from the investigation back into your SecOps.

Determine the connections between past and future incidents by the same threat actors or methods and capture these learnings to avoid repeating manual work and analysis delays in the future.

These learnings can take a number of forms, but common practices include analysis of:

- Indicators of Compromise (IoCs).

Record any applicable IoCs such as file hashes, malicious IP addresses, and email attributes into your SOC threat intelligence systems.

- Unknown or unpatched vulnerabilities.

Your analysts can initiate processes to ensure that missing security patches get applied, misconfigurations are corrected, and vendors (including Microsoft) are informed of "zero day" vulnerabilities so that they can create and distribute security patches.

- Internal actions such as enabling logging on assets covering your cloud-based and on-premises resources.

Review your existing security baselines and consider adding or changing security controls. For example, see the [Azure Active Directory security operations guide](#) for information on enabling the appropriate level of auditing in the directory before the next incident happens.

Review your response processes to identify and resolve any gaps found during the incident.

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your SOC
- [Playbooks](#) for detailed guidance on responding to common attack methods
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Key Microsoft security resources

Resource	Description
----------	-------------

Resource	Description
2021 Microsoft Digital Defense Report	A report that encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats.
Microsoft Cybersecurity Reference Architectures	A set of visual architecture diagrams that show Microsoft's cybersecurity capabilities and their integration with Microsoft cloud platforms such as Microsoft 365 and Microsoft Azure and third-party cloud platforms and apps.
Minutes matter infographic download	An overview of how Microsoft's SecOps team does incident response to mitigate ongoing attacks.
Azure Cloud Adoption Framework security operations	Strategic guidance for leaders establishing or modernizing a security operation function.
Microsoft security best practices for security operations	How to best use your SecOps center to move faster than the attackers targeting your organization.
Microsoft cloud security for IT architects model	Security across Microsoft cloud services and platforms for identity and device access, threat protection, and information protection.
Microsoft security documentation	Additional security guidance from Microsoft.

Incident response playbooks

Article • 08/26/2022 • 2 minutes to read

You need to respond quickly to detected security attacks to contain and remediate its damage. As new widespread cyberattacks happen, such as [Nobelium](#) and the [Exchange Server vulnerability](#), Microsoft will respond with detailed incident response guidance.

You also need detailed guidance for common attack methods that malicious users employ every day. To address this need, use incident response playbooks for these types of attacks:

- [Phishing](#)
- [Password spray](#)
- [App consent grant](#)
- [Compromised and malicious applications](#)

Each playbook includes:

- **Prerequisites:** The specific requirements you need to complete before starting the investigation. For example, logging that should be turned on and roles and permissions that are required.
- **Workflow:** The logical flow that you should follow to perform the investigation.
- **Checklist:** A list of tasks for the steps in the flow chart. This checklist can be helpful in highly-regulated environments to verify what you have done.
- **Investigation steps:** Detailed step-by-step guidance for the specific investigation.

Also see [Microsoft DART ransomware approach and best practices](#) for information about how the Microsoft Detection and Response Team (DART) deals with ransomware attacks.

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Phishing investigation

Article • 02/01/2023 • 23 minutes to read

This article provides guidance on identifying and investigating phishing attacks within your organization. The step-by-step instructions will help you take the required remedial action to protect information and minimize further risks.

This article contains the following sections:

- **Prerequisites:** Covers the specific requirements you need to complete before starting the investigation. For example, logging that should be turned on, roles and permissions required, among others.
- **Workflow:** Shows the logical flow that you should follow to perform this investigation.
- **Checklist:** Contains a list of tasks for each of the steps in the flow chart. This checklist can be helpful in highly regulated environments to verify what you have done or simply as a quality gate for yourself.
- **Investigation steps:** Includes a detailed step-by-step guidance for this specific investigation.

Prerequisites

Here are general settings and configurations you should complete before proceeding with the phishing investigation.

Account details

Before proceeding with the investigation, it is recommended that you have the user name, user principal name (UPN) or the email address of the account that you suspect is compromised.

Microsoft 365 base requirements

Verify auditing settings

Verify that *mailbox auditing on by default* is turned on by running the following command in [Exchange Online PowerShell](#):

PowerShell

```
Get-OrganizationConfig | Format-List AuditDisabled
```

The value **False** indicates that mailbox auditing is enabled for all mailboxes in the organization, regardless of the value of the *AuditEnabled* property on individual mailboxes. For more information, see [Verify mailbox auditing on by default is turned on](#).

Message trace

Message trace logs are invaluable components that help to find the original source of the message as well as the intended recipients. You can use the *message trace* functionality in Exchange admin center (EAC) at <https://admin.exchange.microsoft.com/#/messagetrace> or with the `Get-MessageTrace` cmdlet in Exchange Online PowerShell.

ⓘ Note

Message trace is also available in the Microsoft 365 Defender portal at <https://security.microsoft.com> under **Email & collaboration > Exchange message trace**, but that's just a passthrough link to message trace in the EAC.

Several components of the *message trace* functionality are self-explanatory but *Message-ID* is a unique identifier for an email message and requires thorough understanding. To get the *Message-ID* for an email of interest, you need to examine the raw email headers.

Audit log search

You search the [unified audit log](#) to view all the activities of the user and admin in your Microsoft 365 organization.

Are the sign-in logs and/or audit logs exported to an external system?

Since most of the Azure Active Directory (Azure AD) [sign-in](#) and audit data will get overwritten after 30 or 90 days, we recommend that you leverage Sentinel, Azure Monitor or an external security information and event management (SIEM) system.

Roles and permissions required

Permissions in Azure AD

We recommend membership in the following roles for the account that does the investigation:

- [Global Reader](#)
- [Security Reader](#)
- As a last resort, you can always fall back to the role of a [Global Administrator / Company Administrator](#)

Permissions in Microsoft 365

Generally speaking, the [Global Reader](#) or the [Security Reader](#) role groups in the Microsoft 365 Defender portal or the Microsoft Purview compliance portal should give you sufficient permissions to search the relevant logs.

Note

Accounts that are members of the [View-Only Audit Logs](#) or [Audit Logs](#) role groups only in the the Microsoft 365 Defender portal or the Microsoft Purview compliance portal won't be able to search the Microsoft 365 audit log. In this scenario, you must assign permissions in Exchange Online. For more information, see [Before you search the audit log](#).

if you're unsure about the role groups to use, see [Find the permissions required to run any Exchange cmdlet](#).

Microsoft Defender for Endpoint

If you have Microsoft Defender for Endpoint (MDE), you should leverage it for this flow. For more information, see [Tackling phishing with signal-sharing and machine learning](#).

System requirements

Hardware requirements

The system should be able to run PowerShell.

Software requirements

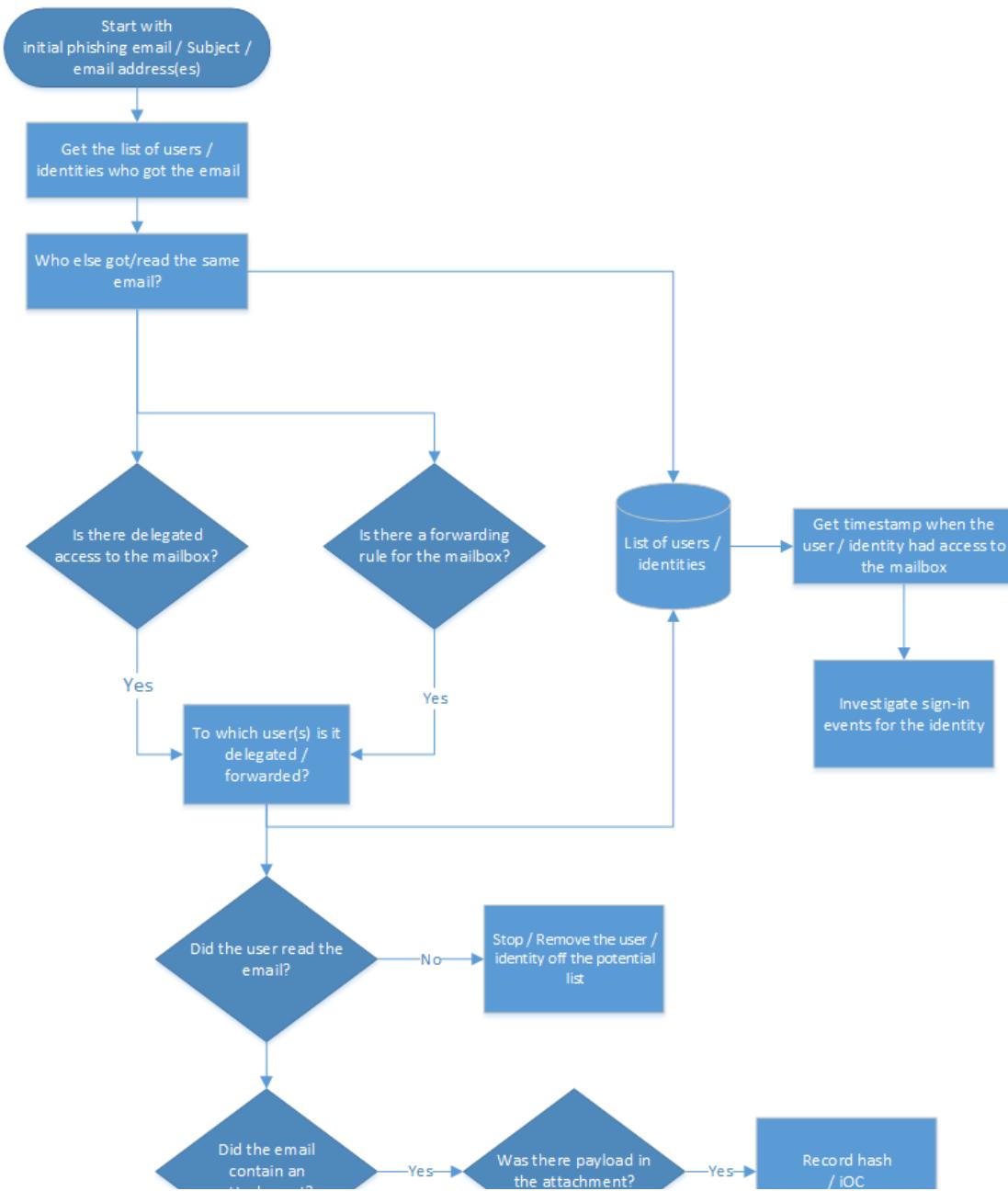
The following PowerShell modules are required for the investigation of the cloud environment:

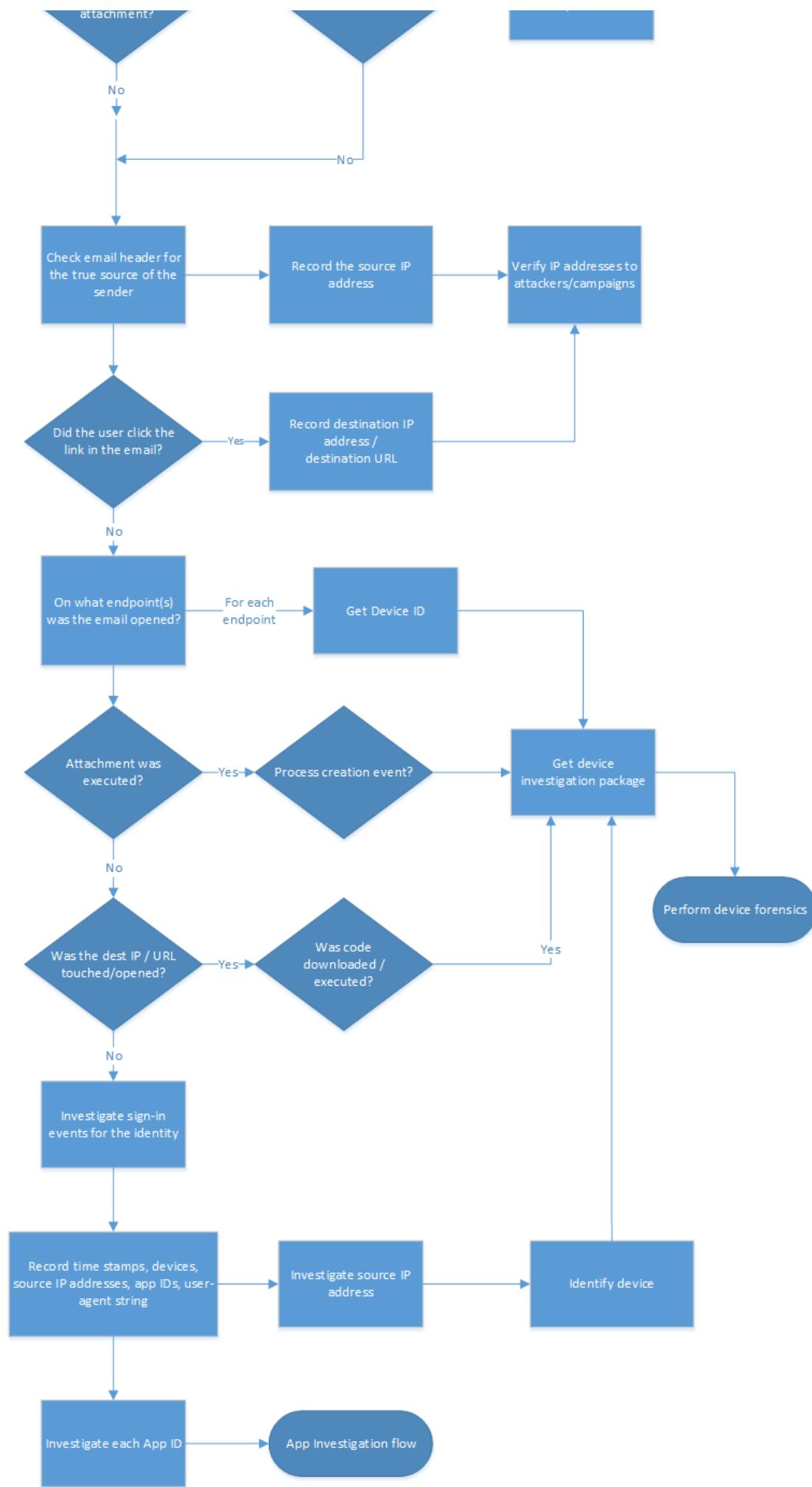
- Azure AD PowerShell for Graph module. For installation instructions, see [Install Azure Active Directory PowerShell for Graph](#).

If you need older cmdlets in the MSOnline (v1) Azure AD module, see [Azure Active Directory \(MSOnline\)](#).

- Exchange Online PowerShell module: For installation instructions, see [Install and maintain the Exchange Online PowerShell module](#).
- Azure AD Incident Response PowerShell module: For installation instructions, see [Azure AD Incident Response PowerShell Module](#)

Workflow





You can also:

- Download the phishing and other incident response playbook workflows as a [PDF ↗](#).
- Download the phishing and other incident response playbook workflows as a [Visio file ↗](#).

Checklist

This checklist will help you evaluate your investigation process and verify whether you have completed all the steps during investigation:

<input type="checkbox"/>	Review initial phishing email
<input type="checkbox"/>	Get the list of users who got this email
<input type="checkbox"/>	Get the latest dates when the user had access to the mailbox
<input type="checkbox"/>	Is delegated access configured on the mailbox?
<input type="checkbox"/>	Are there forwarding rules configured on the mailbox?
<input type="checkbox"/>	Review your Exchange mail flow rules (transport rules)
<input type="checkbox"/>	Find the email messages
<input type="checkbox"/>	Did the user read or open the email?
<input type="checkbox"/>	Who else got the same email?
<input type="checkbox"/>	Did the email contain an attachment?
<input type="checkbox"/>	Was there a payload in the attachment?
<input type="checkbox"/>	Check email header for true source of the sender
<input type="checkbox"/>	Verify IP addresses to attackers/campaigns
<input type="checkbox"/>	Did the user click links in the email?
<input type="checkbox"/>	On what endpoint was the email opened?
<input type="checkbox"/>	Was the attachment payload executed?
<input type="checkbox"/>	Was the destination IP or URL touched or opened?
<input type="checkbox"/>	Was malicious code executed?

- | |
|--|
| <input type="checkbox"/> What sign-ins happened with the account for the federated scenario? |
| <input type="checkbox"/> What sign-ins happened with the account for the managed scenario? |
| <input type="checkbox"/> Investigate the source IP address |
| <input type="checkbox"/> Investigate the device ID found |
| <input type="checkbox"/> Investigate each App ID |

You can also download the phishing and other incident playbook checklists as an [Excel file](#).

Investigation steps

For this investigation, it is assumed that you either have a sample phishing email, or parts of it like the sender's address, subject of the email, or parts of the message to start the investigation. Also make sure that you have completed / enabled all settings as recommended in the [Prerequisites](#) section.

This playbook is created with the intention that not all Microsoft customers and their investigation teams will have the full Microsoft 365 E5 or Azure AD Premium P2 license suite available or configured in the tenant that is being investigated. We will however highlight additional automation capabilities when appropriate.

Get the list of users / identities who got the email

As the very first step, you need to get a list of users / identities who received the phishing email. The objective of this step is to record a list of potential users / identities that you'll later use to iterate through for additional investigation steps. Refer to the [Workflow](#) section for a high-level flow diagram of the steps you need to follow during this investigation.

We do not give any recommendations in this playbook on how you want to record this list of potential users / identities. Depending on the size of the investigation, you can leverage an Excel book, a CSV file, or even a database for larger investigations. There are multiple ways to obtain the list of identities in a given tenant, and here are some examples.

Create a Content search in the Microsoft Purview compliance portal

Use the indicators that you've collected to create and run a Content search. For instructions, see [Create a content search](#).

For a full list of searchable email properties, see [searchable email properties](#).

The following example returns messages that were received by users between April 13, 2022 and April 14, 2022 and that contain the words "action" and "required" in the subject line:

```
SearchFilter  
  
(Received:4/13/2022..4/14/2022) AND (Subject:'Action required')
```

The following example query returns messages that were sent by `chatsuwloginsset12345@outlook.com` and that contain the exact phrase "*Update your account information*" in the subject line.

```
SearchFilter  
  
(From:chatsuwloginsset12345@outlook.com) AND (Subject:"Update your account information")
```

For more information, see how to [search for and delete messages in your organization](#).

Use the Search-Mailbox cmdlet in Exchange Online PowerShell

You can also use the **Search-Mailbox** cmdlet in [Exchange Online PowerShell](#) to perform a specific query against a target mailbox of interest and copy the results to an unrelated destination mailbox.

The following example query searches Jane Smith mailbox for an email that contains the phrase *Invoice* in the subject and copies the results to IRMailbox in a folder named "Investigation."

```
PowerShell  
  
Search-Mailbox -Identity "Jane Smith" -SearchQuery "Subject:Invoice" -  
TargetMailbox "IRMailbox" -TargetFolder "Investigation" LogLevel Full
```

In this example command, the query searches all tenant mailboxes for an email that contains the phrase "InvoiceUrgent" in the subject and copies the results to IRMailbox in a folder named "Investigation."

```
PowerShell
```

```
Get-Mailbox | Search-Mailbox -SearchQuery 'InvoiceUrgent vote' -  
TargetMailbox "IRMailbox" -TargetFolder "Investigation" -LogLevel Full
```

For detailed syntax and parameter information, see [Search-Mailbox](#).

Is delegated access configured on the mailbox?

Use the following script to check whether delegated access is configured on the mailbox: [https://github.com/OfficeDev/O365-
InvestigationTooling/blob/master/DumpDelegatesandForwardingRules.ps1](https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/DumpDelegatesandForwardingRules.ps1).

To create this report, run a small PowerShell script that gets a list of all your users. Then, use the Get-MailboxPermission cmdlet to create a CSV file of all the mailbox delegates in your tenancy.

Look for unusual names or permission grants. If you see something unusual, contact the mailbox owner to check whether it is legitimate.

Are there forwarding rules configured for the mailbox?

You need to check each identified mailbox for mailbox forwarding (also known as *SMTP forwarding*) or Inbox rules that forward email messages to external recipients (typically, newly-created Inbox rules).

- To check all mailboxes for mailbox forwarding, run the following command in [Exchange Online PowerShell](#):

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize unlimited |  
Format-Table -Auto  
MicrosoftOnlineServicesID,ForwardingSmtpAddress,DeliverToMailboxAndForw  
ard | Export-csv C:\Temp\Forwarding.csv -NoTypeInformation
```

- To check for Inbox rules that were created in mailboxes between the specified dates, run the following command in Exchange Online PowerShell:

PowerShell

```
Search-UnifiedAuditLog -StartDate 12/16/2021 -EndDate 03/16/2022 -  
ResultSize 5000 -RecordType exchangeadmin -Operations New-InboxRule |  
Export-csv NoTypeInformation -Path c:\temp\Inboxrulesoutput.csv
```

- You can also use the **Auto-forwarded messages** report in the Exchange admin center (EAC). For instructions, see [Auto forwarded messages report in Exchange Online](#).

Notes:

- Look for unusual target locations, or any kind of external addressing.
- Look for forwarding rules with unusual key words in the criteria such as *all mail with the word invoice in the subject*. Contact the mailbox owner to check whether it is legitimate.

Review Inbox rules

Check for the removal of Inbox rules, considering the timestamps in proximity to your investigation. As an example, use the following command in [Exchange Online PowerShell](#):

PowerShell

```
Search-UnifiedAuditLog -StartDate 12/16/2021 -EndDate 03/16/2022 -Operations Remove-InboxRule | Export-Csv NoTypeInformation -Path c:\temp\removedInboxRules.csv
```

Review Exchange mail flow rules (transport rules)

There are two ways to get the list of Exchange mail flow rules (also known as transport rules) in your organization:

1. In the Exchange admin center or Exchange Online PowerShell. For instructions, see [View or modify a mail flow rule](#).
2. The **Exchange transport rule** report in the Exchange admin center. For instructions, see [Exchange transport rule report in Exchange Online](#).

Look for new rules, or rules that have been modified to redirect the mail to external domains. The number of rules should be known and relatively small. You can do an audit log search to determine who created the rule and from where they created it. If you see something unusual, contact the creator to determine if it is legitimate.

Get the latest dates when the user had access to the mailbox

In the Microsoft 365 security & compliance center, navigate to [unified audit log](#). Under **Activities** in the drop-down list, you can filter by **Exchange Mailbox Activities**.

The capability to list compromised users is available in the [Microsoft 365 security & compliance center](#).

This report shows activities that could indicate a mailbox is being accessed illicitly. It includes created or received messages, moved or deleted messages, copied or purged messages, sent messages using send on behalf or send as, and all mailbox sign ins. The data includes date, IP address, user, activity performed, the item affected, and any extended details.

Note

For this data to be recorded, you must enable the **mailbox auditing** option.

The volume of data included here could be very substantial, so focus your search on users that would have high-impact if breached. Look for unusual patterns such as odd times of the day, or unusual IP addresses, and look for patterns such as high volumes of moves, purges, or deletes.

Did the user read / open the email?

There are two main cases here:

- The mailbox is in Exchange Online.
- The mailbox is in on-premises Exchange (Exchange hybrid).

Did the Exchange Online user open the email

Use the **Search-Mailbox** cmdlet in [Exchange Online PowerShell](#) to do a specific search query against a target mailbox of interest and copy the results to an unrelated destination mailbox.

The following example query searches Janes Smith's mailbox for an email that contains the phrase *Invoice* in the subject and copies the results to *IRMailbox* in a folder named *Investigation*.

PowerShell

```
Search-Mailbox -Identity "Jane Smith" -SearchQuery "Subject:Invoice" -  
TargetMailbox "IRMailbox" -TargetFolder "Investigation" LogLevel Full
```

The following sample query searches all tenant mailboxes for an email that contains the phrase *InvoiceUrgent* in the subject and copies the results to *IRMailbox* in a folder

named *Investigation*.

PowerShell

```
Get-Mailbox | Search-Mailbox -SearchQuery 'InvoiceUrgent vote' -  
TargetMailbox "IRMailbox" -TargetFolder "Investigation" -LogLevel Full
```

Did the user open the email in Exchange hybrid

Use the **Get-MessageTrackingLog** cmdlet to search for message delivery information stored in the message tracking log. Here's an example:

PowerShell

```
Get-MessageTrackingLog -Server Mailbox01 -Start "03/13/2022 09:00:00" -End  
"03/15/2022 17:00:00" -Sender "john@contoso.com"
```

For detailed syntax and parameter information, see [Get-MessageTrackingLog](#).

Who else got the same email?

There are two main cases here:

- The mailbox is in Exchange Online.
- The mailbox is in on-premises Exchange (Exchange hybrid).

The workflow is essentially the same as explained in the [Get the list of users / identities who got the email](#) section earlier in this article.

Find the email in Exchange Online

Use the **Search-Mailbox** cmdlet to perform a specific search query against a target mailbox of interest and copy the results to an unrelated destination mailbox.

This sample query searches all tenant mailboxes for an email that contains the subject *InvoiceUrgent* in the subject and copies the results to *IRMailbox* in a folder named *Investigation*.

PowerShell

```
Get-Mailbox | Search-Mailbox -SearchQuery "Subject:InvoiceUrgent" -  
TargetMailbox "IRMailbox" -TargetFolder "Investigation" -LogLevel Full
```

Find the email in on-premises Exchange

Use the **Get-MessageTrackingLog** cmdlet to search for message delivery information stored in the message tracking log. Here's an example:

```
PowerShell
```

```
Get-MessageTrackingLog -Server Mailbox01 -Start "03/13/2018 09:00:00" -End  
"03/15/2018 17:00:00" -MessageSubject "InvoiceUrgent"
```

For detailed syntax and parameter information, see [Get-MessageTrackingLog](#).

Did the email contain an attachment?

There are two main cases here:

- The mailbox is in Exchange Online.
- The mailbox is in on-premises Exchange (Exchange hybrid).

Find out if the message contained an attachment in Exchange Online

If the mailbox is in Exchange Online, you have two options:

- Use the classic **Search-Mailbox** cmdlet
- Use the **New-ComplianceSearch** cmdlet

Use the **Search-Mailbox** cmdlet to perform a specific search query against a target mailbox of interest and copy the results to an unrelated destination mailbox. Here's an example:

```
PowerShell
```

```
Get-Mailbox -ResultSize unlimited | Search-Mailbox -SearchQuery  
attachment:trojan* -TargetMailbox "IRMailbox" -TargetFolder "Investigation"  
-LogLevel Full
```

For detailed syntax and parameter information, see [Search-Mailbox](#).

The other option is to use the **New-ComplianceSearch** cmdlet. Here's an example:

```
PowerShell
```

```
New-ComplianceSearch -Name "Investigation" -ExchangeLocation "Research  
Department" -ContentMatchQuery "from:pilar@contoso.com AND
```

```
hasattachment:true"
```

For detailed syntax and parameter information, see [New-ComplianceSearch](#).

Find out if the message contained an attachment in on-premises Exchange

Note

In Exchange Server 2013, this procedure requires Cumulative Update 12 (CU12) or later. For more information, see [this article](#).

Use the **Search-Mailbox** cmdlet to search for message delivery information stored in the message tracking log. Here's an example:

PowerShell

```
Search-Mailbox -Identity "Jane Smith"-SearchQuery  
AttachmentNames:attachment_name -TargetMailbox "IRMailbox" -TargetFolder  
"Investigation" -LogLevel Full
```

For detailed syntax and parameter information, see [Search-Mailbox](#).

Was there a payload in the attachment?

Look for potential malicious content in the attachment. For example, PDF files, obfuscated PowerShell, or other script codes.

The **View data by Email > Malware** view in the **Threat protection status** report shows the number of incoming and outgoing messages that were detected as containing malware for your organization. For more information, see [Threat protection status report: View data by Email > Malware](#).

Check email header for true source of the sender

Many of the components of the message trace functionality are self-explanatory but you need to thoroughly understand about *Message-ID*. The *Message-ID* is a unique identifier for an email message.

To obtain the *Message-ID* for an email of interest, you need to examine the raw email headers. For instructions on how to do this in Microsoft Outlook or Outlook on the Web

(formerly known as Outlook Web App or OWA) see [View internet message headers in Outlook](#)

When viewing an email header, it is recommended to copy and paste the header information into an email header analyzer provided by [MXToolbox](#) or [Azure](#) for readability.

- **Headers Routing Information:** The routing information provides the route of an email as its being transferred between computers.
- **Sender Policy Framework (SPF):** An email validation to help prevent/detect spoofing. In the SPF record, you can determine which IP addresses and domains can send email on behalf of the domain.
- **SPF = Pass:** The SPF TXT record determined the sender is permitted to send on behalf of a domain.
 - SPF = Neutral
 - SPF = Fail: The policy configuration determines the outcome of the message Sender IP
 - SMTP Mail: Validate if this is a legitimate domain

For more information about SPF, see [How Microsoft 365 uses SPF to prevent spoofing](#)

- **Common Values:** Here is a breakdown of the most commonly used and viewed headers, and their values. This is valuable information and you can use them in the **Search** fields in Threat Explorer.
 - From address
 - Subject
 - Message ID
 - To address
 - Return-path address
- **Authentication-Results:** You can find what your email client authenticated when the email was sent. It will provide you with SPF and DKIM authentication.
- **Originating IP:** The original IP can be used to determine if the IP is blocklisted and to obtain the geo location.
- **Spam Confidence Level (SCL):** This determines the probability of an incoming email is spam.
 - -1: Bypass most spam filtering from a safe sender, safe recipient, or safe listed IP address (trusted partner)
 - 0, 1: Non-spam because the message was scanned and determined to be clean

- 5, 6: Spam
- 7, 8, 9: High confidence spam

The SPF record is stored within a DNS database and is bundled with the DNS lookup information. You can manually check the Sender Policy Framework (SPF) record for a domain by using the *nslookup* command:

1. Open the command prompt (**Start > Run > cmd**).
2. Type the command as: `nslookup -type=txt` a space, and then the domain/host name. For example:

DOS

```
nslookup -type=txt domainname.com
```

 **Note**

`-all` (reject or fail them - don't deliver the email if anything does not match), this is recommended.

Check if DKIM is enabled on your custom domains in Microsoft 365

You need to publish two CNAME records for every domain they want to add the domain keys identified mail (DKIM). See how to [use DKIM to validate outbound email sent from your custom domain](#).

Check for domain-based message authentication, reporting, and conformance (DMARC)

You can use this feature to [validate outbound email in Microsoft 365](#).

Verify IP addresses to attackers/campaigns

To verify or investigate IP addresses that have been identified from the previous investigation steps, you can use any of these options:

- VirusTotal
- Microsoft Defender for Endpoint
- Public Sources:

- [Ipinfo.io](#) - Has a free option to obtain geo-location
- [Censys.io](#) - Has a free option to obtain information about what their passive scans of the internet know
- [AbuseIPDB.com](#) - Has a free option that provides some geolocation
- Ask Bing and Google - Search on the IP address

URL reputation

You can use any Windows 10 device and Microsoft Edge browser which leverages the [SmartScreen](#) technology.

Here are a few third-party URL reputation examples

- [Trend Micro Site Safety Check](#)
- [Google Transparency Report](#)
- [Talos Intelligence](#)

As you investigate the IP addresses and URLs, look for and correlate IP addresses to indicators of compromise (IOCs) or other indicators, depending on the output or results and add them to a list of sources from the adversary.

Did the user click links in the email?

If the user has clicked the link in the email (on-purpose or not), then this action typically leads to a new process creation on the device itself. Depending on the device this was performed, you need perform device-specific investigations. For example, Windows vs Android vs iOS. In this article, we have described a general approach along with some details for Windows-based devices. If you are using Microsoft Defender for Endpoint (MDE), then you can also leverage it for iOS and soon Android.

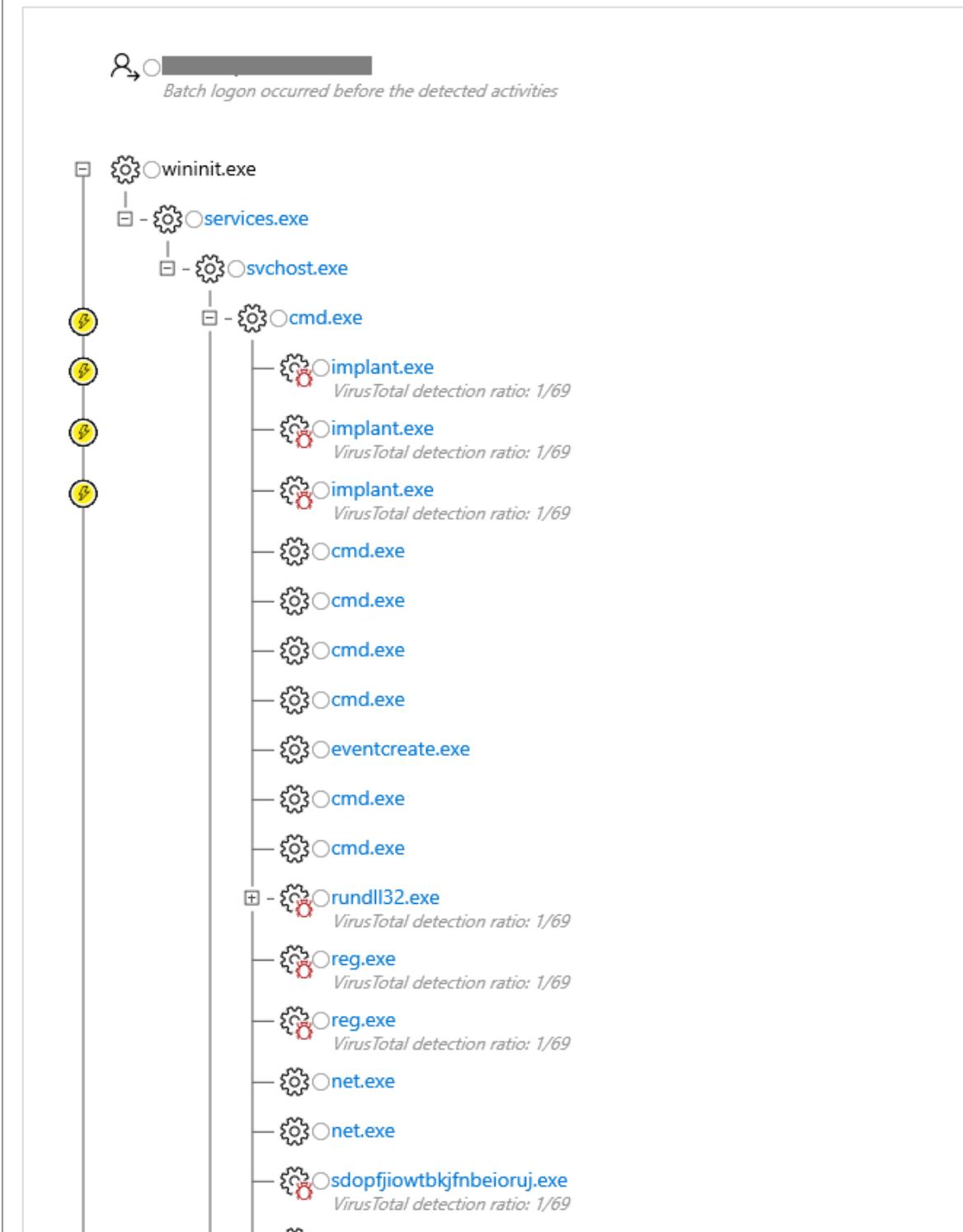
You can investigate these events using Microsoft Defender for Endpoint.

1. **VPN/proxy logs** Depending on the vendor of the proxy and VPN solutions, you need to check the relevant logs. Ideally you are forwarding the events to your SIEM or to Microsoft Sentinel.
2. **Using Microsoft Defender for Endpoint** This is the best-case scenario, because you can use our threat intelligence and automated analysis to help your investigation. For more details, see [how to investigate alerts in Microsoft Defender for Endpoint](#).

The **Alert process tree** takes alert triage and investigation to the next level, displaying the aggregated alerts and surrounding evidences that occurred within

the same execution context and time period.

Alert process tree



3. Windows-based client devices

Make sure you have enabled the [Process Creation Events](#) option. Ideally, you should also enable [command-line Tracing Events](#).

On Windows clients, which have the above-mentioned Audit Events enabled prior to the investigation, you can check Audit Event 4688 and determine the time when the email was delivered to the user:

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

Security ID:	SYSTEM
Account Name:	WIN-GG82ULGC9GOS
Account Domain:	CONTOSO
Logon ID:	0x8E7

Target Subject:

Security ID:	CONTOSO\dadmin
Account Name:	dadmin
Account Domain:	CONTOSO
Logon ID:	0x4A5AF0

Process Information:

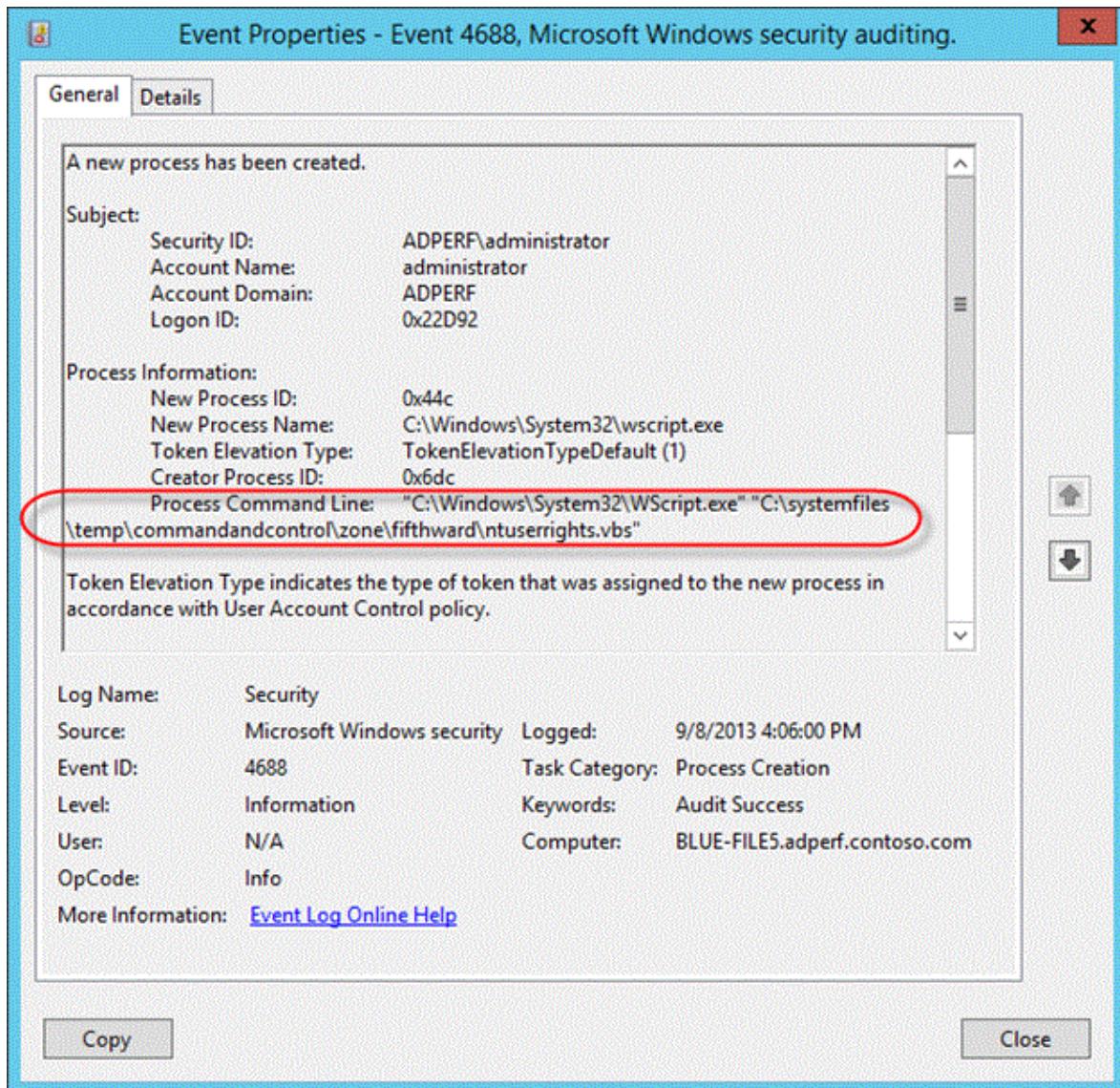
New Process ID:	0x2bc
New Process Name:	C:\Windows\System32\rundll32.exe
Token Elevation Type:	%&1938
Mandatory Label:	Mandatory Label\Medium Mandatory Level
Creator Process ID:	0xe74
Creator Process Name:	C:\Windows\explorer.exe
Process Command Line:	

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.



On what endpoint was the email opened?

The tasks here are similar to the previous investigation step: [Did the user click links in the email?](#)

Was the attached payload executed?

The tasks here are similar to the previous investigation step: [Did the user click links in the email?](#)

Was the destination IP / URL touched or opened?

The tasks here are similar to the previous investigation step: [Did the user click links in the email?](#)

Was malicious code executed?

The tasks here are similar to the previous investigation step: [Did the user click links in the email?](#)

What sign-ins happened with the account?

Check the various sign-ins that happened with the account.

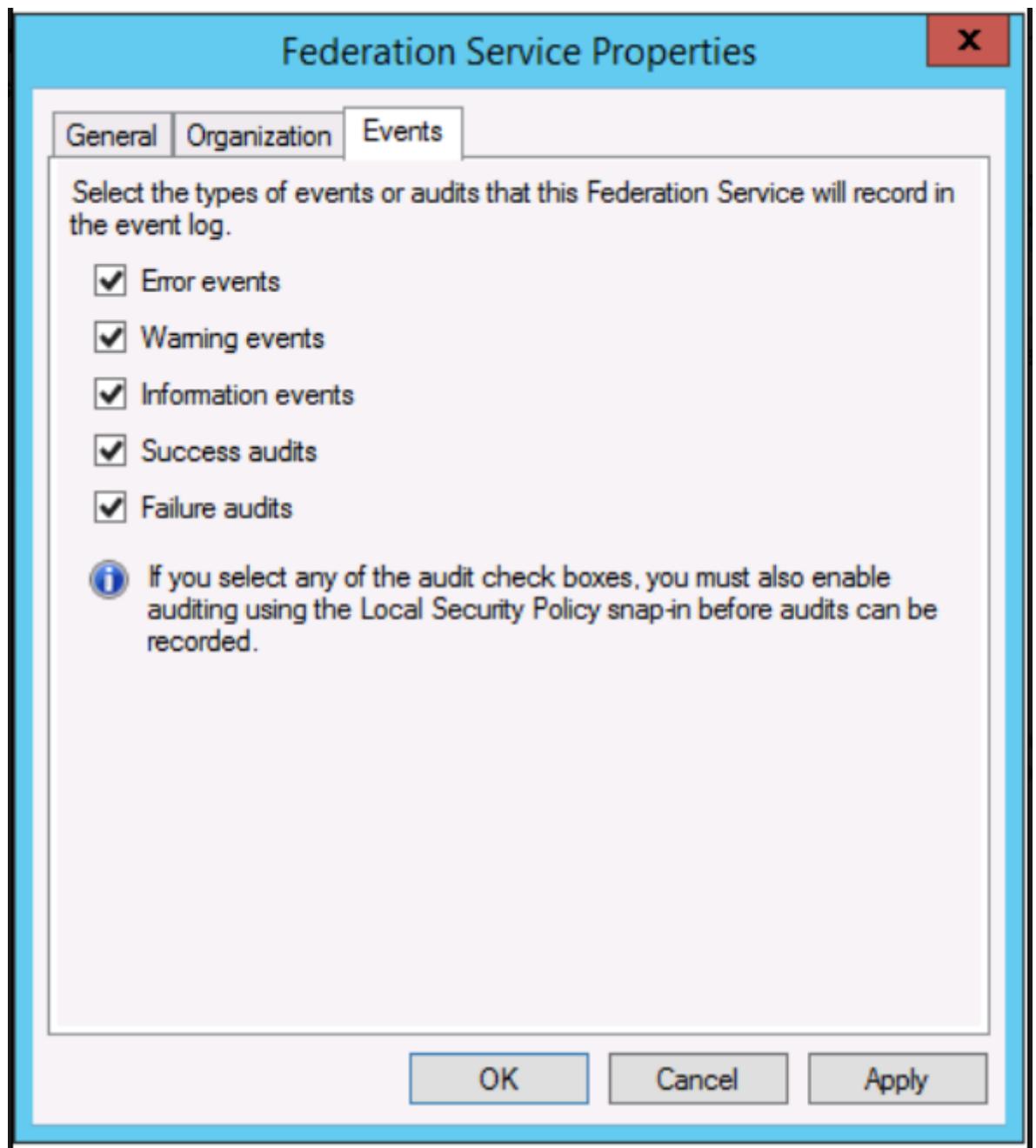
Federated scenario

The audit log settings and events differ based on the operating system (OS) Level and the Active Directory Federation Services (ADFS) Server version.

See the following sections for different server versions.

Server 2012 R2

By default, security events are not audited on Server 2012 R2. You need to enable this feature on each ADFS Server in the Farm. In the ADFS Management console and select **Edit Federation Service Properties**.



You also need to enable the OS Auditing Policy.

Open the command prompt, and run the following command as an administrator.

```
DOS
auditpol.exe /set /subcategory:"Application Generated" /failure:enable
/success:enable
```

For more details, see [how to configure ADFS servers for troubleshooting](#).

You may want to also download the ADFS PowerShell modules from:

- [GitHub ↗](#)
- [Microsoft scriptcenter ↗](#)

Server 2016 and newer

By default, ADFS in Windows Server 2016 has basic auditing enabled. With basic auditing, administrators can see five or less events for a single request. But you can raise or lower the auditing level by using this command:

PowerShell

```
Set-AdfsProperties -AuditLevel Verbose
```

For more details, see [auditing enhancements to ADFS in Windows server](#).

If you have Azure AD Connect Health installed, you should also look into the Risky IP report. The failed sign-in activity client IP addresses are aggregated through Web Application proxy servers. Each item in the Risky IP report shows aggregated information about failed AD FS sign-in activities that exceed the designated threshold.

TIMESTAMP	TRIGGER TYPE	IP ADDRESS	BAD PASSWORD ERROR COUNT	EXTRANET LOCKOUT ERROR COUNT	UNIQUE USERS ATTEMPTED
2/28/2018 6:00 PM	hour	104.208.238.9	0	284	14
2/28/2018 6:00 PM	hour	104.44.252.135	0	27	1
2/28/2018 6:00 PM	hour	168.61.144.85	0	164	2

For more details, see [Risky IP report](#).

Server 2012 R2

Event ID 342 – "The user name or password are incorrect" in the ADFS admin logs.

For the actual audit events, you need to look at the Security events logs and you should look for events with Event ID 411 for *Classic Audit Failure* with the source as *ADFS Auditing*. Also look for Event ID 412 on successful authentication.

Event ID 411 - *SecurityTokenValidationFailureAudit Token validation failed*. See inner exception for more details.

Event Properties - Event 411, AD FS Auditing

General Details

Token validation failed. See inner exception for more details.

Additional Data

Activity ID: c5f10b6a-c2c6-4ba5-2600-0080000000fb

Token Type: <http://schemas.microsoft.com/ws/2006/05/identitymodel/tokens/UserName>

Client IP: 67.170.69.0

Error message: ramical@rcdemos.net - The user name or password is incorrect

Exception details:

```
System.IdentityModel.Tokens.SecurityTokenValidationException: ramical@rcdemos.net --->
System.ComponentModel.Win32Exception: The user name or password is incorrect
   at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetLsaLogonUserHandle(SafeHGlobalHandle
pLogonInfo, Int32 logonInfoSize, SafeCloseHandle& tokenHandle, SafeLsaReturnBufferHandle& profileHandle)
   at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetLsaLogonUserInfo(SafeHGlobalHandle pLogonInfo,
Int32 logonInfoSize, DateTime& nextPasswordChange, DateTime& lastPasswordChange, String
authenticationType, String issuerName)
   at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetLsaLogonUser(String domain, String username,
String password, DateTime& nextPasswordChange, DateTime& lastPasswordChange, String issuerName)
   at Microsoft.IdentityServer.Service.LocalAccountStores.ActiveDirectory.ActiveDirectoryCpTrustStore.ValidateUser
(IAuthenticationContext context)
--- End of inner exception stack trace ---
   at Microsoft.IdentityServer.Service.LocalAccountStores.ActiveDirectory.ActiveDirectoryCpTrustStore.ValidateUser
```

Log Name: Security

Source: AD FS Auditing

Event ID: 411

Level: Information

User: [Redacted]

OpCode:

More Information: [Event Log Online Help](#)

Copy **Close**

Event 412, AD FS Auditing

General Details

A token of type '<http://schemas.microsoft.com/ws/2006/05/identitymodel/tokens/Kerberos>' for relying party '<http://adfs.salonovi.cz/adfs/services/trust>' was successfully authenticated. See audit 501 with the same Instance ID for caller identity.

Instance ID: cd1478d2-71e8-4090-9410-2cd35bb37668

Activity ID: 00000000-0000-0000-f55f-0080000000c1

Log Name: Security

Source: AD FS Auditing

Event ID: 412

Level: Information

Logged: 2/14/2016 4:23:34 PM

Task Category: (3)

Keywords: Classic,Audit Success

You may need to correlate the Event with the corresponding Event ID 501.

Server 2016 and newer

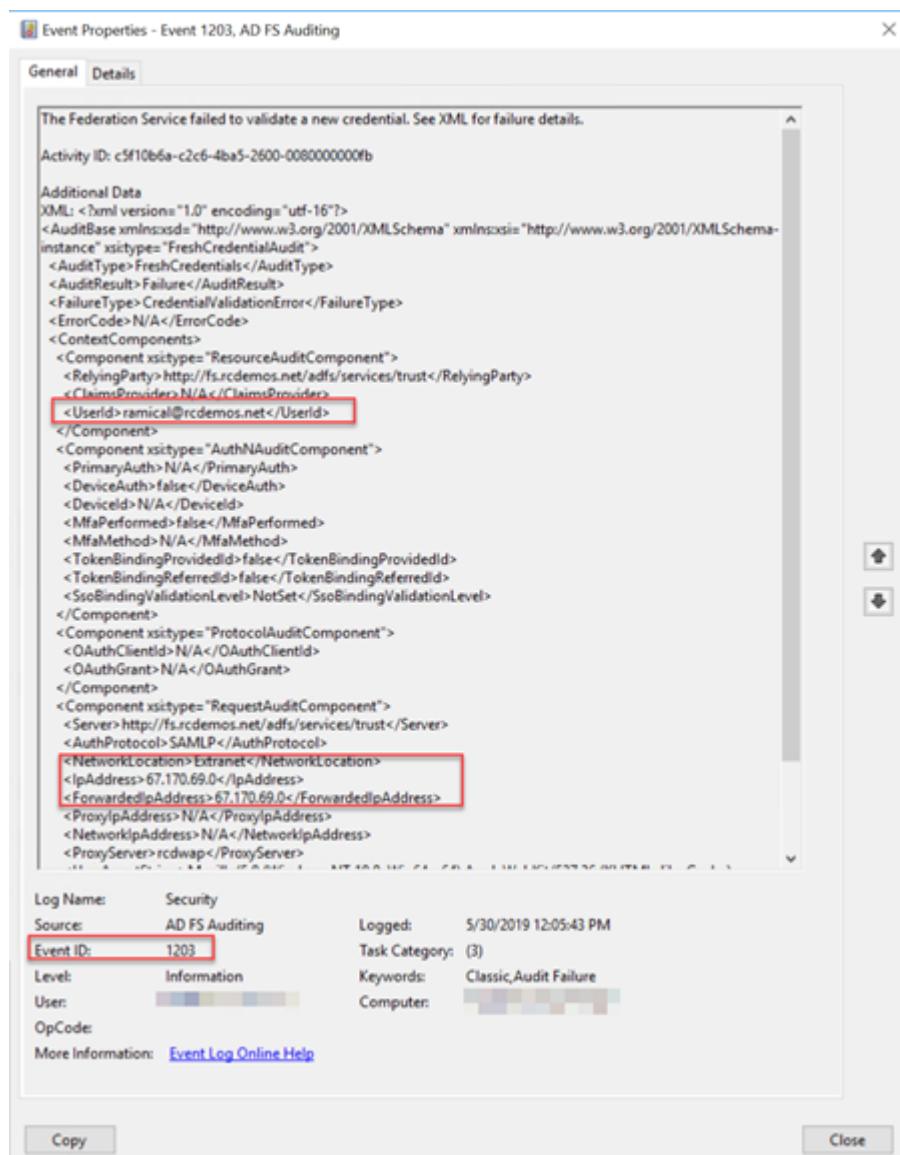
For the actual audit events you need to look at the security events logs and you should look for events with look for Event ID 1202 for successful authentication events and 1203 for failures

Example for Event ID1202:

Event ID 1202 FreshCredentialSuccessAudit The Federation Service validated a new credential. See XML for details.

Example for Event ID 1203:

Event ID 1203 FreshCredentialFailureAudit The Federation Service failed to validate a new credential. See XML for failure details.



An account was successfully logged on.

Subject:

Security ID:	AZURE\adfssrv
Account Name:	adfssrv
Account Domain:	AZURE
Logon ID:	0x5F2648

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	No

Impersonation Level: Identification

New Logon:

Security ID:	AZURE\leonardo
Account Name:	leonardo
Account Domain:	AZURE
Logon ID:	0xB68A5472
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	(d87e088d-9fef-c358-c040-fce6456b035b)

Process Information:

Process ID:	0xe2c
Process Name:	C:\Windows\ADFS\Microsoft.IdentityServer.ServiceHost.exe

Network Information:

Workstation Name:	ADFSFRACAS2016
Source Network Address:	-
Source Port:	-

Detailed Authentication Information:

Logon Process:	W
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

This event is generated when a logon session is created. It is generated on the computer that user accessed.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
Keywords: Audit Success
Logged: 3/4/2021 9:47:36 AM
Task Category: Logon
Computer: ADFSfracas2016.azure.int
More Information: [Event Log Online Help](#)

Copy **Close**

To get the full list of ADFS Event ID per OS Level, refer to [GetADFSEventList](#).

Managed scenario

Check the Azure AD sign-in logs for the user(s) you are investigating.

- Navigate to the [Azure AD portal](#) > [Sign-in](#) screen
- Check the [sign-in activities](#)
- Check the [PowerShell function on GitHub](#)

In the Azure AD portal, navigate to the [Sign-ins](#) screen and add/modify the display filter for the timeframe you found in the previous investigation steps as well as add the user name as a filter, as shown in this image.

Date	Request ID	User	Application	Status	IP address	Location	Conditional access	Authentication requirement
3/18/2021, 7:28:04 PM	H14d130-6446-4993-89df-8a05720069...	John Castro	Azure Advanced Threat Protection	Success	[REDACTED]	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 7:27:50 PM	bf8f246e-9175-4d4c-a327-a378c0991000	John Gardner	Azure Portal	Success	[REDACTED] 9.79	Redmond, Washington, US	Success	Multi-factor authentication
3/18/2021, 7:27:48 PM	7168b0d7-013f-40b0-88c5-620de11f12...	John Gardner	Azure Portal	Success	[REDACTED] 9.79	Redmond, Washington, US	Success	Multi-factor authentication
3/18/2021, 7:27:45 PM	61507a7-a07b-4b65-bfd4-ac175870700	John Gardner	Azure Portal	Interrupted	[REDACTED] 9.79	Redmond, Washington, US	Failure	Multi-factor authentication
3/18/2021, 6:27:58 PM	88d3d4c2-ffbc-4937-ab1d-f6ba61704400	John Castro	Azure Advanced Threat Protection	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:27:56 PM	59c17fc-271d-4efc-b4e9-09b3d304...	John Castro	Azure Advanced Threat Protection	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:16 PM	ad856c7-4203-4d02-9304-4361638210...	John Castro	Office365 Shell WCSS-Client	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:16 PM	b2bfb2bd-040c-428e-90d-532095a40...	John Castro	Office365 Shell WCSS-Client	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:15 PM	771af70e-6a2f-482b-b607-31db37a7c4...	John Castro	Office365 Shell WCSS-Client	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:06 PM	d393d47-ecb0-42e1-846-b6ab4fe62a2...	John Castro	Microsoft 365 Security and Compliance ...	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:25:55 PM	f0330206-2739-4002-b69f-1bb713607...	John Castro	Azure Portal	Success	[REDACTED] 121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:25:58 PM	718b1c57-f16b-4630-93ff-e0979016601	John Castro	Azure Portal	Interrupted	[REDACTED] 121	Mckinney, Texas, US	Failure	Multi-factor authentication

You can also search using Graph API. For example, filter on **User properties** and get **lastSignInDate** along with it. Search for a specific user to get the last signed in date for this user. For example, <https://graph.microsoft.com/beta/users?>

```
$filter=startswith(displayName,'Dhanyah')&$select=displayName,signInActivity
```

Or you can use the PowerShell command `Get-AzureADUserLastSignInActivity` to get the last interactive sign-in activity for the user, targeted by their object ID. This example writes the output to a date and time stamped CSV file in the execution directory.

PowerShell

```
Get-AzureADUserLastSignInActivity -TenantId 536279f6-1234-2567-be2d-61e352b51eeef -UserObjectId 69447235-0974-4af6-bfa3-d0e922a92048 -CsvOutput
```

Or you can use this command from the AzureADIncidentResponse PowerShell module:

PowerShell

```
Get-AzureADIRSignInDetail -UserId johcast@Contoso.com -TenantId 536279f6-1234-2567-be2d-61e352b51eeef -RangeFromDaysAgo 29 -RangeToDaysAgo 3
```

Investigate source IP address

Based on the source IP addresses that you found in the Azure AD sign-in logs or the ADFS/Federation Server log files, investigate further to know from where the traffic originated.

Managed user

For a managed scenario, you should start looking at the sign-in logs and filter based on the source IP address:

Date	Request ID	User	Application	Status	IP address	Location	Conditional access	Authentication requirement
3/18/2021, 7:28:04 PM	f414d130-6446-4993-89af-8a0572069000	John Castro	Azure Advanced Threat Protection	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:27:58 PM	38de4e4d-fbfe-4937-abf4-fdbab17e4000	John Castro	Azure Advanced Threat Protection	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:27:56 PM	59c1c75c-2764-4e2d-b4ac-c95ca8304000	John Castro	Azure Advanced Threat Protection	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:16 PM	a4d556c7-e203-4cb2-930d-4e36d8210700	John Castro	Office365 Shell WCSS-Client	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:16 PM	b2b12bae-040c-428a-904b-352893a624000	John Castro	Office365 Shell WCSS-Client	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:15 PM	771a7fe6-6a2f-482d-b6f7-31bd3a7e24000	John Castro	Office365 Shell WCSS-Client	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:26:06 PM	e395e47-rebc-42c3-84ec-0a4696a2e4000	John Castro	Microsoft 365 Security and Compliance C...	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:25:55 PM	f33302a6-c729-4b02-bb6f-0fb913607001	John Castro	Azure Portal	Success	67.11.183.121	Mckinney, Texas, US	Success	Multi-factor authentication
3/18/2021, 6:25:38 PM	718b1c67-f16b-4630-93ff-e0b979016601	John Castro	Azure Portal	Interrupted	67.11.183.121	Mckinney, Texas, US	Failure	Multi-factor authentication

Or you can use this command from the AzureADIncidentResponse PowerShell module:

PowerShell

```
Get-AzureADIRSignInDetail -IpAddress 1.2.3.4 -TenantId 536279f6-1234-2567-be2d-61e352b51eeef -RangeFromDaysAgo 29 -RangeToDaysAgo 3 -OutGridView
```

When you look into the results list, navigate to the **Device info** tab. Depending on the device used, you'll get varying output. Here are a few examples:

- Example 1 - Un-managed device (BYOD):

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Device ID						
Browser	Edge 88.0.705					
Operating System	Windows 10					
Compliant	No					
Managed	No					
Join Type						

- Example 2 - Managed device (Azure AD join or hybrid Azure AD join):

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Device ID		2d0bd589-90ca-429a-89b2-03153f390c47				
Browser	Chrome Mobile 88.0.4324					
Operating System	Android					
Compliant	No					
Managed	No					
Join Type	Azure AD registered					

Check for the DeviceID if one is present. You should also look for the OS and the browser or *UserAgent* string.

Basic info		Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Date	3/23/2021, 9:14:28 PM	User	Jing [REDACTED]				Token issuer type Azure AD
Request ID	fc73342f-621b-4ecd-8da9-bed8a3f82001	Username	[REDACTED]				Token issuer name
Correlation ID	2afc1be9-7207-4f7a-bbd1-521bf47feb73	User type	Member				Latency 135ms
Authentication requirement	Multi-factor authentication	User ID	360df853-0081-4b0d-af94-11dab1251fac				Flagged for review No
Status	Success	Sign-in identifier					
		Sign-in identifier type	proxyAddress				
		Application	Microsoft Teams Web Client				
		Application ID	5e3ce6c0-2b1f-4285-8d4b-75ee78787346				
		Resource					
		Resource ID					
		Resource tenant ID	536279f6-15cc-45f2-be2d-61e352b51eef				
		Home tenant ID	536279f6-15cc-45f2-be2d-61e352b51eef				
		Client app	Browser				
		User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 Edg/89.0.774.57				

Record the *CorrelationID*, *Request ID* and *timestamp*. You should use *CorrelationID* and *timestamp* to correlate your findings to other events.

Federated user/application

Follow the same procedure that is provided for [Federated sign-in scenario](#).

Look for and record the *DeviceID*, *OS Level*, *CorrelationID*, *RequestID*.

Investigate the identified DeviceID

This step is relevant for only those devices that are known to Azure AD. For example, from the previous steps, if you found one or more potential device IDs, then you can investigate further on this device. Look for and record the *DeviceID* and *Device Owner*.

Investigate each AppID

The starting point here are the sign-in logs and the app configuration of the tenant or the federation servers' configuration.

Managed scenario

From the previously found sign-in log details, check the *Application ID* under the **Basic info** tab:

Basic info						
Date	3/23/2021, 9:14:28 PM	User	Jing [REDACTED]	Token issuer type	Azure AD	
Request ID	fc73342f-621b-4ecd-8da9-bed8a3f82001	Username	[REDACTED]	Token issuer name		
Correlation ID	2afc1be9-7207-4f7a-bbd1-521bf47feb73	User type	Member	Latency	135ms	
Authentication requirement	Multi-factor authentication	User ID	360df853-0081-4b0d-af94-11dab1251fac	Flagged for review	No	
Status	Success	Sign-in identifier		User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 Edg/89.0.774.57	
		Sign-in identifier type	proxyAddress			
		Application	Microsoft Teams Web Client			
		Application ID	5e3ce6c0-2b1f-4285-8d4b-75ee78787346			
		Resource				
		Resource ID				
		Resource tenant ID	536279f6-15cc-45f2-be2d-61e352b51eef			
		Home tenant ID	536279f6-15cc-45f2-be2d-61e352b51eef			
		Client app	Browser			

Note the differences between the Application (and ID) to the Resource (and ID). The application is the client component involved, whereas the Resource is the service / application in Azure AD.

With this AppID, you can now perform research in the tenant. Here's an example:

```
PowerShell

Get-AzureADApplication -Filter "AppId eq '30d4cbf1-c561-454e-bf01-528cd5eaf58'"

ObjectId | AppId
| DisplayName

3af6dc4e-b0e5-45ec-8272-56f3f3f875ad    30d4cbf1-c561-454e-bf01-
528cd5eaf58          Claims X-Ray
```

With this information, you can search in the Enterprise Applications portal. Navigate to All Applications and search for the specific AppID.

The screenshot shows the 'Enterprise applications | All applications (Preview)' page. The search bar contains the AppID: 30d4cbf1-c561-454e-bf01-528cd5eaf58. The results table has columns: Name, Object ID, Application ID, and Homepage URL. The first result is 'Claims X-Ray' with Object ID 3af6dc4e-b0e5-45ec-8272-56f3f3f875ad and Application ID 30d4cbf1-c561-454e-bf01-528cd5eaf58. The Application ID column is highlighted with a red box.

Name	Object ID	Application ID	Homepage URL
Claims X-Ray	3af6dc4e-b0e5-45ec-8272-56f3f3f875ad	30d4cbf1-c561-454e-bf01-528cd5eaf58	https://account.activedirectory.windowsazure.com:44...

Additional incident response playbooks

Examine guidance for identifying and investigating these additional types of attacks:

- Password spray
- App consent
- Microsoft DART ransomware approach and best practices

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Password spray investigation

Article • 02/01/2023 • 19 minutes to read

This article provides guidance on identifying and investigating password spray attacks within your organization and take the required remedial action to protect information and minimize further risks.

This article contains the following sections:

- **Prerequisites:** Covers the specific requirements you need to complete before starting the investigation. For example, logging that should be turned on, roles and permissions required, among others.
- **Workflow:** Shows the logical flow that you should follow to perform this investigation.
- **Checklist:** Contains a list of tasks for each of the steps in the flow chart. This checklist can be helpful in highly regulated environments to verify what you have done or simply as a quality gate for yourself.
- **Investigation steps:** Includes a detailed step-by-step guidance for this specific investigation.
- **Recovery:** Contains high-level steps on how to recover/mitigate from a password spray attack.
- **References:** Contains additional reading and reference materials.

Prerequisites

Before starting the investigation, make sure you have completed the setup for logs and alerts and additional system requirements.

For Azure AD monitoring follow our recommendations and guidance in our [Azure AD SecOps Guide](#).

Set up ADFS logging

Event logging on ADFS 2016

By default, the Microsoft Active Directory Federation Services (ADFS) in Windows Server 2016 has a basic level of auditing enabled. With basic auditing, administrators can see five or less events for a single request. Set logging to the highest level and send the AD FS (& security) logs to a SIEM to correlate with AD authentication as well as Azure AD.

To view the current auditing level, you can use this PowerShell command:

```
PowerShell

Get-AdfsProperties
```



```
PS C:\Users\Administrator> Get-AdfsProperties

AcceptableIdentifiers : {}
AddProxyAuthorizationRules : []
AuditLevel : {Basic}
AutoCertificateRollover : True
CertificateCriticalThreshold : 2
CertificateDuration : 365
AuthenticationContextOrder : {urn:oasis:names:tc:SAML:2.0:ac:classes:Password, urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, urn:oasis:names:tc:SAML:2.0:ac:classes:X509...}
ArtifactDbConnection : Data Source=np:\\.\pipe\microsoft##widtsql\query;Initial Catalog=AdfsArtifactStore;Integrated Security=True
AuthenticContextOrder : {urn:oasis:names:tc:SAML:2.0:ac:classes:Password, urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, urn:oasis:names:tc:SAML:2.0:ac:classes:X509...}
```

This table contains the auditing levels that are available.

Audit level	PowerShell syntax	Description
None	<code>Set-AdfsProperties -AuditLevel None</code>	Auditing is disabled and no events will be logged
Basic (Default)	<code>Set-AdfsProperties -AuditLevel Basic</code>	No more than 5 events will be logged for a single request
Verbose	<code>Set-AdfsProperties -AuditLevel Verbose</code>	All events will be logged. This will log a significant amount of information per request.

To raise or lower the auditing level, use this PowerShell command:

```
PowerShell

Set-AdfsProperties -AuditLevel <None | Basic | Verbose>
```

Set up ADFS 2012 R2/2016/2019 security logging

1. Click Start, navigate to Programs > Administrative Tools, and then click Local Security Policy.
2. Navigate to the Security Settings\Local Policies\User Rights Management folder, and then double-click Generate security audits.

3. On the **Local Security Setting** tab, verify that the ADFS service account is listed. If it is not present, click **Add User or Group** and add it to the list, and then click **OK**.
4. To enable auditing, open a command prompt with elevated privileges and run the following command:

DOS

```
auditpol.exe /set /subcategory:"Application Generated" /failure:enable  
/success:enable
```

5. Close Local Security Policy.
6. Next, open the ADFS Management snap-in, click **Start**, navigate to **Programs > Administrative Tools**, and then click **ADFS Management**.
7. In the Actions pane, click **Edit Federation Service Properties**.
8. In the **Federation Service Properties** dialog box, click the **Events** tab.
9. Select the **Success audits** and **Failure audits** check boxes.
10. Click **OK** to finish and save the configuration.

Install Azure AD Connect Health for ADFS

The Azure Active Directory (Azure AD) Connect Health for ADFS agent allows you to have greater visibility into your federation environment. It provides you with several pre-configured dashboards like usage, performance monitoring as well as risky IP reports.

To install ADFS Connect Health, go through the [requirements for using Azure AD Connect Health](#), and then install the [Azure ADFS Connect Health Agent](#).

Set up risky IP alerts using the [ADFS Risky IP Report Workbook](#)

After Azure AD Connect Health for ADFS is configured, you should monitor and set up alerting using the ADFS Risky IP report workbook and Azure Monitor. The benefits of using this report are:

- Detection of IP addresses that exceed a threshold of failed password-based logins.
- Supports failed logins due to bad password or due to extranet lockout state.
- Supports enabling alerts through Azure Alerts.

- Customizable threshold settings that match with the security policy of an organization.
- Customizable queries and expanded visualizations for further analysis.
- Expanded functionality from the previous Risky IP report, which will be deprecated after January 24, 2022.

Set up SIEM tool alerts on Microsoft Sentinel

To set up SIEM tool alerts, go through the tutorial on [out of the box alerting](#).

SIEM integration into Microsoft Defender for Cloud Apps

Connect the Security Information and Event Management (SIEM) tool to Microsoft Defender for Cloud Apps, which currently supports Micro Focus ArcSight and generic common event format (CEF).

For more information, see [Generic SIEM Integration](#).

SIEM integration with Graph API

You can connect SIEM with the Microsoft Graph Security API by using any of the following options:

- **Directly using the supported integration options** – Refer to the list of supported integration options like writing code to directly connect your application to derive rich insights. Leverage samples to get started.
- **Use native integrations and connectors built by Microsoft partners** – Refer to the Microsoft Graph Security API partner solutions to use these integrations.
- **Use connectors built by Microsoft** – Refer to the list of connectors that you can use to connect with the API through a variety of solutions for Security Incident and Event Management (SIEM), Security Response and Orchestration (SOAR), Incident Tracking and Service Management (ITSM), reporting, and so on.

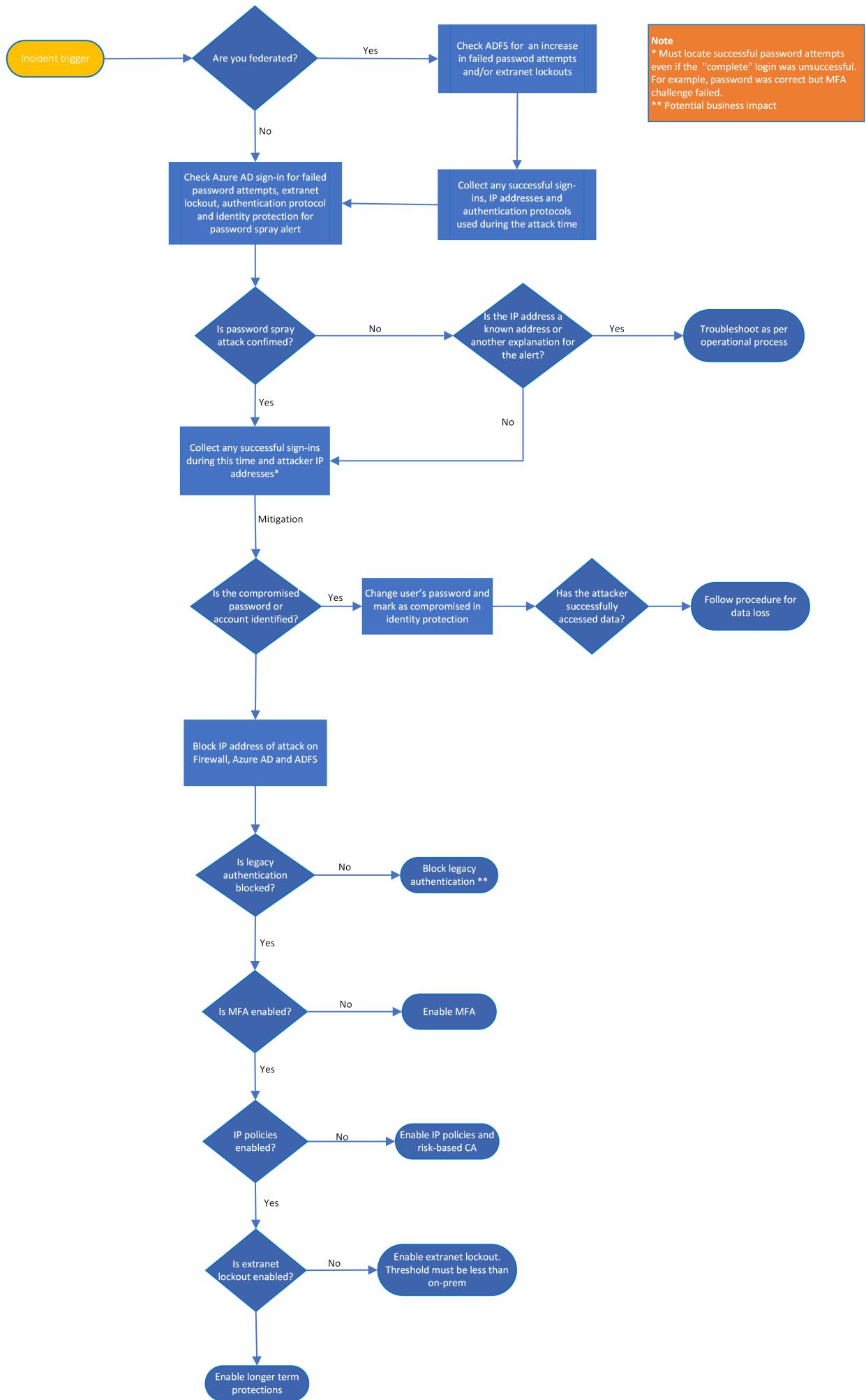
For more information, see [security solution integrations using the Microsoft Graph Security API](#).

Using Splunk

You can also use the Splunk platform to set up alerts.

- Watch this video tutorial on how to create [Splunk alerts ↗](#)
- For more information, see [Splunk alerting manual ↗](#)

Workflow



You can also:

- Download the password spray and other incident response playbook workflows as a [PDF](#).
- Download the password spray and other incident response playbook workflows as a [Visio file](#).

Checklist

Investigation triggers

- Received a trigger from SIEM, firewall logs, or Azure AD
- Azure AD Identity Protection Password Spray feature or Risky IP
- Large number of failed sign-ins (Event ID 411)
- Spike in Azure AD Connect Health for ADFS
- Another security incident (for example, phishing)
- Unexplained activity, such as a sign-in from unfamiliar location or a user getting unexpected MFA prompts

Investigation

- What is being alerted?
- Can you confirm this is a password spray?
- Determine timeline for attack.
- Determine the IP address(es) of the attack.
- Filter on successful sign-ins for this time period and IP address, including successful password but failed MFA
- Check [MFA reporting](#)
- Is there anything out of the ordinary on the account, such as new device, new OS, new IP address used? Use Defender for Cloud Apps or Azure Information Protection to detect suspicious activity.
- Inform local authorities/third parties for assistance.
- If you suspect a compromise, check for data exfiltration.
- Check associated account for suspicious behavior and look to correlate to other possible accounts and services as well as other malicious IP addresses.
- Check accounts of anyone working in the same office/delegated access - password hygiene (make sure they are not using the same password as the compromised account)
- Run ADFS help

Mitigations

Check the [References](#) section for guidance on how to enable features.

- [Block IP address of attacker](#) (keep an eye out for changes to another IP address)
- Changed user's password or suspected compromise
- [Enable ADFS Extranet Lockout](#)
- [Disabled Legacy authentication](#)
- [Enabled Azure Identity Protection](#) (sign in and user risk policies)
- [Enabled MFA](#) (if not already)
- [Enabled Password Protection](#)
- [Deploy Azure AD Connect Health for ADFS](#) (if not already)

Recovery

- Tag bad IP address in Defender for Cloud Apps, SIEM, ADFS and Azure AD
- Check for other forms of mailbox persistence such as forwarding rules or additional delegations added
- [MFA as primary authentication](#)
- [Configure SIEM integrations with Cloud](#)
- Configure Alerting - Identity Protection, ADFS Health Connect, SIEM and Defender for Cloud Apps
- Lessons Learnt (include key stakeholders, third parties, communication teams)
- Security posture review/improvements
- [Plan to run regular attack simulators](#)

You can also download the password spray and other incident playbook checklists as an [Excel file ↗](#).

Investigation steps

Password spray incident response

Let's understand a few password spray attack techniques before proceeding with the investigation.

Password compromise: An attacker has successfully guessed the user's password but has not been able to access the account due to other controls such as multi-factor authentication (MFA).

Account compromise: An attacker has successfully guessed the user's password and has successfully gained access to the account.

Environment discovery

Identify authentication type

As the very first step, you need to check what authentication type is used for a tenant/verified domain that you are investigating.

To obtain the authentication status for a specific domain name, use the [Get-MsolDomain](#) PowerShell command. Here's an example:

```
PowerShell
```

```
Connect-MsolService  
Get-MsolDomain -DomainName "contoso.com"
```

Is the authentication federated or managed?

If the authentication is federated, then successful sign-ins will be stored in Azure AD. The failed sign-ins will be in their Identity Provider (IDP). For more information, see [ADFS troubleshooting and event logging](#).

If the authentication type is managed, (Cloud only, password hash sync (PHS) or pass-through authentication (PTA)), then successful and failed sign-ins will be stored in the Azure AD sign-in logs.

 Note

The **Staged Rollout** feature allows the tenant domain name to be federated but specific users to be managed. Determine if any users are members of this group.

Is Azure AD Connect Health enabled for ADFS?

- The [RiskyIP report](#) will provide suspect IPs and date/time. Notifications should be enabled.
- Also check the [federated sign-ins investigation from the Phishing playbook](#)

Is the advanced logging enabled in ADFS?

- This is a requirement for ADFS Connect Health but it can be enabled independently
- See how to [enable ADFS Health Connect](#))
- Also check the [Federated sign-ins investigation from the Phishing playbook](#)

Are the logs stored in SIEM?

To check whether you are storing and correlating logs in a Security Information and Event Management (SIEM) or in any other system, check the following:

- Log analytics- pre-built queries
- Sentinel- pre-built queries
- Splunk – pre-built queries
- Firewall logs
- UAL if > 30 days

Understanding Azure AD and MFA reporting

It is important that you understand the logs that you are seeing to be able to determine compromise. Below are our quick guides to understanding Azure AD Sign-Ins and MFA reporting to help with this. Refer to these articles:

- [MFA reporting](#)
- [Understanding Sign Ins](#)

Incident triggers

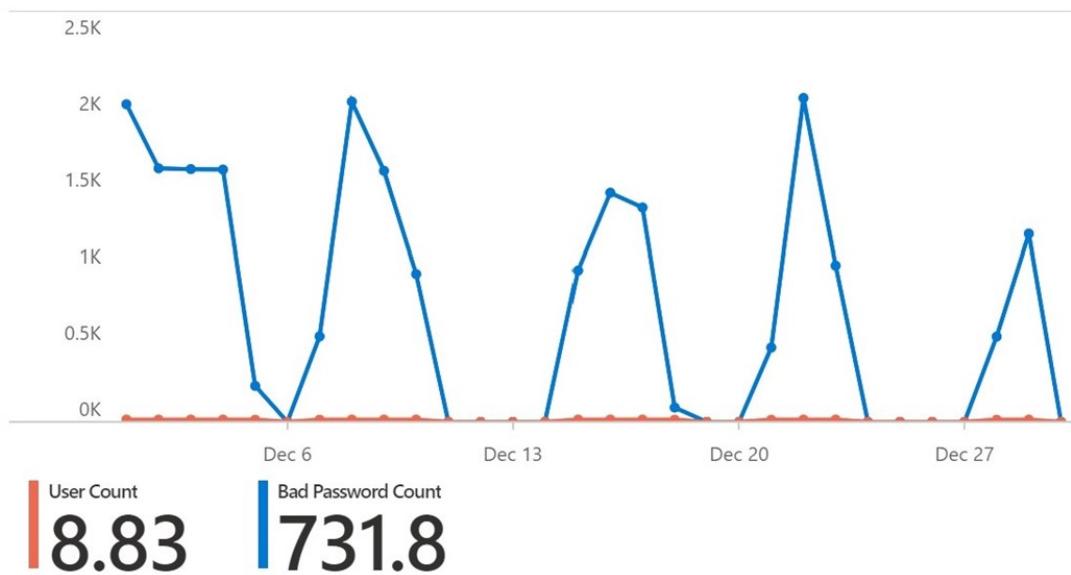
An incident trigger is an event or a series of events that causes predefined alert to trigger. An example of this is the number of bad password attempts has gone above your predefined threshold. Below are further examples of triggers that can be alerted in password spray attacks and where these alerts are surfaced. Incident triggers include:

- Users
- IP
- User agent strings
- Date/time
- Anomalies
- Bad password attempts

Bad Password Attempts

adfs: https://adfs.onmicrosoft.com/.net

From last 30 days



Top 50 users in past week

Graph depicting number of bad password attempts

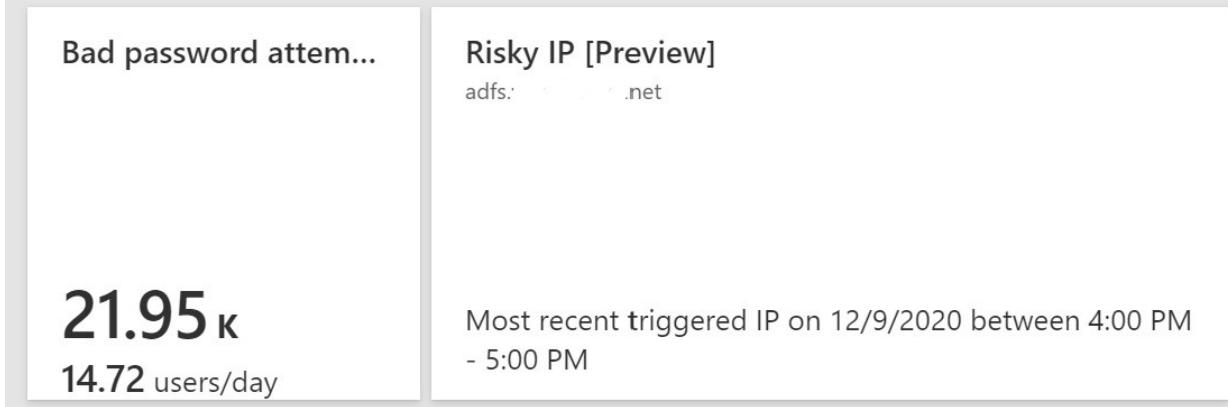
Unusual spikes in activity are key indicators through Azure AD Health Connect (assuming this is installed). Other indicators are:

- Alerting through SIEM shows a spike when you collate the logs.
- Larger than normal log size for ADFS failed sign-ins (this can be an alert in SIEM tool).
- Increased amounts of 342/411 event IDs – username or password is incorrect. Or 516 for extranet lockout.
- Hit failed authentication request threshold – Risky IP in Azure AD or SIEM tool alert/both 342 and 411 errors (To be able to view this information, the advanced logging should be turned on.)

Risky IP in Azure AD Health Connect portal

Risky IP will alert when the customized threshold has been reached for bad passwords in an hour and bad password count in a day as well as extranet lockouts.

Reports



Risky IP report data

The details of failed attempts are available in the tabs **IP address** and **extranet lockouts**.

TimeStamp	Trigger Type	IP Address	Bad Password Error Count	Extranet Lockout Error Count	Unique Users Attempted
2/17/2021 5:00 PM	hour	[REDACTED]	0	17	9
2/17/2021 4:00 PM	hour	[REDACTED]	0	8	5
2/17/2021 12:00 AM	day	[REDACTED]	0	27	12
2/5/2021 7:00 AM	hour	[REDACTED]	0	6	5

IP address and extranet lockouts in the Risky IP report

Detect password spray in Azure Identity Protection

Azure Identity Protection is an Azure AD Premium P2 feature that has a password-spray detection risk alert and search feature that you can utilize to get additional information or set up automatic remediation.

Detection time ↑↓	User ↑↓	Detection type ↑↓	Risk level ↑↓
2/23/2021, 10:16:49 AM	[REDACTED]	Password spray	High
2/18/2021, 9:43:14 PM	[REDACTED]	Password spray	High
2/18/2021, 9:09:02 PM	[REDACTED]	Password spray	High
2/18/2021, 8:27:18 PM	[REDACTED]	Password spray	High
2/17/2021, 9:21:12 AM	[REDACTED]	Password spray	High
2/10/2021, 10:25:20 AM	[REDACTED]	Password spray	High
2/6/2021, 8:55:56 AM	[REDACTED]	Password spray	High
2/4/2021, 9:23:12 AM	[REDACTED]	Password spray	High
2/3/2021, 9:34:26 AM	[REDACTED]	Password spray	High

Details of a password spray attack

Low and slow attack indicators

Low and slow attack indicators are those where thresholds for account lockout or bad passwords are not being hit. You can detect these indicators through:

- Failures in GAL order
- Failures with repetitive attributes (UA, target AppID, IP block/location)
- Timing – automated sprays tend to have a more regular time interval between attempts.

Investigation and mitigation

 Note

You can perform investigation and mitigation simultaneously during sustained/ongoing attacks.

1. Turn advanced logging on ADFS if it is not already turned on.
2. Determine the date and time of start of the attack.
3. Determine the attacker IP address (might be multiple sources and multiple IP addresses) from the firewall, ADFS, SIEM or Azure AD.
4. Once password spray confirmed, you might have to inform the local agencies (police, third parties, among others).
5. Collate and monitor the following Event IDs for ADFS:

ADFS 2012 R2

- Audit event 403 – user agent making the request
- Audit event 411 – failed authentication requests
- Audit event 516 – extranet lockout
- Audit Event 342 – failed authentication requests
- Audit Event 412 - Successful log in

6. To collect the *Audit Event 411 - failed authentication requests*, use the following [script](#):

PowerShell

```
PARAM ($PastDays = 1, $PastHours)
#####
#ADFSBadCredsSearch.ps1
#Version 1.0
#Date: 6-20-2016
#Author: Tim Springston [MSFT]
#Description: This script will parse the ADFS server's (not proxy)
security ADFS
```

```

#for events which indicate an incorrectly entered username or password.
The script can specify a
#past period to search the log for and it defaults to the past 24
hours. Results will be placed into a CSV for
#review of UPN, IP address of submitter, and timestamp.
*****cls
if ($PastHours -gt 0)
{$PastPeriod = (Get-Date).AddHours(-($PastHours))}
else
{$PastPeriod = (Get-Date).AddDays(-($PastDays))}

$Outputfile = $Pwd.path + "\BadCredAttempts.csv"
$CS = get-wmiobject -class win32_computersystem
$Hostname = $CS.Name + '.' + $CS.Domain
$Instances = @{}
$OSVersion = gwmi win32_operatingsystem
[int]$BN = $OSVersion.Buildnumber
if ($BN -lt 9200){$ADFSLogName = "AD FS 2.0/Admin"}
else {$ADFSLogName = "AD FS/Admin"}
$Users = @()
$IPAddresses = @()
$Times = @()
$AllInstances = @()
Write-Host "Searching event log for bad credential events..."
if ($BN -ge 9200) {Get-Winevent -FilterHashTable @{LogName= "Security";
>StartTime=$PastPeriod; ID=411} -ErrorAction SilentlyContinue | Where-
Object{$_.Message -match "The user name or password is incorrect"} | %
{
$Instance = New-Object PSObject
$UPN = $_.Properties[2].Value
$UPN = $UPN.Split("-")[0]
$IPAddress = $_.Properties[4].Value
$Users += $UPN
$IPAddresses += $IPAddress
$Times += $_.TimeCreated
add-member -inputobject $Instance -membertype noteproperty -name
>"UserPrincipalName" -value $UPN
add-member -inputobject $Instance -membertype noteproperty -name "IP
Address" ->value $IPAddress
add-member -inputobject $Instance -membertype noteproperty -name "Time"
-value >($_.TimeCreated).ToString()
$AllInstances += $Instance
$instance = $null
}
}
$AllInstances | select * | Export-Csv -Path $Outputfile -append -force
->NoTypeInformation
Write-Host "Data collection finished. The output file can be found at
>$outputfile`."
$AllInstances = $null

```

Along with the above event IDs, collate the *Audit Event 1203 – Fresh Credential Validation Error*.

1. Collate all successful sign-ins for this time on ADFS (if federated). A quick sign-in and logout (at the same second) can be an indicator of a password being guessed successfully and being tried by the attacker.
2. Collate any Azure AD successful or interrupted events for this time-period for both federated and managed scenarios.

Monitor and collate Event IDs from Azure AD

See how to find the [meaning of error logs](#).

The following Event IDs from Azure AD are relevant:

- 50057 - User account was disabled
- 50055 - Password expired
- 50072 - User prompted to provide MFA
- 50074 - MFA required
- 50079 - user needs to register security info
- 53003 - User blocked by Conditional Access
- 53004 - Cannot configure MFA due to suspicious activity
- 530032 - Blocked by Conditional Access on Security Policy
- Sign-In status Success, Failure, Interrupt

Collate event IDs from Sentinel playbook

You can get all the Event IDs from the Sentinel Playbook that is available on [GitHub](#).

Isolate and confirm attack

Isolate the ADFS and Azure AD successful and interrupted sign-in events. These are your accounts of interest.

Block the IP Address ADFS 2012R2 and above for federated authentication. Here's an example:

PowerShell

```
Set-AdfsProperties -AddBannedIps "1.2.3.4", "::3", "1.2.3.4/16"
```

Collect ADFS logs

Collect multiple event IDs within a time frame. Here's an example:

PowerShell

```
Get-WinEvent -ProviderName 'ADFS' | Where-Object { $_.ID -eq '412' -or $_.ID -eq '411' -or $_.ID -eq '342' -or $_.ID -eq '516' -and $_.TimeCreated -gt ((Get-Date).AddHours(-"8")) }
```

Collate ADFS logs in Azure AD

Azure AD Sign-In reports include ADFS sign-in activity when you use Azure AD Connect Health. Filter sign-in logs by Token Issuer Type "Federated".

Here's an example PowerShell command to retrieve sign-in logs for a specific IP address:

PowerShell

```
Get-AzureADIRSignInDetail -TenantId b446a536-cb76-4360-a8bb-6593cf4d9c7f -  
IpAddress 131.107.128.76
```

Also, search the Azure portal for time frame, IP address and successful and interrupted sign-in as shown in these images.

Service principal sign-ins	Managed identity
Azure Portal	Success
Azure Portal	Success
Microsoft Cloud App...	Success
Microsoft Cloud App...	Interrupted
Azure DevOps	Success
Azure Portal	Success
Azure Portal	Success

Searching for sign-ins within a specific time frame

Date : **Last 24 hours** Show dates as : **Local** IP address starts with **X** Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User
12/30/2020, 10:26:01...	4abefc58-44eb-4a25...	Admin
12/30/2020, 10:25:58...	296d90b2-b8c1-41a...	Admin

IP address

Apply

Azure Portal

Status	Managed identity sign-ins
Success	Success
Success	Success

Searching for sign-ins on a specific IP address

Date : **Last 1 month** Show dates as : **Local** Status : **None Selected** Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User
------	------------	------

Status

Success
 Failure
 Interrupted

Apply

Searching for sign-ins based on the status

You can then download this data as a .csv file for analysis. For more information, see [Sign-in activity reports in the Azure Active Directory portal](#).

Prioritize findings

It is important to be able to react to the most critical threat. This can be the attacker has successfully obtained access to an account and therefore can access/exfiltrate data. The attacker has the password but may not be able to access the account for example they have the password but are not passing the MFA challenge. Also, the attacker could not be guessing passwords correctly but continuing to try. During analysis, prioritize these findings:

- Successful sign-ins by known attacker IP address
- Interrupted sign-in by known attacker IP address
- Unsuccessful sign-ins by known attacker IP address
- Other unknown IP address successful sign-ins

Check legacy authentication

Most attacks use legacy authentication. There are a number of ways to determine the protocol of the attack.

1. In Azure AD, navigate to **Sign-Ins** and filter on **Client App**.

2. Select all the legacy authentication protocols that are listed.

The screenshot shows the Azure AD Sign-Ins blade with the following interface elements:

- Date filter: Last 24 hours
- Show dates as: Local
- Count: 13 selected

The main table displays "User sign-ins (interactive)" with columns: Date, Request ID, and a status bar indicating "No sign-ins found".

A modal dialog is open on the right side, listing authentication clients categorized into Modern and Legacy protocols:

- Modern Authentication Clients** (unchecked):
 - Browser
 - Mobile Apps and Desktop clients
- Legacy Authentication Clients** (checked):
 - Autodiscover
 - Exchange ActiveSync
 - Exchange Online Powershell
 - Exchange Web Services
 - IMAP
 - MAPI Over HTTP
 - Offline Address Book
 - Other clients
 - Outlook Anywhere (RPC over HTTP)
 - POP
 - Reporting Web Services
 - SMTP
 - Universal Outlook

List of legacy protocols

3. Or if you have an Azure workspace, you can use the pre-built legacy authentication workbook located in the Azure Active Directory portal under **Monitoring and Workbooks**.

The screenshot shows the Azure AD Audit Log interface. It includes sections for:

- Usage (4):**
 - Sign-ins
 - Sign-ins using Legacy Authent...
 - App Consent Audit
 - Access Package Activity
- Conditional access (3):**
 - Conditional Access Insights an...
 - Sign-ins by Conditional Access...
 - Sign-ins by Grant Controls
- Troubleshoot (4):**
 - Sensitive Operations Report
 - Sign-ins Failure Analysis
 - Provisioning Analysis
 - Archived Log Date Range

Legacy authentication workbook

Block IP address Azure AD for managed scenario (PHS including staging)

1. Navigate to New named locations.

The screenshot shows the 'New named location' form. It includes fields for:

- Name ***: Blocked IP Address (highlighted with a green checkmark).
- Define the location using:**
 - IP ranges
 - Countries/Regions
- Mark as trusted location ⓘ
- IP ranges** section:
 - Add a new IP range (ex: 40.77.182.32/27)
 - No IP ranges

2. Create a CA policy to target all applications and block for this named location only.

Has the user used this operating system, IP, ISP, device, or browser before?

If the user has not used them before and this activity is unusual, then flag the user and investigate all of their activities.

Is the IP marked as "risky"?

Ensure you record successful passwords but failed multi-factor authentication (MFA) responses, as this activity indicates that the attacker is getting the password but not passing MFA. Set aside any account that appears to be a normal sign-in, for example, passed MFA, location and IP not out of the ordinary.

MFA reporting

It is important to also check MFA logs as an attacker could have successfully guessed a password but be failing the MFA prompt. The Azure AD MFA logs shows authentication details for events when a user is prompted for multi-factor authentication. Check and make sure there are no large suspicious MFA logs in Azure AD. For more information, see [how to use the sign-ins report to review Azure AD Multi-Factor Authentication events](#).

Additional checks

In Defender for Cloud Apps, investigate activities and file access of the compromised account. For more information, see:

- [Investigate compromise with Defender for Cloud Apps](#)
- [Investigate anomalies with Defender for Cloud Apps](#)

Check whether the user has access to additional resources, such as virtual machines (VMs), domain account permissions, storage, among others. If data has been breached, then you should inform additional agencies, such as the police.

Immediate remedial actions

1. Change the password of any account that is suspected to have been breached or if the account password has been discovered. Additionally, block the user. Make sure you follow the guidelines for [revoking emergency access](#).
2. Mark any account that has been compromised as "*compromised*" in Azure Identity Protection.
3. Block the IP address of the attacker. Be cautious while performing this action as attackers can use legitimate VPNs and this could create more risk as they change IP addresses as well. If you are using Cloud Authentication, then block the IP address in Defender for Cloud Apps or Azure AD. If federated, you need to block the IP address at the firewall level in front of the ADFS service.

4. [Block legacy authentication](#) if it is being used (this action, however, could impact business).
5. [Enable MFA](#) if it is not already done.
6. [Enable Identity Protection](#) for the user risk and sign-in risk
7. Check the data that has been compromised (emails, SharePoint, OneDrive, apps). See how to use the [activity filter in Defender for Cloud Apps](#).
8. Maintain password hygiene. For more information, see [Azure AD password protection](#).
9. You can also refer to [ADFS Help](#).

Recovery

Password protection

Implement password protection on Azure AD and on-premises by enabling the custom-banned password lists. This configuration will prevent users from setting weak passwords or passwords associated with your organization:

Authentication methods | Password protection

- Azure AD Security

Manage

- Policy
- Password protection**

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes

Custom banned password list ⓘ

contoso	✓
fabrikam	✓
wolverine	✓
howard	✓
northwind	✓
michigan	✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes

Mode ⓘ Enforced

Enabling password protection

For more information, see [how to defend against password spray attacks](#).

Tagging IP address

Tag the IP addresses in Defender for Cloud Apps to receive alerts related to future use:

The screenshot shows the Microsoft Defender for Cloud Apps Activity log interface. At the top, it displays a single activity: "Failed log on (Failure message: This error occurred due to...)" by user "Office 365" on "192.68.11.219". Below this, there are tabs for "OPEN ALERTS", "ACTIVITIES", and "ADMIN ACTIVITIES". On the left, under "Tags", it shows "192.68.11.219 RISKY IP ADDRESS" and "ISP: D". On the right, there's a chart titled "IP ACTIVITIES (30 DAYS) See all" showing activity counts for April and May, and a section for "IP LOCATION" stating "Location is not available for this IP address". At the bottom, there are buttons for "User" and "IP address" actions like "Tag as a Corporate IP and add to whitelist", "Tag as a VPN IP and add to whitelist", and "Tag as a Risky IP and add to blacklist".

Tagging IP addresses

In Defender for Cloud Apps, "tag" IP address for the IP scope and set up an alert for this IP range for future reference and accelerated response.

The screenshot shows the "Policy template" configuration page. It includes fields for "Policy template *", "Policy name *", "Policy severity *", "Category *", and a "Description" box. The "Policy template" dropdown is set to "Logon from a risky IP address". The "Policy name" input field contains "Password Spray". The "Policy severity" dropdown has three color-coded options: grey, orange, and red. The "Category" dropdown is set to "Threat detection". The "Description" box contains the text: "Alert when a user logs on from a risky IP address to your sanctioned services. 'Risky' IP category contains by default anonymous proxies and TOR exits point. You can add more IP addresses to this category through the 'IP addresses range' settings page."

Create filters for the policy

Act on:

- Single activity
Every activity that matches the filters
- Repeated activity:
Repeated activity by a single user

The screenshot shows the "ACTIVITIES MATCHING ALL OF THE FOLLOWING" filter configuration. It includes a "Raw IP address" field containing "1.2.3.4" and an "equals" dropdown. There are also two "IP address" fields with dropdowns and a plus sign icon for adding more conditions. A "Edit and preview results" button is located in the top right corner.

Setting alerts for a specific IP address

Configure alerts

Depending on your organization needs, you can configure alerts.

[Set up alerting in your SIEM tool](#) and look at improving logging gaps. Integrate ADFS, Azure AD, Office 365 and Defender for Cloud Apps logging.

Configure the threshold and alerts in ADFS Health Connect and Risky IP portal.

Threshold Settings X

H Save X Discard ...

(Bad U/P + Extranet Lockout)/Day * ⓘ

100

(Bad U/P + Extranet Lockout)/Hour * ⓘ

50

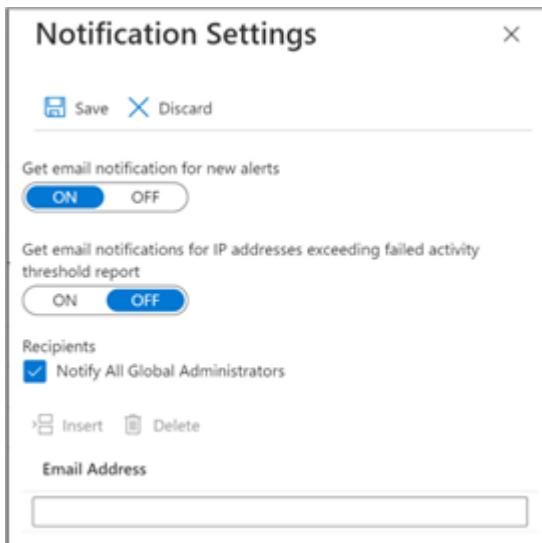
Extranet Lockout - Day * ⓘ

20

Extranet Lockout - Hour * ⓘ

10

Configure threshold settings



Configure notifications

See how to [configure alerts in the Identity Protection portal](#).

Set up sign-in risk policies with either Conditional Access or Identity Protection

- [Configure Sign-In risk](#)
- [Configure User Risk](#)
- [Configure policy alerts in Defender for Cloud Apps](#)

Recommended defenses

- Educate end users, key stakeholders, front line operations, technical teams, cyber security and communications teams
- Review security control and make necessary changes to improve or strengthen security control within your organization
- Suggest Azure AD configuration assessment
- Run regular [attack simulator](#) exercises

References

Prerequisites

- [Sentinel Alerting](#)
- [SIEM integration into Defender for Cloud Apps](#)
- [SIEM integration with Graph API](#)
- [Splunk alerting video ↗](#)

- Splunk alerting manual ↗
- Installing ADFS Health Connect
- Understanding Azure AD sign-in logs
- Understanding MFA reporting

Mitigations

- Mitigations for password spray ↗
- Enable password protection
- Block legacy authentication
- Block IP address on ADFS
- Access controls (including blocking IP addresses) ADFS v3
- ADFS Password Protection
- Enable ADFS Extranet Lockout
- MFA as primary authentication
- Enable Identity Protection
- Azure AD audit activity reference
- Azure AD audit logs schema
- Azure AD sign-in logs schema
- Azure AD audit log Graph API
- Risky IP Alerts ↗
- ADFS Help ↗

Recovery

- SIEM tool integrations
- Create Defender for Cloud Apps alerts
- Create Risky IP and ADFS Health Connect Alerts
- Identity Protection alerts
- Attack simulator

Additional incident response playbooks

Examine guidance for identifying and investigating these additional types of attacks:

- Phishing
- App consent
- Microsoft DART ransomware approach and best practices

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

App consent grant investigation

Article • 02/01/2023 • 21 minutes to read

This article provides guidance on identifying and investigating app consent attacks, protecting information, and minimizing further risks.

This article contains the following sections:

- **Prerequisites:** Covers the specific requirements you need to complete before starting the investigation. For example, logging that should be turned on, roles and permissions required, among others.
- **Workflow:** Shows the logical flow that you should follow to perform this investigation.
- **Checklist:** Contains a list of tasks for each of the steps in the flow chart. This checklist can be helpful in highly regulated environments to verify what you have done or simply as a quality gate for yourself.
- **Investigation steps:** Includes a detailed step-by-step guidance for this specific investigation.
- **Recovery:** Contains high level steps on how to recover/mitigate from an Illicit Application Consent grant attack.
- **References:** Contains additional reading and reference materials.

Prerequisites

Here are general settings and configurations you should complete to perform an investigation for Application Consent Grants. Before starting the investigation, make sure you have read about the types of consent permissions explained in [Consent permission types](#).

Customer data

To start the investigation process, you need the following data:

- Access to the tenant as a Global Admin - A Cloud only account (not part of their on-premises environment)
- Detail of indicators of compromise (IoCs)
- The date and time when you noticed the incident
- Date range
- Number of compromised accounts
- Name(s) of compromised accounts

- Roles of the compromised account
- Are the accounts highly privileged (GA Microsoft Exchange, SharePoint)?
- Are there any Enterprise Applications that are related to the incident?
- Did any users report about any applications that were requesting permissions to data on their behalf?

System requirements

Ensure you complete the following installations and configuration requirements:

1. The AzureAD PowerShell module is installed.
2. You have global administrator rights on the tenant that the script will be run against.
3. You are assigned local administrator role on the computer that you will use to run the scripts.

Install the AzureAD module

Use this command to install the AzureAD module.

PowerShell

```
Install-Module -Name AzureAD -Verbose
```

 **Note**

If you are prompted to install the modules from an untrusted repository, type **Y** and press **Enter**.

Install the MSOnline PowerShell module

1. Run the Windows PowerShell app with elevated privileges (run as administrator).
2. Run this command to allow PowerShell to run signed scripts.

PowerShell

```
Set-ExecutionPolicy RemoteSigned
```

3. Install the MSOnline module with this command.

```
PowerShell
```

```
Install-Module -Name MSOnline -Verbose
```

ⓘ Note

If you are prompted to install the modules from an untrusted repository, type Y and press Enter.

Download the AzureADPSPermissions Script from GitHub

1. Download the [Get-AzureADPSPermissions.ps1](#) script from GitHub to a folder from which you will run the script. The output file "permissions.csv" will also be written to this same folder.
2. Open a PowerShell instance as an administrator and open the folder in which you saved the script.
3. Connect to your directory using the `Connect-AzureAD` cmdlet. Here's an example.

```
PowerShell
```

```
Connect-AzureAD -tenantid "2b1a14ac-2956-442f-9577-1234567890ab" -  
AccountId "user1@contoso.onmicrosoft.com"
```

4. Run this PowerShell command.

```
PowerShell
```

```
Get-AzureADPSPermissions.ps1 | Export-csv -Path "Permissions.csv" -  
NoTypeInformation
```

Disconnect your AzureAD session with this command.

```
PowerShell
```

```
Disconnect-AzureAD
```

Consent terminologies

What are application consent grants?

Consent is the process of granting authorization to an application to access protected resources on the users' behalf. An administrator or user can be asked for consent to allow access to their organization/individual data.

An application is granted access to data based on a particular user or for the entire organization. These consents, however, can be misused by attackers to gain persistence to the environment and access sensitive data. These types of attacks are called Illicit Consent Grants, which can happen through a phishing email, a user account compromise through password spray, or when an attacker registers an application as a legitimate user. In scenarios where a Global Admin account is compromised, then the registration and consent grant are for tenant-wide and not just for one user.

Before an application can access your organization's data, a user must grant the application permissions to do so. Different permissions allow different levels of access. By default, all users are allowed to consent to applications for permissions that don't require administrator consent. For instance, by default, a user can consent to allow an app to access their mailbox but can't consent to allow an app unfettered access to read and write to all files in your organization.

Note

By allowing users to grant apps access to data, users can easily acquire useful applications and be productive. However, in some situations, this configuration can represent a risk if it's not monitored and controlled carefully.

Roles that can grant consent on behalf of the organization

To be able to grant **tenant-wide admin consent**, you must sign in as one of the following:

- Global Administrator
- Application Administrator
- Cloud Application Administrator

Consent types

- **Administrator** - Indicates the consent was provided by the administrator (on behalf of the organization)
- **Individual user** - Indicates the consent was granted by the user and only has access to that user's information

- Accepted values
 - *AllPrincipals* - Consented by an administrator for the entire tenancy
 - *Principal* – Consented by the individual user for data only related to that account

Consent and permissions

The actual user experience of granting consent will differ depending on the policies set on the user's tenant, the user's scope of authority (or role), and the type of permissions being requested by the client application. This means that application developers and tenant admins have some control over the consent experience. Admins have the flexibility of setting and deactivating policies on a tenant or app to control the consent experience in their tenant. Application developers can dictate what types of permissions are being requested and if they want to guide users through the user consent flow or the admin consent flow.

- **User consent flow** - When an application developer directs users to the authorization endpoint with the intent to record consent for only the current user.
- **Admin consent flow** - When an application developer directs users to the admin consent endpoint with the intent to record consent for the entire tenant. To ensure the admin consent flow works properly, application developers must list all permissions in the **RequiredResourceAccess** property in the application manifest.

Delegated permissions vs. application permissions

Delegated permissions are used by apps that have a signed-in user present and can have consents applied by the administrator or user.

Application permissions are used by apps that run without a signed-in user present. For example, apps that run as background services or daemons. Application permissions can be consented only by an administrator.

For more information see:

- [Admin consent workflow for admin approval for specific applications](#)
- [Publisher verification program](#)
- [Configure how end users consent to applications](#)

Classifying risky permissions

There are thousands (at least) of permissions in the system, and not feasible to list out or parse all of these. The list below will address commonly misused permissions, and others that would create catastrophic impact if misused.

At a high level, we have observed the following "root" delegated (App+User) permissions being misused in consent phishing attacks. Root equates to the top level. For example, *Contacts.** means to include all delegated permutations of Contacts permissions: *Contacts.Read*, *Contacts.ReadWrite*, *Contacts.Read.Shared*, and *Contacts.ReadWrite.Shared*.

1. *Mail.** (including *Mail.Send**, but not *Mail.ReadBasic**)
2. *Contacts.**
3. *MailboxSettings.**
4. *People.**
5. *Files.**
6. *Notes.**
7. *Directory.AccessAsUser.All*
8. *User_Impersonation*

The first seven permissions in the list above are for Microsoft Graph and the "legacy" API equivalents, such as Azure Active Directory (Azure AD) Graph and Outlook REST. The eighth permission is for Azure Resource Manager (ARM), and could also be dangerous on any API that exposes sensitive data with this blanket impersonation scope.

As per our observation, attackers have used a combination of the first six permissions in the in 99% of the consent phishing attacks. Most people don't think of the delegated version of *Mail.Read* or *Files.Read* as a high-risk permission, however, the attacks we've seen are generally widespread attacks targeting end users, rather than spear phishing against admins who can actually consent to the dangerous permissions. It is recommended to bubble apps with these "critical" level of impact permissions. Even if the applications do not have malicious intent, and if a bad actor were to compromise the app identity, then your entire organization could be at risk.

For the highest risk impact permissions, start here:

- Application permission (AppOnly/AppRole) versions of all the above permissions, where applicable

Delegated and AppOnly versions of the following permissions:

- *Application.ReadWrite.All*
- *Directory.ReadWrite.All*
- *Domain.ReadWrite.All**

- *EduRoster.ReadWrite.All**
- *Group.ReadWrite.All*
- *Member.Read.Hidden**
- *RoleManagement.ReadWrite.Directory*
- *User.ReadWrite.All**
- *User.ManageCreds.All*
- All other AppOnly permissions that allow write access

For the lowest risk impact permissions list, start here:

- *User.Read*
- *User.ReadBasic.All*
- *Open_id*
- *Email*
- *Profile*
- *Offline_access* (only if paired with other permissions on this "lowest risk" list)

Viewing permissions

1. To view the permissions, navigate to the **Registration** screen in the enterprise application.

The screenshot shows the Microsoft Azure portal interface for managing a registered application named "DaRT-GraphAPI". The top navigation bar includes "Home" and "DaRT-GraphAPI". The main content area has a search bar, a "Delete" button, and an "Endpoints" link. A feedback message says "Got a second? We would love your feedback on Microsoft identity". Below this, the "Call APIs" section displays icons for various Microsoft services. At the bottom, a call-to-action button says "View API permissions". The left sidebar under "Manage" lists several configuration options: Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, and Owners. The "API permissions" option is highlighted.

2. Select **View API permissions**.

Home > Inc. > DaRT-GraphAPI

DaRT-GraphAPI | API permissions

Search (Ctrl+)/ Refresh | Got feedback?

Overview Quickstart Integration assistant (preview)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission	Grant admin consent for	Inc.	Admin consent req...	Status	...
▼ Microsoft Graph (3)					
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted	...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted	...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted	...

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners

3. Select **Add a permission** and the following screen is displayed.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Azure Data Lake Access to storage and compute for big data analytic scenarios
---	---	---

4. Select **Microsoft Graph** to view the different types of permissions.

Request API permissions

X

< All APIs



Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Start typing a reply url to filter these results

Permission

Admin consent required

> AccessReview

> AdministrativeUnit

> Application

> AppRoleAssignment

> ApprovalRequest

> AuditLog (1)

> BitlockerKey

5. Select the type of permissions the registered application is using: **Delegated permissions** or **Application permissions**. In the above image, **Application permissions** is selected.

6. You can search for one of the high-risk impact permissions such as **EduRoster**.

Request API permissions

X

< All APIs



Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Edu

Permission

Admin consent required

> EduAdministration

> EduAssignments

> EduRoster

7. Select **EduRoster** and expand the permissions.

Request API permissions

[All APIs](#) Microsoft Graph https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

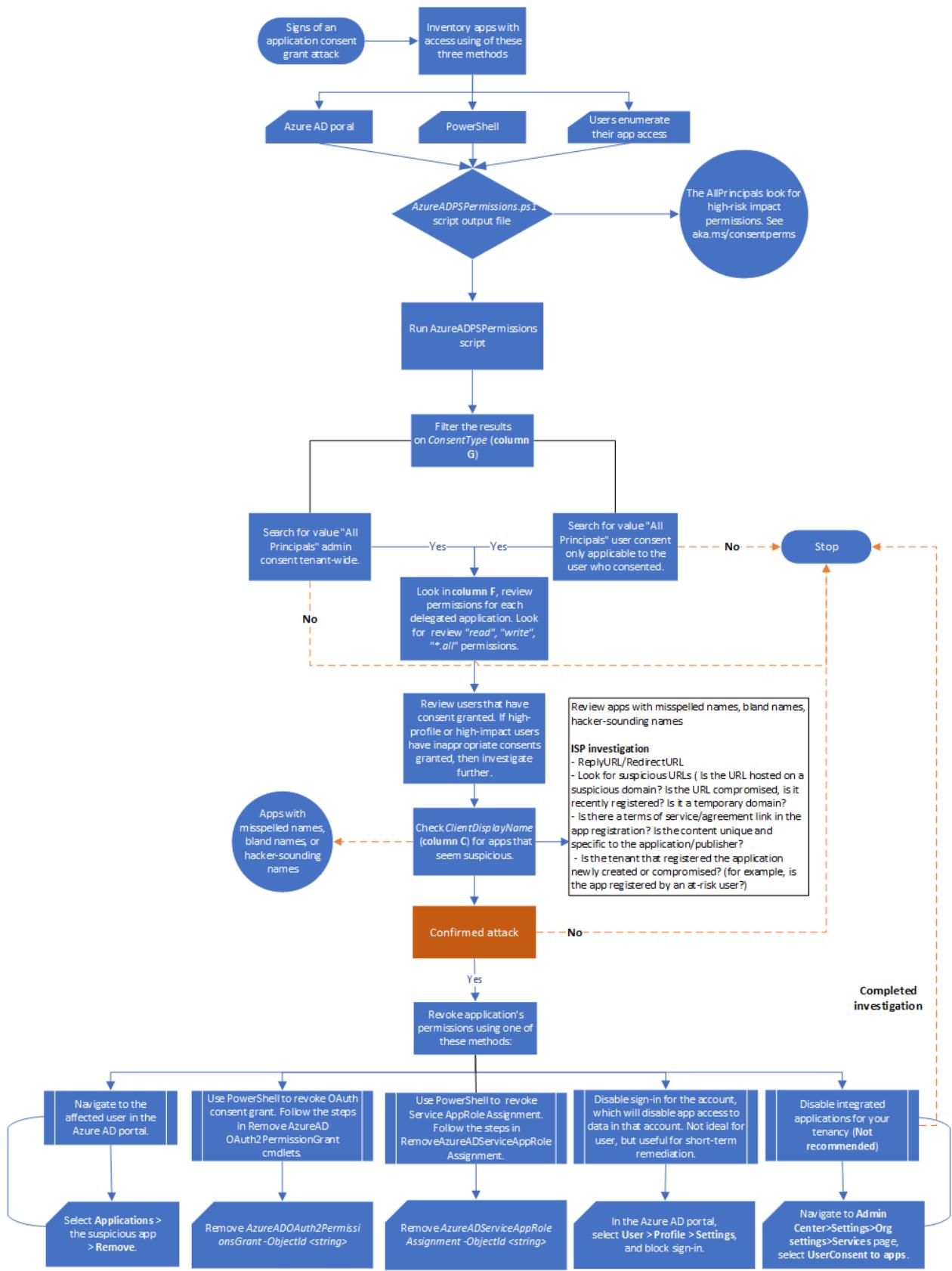
Select permissions expand all

Permission	Admin consent required
> EduAdministration	
> EduAssignments	
> EduRoster	
<input type="checkbox"/> EduRoster.Read.All ⓘ Read the organization's roster	Yes
<input type="checkbox"/> EduRoster.ReadBasic.All ⓘ Read a limited subset of the roster	Allows the app to read and write the structure of schools and classes in the organization's roster and education-specific information about all users to be read and written.
<input checked="" type="checkbox"/> EduRoster.ReadWrite.All ⓘ Read and write the organization's roster	Yes

8. You can now assign or review these permissions.

For more information, read [Graph Permissions](#).

Workflow



You can also:

- Download the app consent grant and other incident response playbook workflows as a [PDF](#).
- Download the app consent grant and other incident response playbook workflows as a [Visio file](#).

Checklist

Use this checklist to perform application consent grant validation.

- **Requirements**

Make sure you have access to the tenant as a Global Admin. This is a cloud-only account and is not part of your on-premises environment.

- **Indicators of compromise (IoC)**

Check the following indicators of compromise (IoC):

- When did you notice the incident?
- Date range of the incident (how far left is the goal post?)
- Number of compromised accounts
- Name(s) of compromised accounts
- Roles of the compromised account(s)
- Are the compromised accounts highly privileged, a standard user, or a combination

- **Roles**

You must be assigned with these roles:

- Global administrator rights on the tenant to execute the script
- Local Administrator role on the computer from which will run the script

- **PowerShell configuration**

Configure your PowerShell environment with the following:

- Install the Azure AD PowerShell module.
- Run the Windows PowerShell app with elevated privileges. (Run as administrator).
- Configure PowerShell to run signed scripts.
- Download the [Get-AzureADPermissions.ps1](#) script.

- **Investigation triggers**

- Account compromise
- App Consent settings modified on the tenant
- Alert/audit event status reason "risky application" detected
- Noticed odd looking applications

You can also download the app consent grant and other incident playbook checklists as an [Excel file](#).

Investigation steps

You can use the following two methods to investigate application consent grants:

- Azure portal
- PowerShell script

ⓘ Note

Using the Azure portal *will only allow you to see Admin Consent Grants for the last 90 days and based on this, we recommend using the PowerShell script method only to reduce the attacker registers investigation steps.*

Method 1 – Using the Azure portal

You can use the Azure Active Directory portal to find applications to which any individual user has granted permissions.

1. Sign in to the **Azure portal** as an administrator.
2. Select the **Azure Active Directory** icon.
3. Select **Users**.
4. Select the user that you want to review.
5. Select **Applications**.
6. You can see the list of apps that are assigned to the user and what permissions these applications have.

Method 2 - Using PowerShell

There are several PowerShell tools you can use to investigate illicit consent grants, such as:

- HAWK tool
- AzureAD incident response module
- The [Get-AzureADPSPermissions.ps1](#) script from GitHub

PowerShell is the easiest tool and does not require you to modify anything in the tenancy. We are going to base our investigation on the public documentation from the Illicit Consent Grant attack.

Run `Get-AzureADPSPermissions.ps1`, to export all of the OAuth consent grants and OAuth apps for all users in your tenancy into a .csv file. See the [Prerequisites](#) section to

download and run the `Get-AzureADPSPermissions` script.

1. Open a PowerShell instance as an administrator and open the folder where you saved the script.
2. Connect to your directory using the following `Connect-AzureAD` command. Here's an example.

```
PowerShell
```

```
Connect-AzureAD -tenantid "2b1a14ac-2956-442f-9577-1234567890ab" -  
AccountId "user1@contoso.onmicrosoft.com"
```

3. Run this PowerShell command.

```
PowerShell
```

```
Get-AzureADPSPermissions.ps1 | Export-csv  
c:\temp\consentgrants\Permissions.csv -NoTypeInformation
```

4. Once the script completes, it is recommended to disconnect the Azure AD session with this command.

```
PowerShell
```

```
Disconnect-AzureAD
```

ⓘ Note

The script may take hours to complete, depending on the size and permissions configured as well as your connection.

5. The script creates a file named `Permissions.csv`.

6. Open the file, filter or format the data into a table and save as an `.xlsx` file (for filtering).

The **column headers** for output are shown in this image.

1	A	B	C	D	E	F	G	H	I
	PermissionType	ClientObjectid	ClientDisplayName	ResourceObjectId	ResourceDisplayName	Permission	ConsentType	PrincipalObjectid	PrincipalDisplayName

7. In the **ConsentType** column (G), search for the value **AllPrincipals**. The **AllPrincipals** permission allows the client application to access everyone's content in the tenancy. Native Microsoft 365 applications need this permission to work

correctly. ***Every non-Microsoft application with this permission should be reviewed carefully.***

8. In the **Permission** column (F), review the permissions that each delegated application has. Look for **Read** and **Write** permission or *****. **All** permission, and review these carefully because they may not be appropriate.

Delegated	82fd90a5-24e7-4e26-af38-6286a9c7fa25	UIPath - SPO bot file	841fbcd1-cbb6-4ebe-b382-c4c843a1069c	UIPath - SPO bot file	Files.ReadWrite.All	AllPrincipals
-----------	--------------------------------------	-----------------------	--------------------------------------	-----------------------	---------------------	---------------

(!) Note

Review the specific users that have consents granted. If high profile or high impact users have inappropriate consents granted, you should investigate further.

9. In the **ClientDisplayName** column (C), look for apps that seem suspicious, such as:

- Apps with misspelled names

Delegated	9139c7ae-44ad-46e9-9f3b-a6a3f2370316	Drivers3dge	841fbcd1-cbb6-4ebe-b382-c4c843a1069c	Power BI Service	Dataset.ReadWrite.All	AllPrincipals
-----------	--------------------------------------	-------------	--------------------------------------	------------------	-----------------------	---------------

- Unusual or bland names

Delegated	82fd90a5-24e7-4e26-af38-6286a9c7fa25	Email	841fbcd1-cbb6-4ebe-b382-c4c843a1069c	Microsoft Graph	Files.ReadWrite.All	AllPrincipals
-----------	--------------------------------------	-------	--------------------------------------	-----------------	---------------------	---------------

- Hacker-sounding names. You must review these names carefully.

Delegated	9139c7ae-44ad-46e9-9f3b-a6a3f2370316	Intelligence	841fbcd1-cbb6-4ebe-b382-c4c843a1069c	Power BI Service	Dataset.ReadWrite.All	AllPrincipals
-----------	--------------------------------------	--------------	--------------------------------------	------------------	-----------------------	---------------

Example Output: AllPrincipals and read write all. Applications may not have anything suspicious like bland names and are using MS graph. However, perform research and determine the purpose of the applications and the actual permissions the applications have in the tenant, as shown in this example.

PermissionType	ClientObjectId	ClientDisplayName	ResourceObjectId	ResourceDisplayName	Permission	ConsentType	PrincipalObjectId	PrincipalDisplayName
Delegated		Webex Teams Enterprise Content Management		Microsoft Graph	Files.ReadWrite.All	AllPrincipals		
Delegated		Roombelt		Microsoft Graph	Calendars.ReadWrite	AllPrincipals		
Delegated		Lightboard Studio		Microsoft Graph	Files.ReadWrite.AppFolder	AllPrincipals		
Delegated		PRIME Graph API - QA		Microsoft Graph	Calendars.ReadWrite	AllPrincipals		
Delegated		PRIME Graph API - PRD		Microsoft Graph	Calendars.ReadWrite	AllPrincipals		
Delegated		PRIME Graph API - UAT		Microsoft Graph	Calendars.ReadWrite	AllPrincipals		
Delegated		Power_BI		Power BI Service	Dataset.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Dashboard.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Report.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Workspace.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Capacity.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	StorageAccount.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Dataflow.ReadWrite.All	AllPrincipals		
Delegated		Power_BI		Power BI Service	Gateway.ReadWrite.All	AllPrincipals		
Delegated		UIPath - SPO bot file		Microsoft Graph	Files.ReadWrite	AllPrincipals		
Delegated		UIPath - SPO bot file		Microsoft Graph	Files.ReadWrite.All	AllPrincipals		

Here are some useful tips to review information security policy (ISP) investigations:

1. ReplyURL/RedirectURL

- Look for suspicious URLs

2. Is the URL hosted on a suspicious domain?

- Is it compromised?
 - Is the domain recently registered?
 - Is it a temporary domain?
3. Are there terms of service/service agreement link in the app registration?
 4. Are the contents unique and specific to the application/publisher?
 5. Is the tenant that registered the application either newly created or compromised (for example, is the app registered by an at-risk user)?

Details of consent grant attack

Attack techniques

While [each attack tends to vary, the core attack techniques are ↗](#):

- An attacker registers an app with an OAuth 2.0 provider, such as Azure AD.
- The app is configured in a way that makes it seem legitimate. For example, attackers might use the name of a popular product available in the same ecosystem.
- The attacker gets a link directly from users, which may be done through conventional email-based phishing, by compromising a non-malicious website, or through other techniques.
- The user selects the link and is shown an authentic consent prompt asking them to grant the malicious app permissions to data.
- If a user selects 'Accept', they will grant the app permissions to access sensitive data.
- The app gets an authorization code, which it redeems for an access token, and potentially a refresh token.
- The access token is used to make API calls on behalf of the user.
- If the user accepts, the attacker can gain access to the user's mails, forwarding rules, files, contacts, notes, profile, and other sensitive data and resources.



Permissions requested

Risky App
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Maintain access to data you have given it access to
- ✓ Read your contacts
- ✓ Sign you in and read your profile
- ✓ Read your mail
- ✓ Send mail as you
- ✓ Read all OneNote notebooks that you can access
- ✓ Read and write to your mailbox settings
- ✓ Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel

Accept

Finding signs of an attack

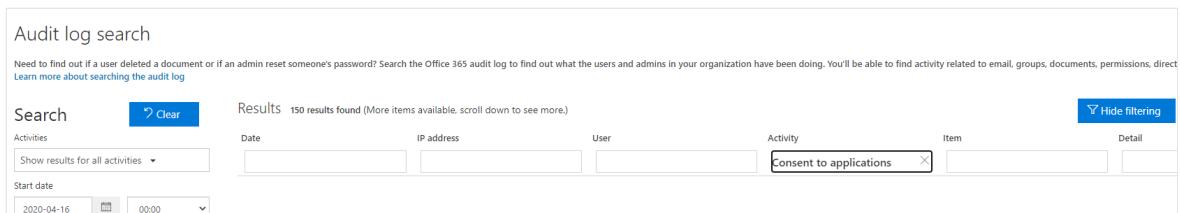
1. Open the [Security & Compliance Center](#).
2. Navigate to **Search** and select **Audit log search**.
3. Search (all activities and all users) and enter the start date and end date if required, and then select **Search**.

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search		Results: 150 results found (More items available, scroll down to see more.)				Filter results	Export results
Activities	Show results for all activities	Date	IP address	User	Activity	Item	Detail
Show results for all activities	▼	2020-07-15 16:01:34		Service Account	SearchHttpStatus		
Start date	2020-04-16	00:00		6079800b-25ea-44b1-b494-a15f218cf62d	SearchCustomerInsight		
End date	2020-07-16	00:00	2020-07-15 14:40:24	6079800b-25ea-44b1-b494-a15f218cf62d	SearchCustomerInsight		
Show results for all users	▼	2020-07-15 14:40:23		Service Account	SearchMailFlowStatusSummary		
Show results for all users	▼	2020-07-15 14:40:20		6079800b-25ea-44b1-b494-a15f218cf62d	SearchCustomerInsight		
Add all or part of a file name, folder name, or URL	○	2020-07-15 14:40:15		Service Account	SearchAggCompromiseReport		
Add all or part of a file name, folder name, or URL	○	2020-07-15 14:40:09		Service Account	SearchAggTPSReportData		
Add all or part of a file name, folder name, or URL	○	2020-07-15 14:40:06		Service Account	AggregateMailMetaData		

4. Select **Filter results** and in the **Activity** field, enter **Consent** to application.



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, direct...

Search Clear

Results 150 results found (More items available, scroll down to see more.)

Activities

Show results for all activities

Date IP address User Activity Item Detail

Consent to applications

Start date

2020-04-16 00:00

Hide filtering

5. If you have activity under consent to grant, continue as directed below.
6. Select the result to see the details of the activity. Select **More Information** to get details of the activity.
7. Check whether IsAdminContent is set to 'True'.

! Note

This process can take from 30 minutes up to 24 hours for the corresponding audit log entry to be displayed in the search results after an event occurs.

The extent of time that an audit record is retained and is searchable in the audit log depends on your Microsoft 365 subscription, and specifically the type of the license that is assigned to a specific user. **If this value is true, it indicates that someone with Global Administrator access may have granted broad access to data. If this is unexpected, take immediate steps to confirm an attack.**

How to confirm an attack?

If you have one or more instances of the IOCs listed above, you need to do further investigation to positively confirm that the attack occurred.

Inventory apps with access in your organization

You can inventory apps for your users using the Azure Active Directory portal, PowerShell, or have your users individually enumerate their application access.

- Use the Azure Active Directory portal to inventory applications and their permissions. This method is thorough, but you can only check one user at a time, which can be time-consuming if you have to check the permissions of several users.
- Use PowerShell to inventory applications and their permissions. This method is the fastest and most thorough, with the least amount of overhead.
- Encourage your users to individually check their apps and permissions and report the results back to the administrators for remediation.

Inventory apps assigned to users

You can use the Azure Active Directory portal to see the list of apps to which any individual user has granted permissions.

1. Sign in to the [Azure Portal](#) with administrative rights.
2. Select the [Azure Active Directory](#) icon.
3. Select **Users**.
4. Select the user that you want to review.
5. Select **Applications**.

You can see the list of apps that are assigned to the user and the permissions granted to these apps.

Determine the scope of the attack

After you have finished inventorying application access, review the audit log to determine the full scope of the breach. Search on the affected users, the time frames that the illicit application had access to your organization, and the permissions the app had. You can search the audit log in the Microsoft 365 Security and Compliance Center.

Important: If auditing was not enabled prior to the possible attack, you will **not** be able to investigate as auditing data will not be available.

How to prevent attacks and mitigate risks?

- Regularly [audit applications](#) and granted permissions in your organization to ensure no unwarranted or suspicious applications have previously been granted access to data.
- [Review, detect, and remediate illicit consent grants in Office 365](#) for additional best practices and safeguards against suspicious applications requesting OAuth consent.

If your organization has the appropriate license:

- Use additional [OAuth application](#) auditing features in Microsoft Defender for Cloud Apps.
- Use [Azure Monitor Workbooks](#) to monitor permissions and consent related activity. The Consent Insights workbook provides a view of apps by number of failed consent requests. This can be helpful to prioritize applications for administrators to review and decide whether to grant them admin consent.

How to stop and remediate an illicit consent grant attack?

After you have identified an application with illicit permissions, **immediately disable the application** following the instructions in [Disable an application](#). Then, contact Microsoft Support to report the malicious application.

Once an application has been disabled in your Azure AD tenant, it cannot obtain new tokens to access data, and other users will not be able to sign in to or grant consent to the app.

ⓘ Note

If you suspect you have encountered a malicious application in your organization, it is better to disable it than to delete it. If you only delete the application, it might return later if another user grants consent. Instead, disable the application to ensure it can't come back later.

Recommended defenses

Steps to protect your organization

There are various consent attack types, but if you follow these recommended defenses, which will mitigate all types of attacks, especially consent phishing, where attackers trick users into granting a malicious app access to sensitive data or other resources. Instead of trying to steal the user's password, an attacker is seeking permission for an attacker-controlled app to access valuable data.

To help prevent consent attacks from affecting Azure AD and Office 365, see the following recommendations:

Set policies

- This setting will have user implications and may not be applicable for an environment. If you are going to allow any consents, ensure the administrators approve the requests.
- Allow consents for applications from verified publishers only and specific types of permissions classified as low impact.

Note

The above recommendations are suggested based on the most ideal, secure configurations. However, as security is a fine balance between functionalities and operations, the most secure configurations might cause additional overheads to administrators. It is a decision best made after consulting with your administrators.

Configure risk-based step-up consent - Enabled by default if user consent to grants is enabled

- Risk-based step-up consent helps reduce user exposure to malicious apps that make illicit consent requests. If Microsoft detects a risky end-user consent request, the request will require a "step-up" to admin consent instead. This capability is enabled by **default**, but it will only result in a behavior change when **end-user consent is enabled**.
- When a risky consent request is detected, the consent prompt will display a message indicating that admin approval is needed. If the admin consent request workflow is enabled, the user can send the request to the admin for further review directly from the consent prompt. If it's not enabled, the following message is displayed:

*AADSTS90094: <clientAppDisplayName> needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it. In this case, an audit event will also be logged with a Category of "**ApplicationManagement**" Activity Type of "**Consent to application**", and Status Reason of "**Risky application detected**".*

Note

Any tasks that require administrator's approval will have operational overhead. The "**Consent and permissions, User consent settings**" is in **Preview** currently. Once it is ready for general availability (GA), the "**Allow user consent from verified publishers, for selected permissions**" feature should reduce administrators' overhead and it is recommended for most organizations.

The screenshot shows the 'User consent settings (Preview)' section. It includes options for 'User consent for applications' (allowing consent for verified publishers or selected permissions) and 'Group owner consent for apps accessing data' (allowing consent for selected group owners). A note at the bottom right says 'Select permissions to classify as low impact'.

Educate your application developers to follow the trustworthy app ecosystem. To help developers build high-quality and secure integrations, we're also announcing [public preview of the Integration Assistant in Azure AD app registrations](#).

- The Integration Assistant analyzes your app registration and benchmarks it against a set of recommended security best practices.
- The Integration Assistant highlights best practices that are relevant during each phase of your integration's lifecycle—from development all the way to monitoring—and ensures every stage is properly configured.
- It's designed to make your job easier, whether you're integrating your first app or you're an expert looking to improve your skills.

Educate your organization on consent tactics ([phishing tactics, admin and user consents](#)):

- Check for poor spelling and grammar. If an email message or the application's consent screen has spelling and grammatical errors, it's likely to be a suspicious application.
- Keep a watchful eye on app names and domain URLs. Attackers like to spoof app names that make it appear to come from legitimate applications or companies but drive you to consent to a malicious app.
- Make sure you recognize the app name and domain URL before consenting to an application.

Promote and allow access to apps you trust

- Promote the use of applications that have been publisher verified. Publisher verification helps admins and end users understand the authenticity of application developers. Over 660 applications by 390 publishers have been verified thus far.

- Configure application consent policies by allowing users to only consent to specific applications you trust, such as applications developed by your organization or from verified publishers.
- Educate your organization on how our permissions and consent [framework works](#).
- Understand the data and permissions an application is asking for and understand how permissions and consent work within our platform.
- Ensure administrators know how to manage and evaluate consent requests.

Audit apps and consented permissions in your organization to ensure applications being used are accessing only the data they need and adhering to the principles of least privilege.

Mitigations

- Educate the customer and provide awareness and training on securing application consent grants
- Tighten the application consent grants process with organizational policy and technical controls
- Set up [Create schedule](#) to review [Consented](#) applications
- You can use PowerShell to disable suspected or malicious apps by [disabling the app](#)

References

The source of the content for this article is the following:

- [Protecting remote workforce application attacks ↗](#)
- [Fostering a secure and trustworthy app ecosystem ↗](#)
- [Investigate risky OAuth apps](#)
- [Managing consent to applications and evaluating consent requests](#)
- [Disable user sign-ins for an enterprise app in Azure Active Directory](#)
- [Understand the permissions and consent framework in the Microsoft identity platform.](#)
- [Understand the difference between delegated permissions and application permissions.](#)
- [Configure how end-users consent to applications](#)
- [Unexpected application in my applications list](#)
- [Detect and Remediate Illicit Consent Grants](#)
- [How and Why Azure AD Applications are Added](#)
- [Application and service principal objects in Azure Active Directory](#)
- [Azure AD Config Documentor ↗](#)

- Managing consent to applications and evaluating consent requests
- Get-AzureADServicePrincipal
- Build 2020: Fostering a secure and trustworthy app ecosystem for all users ↗
- Configure the admin consent workflow
- Admins should evaluate all consent requests carefully before approving a request, especially when Microsoft has detected risk.
- Application Registration vs. Enterprise Applications ↗
- Permissions
- KrebsOnSecurity on AppConsent Phishing ↗

Additional incident response playbooks

Examine guidance for identifying and investigating these additional types of attacks:

- Phishing
- Password spray
- Microsoft DART ransomware approach and best practices

Incident response resources

- Overview for Microsoft security products and resources for new-to-role and experienced analysts
- Planning for your Security Operations Center (SOC)
- Process for incident response process recommendations and best practices
- Microsoft 365 Defender incident response
- Microsoft Defender for Cloud (Azure)
- Microsoft Sentinel incident response

Detecting human-operated ransomware attacks with Microsoft 365 Defender

Article • 09/27/2022 • 13 minutes to read

Note

Want to experience Microsoft 365 Defender? Learn more about how you can [evaluate and pilot Microsoft 365 Defender](#).

Ransomware is a type of extortion attack that destroys or encrypts files and folders, preventing access to critical data or disrupting critical business systems. There are two types of ransomware:

- Commodity ransomware is malware that spreads with phishing or between devices and encrypts files before demanding a ransom.
- Human-operated ransomware is a planned and coordinated attack by active cybercriminals who employ multiple attack methods. In many cases, known techniques and tools are used to infiltrate your organization, find the assets or systems worth extorting, and then demand a ransom. Upon compromising a network, the attacker carries out reconnaissance of assets and systems which can be encrypted or extorted. The attackers then encrypt or exfiltrate data before demanding a ransom.

This article describes proactive detection of new or ongoing human-operated ransomware attacks with the Microsoft 365 Defender portal, an extended detection and response (XDR) solution for the following security services:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps (including the app governance add-on)
- Microsoft Azure AD Identity Protection
- Microsoft Defender for IoT
- Microsoft 365 Business Premium
- Microsoft Defender for Business

For information about preventing ransomware attacks, see [Rapidly protect against ransomware and extortion](#).

The importance of proactive detection

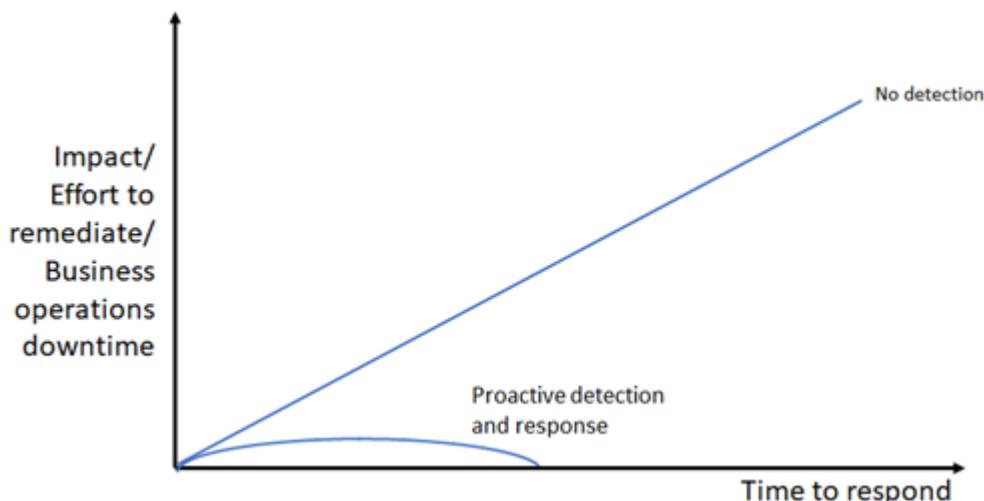
Because human-operated ransomware is typically performed by active attackers who might be performing the steps to infiltrate and discover your most valuable data and systems in real time, the time taken to detect ransomware attacks is crucial.

If pre-ransom activities are detected quickly, the likelihood of a severe attack decreases. The pre-ransom stage typically includes the following techniques: initial access, reconnaissance, credential theft, lateral movement, and persistence. These techniques can initially seem unrelated and often fly under the radar. If these techniques lead to the ransom stage, it's often too late. Microsoft 365 Defender can help identify those small and seemingly unrelated incidents as possibly part of a larger ransomware campaign.

- When detected during the pre-ransom stage, smaller-scale mitigations such as isolating infected devices or user accounts can be used to disrupt and remediate the attack.
- If detection comes at a later stage, such as when the malware used to encrypt files is being deployed, more aggressive remediation steps that can cause downtime might need to be used to disrupt and remediate the attack.

Business operation disruptions are likely when responding to a ransomware attack. The end stage of a ransomware attack is often a choice between downtime caused by attackers with major risks, or a controlled downtime to ensure network safety and give you time to fully investigate. We never recommend paying a ransom. Paying cybercriminals to get a ransomware decryption key provides no guarantee that your encrypted data will be restored. See, [Ransomware response - Microsoft Security Blog](#).

Here's the qualitative relationship of the impact of a ransomware attack and your time to respond for no detection vs. proactive detection and response.



Proactive detection via common malware tools and techniques

In many cases, human-operated ransomware attackers use well-known and field-tested malware tactics, techniques, tools, and procedures including phishing, business email compromise (BEC), and credential theft. Your security analysts must become aware of and familiar with how attackers use common malware and cyberattack methods to gain a foothold in your organization.

To see examples of how ransomware attacks get started with common malware, see these resources:

- [Human-operated ransomware attacks: A preventable disaster](#) ↗
- [Ransomware threat analytics reports in the Microsoft 365 Defender portal](#) ↗

Being familiar with pre-ransom malware, payloads, and activities helps your analysts know what to look for to prevent the later stages of an attack.

Human-operated ransomware attack tactics

Because human-operated ransomware can use known attack techniques and tools, your analysts' understanding and experience with existing attack techniques and tools will be a valuable asset when preparing your SecOps team for focused ransomware detection practices.

Attack tactics and methods

Here are some typical techniques and tools used by ransomware attackers for the following [MITRE ATT&CK](#) ↗ tactics:

Initial access:

- RDP brute force
- Vulnerable internet-facing system
- Weak application settings
- Phishing email

Credential theft:

- Mimikatz
- LSA secrets
- Credential vault
- Credentials in plaintext

- Abuse of service accounts

Lateral movement:

- Cobalt Strike
- WMI
- Abuse of management tools
- PsExec

Persistence:

- New accounts
- GPO changes
- Shadow IT tools
- Schedule tasks
- Service registration

Defense evasion:

- Disabling security features
- Clearing log files
- Deleting attack artifact files
- Resetting timestamps on altered files

Exfiltration:

- Exfiltration of sensitive data Impact (financial leverage):
- Encryption of data in place and in backups
- Deletion of data in place and backups, which might be combined with a preceding exfiltration
- Threat of public leakage of exfiltrated, sensitive data

What to look for

The challenge for security analysts is recognizing when an alert is part of a larger attack chain with the goal of extorting your sensitive data or crucial systems. For example, a detected phishing attack might be:

- A one-off attack to surveil the email messages of someone in the finance department of an organization.
- The pre-ransom part of an attack chain to use compromised user account credentials to discover the resources available to the user account and to compromise other user accounts with higher levels of privilege and access.

This section provides common attack phases and methods and the signal sources that feed into the central Microsoft 365 Defender portal, which creates alerts and incidents composed of multiple related alerts for security analysis. In some cases, there are alternate security portals to view the attack data.

Initial attacks to gain entry

Attacker is attempting to compromise a user account, device, or app.

Attack method	Signal source	Alternate security portals
RDP brute force	Defender for Endpoint	Defender for Cloud Apps
Vulnerable internet-facing system	Windows security features, Microsoft Defender for Servers	
Weak application settings	Defender for Cloud Apps, Defender for Cloud Apps with the app governance add-on	Defender for Cloud Apps
Malicious app activity	Defender for Cloud Apps, Defender for Cloud Apps with the app governance add-on	Defender for Cloud Apps
Phishing email	Defender for Office 365	
Password spray against Azure AD accounts	Azure AD Identity Protection via Defender for Cloud Apps	Defender for Cloud Apps
Password spray against on-premises accounts	Microsoft Defender for Identity	
Device compromise	Defender for Endpoint	
Credential theft	Microsoft Defender for Identity	
Escalation of privilege	Microsoft Defender for Identity	

Recent spike in otherwise typical behavior

Attacker is attempting to probe for additional entities to compromise.

Spike category	Signal source	Alternate security portals

Spike category	Signal source	Alternate security portals
Sign-ins: Numerous failed attempts, attempts to logon to multiple devices in a short period, multiple first-time logons, etc.	Azure AD Identity Protection via Defender for Cloud Apps, Microsoft Defender for Identity	Defender for Cloud Apps
Recently active user account, group, machine account, app	Azure AD Identity Protection via Defender for Cloud Apps (Azure AD), Defender for Identity (Active Directory Domain Services [AD DS])	Defender for Cloud Apps
Recent app activity such as data access	Apps with Defender for Cloud Apps with the app governance add-on	Defender for Cloud Apps

New activity

Attacker is creating new entities to further their reach, install malware agents, or evade detection.

Activity	Signal source	Alternate security portal
New apps that are installed	Defender for Cloud Apps with the app governance add-on	Defender for Cloud Apps
New user accounts	Azure Identity Protection	Defender for Cloud Apps
Role changes	Azure Identity Protection	Defender for Cloud Apps

Suspicious behavior

Attacker is downloading sensitive information, encrypting files, or otherwise collecting or damaging organization assets.

Behavior	Signal source
Malware spread to multiple devices	Defender for Endpoint
Resource scanning	Defender for Endpoint, Defender for Identity
Changes in mailbox forwarding rules	Defender for Office 365

Behavior	Signal source
Data exfiltration and encryption	Defender for Office 365

Monitor for Adversary Disabling Security – as this is often part of human-operated ransomware (HumOR) attack chain

- **Event Logs Clearing** – especially the Security Event log and PowerShell Operational logs
- **Disabling of security tools/controls** (associated with some groups)

Detect ransomware attacks with the Microsoft 365 Defender portal

The Microsoft 365 Defender portal provides a centralized view for information on detections, impacted assets, automated actions taken, and related evidence a combination of:

- An incident queue, which groups related alerts for an attack to provide the full attack scope, impacted assets, and automated remediation actions.
- An alerts queue, which lists all of the alerts being tracked by Microsoft 365 Defender.

Incident and alert sources

Microsoft 365 Defender portal centralizes signals from:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps (including the app governance add-on)
- Microsoft Azure AD Identity Protection
- Microsoft Defender for IoT

This table lists some typical attacks and their corresponding signal source for Microsoft 365 Defender.

Attacks and incidents	Signal source
Cloud identity: Password spray, numerous failed attempts, attempts to log on to multiple devices in a short period, multiple first-time logons, recently active user accounts	Azure AD Identity Protection

Attacks and incidents	Signal source
On-premises identity (AD DS) compromise	Defender for Identity
Phishing	Defender for Office 365
Malicious apps	Defender for Cloud Apps or Defender for Cloud Apps with app governance add-on
Endpoint (device) compromise	Defender for Endpoint
IoT-capable device compromise	Defender for IoT

Filtering ransomware-identified incidents

You can easily filter the incidents queue for incidents that have been categorized by Microsoft 365 Defender as ransomware.

1. From the Microsoft 365 Defender portal navigation pane, go to the incidents queue by selecting **Incidents and alerts > Incidents**.
2. Select **Filters**.
3. Under **Categories**, select **Ransomware**, select **Apply**, and then close the **Filters** pane.

Each filter setting for the incidents queue creates a URL that you can save and access later as a link. These URLs can be bookmarked or otherwise saved and used when needed at a single click. For example, you can create bookmarks for:

- Incidents containing the "ransomware" category. Here is the corresponding [link ↗](#).
- Incidents with a specified **Actor** name known to be performing ransomware attacks.
- Incidents with a specified **Associated threat** name known to be used in ransomware attacks.
- Incidents containing a custom tag that your SecOps team uses for incidents that are known to be part of a larger, coordinated ransomware attack.

Filtering ransomware-identified threat analytics reports

Similar to filtering incidents in the incident queue, you can filter threat analytics reports for reports that include ransomware.

1. From the navigation pane, select **Threat analytics**.
2. Select **Filters**.

3. Under Threat tags, select **Ransomware**, select **Apply**, and then close the **Filters** pane.

You can also click this link.

From the **Detection details** section of many threat analytics reports, you can see a list of alert names created for the threat.

Microsoft 365 Defender APIs

You can also use the Microsoft 365 Defender APIs to query the Microsoft 365 Defender incidents and alerts data in your tenant. A custom app can filter the data, filter it based on custom settings, and then provide a filtered list of links to alerts and incidents that you can easily select to go right to that alert or incident. See [List incidents API in Microsoft 365 Defender | Microsoft Docs](#). You can also integrate your SIEM with Microsoft Defender, see [Integrate your SIEM tools with Microsoft 365 Defender](#).

Microsoft 365 Defender Sentinel Integration

Microsoft Sentinel's Microsoft 365 Defender incident integration allows you to stream all Microsoft 365 Defender incidents into Microsoft Sentinel and keep them synchronized between both portals. Incidents include all associated alerts, entities, and relevant information. Once in Sentinel, incidents will remain bi-directionally synced with Microsoft 365 Defender, allowing you to take advantage of the benefits of both portals in your incident investigation. See, [Microsoft 365 Defender integration with Microsoft Sentinel](#).

Proactive scanning with advanced hunting

[Advanced hunting](#) is a query-based threat hunting tool that lets you explore and inspect events in your network to locate threat indicators and entities. This flexible and customizable analysis tool enables unconstrained hunting for both known and potential threats. Microsoft 365 Defender also supports using a custom query to create [custom detection rules](#), which create alerts based on a query can be and scheduled to run automatically.

For proactive scanning of ransomware activities, you should assemble a catalog of advanced hunting queries for commonly used ransomware attack methods for identities, endpoints, apps, and data. Here are some key sources for ready-to-use advanced hunting queries:

- The [Hunt for ransomware](#) article

- GitHub repository for advanced hunting queries:
 - [Ransomware-specific](#) queries
 - [All categories](#) of queries
- Threat analytics reports
 - Advanced hunting section of the [Ransomware: A pervasive and ongoing threat](#) analyst report
 - Advanced hunting section of other analyst reports

Automated hunting

Advanced hunting queries can also be used to create custom detection rules and actions based on known elements of a ransomware attack method (for example, the use of unusual PowerShell commands). Custom detection rules create alerts that can be seen and addressed by your security analysts.

To create a custom detection rule, select **Create custom detection rule** from the page of an advanced hunting query. Once created, you can specify:

- How often to run the custom detection rule
- The severity of the alert created by the rule
- The MITRE attack phase for the created alert
- Impacted entities
- Actions to take on impacted entities

Prepare your SecOps Team for focused ransomware detection

Preparing your SecOps team for proactive ransomware detection requires:

- Pre-work for your SecOps team and organization
- Security analyst training, as needed
- Ongoing operational work to incorporate the latest attacks and detection experiences of your security analysts

Pre-work for your SecOps team and organization

Consider these steps to get your SecOps team and organization ready for focused ransomware attack prevention:

1. Configure your IT and cloud infrastructure for ransomware prevention with the [Rapidly protect against ransomware and extortion](#) guidance. The phases and tasks

in this guidance can be done in parallel with the following steps.

2. Get the appropriate licenses for the Defender for Endpoint, Defender for Office 365, Defender for Identity, Defender for Cloud Apps, the app governance add-on, Defender for IoT, and Azure AD Identity Protection services.
3. Assemble a catalog of advanced hunting queries tuned for known ransomware attack methods or attack phases.
4. Create the set of custom detection rules for specific advanced hunting queries that create alerts for known ransomware attack methods, including their schedule, alert naming, and automated actions.
5. Determine the set of [custom tags](#) or standards to create new one to identify incidents that are known to be part of a larger, coordinated ransomware attack
6. Determine the set of operational tasks for ransomware incident and alert management. For example:
 - Processes for Tier 1 analyst scanning of incoming incidents and alerts and assignment to Tier 2 analysts for investigation.
 - Manually running advanced hunting queries and their schedule (daily, weekly, monthly).
 - Ongoing changes based on ransomware attack investigation and mitigation experiences.

Security analyst training

As needed, you can provide your security analysts with internal training for:

- Common ransomware attack chains (MITRE attack tactics and common threat techniques and malware)
- Incidents and alerts and how to locate and analyze them in the Microsoft 365 Defender portal using:
 - Alerts and incidents already created by Microsoft 365 Defender
 - Pre-scanned URL-based filters for the Microsoft 365 Defender portal
 - Programmatically via the incidents API
- Advanced hunting queries to use and their manual schedule (daily, weekly, monthly)
- Custom detection rules to use and their settings
- Custom incident tags
- The latest [threat analytics reports for ransomware](#) attacks in the Microsoft 365 Defender portal

Ongoing work based on operational learning and new threats

As part of your SecOps team's ongoing tool and process best practices and security analysts' experiences, you should:

- Update your catalog of advanced hunting queries with:
 - New queries based on the latest threat analytics reports in the Microsoft 365 Defender portal or the [Advanced Hunting GitHub repository](#).
 - Changes to existing ones to optimize for threat identification or for better alert quality.
- Update custom detection rules based on new or changed advanced hunting queries.
- Update the set of operational tasks for ransomware detection.

Responding to ransomware attacks

Article • 09/27/2022 • 7 minutes to read

ⓘ Note

Want to experience Microsoft 365 Defender? Learn more about how you can evaluate and pilot Microsoft 365 Defender.

When you suspect you were or are currently under a ransomware attack, establish secure communications with your incident response team immediately. They can perform the following response phases to disrupt the attack and mitigate the damage:

- Investigation and containment
- Eradication and recovery

This article provides a generalized playbook for responding to ransomware attacks. Consider adapting the described steps and tasks in this article to your own security operations playbook. NOTE: For information about preventing ransomware attacks, see [Rapidly protect against ransomware and extortion](#).

Containment

Containment and investigation should occur as simultaneously as possible; however, you should focus on quickly achieving containment, so you have more time to investigate. These steps help you determine the scope of the attack and to isolate it to only affected entities, such as user accounts and devices.

Step 1: Assess the scope of the incident

Run through this list of questions and tasks to discover the extent of the attack. Microsoft 365 Defender can provide a consolidated view of all impacted or at-risk assets to aid in your incident response assessment. See [Incident response with Microsoft 365 Defender](#). You can use the alerts and the evidence list in the incident to determine:

- Which user accounts might be compromised?
 - Which accounts were used to deliver the payload?
- Which [onboarded](#) and [discovered](#) devices are affected and how?
 - Originating devices
 - Impacted devices
 - Suspicious devices

- Identify any network communication that is associated with the incident.
- Which applications are affected?
- What payloads were spread?
- How is the attacker communicating with the compromised devices? (Network protection must be [enabled](#)):
 - Go to the [indicators page](#) to add a block for the IP and URL (if you have that information).
- What was the payload delivery medium?

Step 2: Preserve existing systems

Run through this list of tasks and questions to protect existing systems from attack:

- If you have online backups, consider disconnecting the backup system from the network until you are confident that the attack is contained, see [Backup and restore plan to protect against ransomware | Microsoft Docs](#).
- If you are experiencing or expect an imminent and active ransomware deployment:
 - [Suspend privileged and local accounts](#) that you suspect are part of the attack. You can do this from the **Users** tab in the properties of the incident in the Microsoft 365 Defender portal.
 - Stop all [remote logon sessions](#).
 - Reset the compromised user account passwords and require the users of compromised user accounts to sign in again.
 - Do the same for user accounts that might be compromised.
 - If shared local accounts are compromised, have your IT admin help you to enforce a password change across all exposed devices. Example Kusto query:

Kusto

```
DeviceLogonEvents | where DeviceName contains (AccountDomain) | take 10
```

- For the devices that are not yet isolated and are not part of the critical infrastructure:
 - Isolate compromised devices from the network but do not shut them off.
 - If you identify the originating or spreader devices, isolate those first.
- Preserve compromised systems for analysis.

Step 3: Prevent the spread

Use this list to keep the attack from spreading to additional entities.

- If shared local accounts are being used in the attack, consider [Blocking Remote Use of Local Accounts](#).
 - Kusto query for all network logons that are local admins:

Kusto

```
DeviceLogonEvents
| where IsLocalAdmin == true and AccountDomain == DeviceName
| extend IsLocalLogon = tobool(todynamic(AdditionalFields).IsLocalLogon)
| where IsLocalLogon==false
```

- Kusto query for non-RDP logons (more realistic for most networks):

Kusto

```
DeviceLogonEvents
| where IsLocalAdmin == true and AccountDomain == DeviceName and LogonType
!= 'RemoteInteractive'
| extend IsLocalLogon = tobool(todynamic(AdditionalFields).IsLocalLogon)
| where IsLocalLogon==false
```

- Quarantine and add indicators for files that are infected.
- Ensure that your antivirus solution is configurable in its optimal protection state. For Microsoft Defender Antivirus, this includes:
 - [Real time protection](#) is enabled.
 - [Tamper protection](#) is enabled. In the Microsoft 365 Defender portal, select **Settings > Endpoints > Advanced features > Tamper protection**.
 - [Attack surface reduction \(ASR\)](#) rules are enabled.
 - [Cloud protection](#) is enabled.
- Disable Exchange ActiveSync and OneDrive sync.
 - To disable Exchange ActiveSync for a mailbox, see [How to disable Exchange ActiveSync for users in Exchange Online](#).
 - To disable other types of access to a mailbox, see:
 - [Enable or disable MAPI for a mailbox](#).
 - [Enable or Disable POP3 or IMAP4 access for a user](#).
 - Pausing OneDrive sync will help protect your cloud data from being updated by potentially infected devices. For more information, see [How to Pause and Resume sync in OneDrive](#).
- Apply relevant patches and configuration changes on affected systems.
- Block ransomware communications using internal and external controls.
- Purge cached content

Investigation

Use this section to investigate the attack and plan your response.

Assess your current situation

- What initially made you aware of the ransomware attack?
 - If IT staff identified the initial threat—such as noticing backups being deleted, antivirus alerts, endpoint detection and response (EDR) alerts, or suspicious system changes—it is often possible to take quick decisive measures to thwart the attack, typically by the containment actions described in this article.
- What date and time did you first learn of the incident?
 - What system and security updates were not installed on devices on that date? This is important to understand what vulnerabilities might have been leveraged so they can be addressed on other devices.
 - What user accounts were used on that date?
 - What new user accounts were created since that date?
 - What programs were added to automatically start around the time that the incident occurred?
- Is there any indication that the attacker is currently accessing systems?
 - Are there any suspected compromised systems that are experiencing unusual activity?
 - Are there any suspected compromised accounts that appear to be actively used by the adversary?
 - Is there any evidence of active command-and-control (C2) servers in EDR, firewall, VPN, web proxy, and other logs?

Identify the ransomware process

- Using [advanced hunting](#), search for the identified process in the process creation events on other devices.

Look for exposed credentials in the infected devices

- For user accounts whose credentials were potentially compromised, reset the account passwords, and require the users to sign in again.
- The following IOAs might indicate lateral movement:

▼ Click to expand

- SuspiciousExploratoryCommands
- MLFileBasedAlert
- IfeoDebuggerPersistence

- SuspiciousRemoteFileDropAndExecution
- ExploratoryWindowsCommands
- IoaStickyKeys
- Mimikatz Defender Amplifier
- Network scanning tool used by PARINACOTA
- DefenderServerAlertMSSQLServer
- SuspiciousLowReputationFileDrop
- SuspiciousServiceExecution
- AdminUserAddition
- MimikatzArtifactsDetector
- Scuba-WdigestEnabledToAccessCredentials
- DefenderMalware
- MLSuspCmdBehavior
- MLSuspiciousRemotelInvocation
- SuspiciousRemoteComponentInvocation
- SuspiciousWmiProcessCreation
- MLCmdBasedWithRemoting
- Process Accesses Lsass
- Suspicious Rundll32 Process Execution
- BitsAdmin
- DefenderCobaltStrikeDetection
- DefenderHacktool
- IoaSuspPSCommandline
- Metasploit
- MLSuspToolBehavior
- RegistryQueryForPasswords
- SuspiciousWdavExclusion
- ASEPRegKey
- CobaltStrikeExecutionDetection
- DefenderBackdoor
- DefenderBehaviorSuspiciousActivity
- DefenderMalwareExecuted
- DefenderServerAlertDomainController
- DupTokenPrivilegeEscalationDetector
- FakeWindowsBinary
- IoaMaliciousCmdlets
- LivingOffTheLandBinary
- MicrosoftSignedBinaryAbuse
- MicrosoftSignedBinaryScriptletAbuse
- MLFileBasedWithRemoting

- MLSuspSvchostBehavior
- ReadSensitiveMemory
- RemoteCodeInjection-IREnabled
- Scuba-EchoSeenOverPipeOnLocalhost
- Scuba-SuspiciousWebScriptFileDrop
- Suspicious DLL registration by odbcconf
- Suspicious DPAPI Activity
- Suspicious Exchange Process Execution
- Suspicious scheduled task launch
- SuspiciousLdapQueryDetector
- SuspiciousScheduledTaskRegistration
- Untrusted application opens a RDP connection

Identify the line of business (LOB) apps that are unavailable due to the incident

- Does the app require an identity?
 - How is authentication performed?
 - How are credentials such as certificates or secrets stored and managed?
- Are evaluated backups of the application, its configuration, and its data available?
- Determine your compromise recovery process.

Eradication and recovery

Use these steps to eradicate the threat and recover damaged resources.

Step 1: Verify your backups

If you have offline backups, you can probably restore the data that has been encrypted after you have removed the ransomware payload (malware) from your environment and after you have verified that there's no unauthorized access in your Microsoft 365 tenant.

Step 2: Add indicators

Add any known attacker communication channels as indicators, blocked in firewalls, in your proxy servers, and on endpoints.

Step 3: Reset compromised users

Reset the passwords of any known compromised user accounts and require a new sign-in.

- Consider resetting the passwords for any privileged account with broad administrative authority, such as the members of the Domain Admins group.
- If a user account might have been created by an attacker, disable the account. Do not delete the account unless there are no plans to perform security forensics for the incident.

Step 4: Isolate attacker control points

Isolate any known attacker control points inside the enterprise from the Internet.

Step 5: Remove malware

Remove the malware from the affected devices.

- Run a full, current antivirus scan on all suspected computers and devices to detect and remove the payload that is associated with the ransomware.
- Do not forget to scan devices that synchronize data or the targets of mapped network drives.

Step 6: Recover files on a cleaned device

Recover files on a cleaned device.

- You can use [File History](#) in Windows 11, Windows 10, Windows 8.1, and System Protection in Windows 7 to attempt to recover your local files and folders.

Step 7: Recover files in OneDrive for Business

Recover files in OneDrive for Business.

- Files Restore in OneDrive for Business allows you to restore an entire OneDrive to a previous point in time within the last 30 days. For more information, see [Restore your OneDrive](#).

Step 8: Recover deleted email

Recover deleted email.

- In the rare case that the ransomware deleted all the email in a mailbox, you can recover the deleted items. See [Recover deleted messages in a user's mailbox in Exchange Online](#).

Step 9: Re-enable Exchange ActiveSync and OneDrive sync

- After you have cleaned your computers and devices and recovered the data, you can re-enable Exchange ActiveSync and OneDrive sync that you previously disabled in step 3 of containment.

Microsoft DART ransomware approach and best practices

Article • 02/01/2023 • 16 minutes to read

[Human-operated ransomware](#) is not a malicious software problem—it's a human criminal problem. The solutions used to address commodity problems aren't enough to prevent a threat that more closely resembles a nation-state threat actor who:

- Disables or uninstalls your antivirus software before encrypting files
- Disables security services and logging to avoid detection
- Locates and corrupts or deletes backups before sending a ransom demand

These actions are commonly done with legitimate programs that you might already have in your environment for administrative purposes. In criminal hands, these tools are used maliciously to carry out attacks.

Responding to the increasing threat of ransomware requires a combination of modern enterprise configuration, up-to-date security products, and the vigilance of trained security staff to detect and respond to the threats before data is lost.

The [Microsoft Detection and Response Team \(DART\)](#) responds to security compromises to help customers become cyber-resilient. DART provides onsite reactive incident response and remote proactive investigations. DART leverages Microsoft's strategic partnerships with security organizations around the world and internal Microsoft product groups to provide the most complete and thorough investigation possible.

This article describes how DART handles ransomware attacks for Microsoft customers so that you can consider applying elements of their approach and best practices for your own security operations playbook.

See these sections for the details:

- [How DART uses Microsoft security services](#)
- [The DART approach to conducting ransomware incident investigations](#)
- [DART recommendations and best practices](#)

Note

This article content was derived from the [A guide to combatting human-operated ransomware: Part 1](#) and [A guide to combatting human-operated ransomware:](#)

How DART uses Microsoft security services

DART relies heavily on data for all investigations and uses existing deployments of Microsoft security services such as [Microsoft Defender for Office 365](#), [Microsoft Defender for Endpoint](#), [Microsoft Defender for Identity](#), and [Microsoft Defender for Cloud Apps](#).

Defender for Endpoint

Defender for Endpoint is Microsoft's enterprise endpoint security platform designed to help enterprise network security analysts prevent, detect, investigate, and respond to advanced threats. Defender for Endpoint can detect attacks using advanced behavioral analytics and machine learning. Your analysts can use Defender for Endpoint for attacker behavioral analytics.

Here's an example of an alert in Microsoft Defender for Endpoint for a pass-the-ticket attack.

The screenshot shows the Microsoft Defender Security Center interface. The left sidebar has a tree view with nodes like 'janetl pc.ftpdemons.net' and 'Alerts > Pass-the-ticket attack'. The main pane displays a detailed alert for a 'Pass-the-ticket attack' on 'janetl pc.ftpdemons.net'. The alert is categorized as 'High' risk and 'New'. It includes sections for 'Alert story' (listing processes like 'nttakm.exe', 'smss.exe', 'smss.exe (92999999 00000004)', 'wminit.exe', 'services.exe', and 'PSXEXSVCE.exe'), 'Details' (showing incident details, detection source as EDR, and detection status as Detected), and 'Alert description' (mentioning a kerberos ticket file was created). There are also tabs for 'Manage alert' (with 'Classify this alert' and 'True alert' buttons) and 'Status' (set to 'New').

Your analysts can also perform advanced hunting queries to pivot off indicators of compromise (IOCs) or search for known behavior if they identify a threat actor group.

Here's an example of how advanced hunting queries can be used to locate known attacker behavior.

The screenshot shows the Microsoft Defender Security Center interface. On the left, the 'Advanced hunting' pane is open, displaying a schema tree for 'Devices' and 'Functions'. Under 'Functions', there are entries for 'FileProfile', 'AssignedIPAddresses', and 'DeviceFromIP'. Below these are 'Queries' sections for 'Shared queries', 'Community', 'Campaigns', 'Collection', and 'Command and Control'. In the center, a PowerShell query editor window is open with the following script:

```
// Finds PowerShell execution events that could involve a download.
DeviceProcessEvents
| where FileLineIn -in ("powershell.exe", "powershell_lse.exe")
| where ProcessCommandLine has ".Net.WebClient"
| or ProcessCommandLine has "DownloadofFile"
| or ProcessCommandLine has "Invoke-WebRequest"
| or ProcessCommandLine has "Invoke-Shellcode"
| or ProcessCommandLine has "Http"
| or ProcessCommandLine has "Start-FileTransfer"
| or ProcessCommandLine has "InvokeUnexec"
| or ProcessCommandLine has "PowerShell"

```

Below the query editor is a table showing event details like Timestamp, DeviceID, DeviceName, and Action. On the right, the 'Inspect record' pane is open, showing asset details for a machine named 'annette-pc' with a risk level of 'High' and exposure level 'High'. It also displays a process tree for 'powershell.exe' under 'WINWORD.EXE', showing its execution time (Aug 12, 2021, 11:44:29.897 PM) and path (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe). A detailed view of the process is shown on the far right.

In Defender for Endpoint, you have access to a real-time expert-level monitoring and analysis service by Microsoft Threat Experts for ongoing suspected actor activity. You can also collaborate with experts on demand for additional insights into alerts and incidents.

Here's an example of how Defender for Endpoint shows detailed ransomware activity.

The screenshot shows an 'Alerts > Ransomware activity detected on 4 devices' page. The main section is titled 'Ransomware activity detected on 4 devices' and shows two affected hosts: 'HOST01' and 'HOST01\administrator'. Below this is a 'What happened' summary and an 'Executive summary' which states: 'Microsoft Threat Experts are tracking a threat in your environment related to ransomware activity on 4 devices. These behaviors may have resulted in credential dumping, lead shell commands via Windows Management Interface (WMI), launch new commands via PowerShell, delete or move generated artifacts on a host system, use tools to persist on systems, disable security tools, attempt to cover their tracks, launch processes through remote file copy, automated collection, creation of an account to allow persistence, adding a program to a startup folder or referencing it with a Registry run key, command and control, using a remote access tool, data encryption for impact and inhibition of system recovery. In ransomware attacks, threat actors encrypt data on target systems to create an interruption in business operations which they then leverage for monetary gain.' It also mentions immediate action steps and a follow-up alert.

The 'Timeline of observed events' table lists specific malicious activities:

Date/Time	Actions
2021-05-08T12:20:54.872Z	T1003: OS Credential Dumping mimikatz.exe loaded crypt32.dll library
2021-05-08T12:20:59.368Z	lazagne.exe process executed command: lsAzoGiczzl
2021-05-08T12:21:02.646Z	T1003: OS Credential Dumping cmd.exe process executed command: reg.exe save hklm\system c:\users\<USER_NAME>\appdata\local\temp\qjgmyhuf
2021-05-08T12:41:34.827Z	T1490: Inhibit System Recovery cmd.exe process executed command: wmic SHADOWCOPY Delete

The 'Impacted device(s)' section lists the four devices involved. To the right, the 'Details' pane shows the alert status as 'Resolved', classification as 'True alert', and determination as 'Malware'. It also lists the detection source as 'Threat Experts', category as 'Ransomware', and techniques used, including T1003, T1113, T1114, T1105, T1490, T1119, and T1017.

Defender for Identity

You use Defender for Identity to investigate known compromised accounts and to find potentially compromised accounts in your organization. Defender for Identity sends alerts for known malicious activity that actors often use such as DC Sync attacks, remote

code execution attempts, and pass-the-hash attacks. Defender for Identity enables you to pinpoint suspect activity and accounts to narrow down the investigation.

Here's an example of how Defender for Identity sends alerts for known malicious activity related to ransomware attacks.

Alerts									
Export		1 Week	Manage alerts						
Filters: Service sources: Microsoft Defender for Identity									
Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last activity ↓
Security principal reconnaissance (LDAP)		■■■ Medium	Unsupported OS	● Resolved	Discovery	MDI	HOST01	Aug 15, 2021 2:45 AM	Aug 15, 2021 2:48 AM
Remote code execution attempt		■■■ Medium	Unsupported alert type	● Resolved	Execution	MDI	3 Hosts	Aug 13, 2021 9:32 AM	Aug 14, 2021 9:12 AM
Security principal reconnaissance (LDAP)		■■■ Medium		● Resolved	Discovery	MDI	HOST02	Aug 12, 2021 8:18 PM	Aug 13, 2021 5:03 PM
User and group membership reconnaissance ...		■■■ Medium		● Resolved	Discovery	MDI	HOST03 5 Acc...	Aug 12, 2021 9:26 PM	Aug 12, 2021 9:26 PM
Suspicious additions to sensitive groups		■■■ Medium	Unsupported alert type	● Resolved	Persistence	MDI	HOST04 2 Acc...	Aug 10, 2021 11:41 PM	Aug 10, 2021 11:41 PM

Defender for Cloud Apps

Defender for Cloud Apps (previously known as Microsoft Defender for Cloud Apps) allows your analysts to detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications. Defender for Cloud Apps is Microsoft's cloud access security broker (CASB) solution that allows for monitoring of cloud services and data access in cloud services by users.

Here's an example of the Defender for Cloud Apps dashboard, which allows analysis to detect unusual behavior across cloud apps.

Dashboard

Filter by app: All apps

<h4>Alerts</h4> <p>7 open alerts Over the last 30 days</p>  <p>Low severity Medium severity High severity</p> <p>Recent alerts:</p> <table><thead><tr><th>Alert</th><th>Date</th></tr></thead><tbody><tr><td>HVT Login from Non-Corporate</td><td>Aug 16, 2021</td></tr><tr><td>Impossible travel activity</td><td>Aug 16, 2021</td></tr><tr><td>Risky sign-in: Unfamiliar sign-i...</td><td>Aug 16, 2021</td></tr></tbody></table> <p>View all alerts</p>	Alert	Date	HVT Login from Non-Corporate	Aug 16, 2021	Impossible travel activity	Aug 16, 2021	Risky sign-in: Unfamiliar sign-i...	Aug 16, 2021	<h4>Discovered apps</h4> <p>No discovered apps Over the last 30 days Updated on Aug 16, 2021, 1:57 PM View all discovered apps</p>	<h4>Top users to investigate</h4> <p>1000+ users to investigate Investigation priority is calculated by the user's alerts and activities over the past 7 days</p> <table><thead><tr><th>Name</th><th>Investigation priority score</th></tr></thead><tbody><tr><td>MEGHAN BOWERS</td><td>250</td></tr><tr><td>JEFF LEATHERMAN</td><td>184</td></tr><tr><td>MIKE JONES</td><td>176</td></tr><tr><td>JOHN WOOD</td><td>171</td></tr><tr><td>JIM BOB</td><td>166</td></tr><tr><td>KAREN SMITH</td><td>146</td></tr><tr><td>HELP DESK</td><td>138</td></tr></tbody></table> <p>View all users to investigate</p>	Name	Investigation priority score	MEGHAN BOWERS	250	JEFF LEATHERMAN	184	MIKE JONES	176	JOHN WOOD	171	JIM BOB	166	KAREN SMITH	146	HELP DESK	138
Alert	Date																									
HVT Login from Non-Corporate	Aug 16, 2021																									
Impossible travel activity	Aug 16, 2021																									
Risky sign-in: Unfamiliar sign-i...	Aug 16, 2021																									
Name	Investigation priority score																									
MEGHAN BOWERS	250																									
JEFF LEATHERMAN	184																									
MIKE JONES	176																									
JOHN WOOD	171																									
JIM BOB	166																									
KAREN SMITH	146																									
HELP DESK	138																									

Microsoft Secure Score

The set of Microsoft 365 Defender services provides live remediation recommendations to reduce the attack surface. Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating that more improvement actions have been taken. See the [Secure Score](#) documentation to find out more about how your organization can leverage this feature to prioritize remediation actions that are based on their environment.

The DART approach to conducting ransomware incident investigations

You should make every effort to determine how the adversary gained access to your assets so that vulnerabilities can be remediated. Otherwise, it is highly likely that the same type of attack will take place again in the future. In some cases, the threat actor takes steps to cover their tracks and destroy evidence, so it is possible that the entire chain of events may not be evident.

The following are three key steps in DART ransomware investigations:

Step	Goal	Initial questions
1. Assess the current situation	Understand the scope	What initially made you aware of a ransomware attack? What time/date did you first learn of the incident? What logs are available and is there any indication that the actor is currently accessing systems?
2. Identify the affected line-of-business (LOB) apps	Get systems back online	Does the application require an identity? Are backups of the application, configuration, and data available? Are the content and integrity of backups regularly verified using a restore exercise?
3. Determine the compromise recovery (CR) process	Remove attacker control from the environment	N/A

Step 1. Assess the current situation

An assessment of the current situation is critical to understanding the scope of the incident and for determining the best people to assist and to plan and scope the investigation and remediation tasks. Asking the following initial questions is crucial in helping to determine the situation.

What initially made you aware of the ransomware attack?

If the initial threat was identified by IT staff—such as noticing backups being deleted, antivirus alerts, endpoint detection and response (EDR) alerts, or suspicious system changes—it is often possible to take quick decisive measures to thwart the attack, typically by disabling all inbound and outbound Internet communication. This may temporarily affect business operations, but that would typically be much less impactful than an adversary deploying ransomware.

If the threat was identified by a user call to the IT helpdesk, there may be enough advance warning to take defensive measures to prevent or minimize the effects of the attack. If the threat was identified by an external entity (like law enforcement or a financial institution), it is likely that the damage is already done, and you will see evidence in your environment that the threat actor has already gained administrative control of your network. This can range from ransomware notes, locked screens, or ransom demands.

What date/time did you first learn of the incident?

Establishing the initial activity date and time is important because it helps narrow the scope of the initial triage for quick wins by the attacker. Additional questions may include:

- What updates were missing on that date? This is important to understand what vulnerabilities may have been exploited by the adversary.
- What accounts were used on that date?
- What new accounts have been created since that date?

What logs are available, and is there any indication that the actor is currently accessing systems?

Logs—such as antivirus, EDR, and virtual private network (VPN)—are an indicator of suspected compromise. Follow-up questions may include:

- Are logs being aggregated in a Security Information and Event Management (SIEM) solution—such as [Microsoft Sentinel](#), Splunk, ArcSight, and others—and

current? What is the retention period of this data?

- Are there any suspected compromised systems that are experiencing unusual activity?
- Are there any suspected compromised accounts that appear to be actively used by the adversary?
- Is there any evidence of active command and controls (C2s) in EDR, firewall, VPN, web proxy, and other logs?

As part of assessing the current situation, you might need an Active Directory Domain Services (AD DS) domain controller that was not compromised, a recent backup of a domain controller, or a recent domain controller taken offline for maintenance or upgrades. Also determine whether [multifactor authentication \(MFA\)](#) was required for everyone in the company and if [Azure Active Directory \(Azure AD\)](#) was used.

Step 2. Identify the LOB apps that are unavailable due to the incident

This step is critical in figuring out the quickest way to get systems back online while obtaining the evidence required.

Does the application require an identity?

- How is authentication performed?
- How are credentials such as certificates or secrets stored and managed?

Are tested backups of the application, configuration, and data available?

- Are the contents and integrity of backups regularly verified using a restore exercise? This is particularly important after configuration management changes or version upgrades.

Step 3. Determine the compromise recovery process

This step may be necessary if you have determined that the control plane, which is typically AD DS, has been compromised.

Your investigation should always have a goal of providing output that feeds directly into the CR process. CR is the process that removes attacker control from an environment and tactically increase security posture within a set period. CR takes place post-security breach. To learn more about CR, read the Microsoft Compromise Recovery Security Practice team's [CRSP: The emergency team fighting cyber attacks beside customers](#) blog article.

Once you have gathered the responses to the questions above, you can build a list of tasks and assign owners. A key factor in a successful incident response engagement is thorough, detailed documentation of each work item (such as the owner, status, findings, date, and time), making the compilation of findings at the end of the engagement a straightforward process.

DART recommendations and best practices

Here are DART's recommendations and best practices for containment and post-incident activities.

Containment

Containment can only happen once the analysis has determined what needs to be contained. In the case of ransomware, the adversary's goal is to obtain credentials that allow administrative control over a highly available server and then deploy the ransomware. In some cases, the threat actor identifies sensitive data and exfiltrates it to a location they control.

Tactical recovery will be unique for your organization's environment, industry, and level of IT expertise and experience. The steps outlined below are recommended for short-term and tactical containment steps your organization can take. To learn more about for long-term guidance, see [securing privileged access](#). For a comprehensive view of ransomware and extortion and how to prepare and protect your organization, see [Human-operated ransomware](#).

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

- Which user accounts were compromised?
- Which devices are affected?
- Which applications are affected?

Step 2: Preserve existing systems

- Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.
- Isolate compromised systems from the network, but do not shut them off.

- Isolate at least one known good domain controller in every domain—two is even better. Either disconnect them from the network or shut them down entirely. The object here is to stop the spread of ransomware to critical systems—identity being among the most vulnerable. If all your domain controllers are virtual, ensure that the virtualization platform's system and data drives are backed up to offline external media that is not connected to the network, in case the virtualization platform itself is compromised.
- Isolate critical known good application servers, for example SAP, configuration management database (CMDB), billing, and accounting systems.

These two steps can be done concurrently as new threat vectors are discovered. Disable those threat vectors and then try to find a known good system to isolate from the network.

Other tactical containment actions can include:

- [Reset the krbtgt password](#), twice in rapid succession. Consider using a [scripted, repeatable process ↗](#). This script enables you to reset the krbtgt account password and related keys while minimizing the likelihood of Kerberos authentication issues being caused by the operation. To minimize potential issues, the krbtgt lifetime can be reduced one or more times prior to the first password reset so that the two resets are done quickly. Note that all domain controllers that you plan to keep in your environment must be online.
- Deploy a Group Policy to the entire domain(s) that prevents privileged login (Domain Admins) to anything but domain controllers and privileged administrative-only workstations (if any).
- Install all missing security updates for operating systems and applications. Every missing update is a potential threat vector that adversaries can quickly identify and exploit. Microsoft Defender for Endpoint's [Threat and Vulnerability Management](#) provides an easy way to see exactly what is missing—as well as the potential impact of the missing updates.
 - For Windows 10 (or higher) devices, confirm that the current version (or n-1) is running on every device.
 - Deploy [attack surface reduction \(ASR\) rules](#) to prevent malware infection.
 - Enable all [Windows 10 security features](#).
- Check that every external facing application, including VPN access, is protected by multifactor authentication, preferably using an authentication application that is running on a secured device.

- For devices not using Defender for Endpoint as their primary antivirus software, run a full scan with [Microsoft Safety Scanner](#) on isolated known good systems before reconnecting them to the network.
- For any legacy operating systems, upgrade to a supported OS or decommission these devices. If these options are not available, take every possible measure to isolate these devices, including network/VLAN isolation, Internet Protocol security (IPsec) rules, and login restrictions, so they are only accessible to the applications by the users/devices to provide business continuity.

The riskiest configurations consist of running mission critical systems on legacy operating systems as old as Windows NT 4.0 and applications, all on legacy hardware. Not only are these operating systems and applications insecure and vulnerable, if that hardware fails, backups typically cannot be restored on modern hardware. Unless replacement legacy hardware is available, these applications will cease to function. Strongly consider converting these applications to run on current operating systems and hardware.

Post-incident activities

DART recommends implementing the following security recommendations and best practices after each incident.

- Ensure that best practices are in place for [email and collaboration solutions](#) to make it more difficult for attackers to abuse them while allowing internal users to access external content easily and safely.
- Follow [Zero Trust](#) security best practices for remote access solutions to internal organizational resources.
- Starting with critical impact administrators, follow best practices for account security including using [passwordless authentication](#) or MFA.
- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
 - For cloud and forest/domain administrative access, use Microsoft's [privileged access model \(PAM\)](#).
 - For endpoint administrative management, use the [local administrative password solution \(LAPS\)](#).
- Implement data protection to block ransomware techniques and to confirm rapid and reliable recovery from an attack.

- Review your critical systems. Check for protection and backups against deliberate attacker erasure or encryption. It's important that you periodically test and validate these backups.
- Ensure rapid detection and remediation of common attacks on endpoint, email, and identity.
- Actively discover and continuously improve the security posture of your environment.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

PAM

Using the [PAM](#) (formerly known as the tiered administration model) enhances Azure AD's security posture. This involves:

- Breaking out administrative accounts in a "planed" environment—one account for each level, usually four:
- Control Plane (formerly Tier 0): Administration of domain controllers and other crucial identity services, such as Active Directory Federation Services (ADFS) or Azure AD Connect. This also includes server applications that require administrative permissions to AD DS, such as Exchange Server.
- The next two planes were formerly Tier 1:
 - Management Plane: Asset management, monitoring, and security.
 - Data/Workload Plane: Applications and application servers.
- The next two planes were formerly Tier 2:
 - User Access: Access rights for users (such as accounts).
 - App Access: Access rights for applications.
- Each one of these planes will have a *separate administrative workstation for each plane* and will only have access to systems in that plane. Other accounts from other planes will be denied access to workstations and servers in the other planes through user rights assignments set to those machines.

The net result of the PAM is that:

- A compromised user account will only have access to the plane to which it belongs.
- More sensitive user accounts will not be logging into workstations and servers with a lower plane's security level, thereby reducing lateral movement.

LAPS

By default, Microsoft Windows and AD DS have no centralized management of local administrative accounts on workstations and member servers. This usually results in a common password that is given for all these local accounts, or at the very least in groups of machines. This enables would-be attackers to compromise one local administrator account, and then use that account to gain access to other workstations or servers in the organization.

Microsoft's [LAPS](#) mitigates this by using a Group Policy client-side extension that changes the local administrative password at regular intervals on workstations and servers according to the policy set. Each of these passwords are different and stored as an attribute in the AD DS computer object. This attribute can be retrieved from a simple client application, depending on the permissions assigned to that attribute.

LAPS requires the AD DS schema to be extended to allow for the additional attribute, the LAPS Group Policy templates to be installed, and a small client-side extension to be installed on every workstation and member server to provide the client-side functionality.

You can get LAPS from the [Microsoft Download Center](#).

Incident response playbooks

Examine guidance for identifying and investigating these types of attacks:

- [Phishing](#)
- [Password spray](#)
- [App consent grant](#)

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices

- Microsoft 365 Defender incident response
- Microsoft Defender for Cloud (Azure)
- Microsoft Sentinel incident response

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021
- [Human-operated ransomware](#)
- [Rapidly protect against ransomware and extortion](#)
- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat](#) threat analytics report in the Microsoft 365 Defender portal
- [Microsoft DART ransomware case study](#)

Microsoft 365:

- [Deploy ransomware protection for your Microsoft 365 tenant](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)
- [Protect your Windows 10 PC from ransomware](#)
- [Handling ransomware in SharePoint Online](#)
- [Threat analytics reports for ransomware](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- [Find ransomware with advanced hunting](#)

Microsoft Azure:

- [Azure Defenses for Ransomware Attack](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Backup and restore plan to protect against ransomware](#)
- [Help protect from ransomware with Microsoft Azure Backup](#) (26-minute video)
- [Recovering from systemic identity compromise](#)
- [Advanced multistage attack detection in Microsoft Sentinel](#)
- [Fusion Detection for Ransomware in Microsoft Sentinel](#)

Microsoft Defender for Cloud Apps:

- [Create anomaly detection policies in Defender for Cloud Apps](#)

Microsoft Security team blog posts:

- [3 steps to prevent and recover from ransomware \(September 2021\)](#) ↗
- [A guide to combatting human-operated ransomware: Part 1 \(September 2021\)](#) ↗

Key steps on how Microsoft's DART conducts ransomware incident investigations.

- [A guide to combatting human-operated ransomware: Part 2 \(September 2021\)](#) ↗

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#) ↗

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#) ↗

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#) ↗

- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#) ↗

Compromised and malicious applications investigation

Article • 08/26/2022 • 16 minutes to read

This article provides guidance on identifying and investigating malicious attacks on one or more applications in a customer tenant. The step-by-step instructions will help you take the required remedial action to protect information and minimize further risks.

- **Prerequisites:** Covers the specific requirements you need to complete before starting the investigation. For example, logging that should be turned on, roles and permissions required, among others.
- **Workflow:** Shows the logical flow that you should follow to perform this investigation.
- **Investigation steps:** Includes a detailed step-by-step guidance for this specific investigation.
- **Containment steps:** Contains steps on how to disable the compromised applications.
- **Recovery steps:** Contains high-level steps on how to recover/mitigate from a malicious attack on compromised applications.
- **References:** Contains additional reading and reference materials.

Prerequisites

Before starting the investigation, make sure you have the correct tools and permissions to gather detailed information on the applications that you suspect to be compromised by the malicious attack.

- To leverage Identity protection signals, the tenant must be licensed for Azure Active Directory (Azure AD) Premium P2.
 - Understanding of the [Identity Protection risk concepts](#)
 - Understanding of the [Identity Protection investigation concepts](#)
- An account with the following directory roles:
 - Global administrator
 - Security administrator
- Ability to use [Microsoft Graph Explorer](#) and be familiar (to some extent) with the Microsoft Graph API.

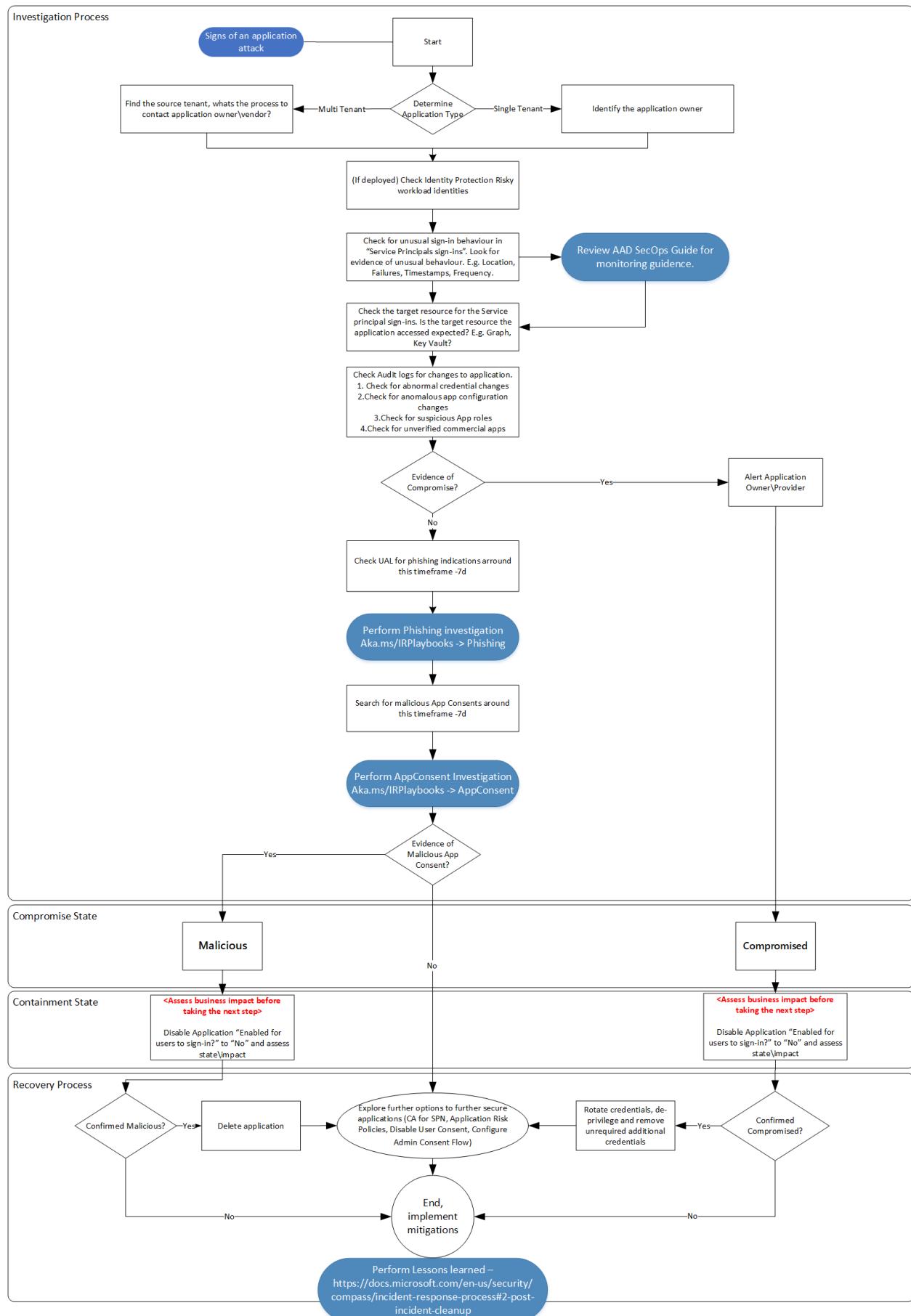
- Familiarize yourself with the [application auditing concepts](#) (part of <https://aka.ms/AzureADSecOps>).
- Make sure all Enterprise apps in your tenant have an owner set for the purposes of accountability. Review the concepts on [overview of app owners](#) and [assigning app owners](#).
- Familiarize yourself with the concepts of the [App Consent grant investigation](#) (part of <https://aka.ms/IRPlaybooks>).
- Make sure you understand the following Azure AD permissions:
 - [Risky permissions](#)
 - [Consent model and the Admin consent workflow](#)
- Familiarize yourself with the concepts of [Workload identity risk detections](#).
- You must have full Microsoft 365 E5 license to leverage Microsoft Defender for Cloud Apps.
 - Understand the concepts of [anomaly detection alert investigation](#)
- Familiarize yourself with the following application management policies:
 - [Azure AD application authentication methods API overview \(preview\)](#)
 - [appManagementPolicy resource type](#)
- Familiarize yourself with the following App Governance policies:
 - [The App Governance blog](#)
 - [App governance add-on to Defender for Cloud Apps](#)

Required tools

For an effective investigation, install the following PowerShell module and the toolkit on your investigation machine:

- [Azure AD Incident Response PowerShell Module](#)
- [Azure AD Toolkit](#)

Workflow



Investigation steps

For this investigation, it is assumed that you either have a indication for a potential application compromise in the form of a user report, Azure AD sign-in logs example, or Identity protection detection. Make sure to complete and enable all required prerequisite steps.

This playbook is created with the intention that not all Microsoft customers and their investigation teams will have the full Microsoft 365 E5 or Azure AD Premium P2 license suite available or configured in the tenant that is being investigated. We will however highlight additional automation capabilities when appropriate.

Determine application type

It is important to determine the type of application (multi or single tenant) early in the investigation phase to get the correct information needed to reach out to the application owner. For more information, see [Tenancy in Azure Active Directory](#).

Multi-tenant applications

For multi-tenant applications, the application is hosted and managed by a third party. Identify the process needed to reach out and report issues to the application owner.

Single-tenant applications

Find the contact details of the application owner within your organization. You can find it under the **Owners** tab on the **Enterprise Applications** section. Alternatively, your organization may have a database that has this information.

You can also execute this Microsoft Graph query:

```
HTTP
```

```
GET https://graph.microsoft.com/v1.0/applications/{id}/owners
```

Check Identity Protection - risky workload identities

This feature is in preview at the time of writing this playbook and licensing requirements will apply to its usage. Risky workload identities can be the trigger to investigate a Service Principal, but can also be used to further investigate into other triggers you may have identified. You can check the **Risk State** of a Service Principal using the **Identity Protection - risky workload identities** tab, or you can use Microsoft Graph API.

rove > Security

Security | Risk detections

Search (Ctrl+ /)

Getting started

Protect

- Conditional Access
- Identity Protection
- Security Center
- Continuous access evaluation
- Verifiable credentials (Preview)

Manage

- Identity Secure Score
- Named locations
- Authentication methods
- MFA

Report

Learn more Download Refresh

Something went wrong. Please retry.

Auto refresh : Every 5 minutes

Detection type : Leaked credentials

User detections	Workload identity
Detection time ↑	Activity time
3/30/2022, 3:11:19 PM	3/30/2022, 3:11:19 PM
3/30/2022, 11:05:00 AM	3/30/2022, 11:05:00 AM
3/16/2022, 7:16:54 PM	3/16/2022, 7:16:54 PM
3/16/2022, 7:15:28 PM	3/16/2022, 7:15:28 PM
3/16/2022, 7:11:21 PM	3/16/2022, 7:11:21 PM

Risk Detection Details

Service principal's risk report Service principal's sign-ins ...

Detection type	Suspicious sign-ins ⓘ
Risk state	At risk
Risk level	High
Risk detail	-
Source	Unknown
Detection timing	Offline
Activity	Service Principal
Detection time	1/11/2022, 6:59 PM
Detection last updated	1/11/2022, 6:59 PM
Application ID	971b68fa-7541-4192-be59-c0ff3b5e1851
Key ID	3f932b5b-2bd6-4d09-8817-fb174bab9d3
Service principal name	Contoso Sales Tracker
Service principal ID	1baef386-7491-4ee6-9376-72c5a66e7805

Risk Detection Details

Service principal's risk report Service principal's sign-ins ...

Detection type : Leaked credentials ⓘ

Learn how to investigate ↗

Risk state	At risk
Risk level	High
Risk detail	-
Source	Identity Protection
Detection timing	Offline
Activity	Service Principal
Detection time	3/16/2022, 7:16 PM
Detection last updated	3/16/2022, 7:16 PM
Application ID	ede08db0-9492-4a0c-8ae3-8ddd056c5d75
Key ID	d4b0863a-4c14-4719-8478-a3b87882fbde
Service principal name	Contoso HR App
Service principal ID	0fbef39d-9e8c-460b-860e-8ae5abcdffd7
Additional info	Click here for more details ↗

```

    "id": "e407433475eb8535760466a74166db5d680c0e384914355d22675895b8436a5f",
    "requestId": null,
    "correlationId": null,
    "riskEventType": "leakedCredentials",
    "riskState": "atRisk",
    "riskLevel": "high",
    "riskDetail": "none",
    "source": "IdentityProtection",
    "detectionTimingType": "offline",
    "activity": "servicePrincipal",
    "tokenIssuerType": "AzureAD",
    "ipAddress": null,
    "activityDateTime": "2022-02-16T02:09:15.7173479Z",
    "detectedDateTime": "2022-02-16T02:09:15.7173479Z",
    "lastUpdatedDateTime": "2022-02-16T02:09:15Z",
    "servicePrincipalId": "db734a9a-e775-4847-9a40-557ecb27705f",
    "servicePrincipalDisplayName": "Contoso Front Desk",
    "appId": "e1337603-ebe0-4739-82ce-f3c80d1a0d17",
    "keyIds": [],
    "additionalInfo": "[{\\"Key\\":\\"alertUrl\\",\\"Value\\":\\"https://github.com/eitzman/Maximum_effort/blob/c983800966a0cac689695c391be93c9eac680ee3/time_to_make_the_chimichangas.txt#L2\\"}]",
    "location": null
}

```

Check for unusual sign-in behavior

The first step of the investigation is to look for evidence of unusual authentications patterns in the usage of the Service Principal. Within the Azure portal, Azure Monitor, Azure Sentinel, or the Security Information and Event Management (SIEM) system of your organization's choice, look for the following in the **Service principal sign-ins** section:

- Location - is the Service Principal authenticating from locations\IP addresses that you would not expect?
- Failures - are there a large number of authentication failures for the Service Principal?
- Timestamps - are there successful authentications that are occurring at times that you would not expect?
- Frequency - is there an increased frequency of authentications for the Service Principal?
- Leak Credentials - are any application credentials hard coded and published on a public source like GitHub?

If you have deployed Identity Protection - risky workload identities, check the **Suspicious Sign-ins and Leak Credentials detections**. For more information, see [workload identity risk detentions](#).

Check the target resource

Within Service principal sign-ins, also check the **Resource** that the Service Principal was accessing during the authentication. It is important to have input from the application

owner as they will be familiar with which resources the Service Principal should be accessing.

Application	Azure AD Domain Services Sync
Application ID	f9b1f212-f117-47ae-9e26-355e0ec5f9f2
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000

Check for abnormal credential changes

Use Audit logs to get information on credential changes on applications and service principals. Filter for **Category** by Application Management, and **Activity** by **Update Application – Certificates and secrets management**.

- Check whether there are newly created or unexpected credentials assigned to the service principal.
- Check for credentials on Service Principal using Microsoft Graph API.
- Check both the application and associated service principal objects.
- Check any [custom role](#) that maybe have been created or modified. Note the permissions marked below:

<input type="checkbox"/> microsoft.directory/applications.myOrganization/allProperties/read	Read all properties of single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/allProperties/update	Update all properties on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/audience/update	Update the supported account type on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/authentication/update	Update the reply URL, logout URL, implicit flow, and publisher domain on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/basic/update	Update basic properties of single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/credentials/update	Update the certificates and client secrets on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/delete	Delete single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/owners/read	Read owners on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/owners/update	Update owner on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/permissions/update	Update exposed permissions and required permissions on single-directory applications.
<input type="checkbox"/> microsoft.directory/applications.myOrganization/standard/read	Read standard properties of single-directory applications.

If you have deployed the app governance add-on, check the Azure portal for alerts relating to the application. For more information, see [Get started with app threat detection and remediation](#).

If you have deployed Identity Protection, check the "Risk detections" report and in the user or workload identity "risk history".

The screenshot shows the Microsoft Defender for Cloud Apps portal under the 'Security' section. On the left, there's a navigation menu with categories like 'Getting started', 'Protect', 'Manage', and 'Report'. The main area is titled 'Risk detections' and shows a single alert: 'Something went wrong. Please retry.' with an auto-refresh interval of 'Every 5 minutes'. The alert type is 'Leaked credentials'. Below this, there's a table of user detections for 'Workload identity'.

Detection time	Activity time
3/30/2022, 3:11:19 PM	3/30/2022, 3:11:19 PM
3/30/2022, 11:05:00 AM	3/30/2022, 11:05:00 AM
3/16/2022, 7:16:54 PM	3/16/2022, 7:16:54 PM
3/16/2022, 7:15:28 PM	3/16/2022, 7:15:28 PM
3/16/2022, 7:11:21 PM	3/16/2022, 7:11:21 PM

To the right, a detailed view of the first detection is shown:

Risk Detection Details

- Detection type:** Suspicious sign-ins [Learn how to investigate](#)
- Risk state:** At risk
- Risk level:** High
- Risk detail:** -
- Source:** Unknown
- Detection timing:** Offline
- Activity:** Service Principal
- Detection time:** 1/11/2022, 6:59 PM
- Detection last updated:** 1/11/2022, 6:59 PM
- Application ID:** 971b68fa-7541-4192-be59-c0ff3b5e1851
- Key ID:** 3f932b5b-2bd6-4d09-8817-fb174bab9d3
- Service principal name:** Contoso Sales Tracker
- Service principal ID:** 1baef386-7491-4ee6-9376-72c5a66e7805

If you have deployed Microsoft Defender for Cloud Apps, ensure that the "Unusual addition of credentials to an OAuth app" policy is enabled, and check for open alerts. For more information, see [Unusual addition of credentials to an OAuth app](#).

Additionally, you can query the `servicePrincipalRiskDetections` and user `riskDetections` APIs to retrieve these risk detections.

Search for anomalous app configuration changes

- Check the API permissions assigned to the app to ensure that the permissions are consistent with what is expected for the app.
- Check Audit logs (filter **Activity** by **Update Application** or **Update Service Principal**).
- Confirm whether the connection strings are consistent and whether has the sign-out URL has been modified.
- Confirm whether the domains in the URL are in-line with those registered.
- Determine whether anyone has added an unauthorized redirect URL.
- Confirm ownership of the redirect URI that you own to ensure it did not expire and was claimed by an adversary.

Also, if you have deployed Microsoft Defender for Cloud Apps, check the Azure portal for alerts relating to the application you are currently investigating. Not all alert policies are enabled by default for OAuth apps, so ensure that these are all enabled. For more information, see the [OAuth app policies](#). You can also view information about the apps prevalence and recent activity under the **Investigation > OAuth Apps** tab.

Check for suspicious application roles

- This can also be investigated using the Audit logs. Filter Activity by **Add app role assignment to service principal**.
- Confirm whether the assigned roles have high privilege.
- Confirm whether those privileges are necessary.

Check for unverified commercial apps

- Check whether commercial gallery (published and verified versions) applications are being used.

Check for indications of keyCredential property information disclosure

Review your tenant for potential keyCredential property information disclosure as outlined in [CVE-2021-42306 ↗](#).

To identify and remediate impacted Azure AD applications associated with impacted Automation Run-As accounts, please navigate to the [remediation guidance Github Repo ↗](#).

Important

Evidence of compromise: If you discover evidence of compromise, then it is important to take the steps highlighted in the containment and recovery sections. This will help address the risk, but will need further investigation to understand the source of the compromise to avoid further impact and ensure bad actors are removed.

There are two primary methods of gaining access to systems via the use of applications. The first involves an application being consented to by an administrator or user, usually via a phishing attack. This would be part of initial access to a system and is often referred to as "consent phishing".

The second method involves an already compromised administrator account creating a new app for the purposes of persistence, data collection and to stay under the radar. For example, an OAuth app could be created by a compromised administrator with a seemingly innocuous name, avoiding detection and allowing long term access to data without the need for an account. This is often seen in nation state attacks.

Below are some of the steps which can be taken to investigate further.

Check M365 Unified Audit Log (UAL) for phishing indications for the past 7 days

Sometimes, when attackers use malicious or compromised applications as a means of persistence or to exfiltrate data, a phishing campaign is involved. Based on the findings from the previous steps, you should review the identities of:

- Application Owners
- Consent Admins

Review the identities for indications of phishing attacks in the last 24 hours. Increase this time span if needed to 7, 14, and 30 days if there are no immediate indications. For a detailed phishing investigation playbook, see the [Phishing Investigation Playbook](#).

Search for malicious application consents for the past 7 days

To get an application added to a tenant, attackers spoof users or admins to consent to applications. To know more about the signs of an attack, see the [Application Consent Grant Investigation Playbook](#).

Check application consent for the flagged application

Check Audit logs

To see all consent grants for that application, filter Activity by **Consent to application**.

- Use the Azure AD Portal Audit Logs
- Use Microsoft Graph to query the Audit logs
 - a) Filter for a specific time frame:

HTTP

```
GET https://graph.microsoft.com/v1.0/auditLogs/auditLogs/directoryAudits?  
&$filter=activityDateTime le 2022-01-24
```

- b) Filter the Audit Logs for 'Consent to Applications' audit log entries:

HTTP

```

https://graph.microsoft.com/v1.0/auditLogs/directoryAudits?directoryAudits?
$filter=ActivityType eq 'Consent to application'

"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#auditLogs/directoryAudits",
"value": [
  {
    "id": "Directory_0da73d01-0b6d-4c6c-a083-
afc8c968e655_78XJB_266233526",
    "category": "ApplicationManagement",
    "correlationId": "0da73d01-0b6d-4c6c-a083-afc8c968e655",
    "result": "success",
    "resultReason": "",
    "activityDisplayName": "Consent to application",
    "activityDateTime": "2022-03-25T21:21:37.9452149Z",
    "loggedByService": "Core Directory",
    "operationType": "Assign",
    "initiatedBy": {
      "app": null,
      "user": {
        "id": "8b3f927e-4d89-490b-aaa3-e5d4577f1234",
        "displayName": null,
        "userPrincipalName": "admin@contoso.com",
        "ipAddress": "55.154.250.91",
        "userType": null,
        "homeTenantId": null,
        "homeTenantName": null
      }
    },
    "targetResources": [
      {
        "id": "d23d38a1-02ae-409d-884c-60b03cad989",
        "displayName": "Graph explorer (official site)",
        "type": "ServicePrincipal",
        "userPrincipalName": null,
        "groupType": null,
        "modifiedProperties": [
          {
            "displayName": "ConsentContext.IsAdminConsent",
            "oldValue": null,
            "newValue": "\"True\""
          },
        ]
      }
    ]
  }
]

```

c) Use Log Analytics

```

AuditLogs
| where ActivityDisplayName == "Consent to application"

```

For more information, see the [Application Consent Grant Investigation Playbook](#).

Determine if there was suspicious end-user consent to the application

A user can authorize an application to access some data at the protected resource, while acting as that user. The permissions that allow this type of access are called "delegated permissions" or [user consent](#).

To find apps that have been consented by users, use LogAnalytics to search the Audit logs:

```
AuditLogs  
| where ActivityDisplayName == "Consent to application" and  
(parse_json(tostring(parse_json(tostring(TargetResources[0].modifiedProperties))[0].newValue)) <> "True")
```

Check Audit logs to find whether the permissions granted are too broad (tenant-wide or admin-consented)

Reviewing the permissions granted to an application or Service Principal can be a time-consuming task. Start with understanding the potentially [risky permissions](#) in Azure AD.

Now, follow the guidance on how to enumerate and review permissions in the [App consent grant investigation](#).

Check whether the permissions were granted by user identities that should not have the ability to do this, or whether the actions were performed at strange dates and times

Review using Audit Logs:

```
AuditLogs  
| where OperationName == "Consent to application"  
//| where parse_json(tostring(TargetResources[0].modifiedProperties))  
[4].displayName == "ConsentAction.Permissions"
```

You can also use the Azure AD Audit logs, filter by **Consent to application**. In the Audit Log details section, click **Modified Properties**, and then review the

ConsentAction.Permissions:

Audit Log Details			
Activity	Target(s)	Modified Properties	
Target	Property Name	Old Value	New Value
Graph exp...	ConsentContext...	"True"	
Graph exp...	ConsentContext...	"False"	
Graph exp...	ConsentContext...	"False"	
Graph exp...	ConsentContext...	"WindowsAzureActiveDirectoryIntegratedApp"	
Graph exp...	ConsentAction....	"[[Id: oTg90q4CnUCITGCwPK3JiXq_sHy-kV5LnYXsSNlcUgp-kj-LiU0LSaqj5dRXf4lv, ClientId: d23d38a1-02ae-409d-884c-60b03cad989, PrincipalId: 8b3f927e-4d89-490b-aaa3-e5d4577f896f, ResourceId: 7cb0bf7a-91be-4b5e-9d85-ec48d95c520a, ConsentType: Principal, Scope: UserAuthenticationMethod.Read UserAuthenticationMethod.Read.All UserAuthenticationMethod.ReadWrite UserAuthenticationMethod.ReadWrite.All openid profile Policy.Read.All Policy.Read.ConditionalAccess Policy.Read.PermissionGrant Policy.ReadWrite.ApplicationConfiguration Policy.ReadWrite.AuthenticationFlows Policy.ReadWrite.AuthenticationMethod Policy.ReadWrite.Authorization Policy.ReadWrite.ConditionalAccess Policy.ReadWrite.ConsentRequest Policy.ReadWrite.DeviceConfiguration Policy.ReadWrite.FeatureRollout Policy.ReadWrite.PermissionGrant Policy.ReadWrite.TrustFramework Group.Read.All Group.ReadWrite.All PrivilegedAccess.Read.AzureAD PrivilegedAccess.Read.AzureResources PrivilegedAccess.ReadWrite.AzureAD PrivilegedAccess.ReadWrite.AzureADGroup PrivilegedAccess.ReadWrite.AzureResources Directory.AccessAsUser.All Directory.Read.All Directory.ReadWrite.All IdentityProvider.Read.All offline_access Application.Read.All Application.ReadWrite.All, CreatedDateTime: , LastModifiedDateTime]] => [[Id: oTg90q4CnUCITGCwPK3JiXq_sHy-	

Containment steps

Once you have identified one or more applications or workload identities as either malicious or compromised, you may not immediately want to roll the credentials for this application, nor you want to immediately delete the application. It is highly recommended, that you follow the best practice guidance for [incident response](#).

 **Important**

Before you perform the following step, your organization must weigh up the security impact and the business impact of disabling an application. If the business impact of disabling an application is too great, then consider preparing and moving to the Recovery stage of this process.

Disable compromised application

A typical containment strategy involves the disabling of sign-ins to the application identified, to give your incident response team or the affected business unit time to evaluate the impact of deletion or key rolling. If your investigation leads you to believe that administrator account credentials have also been compromised, this type of activity should be coordinated with an eviction event to ensure that all routes to accessing the tenant are cut off simultaneously.

A screenshot of the Azure portal showing the properties of a GitHub Enterprise Application. The 'Properties' tab is active. A warning message at the top right says: "Setting 'Enabled for users to sign-in' to 'No' blocks all users from accessing the application. Ensure that users do not need to access the application before setting to 'No'." Below this, there are fields for 'Name' (set to GitHub.com), 'Homepage URL' (set to https://github.com/business), and a 'Logo' (the GitHub logo). On the left sidebar, other tabs like 'Overview', 'Deployment Plan', and 'Manage' are visible.

You can also use the following PowerShell code to disable the sign-in to the app:

PowerShell

```
# The AppId of the app to be disabled
$appId = "{AppId}"

# Check if a service principal already exists for the app
$servicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$appId'"
if ($servicePrincipal) {
    # Service principal exists already, disable it
    Set-AzureADServicePrincipal -ObjectId $servicePrincipal.ObjectId -
    AccountEnabled $false
} else {
    # Service principal does not yet exist, create it and disable it at the
    # same time
    $servicePrincipal = New-AzureADServicePrincipal -AppId $appId -
```

```
    AccountEnabled $false  
}
```

Recovery steps

Remediate Service Principals

1. List all credentials assigned to the **Risky Service Principal**. The best way to do this is to perform a Microsoft Graph call using GET ~/application/{id} where id passed is the application object ID.
 - Parse the output for credentials. The output may contain passwordCredentials or keyCredentials. Record the keyIds for all.

```
"keyCredentials": [],  
    "parentalControlSettings": {  
        "countriesBlockedForMinors": [],  
        "legalAgeGroupRule": "Allow"  
    },  
    "passwordCredentials": [  
        {  
            "customKeyIdentifier": null,  
            "displayName": "Test",  
            "endDateTime": "2021-12-16T19:19:36.997Z",  
            "hint": "7~-",  
            "keyId": "9f92041c-46b9-4ebc-95fd-e45745734bef",  
            "secretText": null,  
            "startDateTime": "2021-06-16T18:19:36.997Z"  
        }  
    ],
```

2. Add a new (x509) certificate credential to the application object using the application addKey API.

```
POST ~/applications/{id}/addKey
```

3. Immediately remove all old credentials. For each old password credential, remove it by using:

```
POST ~/applications/{id}/removePassword
```

For each old key credential, remove it by using:

```
POST ~/applications/{id}/removeKey
```

4. Remediate all Service Principals associated with the application. Follow this if your tenant hosts/registers a multi-tenant application, and/or registers multiple service principals associated to the application. Perform similar steps to what is listed above:

- GET ~/servicePrincipals/{id}
- Find passwordCredentials and keyCredentials in the response, record all old keyIds
- Remove all old password and key credentials. Use:

```
POST ~/servicePrincipals/{id}/removePassword and POST  
~/servicePrincipals/{id}/removeKey for this, respectively.
```

Remediate affected Service Principal resources

Remediate KeyVault secrets that the Service Principal has access to by rotating them, in the following priority:

- Secrets directly exposed with [GetSecret](#) calls.
- The rest of the secrets in exposed KeyVaults.
- The rest of the secrets across exposed subscriptions.

For more information, see [Interactively removing and rolling over the certificates and secrets of a Service Principal or Application](#).

For Azure AD SecOps guidance on applications, see [Azure Active Directory security operations guide for Applications](#).

In order of priority, this scenario would be:

- Update Graph PowerShell cmdlets (Add/Remove ApplicationKey + ApplicationPassword) doc to include examples for credential roll-over.
- Add custom cmdlets to Microsoft Graph PowerShell that simplifies this scenario.

Disable or delete malicious applications

An application can either be disabled or deleted. To disable the application, under **Enabled for users to sign in**, move the toggle to **No**.

You can delete the application, either temporarily or permanently, in the Azure portal or through the Microsoft Graph API. When you soft delete, the application can be recovered up to 30 days after deletion.

```
DELETE /applications/{id}
```

To permanently delete the application, use this Microsoft Graph API call:

```
DELETE /directory/deletedItems/{id}
```

If you disable or if you soft delete the application, set up monitoring in Azure AD Audit logs to learn if the state changes back to enabled or recovered.

Logging for enabled:

- **Service** - Core Directory
- **Activity Type** - Update Service Principle
- **Category** - Application Management
- **Initiated by (actor)** - UPN of actor
- **Targets** - App ID and Display Name
- **Modified Properties** - Property Name = account enabled, new value = true

Logging for recovered:

- **Service** - Core Directory
- **Activity Type** - Add Service Principle
- **Category** - Application Management
- **Initiated by (actor)** - UPN of actor
- **Targets** - App ID and Display Name
- **Modified Properties** - Property name = account enabled, new value = true

Implement Identity Protection for workload identities

Suspicious sign-ins: When risk detection indicates unusual sign-in properties or patterns, as well as unusual addition of credentials to an OAuth App, that may be an indicator of compromise. The detection baselines sign-in behavior between 2 and 60 days, and fires if one or more of the following unfamiliar properties occur during a subsequent sign-in:

- IP address / ASN
- Target resource
- User agent
- Hosting/non-hosting IP change
- IP country
- Credential type

When this detection is fired, the account is marked as high risk because this can indicate account takeover for the subject application. Note that the legitimate changes to an application's configuration will sometimes trigger this detection.

For more information, see [Securing workload identities with Identity Protection](#).

These alerts appear in the Identity Protection portal and can be exported into SIEM tools through the [Identity Protection APIs](#).

The screenshot shows the Microsoft Azure Security - Risk detections page. The URL is https://portal.azure.com/?Microsoft_AAD_IAM_security.riskyServicePrincipals=true#blade/Microsoft_AAD_RiskyServicePrincipalsBlade. The user is balas@contoso.com from the CONTOSO tenant. The main title is "Security | Risk detections". On the left, there's a sidebar with "Getting started", "Protect" (Conditional Access, Identity Protection, Security Center), "Manage" (Continuous access evaluation, Verifiable credentials (Preview)), and "Report". The main content area has a search bar and filters for "Auto refresh: Off", "Detection time: Last 90 days", "Show dates as: Local", "Detection type: None Selected", "Risk state: 2 selected", "Risk level: None Selected", and "Add filters". Below these filters, there are two tabs: "User detections" (selected) and "Workload identity detections" (highlighted with a red box). A table lists detected entities with columns: Detection time, Service principal name, Detection type, Risk state, and Risk level. The first row shows "10/31/2021, 11:40:48 PM" for "Risky Test App 2", "Risk detected" for detection type, "Confirmed compromised" for risk state, and "High" for risk level. The second row shows "10/27/2021, 12:13:00 PM" for "Risky Test App 3", "Risk detected" for detection type, "Confirmed compromised" for risk state, and "High" for risk level. The third row shows "10/19/2021, 8:53:56 PM" for "AADIP-SP-Risk-Test-App", "Azure AD threat intelli..." for detection type, "At risk" for risk state, and "High" for risk level. The fourth row shows "10/19/2021, 8:00:00 PM" for "Risky Test App 3", "Risk detected" for detection type, "At risk" for risk state, and "High" for risk level. The fifth row shows "10/19/2021, 8:00:00 PM" for "Risky Test App 2", "Risk detected" for detection type, "At risk" for risk state, and "High" for risk level.

Detection time	Service principal name	Detection type	Risk state	Risk level
10/31/2021, 11:40:48 PM	Risky Test App 2	Risk detected	Confirmed compromised	High
10/27/2021, 12:13:00 PM	Risky Test App 3	Risk detected	Confirmed compromised	High
10/19/2021, 8:53:56 PM	AADIP-SP-Risk-Test-App	Azure AD threat intelli...	At risk	High
10/19/2021, 8:00:00 PM	Risky Test App 3	Risk detected	At risk	High
10/19/2021, 8:00:00 PM	Risky Test App 2	Risk detected	At risk	High

Conditional Access for risky workload identities

Conditional Access allows you to block access for specific accounts that you designate when Identity Protection marks them as "at risk." Note that the enforcement through

Conditional Access is currently limited to single-tenant applications only.

The screenshot shows the 'New Conditional Access policy' configuration page. It includes sections for 'Control access based on Conditional Access policy' (with a link to 'Learn more'), 'Name' (set to 'Risk for Workload Identities'), 'Assignments' (with 'Users or workload identities' and 'Specific service principals included' options), 'Cloud apps or actions' (set to 'All cloud apps'), 'Conditions' (set to '1 condition selected'), 'Access controls' (set to 'Block access'), and 'Service principal risk (Preview)' (set to '2 included'). A note indicates that some conditions are not available due to the 'Workload identities (Preview)' selection. On the right, there's a 'Configure service principal risk levels' section with 'Yes' selected, and checkboxes for 'High', 'Medium', and 'Low' risk levels.

For more information, see [Conditional Access for workload identities](#).

Implement application risk policies

Review user consent settings

Review the user consent settings under **Azure Active Directory > Enterprise applications > Consent and permissions > User consent settings**.

The screenshot shows the 'User consent for applications' configuration page. It includes a note about configuring whether users are allowed to consent for applications to access the organization's data. Three options are listed: 'Do not allow user consent' (radio button unselected, note: 'An administrator will be required for all apps.'), 'Allow user consent for apps from verified publishers, for selected permissions (Recommended)' (radio button selected, note: 'All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.' and '7 permissions classified as low impact'), and 'Allow user consent for apps' (radio button unselected, note: 'All users can consent for any app to access the organization's data.').

To review configuration options, see [Configure how users consent to apps](#).

Implement admin consent flow

When an application developer directs users to the admin consent endpoint with the intent to give consent for the entire tenant, it is known as admin consent flow. To ensure the admin consent flow works properly, application developers must list all permissions in the `RequiredResourceAccess` property in the application manifest.

Most organizations disable the ability for their users to consent to applications. To give users the ability to still request consent for applications and to have an administrative review capability, it is recommended to implement the admin consent workflow. Follow the [admin consent workflow steps](#) to configure it in your tenant.

For high privileged operations such as admin consent, you have a privileged access strategy defined as per our [guidance](#).

Review risk-based step-up consent settings

Risk-based step-up consent helps reduce user exposure to malicious apps. For example, consent requests for newly registered multi-tenant apps that are not publisher verified and require non-basic permissions are considered risky. If a risky user consent request is detected, the request requires a "step-up" to admin consent instead. This step-up capability is enabled by default, but it results in a behavior change only when user consent is enabled.

Make sure it is enabled in your tenant and review the configuration settings outlined [here](#).

References

- [Incident Response Playbooks](#)
- [App consent grant](#)
- [Azure AD Identity Protection risks](#)
- [Azure AD security monitoring guide](#)
- [Application auditing concepts](#)
- [Configure how users consent to applications](#)
- [Configure the admin consent workflow](#)
- [Unusual addition of credentials to an OAuth app](#)
- [Securing workload identities with Identity Protection](#)
- [Holistic compromised identity signals from Microsoft](#)

Additional incident response playbooks

Examine guidance for identifying and investigating these additional types of attacks:

- [Phishing](#)
- [Password spray](#)
- [App consent grant](#)
- [Microsoft DART ransomware approach and best practices](#)

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices
- [Microsoft 365 Defender](#) incident response
- [Microsoft Defender for Cloud \(Azure\)](#)
- [Microsoft Sentinel](#) incident response

Microsoft Security Best Practices module: Identity and access management

Article • 08/26/2022 • 2 minutes to read

Identity and access management is critical to both security assurances as an access control as well as enterprise enablement of applications and services.

The following videos provide guidance on identity and access management.

Part 1: Introduction - Identity Attacks & Key Capabilities (5:44 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6Dr?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6Dr?postJs||Msg=true)

Part 2: Consistency (4:20 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qe8t?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qe8t?postJs||Msg=true)

Part 3: Critical Best Practices (4:24 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qh9s?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qh9s?postJs||Msg=true)

Part 4: Password (Hash) Synchronization with Cloud (4:08 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6DU?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6DU?postJs||Msg=true)

Part 5: Password Protection from Cloud (3:00 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qbKb?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qbKb?postJs||Msg=true)

Part 6: General Guidance (2:38 long)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qbKi?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qbKi?postJs||Msg=true)

Next steps

See the [Identity and access management](#) and [Capabilities](#) topics.

See also

[PowerPoint slides](#) for the Microsoft Azure Security Compass Workshop

[Zero Trust Security Model and Framework ↗](#)

[Microsoft security documentation](#)

Microsoft security best practices for identity and access management

Article • 02/01/2023 • 7 minutes to read

In cloud-based architecture, identity provides the basis of a large percentage of security assurances. While legacy IT infrastructure often heavily relied on firewalls and network security solutions at the internet egress points for protection against outside threats, these controls are less effective in cloud architectures with shared services being accessed across cloud provider networks or the internet.

It is challenging or impossible to write concise firewall rules when you don't control the networks where these services are hosted, different cloud resources spin up and down dynamically, cloud customers may share common infrastructure, and employees and users expect to be able to access data and services from anywhere. To enable all these capabilities, you must manage access based on identity authentication and authorization controls in the cloud services to protect data and resources and to decide which requests should be permitted.

Additionally, using a cloud-based identity solution like Azure Active Directory (Azure AD) offers additional security features that legacy identity services cannot because they can apply threat intelligence from their visibility into a large volume of access requests and threats across many customers.

A single enterprise directory

Best practice: Establish a single enterprise directory for managing identities of full-time employees and enterprise resources.

A single authoritative source for identities increases clarity and consistency for all roles in IT and Security. This reduces security risk from human errors and automation failures resulting from complexity. By having a single authoritative source, teams that need to make changes to the directory can do so in one place and have confidence that their change will take effect everywhere.

For Azure, designate a single Azure AD tenant as the authoritative source for your organization's accounts.

For more information, see [What is hybrid identity?](#)

Synchronized identity systems

Best practice: Synchronize your cloud identity with your existing identity systems.

Consistency of identities across cloud and on-premises will reduce human errors and resulting security risk. Teams managing resources in both environments need a consistent authoritative source to achieve security assurances.

For Azure, synchronize Azure AD with your existing authoritative on-premises Active Directory Domain Services (AD DS) using [hybrid identity](#).

This is also required for an Office 365 migration, so it is often already done before Azure migration and development projects begin.

Cloud provider identity source for third parties

Best practice: Use cloud identity services to host non-employee accounts such as vendors, partners, and customers, rather than including them in your on-premises directory.

This reduces risk by granting the appropriate level of access to external entities instead of the full default permissions given to full-time employees. This least privilege approach and clear differentiation of external accounts from company staff makes it easier to prevent and detect attacks coming in from these vectors. Additionally, management of these identities is done by the external also increases productivity by parties, reducing effort required by company HR and IT teams.

For example, these capabilities natively integrate into the same Azure AD identity and permission model used by Azure and Office 365:

- [Azure AD](#) for employees and enterprise resources.
- [Azure AD B2B](#) for business partners.
- [Azure AD B2C](#) customers or citizens.

For more information, see the [Azure AD federation compatibility list](#).

Passwordless or multi-factor authentication for administrative accounts

Best practice: All users should be converted to use passwordless authentication or multi-factor authentication (MFA) over time.

The details of this recommendation are in the administration section [passwordless or multi-factor authentication for admins](#)

The same recommendation applies to all users but should be applied first and strongest to accounts with administrative privileges.

You can also reduce use of passwords by applications using [Managed Identities](#) to grant access to resources in Azure.

Block legacy authentication

Best practice: Disable insecure legacy protocols for internet-facing services.

Legacy authentication methods are among the top attack vectors for cloud-hosted services. Created before multifactor-authentication existed, legacy protocols don't support additional factors beyond passwords and are therefore prime targets for password spraying, dictionary, or brute force attacks. As an example, nearly 100% of all password spray attacks against Office 365 customers use legacy protocols. Additionally, these older protocols frequently lack other attack countermeasures, such as account lockouts or back-off timers. Services running on Microsoft's cloud that block legacy protocols have observed a 66% reduction in successful account compromises.

For Azure and other Azure AD-based accounts, configure [Conditional Access to block legacy protocols](#).

Disabling legacy authentication can be difficult, as some users may not want to move to new client software that supports modern authentication methods. However, moving away from legacy authentication can be done gradually. Start by using metrics and logging from your authentication provider to determine the how many users still authenticate with old clients. Next, disable any down-level protocols that aren't in use, and set up Conditional Access for all users who aren't using legacy protocols. Finally, give plenty of notice and guidance to users on how to upgrade before blocking legacy authentication for all users on all services at a protocol level.

No on-premises admin accounts in cloud identity providers

Best practice: Don't synchronize highly privileged Active Directory Domain Services accounts (like Domain, Enterprise, and Schema admins) to Azure AD.

This mitigates the risk of an adversary pivoting to full control of on-premises assets following a successful compromise of a cloud account. This helps contain the scope of an incident from growing significantly.

This is related to the [critical impact account dependencies](#) guidance that mitigates the inverse risk of pivoting from on-premises to cloud assets.

Modern password protection

Best practice: Provide modern and effective protections for accounts that cannot go passwordless ([passwordless or multi-factor authentication for admins](#)).

Legacy identity providers mostly checked to make sure passwords had a good mix of character types and minimum length, but we have learned that these controls in practice led to passwords with less entropy that could be cracked easier:

- Microsoft - <https://www.microsoft.com/research/publication/password-guidance/>
- NIST - <https://pages.nist.gov/800-63-3/sp800-63b.html>

Identity solutions today need to be able to respond to types of attacks that didn't even exist one or two decades ago such as password sprays, breach replays (also called *credential stuffing*) that test username/password pairs from other sites' breaches, and phishing man-in-the-middle attacks. Cloud identity providers are uniquely positioned to offer protection against these attacks. Since they handle such large volumes of sign-ons, they can apply better anomaly detection and use a variety of data sources to both proactively notify companies if their users' passwords have been found in other breaches, as well as validate that any given sign in appears legitimate and is not coming from an unexpected or known-malicious host.

Additionally, synchronizing passwords to the cloud to support these checks also add resiliency during some attacks. Customers affected by (Not)Petya attacks were able to continue business operations when password hashes were synchronized to Azure AD (vs. near zero communications and IT services for customers affected organizations that had not synchronized passwords).

For Azure, enable modern protections in Azure AD with these steps:

1. [Implement password hash synchronization with Azure AD Connect sync](#)
2. Choose whether to automatically remediate these issues or manually remediate them based on a report:
 - **Automatic Enforcement** - Automatically remediate high risk passwords with Conditional Access [leveraging Azure AD Identity Protection risk assessments](#)
 - **Report & Manually Remediate** - View reports and manually remediate accounts

- **Azure AD reporting** - Risk events are part of Azure AD's security reports. For more information, see the [users at risk security report](#) and the [risky sign-ins security report](#).
- **Azure AD Identity Protection** - Risk events are also part of the reporting capabilities of [Azure Active Directory Identity Protection](#).

Use the [Identity Protection risk events API](#) to gain programmatic access to security detections using Microsoft Graph.

Cross-platform credential management

Best practice: Use a single identity provider for authenticating all platforms (Windows, Linux, and others) and cloud services.

A single identity provider for all enterprise assets will simplify management and security, minimizing the risk of oversights or human mistakes. Deploying multiple identity solutions (or an incomplete solution) can result in unenforceable password policies, passwords not reset after a breach, proliferation of passwords (often stored insecurely), and former employees retaining passwords after termination.

For example, Azure AD can be used to authenticate:

- Windows
- [Linux](#)
- Azure
- Office 365
- [Amazon Web Services \(AWS\)](#)
- [Google Services](#)
- Remote access to [legacy on-premises applications](#)
- Third-party [SaaS providers](#)

Conditional Access for users with Zero Trust

Best practice: Authentication for all users should include measurement and enforcement of key security attributes to support a Zero Trust strategy.

The details of this recommendation are in [Common Zero Trust identity and device access policies](#). The same recommendation applies to all users, but should be applied first to accounts with administrative privileges.

You can also reduce use of passwords by applications using [Managed Identities](#) to grant access to resources in Azure.

Simulate attacks

Best practice: Regularly simulate attacks against your users to educate and empower them.

People are a critical part of your defense, so ensure they have the knowledge and skills to avoid and resist attacks will reduce your overall organizational risk.

You can use [Attack simulation training in Microsoft Defender for Office 365](#) or any number of third-party offerings.

Next step

Review identity and device access [capabilities](#).

See also

[Zero Trust Security Model and Framework](#) ↗

[Microsoft security documentation](#)

Identity and access management capabilities

Article • 08/26/2022 • 3 minutes to read

This article lists capabilities that can help with identity.

Cloud identity services

Capability	Description	See more
Azure Active Directory (Azure AD)	Establish a single Azure AD enterprise directory for managing identities of full-time employees and enterprise resources. A single authoritative source increases clarity and consistency for all roles in IT and security and reduces security risk from human errors and automation failures resulting from complexity.	Azure Active Directory documentation
Azure AD Connect	Synchronize Azure AD with your existing authoritative on-premises Active Directory using Azure AD connect. This is also required for an Office 365 migration, so it is often already done before Azure migration and development projects begin.	What is hybrid identity with Azure Active Directory?
Azure AD B2B collaboration	Use Azure AD business-to-business (B2B) collaboration to host non-employee accounts like vendors and partners. This reduces risk by granting the appropriate level of access to external entities instead of the full default permissions given to full-time employees. This least privilege approach and clear differentiation of external accounts from company staff makes it easier to prevent and detect attacks coming in from these vectors.	Azure Active Directory B2B documentation
Azure AD B2C	Use Azure AD B2C for consumer and citizen accounts. Azure AD B2C is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page (SPA), and other applications.	Azure Active Directory B2C documentation

Identity security capabilities

Capability	Description	More information
Azure Multi-Factor Authentication (MFA)	MFA provides additional security by requiring a second form of authentication.	How MFA works
Passwordless authentication	<p>Azure AD supports several methods of passwordless authentication, including Windows Hello for Business, Microsoft Authenticator app, and FIDO2 security keys. Passwordless authentication methods are convenient because the password is removed and replaced with something you have, plus something you are or something you know.</p>	Passwordless authentication options for Azure Active Directory
Conditional Access	<p>With Conditional Access, Azure AD evaluates the conditions of the user login and uses conditional access policies you create to allow access. For example, you can create a Conditional Access policy to require device compliance for access to sensitive data. This greatly reduces the risk that a person with a stolen identity can access your sensitive data. It also protects sensitive data on the devices, because the devices must meet specific requirements for health and security.</p>	Conditional Access documentation Common Conditional Access policies
Azure AD self-service password reset (SSPR)	<p>SSPR allows your users to reset their passwords securely and without helpdesk intervention, by providing verification of multiple authentication methods that the administrator can control.</p>	How it works: Azure AD self-service password reset
Azure Active Directory Identity Protection	<p>Azure AD Identity Protection enables you to detect potential vulnerabilities affecting your organization's identities and configure automated remediation policy to low, medium, and high sign-in risk and user risk.</p>	What is Azure Active Directory Identity Protection?
Azure AD password protection for Windows Server Active Directory	<p>Protect on-premises Active Directory accounts with Azure AD password protection. This does the same checks on-premises as Azure AD does for cloud-based changes. These checks are performed during password changes and password reset scenarios.</p>	Enforce Azure AD password protection for Windows Server Active Directory

Additional identity security capabilities for administrators

Capability	Description	More information
Azure AD Privileged Identity Management	Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.	What is Azure AD Privileged Identity Management?
Managed Identities	You can reduce use of passwords by applications using Managed Identities to grant access to resources in Azure	What are managed identities for Azure resources?

See also

[Zero Trust Security Model and Framework](#)

[Microsoft security documentation](#)

Microsoft Security Best Practices module: Network security and containment

Article • 06/08/2022 • 2 minutes to read

Network Security & Containment helps reduce organizational risk by providing access controls to limit the ability of attackers to traverse the enterprise environment without impeding legitimate communications and interactions.

See the [Network security and containment](#) and [Capabilities](#) topics for more information.

The following videos provide guidance on network security and containment. You can also download the [PowerPoint slides](#) associated with these videos.

Part 1: Introduction - Overview of Azure Network Security (21:31)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7f?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7f?postJs||Msg=true)

Part 2: Enterprise Consistency & Segmentation Alignment (04:15)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qhbs?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qhbs?postJs||Msg=true)

Part 3: Pragmatic Containment Strategy (04:14)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjui?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjui?postJs||Msg=true)

Part 4: Internet Edge Strategy (01:59)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6G3?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6G3?postJs||Msg=true)

Part 5: ExpressRoute Termination (02:24)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Nd?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Nd?postJs||Msg=true)

Part 6: Deprecating Legacy Technology (02:35)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9H4?postJsllMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9H4?postJsllMsg=true)

Part 7: Subnet & NSG Design (03:04)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9H5?postJsllMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9H5?postJsllMsg=true)

Part 8: DDoS Mitigations (02:41)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuA?postJsllMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuA?postJsllMsg=true)

Part 9: Azure Ingress/Egress Security (02:08)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuL?postJsllMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjuL?postJsllMsg=true)

Part 10: Advanced Visibility (02:09)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7i?postJsllMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm7i?postJsllMsg=true)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Network security and containment

Article • 06/08/2022 • 11 minutes to read

Network security has been the traditional lynchpin of enterprise security efforts. However, cloud computing has increased the requirement for network perimeters to be more porous and many attackers have mastered the art of attacks on identity system elements (which nearly always bypass network controls). These factors have increased the need to focus primarily on identity-based access controls to protect resources rather than network-based access controls.

These do diminish the role of network security controls, but do not eliminate it entirely. While network security is no longer the primary focus for securing cloud-based assets, it is still a top priority for the large portfolio of legacy assets (which were built with the assumption that a network firewall-based perimeter was in place). Many attackers still employ scanning and exploit methods across public cloud provider IP ranges, successfully penetrating defenses for those who don't follow basic network security hygiene. Network security controls also provide a defense-in-depth element to your strategy that help protect, detect, contain, and eject attackers who make their way into your cloud deployments.

In the category of network security and containment, we have the following best practice recommendations:

- Align network segmentation with overall strategy
- Centralize network management and security
- Build a network containment strategy
- Define an internet edge strategy

Centralize network management and security

Centralize the organizational responsibility for management and security of core networking functions such as cross-premises links, virtual networking, subnetting, and IP address schemes as well as network security elements such as virtual network appliances, encryption of cloud virtual network activity and cross-premises traffic, network-based access controls, and other traditional network security components.

When you centralize network management and security you reduce the potential for inconsistent strategies that can create potential attacker exploitable security risks. Because all divisions of the IT and development organizations do not have the same

level of network management and security knowledge and sophistication, organizations benefit from leveraging a centralized network team's expertise and tooling.

[Microsoft Defender for Cloud](#) can be used to help centralize the management of network security.

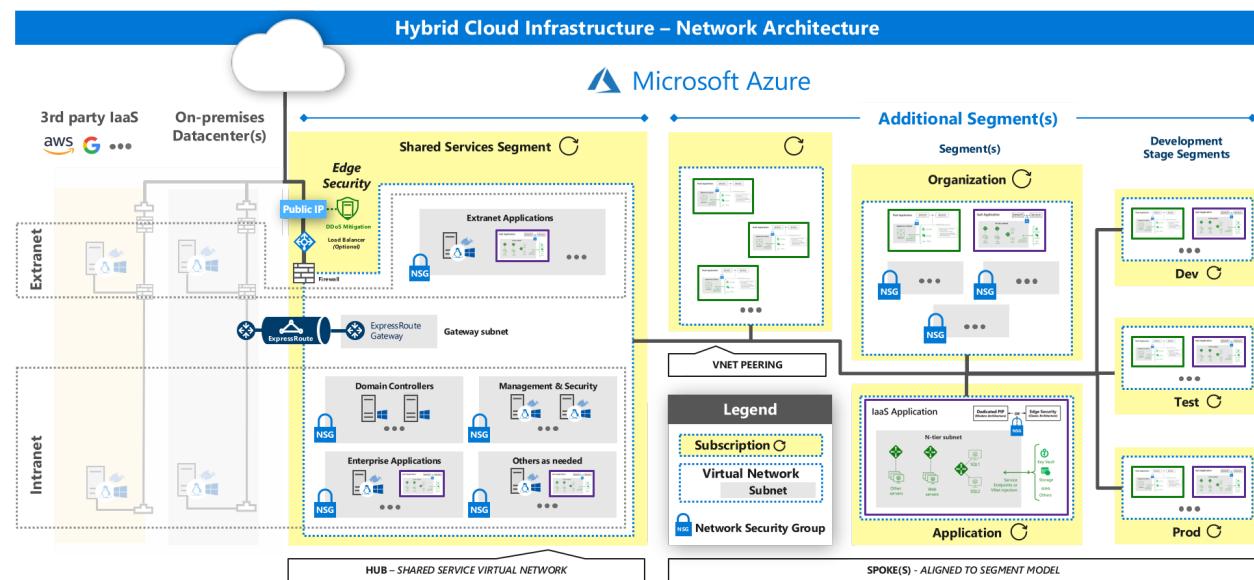
Align network segmentation with enterprise segmentation strategy

Align your network segmentation model with the enterprise segmentation model for your organization (defined in Governance, Risk, and Compliance section).

This will reduce confusion and resulting challenges with different technical teams (networking, identity, applications, etc.) each developing their own segmentation and delegation models that don't align with each other. This leads to a straightforward and unified security strategy, which helps reduce the number of errors due to human error and inability to increase reliability through automation.

Please compare images in [Network security and containment](#).

Reference Enterprise Design - Azure Network Security



Evolve security beyond network controls

Ensure technical controls can effectively prevent, detect, and respond to threats outside the networks you control.

As organizations shift to modern architectures, many services and components required for applications will be accessed over the internet or on cloud provider networks, often by mobile and other devices off the network. Traditional network controls based on a “*trusted intranet*” approach will not be able to effectively provide security assurances for these applications. This shifting landscape is captured well by principles documented by the [Jericho Forum](#) and ‘Zero Trust’ approaches.

Build a risk containment strategy based on a combination of network controls and application, identity, and other control types.

- Ensure that resource grouping and administrative privileges align to the segmentation model (see figure XXXX)
- Ensure you are designing security controls that identify and allow expected traffic, access requests, and other application communications between segments. Monitor communications between segments to identify any unexpected communications so you can investigate whether to set alerts or block traffic to mitigate risk of adversaries crossing segmentation boundaries.

Build a security containment strategy

Create a risk containment strategy that blends proven approaches including:

- Existing network security controls and practices
- Native security controls available in Azure
- Zero-trust approaches

Containment of attack vectors within an environment is critical. However, in order to be effective in cloud environments, traditional approaches may prove inadequate and security organizations need to evolve their methods.

- Consistency of controls across on-premises and cloud infrastructure is important, but defenses are more effective and manageable when leveraging native capabilities provided by a cloud service provider, dynamic just-in-time (JIT) approaches, and integrated identity and password controls, such as those recommended by zero trust/continuous validation approaches.
- A network security best practice is to make sure there are network access controls between network constructs. These constructs can represent virtual networks, or subnets within those virtual networks. This works to protect and contain East-West traffic within your cloud network infrastructure.

- An important network security design decision is to use or not use host-based firewalls. Host-based firewalls support a comprehensive defense in-depth strategy. However, to be of most use they require significant management overhead. If your organization has found them effective in helping you protect and discover threats in the past, you might consider using them for your cloud-based assets. If you discover that they have not added significant value, discontinue their use and explore native solutions on your cloud service provider's platform that deliver similar value.

An evolving emerging best practice recommendation is to adopt a Zero Trust strategy based on user, device, and application identities. In contrast to network access controls that are based on elements such as source and destination IP address, protocols, and port numbers, Zero Trust enforces and validates access control at "access time". This avoids the need to play a prediction game for an entire deployment, network, or subnet – only the destination resource needs to provide the necessary access controls.

- Azure Network Security Groups can be used for basic layer 3 & 4 access controls between Azure Virtual Networks, their subnets, and the Internet.
- Azure Web Application Firewall and the Azure Firewall can be used for more advanced network access controls that require application layer support.
- Local Admin Password Solution (LAPS) or a third-party Privileged Access Management can set strong local admin passwords and just in time access to them

Additionally, third parties offer microsegmentation approaches that may enhance your network controls by applying zero trust principles to networks you control with legacy assets on them.

Define an internet edge strategy

Choose whether to use native cloud service provider controls or virtual network appliances for internet edge security.

Internet edge traffic (sometimes referred to as "North-South" traffic) represents network connectivity between your assets in the cloud and the Internet. Legacy workloads require protection from Internet endpoints because they were built with the assumption that an internet firewall protected them against these attacks. An Internet edge strategy is intended to mitigate as many attacks from the internet as is reasonable to detect or block.

There are two primary choices that can provide Internet edge security controls and monitoring:

- Cloud Service Provider Native Controls ([Azure Firewall](#) + [Web Application Firewall (WAF)]/azure/application-gateway/waf-overview))
- Partner Virtual Network Appliances (Firewall and WAF Vendors available in [Azure Marketplace](#))
- Cloud service provider native controls typically offer basic security that is good enough for common attacks, such as the OWASP Top 10.
- In contrast, cloud service provider partner capabilities often provide much more advanced features that can protect against sophisticated (but often uncommon) attacks. Partner solutions consistently cost more than native controls. In addition, configuration of partner solutions can be very complex and more fragile than native controls because they do not integrate with cloud's fabric controllers.

The decision to use native versus partner controls should be based on your organization's experience and requirements. If the features of the advanced firewall solutions don't provide sufficient return on investment, you may consider using the native capabilities that are designed to be easy to configure and scale.

Discontinue legacy network security technology

Discontinue the use of signature-based Network Intrusion Detection/Network Intrusion Prevention (NIDS/NIPS) Systems and Network Data Leakage/Loss Prevention (DLP).

The major cloud service providers already filter for malformed packets and common network layer attacks, so there's no need for a NIDS/NIPS solution to detect those. In addition, traditional NIDS/NIPS solutions are typically driven by signature-based approaches (which are considered outdated) and are easily evaded by attackers and typically produce a high rate of false positives.

Network-based DLP is decreasingly effective at identifying both inadvertent and deliberate data loss. The reason for this is that most modern protocols and attackers use network-level encryption for inbound and outbound communications. The only viable workaround for this is "SSL-bridging" which provides an "authorized man-in-the-middle" that terminates and then reestablishes encrypted network connections. The SSL-bridging approach has fallen out of favor because of the level of trust required for the partner running the solution and the technologies that are being used.

Based on this rationale, we offer an all-up recommendation that you discontinue use of these legacy network security technologies. However, if your organizational experience

is that these technologies have had a palpable impact on preventing and detecting real attacks, you can consider porting them to your cloud environment.

Design virtual network subnet security

Design virtual networks and subnets for growth.

Most organizations end up adding more resources to their networks than they initially planned for. When this happens, IP addressing and subnetting schemes need to be refactored to accommodate the extra resources. This is a labor-intensive process. There is limited security value in creating a very large number of small subnets and then trying to map network access controls (such as security groups) to each of them.

We recommend that you plan your subnets based on common roles and functions that use common protocols for those roles and functions. This allows you to add resources to the subnet without needing to make changes to security groups that enforce network level access controls.

Do not use “*all open*” rules for inbound and outbound traffic to and from subnets. Use a *network “least privilege”* approach and only allow relevant protocols. This will decrease your overall network attack surface on the subnet.

All open rules (allowing inbound/outbound to and from 0.0.0.0-255.255.255.255) provide a false sense of security since such a rule enforces no security at all.

However, the exception to this is if you want to use security groups only for network logging. We do not recommend this, but it is an option if you have another network access control solution in place.

[Azure Virtual Network subnets](#) can be designed in this way.

Mitigate DDoS attacks

Enable Distributed Denial of Service (DDoS) mitigations for all business-critical web application and services.

DDoS attacks are prevalent and are easily carried out by unsophisticated attackers. There are even “DDoS as a service” options on the dark net. DDoS attacks can be very debilitating and completely block access to your services and even take down the services, depending on the type of DDoS attack.

The major cloud service providers offer DDoS protection of services of varying effectiveness and capacity. The cloud service providers typically provide two DDoS

protection options:

- DDoS protection at the cloud network fabric level – all customers of the cloud service provider benefit from these protections. The protection is usually focused at the network (layer 3) level.
- DDoS protection at higher levels that profile your services – this kind of protection will baseline your deployments and then use machine learning techniques to detect anomalous traffic and proactively protect based on their protection before there is service degradation

We recommend that you adopt the advance protection for any services where downtime will have negative impact on the business.

An example of advanced DDoS protection is the [Azure DDoS Protection Service](#).

Decide upon an internet ingress/egress policy

Choose to route traffic destined for the Internet through on-premises security devices or allow Internet connectivity through cloud-based network security devices.

Routing Internet traffic through on-premises network security devices is also known as “forced tunneling”. In a forced tunneling scenario, all connectivity to the Internet is forced back to on-premises network security devices through a cross-premises WAN link. The goal is to provide network security teams greater security and visibility for Internet traffic. Even when your resources in the cloud try to respond to incoming requests from the Internet, the responses will be forced through on-premises network security devices.

Alternately, forced tunneling fits a “*datacenter expansion*” paradigm and can work well for a quick proof of concept, but scales poorly because of the increased traffic load, latency, and cost.

The recommended approach for production enterprise use is to allow cloud resources to initiate and respond to Internet request directly through cloud network security devices defined by your [internet edge strategy](#).

The direct Internet approach fits the Nth datacenter paradigm (for example, Azure datacenters are a natural part of my enterprise). This approach scales much better for an enterprise deployment as it removes hops that add load, latency, and cost.

We recommend that you avoid [forced tunneling](#) for the reasons noted above.

Enable enhanced network visibility

You should enable enhanced network visibility by integrating network logs into a Security information and event management (SIEM) like Microsoft Sentinel or a third partner solution such as Splunk, QRadar, or ArcSight ESM.

Integrating logs from your network devices, and even raw network traffic itself, will provide you greater visibility over potential security threats flowing over the wire. This log information can be integrated in advanced SIEM solutions or other analytics platforms. The modern machine learning based analytics platforms support ingestion of extremely large amounts of information and can analyze large datasets very quickly. In addition, these solutions can be tuned to significantly reduce false positive alerts.

Examples of network logs that provide visibility include:

- Security group logs – [flow logs](#) and diagnostic logs
- [Web application firewall logs](#)
- [Virtual network taps](#) and their equivalents
- [Azure Network Watcher](#)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Network security and containment capabilities

Article • 06/08/2022 • 3 minutes to read

This article lists capabilities that can help with network traffic and containment.

Capabilities that work with SaaS, PaaS, and IaaS apps

Capability	Description	More information
Azure ExpressRoute	Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections.	Azure ExpressRoute Azure ExpressRoute for Office 365

Capabilities that work with PaaS and IaaS apps

Capability	Description	More information
Azure Application Gateway	Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port. With Application Gateway, you can make routing decisions based on additional attributes of an HTTP request, such as URI path or host headers.	What is Azure Application Gateway?
Azure Traffic Manager	Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.	What is Traffic Manager?

Additional capabilities for IaaS apps

Capability	Description	More information
Azure Virtual Network	<p>Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.</p>	What is Azure Virtual Network?
Point-to-site virtual private network (VPN) and Site-to-site VPN	<p>You can connect your on-premises computers and networks to a virtual network using any combination of these VPN options and Azure ExpressRoute.</p>	Point-to-site VPN
Security groups and Network virtual appliances	<p>You can filter network traffic between subnets using either or both of these options.</p> <p>Network security groups and application security groups can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.</p>	Network security groups
	<p>A network virtual appliance is a VM that performs a network function, such as a firewall, WAN optimization, or other network function.</p>	Application security groups Network virtual appliances (Azure Marketplace)
Route tables and border gateway protocol (BGP) routes	<p>Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the options to override the default routes Azure creates.</p>	Route tables About BGP with Azure VPN Gateway

Capability	Description	More information
Azure DDoS Protection	<p>Azure DDoS protection, combined with application design best practices, provide defense against DDoS attacks.</p> <p>Azure DDoS Protection Basic is automatically enabled as part of the Azure platform and provides real-time mitigation of common network-level attacks.</p> <p>DDoS Protection Standard provides additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard can mitigate the following types of attacks: volumetric attacks, protocol attacks, and resource (application) layer attacks.</p>	Azure DDoS Protection Standard overview
Azure Firewall	Cloud-native network security to protect your Azure Virtual Network resources.	Azure Firewall

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Securing privileged access

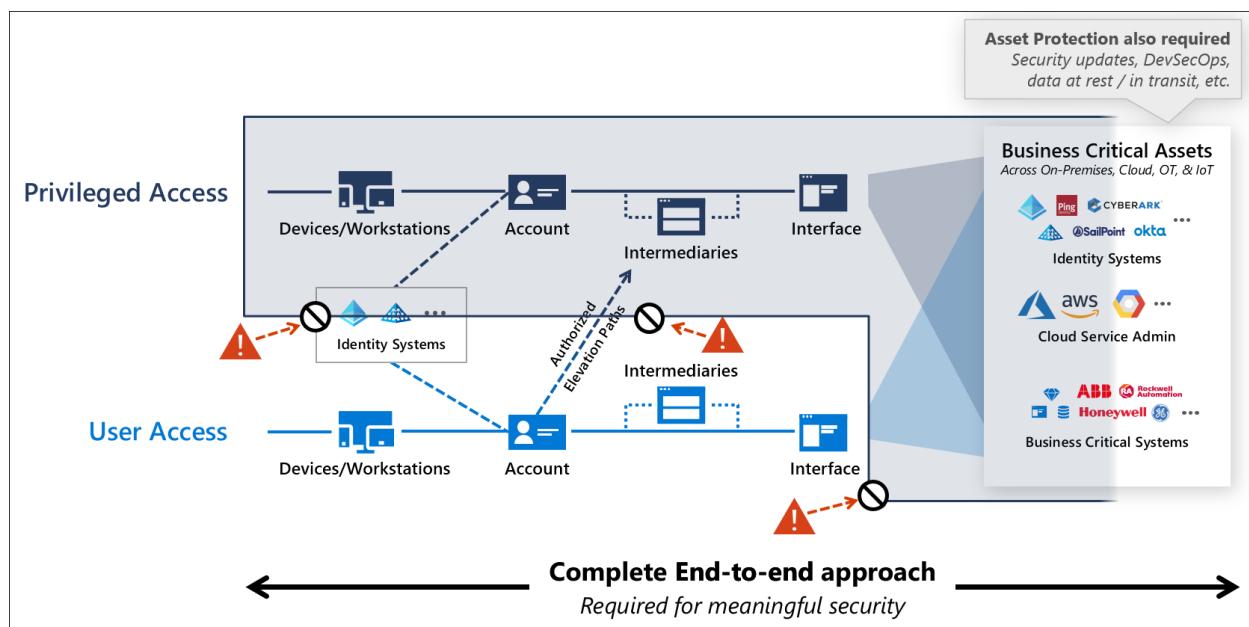
Article • 12/16/2022 • 2 minutes to read

Organizations should make securing privileged access the top security priority because of the significant potential business impact (and high likelihood) of attackers compromising this level of access.

Privileged access includes IT administrators with control of large portions of the enterprise estate and other users with access to business critical assets.

Attackers frequently exploit weaknesses in privileged access security during [human operated ransomware attacks](#) and targeted data theft. Privileged access accounts and workstations are so attractive to attackers because these targets allow them to rapidly gain broad access to the business assets in the enterprise, often resulting in rapid and significant business impact.

The following diagram summarizes the recommended privileged access strategy to create an isolated virtual zone that these sensitive accounts can operate in with low risk.



Securing privileged access effectively seals off unauthorized pathways completely and leaves a select few authorized access pathways that are protected and closely monitored. This diagram is discussed in more detail in the article, [Privileged Access Strategy](#).

Building this strategy requires a holistic approach combining multiple technologies to protect and monitor those authorized escalation paths using Zero Trust principles including explicit validation, least privilege, and assume breach. This strategy requires

multiple complementary initiatives that establish a holistic technology approach, clear processes, and rigorous operational execution to build and sustain assurances over time.

Get started and measure progress

Image	Description	Image	Description
	<p>Rapid Modernization Plan (RaMP)</p> <ul style="list-style-type: none">- Plan and implement the most impactful quick wins		<p>Best practices Videos and Slides</p>

Industry references

Securing privileged access is also addressed by these industry standards and best practices.

UK National Cyber Security Center (NCSC) ↗	Australian Cyber Security Center (ACSC) ↗	MITRE ATT&CK ↗
---	--	---------------------------

Next steps

Strategy, design, and implementation resources to help you rapidly secure privileged access for your environment.

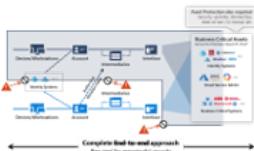
Image	Article	Description
	Strategy	Overview of privileged access strategy
	Success criteria	Strategic success criteria
	Security levels	Overview of security levels for accounts, devices, intermediaries, and interfaces

Image	Article	Description
	Accounts	Guidance on security levels and controls for accounts
	Intermediaries	Guidance on security levels and controls for intermediaries
	Interfaces	Guidance on security levels and controls for interfaces
	Devices	Guidance on security levels and controls for devices and workstations
	Enterprise access model	Overview of Enterprise Access Model (successor to legacy tier model)
	ESAE Retirement	Information on retirement of legacy administrative forest

Privileged access: Strategy

Article • 09/02/2022 • 10 minutes to read

Microsoft recommends adopting this privileged access strategy to rapidly lower the risks to your organization from high impact and high likelihood attacks on privileged access.

Privileged access should be the top security priority at every organization. Any compromise of these users has a high likelihood of significant negative impact to the organization. Privileged users have access to business critical assets in an organization, nearly always causing major impact when attackers compromise their accounts.

This strategy is built on Zero Trust principles of explicit validation, least privilege, and assumption of breach. Microsoft has provided [implementation guidance](#) to help you rapidly deploy protections based on this strategy

Important

There is no single "silver bullet" technical solution that will magically mitigate privileged access risk, you must blend multiple technologies together into a holistic solution that protects against multiple attacker entry points. Organizations must bring the right tools for each part of the job.

Why is privileged access important?

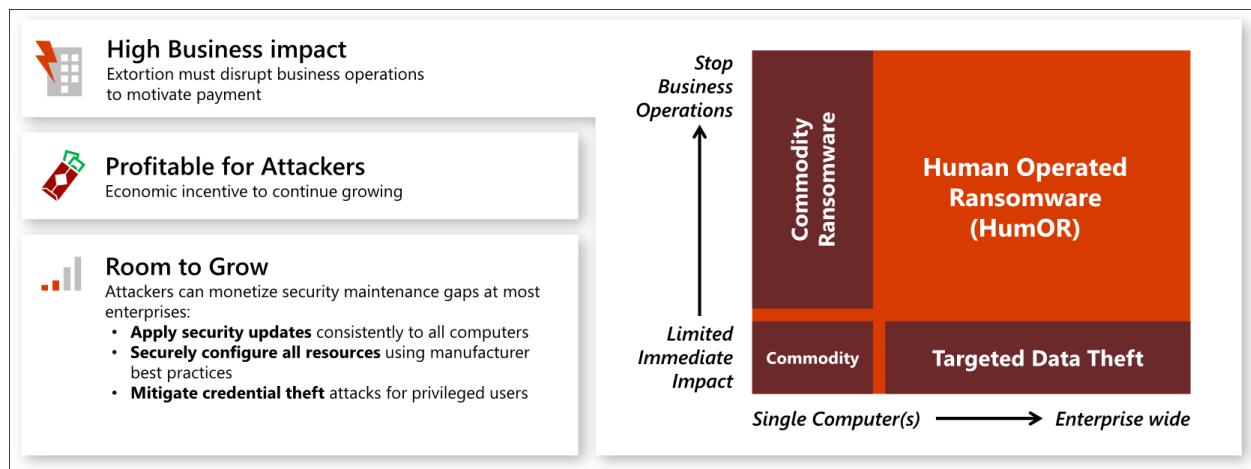
Security of privileged access is critically important because it is foundational to all other security assurances, an attacker in control of your privileged accounts can undermine all other security assurances. From a risk perspective, loss of privileged access is a high impact event with a high likelihood of happening that is growing at an alarming rate across industries.

These attack techniques were initially used in targeted data theft attacks that resulted in many high profile breaches at familiar brands (and many unreported incidents). More recently these techniques have been adopted by ransomware attackers, fueling an explosive growth of highly profitable human operated ransomware attacks that intentionally disrupt business operations across industry.

Important

Human operated ransomware  is different from commodity single computer ransomware attacks that target a single workstation or device.

This graphic describes how this extortion based attack is growing in impact and likelihood using privileged access:



- High business impact
 - It is difficult to overstate the potential business impact and damage of a loss to privileged access. Attacker's with privileged access effectively have full control of all enterprise assets and resources, giving them the ability to disclose any confidential data, stop all business processes, or subvert business processes and machines to damage property, hurt people, or worse. Massive business impact has been seen across every industry with:
 - **Targeted data theft** - attackers use privileged access to access and steal sensitive intellectual property for their own use it or to sell/transfer to your competitors or foreign governments
 - **Human-operated ransomware (HumOR)** - attackers use privileged access to steal and/or encrypt all data and systems in the enterprise, often stopping all business operations. They then extort the target organization by demanding money to not disclose the data and/or providing the keys to unlock it.
- High likelihood of occurrence
 - The prevalence of privileged access attacks has grown since the advent of modern credential theft attacks starting with [pass the hash techniques](#). These techniques first jumped in popularity with criminals starting with the 2008 release of the attack tool "Pass-the-Hash Toolkit" and have grown into a suite of reliable attack techniques (mostly based on the [Mimikatz](#) toolkit). This weaponization and automation of techniques allowed the attacks (and their subsequent impact) to grow at a rapid rate, limited only by the target organization's vulnerability to the attacks and the attacker's monetization/incentive models.
 - Prior to the advent of human-operated ransomware (HumOR), these attacks were prevalent but often unseen or misunderstood because of:

- **Attacker monetization limits** - Only groups and individuals who knew how to monetize sensitive intellectual property from target organizations could profit from these attacks.
- **Silent impact** - Organizations often missed these attacks because they didn't have detection tools, and also had a hard time seeing and estimating the resulting business impact (for example, how their competitors were using their stolen intellectual property and how that affected prices and markets, sometimes years later). Additionally, organizations who saw the attacks often stayed silent about them to protect their reputations.
- Both the silent impact and attacker monetization limitations on these attacks are disintegrating with the advent of human operated ransomware, which is growing in volume, impact, and awareness because it is both:
 - **Loud and disruptive** - to business processes to payment of extortion demands.
 - **Universally applicable** - Every organization in every industry is financially motivated to continue operations uninterrupted.

For these reasons, privileged access should be the top security priority at every organization.

Building your privileged access strategy

Privileged access strategy is a journey that must be composed of quick wins and incremental progress. Each step in your privileged access strategy must take you closer to "seal" out persistent and flexible attackers from privileged access, who are like water trying to seep into your environment through any available weakness.

This guidance is designed for all enterprise organizations regardless of where you already are in the journey.

Holistic practical strategy

Reducing risk from privileged access requires a thoughtful, holistic, and prioritized combination of risk mitigations spanning multiple technologies.

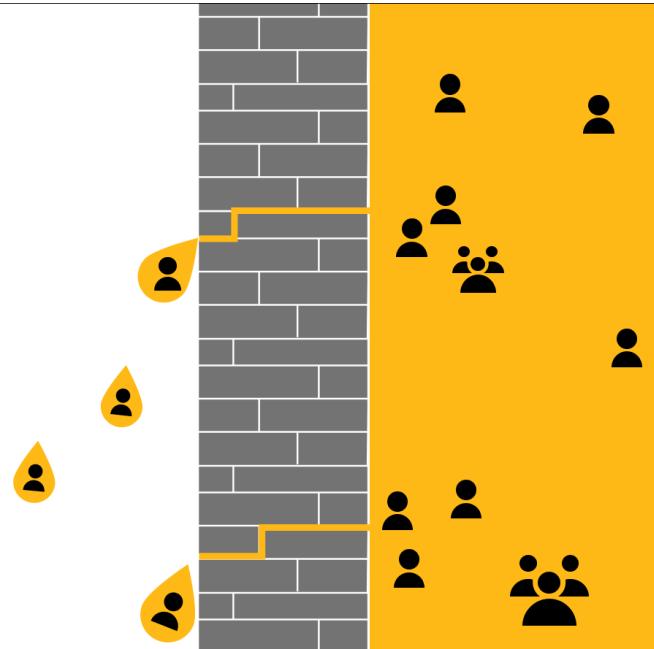
Building this strategy requires recognition that attackers are like water as they have numerous options they can exploit (some of which can appear insignificant at first), attackers are flexible in which ones they use, and they generally take the path of least resistance to achieving their objectives.

Attackers are like water

Attackers take path of least resistance to achieve objectives

- Established paths/methods
- Easiest new openings

Attackers only bother when they get good **return on investment (ROI)**



The paths attackers prioritize in actual practice are a combination of:

- Established techniques (often automated into attack tools)
- New techniques that are easier to exploit

Because of the diversity of technology involved, this strategy requires a complete strategy that combines multiple technologies and follows [Zero Trust principles](#).

ⓘ Important

You must adopt a strategy that includes multiple technologies to defend against these attacks. Simply implementing a privileged identity management / privileged access management (PIM/PAM) solution is not sufficient. For more information see, [Privileged access Intermediaries](#).

- The attackers are goal-oriented and technology agnostic, using any type of attack that works.
- The access control backbone you are defending is integrated into most or all systems in the enterprise environment.

Expecting you can detect or prevent these threats with just network controls or a single privileged access solution will leave you vulnerable to many other types of attacks.

Strategic assumption - Cloud is a source of security

This strategy uses cloud services as the primary source of security and management capabilities rather than on-premises isolation techniques for several reasons:

- **Cloud has better capabilities** - The most powerful security and management capabilities available today come from cloud services, including sophisticated tooling, native integration, and massive amounts of security intelligence like the 8+ trillion security signals a day Microsoft uses for our security tools.
- **Cloud is easier and faster** - Adopting cloud services requires little to no infrastructure for implementing and scaling up, enabling your teams to focus on their security mission rather than technology integration.
- **Cloud requires less maintenance** - The cloud is also managed, maintained, and secured consistently by vendor organizations with teams dedicated to that single purpose for thousands of customer organizations, reducing the time and effort for your team to rigorously maintain capabilities.
- **Cloud keeps improving** - Features and functionality in cloud services are constantly being updated without a need for your organization to invest ongoing.

Building the recommended strategy

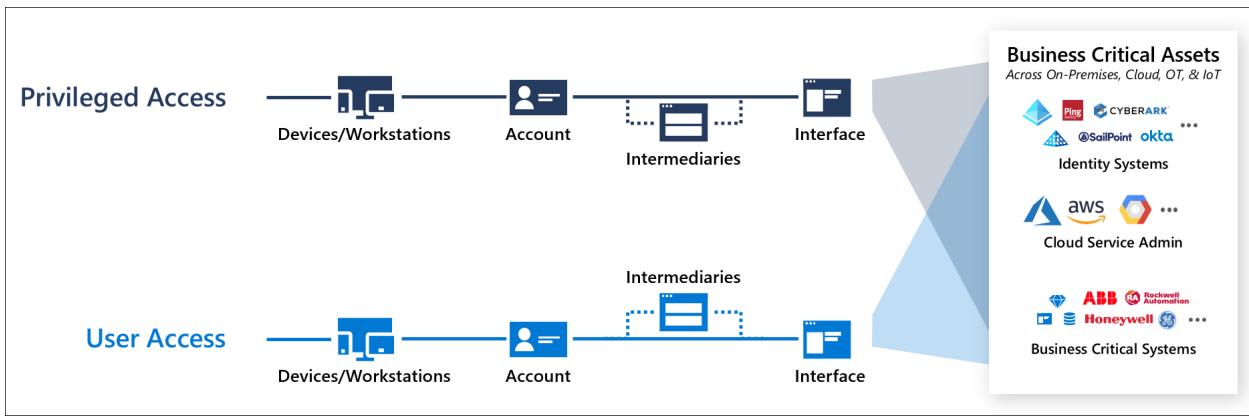
Microsoft's recommended strategy is to incrementally build a 'closed loop' system for privileged access that ensures only trustworthy '[clean](#)' devices, accounts, and intermediary systems can be used for privileged access to business sensitive systems.

Much like waterproofing something complex in real life like a boat, you need to design this strategy with an intentional outcome, establish and follow standards carefully, and continually monitor and audit the outcomes so that you remediate any leaks. You wouldn't just nail boards together in a boat shape and magically expect a waterproof boat. You would focus first on building and waterproofing significant items like the hull and critical components like the engine and steering mechanism (while leaving ways for people to get in), then later waterproofing comfort items like radios, seats, and the like. You would also maintain it over time as even the most perfect system could spring a leak later, so you need to keep up with preventive maintenance, monitor for leaks, and fix them to keep it from sinking.

Securing Privileged Access has two simple goals

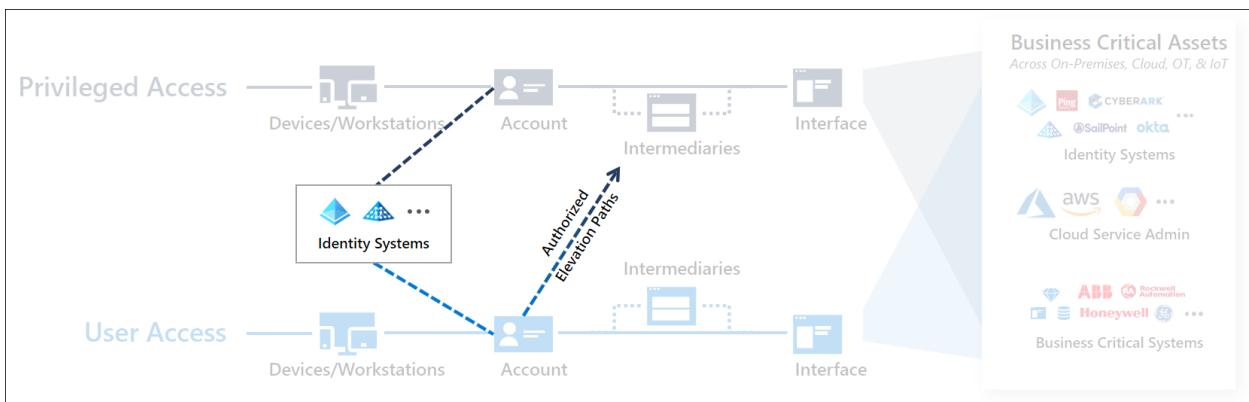
1. Strictly limit the ability to perform privileged actions to a few authorized pathways
2. Protect and closely monitor those pathways

There are two types of pathways to accessing the systems, user access (to use the capability) and privileged access (to manage the capability or access a sensitive capability)



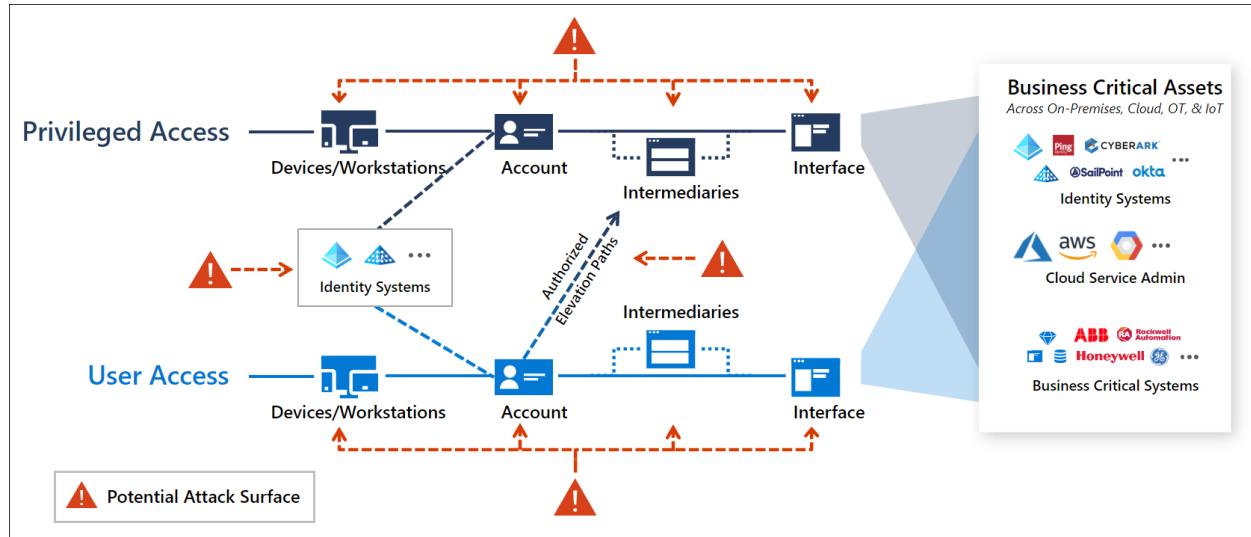
- **User Access** - the lighter blue path on the bottom of the diagram depicts a standard user account performing general productivity tasks like email, collaboration, web browsing, and use of line-of-business applications or websites. This path includes an account logging on to a device or workstations, sometimes passing through an intermediary like a remote access solution, and interacting with enterprise systems.
- **Privileged Access** - the darker blue path on the top of the diagram depicts privileged access, where privileged accounts like IT Administrators or other sensitive accounts access business critical systems and data or perform administrative tasks on enterprise systems. While the technical components may be similar in nature, the damage an adversary can inflict with privileged access is much higher.

The full access management system also includes identity systems and authorized elevation paths.



- **Identity Systems** - provide identity directories that host the accounts and administrative groups, synchronization and federation capabilities, and other identity support functions for standard and privileged users.
- **Authorized Elevation Paths** - provide means for standard users to interact with privileged workflows, such as managers or peers approving requests for administrative rights to a sensitive system through a just in time (JIT) process in a Privileged Access Management / Privileged Identity management system.

These components collectively comprise the privileged access attack surface that an adversary may target to attempt gaining elevated access to your enterprise:



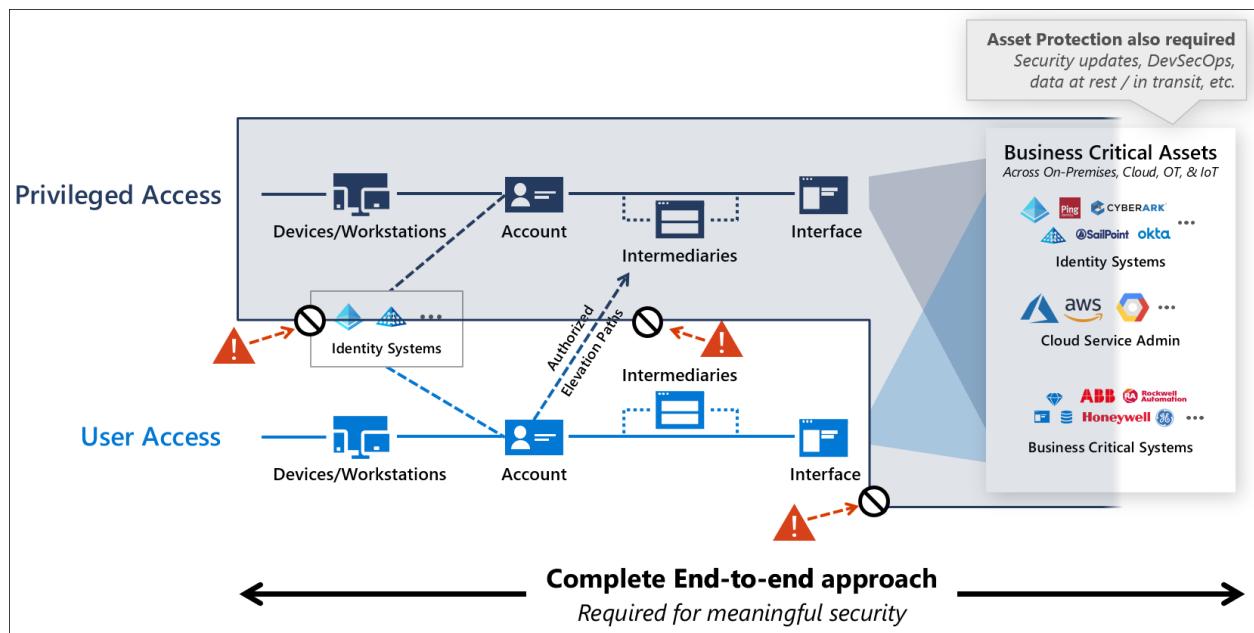
ⓘ Note

For on-premises and infrastructure as a service (IaaS) systems hosted on a customer managed operating system, the attack surface dramatically increases with management and security agents, service accounts, and potential configuration issues.

Creating a sustainable and manageable privileged access strategy requires closing off all unauthorized vectors to create the virtual equivalent of a control console physically attached to a secure system that represents the only way to access it.

This strategy requires a combination of:

- **Zero Trust access control** described throughout this guidance, including the rapid modernization plan (RAMP)
- **Asset protection** to protect against direct asset attacks by applying good security hygiene practices to these systems. Asset protection for resources (beyond access control components) is out of scope of this guidance, but typically includes rapid application of security updates/patches, configuring operating systems using manufacturer/industry security baselines, protecting data at rest and in transit, and integrating security best practices to development / DevOps processes.



Strategic initiatives in the journey

Implementing this strategy requires four complementary initiatives that each have clear outcomes and success criteria

1. End-to-end Session Security - Establish explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths.
 - a. Success Criteria: Each session will validate that each user accounts and device are trusted at a sufficient level before allowing access.
2. Protect & Monitor Identity Systems including Directories, Identity Management, Admin Accounts, Consent grants, and more
 - a. Success Criteria: Each of these systems will be protected at a level appropriate for the potential business impact of accounts hosted in it.
3. Mitigate Lateral Traversal to protect against lateral traversal with local account passwords, service account passwords, or other secrets
 - a. Success Criteria: Compromising a single device will not immediately lead to control of many or all other devices in the environment
4. Rapid Threat Response to limit adversary access and time in the environment
 - a. Success Criteria: Incident response processes impede adversaries from reliably conducting a multi-stage attack in the environment that would result in loss of privileged access. (as measured by reducing the mean time to remediate (MTTR) of incidents involving privileged access to near zero and reducing MTTR of all incidents to a few minutes so adversaries don't have time to target privileged access)

Next steps

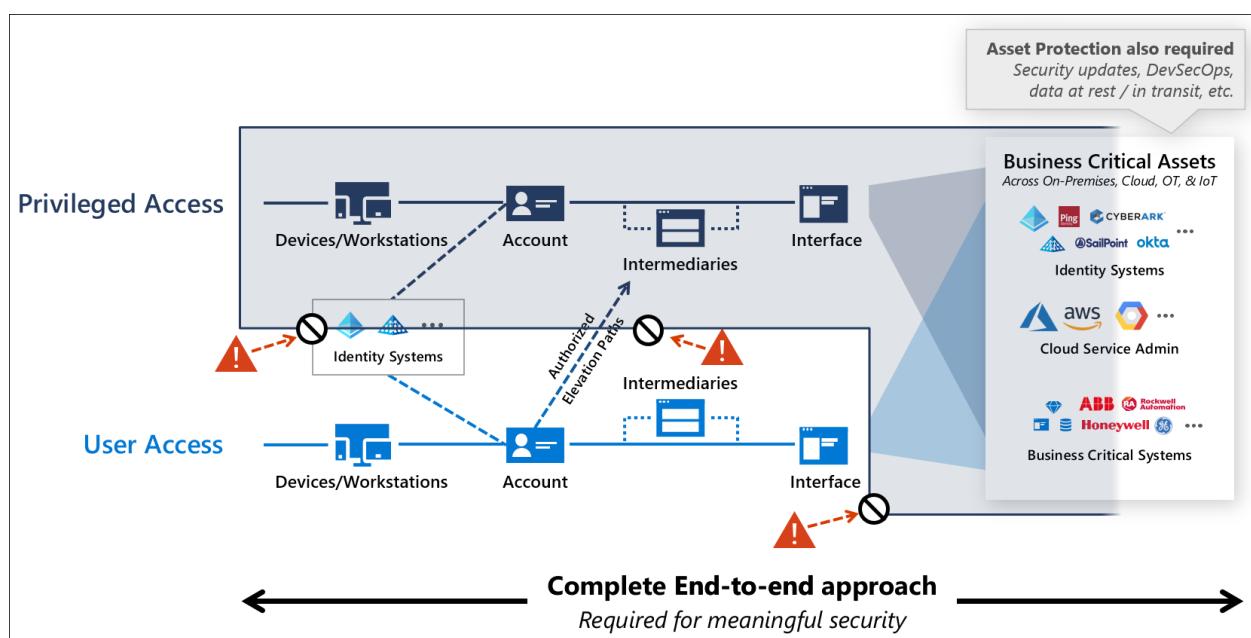
- Securing privileged access overview
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model
- Enhanced Security Admin Environment (ESAE) retirement

Success criteria for privileged access strategy

Article • 09/02/2022 • 7 minutes to read

This document describes the success criteria for a [privileged access strategy](#). This section describes strategic perspectives of success for a privileged access strategy. For a roadmap on how to adopt this strategy, see the [rapid modernization plan \(RaMP\)](#). For implementation guidance, see [privileged access deployment](#)

Implementing a holistic strategy using Zero Trust approaches creates a "seal" of sorts over the access control for privileged access that makes it resistant to attackers. This strategy is accomplished by limiting pathways to privileged access only a select few, and then closely protecting and monitoring those authorized pathways.



A successful strategy must address the all points attackers can use to intercept privileged access workflows including four distinct initiatives:

- **Privileged Access workflow** elements of the privileged access workflow including underlying devices, operating systems, applications, and identities
- **Identity systems** hosting the privileged accounts and the groups, and other artifacts that confer privilege on the accounts
- **User access workflow** and authorized elevation paths that can lead to privileged access
- **Application interfaces** where zero trust access policy is enforced and role-based access control (RBAC) is configured to grant privileges

Note

A complete security strategy also includes asset protections that are beyond the scope of access control, such as data backups and protections against attacks on the application itself, the underlying operating system and hardware, on service accounts used by the application or service, and on data while at rest or in transit. For more information on modernizing a security strategy for cloud, see [Define a security strategy](#).

An attack consists of human attackers leveraging automation and scripts to attack an organization composed of humans, the processes they follow, and the technology they use. Because of this complexity of both attackers and defenders, the strategy must be multi-faceted to guard against all the people, process, and technology ways that the security assurances could inadvertently be undermined.

Ensuring sustainable long-term success requires meeting the following criteria:

- [Ruthless prioritization](#)
- [Balance security and productivity](#)
- [Strong partnerships within the organization](#)
- [Disrupt attacker return on investment](#)
- [Follow clean source principle](#)

Ruthless prioritization

Ruthless prioritization is the practice of taking the most effective actions with the fastest time to value first, even if those efforts don't fit pre-existing plans, perceptions, and habits. This strategy lays out the set of steps that have been learned in the fiery crucible of many major cybersecurity incidents. The learnings from these incidents form the steps we help organizations take to ensure that these crises don't happen again.

While it's always tempting for security professionals to try to optimize familiar existing controls like network security and firewalls for newer attacks, this path consistently leads to failure. [Microsoft's Detection and Response Team \(DART\)](#) has been responding to privileged access attacks for nearly a decade and consistently sees these classic security approaches fail to detect or stop these attacks. While network security provides necessary and important basic security hygiene, it's critical to break out of these habits and focus on mitigations that will deter or block real world attacks.

Ruthlessly prioritize the security controls recommended in this strategy, even if it challenges existing assumptions and forces people to learn new skills.

Balance security and productivity

As with all elements of security strategy, privileged access should ensure that both productivity and security goals are met.

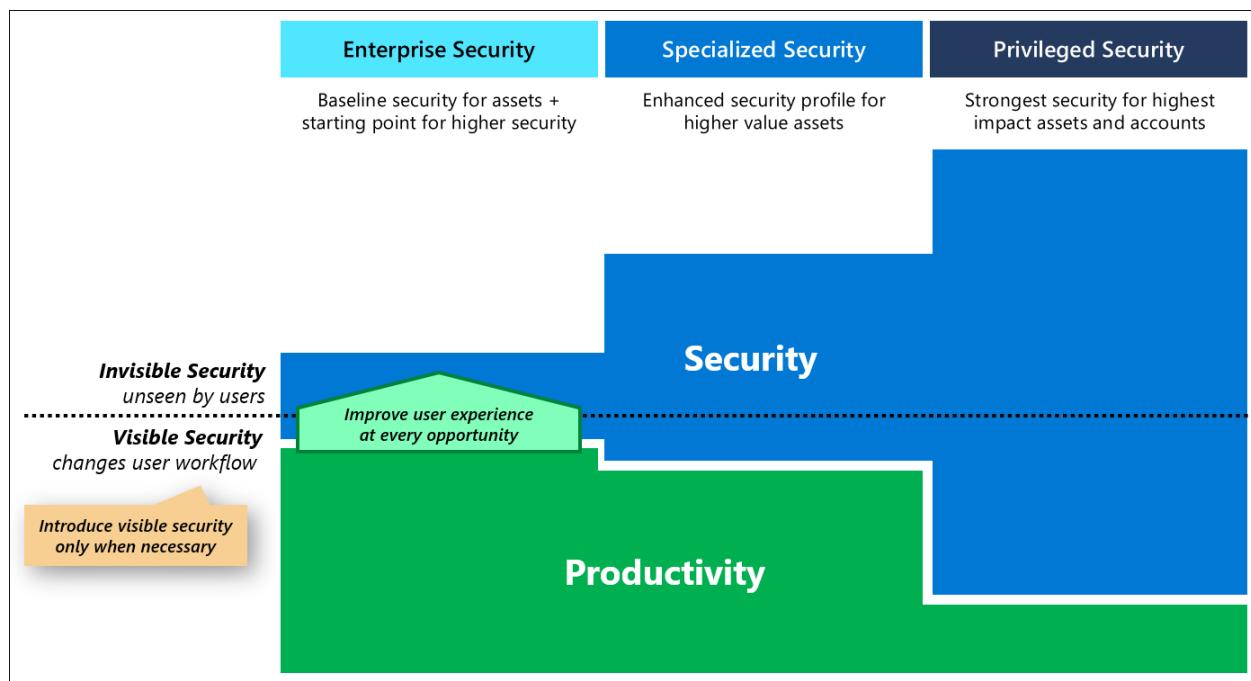
Balancing security avoids the extremes that create risk for the organization by:

- Avoiding overly strict security that causes users to go outside the secure policies, pathways, and systems.
- Avoiding weak security that harms productivity by allowing adversaries to easily compromise the organization.

For more information about security strategy, see [Defining a security strategy](#).

To minimize negative business impact from security controls, you should prioritize invisible security controls that improve user workflows, or at least don't impede or change user workflows. While security sensitive roles may need visible security measures that change their daily workflows to provide security assurances, this implementation should be done thoughtfully to limit the usability impact and scope as much as possible.

This strategy follows this guidance by defining three profiles (detailed later in Keep it Simple - Personas and Profiles)



Strong partnerships within the organization

Security must work to build partnerships within the organization to be successful. In addition to the timeless truth that "none of us is as smart as all of us," the nature of security is to be a support function to protect someone else's resources. Security isn't

accountable for the resources they help protect (profitability, uptime, performance, etc.), *security is a support function that provides expert advice and services to help protect the intellectual property and business functionality that is important to the organization.*

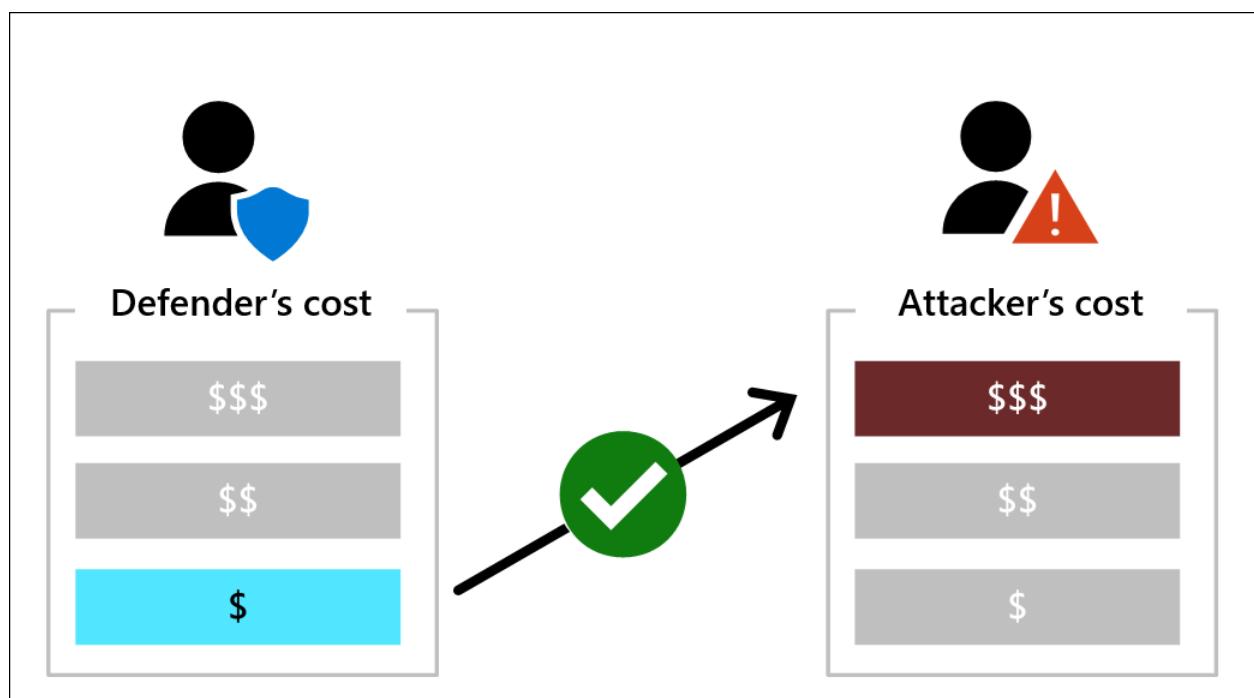
Security should **always work as a partner** in support of business and mission objectives. While security should not shy away from giving direct advice like recommending against accepting a high risk, security should also always frame that advice in terms of the business risk relative to other risks and opportunities managed by the resource owners.

While some parts of security can be planned and executed successfully mostly within security organization, many like securing privileged access require working closely with IT and business organizations to understand which roles to protect, and help update and redesign workflows to ensure they are both secure and allow people to do their jobs. For more information on this idea, see the section [Transformations, mindsets, and expectations](#) in the security strategy guidance article.

Disrupt attacker return on investment

Maintain focus on pragmatism by ensuring that defensive measures are likely to meaningfully disrupt the attacker value proposition of attacking you, increasing cost and friction on the attacker's ability to successfully attack you. Evaluating how defensive measures would impact the adversary's cost of attack provides both a healthy reminder to focus on the attackers perspective as well as a structured mechanism to compare the effectiveness of different mitigation options.

Your goal should be to increase the attackers cost while minimizing your own security investment level:



Disrupt attacker return on investment (ROI) by increasing their cost of attack across the elements of the privileged access session. This concept is described in more detail in the article [Success criteria for privileged access strategy](#).

ⓘ Important

A privileged access strategy should be comprehensive and provide defense in depth, but must avoid the Expense in depth fallacy where defenders simply pile on more same (familiar) type controls (often network firewalls/filters) past the point where they add any meaningful security value.

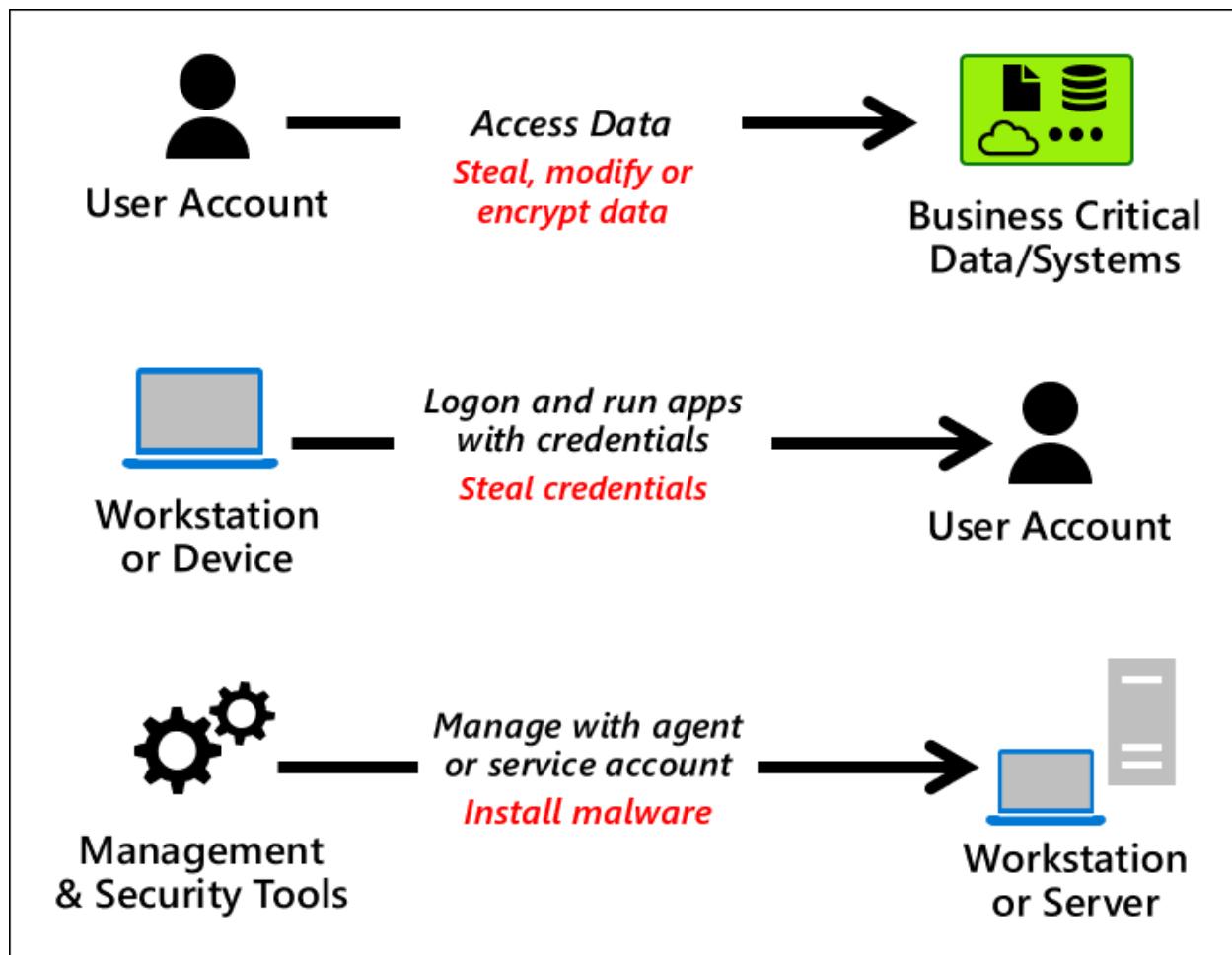
For more information on attacker ROI, see the short video and in-depth discussion [Disrupting attacker return on investment](#).

Clean source principle

The clean source principle requires all security dependencies to be as trustworthy as the object being secured.



Any subject in control of an object is a security dependency of that object. If an adversary can control anything in control of a target object, they can control that target object. Because of this threat, you must ensure that the assurances for all security dependencies are at or above the desired security level of the object itself. This principle applies across many types of control relationships:



While simple in principle, this concept gets complex easily in the real world as most enterprises grew organically over decades and have many thousands of control relationships recursively that build on each other, loop back on each other, or both. This web of control relationships provides many access paths that an attacker can discover and navigate during an attack, often with automated tools.

Microsoft's recommended privileged access strategy is effectively a plan to untangle the most important parts of this knot first using a Zero Trust approach, by explicitly validating that the source is clean before allowing access to the destination.

In all cases, the trust level of the source must be the same or higher than the destination.

- The only notable exception to this principle is allowing the use of unmanaged personal devices and partner devices for enterprise scenarios. This exception enables enterprise collaboration and flexibility and can be mitigated to an acceptable level for most organizations because of the low relative value of the enterprise assets. For more context on BYOD security, see the blog post [How a BYOD policy can reduce security risk in the public sector ↗](#).
- This same exception cannot be extended to specialized security and privileged security levels however because of the security sensitivity of these assets. Some PIM/PAM vendors may advocate that their solutions can mitigate device risk from

lower-level devices, but we respectfully disagree with those assertions based on our experience investigating incidents. The asset owners in your organization may choose to accept risk of using enterprise security level devices to access specialized or privileged resources, but Microsoft does not recommend this configuration. For more information, see the intermediary guidance for Privileged Access Management / Privileged Identity management.

The privileged access strategy accomplishes this principle primarily by enforcing Zero Trust policy with Conditional Access on inbound sessions at interfaces and intermediaries. The clean source principle starts with getting a new device from an OEM that is built to your security specifications including operating system version, security baseline configuration, and other requirements such as using [Windows Autopilot](#) for deployment.

Optionally, the clean source principle can extend into a highly rigorous review of each component in the supply chain including installation media for operating systems and applications. While this principle would be appropriate for organizations facing highly sophisticated attackers, it should be a lower priority than the other controls in this guidance.

Next steps

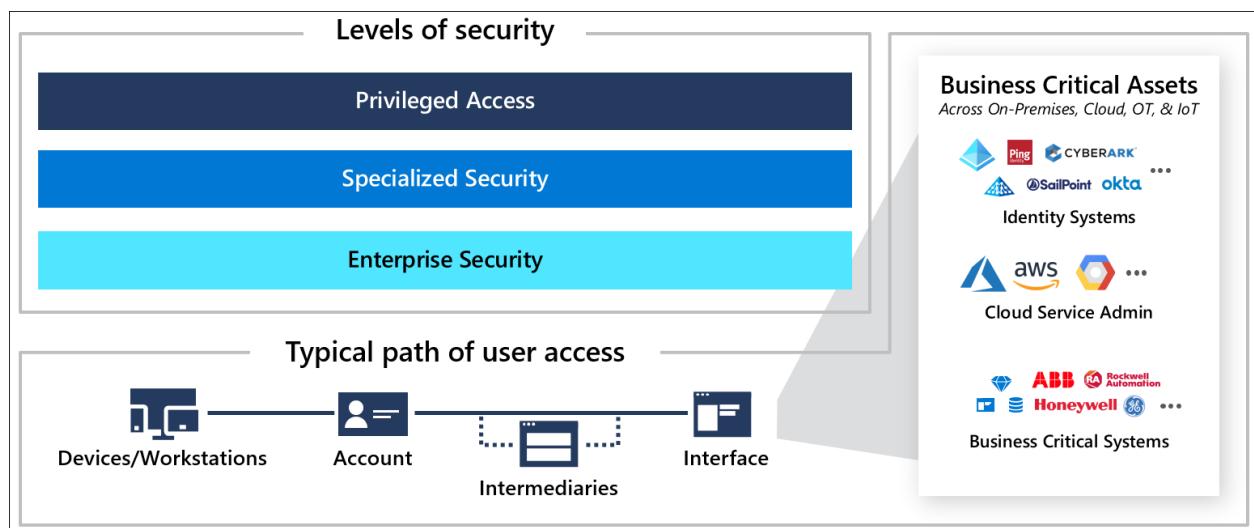
- [Securing privileged access overview](#)
- [Privileged access strategy](#)
- [Security levels](#)
- [Privileged access accounts](#)
- [Intermediaries](#)
- [Interfaces](#)
- [Privileged access devices](#)
- [Enterprise access model](#)

Privileged access security levels

Article • 09/02/2022 • 4 minutes to read

This document describes the security levels of a [privileged access strategy](#). For a roadmap on how to adopt this strategy, see the [rapid modernization plan \(RaMP\)](#). For implementation guidance, see [privileged access deployment](#).

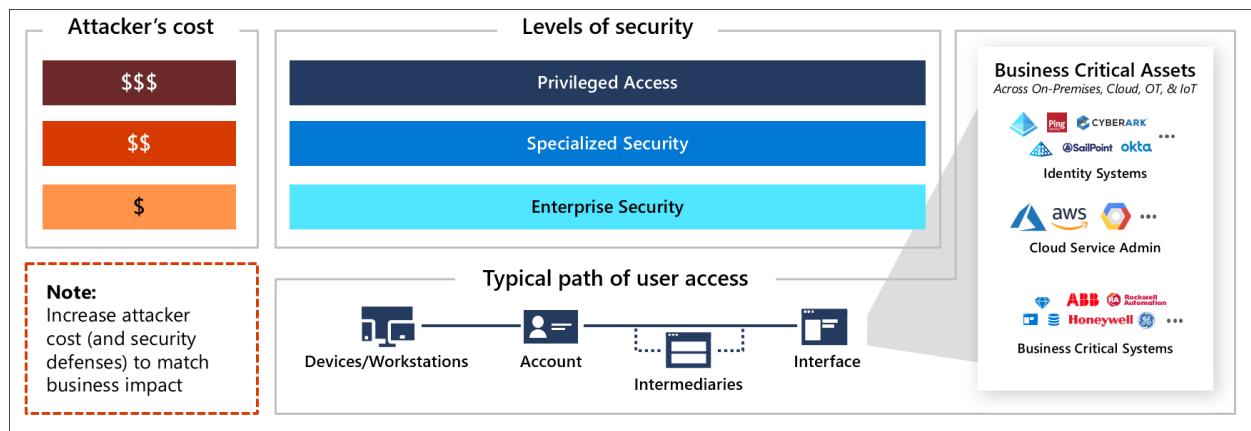
These levels are primarily designed to provide simple and straightforward technical guidance so that organizations can rapidly deploy these critically important protections. The privileged access strategy recognizes that organizations have unique needs, but also that custom solutions create complexity that results in higher costs and lower security over time. To balance this need, the strategy provides firm prescriptive guidance for each level and flexibility through allowing organizations to choose when each role will be required to meet the requirements of that level.



Making things simple helps people understand it and lowers the risk they will be confused and make mistakes. While the underlying technology is almost always complex, it is critical to keep things simple rather than creating custom solutions that are difficult to support. For more information, see [Security design principles](#).

Designing solutions that are focused on the needs of the administrators and end users, will keep it simple for them. Designing solutions that are simple for security and IT personnel to build, assess, and maintain (with automation where possible) leads to less security mistakes and more reliable security assurances.

The recommended privileged access security strategy implements a simple three level system of assurances, that span across areas, designed to be easy to deploy for: accounts, devices, intermediaries, and interfaces.



Each successive level drives up attacker costs, with additional level of Defender for Cloud investment. The levels are designed to target the 'sweet spots' where defenders get the most return (attacker cost increase) for each security investment they make.

Each role in your environment should be mapped to one of these levels (and optionally increased over time as part of a security improvement plan). Each profile is clearly defined as a technical configuration and automated where possible to ease deployment and speed up security protections. For implementation details see the article, [Privileged access roadmap](#).

The security levels used throughout this strategy are:

- **Enterprise security** is suitable for all enterprise users and productivity scenarios. In the progression of the rapid modernization plan, enterprise also serves as the starting point for specialized and privileged access as they progressively build on the security controls in enterprise security.

ⓘ Note

Weaker security configurations do exist, but aren't recommended by Microsoft for enterprise organizations today because of the skills and resources attackers have available. For information on what attackers can buy from each other on the dark markets and average prices, see the video [Top 10 Best Practices for Azure Security](#)

- **Specialized security** provides increased security controls for roles with an elevated business impact (if compromised by an attacker or malicious insider).

Your organization should have documented criteria for specialized and privileged accounts (for example, potential business impact is over \$1M USD) and then identify all the roles and accounts meeting that criteria. (used throughout this strategy, including in the Specialized Accounts)

Specialized roles typically include:

- **Developers** of business critical systems.
- **Sensitive business roles** such as users of SWIFT terminals, researchers with access to sensitive data, personnel with access to financial reporting prior to public release, payroll administrators, approvers for sensitive business processes, and other high impact roles.
- **Executives** and personal assistants / administrative assistants that regularly handle sensitive information.
- **High impact social media accounts** that could damage the company reputation.
- **Sensitive IT Admins** with a significant privileges and impact, but are not enterprise-wide. This group typically includes administrators of individual high impact workloads. (for example, enterprise resource planning administrators, banking administrators, help desk /tech support roles, etc.)

Specialized Account security also serves as an interim step for privileged security, which further builds on these controls. See [privileged access roadmap](#) for details on recommended order of progression.

- **Privileged security** is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider. This level typically includes technical roles with administrative permissions on most or all enterprise systems (and sometimes includes a select few business critical roles)

Privileged accounts are focused on security first, with productivity defined as the ability to easily and securely perform sensitive job tasks securely. These roles will not have the ability to do both sensitive work and general productivity tasks (browse the web, install and use any app) using the same account or the same device/workstation. They will have highly restricted accounts and workstations with increased monitoring of their actions for anomalous activity that could represent attacker activity.

Privileged access security roles typically include:

- Azure AD Global Administrators and [related roles](#)
- Other identity management roles with administrative rights to an enterprise directory, identity synchronization systems, federation solution, virtual directory, privileged identity/access management system, or similar.
- Roles with membership in these on-premises Active Directory groups
 - Enterprise Admins
 - Domain Admins
 - Schema Admin

- BUILTIN\Administrators
- Account Operators
- Backup Operators
- Print Operators
- Server Operators
- Domain Controllers
- Read-only Domain Controllers
- Group Policy Creator Owners
- Cryptographic Operators
- Distributed COM Users
- Sensitive on-premises Exchange groups (including Exchange Windows Permissions and Exchange Trusted Subsystem)
- Other Delegated Groups - Custom groups that may be created by your organization to manage directory operations.
- Any local administrator for an underlying operating system or cloud service tenant that is hosting the above capabilities including
 - Members of local administrators group
 - Personnel who know the root or built in administrator password
 - Administrators of any management or security tool with agents installed on those systems

Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

Privileged access: Accounts

Article • 02/01/2023 • 5 minutes to read

Account security is a critical component of [securing privileged access](#). End to end Zero Trust security for sessions requires strongly establishing that the account being used in the session is actually under the control of the human owner and not an attacker impersonating them.

Strong account security starts with secure provisioning and full lifecycle management through to deprovisioning, and each session must establish strong assurances that the account isn't currently compromised based on all available data including historical behavior patterns, available threat intelligence, and usage in the current session.

Account security

This guidance defines three security levels for account security that you can use for assets with different sensitivity levels:

End-to-end Protection For Privileged Sessions	Enterprise Security	Specialized Security	Privileged Security
	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
 Role Recommendation For privileged access role	 Standard users	 High impact users / developers	 IT Operations
 Device Physical device initiating session			
 Account with access to resources Profile Summary	Enterprise Account <ul style="list-style-type: none">Enforce strong multi-factor authentication (MFA)Enforce account/session riskMonitor and respond to alerts	Specialized Account <ul style="list-style-type: none">Enterprise Security Plus...<ul style="list-style-type: none">Tag accounts as sensitivePrioritize security response for accounts	Privileged Account <ul style="list-style-type: none">Specialized Security Plus...<ul style="list-style-type: none">Explicitly restrict account usage to specific devicesExplicitly monitor for anomalous usage within the enterprise
 Intermediary Remote Access / Admin Broker			
 Interface Controlling resource access			

These levels establish clear and implementable security profiles appropriate for each sensitivity level that you can assign roles to and scale out rapidly. All of these account security levels are designed to maintain or improve productivity for people by limiting or eliminating interruption to user and admin workflows.

Planning account security

This guidance outlines the technical controls required to meet each level. Implementation guidance is in the [privileged access roadmap](#).

Account security controls

Achieving security for the interfaces requires a combination of technical controls that both protect the accounts and provide signals to be used in a Zero Trust policy decision (see Securing Interfaces for policy configuration reference).

The controls used in these profiles include:

- Multi-factor authentication - providing diverse sources of proof that the (designed to be as easy as possible for users, but difficult for an adversary to mimic).
- Account risk - Threat and Anomaly Monitoring - using UEBA and Threat intelligence to identify risky scenarios
- Custom monitoring - For more sensitive accounts, explicitly defining allowed/accepted behaviors/patterns allows early detection of anomalous activity. This control is not suitable for general purpose accounts in enterprise as these accounts need flexibility for their roles.

The combination of controls also enables you to improve both security and usability - for example a user who stays within their normal pattern (using the same device in same location day after day) does not need to be prompted for outside MFA every time they authenticate.

	Enterprise Security	Specialized Security	Privileged Security
Account with access to resources	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
Profile Summary	Enterprise Account	Specialized Account	Privileged Account
Security Benefit	<ul style="list-style-type: none">• Enforce Strong MFA• Enforce Account/Session risk	<ul style="list-style-type: none">• Enterprise Security Plus...• Tag accounts as sensitive• Prioritize security response for accounts	<ul style="list-style-type: none">• Specialized Security Plus...• Explicitly restrict account usage to specific devices• Explicitly monitor for anomalous usage within the enterprise
Implementation Effort/Cost	<ul style="list-style-type: none">• Insider Coercion/Extortion• Targeted Workstation Compromise	<ul style="list-style-type: none">• Insider Coercion/Extortion	<ul style="list-style-type: none">• Insider Coercion/Extortion <i>with sophisticated execution</i>

Enterprise security accounts

The security controls for enterprise accounts are designed to create a secure baseline for all users and provide a secure foundation for specialized and privileged security:

- Enforce strong multi-factor authentication (MFA) - Ensure that the user is authenticated with strong MFA provided by an enterprise-managed identity

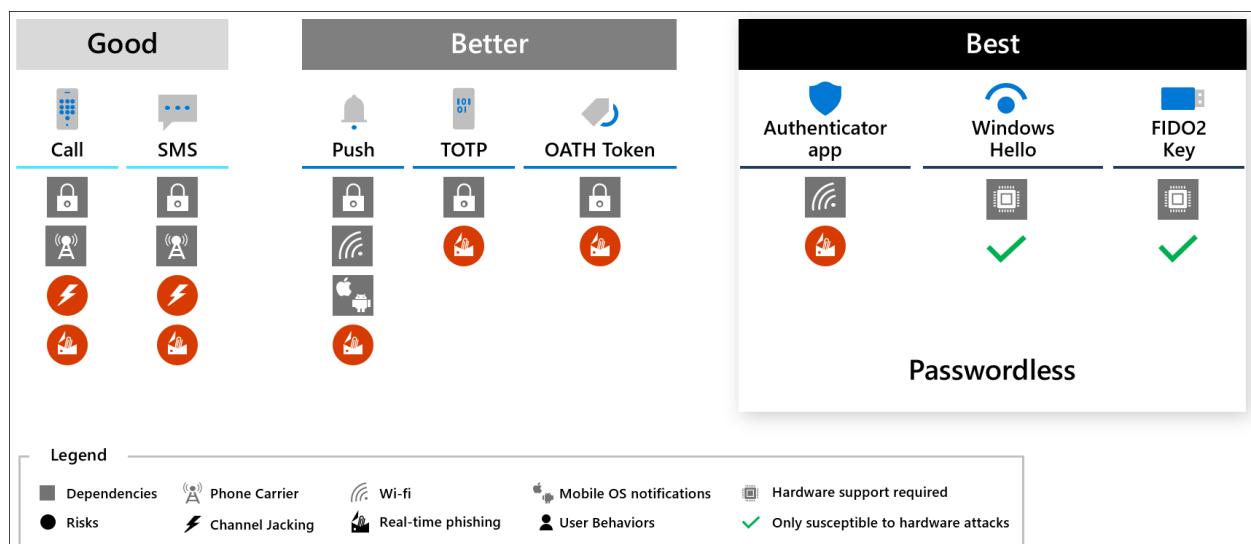
system (detailed in the diagram below). For more information about multi-factor authentication, see [Azure security best practice 6](#).

ⓘ Note

While your organization may choose to use an existing weaker form of MFA during a transition period, attackers are increasingly evading the weaker MFA protections, so all new investment into MFA should be on the strongest forms.

- Enforce account/session risk - ensure that the account is not able to authenticate unless it is at a low (or medium?) risk level. See Interface Security Levels for details on conditional enterprise account security.
- Monitor and respond to alerts - Security operations should integrate account security alerts and get sufficient training on how these protocols and systems work to ensure they are able to rapidly comprehend what an alert means and react accordingly.
 - Enable [Azure AD Identity Protection](#)
 - [Investigate risk Azure AD Identity Protection](#)
 - [Troubleshoot/Investigate Conditional Access Sign-in failures](#)

The following diagram provides a comparison to different forms of MFA and passwordless authentication. Each option in the best box is considered both high security and high usability. Each has different hardware requirements so you may want to mix and match which ones apply to different roles or individuals. All Microsoft passwordless solutions are recognized by Conditional Access as multi-factor authentication because they require combining something you have with either biometrics, something you know, or both.



Note

For more information on why SMS and other phone based authentication is limited, see the blog post [It's Time to Hang Up on Phone Transports for Authentication](#).

Specialized accounts

Specialized accounts are a higher protection level suitable for sensitive users. Because of their higher business impact, specialized accounts warrant additional monitoring and prioritization during security alerts, incident investigations, and threat hunting.

Specialized security builds on the strong MFA in enterprise security by identifying the most sensitive accounts and ensuring alerts and response processes are prioritized:

1. Identify Sensitive Accounts - See specialized security level guidance for identifying these accounts.
2. Tag Specialized Accounts - Ensure each sensitive account is tagged
 - a. [Configure Microsoft Sentinel Watchlists](#) to identify these sensitive accounts
 - b. [Configure Priority account protection in Microsoft Defender for Office 365](#) and designate specialized and privileged accounts as priority accounts -
3. Update Security Operations processes - to ensure these alerts are given the highest priority
4. Set up Governance - Update or create governance process to ensure that
 - a. All new roles to are evaluated for specialized or privileged classifications as they are created or changed
 - b. All new accounts are tagged as they are created
 - c. Continuous or periodic out of band checks to ensure that roles and accounts didn't get missed by normal governance processes.

Privileged accounts

Privileged accounts have the highest level of protection because they represent a significant or material potential impact on the organization's operations if compromised.

Privileged accounts always include IT Admins with access to most or all enterprise systems, including most or all business critical systems. Other accounts with a high business impact may also warrant this additional level of protection. For more information about which roles and accounts should be protected at what level, see the article [Privileged Security](#).

In addition to specialized security , privileged account security increases both:

- Prevention - add controls to restrict the usage of these accounts to the designated devices, workstations, and intermediaries.
- Response - closely monitor these accounts for anomalous activity and rapidly investigate and remediate the risk.

Configuring privileged account security

Follow the guidance in the [Security rapid modernization plan](#) to both increase the security of your privileged accounts and decrease your cost to manage.

Next steps

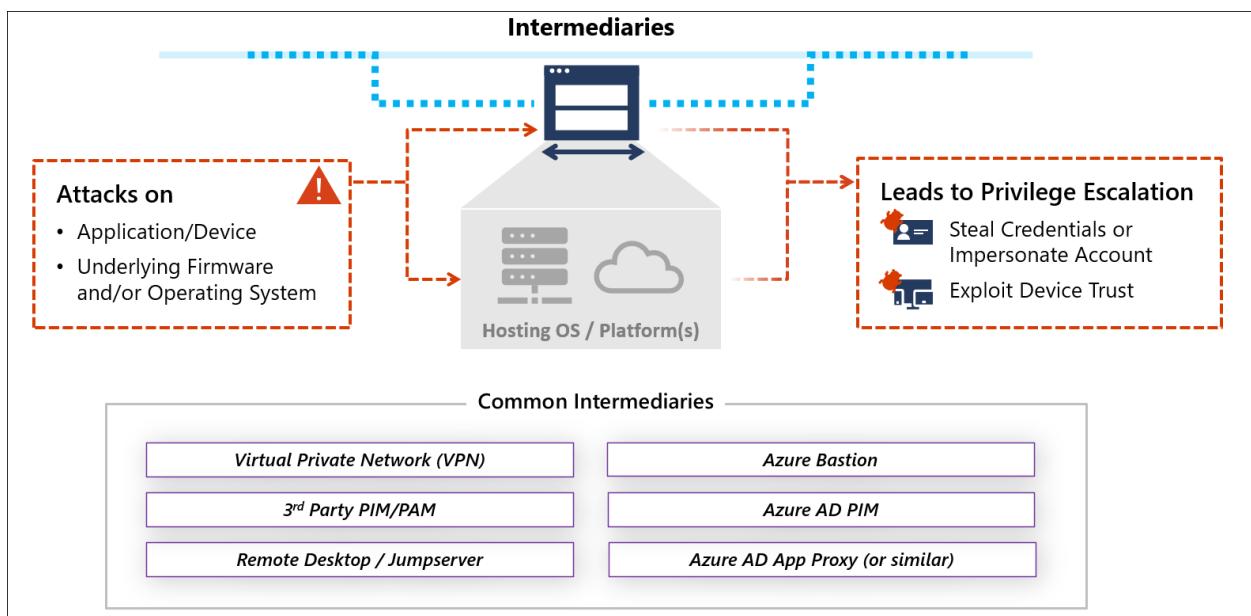
- [Securing privileged access overview](#)
- [Privileged access strategy](#)
- [Measuring success](#)
- [Security levels](#)
- [Intermediaries](#)
- [Interfaces](#)
- [Privileged access devices](#)
- [Enterprise access model](#)

Privileged access: Intermediaries

Article • 09/02/2022 • 12 minutes to read

Security of intermediary devices is a critical component of [securing privileged access](#).

Intermediaries add link to the chain of Zero Trust assurance for the user or administrator's end to end session, so they must sustain (or improve) the Zero Trust security assurances in the session. Examples of intermediaries include virtual private networks (VPNs), jump servers, virtual desktop infrastructure (VDI), as well as application publishing through access proxies.



An attacker can attack an intermediary to attempt to escalating privileges using credentials stored on them, get network remote access to corporate networks, or exploit trust in that device if being used for Zero Trust access decisions. Targeting intermediaries has become an all too common, especially for organizations that don't rigorously maintain the security posture of these devices. For example, [credentials collected from VPN devices](#).

	Enterprise Security	Specialized Security	Privileged Security
Intermediary Remote Access / Admin Broker	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
No Privilege Escalation Risk <i>Provides network access and/or access to existing account privileges</i>	Enterprise Intermediary	Specialized Intermediary	Privileged Intermediary
Privilege Escalation Risk <i>Provides potential privileged escalation path for attackers</i>		Azure AD App Proxy (or similar) Azure Bastion Azure AD PIM	Virtual Private Network (VPN) Remote Desktop / Jumpserver 3rd Party PIM/PAM
Profile Summary	Enterprise and Specialized have same requirements <ul style="list-style-type: none"> • Rapidly apply security updates (often neglected) • Apply secure configuration for application and any underlying operating system (using manufacturer or industry baselines/recommendations) • Solution administration restricted to roles protected by <u>specialized or higher</u> session security 	Enterprise Security Plus <ul style="list-style-type: none"> • Solution administration restricted to roles protected by <u>privileged</u> session security • May be dedicated device or service for privileged roles 	

Intermediaries vary in purpose and technology, but typically provide remote access, session security, or both:

- **Remote access** - Enable access to systems on enterprise networks from the internet
- **Session security** - Increase security protections and visibility for a session
 - **Unmanaged device scenario** - Providing a managed virtual desktop to be accessed by unmanaged devices (for example, personal employee devices) and/or devices managed by a partner/vendor.
 - **Administrator security scenario** - Consolidate administrative pathways and/or increase security with just in time access, session monitoring and recording, and similar capabilities.

Ensuring security assurances are sustained from the originating device and account through to the resource interface requires understanding the risk profile of the intermediary and mitigation options.

Attacker opportunity and value

Different intermediary types perform unique functions so they each require a different security approach, though there are some critical commonalities like rapidly applying security patches to appliances, firmware, operating systems, and applications.

	Attacker Opportunity <i>Available attack surface</i>	Attacker Value <i>What attacker can gain from compromise</i>		
		Get Network Connectivity	Impersonate Device Identity	Steal Account Credentials
Azure AD App Proxy (or similar)	Limited attack surface <ul style="list-style-type: none"> Internet exposed Cloud provider managed service that requires authentication before connection 	No	No	No
Azure Bastion			No	No
Azure AD PIM				Varies
Virtual Private Network (VPN)	Significant attack surface <ul style="list-style-type: none"> Internet exposure Application/OS must be maintained/patched 	Yes	Yes	Yes
Remote Desktop / Jumpserver				
3rd Party PIM/PAM	Variable attack surface <ul style="list-style-type: none"> Intranet Exposure Application/OS must be maintained/patched 	No	No	Yes

The **attacker opportunity** is represented by the available attack surface an attack operator can target:

- Native cloud services like Azure AD PIM, Azure Bastion, and Azure AD App Proxy offer a limited attack surface to attackers. While they are exposed to the public internet, customers (and attackers) have no access to underlying operating systems providing the services and they are typically maintained and monitored consistently via automated mechanisms at the cloud provider. This smaller attack surface limits the available options to attackers vs. classic on-premises applications and appliances that must be configured, patched, and monitored by IT personnel who are often overwhelmed by conflicting priorities and more security tasks than they have time to complete.
- Virtual Private Networks (VPNs) and Remote Desktops / Jump servers frequently have a significant attacker opportunity as they are exposed to the internet to provide remote access and the maintenance of these systems is frequently neglected. While they only have a few network ports exposed, attackers only need access to one unpatched service for an attack.
- Third-party PIM/PAM services are frequently hosted on-premises or as a VM on Infrastructure as a Service (IaaS) and are typically only available to intranet hosts. While not directly internet exposed, a single compromised credential may allow attackers to access the service over VPN or another remote access medium.

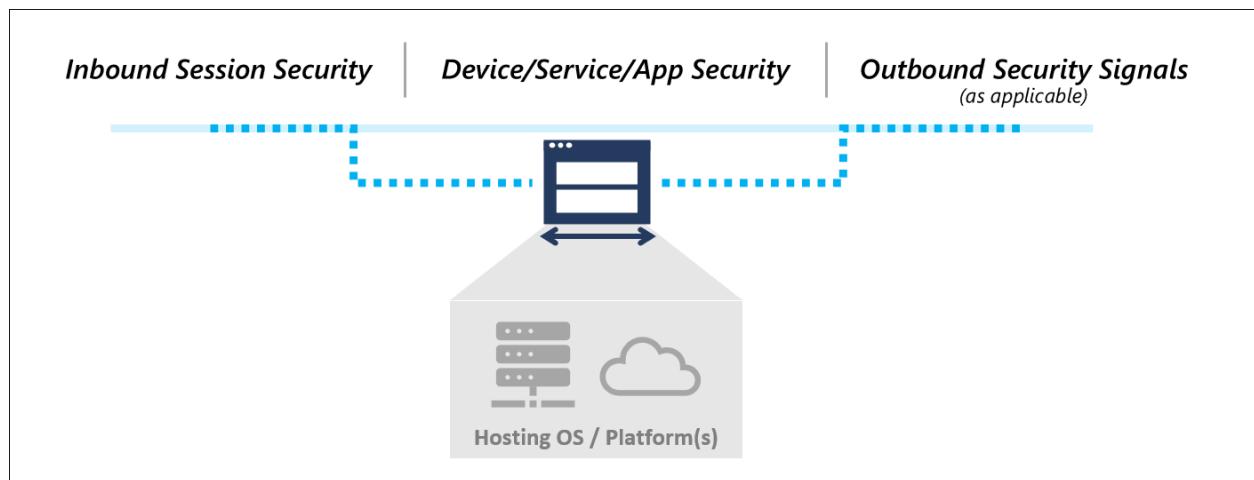
Attacker value represents what an attacker can gain by compromising an intermediary. A compromise is defined as an attacker gaining full control over the application/VM and/or an administrator of the customer instance of the cloud service.

The ingredients that attackers can collect from an intermediary for the next stage of their attack include:

- **Get network connectivity** to communicate with most or all resource on enterprise networks. This access is typically provided by VPNs and Remote Desktop / Jump server solutions. While Azure Bastion and Azure AD App Proxy (or similar third-party solutions) solutions also provide remote access, these solutions are typically application or server-specific connections and don't provide general network access
- **Impersonate device identity** - can defeat Zero Trust mechanisms if a device is required for authentication and/or be used by an attacker to gather intelligence on the targets networks. Security Operations teams often don't closely monitor device account activity and focus only on user accounts.
- **Steal account credentials** to authenticate to resources, which are the most valuable asset to attackers as it offers the ability to elevate privileges to access their ultimate goal or the next stage in the attack. Remote Desktop / Jump servers and third-party PIM/PAM are the most attractive targets and have the "All your eggs in one basket" dynamic with increased attacker value and security mitigations:
 - **PIM/PAM** solutions typically store the credentials for most or all privileged roles in the organization, making them a highly lucrative target to compromise or to weaponize.
 - **Azure AD PIM** doesn't offer attackers the ability to steal credentials because it unlocks privileges already assigned to an account using MFA or other workflows, but a poorly designed workflow could allow an adversary to escalate privileges.
 - **Remote Desktop / Jump servers** used by administrators provide a host where many or all sensitive sessions pass through, enabling attackers to use standard credential theft attack tools to steal and reuse these credentials.
 - **VPNs** can store credentials in the solution, providing attackers with a potential treasure trove of privilege escalation, leading to the strong recommendation to use Azure AD for authentication to mitigate this risk.

Intermediary security profiles

Establishing these assurances requires a combination of security controls, some of which are common to many intermediaries, and some of which specific to the type of intermediary.



An intermediary is a link in the Zero Trust chain that presents an interface to users/devices and then enables access to the next interface. The security controls must address inbound connections, security of the intermediary device/application/service itself, and (if applicable) provide Zero Trust security signals for the next interface.

Common security controls

The common security elements for intermediaries are focused on maintaining good security hygiene for enterprise and specialized levels, with additional restrictions for privilege security.

	Enterprise Security	Specialized Security	Privileged Security	
Profile Summary	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts	
Intermediary Remote Access / Admin Broker	Enterprise Intermediary	Specialized Intermediary	Privileged Intermediary	
	Enterprise and Specialized have same requirements		Enterprise Security Plus	
	<ul style="list-style-type: none"> Rapidly apply security updates (often neglected) Apply secure configuration for application and any underlying operating system (using manufacturer or industry baselines/recommendations) Solution administration restricted to roles protected by <u>specialized or higher</u> session security 		<ul style="list-style-type: none"> Solution administration restricted to roles protected by <u>privileged</u> session security May be dedicated device or service for privileged roles 	

These security controls should be applied to all types of intermediaries:

- **Enforce inbound connection security** - Use Azure AD and Conditional Access to ensure all inbound connections from devices and accounts are known, trusted, and allowed. For more information, see the article [Securing privileged interfaces](#) for detailed definitions for device and account requirements for enterprise and specialized.
- **Proper system maintenance** - All intermediaries must follow good security hygiene practices including:
 - **Secure configuration** - Follow manufacturer or industry security configuration baselines and best practices for both the application and any underlying

- operating systems, cloud services, or other dependencies. Applicable guidance from Microsoft includes the Azure Security Baseline and Windows Baselines.
- **Rapid patching** - Security updates and patches from the vendors must be applied rapidly after release.
 - **Role-Based Access Control (RBAC)** models can be abused by attackers to escalate privileges. The RBAC model of the intermediary must be carefully review to ensure that only authorized personnel that are protected at a specialized or privileged level are granted administrative privileges. This model must include any underlying operating systems or cloud services (root account password, local administrator users/groups, tenant administrators, etc.).
 - **Endpoint detection and response (EDR) and outbound trust signal** - Devices that include a full operating system should be monitored and protected with an EDR like Microsoft Defender for Endpoint. This control should be configured to provides device compliance signals to Conditional Access so that policy can enforce this requirement for interfaces.

Privileged Intermediaries require additional security controls:

- **Role-Based Access Control (RBAC)** - Administrative rights must be restricted to only privileged roles meeting that standard for workstations and accounts.
- **Dedicated devices (optional)** - because of the extreme sensitivity of privileged sessions, organizations may choose to implement dedicated instances of intermediary functions for privileged roles. This control enables additional security restrictions for these privileged intermediaries and closer monitoring of privileged role activity.

Security guidance for each intermediary type

This section contains specific security guidance unique to each type of intermediary.

Privileged Access Management / Privileged Identity management

One type of intermediary designed explicitly for security use cases is privileged identity management / privileged access management (PIM/PAM) solutions.

Use cases and scenarios for PIM/PAM

PIM/PAM solutions are designed to increase security assurances for sensitive accounts that would be covered by specialized or privileged profiles, and typically focus first on IT administrators.

While features vary between PIM/PAM vendors, many solutions provide security capabilities to:

- Simplify service account management and password rotation (a critically important capability)
- Provide advanced workflows for just in time (JIT) access
- Record and monitor administrative sessions

Important

PIM/PAM capabilities provide excellent mitigations for some attacks, but do not address many privileged access risks, notably risk of device compromise. While some vendors advocate that their PIM/PAM solution is a 'silver bullet' solution that can mitigate device risk, our experience investigating customer incidents has consistently proven that this does not work in practice.

An attacker with control of a workstation or device can use those credentials (and privileges assigned to them) while the user is logged on (and can often steal credentials for later use as well). A PIM/PAM solution alone cannot consistently and reliably see and mitigate these device risks, so you must have discrete device and account protections that complement each other.

Security risks and recommendations for PIM/PAM

The capabilities from each PIM/PAM vendor vary on how to secure them, so review and follow your vendor's specific security configuration recommendations and best practices.

Note

Ensure you set up a second person in business critical workflows to help mitigate insider risk (increases the cost/friction for potential collusion by insider threats).

End-user Virtual Private Networks

Virtual Private Networks (VPNs) are intermediaries that provide full network access for remote endpoints, typically require the end user to authenticate, and can store credentials locally to authenticate inbound user sessions.

ⓘ Note

This guidance refers only to "point to site" VPNs used by users, not "site to site" VPNs that are typically used for datacenter/application connectivity.

Use cases and scenarios for VPNs

VPNs establish remote connectivity to enterprise network to enable resource access for users and administrators.

Security risks and recommendations for VPNs

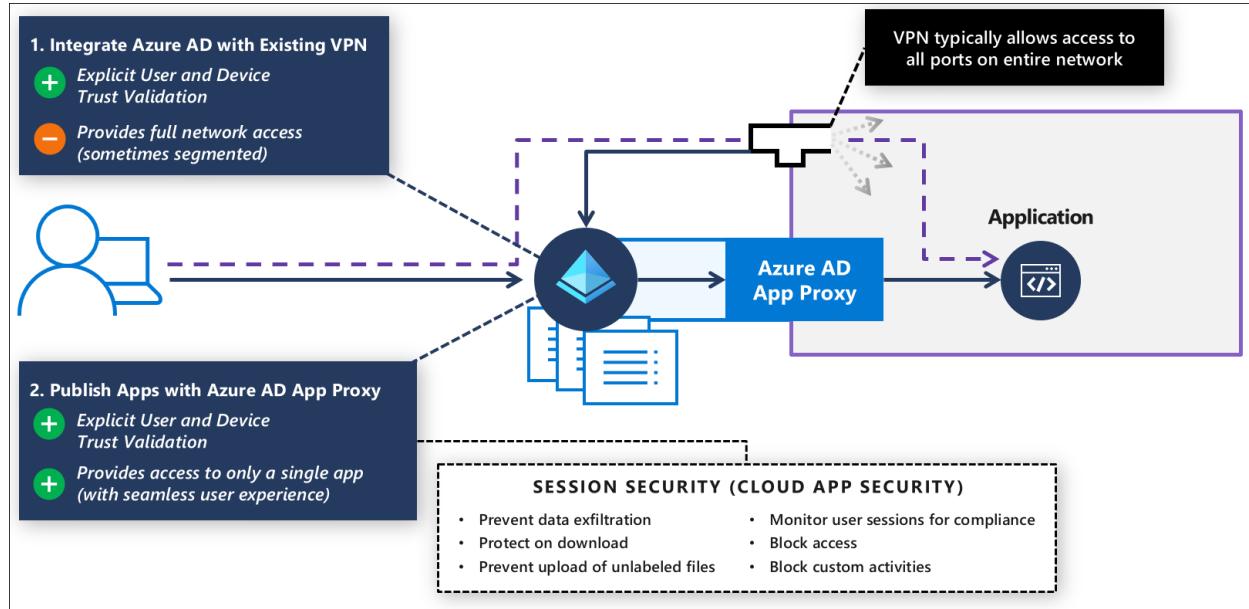
The most critical risks to VPN intermediaries are from maintenance neglect, configuration issues, and local storage of credentials.

Microsoft recommends a combination of controls for VPN intermediaries:

- **Integrate Azure AD authentication** - to reduce or eliminate risk of locally stored credentials (and any overhead burden to maintain them) and enforce Zero Trust policies on inbound accounts/devices with conditional access. For guidance on integrating, see
 - [Azure VPN AAD integration](#)
 - [Enable Azure AD Authentication on the VPN gateway](#)
 - Integrating third-party VPNs
 - [Cisco AnyConnect](#)
 - Palo Alto Networks [GlobalProtect](#) and [Captive Portal](#)
 - [F5](#)
 - [Fortinet FortiGate SSL VPN](#)
 - [Citrix NetScaler](#)
 - [Zscaler Private Access \(ZPA\)](#)
 - and [more](#)
- **Rapid patching** - Ensure that all organizational elements support rapid patching including:
 - **Organizational sponsorship** and leadership support for requirement
 - **Standard technical processes** for updating VPNs with minimal or zero downtime. This process should include VPN software, appliances, and any underlying operating systems or firmware
 - **Emergency processes** to rapidly deploy critical security updates
 - **Governance** to continually discover and remediate any missed items
- **Secure configuration** - The capabilities from each VPN vendor vary on how to secure them, so review and follow your vendor's specific security configuration

recommendations and best practices

- **Go beyond VPN** - Replace VPNs over time with more secure options like Azure AD App Proxy or Azure Bastion as these provide only direct application/server access rather than full network access. Additionally Azure AD App Proxy allows session monitoring for additional security with Microsoft Defender for Cloud Apps.



Azure AD App Proxy

Azure AD App Proxy and similar third-party capabilities provide remote access to legacy and other applications hosted on-premises or on IaaS VMs in the cloud.

Use cases and scenarios for Azure AD App Proxy

This solution is suitable for publishing legacy end-user productivity applications to authorized users over the internet. It can also be used for publishing some administrative applications.

Security risks and recommendations for Azure AD App Proxy

Azure AD App proxy effectively retrofits modern Zero Trust policy enforcement to existing applications. For more information, see Security considerations for Azure AD Application Proxy

Azure AD Application Proxy can also integrate with Microsoft Defender for Cloud Apps to add Conditional Access App Control session security to:

- Prevent data exfiltration
- Protect on download

- Prevent upload of unlabeled files
- Monitor user sessions for compliance
- Block access
- Block custom activities

For more information, see [Deploy Defender for Cloud Apps Conditional Access App Control for Azure AD apps](#)

As you publish applications via the Azure AD Application Proxy, Microsoft recommends having application owners work with security teams to follow least privilege and ensure access to each application is made available to only the users that require it. As you deploy more apps this way, you may be able to offset some end-user point to site VPN usage.

Remote Desktop / jump server

This scenario provides a full desktop environment running one or more applications. This solution has a number of different variations including:

- **Experiences** - Full desktop in a window or a single application projected experience
- **Remote host** - may be a shared VM or a dedicated desktop VM using Windows Virtual Desktop (WVD) or another Virtual Desktop Infrastructure (VDI) solution.
- **Local device** - may be a mobile device, a managed workstation, or a personal/partner managed workstation
- **Scenario** - focused on user productivity applications or on administrative scenarios, often called a 'jump server'

Use cases and security recommendations for Remote Desktop / Jump server

The most common configurations are:

- Direct Remote Desktop Protocol (RDP) - This configuration is not recommended for internet connections because RDP is a protocol that has limited protections against modern attacks like password spray. Direct RDP should be converted to either:
 - RDP through a gateway published by Azure AD App Proxy
 - Azure Bastion
- RDP through a gateway using
 - Remote Desktop Services (RDS) included in Windows Server. Publish with Azure AD Application Proxy.

- Windows Virtual Desktop (WVD) - Follow Windows Virtual Desktop security best practices.
- Third-party VDI - Follow manufacturer or industry best practices, or adapt WVD guidance to your solution
- Secure Shell (SSH) server - providing remote shell and scripting for technology departments and workload owners. Securing this configuration should include:
 - Following industry/manufacturer best practices to securely configure it, change any default passwords (if applicable), and using SSH keys instead of passwords, and securely storing and managing SSH keys.
 - Use Azure Bastion for SSH remoting to resources hosted in Azure - Connect to a Linux VM using Azure Bastion

Azure Bastion

Azure Bastion is an intermediary that is designed to provide secure access to Azure resources using a browser and the Azure portal. Azure Bastion provides access resources in Azure that support Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols.

Use cases and scenarios for Azure Bastion

[Azure Bastion](#) effectively provides a flexible solution that can be used by IT Operations personnel and workload administrators outside of IT to manage resources hosted in Azure without requiring a full VPN connection to the environment.

Security risks and recommendations for Azure Bastion

Azure Bastion is accessed through the Azure portal, so ensure that your Azure portal [interface](#) requires the appropriate [level of security](#) for the resources in it and roles using it, typically privileged or specialized level.

Additional guidance is available in the Azure Bastion Documentation

Next steps

- [Securing privileged access overview](#)
- [Privileged access strategy](#)
- [Measuring success](#)
- [Security levels](#)
- [Privileged access accounts](#)
- [Interfaces](#)

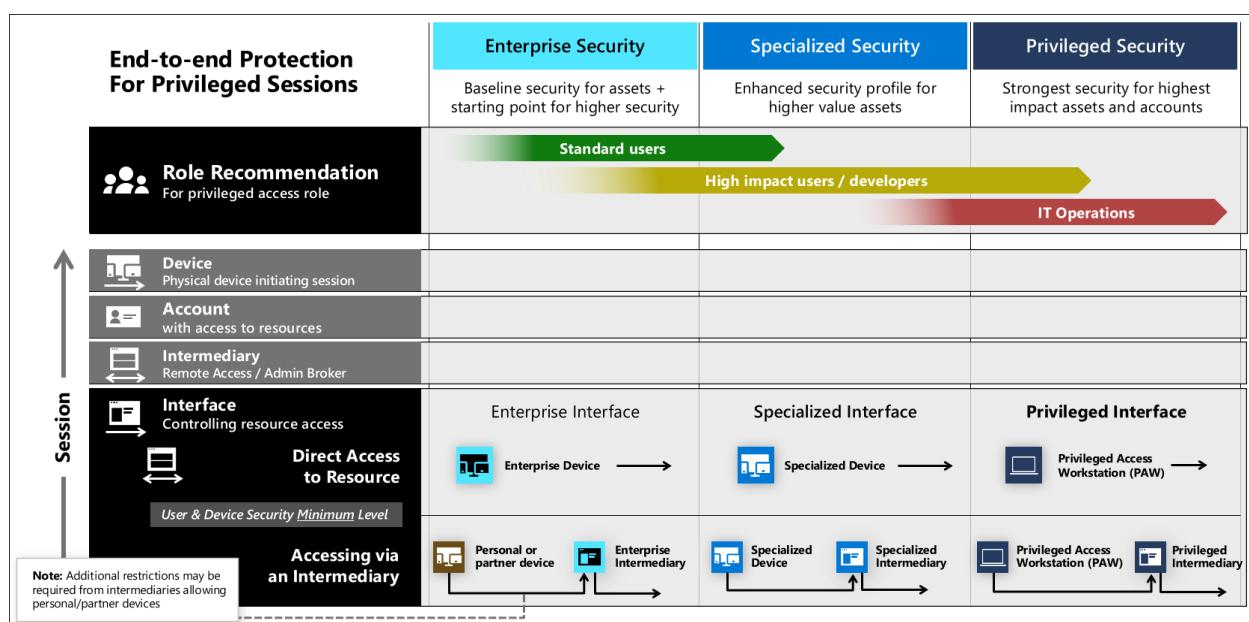
- Privileged access devices
- Enterprise access model

Privileged access: Interfaces

Article • 09/02/2022 • 4 minutes to read

A critical component of [securing privileged access](#) is the application of zero trust policy to ensure that devices, accounts, and intermediaries meet security requirements before providing access.

This policy ensures users and devices initiating the inbound session are known, trusted, and allowed to access the resource (via the interface). The policy enforcement is performed by the Azure AD Conditional Access policy engine that evaluates policy assigned to the specific application interface (such as Azure portal, Salesforce, Office 365, AWS, Workday, and others).



This guidance defines three security levels for interface security that you can use for assets with different sensitivity levels. These levels are configured in the [securing privileged access rapid modernization plan \(RAMP\)](#) and correspond to [security levels of accounts and devices](#).

The security requirements for inbound sessions to interfaces apply to accounts and the source device, whether it's a direct connection from [physical devices](#) or a Remote Desktop / Jump server [intermediary](#). Intermediaries can accept sessions from personal devices to provide enterprise security level (for some scenarios), but specialized or privileged intermediaries should not allow connections from lower levels because of the security sensitive nature of their roles.

ⓘ Note

These technologies provide strong end to end access control to the application interface, but the resource itself must also be secured from out of band attacks on the application code/functionality, unpatched vulnerabilities or configuration errors in the underlying operating system or firmware, on data at rest or in transit, supply chains, or other means.

Ensure to assess and discover risks to the assets themselves for complete protection. Microsoft provides tooling and guidance to help you with that including **Microsoft Defender for Cloud**, **Microsoft Secure Score**, and **threat modelling guidance** ↗.

Interface examples

Interfaces come in different forms, typically as:

- Cloud service/application websites such as Azure portal, AWS, Office 365
- Desktop Console managing an on-premises application (Microsoft Management Console (MMC) or custom application)
- Scripting/Console Interface such as Secure Shell (SSH) or PowerShell

While some of these directly support Zero Trust enforcement via the Azure AD Conditional Access policy engine, some of them will need to be published via an **intermediary** such as Azure AD App Proxy or Remote Desktop / jump server.

Interface security

The ultimate goal of interface security is to ensure that each inbound session to the interface is known, trusted, and allowed:

- Known – User is authenticated with strong authentication and device is authenticated (with exceptions for personal devices using a Remote Desktop or VDI solution for enterprise access)
- Trusted – Security health is explicitly validated and enforced for **accounts** and **devices** using a Zero Trust policy engine
- Allowed – Access to the resources follows least privilege principle using a combination of controls to ensure it can only be accessed
 - By the right users
 - At the right time (just in time access, not permanent access)
 - With the right approval workflow (as needed)
 - At an acceptable risk/trust level

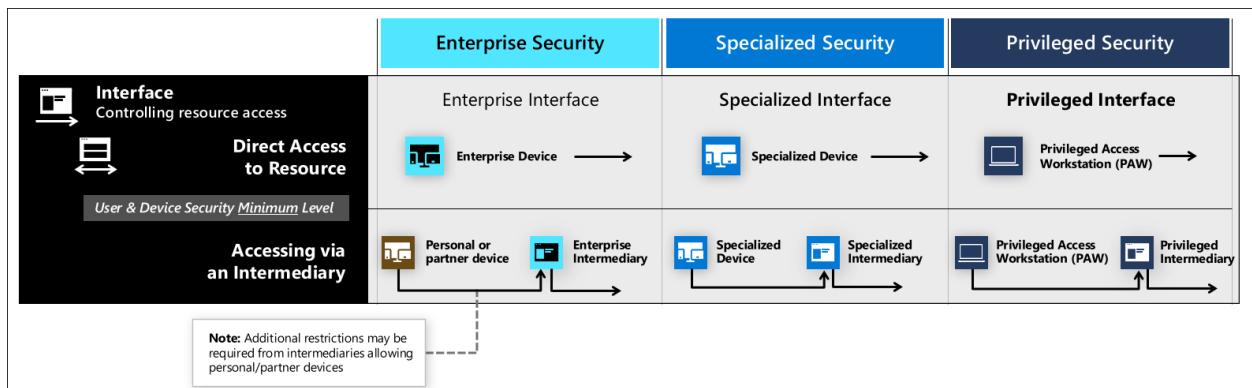
Interface security controls

Establishing interface security assurances requires a combination of security controls including:

- Zero Trust policy enforcement - using Conditional Access to ensure that the inbound sessions meet the requirements for:
 - Device Trust to ensure the device at minimum:
 - Is managed by the enterprise
 - Has endpoint detection and response on it
 - Is [compliant with organizations configuration requirements](#)
 - Isn't infected or under attack during the session
 - User Trust is high enough based on signals including:
 - Multi-factor authentication usage during initial logon (or added later to increase trust)
 - Whether this session matches historical behavior patterns
 - Whether the account or current session triggers any alerts based on threat intelligence
 - [Azure AD Identity Protection risk](#)
- Role-based access control (RBAC) model that combines enterprise directory groups/permissions and application-specific roles, groups, and permissions
- Just in time access workflows that ensure specific requirements for privileges (peer approvals, audit trail, privileged expiration, etc.) are enforced before allowing privileges the account is eligible for.

Interface security levels

This guidance defines three levels of security. For more information on these levels, see [Keep it Simple - Personas and Profiles](#). For implementation guidance, see the [rapid modernization plan](#).



Enterprise interface

Enterprise interface security is suitable for all enterprise users and productivity scenarios. Enterprise also serves as a starting point for higher sensitivity workloads that you can incrementally build on to reach specialized and privileged access levels of assurance.

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the enterprise or higher level
 - To support, bring your own device (BYOD) scenarios, personal devices, and partner-managed devices may be allowed connect if they use an enterprise intermediary such as a dedicated [Windows Virtual Desktop \(WVD\)](#) or similar Remote Desktop / Jump server solution.
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the specialized or privileged security level

Specialized interface

Security controls for specialized interfaces should include

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the specialized or privileged level
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the specialized or privileged security level
- Just in time access workflows (optional) - that enforce least privilege by ensuring privileges are used only by authorized users during the time they are needed.

Privileged interface

Security controls for specialized interfaces should include

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the privileged level
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the privileged security level
- Just in time access workflows (required) that enforce least privilege by ensuring privileges are used only by authorized users during the time they are needed.

Next steps

- [Securing privileged access overview](#)
- [Privileged access strategy](#)
- [Measuring success](#)
- [Security levels](#)

- Privileged access accounts
- Intermediaries
- Privileged access devices
- Enterprise access model

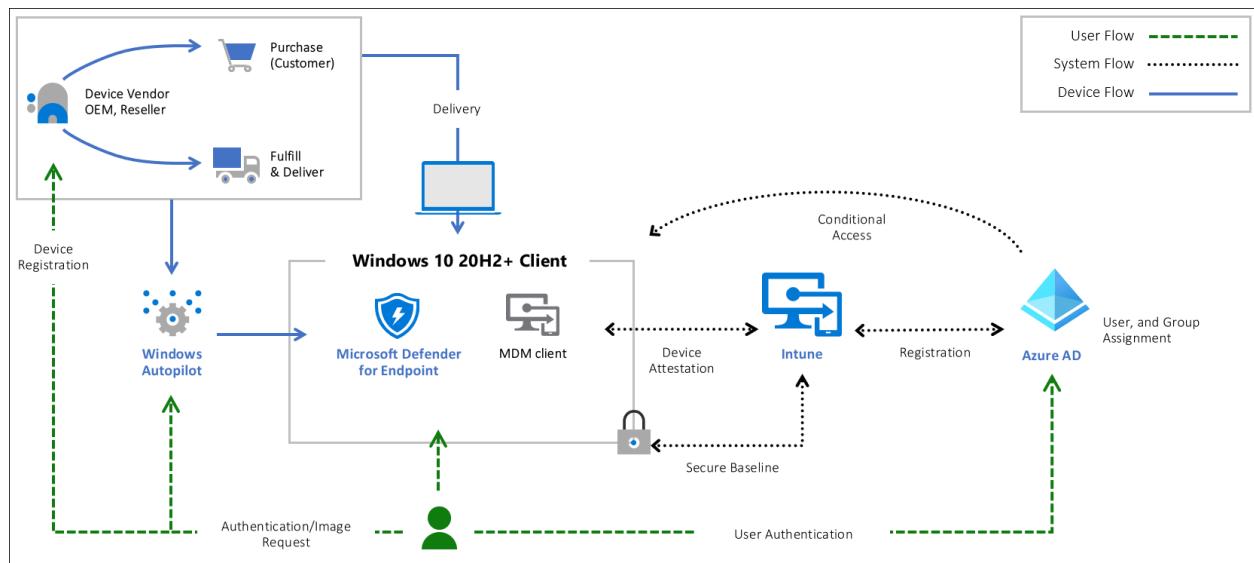
Securing devices as part of the privileged access story

Article • 09/02/2022 • 6 minutes to read

This guidance is part of a complete [privileged access strategy](#) and is implemented as part of the [Privileged access deployment](#)

End to end zero trust [security for privileged access](#) requires a strong foundation of device security upon which to build other security assurances for the session. While security assurances may be enhanced in the session, they will always be limited by how strong the security assurances are in the originating device. An attacker with control of this device can impersonate users on it or steal their credentials for future impersonation. This risk undermines other assurances on the account, intermediaries like jump servers, and on the resources themselves. For more information, see [clean source principle](#)

The article provides an overview of security controls to provide a secure workstation for sensitive users throughout its lifecycle.



This solution relies on core security capabilities in the Windows 10 operating system, Microsoft Defender for Endpoint, Azure Active Directory, and Microsoft InTune.

Who benefits from a secure workstation?

All users and operators benefit from using a secure workstation. An attacker who compromises a PC or device can impersonate or steal credentials/tokens for all accounts that use it, undermining many or all other security assurances. For administrators or sensitive accounts, this allows attackers to escalate privileges and increase the access

they have in your organization, often dramatically to domain, global, or enterprise administrator privileges.

For details on security levels and which users should be assigned to which level, see [Privileged access security levels](#)

Device Security Controls

The successful deployment of a secure workstation requires it to be part of an end to end approach including devices, [accounts](#), [intermediaries](#), and security policies applied to your [application interfaces](#). All elements of the stack must be addressed for a complete privileged access security strategy.

This table summarizes the security controls for different device levels:

Profile	Enterprise	Specialized	Privileged
Microsoft Endpoint Manager (MEM) managed	Yes	Yes	Yes
Deny BYOD Device enrollment	No	Yes	Yes
MEM security baseline applied	Yes	Yes	Yes
Microsoft Defender for Endpoint	Yes*	Yes	Yes
Join personal device via Autopilot	Yes*	Yes*	No
URLs restricted to approved list	Allow Most	Allow Most	Deny Default
Removal of admin rights		Yes	Yes
Application execution control (AppLocker)		Audit -> Enforced	Yes
Applications installed only by MEM		Yes	Yes

ⓘ Note

The solution can be deployed with new hardware, existing hardware, and bring your own device (BYOD) scenarios.

At all levels, good security maintenance hygiene for security updates will be enforced by Intune policies. The differences in security as the device security level increases are focused on reducing the attack surface that an attacker can attempt to exploit (while preserving as much user productivity as possible). Enterprise and specialized level devices allow productivity applications and general web browsing, but privileged access

workstations do not. Enterprise users may install their own applications, but specialized users may not (and are not local administrators of their workstations).

 **Note**

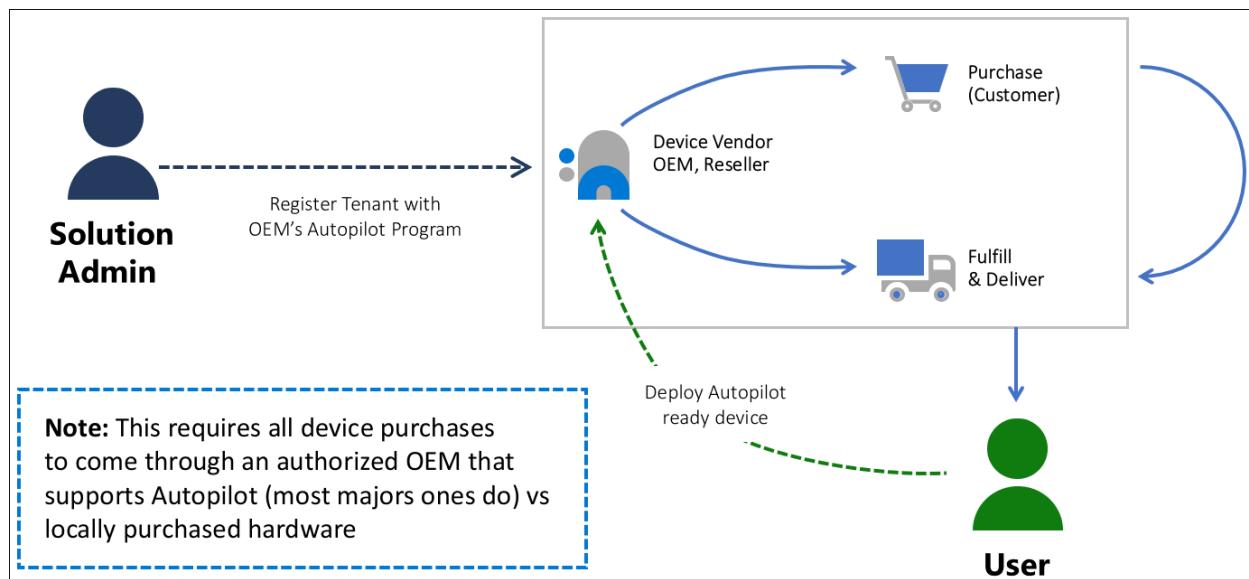
Web browsing here refers to general access to arbitrary websites which can be a high risk activity. Such browsing is distinctly different from using a web browser to access a small number of well-known administrative websites for services like Azure, Microsoft 365, other cloud providers, and SaaS applications.

Hardware root of trust

Essential to a secured workstation is a supply chain solution where you use a trusted workstation called the 'root of trust'. Technology that must be considered in the selection of the root of trust hardware should include the following technologies included in modern laptops:

- [Trusted Platform Module \(TPM\) 2.0](#)
- [BitLocker Drive Encryption](#)
- [UEFI Secure Boot](#)
- [Drivers and Firmware Distributed through Windows Update](#)
- [Virtualization and HVCI Enabled](#)
- [Drivers and Apps HVCI-Ready](#)
- [Windows Hello](#)
- [DMA I/O Protection](#)
- [System Guard](#)
- [Modern Standby](#)

For this solution, root of trust will be deployed using [Windows Autopilot](#) technology with hardware that meets the modern technical requirements. To secure a workstation, Autopilot lets you leverage Microsoft OEM-optimized Windows 10 devices. These devices come in a known good state from the manufacturer. Instead of reimaging a potentially insecure device, Autopilot can transform a Windows 10 device into a "business-ready" state. It applies settings and policies, installs apps, and even changes the edition of Windows 10.



Device roles and profiles

This guidance shows how to harden Windows 10 and reduce the risks associated with device or user compromise. To take advantage of the modern hardware technology and root of trust device, the solution uses [Device Health Attestation](#). This capability is present to ensure the attackers cannot be persistent during the early boot of a device. It does so by using policy and technology to help manage security features and risks.

End-to-end Protection For Privileged Sessions	Enterprise Security	Specialized Security	Privileged Security
	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
Role Recommendation For privileged access role	Standard users	High impact users / developers	IT Operations
Device Physical device initiating session Profile Summary	Enterprise Device <i>Protect existing attack surface</i> • Centrally Managed Policies • Productivity & Admin Apps • Endpoint Detection and Response (EDR) • Monitor app and browser activity	Specialized Device <i>Limit new attack surface</i> Enterprise Security Plus... • No local admin privileges • Block unexpected applications	Privileged Access Workstation (PAW) <i>Highly Restricted attack surface</i> Specialized Security Plus... • Restricted applications (limited or no productivity apps) • Restricted web browsing
Account with access to resources			
Intermediary Remote Access / Admin Broker			
Interface Controlling resource access			

- **Enterprise Device** – The first managed role is good for home users, small business users, general developers, and enterprises where organizations want to raise the minimum security bar. This profile permits users to run any applications and browse any website, but an anti-malware and endpoint detection and response (EDR) solution like [Microsoft Defender for Endpoint](#) is required. A policy-based approach to increase the security posture is taken. It provides a secure means to work with customer data while also using productivity tools like email and web

browsing. Audit policies and Intune allow you to monitor an Enterprise workstation for user behavior and profile usage.

The enterprise security profile in the [privileged access deployment](#) guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

- **Specialized Device** – This represents a significant step up from enterprise usage by removing the ability to self-administer the workstation and limiting which applications may run to only the applications installed by an authorized administrator (in the program files and pre-approved applications in the user profile location. Removing the ability to install applications may impact productivity if implemented incorrectly, so ensure that you have provided access to Microsoft store applications or corporate managed applications that can be rapidly installed to meet users needs. For guidance on which users should be configured with specialized level devices, see [Privileged access security levels](#)
 - The Specialized security user demands a more controlled environment while still being able to do activities such as email and web browsing in a simple-to-use experience. These users expect features such as cookies, favorites, and other shortcuts to work but do not require the ability to modify or debug their device operating system, install drivers, or similar.

The specialized security profile in the [privileged access deployment](#) guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

- **Privileged Access Workstation (PAW)** – This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive job tasks. This makes the PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications and web browsing. While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in the organization.
 - A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).

The privileged security profile in the [privileged access deployment](#) guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

Next steps

[Deploy a secure Azure-managed workstation.](#)

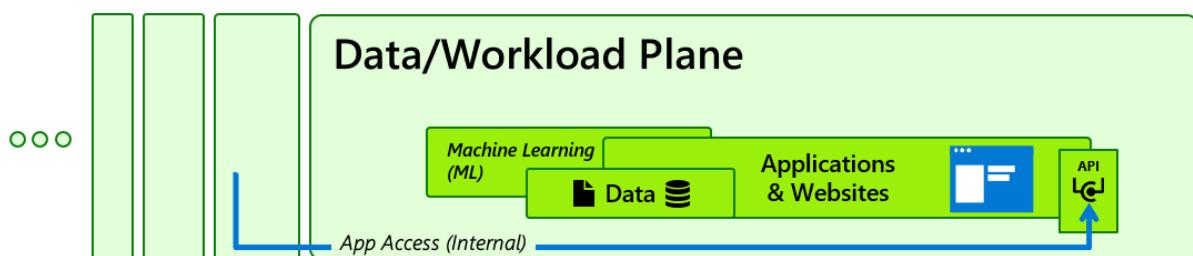
Enterprise access model

Article • 09/02/2022 • 3 minutes to read

This document describes an overall enterprise access model that includes context of how a [privileged access strategy](#) fits in. For a roadmap on how to adopt a privileged access strategy, see the [rapid modernization plan \(RaMP\)](#). For implementation guidance to deploy this, see [privileged access deployment](#)

Privileged access strategy is part of an overall enterprise access control strategy. This enterprise access model shows how privileged access fits into an overall enterprise access model.

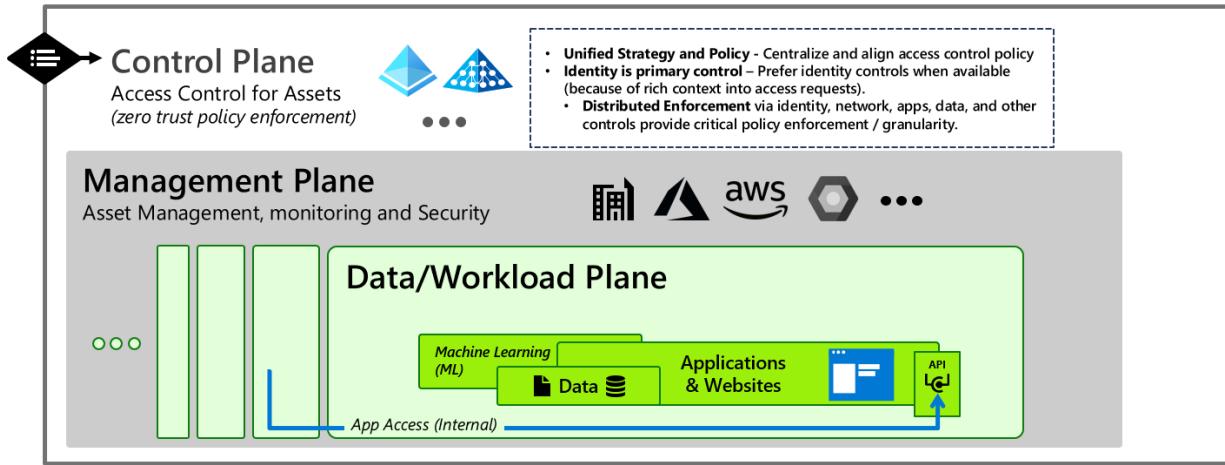
The primary stores of business value that an organization must protect are in the Data/Workload plane:



The applications and data typically store a large percentage of an organization's:

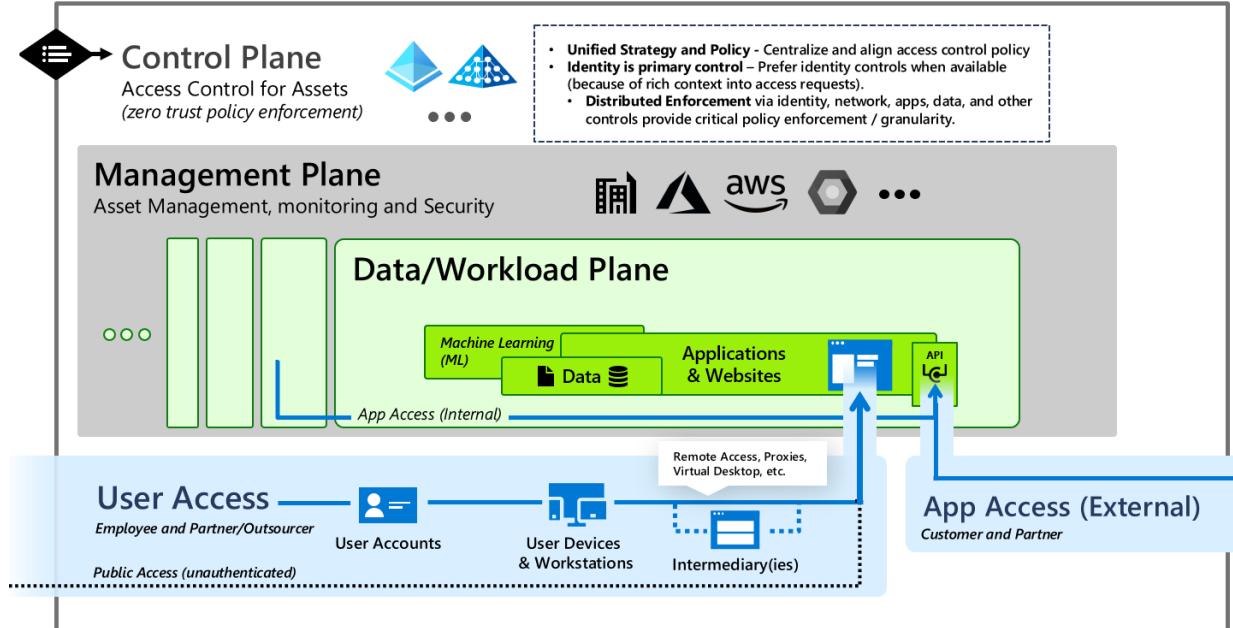
- **Business processes** in applications and workloads
- **Intellectual property** in data and applications

The enterprise IT organization manages and supports the workloads and the infrastructure they are hosted on, whether it's on-premises, on Azure, or a third-party cloud provider, creating a **management plane**. Providing consistent access control to these systems across the enterprise requires a **control plane** based on centralized enterprise identity system(s), often supplemented by network access control for older systems like operational technology (OT) devices.

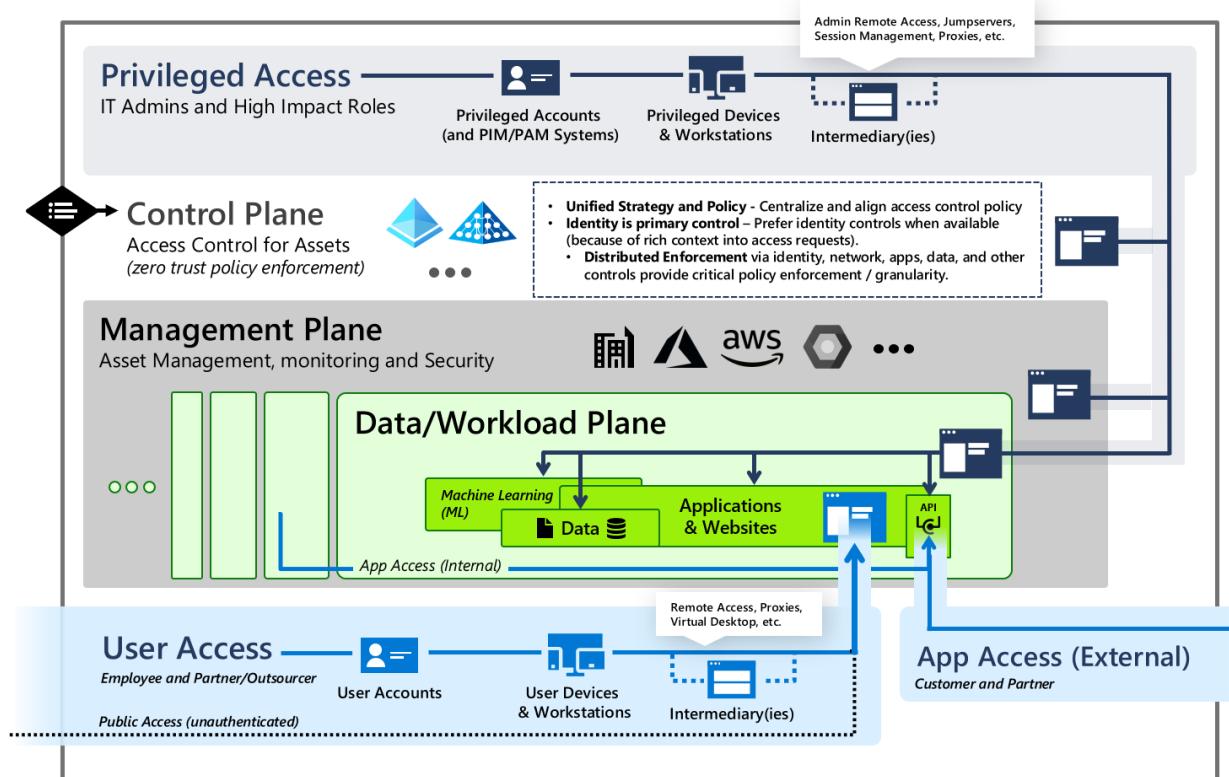


Each of these planes has control of the data and workloads by virtue of their functions, creating an attractive pathway for attackers to abuse if they can gain control of either plane.

For these systems to create business value, they must be accessible to internal users, partners, and customers using their workstations or devices (often using remote access solutions) - creating **user access** pathways. They must also frequently be available programmatically via application programming interfaces (APIs) to facilitate process automation, creating **application access** pathways.



Finally, these systems must be managed and maintained by IT staff, developers, or others in the organizations, creating **privileged access** pathways. Because of the high level of control they provide over business critical assets in the organization, these pathways must be stringently protected against compromise.

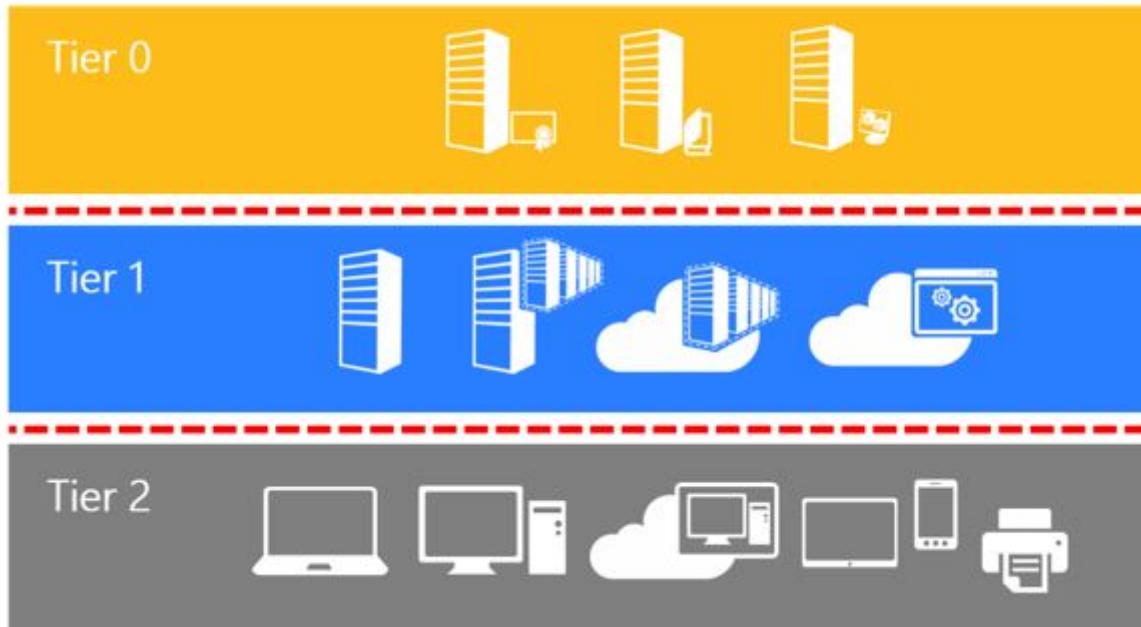


Providing consistent access control in the organization that enables productivity and mitigates risk requires you to

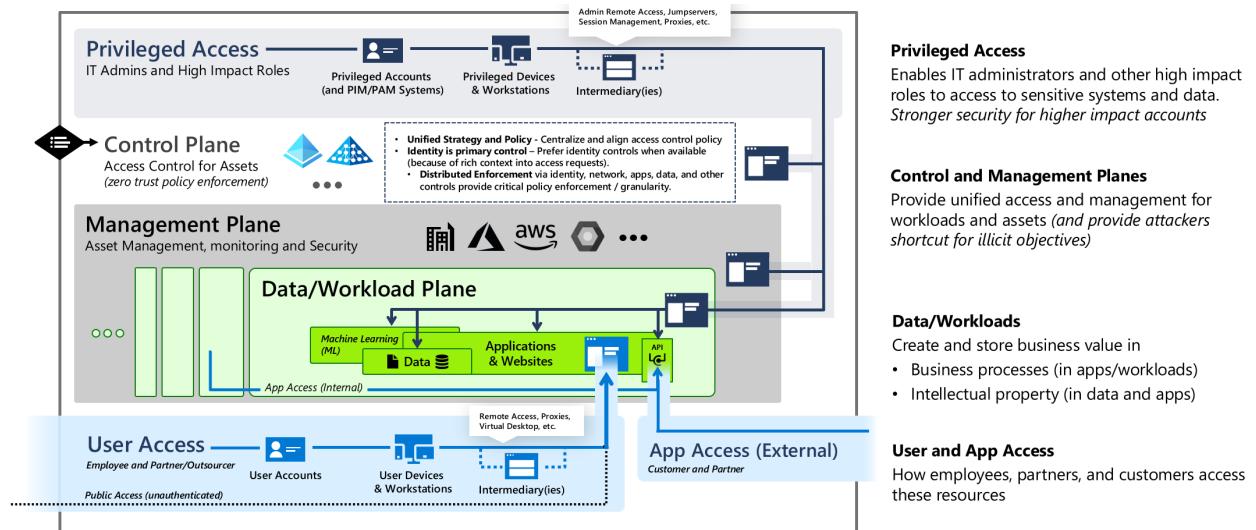
- Enforce Zero Trust principles on all access
 - Assume Breach of other components
 - Explicit validation of trust
 - Least privilege access
- Pervasive security and policy enforcement across
 - Internal and external access to ensure consistent policy application
 - All access methods including users, admins, APIs, service accounts, etc.
- Mitigate unauthorized privilege escalation
 - Enforce hierarchy – to prevent control of higher planes from lower planes (via attacks or abuse of legitimate processes)
 - Control plane
 - Management plane
 - Data/workload plane
 - Continuously audit for configuration vulnerabilities enabling inadvertent escalation
 - Monitor and respond to anomalies that could represent potential attacks

Evolution from the legacy AD tier model

The enterprise access model supersedes and replaces the legacy tier model that was focused on containing unauthorized escalation of privilege in an on-premises Windows Server Active Directory environment.



The enterprise access model incorporates these elements as well as full access management requirements of a modern enterprise that spans on-premises, multiple clouds, internal or external user access, and more.



Tier 0 scope expansion

Tier 0 expands to become the control plane and addresses all aspects of access control, including networking where it is the only/best access control option, such as legacy OT options

Tier 1 splits

To increase clarity and actionability, what was tier 1 is now split into the following areas:

- **Management plane** – for enterprise-wide IT management functions
- **Data/Workload plane** – for per-workload management, which is sometimes performed by IT personnel and sometimes by business units

This split ensures focus for protecting business critical systems and administrative roles that have high intrinsic business value, but limited technical control. Additionally, this split better accommodates developers and DevOps models vs. focusing too heavily on classic infrastructure roles.

Tier 2 splits

To ensure coverage for application access and the various partner and customer models, Tier 2 was split into the following areas:

- **User access** – which includes all B2B, B2C, and public access scenarios
- **App access** – to accommodate API access pathways and resulting attack surface

Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices

Privileged access deployment

Article • 02/01/2023 • 23 minutes to read

This document will guide you through implementing the technical components of the [privileged access strategy](#), including secure accounts, workstations and devices, and interface security (with conditional access policy).

	Enterprise Security	Specialized Security	Privileged Security
	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
 Device Physical device initiating session	Enterprise Device	Specialized Device	Privileged Access Workstation (PAW)
 Account with access to resources	Enterprise Account	Specialized Account	Privileged Account
 Intermediary Remote Access / Admin Broker	Enterprise Intermediary	Specialized Intermediary	Privileged Intermediary
 Interface Controlling resource access	Enterprise Interface	Specialized Interface	Privileged Interface

This guidance sets up all of the profiles for all three security levels and should be assigned your organizations roles based on the [Privileged access security levels](#) guidance. Microsoft recommends configuring them in the order described in the [rapid modernization plan \(RAMP\)](#)

License requirements

The concepts covered in this guide assume you have Microsoft 365 Enterprise E5 or an equivalent SKU. Some of the recommendations in this guide can be implemented with lower SKUs. For more information, see [Microsoft 365 Enterprise licensing](#).

To automate license provisioning, consider [group-based licensing](#) for your users.

Azure Active Directory configuration

Azure Active Directory (Azure AD) manages users, groups, and devices for your administrator workstations. Enable identity services and features with an [administrator account](#).

When you create the secured workstation administrator account, you expose the account to your current workstation. Make sure you use a known safe device to do this initial configuration and all global configuration. To reduce the attack exposure for the first-time experience, consider following the [guidance to prevent malware infections](#).

Require multi-factor authentication, at least for your administrators. See [Conditional Access: Require MFA for administrators](#) for implementation guidance.

Azure AD users and groups

1. From the Azure portal, browse to **Azure Active Directory > Users > New user**.
2. Create your device user by following the steps in the [create user tutorial](#).
3. Enter:
 - **Name** - Secure Workstation Administrator
 - **User name** - `secure-ws-user@contoso.com`
 - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
 - **Usage Location** - For example **United Kingdom**, or your desired location from the list.
4. Select **Create**.

Create your device administrator user.

1. Enter:
 - **Name** - Secure Workstation Administrator
 - **User name** - `secure-ws-admin@contoso.com`
 - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
 - **Usage Location** - For example **United Kingdom**, or your desired location from the list.
2. Select **Create**.

Next, you create four groups: **Secure Workstation Users**, **Secure Workstation Admins**, **Emergency BreakGlass** and **Secure Workstation Devices**.

From the Azure portal, browse to **Azure Active Directory > Groups > New group**.

1. For the workstation users group, you might want to configure [group-based licensing](#) to automate provisioning of licenses to users.
2. For the workstation users group, enter:
 - **Group type** - Security
 - **Group name** - Secure Workstation Users
 - **Membership type** - Assigned

3. Add your secure workstation user: `secure-ws-user@contoso.com`

4. You can add any other users that will be using secure workstations.

5. Select **Create**.

6. For the Privileged Workstation Admins group, enter:

- **Group type** - Security
- **Group name** - Secure Workstation Admins
- **Membership type** - Assigned

7. Add your secure workstation user: `secure-ws-admin@contoso.com`

8. You can add any other users that will be managing secure workstations.

9. Select **Create**.

10. For the Emergency BreakGlass group, enter:

- **Group type** - Security
- **Group name** - Emergency BreakGlass
- **Membership type** - Assigned

11. Select **Create**.

12. Add Emergency Access accounts to this group.

13. For the workstation devices group, enter:

- **Group type** - Security
- **Group name** - Secure Workstations
- **Membership type** - Dynamic Device
- **Dynamic Membership rules** - `(device.devicePhysicalIds -any _ -contains "[OrderID]:PAW")`

14. Select **Create**.

Azure AD device configuration

Specify who can join devices to Azure AD

Configure your devices setting in Active Directory to allow your administrative security group to join devices to your domain. To configure this setting from the Azure portal:

1. Go to **Azure Active Directory > Devices > Device settings**.

2. Choose **Selected** under **Users may join devices to Azure AD**, and then select the "Secure Workstation Users" group.

Remove local admin rights

This method requires that users of the VIP, DevOps, and Privileged workstations have no administrator rights on their machines. To configure this setting from the Azure portal:

1. Go to **Azure Active Directory > Devices > Device settings**.
2. Select **None** under **Additional local administrators on Azure AD joined devices**.

Refer to [How to manage the local administrators group on Azure AD joined devices](#) for details on how to manage members of the local administrators group.

Require multi-factor authentication to join devices

To further strengthen the process of joining devices to Azure AD:

1. Go to **Azure Active Directory > Devices > Device settings**.
2. Select **Yes** under **Require Multi-Factor Auth to join devices**.
3. Select **Save**.

Configure mobile device management

From the Azure portal:

1. Browse to **Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune**.
2. Change the **MDM user scope** setting to **All**.
3. Select **Save**.

These steps allow you to manage any device with Microsoft Endpoint Manager. For more information, see [Intune Quickstart: Set up automatic enrollment for Windows 10 devices](#).

You create Intune configuration and compliance policies in a future step.

Azure AD Conditional Access

Azure AD Conditional Access can help restrict privileged administrative tasks to compliant devices. Predefined members of the **Secure Workstation Users** group are required to perform multi-factor authentication when signing in to cloud applications. A best practice is to exclude emergency access accounts from the policy. For more information, see [Manage emergency access accounts in Azure AD](#).

Conditional Access only allowing secured workstation ability to access Azure portal

Organizations should block Privileged Users from being able to connect to cloud management interfaces, portals and PowerShell, from non-PAW devices.

To block unauthorized devices from being able to access cloud management interfaces, follow the guidance in the article [Conditional Access: Filters for Devices \(preview\)](#). It's essential that while deploying this feature you consider, [emergency access account](#) functionality. These accounts should be used only for extreme cases and the account managed through policy.

Note

You will need to create a user group, and include your emergency user that can bypass the Conditional Access policy. For our example we have a security group called **Emergency BreakGlass**

This policy set will ensure that your Administrators must use a device that is able to present a specific device attribute value, that MFA is satisfied, and the device is marked as compliant by Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

Organizations should also consider blocking legacy authentication protocols in their environments. There are multiple ways to accomplish this task, for more information about blocking legacy authentication protocols, see the article, [How to: Block legacy authentication to Azure AD with Conditional Access](#).

Microsoft Intune configuration

Device enrollment deny BYOD

In our sample, we recommend that BYOD devices not be permitted. Using [Intune BYOD enrollment](#) allows users to enroll devices that are less, or not trusted. However it's important to note that in organizations that have a limited budget to purchase new devices, looking to use existing hardware fleet, or considering non-windows devices, might consider the BYOD capability in Intune to deploy the Enterprise profile.

The following guidance will configure Enrollment for deployments that will deny BYOD access.

Set enrollment restrictions preventing BYOD

1. In the Microsoft Endpoint Manager admin center [↗](#), choose > Devices > Enrollment restrictions > choose the default restriction All Users
2. Select Properties > Platform settings Edit
3. Select Block for All types, except Windows MDM.
4. Select Block for all Personally owned items.

Create an Autopilot deployment profile

After creating a device group, you must create a deployment profile to configure the Autopilot devices.

1. In the Microsoft Endpoint Manager admin center [↗](#), choose Device enrollment > Windows enrollment > Deployment Profiles > Create Profile.
2. Enter:
 - Name - Secure workstation deployment profile.
 - Description - Deployment of secure workstations.
 - Set Convert all targeted devices to Autopilot to Yes. This setting makes sure that all devices in the list get registered with the Autopilot deployment service. Allow 48 hours for the registration to be processed.
3. Select Next.
 - For Deployment mode, choose **Self-Deploying (Preview)**. Devices with this profile are associated with the user who enrolls the device. During the deployment, it is advisable to use the Self-Deployment mode features to include:
 - Enrolls the device in Intune Azure AD automatic MDM enrollment, and only allow for a device to be accessed until all policies, applications, certificates, and networking profiles are provisioned on the device.
 - User credentials are required to enroll the device. It's essential to note that deploying a device in the **Self-Deploying** mode will allow you to deploy laptops in a shared model. No user assignment will happen until the device is assigned to a user for the first time. As a result, any user policies such as BitLocker will not be enabled until a user assignment is completed. For more information about how to log on to a secured device, see [selected profiles](#).
 - Select your Language (Region), User account type standard.
4. Select Next.
 - Select a scope tag if you have preconfigured one.
5. Select Next.

6. Choose **Assignments** > **Assign to** > **Selected Groups**. In **Select groups to include**, choose **Secure Workstations**.

7. Select **Next**.

8. Select **Create** to create the profile. The Autopilot deployment profile is now available to assign to devices.

Device enrollment in Autopilot provides a different user experience based on device type and role. In our deployment example, we illustrate a model where the secured devices are bulk deployed and can be shared, but when used for the first time, the device is assigned to a user. For more information, see [Intune Autopilot device enrollment](#).

Enrollment Status Page

The Enrollment Status Page (ESP) displays provisioning progress after a new device is enrolled. To ensure that devices are fully configured before use, Intune provides a means to **Block device use until all apps and profiles are installed**.

Create and assign enrollment status page profile

1. In the [Microsoft Endpoint Manager admin center](#), choose **Devices** > **Windows** > **Windows enrollment** > **Enrollment Status Page** > **Create profile**.
2. Provide a **Name** and **Description**.
3. Choose **Create**.
4. Choose the new profile in the **Enrollment Status Page** list.
5. Set **Show app profile installation progress** to **Yes**.
6. Set **Block device use until all apps and profiles are installed** to **Yes**.
7. Choose **Assignments** > **Select groups** > choose **Secure Workstation** group > **Select** > **Save**.
8. Choose **Settings** > choose the settings you want to apply to this profile > **Save**.

Configure Windows Update

Keeping Windows 10 up to date is one of the most important things you can do. To maintain Windows in a secure state, you deploy an [update ring](#) to manage the pace that updates are applied to workstations.

This guidance recommends that you create a new update ring and change the following default settings:

1. In the [Microsoft Endpoint Manager admin center](#), choose **Devices** > **Software updates** > **Windows 10 Update Rings**.

2. Enter:

- Name - Azure-managed workstation updates
- Servicing channel - Semi-annual channel
- Quality update deferral (days) - 3
- Feature update deferral period (days) - 3
- Automatic update behavior - Auto install and reboot without end-user control
- Block user from pausing Windows updates - Block
- Require user's approval to restart outside of work hours - Required
- Allow user to restart (engaged restart) - Required
- Transition users to engaged restart after an auto-restart (days) - 3
- Snooze engaged restart reminder (days) - 3
- Set deadline for pending restarts (days) - 3

3. Select **Create**.

4. On the **Assignments** tab, add the **Secure Workstations** group.

For more information about Windows Update policies, see [Policy CSP - Update](#).

Microsoft Defender for Endpoint Intune integration

Microsoft Defender for Endpoint and Microsoft Intune work together to help prevent security breaches. They can also limit the impact of breaches. ATP capabilities provide real-time threat detection as well as enable extensive auditing and logging of the end-point devices.

To configure integration of Windows Defender for Endpoint and Microsoft Endpoint Manager:

1. In the [Microsoft Endpoint Manager admin center](#), choose **Endpoint Security > Microsoft Defender ATP**.
2. In step 1 under **Configuring Windows Defender ATP**, select **Connect Windows Defender ATP to Microsoft Intune in the Windows Defender Security Center**.
3. In the Windows Defender Security Center:
 - a. Select **Settings > Advanced features**.
 - b. For **Microsoft Intune connection**, choose **On**.
 - c. Select **Save preferences**.
4. After a connection is established, return to Microsoft Endpoint Manager and select **Refresh** at the top.

5. Set Connect Windows devices version(20H2) 19042.450 and above to Windows Defender ATP to On.

6. Select Save.

Create the device configuration profile to onboard Windows devices

1. Sign in to the [Microsoft Endpoint Manager admin center](#), choose **Endpoint security > Endpoint detection and response > Create profile**.

2. For **Platform**, select **Windows 10 and Later**.

3. For **Profile type**, select **Endpoint detection and response**, and then select **Create**.

4. On the **Basics** page, enter a *PAW - Defender for Endpoint* in the **Name** field and **Description** (optional) for the profile, then choose **Next**.

5. On the **Configuration settings** page, configure the following option in **Endpoint Detection and Response**:

- **Sample sharing for all files:** Returns or sets the Microsoft Defender Advanced Threat Protection Sample Sharing configuration parameter.

[Onboard Windows 10 machines using Microsoft Endpoint Configuration Manager](#) has more details on these Microsoft Defender ATP settings.

6. Select **Next** to open the **Scope tags** page. Scope tags are optional. Select **Next** to continue.

7. On the **Assignments** page, select **Secure Workstation** group. For more information on assigning profiles, see [Assign user and device profiles](#).

Select **Next**.

8. On the **Review + create** page, when you're done, choose **Create**. The new profile is displayed in the list when you select the policy type for the profile you created. **OK**, and then **Create** to save your changes, which creates the profile.

For more information, see [Windows Defender Advanced Threat Protection](#).

Finish workstation profile hardening

To successfully complete the hardening of the solution, download and execute the appropriate script. Find the download links for your desired **profile level**:

Profile	Download location	Filename
Enterprise	https://aka.ms/securedworkstationgit	Enterprise-Workstation-Windows10-(20H2).ps1
Specialized	https://aka.ms/securedworkstationgit	Specialized - Windows10-(20H2).ps1
Privileged	https://aka.ms/securedworkstationgit	Privileged-Windows10-(20H2).ps1

 **Note**

The removal of admin rights and access, as well as, Application execution control (AppLocker) are managed by the policy profiles that are deployed.

After the script successfully executes, you can make updates to profiles and policies in Intune. The scripts will create policies and profiles for you, but you must assign the policies to your **Secure Workstations** device group.

- Here's where you can find the Intune device configuration profiles created by the scripts: [Azure portal > Microsoft Intune > Device configuration > Profiles](#).
- Here's where you can find the Intune device compliance policies created by the scripts: [Azure portal > Microsoft Intune > Device Compliance > Policies](#).

Run the Intune data export script `DeviceConfiguration_Export.ps1` from the [DeviceConfiguration GitHub repository](#) to export all current Intune profiles for comparison, and evaluation of the profiles.

Set rules in the Endpoint Protection Configuration Profile for Microsoft Defender Firewall

Windows Defender Firewall policy settings are included in the Endpoint Protection Configuration Profile. The behavior of the policy applied in described in the table below.

Profile	Inbound Rules	Outbound Rules	Merge behavior
Enterprise	Block	Allow	Allow
Specialized	Block	Allow	Block
Privileged	Block	Block	Block

Enterprise: This configuration is the most permissive as it mirrors the default behavior of a Windows Install. All inbound traffic is blocked except for rules that are explicitly defined in

the local policy rules as merging of local rules is set to allowed. All outbound traffic is allowed.

Specialized: This configuration is more restrictive as it ignores all locally defined rules on the device. All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. All outbound traffic is allowed.

Privileged: All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. Outbound traffic is also blocked apart from explicit rules that allow DNS, DHCP, NTP, NSCI, HTTP, and HTTPS traffic. This configuration not only reduces the attack surface presented by the device to the network it limits the outbound connections that the device can establish to only those connections required to administer cloud services.

Rule	Direction	Action	Application / Service	Protocol	Local Ports	Remote Ports
World Wide Web Services (HTTP Traffic-out)	Outbound	Allow	All	TCP	All ports	80
World Wide Web Services (HTTPS Traffic-out)	Outbound	Allow	All	TCP	All ports	443
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	546	547
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	Outbound	Allow	Dhcp	TCP	546	547

Rule	Direction	Action	Application / Service	Protocol	Local Ports	Remote Ports
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	68	67
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out)	Outbound	Allow	Dhcp	TCP	68	67
Core Networking - DNS (UDP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	UDP	All Ports	53
Core Networking - DNS (UDP-Out)	Outbound	Allow	Dnscache	UDP	All Ports	53
Core Networking - DNS (TCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All Ports	53
Core Networking - DNS (TCP-Out)	Outbound	Allow	Dnscache	TCP	All Ports	53
NSCI Probe (TCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All ports	80
NSCI Probe - DNS (TCP-Out)	Outbound	Allow	NlaSvc	TCP	All ports	80
Windows Time (UDP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All ports	80

Rule	Direction	Action	Application / Service	Protocol	Local Ports	Remote Ports
Windows Time Probe - DNS (UDP-Out)	Outbound	Allow	W32Time	UDP	All ports	123
Delivery Optimization (TCP-In)	Inbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	7680	All ports
Delivery Optimization (TCP-In)	Inbound	Allow	DoSvc	TCP	7680	All ports
Delivery Optimization (UDP-In)	Inbound	Allow	%SystemRoot%\system32\svchost.exe	UDP	7680	All ports
Delivery Optimization (UDP-In)	Inbound	Allow	DoSvc	UDP	7680	All ports

ⓘ Note

There are two rules defined for each rule in the Microsoft Defender Firewall configuration. To restrict the inbound and outbound rules to Windows Services, e.g. DNS Client, both the service name, DNSCache, and the executable path, C:\Windows\System32\svchost.exe, need to be defined as separate rule rather than a single rule that is possible using Group Policy.

You can make additional changes to the management of both inbound and outbound rules as needed for your permitted and blocked services. For more information, see [Firewall configuration service](#).

URL lock proxy

Restrictive URL traffic management includes:

- Deny All outbound traffic except selected Azure and Microsoft services including Azure Cloud Shell and the ability to allows self-service password reset.
- The Privileged profile restricts the endpoints on the internet that the device can connect to using the following URL Lock Proxy configuration.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet  
Settings]  
"ProxyEnable"=dword:00000001  
"ProxyServer"="127.0.0.2:8080"  
"ProxyOverride"="*.azure.com;*.azure.net;*.microsoft.com;*.windowsupdate.com;*  
.microsoftonline.com;*.microsoftonline.cn;*.windows.net;*.windowsazure.com;*.w  
indowsazure.cn;*.azure.cn;*.loganalytics.io;*.applicationinsights.io;*.vsasset  
s.io;*.azure-  
automation.net;*.visualstudio.com,portal.office.com;*.aspnetcdn.com;*.sharepoi  
ntonline.com;*.msecnd.net;*.msocdn.com;*.webtrends.com"  
"AutoDetect"=dword:00000000
```

The endpoints listed in the ProxyOverride list are limited to those endpoints needed to authenticate to Azure AD and access Azure or Office 365 management interfaces. To extend to other cloud services, add their administration URL to the list. This approach is designed to limit access to the wider internet to protect privileged users from internet-based attacks. If this approach is deemed too restrictive, then consider using the approach described below for the privileged role.

Enable Microsoft Cloud Application Security, URLs restricted list to approved URLs (Allow most)

In our roles deployment it is recommended that for Enterprise, and Specialized deployments, where a strict *deny all* web browsing is not desirable, that using the capabilities of a cloud access security broker (CASB) such as [Microsoft Defender for Cloud Apps](#) be utilized to block access to risky, and questionable web sites. The solution addresses a simple way to block applications and websites that have been curated. This solution is similar to getting access to the block list from sites such as the Spamhaus Project who maintains [the Domain Block List \(DBL\)](#): a good resource to use as an advanced set of rules to implement for blocking sites.

The solution will provide you:

- Visibility: detect all cloud services; assign each a risk ranking; identify all users and third-party apps able to log in
- Data security: identify and control sensitive information (DLP); respond to classification labels on content
- Threat protection: offer adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware
- Compliance: supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

Enable Defender for Cloud Apps and connect to Defender ATP to block access the risky URLs:

- In [Microsoft Defender Security Center](#) > Settings > Advanced features, set Microsoft Defender for Cloud Apps integration > **ON**
- In [Microsoft Defender Security Center](#) > Settings > Advanced features, set Custom network indicators > **ON**
- In [Microsoft Defender for Cloud Apps portal](#) > Settings > Microsoft Defender ATP integration > Select **Block unsanctioned apps**

Manage local applications

The secure workstation moves to a truly hardened state when local applications are removed, including productivity applications. Here, you add Visual Studio Code to allow connection to Azure DevOps for GitHub to manage code repositories.

Configuring the Company Portal your for custom apps

An Intune-managed copy of the [Company Portal](#) gives you on-demand access to additional tools that you can push down to users of the secured workstations.

In a secured mode, application installation is restricted to managed applications that are delivered by Company Portal. However, installing the Company Portal requires access to Microsoft Store. In your secured solution, you [add and assign the Windows 10 Company Portal app for Autopilot provisioned devices](#).

 **Note**

Make sure you assign the Company Portal app to the **Secure Workstation Device Tag** group used to assign the Autopilot profile.

Deploy applications using Intune

In some situations, applications like the Microsoft Visual Studio Code are required on the secured workstation. The following example provides instructions to install Microsoft Visual Studio Code to users in the security group **Secure Workstation Users**.

Visual Studio Code is provided as an EXE package so it needs to be packaged as an [.intunewin](#) format file for deployment using Microsoft Endpoint Manager using the [Microsoft Win32 Content Prep Tool](#).

Download the Microsoft Win32 Content Prep Tool locally to a workstation and copy it to a directory for packaging, for example, C:\Packages. Then create a Source and Output directory under C:\Packages.

Package Microsoft Visual Studio Code

1. Download the offline installer [Visual Studio Code for Windows 64-bit](#).
2. Copy the downloaded Visual Studio Code exe file to C:\Packages\Source
3. Open a PowerShell console and navigate to C:\Packages
4. Type .\IntuneWinAppUtil.exe -c C:\Packages\Source\ -s
C:\Packages\Source\VSCodeUserSetup-x64-1.51.1.exe -o
C:\Packages\Output\VSCodeUserSetup-x64-1.51.1
5. Type Y to create the new output folder. The intunewin file for Visual Studio Code will be created in this folder.

Upload VS Code to Microsoft Endpoint Manager

1. In the Microsoft Endpoint Manager admin center, browse to Apps > Windows > Add
2. Under Select app type, choose Windows app (Win32)
3. Click Select app package file, click Select a file, then select the VSCodeUserSetup-x64-1.51.1.intunewin from C:\Packages\Output\VSCodeUserSetup-x64-1.51.1. Click OK
4. Enter Visual Studio Code 1.51.1 in the Name field
5. Enter a description for Visual Studio Code in the Description field
6. Enter Microsoft Corporation in the Publisher Field
7. Download <https://jsarray.com/images/page-icons/visual-studio-code.png> and select image for the logo. Select Next
8. Enter VSCodeSetup-x64-1.51.1.exe /SILENT in the Install command field
9. Enter C:\Program Files\Microsoft VS Code\unins000.exe in the Uninstall command field
10. Select Determine behavior based on return codes from the Device Restart behavior dropdown list. Select Next
11. Select 64-bit from the Operating system architecture checkbox dropdown
12. Select Windows 10 1903 from the Minimum operating system checkbox dropdown. Select Next
13. Select Manually configure detection rules from the Rules format dropdown list
14. Click Add and then select File form the Rule type dropdown
15. Enter C:\Program Files\Microsoft VS Code in the Path field
16. Enter unins000.exe in the File or folder field
17. Select File or folder exists from the dropdown list, Select OK and then select Next

18. Select **Next** as there are no dependencies on this package
19. Select **Add Group** under **Available for enrolled devices**, add **Privileged Users group**.
Click **Select** to confirm group. Select **Next**
20. Click **Create**

Use PowerShell to create custom apps and settings

There are some configuration settings that we recommend, including two Defender for Endpoint recommendations, that must be set using PowerShell. These configuration changes cannot be set via policies in Intune.

You can also use PowerShell to extend host management capabilities. The [PAW-DeviceConfig.ps1](#) script from GitHub is an example script that configures the following settings:

- Removes Internet Explorer
- Removes PowerShell 2.0
- Removes Windows Media Player
- Removes Work Folders Client
- Removes XPS Printing
- Enables and configures Hibernate
- Implements registry fix to enable AppLocker DLL rule processing
- Implements registry settings for two Microsoft Defender for Endpoint recommendations that cannot be set using Endpoint Manager.
 - Require users to elevate when setting a network's location
 - Prevent saving of network credentials
- Disable Network Location Wizard - prevents users from setting network location as Private and therefore increasing the attack surface exposed in Windows Firewall
- Configures Windows Time to use NTP and sets the Auto Time service to Automatic
- Downloads and sets the desktop background to a specific image to easily identify the device as a ready-to-use, privileged workstation.

The [PAW-DeviceConfig.ps1](#) script from GitHub.

1. Download the script [PAW-DeviceConfig.ps1] to a local device.
2. Browse to the **Azure portal > Microsoft Intune > Device configuration > PowerShell scripts > Add**. Provide a Name for the script and specify the Script location.
3. Select **Configure**.
 - a. Set Run this script using the logged on credentials to **No**.
 - b. Select **OK**.
4. Select **Create**.
5. Select **Assignments > Select groups**.

- a. Add the security group **Secure Workstations**.
- b. Select **Save**.

Validate and test your deployment with your first device

This enrollment assumes that you will use a physical computing device. It is recommended that as part of the procurement process that the OEM, Reseller, distributor, or partner [register devices in Windows Autopilot](#).

However for testing it is possible to stand up [Virtual Machines](#) as a test scenario. However note enrollment of personally joined devices will need to be revised to allow this method of joining a client.

This method works for Virtual Machines or physical devices that have not been previously registered.

1. Start the device and wait for the username dialog to be presented
2. Press `SHIFT + F10` to display command prompt
3. Type `PowerShell`, hit Enter
4. Type `Set-ExecutionPolicy RemoteSigned`, hit Enter
5. Type `Install-Script GetWindowsAutopilotInfo`, hit Enter
6. Type `Y` and click Enter to accept PATH environment change
7. Type `Y` and click Enter to install NuGet provider
8. Type `Y` to trust the repository
9. Type Run `Get-WindowsAutoPilotInfo -GroupTag PAW -outputfile C:\device1.csv`
10. Copy the CSV from the Virtual Machine or Physical device

Import devices into Autopilot

1. In the Microsoft Endpoint Manager admin center, go to **Devices > Windows Devices > Windows enrollment > Devices**
2. Select **Import** and choose your CSV file.
3. Wait for the `Group Tag` to be updated to `PAW` and the `Profile Status` to change to `Assigned`.

 **Note**

The Group Tag is used by the Secure Workstation dynamic group to make the device a member of its group,

4. Add the device to the **Secure Workstations** security group.
5. On the Windows 10 device you wish to configure, go to **Windows Settings > Update & Security > Recovery**.
 - a. Choose **Get started** under **Reset this PC**.
 - b. Follow the prompts to reset and reconfigure the device with the profile and compliance policies configured.

After you have configured the device, complete a review and check the configuration. Confirm that the first device is configured correctly before continuing your deployment.

Assign devices

To assign devices and users, you need to map the [selected profiles](#) to your security group. All new users who require permissions to the service must be added to the security group as well.

Using Microsoft Defender for Endpoint to monitor and respond to security incidents

- Continuously observe and monitor vulnerabilities and misconfigurations
- Utilize Microsoft Defender for Endpoint to prioritize dynamic threats in the wild
- Drive correlation of vulnerabilities with endpoint detection and response (EDR) alerts
- Use the dashboard to identify machine-level vulnerability during investigations
- Push out remediations to Intune

Configure your [Microsoft Defender Security Center](#). Using guidance at [Threat & Vulnerability Management dashboard overview](#).

Monitoring application activity using Advanced Threat Hunting

Starting at the Specialized workstation, AppLocker is enabled for monitoring of application activity on a workstation. By default Defender for Endpoint captures AppLocker events and Advanced Hunting Queries can be used to determine what applications, scripts, DLL files are being blocked by AppLocker.

Note

The Specialized and Privileged workstation profiles contain the AppLocker policies.

Deployment of the policies is required for monitoring of application activity on a client.

From the Microsoft Defender Security Center Advanced Hunting pane, use the following query to return AppLocker events

Kusto

```
DeviceEvents  
| where Timestamp > ago(7d) and  
ActionType startswith "AppControl"  
| summarize Machines=dcount(DeviceName) by ActionType  
| order by Machines desc
```

Monitoring

- Understand how to review your [Exposure Score](#)
- Review [Security recommendation](#)
- Manage security [remediations](#)
- Manage [endpoint detection and response](#)
- Monitor profiles with [Intune profile monitoring](#).

Next steps

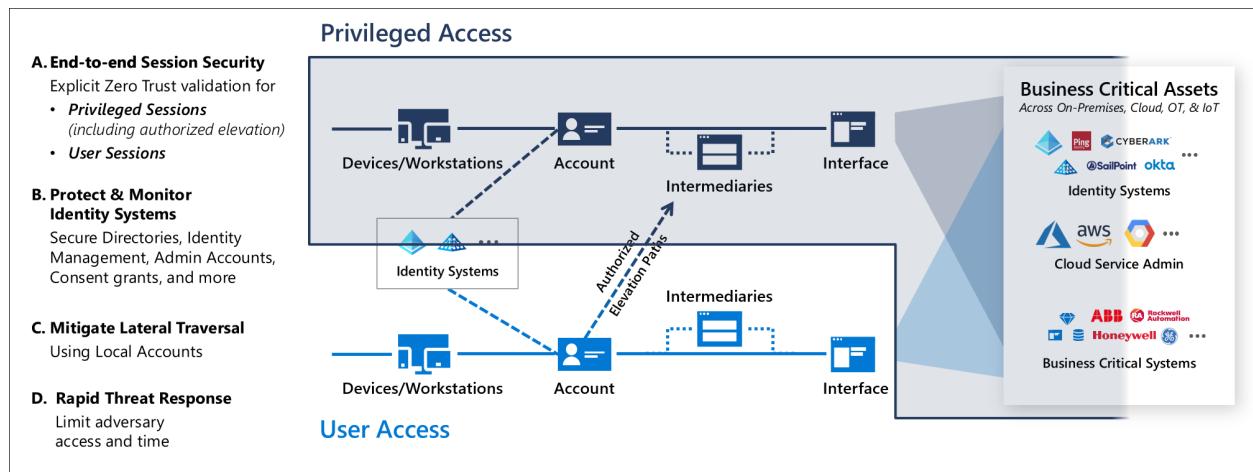
- [Securing privileged access overview](#)
- [Privileged access strategy](#)
- [Measuring success](#)
- [Security levels](#)
- [Privileged access accounts](#)
- [Intermediaries](#)
- [Interfaces](#)
- [Privileged access devices](#)
- [Enterprise access model](#)

Security rapid modernization plan

Article • 09/02/2022 • 13 minutes to read

This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended [privileged access strategy](#).

This roadmap builds on the technical controls established in the [privileged access deployment](#) guidance. Complete those steps and then use the steps in this RAMP to configure the controls for your organization.



ⓘ Note

Many of these steps will have a green/brownfield dynamic as organizations often have security risks in the way they are already deployed or configured accounts. This roadmap prioritizes stopping the accumulation of new security risks first, and then later cleans up the remaining items that have already accumulated.

As you progress through the roadmap, you can utilize Microsoft Secure Score to track and compare many items in the journey with others in similar organizations over time. Learn more about Microsoft Secure Score in the article [Secure score overview](#).

Each item in this RAMP is structured as an initiative that will be tracked and managed using a format that builds on the objectives and key results (OKR) methodology. Each item includes what (objective), why, who, how, and how to measure (key results). Some items require changes to processes and people's knowledge/skills, while others are simpler technology changes. Many of these initiatives will include members outside of the traditional IT Department that should be included in the decision making and implementation of these changes to ensure they are successfully integrated in your organization.

It is critical to work together as an organization, create partnerships, and educate people who traditionally were not part of this process. It is critical to create and maintain buy-in across the organization, without it many projects fail.

Separate and manage privileged accounts

Emergency access accounts

- **What:** Ensure that you are not accidentally locked out of your Azure Active Directory (Azure AD) organization in an emergency situation.
- **Why:** Emergency access accounts rarely used and highly damaging to the organization if compromised, but their availability to the organization is also critically important for the few scenarios when they are required. Ensure you have a plan for continuity of access that accommodates both expected and unexpected events.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
- **How:** Follow the guidance in [Manage emergency access accounts in Azure AD](#).
- **Measure key results:**
 - **Established** Emergency access process has been designed based on Microsoft guidance that meets organizational needs
 - **Maintained** Emergency access has been reviewed and tested within the past 90 days

Enable Azure AD Privileged Identity Management

- **What:** Use Azure AD Privileged Identity Management (PIM) in your Azure AD production environment to discover and secure privileged accounts
- **Why:** Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).

- **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
- **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
- **How:** Deploy and Configure Azure AD Privileged Identity Management using the guidance in the article, [Deploy Azure AD Privileged Identity Management \(PIM\)](#).
- **Measure key results:** 100% of applicable privileged access roles are using Azure AD PIM

Identify and categorize privileged accounts (Azure AD)

- **What:** Identify all roles and groups with high business impact that will require privileged security level (immediately or over time). These administrators will require separate accounts in a later step [Privileged access administration](#).
- **Why:** This step is required to identify and minimize the number of people that require separate accounts and privileged access protection
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
- **How:** After turning on Azure AD Privileged Identity Management, view the users who are in the following Azure AD roles at a minimum based on your organizations risk policies:
 - Global administrator
 - Privileged role administrator
 - Exchange administrator
 - SharePoint administrator

For a complete list of administrator roles, see [Administrator role permissions in Azure Active Directory](#).

- Remove any accounts that are no longer needed in those roles. Then, categorize the remaining accounts that are assigned to admin roles:
- Assigned to administrative users, but also used for non-administrative productivity purposes, like reading and responding to email.
 - Assigned to administrative users and used for administrative purposes only
 - Shared across multiple users
 - For break-glass emergency access scenarios
 - For automated scripts
 - For external users

If you don't have Azure AD Privileged Identity Management in your organization, you can use the PowerShell API. Also start with the Global Administrator role, because a Global Administrator has the same permissions across all cloud services for which your organization has subscribed. These permissions are granted no matter where they were assigned: in the Microsoft 365 admin center, the Azure portal, or by the Azure AD module for Microsoft PowerShell.

- **Measure key results:** Review and Identification of privileged access roles has been completed within the past 90 days

Separate accounts (On-premises AD accounts)

- **What:** Secure on-premises privileged administrative accounts, if not already done. This stage includes:
 - Creating separate admin accounts for users who need to conduct on-premises administrative tasks
 - Deploying Privileged Access Workstations for Active Directory administrators
 - Creating unique local admin passwords for workstations and servers
- **Why:** Hardening the accounts used for administrative tasks. The administrator accounts should have mail disabled and no personal Microsoft accounts should be allowed.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving

- [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
- **How:** All personnel that are authorized to possess administrative privileges must have separate accounts for administrative functions that are distinct from user accounts. **Do not share these accounts between users.**
 - *Standard user accounts* - Granted standard user privileges for standard user tasks, such as email, web browsing, and using line-of-business applications. These accounts are not granted administrative privileges.
 - *Administrative accounts* - Separate accounts created for personnel who are assigned the appropriate administrative privileges.
- **Measure key results:** 100% of on-premises privileged users have separate dedicated accounts

Microsoft Defender for Identity

- **What:** Microsoft Defender for Identity combines on-premises signals with cloud insights to monitor, protect, and investigate events in a simplified format enabling your security teams to detect advanced attacks against your identity infrastructure with the ability to:
 - Monitor users, entity behavior, and activities with learning-based analytics
 - Protect user identities and credentials stored in Active Directory
 - Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
 - Provide clear incident information on a simple timeline for fast triage
- **Why:** Modern attackers may stay undetected for long periods of time. Many threats are hard to find without a cohesive picture of your entire identity environment.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)

- [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
- [Security Compliance management](#) monitors to ensure compliance
- **How:** Deploy and enable [Microsoft Defender for Identity](#) and review any open alerts.
- **Measure key results:** All open alerts reviewed and mitigated by the appropriate teams.

Improve credential management experience

Implement and document self-service password reset and combined security information registration

- **What:** Enable and configure self-service password reset (SSPR) in your organization and enable the combined security information registration experience.
- **Why:** Users are able to reset their own passwords once they have registered. The combined security information registration experience provides a better user experience allowing registration for Azure AD Multi-Factor Authentication and self-service password reset. These tools when used together contribute to lower helpdesk costs and more satisfied users.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
 - [Central IT Operations](#) Helpdesk processes have been updated and personnel has been trained on them
- **How:** To enable and deploy SSPR, see the article [Plan an Azure Active Directory self-service password reset deployment](#).
- **Measure key results:** Self-service password reset is fully configured and available to the organization

Protect admin accounts - Enable and require MFA / Passwordless for Azure AD privileged users

- **What:** Require all privileged accounts in Azure AD to use strong multi-factor authentication
- **Why:** To protect access to data and services in Microsoft 365.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
 - [Central IT Operations](#) Helpdesk processes have been updated and personnel has been trained on them
 - [Central IT Operations](#) Service owner processes have been updated and personnel has been trained on them
- **How:** Turn on Azure AD Multi-Factor Authentication (MFA) and register all other highly privileged single-user non-federated admin accounts. Require multi-factor authentication at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles like:
 - Global administrator
 - Privileged Role administrator
 - Exchange administrator
 - SharePoint administrator

Require administrators to use passwordless sign-in methods such as FIDO2 security keys or Windows Hello for Business in conjunction with unique, long, complex passwords. Enforce this change with an organizational policy document.

Follow the guidance in the following articles, [Plan an Azure AD Multi-Factor Authentication deployment](#) and [Plan a passwordless authentication deployment in Azure Active Directory](#).

- **Measure key results:** 100% of privileged users are using passwordless authentication or a strong form of multi-factor authentication for all logons. See [Privileged Access Accounts](#) for description of multi-factor authentication

Block legacy authentication protocols for privileged user accounts

- **What:** Block legacy authentication protocol use for privileged user accounts.
- **Why:** Organizations should block these legacy authentication protocols because multi-factor authentication cannot be enforced against them. Leaving legacy authentication protocols enabled can create an entry point for attackers. Some legacy applications may rely on these protocols and organizations have the option to create specific exceptions for certain accounts. These exceptions should be tracked and additional monitoring controls implemented.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - **Policy and standards:** establish clear requirements
 - [Identity and Key Management](#) or Central IT Operations [Central IT Operations](#) to implement the policy
 - [Security Compliance management](#) monitors to ensure compliance
- **How:** To block legacy authentication protocols in your organization, follow the guidance in the article [How to: Block legacy authentication to Azure AD with Conditional Access](#).
- **Measure key results:**
 - **Legacy protocols blocked:** All legacy protocols are blocked for all users, with only authorized exceptions
 - **Exceptions** are reviewed every 90 days and expire permanently within one year. Application owners must fix all exceptions within one year of first exception approval

Application consent process

- **What:** Disable end-user consent to Azure AD applications.

Note

This change will require centralizing the decision-making process with your organization's security and identity administration teams.

- **Why:** Users can inadvertently create organizational risk by providing consent for an app that can maliciously access organizational data.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
 - [Central IT Operations](#) Helpdesk processes have been updated and personnel has been trained on them
 - [Central IT Operations](#) Service owner processes have been updated and personnel has been trained on them
- **How:** Establish a centralized consent process to maintain centralized visibility and control of the applications that have access to data by following the guidance in the article, [Managing consent to applications and evaluating consent requests](#).
- **Measure key results:** End users are not able to consent to Azure AD application access

Clean up account and sign-in risks

- **What:** Enable Azure AD Identity Protection and cleanup any risks that it finds.
- **Why:** Risky user and sign-in behavior can be a source of attacks against your organization.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
 - [Central IT Operations](#) Helpdesk processes have been updated for related support calls and personnel has been trained on them

- **How:** Create a process that monitors and manages user and sign-in risk. Decide if you will automate remediation, using Azure AD Multi-Factor Authentication and SSPR, or block and require administrator intervention. Follow the guidance in the article [How To: Configure and enable risk policies](#).
- **Measure key results:** The organization has zero unaddressed user and sign-in risks.

 Note

Conditional Access policies are required to block accrual of new sign-in risks. See the Conditional access section of [Privileged Access Deployment](#)

Admin workstations initial deployment

- **What:** Privileged accounts such as Global Administrators have dedicated workstations to perform administrative tasks from.
- **Why:** Devices where privileged administration tasks are completed are a target of attackers. Securing not only the account but these assets are critical in reducing your attack surface area. This separation limits their exposure to common attacks directed at productivity-related tasks like email and web browsing.
- **Who:** This initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).
 - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
 - **Execution:** This initiative is a collaborative effort involving
 - [Policy and standards](#) team document clear requirements and standards (based on this guidance)
 - [Identity and Key Management](#) or [Central IT Operations](#) to implement any changes
 - [Security Compliance management](#) monitors to ensure compliance
 - [Central IT Operations](#) Helpdesk processes have been updated and personnel has been trained on them
 - [Central IT Operations](#) Service owner processes have been updated and personnel has been trained on them
- **How:** Initial deployment should be to the Enterprise level as described in the article [Privileged Access Deployment](#)
- **Measure key results:** Every privileged account has a dedicated workstation to perform sensitive tasks from.

 Note

This step rapidly establishes a security baseline and must be increased to specialized and privileged levels as soon as possible.

Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

Enhanced Security Admin Environment

Article • 09/02/2022 • 3 minutes to read

The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.

Microsoft's recommendation to use this architectural pattern has been replaced by the modern [privileged access strategy](#) and [rapid modernization plan \(RAMP\)](#) guidance as the default recommended approach for securing privileged users. The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.

What if I already have ESAE?

For customers that have already deployed this architecture to enhance security and/or simplify multi-forest management, there is no urgency to retire or replace an ESAE implementation if it's being operated as designed and intended. As with any enterprise systems, you should maintain the software in it by applying security updates and ensuring software is within [support lifecycle](#).

Microsoft also recommends organizations with ESAE / hardened forests adopt the modern [privileged access strategy](#) using the [rapid modernization plan \(RAMP\)](#) guidance. This complements an existing ESAE implementation and provides appropriate security for roles not already protected by ESAE including Azure AD Global Administrators, sensitive business users, and standard enterprise users. For more information, see the article [Securing privileged access security levels](#).

Why change the recommendation?

When ESAE was originally designed 10 years ago, the focus was on on-premise environments with AD as the local identity provider. ESAE / hardened forest implementations focus on protecting Windows Server Active Directory administrators.

Microsoft recommends the new cloud-based solutions because they can be deployed more quickly to protect a broader scope of administrative and business-sensitive roles and systems.

The [privileged access strategy](#) provides protections and monitoring for a much larger set of sensitive users, while providing incremental lower-cost steps to rapidly build

security assurances.

While still valid for specific use cases, ESAE hardened forest implementations are more costly and more difficult to use, requiring more operational support compared to the newer cloud-based solution (due to the complex nature of that architecture). ESAE implementations are designed to protect only Windows Server Active Directory administrators. The cloud based [privileged access strategy](#) provides protections and monitoring for a much larger set of sensitive users, while providing incremental lower-cost steps to rapidly build security assurances.

What are the valid ESAE use cases?

While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.

In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent operational rigor to the usage and maintenance of the ESAE implementation.

Example scenarios include:

- **Isolated on-premises environments** - where cloud services are unavailable such as offline research laboratories, critical infrastructure or utilities, disconnected operational technology (OT) environments such as Supervisory control and data acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.
- **Highly regulated environments** – industry or government regulation may specifically require an administrative forest configuration.
- **High level security assurance is mandated** - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.

Note

While Microsoft no longer recommends an isolated hardened forest model for most scenarios at most organizations, Microsoft still operates a similar architecture internally (and associated support processes and personnel) because of the extreme security requirements for providing trusted cloud services to organizations around the globe.

Next steps

Review the [privileged access strategy](#) and [rapid modernization plan \(RAMP\)](#) guidance for providing secure environments for privileged users.

Microsoft Security Best Practices module: Privileged administration

Article • 06/08/2022 • 2 minutes to read

Administrative accounts with privileged access to the environment (and associated elements like groups and workstations) must be protected at the highest levels of security assurances to ensure all other security assurances aren't undermined.

See the [Administration](#) topic for more information.

The following videos provide guidance on administration. You can also download the [PowerPoint slides]/microsoft-365/downloads/security-compass-presentation.pptx) associated with these videos.

Part 1: Introduction (05:40)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qbw1?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qbw1?postJs||Msg=true)

Part 2: Admin Quantity (03:14)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qU?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qU?postJs||Msg=true)

Part 3: Managed and Separate Admin Accounts (03:38)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qV?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qV?postJs||Msg=true)

Part 4: Emergency Access (02:28)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qgYn?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qgYn?postJs||Msg=true)

Part 5: Containing Attack Pivot Risk (02:42)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Ap?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Ap?postJs||Msg=true)

Part 6: Admin Account Protection (05:25)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhh?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhh?postJs||Msg=true)

Part 7: Admin Workstation Security (04:09)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9rP?postJsIMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9rP?postJsIMsg=true)

Part 8: Enforcing Access Security (03:13)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qdUw?postJsIMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qdUw?postJsIMsg=true)

Part 9: Simplify Permissions (03:31)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhj?postJsIMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhj?postJsIMsg=true)

Part 10: Admin Account Lifecycle (02:53)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qlSH?postJsIMsg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qlSH?postJsIMsg=true)

Next steps

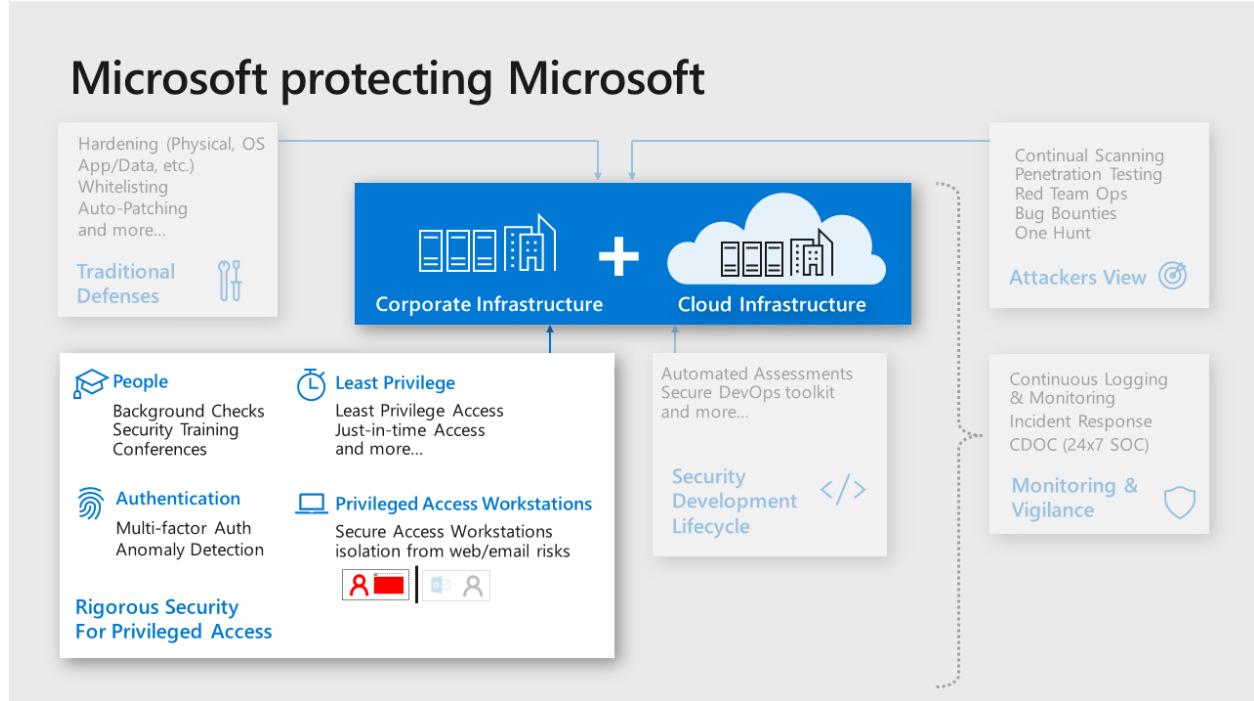
For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Administration

Article • 02/02/2022 • 9 minutes to read

Administration is the practice of monitoring, maintaining, and operating Information Technology (IT) systems to meet service levels that the business requires. Administration introduces some of the highest impact security risks because performing these tasks requires privileged access to a very broad set of these systems and applications. Attackers know that gaining access to an account with administrative privileges can get them access to most or all of the data they would target, making the security of administration one of the most critical security areas.

As an example, Microsoft makes significant investments in protection and training of administrators for our cloud systems and IT systems:



Microsoft's recommended core strategy for administrative privileges is to use the available controls to reduce risk

Reduce risk exposure (scope and time) – The principle of least privilege is best accomplished with modern controls that provide privileges on demand. This help to limit risk by limiting administrative privileges exposure by:

- **Scope – Just Enough Access (JEA)** provides only the required privileges for the administrative operation required (vs. having direct and immediate privileges to many or all systems at a time, which is almost never required).
- **Time – Just in Time (JIT)** approaches provided the required privileged as they are needed.

- **Mitigate the remaining risks** – Use a combination of preventive and detective controls to reduce risks such as isolating administrator accounts from the most common risks phishing and general web browsing, simplifying and optimizing their workflow, increasing assurance of authentication decisions, and identifying anomalies from normal baseline behavior that can be blocked or investigated.

Microsoft has captured and documented best practices for protecting administrative accounts and published prioritized roadmaps for protecting privileged access that can be used as references for prioritizing mitigations for accounts with privileged access.

- [Securing Privileged Access \(SPA\) roadmap for administrators of on premises Active Directory ↗](#)
- [Guidance for securing administrators of Azure Active Directory ↗](#)

Minimize number of critical impact admins

Grant the fewest number of accounts to privileges that can have a critical business impact

Each admin account represents potential attack surface that an attacker can target, so minimizing the number of accounts with that privilege helps limit the overall organizational risk. Experience has taught us that membership of these privileged groups grows naturally over time as people change roles if membership not actively limited and managed.

We recommend an approach that reduces this attack surface risk while ensuring business continuity in case something happens to an administrator:

- Assign at least two accounts to the privileged group for business continuity
- When two or more accounts are required, provide justification for each member including the original two
- Regularly review membership & justification for each group member

Managed accounts for admins

Ensure all critical impact admins are managed by enterprise directory to follow organizational policy enforcement.

Consumer accounts such as Microsoft accounts like @Hotmail.com, @live.com, @outlook.com, don't offer sufficient security visibility and control to ensure the

organization's policies and any regulatory requirements are being followed. Because Azure deployments often start small and informally before growing into enterprise-managed tenants, some consumer accounts remain as administrative accounts long afterward for example, original Azure project managers, creating blind spots, and potential risks.

Separate accounts for admins

Ensure all critical impact admins have a separate account for administrative tasks (vs the account they use for email, web browsing, and other productivity tasks).

Phishing and web browser attacks represent the most common attack vectors to compromise accounts, including administrative accounts.

Create a separate administrative account for all users that have a role requiring critical privileges. For these administrative accounts, block productivity tools like Office 365 email (remove license). If possible, block arbitrary web browsing (with proxy and/or application controls) while allowing exceptions for browsing to the Azure portal and other sites required for administrative tasks.

No standing access / Just in Time privileges

Avoid providing permanent "standing" access for any critical impact accounts

Permanent privileges increase business risk by increasing the time an attacker can use the account to do damage. Temporary privileges force attackers targeting an account to either work within the limited times the admin is already using the account or to initiate privilege elevation (which increases their chance of being detected and removed from the environment).

Grant privileges required only as required using one of these methods:

- **Just in Time** - Enable Azure AD Privileged Identity Management (PIM) or a third party solution to require following an approval workflow to obtain privileges for critical impact accounts
- **Break glass** – For rarely used accounts, follow an emergency access process to gain access to the accounts. This is preferred for privileges that have little need for regular operational usage like members of global admin accounts.

Emergency access or 'Break Glass' accounts

Ensure you have a mechanism for obtaining administrative access in case of an emergency

While rare, sometimes extreme circumstances arise where all normal means of administrative access are unavailable.

We recommend following the instructions at [Managing emergency access administrative accounts in Azure AD](#) and ensure that security operations monitor these accounts carefully.

Admin workstation security

Ensure critical impact admins use a workstation with elevated security protections and monitoring

Attack vectors that use browsing and email like phishing are cheap and common. Isolating critical impact admins from these risks will significantly lower your risk of a major incident where one of these accounts is compromised and used to materially damage your business or mission.

Choose level of admin workstation security based on the options available at <https://aka.ms/securedworkstation>

- **Highly Secure Productivity Device (Enhanced Security Workstation or Specialized Workstation)**

You can start this security journey for critical impact admins by providing them with a higher security workstation that still allows for general browsing and productivity tasks. Using this as an interim step helps ease the transition to fully isolated workstations for both the critical impact admins as well as the IT staff supporting these users and their workstations.

- **Privileged Access Workstation (Specialized Workstation or Secured Workstation)**

These configurations represent the ideal security state for critical impact admins as they heavily restrict access to phishing, browser, and productivity application attack vectors. These workstations don't allow general internet browsing, only allow browser access to Azure portal and other administrative sites.

Critical impact admin dependencies – Account/Workstation

Carefully choose the on-premises security dependencies for critical impact accounts and their workstations

To contain the risk from a major incident on-premises spilling over to become a major compromise of cloud assets, you must eliminate or minimize the means of control that on premises resources have to critical impact accounts in the cloud. As an example, attackers who compromise the on premises Active Directory can access and compromise cloud-based assets that rely on those accounts like resources in Azure, Amazon Web Services (AWS), ServiceNow, and so on. Attackers can also use workstations joined to those on premises domains to gain access to accounts and services managed from them.

Choose the level of isolation from on premises means of control also known as security dependencies for critical impact accounts

- **User Accounts** – Choose where to host the critical impact accounts
 - Native Azure AD Accounts - *Create Native Azure AD Accounts that are not synchronized with on-premises active directory
 - Synchronize from on-premises Active Directory (Not Recommended see [No on-premises admin accounts in cloud identity providers](#) - Leverage existing accounts hosted in the on premises active directory.
- **Workstations** – Choose how you will manage and secure the workstations used by critical admin accounts:
 - Native Cloud Management & Security (Recommended) - Join workstations to Azure AD & Manage/Patch them with Intune or other cloud services. Protect and Monitor with Windows Microsoft Defender ATP or another cloud service not managed by on premises based accounts.
 - Manage with Existing Systems - Join existing AD domain & leverage existing management/security.

This is related to the [No on-premises admin accounts in cloud identity providers](#) to cloud identity providers guidance in the administration section that mitigates the inverse risk of pivoting from cloud assets to on-premises assets

Passwordless Or multi-factor authentication for admins

Require all critical impact admins to use passwordless authentication or multi-factor authentication (MFA).

Attack methods have evolved to the point where passwords alone cannot reliably protect an account. This is well documented in a [Microsoft Ignite Session ↗](#).

Administrative accounts and all critical accounts should use one of the following methods of authentication. These capabilities are listed in preference order by highest cost/difficulty to attack (strongest/preferred options) to lowest cost/difficult to attack:

- **Passwordless (such as Windows Hello)**
[https://aka.ms/HelloForBusiness ↗](https://aka.ms/HelloForBusiness)
- **Passwordless (Authenticator App)**
</azure/active-directory/authentication/howto-authentication-phone-sign-in>
- **Multifactor Authentication**
</azure/active-directory/authentication/howto-mfa-userstates>

Note that SMS Text Message based MFA has become very inexpensive for attackers to bypass, so we recommend you avoid relying on it. This option is still stronger than passwords alone, but is much weaker than other MFA options

Enforce conditional access for admins - Zero Trust

Authentication for all admins and other critical impact accounts should include measurement and enforcement of key security attributes to support a Zero Trust strategy.

Attackers compromising Azure Admin accounts can cause significant harm. Conditional Access can significantly reduce that risk by enforcing security hygiene before allowing access to Azure management.

Configure [Conditional Access policy for Azure management](#) that meets your organization's risk appetite and operational needs.

- Require Multifactor Authentication and/or connection from designated work network
- Require Device **integrity** with Microsoft Defender ATP (Strong Assurance)

Avoid granular and custom permissions

Avoid permissions that specifically reference individual resources or users

Specific permissions create unneeded complexity and confusion as they don't carry the intention to new similar resources. This then accumulates into a complex legacy configuration that is difficult to maintain or change without fear of "breaking something" – negatively impacting both security and solution agility.

Instead of assigning specific resource-specific permissions, use either

- Management Groups for enterprise-wide permissions
- Resource groups for permissions within subscriptions

Instead of granting permissions to specific users, assign access to groups in Azure AD. If there isn't an appropriate group, work with the identity team to create one. This allows you to add and remove group members externally to Azure and ensure permissions are current, while also allowing the group to be used for other purposes such as mailing lists.

Use built-in roles

Use built-in roles for assigning permissions where possible.

Customization leads to complexity that increases confusion and makes automation more complex, challenging, and fragile. These factors all negatively impact security

We recommend that you evaluate the [built-in roles](#) designed to cover most normal scenarios. [Custom roles](#) are a powerful and sometimes useful capability, but they should be reserved for cases when built in roles won't work.

Establish lifecycle management for critical impact accounts

Ensure you have a process for disabling or deleting administrative accounts when admin personnel leave the organization (or leave administrative positions)

See [Manage user and guest user access with access reviews](#) for more details.

Attack simulation for critical impact accounts

Regularly simulate attacks against administrative users with current attack techniques to educate and empower them.

People are a critical part of your defense, especially your personnel with access to critical impact accounts. Ensuring these users (and ideally all users) have the knowledge and skills to avoid and resist attacks will reduce your overall organizational risk.

You can use [Office 365 Attack Simulation](#) capabilities or any number of third party offerings.

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

What is ransomware

Article • 10/26/2022 • 3 minutes to read

Ransomware is a type of cyber security attack that destroys or encrypts files and folders, preventing the owner of the effected device from accessing their data. The cybercriminal can then extort money from the business owner in exchange for a key to unlock the encrypted data. But, even when paid, cybercriminals may not provide the key to return access to the business owner.

Important

Need to start right now? See [Protect your organization against ransomware and extortion](#) to quickly configure your IT infrastructure for the best ransomware protection.

Automated ransomware attacks

Commodity ransomware attacks are usually automated. These cyber attacks can spread like a virus, infect devices through methods like email phishing and malware delivery, and require malware remediation. That means one ransomware prevention technique is to safeguard your mail with a system like *Microsoft Defender for Office 365*, or *Microsoft 365 Defender*, to detect malware and phishing attempts early.

Human-operated ransomware attacks

Human-operated ransomware is the result of an **active attack** by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.

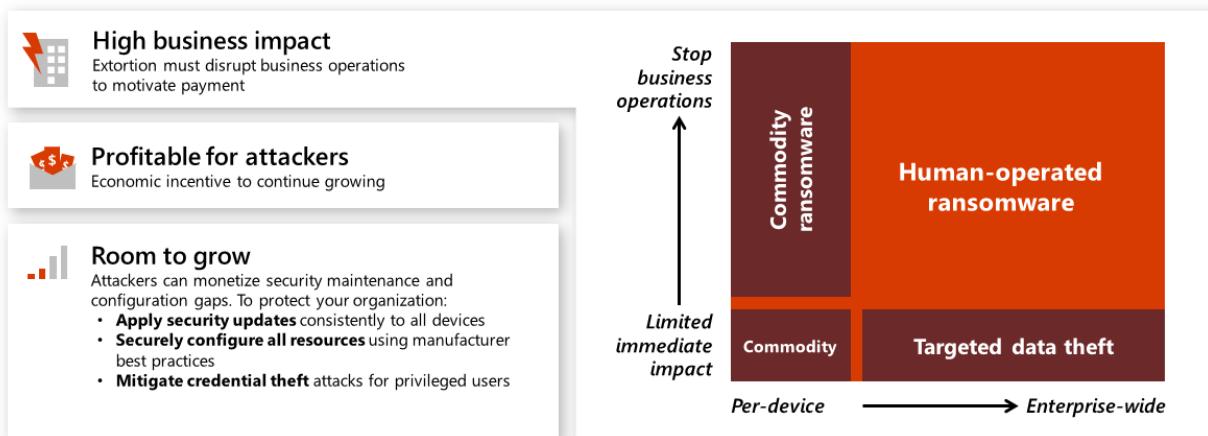
These "hands-on-keyboard" attacks target an organization rather than a single device. *Human-operated* means there is a human attacker using their insights into common system and security misconfigurations to infiltrate the organization, navigate the network, and adapt to the environment and its weaknesses as they go.

Hallmarks of these human-operated ransomware attacks typically include **credential theft** and **lateral movement** with a elevation of the privileges in stolen accounts. Activities might take place during maintenance windows and involve security configuration gaps discovered by cybercriminals. The goal is the **deployment of a ransomware payload** to whatever *high business impact resources* the attackers choose.

ⓘ Important

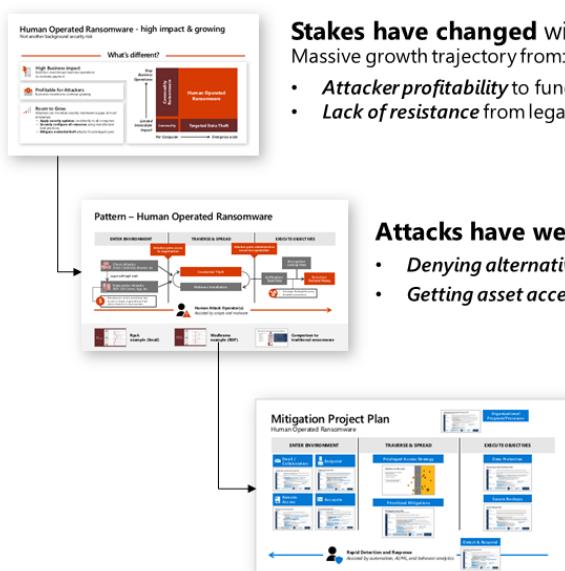
These attacks can be catastrophic to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike commodity ransomware that usually only requires malware remediation, human-operated ransomware will continue to threaten your business operations after the initial encounter.

The graphic below shows how this extortion-based attack is growing in impact and likelihood.



Ransomware protection for your organization

For a comprehensive view of ransomware and extortion and how to protect your organization, use the information in the [Human-Operated Ransomware Mitigation Project Plan](#) PowerPoint presentation. But here's a summary of the guidance:



Stakes have changed with No End in Sight

Massive growth trajectory from:

- Attacker profitability to fund and incent future attacks.
- Lack of resistance from legal, technical, or security obstacles.

Attacks have weaknesses – Successful extortion relies on:

- Denying alternatives to payments – They must prevent you from restoring from backups.
- Getting asset access – Rapid lateral traversal across the enterprise (e.g. IT admin privileges).

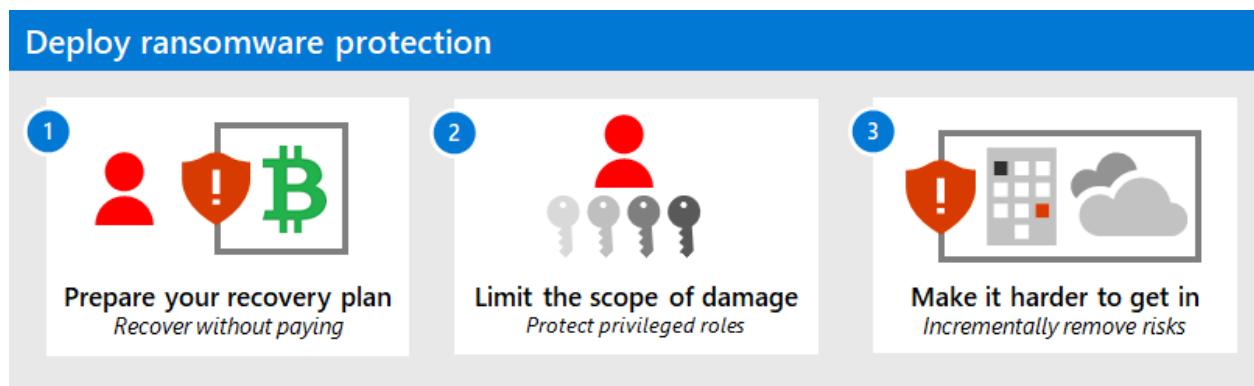
Focus on attack weaknesses first:

- Restore critical business operations – Ensure ability to rapidly restore backups and business processes.
- Protect admins – Strengthen privileged access security.
- Entry points - Prioritize fastest and most effective mitigation of entry points (continually increase attacker cost/friction).

- The stakes of ransomware and extortion-based attacks are high.
- However, the attacks have weaknesses that can reduce your likelihood of being attacked.
- There are three phases to configuring your infrastructure to exploit attack weaknesses.

For the three phases to exploit attack weaknesses, see the [Protect your organization against ransomware and extortion](#) solution to quickly configure your IT infrastructure for the best protection:

1. Prepare your organization to recover from an attack without having to pay the ransom.
2. Limit the scope of damage of a ransomware attack by protecting privileged roles.
3. Make it harder for an attacker to get into your environment by incrementally removing risks.



Download the [Protect your organization from ransomware poster](#) for an overview of the three phases as layers of protection against ransomware attackers.

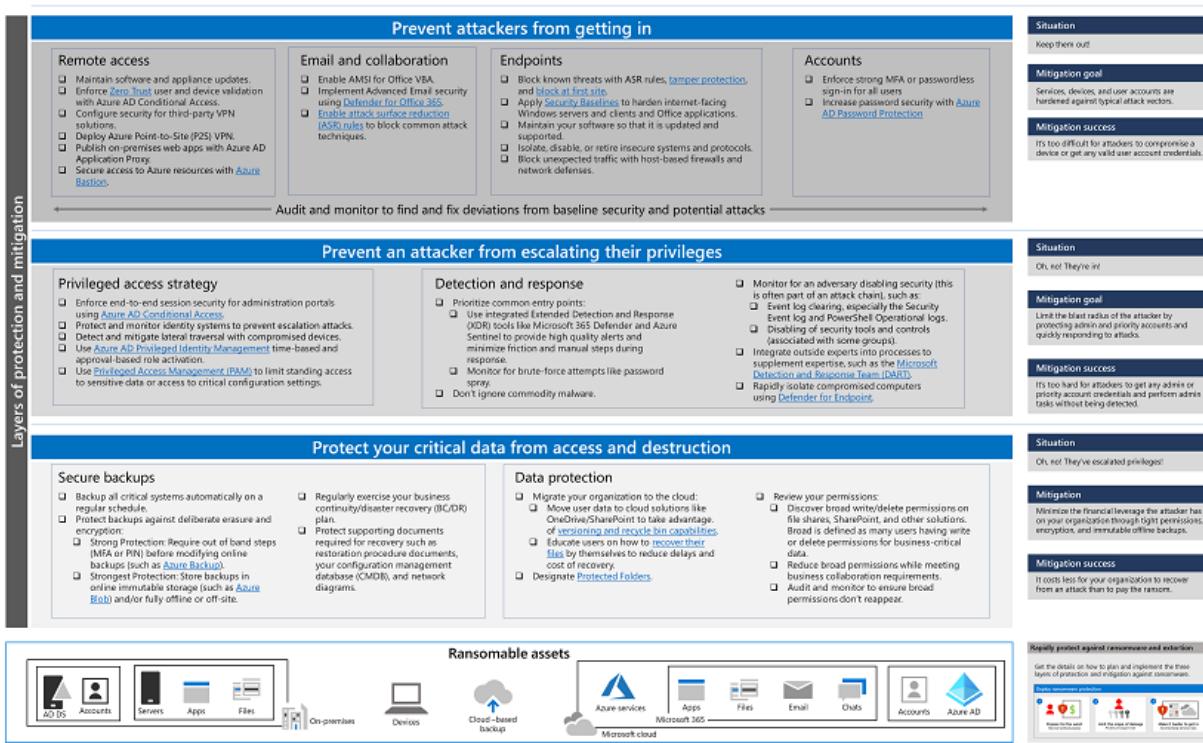


Protect your organization from ransomware

Use this poster as a checklist to deploy features and services for layers of protection and mitigation against ransomware attacks.



Layers of Microsoft cloud security features and other products protect your critical assets from ransomware attackers.



For additional guidance, visit [aka.ms/ransomware](#)

Date of last update: August 2021 | © 2021 Microsoft Corporation. All rights reserved.



Additional ransomware resources

Key information from Microsoft:

- The growing threat of ransomware [↗](#), Microsoft On the Issues blog post on July 20, 2021
- Rapidly protect against ransomware and extortion
- 2021 Microsoft Digital Defense Report [↗](#) (see pages 10-19)
- Ransomware: A pervasive and ongoing threat [↗](#) threat analytics report in the Microsoft 365 Defender portal
- Microsoft's Detection and Response Team (DART) ransomware [approach and best practices](#) and [case study](#)

Microsoft 365:

- Deploy ransomware protection for your Microsoft 365 tenant
- Maximize Ransomware Resiliency with Azure and Microsoft 365 [↗](#)
- Recover from a ransomware attack
- Malware and ransomware protection
- Protect your Windows 10 PC from ransomware [↗](#)

- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware [↗](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- Find ransomware with advanced hunting

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Azure:

- Azure Defenses for Ransomware Attack [↗](#)
- Maximize Ransomware Resiliency with Azure and Microsoft 365 [↗](#)
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup [↗](#) (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel [↗](#)

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021) [↗](#)
- A guide to combatting human-operated ransomware: Part 1 (September 2021) [↗](#)

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021) [↗](#)

Recommendations and best practices.

- Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats (May 2021) [↗](#)

See the **Ransomware** section.

- Human-operated ransomware attacks: A preventable disaster (March 2020) [↗](#)

Includes attack chain analyses of actual attacks.

- Ransomware response—to pay or not to pay? (December 2019) [↗](#)

- Norsk Hydro responds to ransomware attack with transparency (December 2019) [↗](#)

Quickly deploy ransomware preventions

Article • 10/26/2022 • 5 minutes to read

ⓘ Note

This guidance will be updated as new information becomes available.

Providing ransomware protection and mitigating extortion attacks is a priority for organizations large and small because of the high impact of these attacks and rising likelihood an organization will experience one.

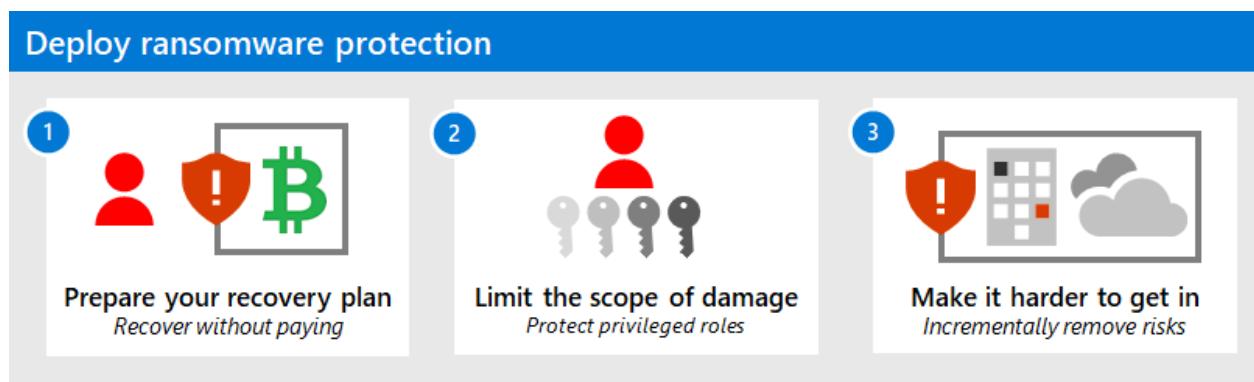
ⓘ Note

If you need a ransomware definition, read the the overview [here](#).

Set up ransomware protection now

Concrete instructions on how to best prepare your organization from many forms of ransomware and extortion.

This guidance is organized in prioritized phases. Each phase links to a separate article. The priority order is designed to ensure you reduce risk *as fast as possible with each phase*, building on an assumption of great urgency that will override normal security and IT priorities, in order to avoid or mitigate these devastating attacks.



It is vital to note that this guidance is structured as prioritized phases that you should follow in the prescribed order. To best adapt this guidance to your situation:

1. Stick with the recommended priorities

Use the phases as a starting plan for what to do first, next, and later so you get the most impactful elements first. These recommendations have been prioritized using the [Zero Trust](#) principle of *assuming a breach*. This forces you to focus on minimizing business risk by assuming the attackers can successfully gain access to your environment through one or more methods.

2. Be proactive and flexible (but *don't skip important tasks*)

Scan through the implementation checklists for all sections of all three phases to see if there are any areas and tasks that you can quickly *complete earlier* (e.g. already have access to a cloud service that hasn't been utilized but could be quickly and easily configured). As you look over the whole plan, be very careful that *these later areas and tasks don't delay completion* of critically important areas like backups and privileged access!

3. Do some items in parallel

Trying to do everything at once can be overwhelming, but some items can naturally be done in parallel. Staff on different teams can be working on tasks at the same time (e.g. backup team, endpoint team, identity team), while also driving for completion of the phases in priority order.

The items in the implementation checklists are in the recommended order of prioritization, not a technical dependency order. Use the checklists to confirm and modify your existing configuration as needed and in a way that works within your organization. For example, in the most important backup element, you backup some systems, but they may not be offline/immutable, or you may not test the full enterprise restore procedures, or you may not have backups of critical business systems or critical IT systems like Active Directory Domain Services (AD DS) domain controllers.

ⓘ Note

See the [3 steps to prevent and recover from ransomware \(September 2021\)](#) Microsoft security blog post for an additional summary of this process.

Phase 1. Prepare your recovery plan

This phase is designed to [minimize the monetary incentive from ransomware attackers](#) by making it:

- Much harder to access and disrupt systems or encrypt or damage key organization data.

- Easier for your organization to recover from an attack without paying the ransom.

Note

While restoring many or all enterprise systems is a difficult endeavor, the alternative of paying an attacker for a recovery key they may or may not deliver, and using tools written by the attackers to try to recover systems and data.

Phase 2. Limit the scope of damage

Make the attackers work a lot harder to [gain access to multiple business critical systems through privileged access roles](#). Limiting the attacker's ability to get privileged access makes it much harder to profit off of an attack on your organization, making it more likely they will give up and go elsewhere.

Phase 3. Make it hard to get in

This last set of tasks is important to raise friction for entry but will take time to complete as part of a larger security journey. The goal of this phase is to make the attackers' work *much* harder as they try to [obtain access to your on-premises or cloud infrastructures](#) at the various common points of entry. There are a lot of these tasks, so it's important to prioritize your work here based on how fast you can accomplish these with your current resources.

While many of these will be familiar and easy to quickly accomplish, it's critically important that ***your work on phase 3 should not slow down your progress on phases 1 and 2!***

Ransomware protection at a glance

You can also see an overview of the phases and their implementation checklists as levels of protection against ransomware attackers with the [Protect your organization from ransomware poster ↗](#).



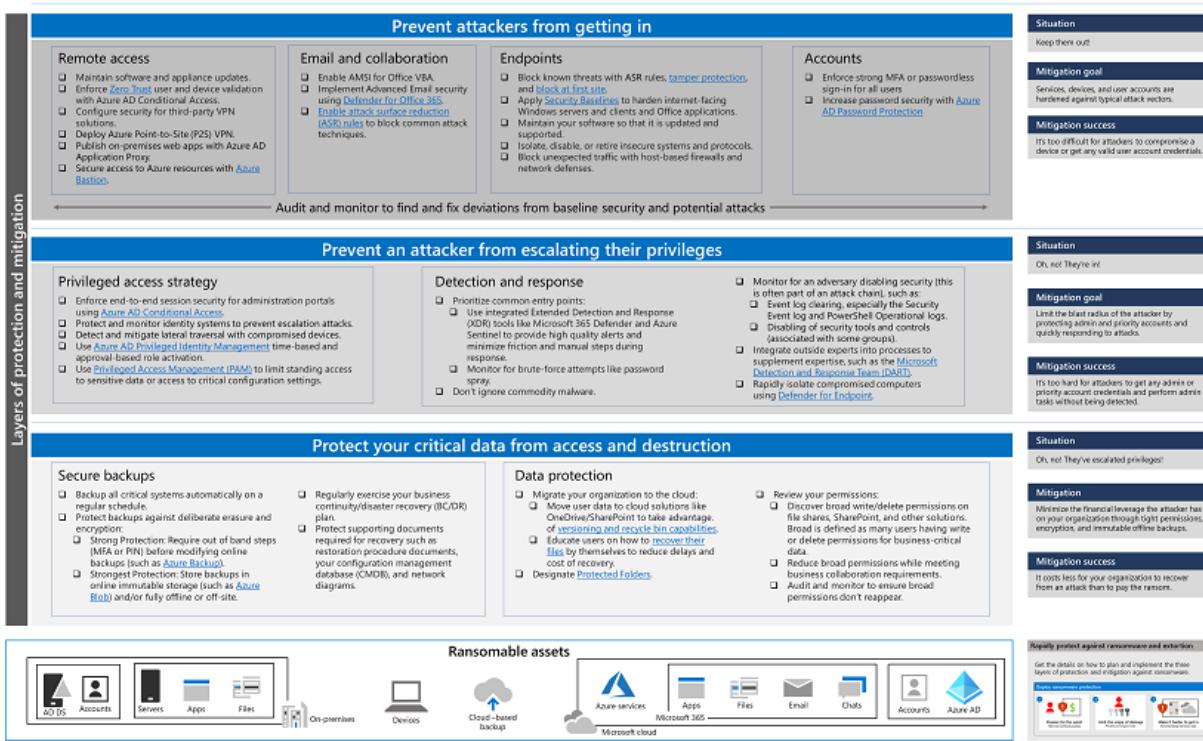
Protect your organization from ransomware

Layers of Microsoft cloud security features and other products protect your critical assets from ransomware attackers.

Use this poster as a checklist to deploy features and services for layers of protection and mitigation against ransomware attacks.



Ransomware attackers



For additional guidance, visit [aka.ms/umconserv](#)

Date of last update: August 2021 | © 2021 Microsoft Corporation. All rights reserved.



Next step

Deploy ransomware protection

1



Prepare your recovery plan
Recover without paying

2



Limit the scope of damage
Protect privileged roles

3



Make it harder to get in
Incrementally remove risks

Start with **Phase 1** to prepare your organization to recover from an attack without having to pay the ransom.

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021

- Human-operated ransomware
- 2021 Microsoft Digital Defense Report [\(see pages 10-19\)](#)
- Ransomware: A pervasive and ongoing threat [threat analytics report in the Microsoft 365 Defender portal](#)
- Microsoft's Detection and Response Team (DART) ransomware [approach](#) and [case study](#)

Microsoft 365:

- Deploy ransomware protection for your Microsoft 365 tenant
- Maximize Ransomware Resiliency with Azure and Microsoft 365 [↗](#)
- Recover from a ransomware attack
- Malware and ransomware protection
- Protect your Windows 10 PC from ransomware [↗](#)
- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware [↗](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- Find ransomware with advanced hunting

Microsoft Azure:

- Azure Defenses for Ransomware Attack [↗](#)
- Maximize Ransomware Resiliency with Azure and Microsoft 365 [↗](#)
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup [↗](#) (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel [↗](#)

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021) [↗](#)
- A guide to combatting human-operated ransomware: Part 1 (September 2021) [↗](#)

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021) [↗](#)

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#) ↗

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#) ↗

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#) ↗
- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#) ↗

Phase 1: Prepare your recovery plan

Article • 10/26/2022 • 7 minutes to read

The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom. While attackers in control of your organization have a variety of ways to pressure you into paying, the demands primarily focus on two categories:

- **Pay to regain access**

Attackers demand payment under the threat that they won't give you back access to your systems and data. This is most frequently done by encrypting your systems and data and demanding payment for the decryption key.

Important

Paying the ransom isn't as simple and clean of a solution as it may seem. Because you're dealing with criminals that are only motivated by payment (and often relatively amateur operators who are using a toolkit provided by someone else), there is a lot of uncertainty around how well paying the ransom will actually work. There is no legal guarantee that they will provide a key that decrypts 100% of your systems and data, or even provide a key at all. The process to decrypt these systems uses homegrown attacker tools, which is often a clumsy and manual process.

- **Pay to avoid disclosure**

Attackers demand payment in exchange for not releasing sensitive or embarrassing data to the dark web (other criminals) or the general public.

To avoid being forced into payment (the profitable situation for attackers), the most immediate and effective action you can take is to ensure your organization can restore your entire enterprise from immutable storage, which neither the attacker nor you can modify.

Identifying the most sensitive assets and protecting them at a higher level of assurance is also critically important but is a longer and more challenging process to execute. We don't want you to hold up other areas in phases 1 or 2, but we recommend you get the process started by bringing together business, IT, and security stakeholders to ask and answer questions like:

- What business assets would be the most damaging if compromised? For example, what assets would our business leadership be willing to pay an extortion demand if attackers controlled them?
- How do these business assets translate to IT assets (such as files, applications, databases, servers, and control systems)?
- How can we protect or isolate these assets so that attackers with access to the general IT environment can't access them?

Secure backups

You must ensure that critical systems and their data are backed up and backups are protected against deliberate erasure or encryption by an attacker.

Attacks on your backups focus on crippling your organization's ability to respond without paying, frequently targeting backups and key documentation required for recovery to force you into paying extortion demands.

Most organizations don't protect backup and restoration procedures against this level of intentional targeting.

Note

This preparation also improves resilience to natural disasters and rapid attacks like WannaCry and (Not)Petya.

[Backup and restore plan to protect against ransomware](#) addresses what to do before an attack to protect your critical business systems and during an attack to ensure a rapid recovery of your business operations.

Program and project member accountabilities

This table describes the overall protection of your data from ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
Central IT Operations or CIO		Executive sponsorship
Program lead from Central IT infrastructure		Drive results and cross-team collaboration

Lead	Implementor	Accountability
	Central IT Infrastructure/Backup	Enable Infrastructure backup
	Central IT Productivity / End User	Enable OneDrive Backup
	Security Architecture	Advise on configuration and standards
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance

Implementation checklist

Apply these best practices to secure your backup infrastructure.

Done	Task	Description
<input type="checkbox"/>	Backup all critical data automatically on a regular schedule.	Allows you to recover data up to the last backup.
<input type="checkbox"/>	Regularly exercise your business continuity/disaster recovery (BC/DR) plan.	Ensures rapid recovery of business operations by treating a ransomware or extortion attack with the same importance as a natural disaster.
<input type="checkbox"/>	Protect backups against deliberate erasure and encryption: - Strong Protection – Require out of band steps (MFA or PIN) before modifying online backups (such as Azure Backup). - Strongest Protection – Store backups in online immutable storage (such as Azure Blob) and/or fully offline or off-site.	Backups that are accessible by attackers can be rendered unusable for business recovery. Implement stronger security to access backups and the inability to change the data stored in backups.

Done	Task	Description
<input type="checkbox"/>	Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB), and network diagrams.	Attackers deliberately target these resources because it impacts your ability to recover. Make sure they survive a ransomware attack.

Implementation results and timelines

Within 30 days, ensure that Mean Time to Recover (MTTR) meets your BC/DR goal, as measured during simulations and real-world operations.

Data protection

You must implement data protection to ensure rapid and reliable recovery from a ransomware attack and to block some techniques of attackers.

Ransomware extortion and destructive attacks only work when all legitimate access to data and systems is lost. Ensuring that attackers cannot remove your ability to resume operations without payment will protect your business and undermine the monetary incentive for attacking your organization.

Program and project member accountabilities

This table describes the overall protection of your organization data from ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
Central IT Operations or CIO		Executive sponsorship
Program lead from Data Security		Drive results and cross-team collaboration
	Central IT Productivity / End User	Implement changes to Microsoft 365 tenant for OneDrive and Protected Folders
	Central IT Infrastructure/Backup	Enable Infrastructure backup

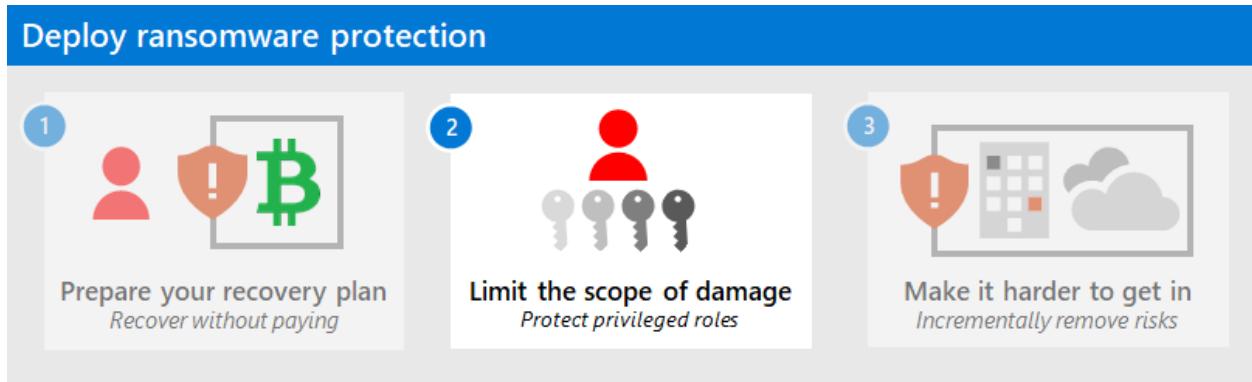
Lead	Implementor	Accountability
	Business / Application	Identify critical business assets
	Security Architecture	Advise on configuration and standards
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance
	User Education Team	Ensure guidance for users reflects policy updates

Implementation checklist

Apply these best practices to protect your organization data.

Done	Task	Description
<input type="checkbox"/>	<p>Migrate your organization to the cloud:</p> <ul style="list-style-type: none"> - Move user data to cloud solutions like OneDrive/SharePoint to take advantage of versioning and recycle bin capabilities. - Educate users on how to recover their files by themselves to reduce delays and cost of recovery. 	User data in the Microsoft cloud can be protected by built-in security and data management features.
<input type="checkbox"/>	Designate Protected Folders .	Makes it more difficult for unauthorized applications to modify the data in these folders.
<input type="checkbox"/>	<p>Review your permissions:</p> <ul style="list-style-type: none"> - Discover broad write/delete permissions on file shares, SharePoint, and other solutions. Broad is defined as many users having write/delete permissions for business-critical data. - Reduce broad permissions for critical data locations while meeting business collaboration requirements. - Audit and monitor critical data locations to ensure broad permissions don't reappear. 	Reduces risk from ransomware activities that rely on broad access.

Next step



Continue with [Phase 2](#) to limit the scope of damage of an attack by protecting privileged roles.

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware ↗](#), Microsoft On the Issues blog post on July 20, 2021
- [Human-operated ransomware](#)
- [Rapidly protect against ransomware and extortion](#)
- [2021 Microsoft Digital Defense Report ↗](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat ↗](#) threat analytics report in the Microsoft 365 Defender portal
- Microsoft's Detection and Response Team (DART) ransomware [approach](#) and [case study](#)

Microsoft 365:

- [Deploy ransomware protection for your Microsoft 365 tenant](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365 ↗](#)
- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)
- [Protect your Windows 10 PC from ransomware ↗](#)
- [Handling ransomware in SharePoint Online](#)
- [Threat analytics reports for ransomware ↗](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- [Find ransomware with advanced hunting](#)

Microsoft Azure:

- [Azure Defenses for Ransomware Attack ↗](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365 ↗](#)
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup ↗ (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel ↗

Microsoft Defender for Cloud Apps:

- [Create anomaly detection policies in Defender for Cloud Apps](#)

Microsoft Security team blog posts:

- A guide to combatting human-operated ransomware: Part 1 (September 2021) ↗
Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.
- A guide to combatting human-operated ransomware: Part 2 (September 2021) ↗
Recommendations and best practices.
- [3 steps to prevent and recover from ransomware \(September 2021\) ↗](#)
- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\) ↗](#)

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\) ↗](#)
Includes attack chain analyses of actual attacks.
- [Ransomware response—to pay or not to pay? \(December 2019\) ↗](#)
- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\) ↗](#)

Phase 2: Limit the scope of damage

Article • 10/26/2022 • 4 minutes to read

In this phase, you protect privileged roles to prevent attackers from obtaining a large scope of access for potential damage to data and systems.

Privileged access strategy

You must implement a comprehensive strategy to reduce the risk of privileged access compromise.

All other security controls can easily be invalidated by an attacker with privileged access in your environment. Ransomware attackers use privileged access as a quick path to control all critical assets in the organization for attack and subsequent extortion.

Program and project member accountabilities

This table describes a privileged access strategy against ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
CISO or CIO		Executive sponsorship
Program lead		Drive results and cross-team collaboration
	IT and Security Architects	Prioritize components integrate into architectures
	Identity and Key Management	Implement identity changes
	Central IT Productivity / End User Team	Implement changes to devices and Office 365 tenant
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance
	User Education Team	Update any password guidance

Implementation checklist

Build a multi-part strategy using the guidance at <https://aka.ms/SPA> that includes this checklist.

Done	Task	Description
<input type="checkbox"/>	Enforce end-to-end session security.	Explicitly validates the trust of users and devices before allowing access to administrative interfaces (using Azure Active Directory Conditional Access).
<input type="checkbox"/>	Protect and monitor identity systems.	Prevents privilege escalation attacks including directories, identity management, administrator accounts and groups, and consent grant configuration.
<input type="checkbox"/>	Mitigate lateral traversal.	Ensures that compromising a single device does not immediately lead to control of many or all other devices using local account passwords, service account passwords, or other secrets.
<input type="checkbox"/>	Ensure rapid threat response.	Limits an adversary's access and time in the environment. See Detection and Response for more information.

Implementation results and timelines

Try to achieve these results in 30-90 days:

- 100 % of admins are required to use secure workstations
- 100 % local workstation/server passwords are randomized
- 100 % privilege escalation mitigations are deployed

Detection and response

Your organization needs responsive detection and remediation of common attacks on endpoints, email, and identities. Minutes matter. You must rapidly remediate common attack entry points to limit the attacker's time to laterally traverse your organization.

Program and project member accountabilities

This table describes the improvement of your detection and response capability against ransomware in terms of a sponsorship/program management/project management

hierarchy to determine and drive results.

Lead	Implementor	Accountability
CISO or CIO		Executive sponsorship
Program lead from Security Operations		Drive results and cross-team collaboration
	Central IT Infrastructure Team	Implement client and server agents/features
	Security Operations	Integrate any new tools into security operations processes
	Central IT Productivity / End User Team	Enable features for Defender for Endpoint, Defender for Office 365, Defender for Identity, and Defender for Cloud Apps
	Central IT Identity Team	Implement Azure AD security and Defender for Identity
	Security Architects	Advise on configuration, standards, and tooling
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance

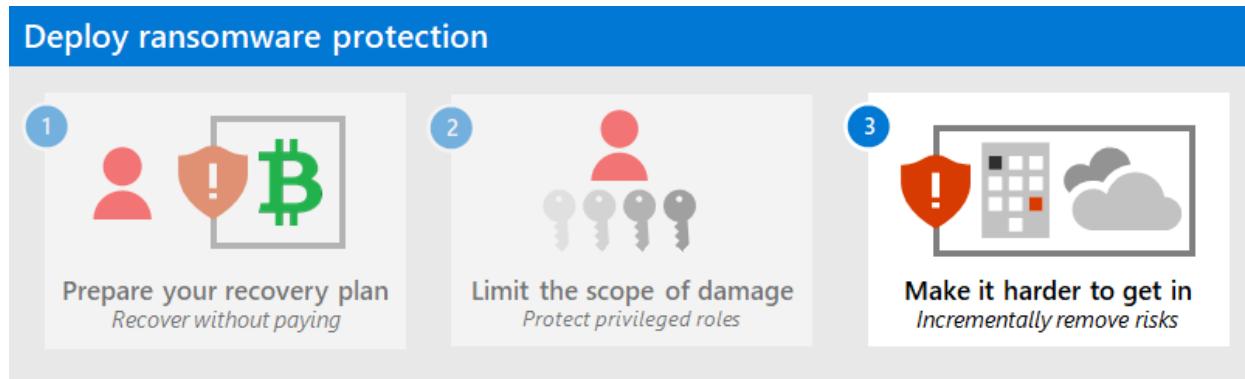
Implementation checklist

Apply these best practices for improving your detection and response.

Done	Task	Description
<input type="checkbox"/>	Prioritize common entry points: <ul style="list-style-type: none">- Use integrated Extended Detection and Response (XDR) tools like Microsoft 365 Defender to provide high quality alerts and minimize friction and manual steps during response.- Monitor for brute-force attempts like password spray.	Ransomware (and other) operators favor endpoint, email, identity, and RDP as entry points.

Done	Task	Description
<input type="checkbox"/>	Monitor for an adversary disabling security (this is often part of an attack chain), such as: <ul style="list-style-type: none"> - Event log clearing, especially the Security Event log and PowerShell Operational logs. - Disabling of security tools and controls. 	Attackers target security detection facilities to continue their attack more safely.
<input type="checkbox"/>	Don't ignore commodity malware.	Ransomware attackers regularly purchase access to target organizations from dark markets.
<input type="checkbox"/>	Integrate outside experts into processes to supplement expertise, such as the Microsoft Detection and Response Team (DART) .	Experience counts for detection and recovery.
<input type="checkbox"/>	Rapidly isolate compromised computers using Defender for Endpoint .	Windows 11 and 10 integration makes this easy.

Next step



Continue with [Phase 3](#) to make it hard for an attacker to get into your environment by incrementally removing risks.

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021
- [Human-operated ransomware](#)
- [Rapidly protect against ransomware and extortion](#)

- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat](#) threat analytics report in the Microsoft 365 Defender portal
- Microsoft's Detection and Response Team (DART) ransomware [approach](#) and [case study](#)

Microsoft 365:

- Deploy ransomware protection for your Microsoft 365 tenant
- Maximize Ransomware Resiliency with Azure and Microsoft 365
- Recover from a ransomware attack
- Malware and ransomware protection
- Protect your Windows 10 PC from ransomware
- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- Find ransomware with advanced hunting

Microsoft Azure:

- [Azure Defenses for Ransomware Attack](#)
- Maximize Ransomware Resiliency with Azure and Microsoft 365
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021)
- A guide to combatting human-operated ransomware: Part 1 (September 2021)

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021)

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#) ↗

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#) ↗

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#) ↗

- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#) ↗

Phase 3: Make it hard to get in

Article • 02/01/2023 • 9 minutes to read

In this phase, you make the attackers work a lot harder to get into your on-premises or cloud infrastructures by incrementally removing the risks at the points of entry.

ⓘ Important

While many of these will be familiar and easy to quickly accomplish, it's critically important that **your work on Phase 3 should not slow down your progress on phases 1 and 2!**

See these sections:

- [Remote access](#)
- [Email and collaboration](#)
- [Endpoints](#)
- [Accounts](#)

Remote access

Gaining access to your organization's intranet through a remote access connection is an attack vector for ransomware attackers. Once an on-premises user account is compromised, an attacker is free to roam on an intranet to gather intelligence, elevate privileges, and install ransomware. The Colonial Pipeline cyberattack in 2021 is an example.

Program and project member accountabilities for remote access

This table describes the overall protection of your remote access solution from ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
CISO or CIO		Executive sponsorship

Lead	Implementor	Accountability
Program lead on the Central IT Infrastructure/Network Team		Drive results and cross-team collaboration
	IT and Security Architects	Prioritize component integration into architectures
	Central IT Identity Team	Configure Azure AD and conditional access policies
	Central IT Operations	Implement changes to environment
	Workload Owners	Assist with RBAC permissions for app publishing
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance
	User Education Team	Update any guidance on workflow changes and perform education and change management

Implementation checklist for remote access

Apply these best practices to protect your remote access infrastructure from ransomware attackers.

Done	Task	Description
<input type="checkbox"/>	Maintain software and appliance updates. Avoid missing or neglecting manufacturer protections (security updates, supported status).	Attackers use well-known vulnerabilities that have not yet been patched as attack vectors.
<input type="checkbox"/>	Configure Azure Active Directory (Azure AD) for existing remote access by including enforcing Zero Trust user and device validation with Conditional Access.	Zero Trust provides multiple levels of securing access to your organization.

Done	Task	Description
<input type="checkbox"/>	Configure security for existing third-party VPN solutions (Cisco AnyConnect , Palo Alto Networks GlobalProtect & Captive Portal , Fortinet FortiGate SSL VPN , Citrix NetScaler, Zscaler Private Access (ZPA), and more).	Take advantage of the built-in security of your remote access solution.
<input type="checkbox"/>	Deploy Azure Point-to-Site (P2S) VPN to provide remote access.	Take advantage of integration with Azure AD and your existing Azure subscriptions.
<input type="checkbox"/>	Publish on-premises web apps with Azure AD Application Proxy .	Apps published with Azure AD Application Proxy do not need a remote access connection.
<input type="checkbox"/>	Secure access to Azure resources with Azure Bastion .	Securely and seamlessly connect to your Azure virtual machines over SSL.
<input type="checkbox"/>	Audit and monitor to find and fix deviations from baseline and potential attacks (see Detection and Response).	Reduce risk from ransomware activities that probe baseline security features and settings.

Email and collaboration

Implement best practices for email and collaboration solutions to make it more difficult for attackers to abuse them, while allowing your workers to access external content easily and safely.

Attackers frequently enter the environment by transferring malicious content in with authorized collaboration tools such as email and file sharing and convincing users to run it. Microsoft has invested in enhanced mitigations that vastly increase protection against these attack vectors.

Program and project member accountabilities for email and collaboration

This table describes the overall protection of your email and collaboration solutions from ransomware in terms of a sponsorship/program management/project

management hierarchy to determine and drive results.

Lead	Implementor	Accountability
CISO, CIO, or Identity Director		Executive sponsorship
Program lead from the Security Architecture team		Drive results and cross-team collaboration
	IT Architects	Prioritize component integration into architectures
	Cloud Productivity or End User Team	Enable Defender for Office 365, ASR, and AMSI
	Security Architecture / Infrastructure + Endpoint	Configuration assistance
	User Education Team	Update guidance on workflow changes
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance

Implementation checklist for email and collaboration

Apply these best practices to protect your email and collaboration solutions from ransomware attackers.

Done	Task	Description
<input type="checkbox"/>	Enable AMSI for Office VBA .	Detect Office macro attacks with endpoint tools like Defender for Endpoint .
<input type="checkbox"/>	Implement Advanced Email security using Defender for Office 365 or a similar solution.	Email is a common entry point for attackers.

Done	Task	Description
<input type="checkbox"/>	<p>Deploy attack surface reduction (ASR) rules to block common attack techniques including:</p> <ul style="list-style-type: none"> - Endpoint abuse such as credential theft, ransomware activity, and suspicious use of PsExec and WMI. - Weaponized Office document activity such as advanced macro activity, executable content, process creation, and process injection initiated by Office applications. <p>Note: Deploy these rules in audit mode first, then assess any negative impact, and then deploy them in block mode.</p>	ASR provides additional layers of protection specifically targeted at mitigating common attack methods.
<input type="checkbox"/>	Audit and monitor to find and fix deviations from baseline and potential attacks (see Detection and Response).	Reduces risk from ransomware activities that probe baseline security features and settings.

Endpoints

Implement relevant security features and rigorously follow software maintenance best practices for endpoints (devices) and applications, prioritizing applications and server/client operating systems directly exposed to Internet traffic and content.

Internet-exposed endpoints are a common entry vector that provides attackers access to the organization's assets. Prioritize blocking common OS and application vulnerabilities with preventive controls to slow or stop them from executing the next stages.

Program and project member accountabilities for endpoints

This table describes the overall protection of your endpoints from ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
Business leadership accountable for business impact of both downtime and attack damage		Executive sponsorship (maintenance)

Lead	Implementor	Accountability
Central IT Operations or CIO		Executive sponsorship (others)
Program lead from the Central IT Infrastructure Team		Drive results and cross-team collaboration
	IT and Security Architects	Prioritize component integration into architectures
	Central IT Operations	Implement changes to environment
	Cloud Productivity or End User Team	Enable attack surface reduction
	Workload/App Owners	Identify maintenance windows for changes
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance

Implementation checklist for endpoints

Apply these best practices to all Windows, Linux, MacOS, Android, iOS, and other endpoints.

Done	Task	Description
<input type="checkbox"/>	Block known threats with attack surface reduction rules, tamper protection , and block at first site .	Don't let lack of use of these built-in security features be the reason an attacker entered your organization.
<input type="checkbox"/>	Apply Security Baselines to harden internet-facing Windows servers and clients and Office applications.	Protect your organization with the minimum level of security and build from there.

Done	Task	Description
<input type="checkbox"/>	Maintain your software so that it is: <ul style="list-style-type: none"> - Updated: Rapidly deploy critical security updates for operating systems, browsers, & email clients - Supported: Upgrade operating systems and software for versions supported by your vendors. 	Attackers are counting on you missing or neglecting manufacturer updates and upgrades.
<input type="checkbox"/>	Isolate, disable, or retire insecure systems and protocols, including unsupported operating systems and legacy protocols .	Attackers use known vulnerabilities of legacy devices, systems, and protocols as entry points into your organization.
<input type="checkbox"/>	Block unexpected traffic with host-based firewall and network defenses.	Some malware attacks rely on unsolicited inbound traffic to hosts as a way of making a connection for an attack.
<input type="checkbox"/>	Audit and monitor to find and fix deviations from baseline and potential attacks (see Detection and Response).	Reduces risk from ransomware activities that probe baseline security features and settings.

Accounts

Just as antique skeleton keys won't protect a house against a modern-day burglar, passwords cannot protect accounts against common attacks we see today. While multi-factor authentication (MFA) was once a burdensome extra step, passwordless authentication improves the sign-in experience using biometric approaches that don't require your users to remember or type a password. Additionally, a [Zero Trust](#) infrastructure stores information about trusted devices, which reduce prompting for annoying out-of-band MFA actions.

Starting with high-privilege administrator accounts, rigorously follow these best practices for account security including using passwordless or MFA.

Program and project member accountabilities for accounts

This table describes the overall protection of your accounts from ransomware in terms of a sponsorship/program management/project management hierarchy to determine and drive results.

Lead	Implementor	Accountability
CISO, CIO, or Identity Director		Executive sponsorship
Program lead from Identity and Key Management or Security Architecture teams		Drive results and cross-team collaboration
	IT and Security Architects	Prioritize component integration into architectures
	Identity and Key Management or Central IT Operations	Implement configuration changes
	Security Policy and Standards	Update standards and policy documents
	Security Compliance Management	Monitor to ensure compliance
	User Education Team	Update password or sign-in guidance and perform education and change management

Implementation checklist for accounts

Apply these best practices to protect your accounts from ransomware attackers.

Done	Task	Description
<input type="checkbox"/>	<ul style="list-style-type: none"> Enforce strong MFA or passwordless sign-in for all users. Start with administrator and priority accounts using one or more of: <ul style="list-style-type: none"> - Passwordless authentication with Windows Hello or the Microsoft Authenticator app. - Azure Multi-Factor Authentication. - A third-party MFA solution. 	Make it harder for an attacker to perform a credential compromise by just determining a user account password.

Done	Task	Description
<input type="checkbox"/>	<p>Increase password security:</p> <ul style="list-style-type: none"> - For Azure AD accounts, use Azure AD Password Protection to detect and block known weak passwords and additional weak terms that are specific to your organization. - For on-premises Active Directory Domain Services (AD DS) accounts, Extend Azure AD Password Protection to AD DS accounts. 	Ensure that attackers can't determine common passwords or passwords based on your organization name.
<input type="checkbox"/>	Audit and monitor to find and fix deviations from baseline and potential attacks (see Detection and Response).	Reduces risk from ransomware activities that probe baseline security features and settings.

Implementation results and timelines

Try to achieve these results within 30 days:

- 100 % of employees are actively using MFA
- 100 % deployment of higher password security

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021
- [Human-operated ransomware](#)
- [Rapidly protect against ransomware and extortion](#)
- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat](#) threat analytics report in the Microsoft 365 Defender portal
- Microsoft's Detection and Response Team (DART) ransomware [approach](#) and [case study](#)

Microsoft 365:

- [Deploy ransomware protection for your Microsoft 365 tenant](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)

- Protect your Windows 10 PC from ransomware ↗
- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware ↗ in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- Find ransomware with advanced hunting

Microsoft Azure:

- Azure Defenses for Ransomware Attack ↗
- Maximize Ransomware Resiliency with Azure and Microsoft 365 ↗
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup ↗ (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel ↗

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021) ↗
- A guide to combatting human-operated ransomware: Part 1 (September 2021) ↗

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021) ↗

Recommendations and best practices.
- Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats (May 2021) ↗

See the **Ransomware** section.

- Human-operated ransomware attacks: A preventable disaster (March 2020) ↗

Includes attack chain analyses of actual attacks.
- Ransomware response—to pay or not to pay? (December 2019) ↗

- Norsk Hydro responds to ransomware attack with transparency (December 2019) ↗

Backup and restore plan to protect against ransomware

Article • 10/12/2022 • 18 minutes to read

Ransomware attacks deliberately encrypt or erase data and systems to force your organization to pay money to attackers. These attacks target your data, your backups, and also key documentation required for you to recover without paying the attackers (as a means to increase the chances your organization will pay).

This article addresses what to do before an attack to protect your critical business systems and during an attack to ensure a rapid recovery of business operations.

Note

Preparing for ransomware also improves resilience to natural disasters and rapid attacks like [WannaCry](#) & [\(Not\)Petya](#).

What is ransomware?

Ransomware is a type of extortion attack that encrypts files and folders, preventing access to important data and systems. Attackers use ransomware to extort money from victims by demanding money, usually in the form of cryptocurrencies, in exchange for a decryption key or in exchange for not releasing sensitive data to the dark web or the public internet.

While early ransomware mostly used malware that spread with phishing or between devices, [human-operated ransomware](#) has emerged where a gang of active attackers, driven by human attack operators, target all systems in an organization (rather than a single device or set of devices). An attack can:

- Encrypt your data
- Exfiltrate your data
- Corrupt your backups

The ransomware leverages the attackers' knowledge of common system and security misconfigurations and vulnerabilities to infiltrate the organization, navigate the enterprise network, and adapt to the environment and its weaknesses as they go.

Ransomware can be staged to exfiltrate your data first, over several weeks or months, before the ransomware actually executes on a specific date.

Ransomware can also slowly encrypt your data while keeping your key on the system. With your key still available, your data is usable to you and the ransomware goes unnoticed. Your backups, though, are of the encrypted data. Once all of your data is encrypted and recent backups are also of encrypted data, your key is removed so you can no longer read your data.

The real damage is often done when the attack exfiltrates files while leaving backdoors in the network for future malicious activity—and these risks persist whether or not the ransom is paid. These attacks can be catastrophic to business operations and difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike early forms of ransomware that only required malware remediation, human-operated ransomware can continue to threaten your business operations after the initial encounter.

Impact of an attack

The impact of a ransomware attack on any organization is difficult to quantify accurately. Depending on the scope of the attack, the impact could include:

- Loss of data access
- Business operation disruption
- Financial loss
- Intellectual property theft
- Compromised customer trust or tarnished reputation
- Legal expenses

How can you protect yourself?

The best way to prevent falling victim to ransomware is to implement preventive measures and have tools that protect your organization from every step that attackers take to infiltrate your systems.

You can reduce your on-premises exposure by moving your organization to a cloud service. Microsoft has invested in native security capabilities that make Microsoft Azure resilient against ransomware attacks and helps organizations defeat ransomware attack techniques. For a comprehensive view of ransomware and extortion and how to protect your organization, use the information in the [Human-Operated Ransomware Mitigation Project Plan](#)  PowerPoint presentation.

You should assume that at some point in time you will fall victim to a ransomware attack. One of the most important steps you can take to protect your data and avoid paying a ransom is to have a reliable backup and restore plan for your business-critical

information. Since ransomware attackers have invested heavily into neutralizing backup applications and operating system features like volume shadow copy, it is critical to have backups that are inaccessible to a malicious attacker.

Azure Backup

[Azure Backup](#) provides security to your backup environment, both when your data is in transit and at rest. With Azure Backup, [you can back up](#):

- On-premises files, folders, and system state
- Entire Windows/Linux VMs
- Azure Managed Disks
- Azure file shares to a storage account
- SQL Server databases running on Azure VMs

The backup data is stored in Azure storage and the guest or attacker has no direct access to backup storage or its contents. With virtual machine backup, the backup snapshot creation and storage is done by Azure fabric where the guest or attacker has no involvement other than quiescing the workload for application consistent backups. With SQL and SAP HANA, the backup extension gets temporary access to write to specific blobs. In this way, even in a compromised environment, existing backups can't be tampered with or deleted by the attacker.

Azure Backup provides built-in monitoring and alerting capabilities to view and configure actions for events related to Azure Backup. Backup Reports serve as a one-stop destination for tracking usage, auditing of backups and restores, and identifying key trends at different levels of granularity. Using Azure Backup's monitoring and reporting tools can alert you to any unauthorized, suspicious, or malicious activity as soon as they occur.

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before [modifying online backups](#).

Learn more about the [security features](#) built into Azure Backup.

Validate backups

Validate that your backup is good as your backup is created and before you restore. We recommend that you use a [Recovery Services vault](#), which is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for

virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (Linux or Windows) and Azure SQL databases as well as on-premises assets. Recovery Services vaults make it easy to organize your backup data and provide features such as:

- Enhanced capabilities to ensure you can secure your backups, and safely recover data, even if production and backup servers are compromised. [Learn more](#).
- Monitoring for your hybrid IT environment (Azure IaaS VMs and on-premises assets) from a central portal. [Learn more](#).
- Compatibility with Azure role-based access control (Azure RBAC), which restricts backup and restore access to a defined set of user roles. Azure RBAC provides various built-in roles, and Azure Backup has three built-in roles to manage recovery points. [Learn more](#).
- Soft delete protection, even if a malicious actor deletes a backup (or backup data is accidentally deleted). Backup data is retained for 14 additional days, allowing the recovery of a backup item with no data loss. [Learn more](#).
- Cross Region Restore which allows you to restore Azure VMs in a secondary region, which is an Azure paired region. You can restore the replicated data in the secondary region any time. This enables you to restore the secondary region data for audit-compliance, and during outage scenarios, without waiting for Azure to declare a disaster (unlike the GRS settings of the vault). [Learn more](#).

 **Note**

There are two types of vaults in Azure Backup. In addition to the Recovery Services vaults, there are also **Backup vaults** that house data for newer workloads supported by Azure Backup.

What to do before an attack

As mentioned earlier, you should assume that at some point in time you will fall victim to a ransomware attack. Identifying your business-critical systems and applying best practices before an attack will get you back up and running as quickly as possible.

Determine what is most important to you

Ransomware can attack while you are planning for an attack so your first priority should be to identify the business-critical systems that are most important to you and begin performing regular backups on those systems.

In our experience, the five most important applications to customers fall into the following categories in this priority order:

- Identity systems – required for users to access any systems (including all others described below) such as Active Directory, [Azure AD Connect](#), AD domain controllers
- Human life – any system that supports human life or could put it at risk such as medical or life support systems, safety systems (ambulance, dispatch systems, traffic light control), large machinery, chemical/biological systems, production of food or personal products, and others
- Financial systems – systems that process monetary transactions and keep the business operating, such as payment systems and related databases, financial system for quarterly reporting
- Product or service enablement – any systems that are required to provide the business services or produce/deliver physical products that your customers pay you for, factory control systems, product delivery/dispatch systems, and similar
- Security (minimum) – You should also prioritize the security systems required to monitor for attacks and provide minimum security services. This should be focused on ensuring that the current attacks (or easy opportunistic ones) are not immediately able to gain (or regain) access to your restored systems

Your prioritized back up list also becomes your prioritized restore list. Once you've identified your critical systems and are performing regular backups, then take steps to reduce your exposure level.

Steps to take before an attack

Apply these best practices before an attack.

Task	Detail
Identify the important systems that you need to bring back online first (using top five categories above) and immediately begin performing regular backups of those systems.	To get back up and running as quickly as possible after an attack, determine today what is most important to you.

Task	Detail
<p>Migrate your organization to the cloud.</p> <p>Consider purchasing a Microsoft Unified Support plan or working with a Microsoft partner to help support your move to the cloud.</p>	<p>Reduce your on-premises exposure by moving data to cloud services with automatic backup and self-service rollback. Microsoft Azure has a robust set of tools to help you backup your business-critical systems and restore your backups faster.</p> <p>Microsoft Unified Support is a cloud services support model that is there to help you whenever you need it. Unified Support:</p> <ul style="list-style-type: none"> Provides a designated team that is available 24x7 with as-needed problem resolution and critical incident escalation Helps you monitor the health of your IT environment and works proactively to make sure problems are prevented before they happen
<p>Move user data to cloud solutions like OneDrive and SharePoint to take advantage of versioning and recycle bin capabilities.</p>	<p>User data in the Microsoft cloud can be protected by built-in security and data management features.</p> <p>It's good to teach users how to restore their own files but you need to be careful that your users do not restore the malware used to carry out the attack. You need to:</p>
<p>Educate users on how to recover their files by themselves to reduce delays and cost of recovery. For example, if a user's OneDrive files were infected by malware, they can restore their entire OneDrive to a previous time.</p> <p>Consider a defense strategy, such as Microsoft 365 Defender, before allowing users to restore their own files.</p>	<p>Ensure your users don't restore their files until you are confident that the attacker has been evicted</p> <p>Have a mitigation in place in case a user does restore some of the malware</p> <p>Microsoft 365 Defender uses AI-powered automatic actions and playbooks to remediate impacted assets back to a secure state. Microsoft 365 Defender leverages automatic remediation capabilities of the suite products to ensure all impacted assets related to an incident are automatically remediated where possible.</p>
<p>Implement the Microsoft cloud security benchmark.</p>	<p>The Microsoft cloud security benchmark is our security control framework based on industry-based security control frameworks such as NIST SP800-53, CIS Controls v7.1. It provides organizations guidance on how to configure Azure and Azure services and implement the security controls. See Backup and Recovery.</p>

Task	Detail
Regularly exercise your business continuity/disaster recovery (BC/DR) plan.	Ensures rapid recovery of business operations by treating a ransomware or extortion attack with the same importance as a natural disaster.
Simulate incident response scenarios. Exercises you perform in preparing for an attack should be planned and conducted around your prioritized backup and restore lists.	Conduct practice exercise(s) to validate cross-team processes and technical procedures, including out of band employee and customer communications (assume all email and chat is down).
Regularly test 'Recover from Zero' scenario to ensure your BC/DR can rapidly bring critical business operations online from zero functionality (all systems down).	
Consider creating a risk register to identify potential risks and address how you will mediate through preventative controls and actions. Add ransomware to risk register as high likelihood and high impact scenario.	<p>A risk register can help you prioritize risks based on the likelihood of that risk occurring and the severity to your business should that risk occur.</p> <p>Track mitigation status via Enterprise Risk Management (ERM) assessment cycle.</p>
Backup all critical business systems automatically on a regular schedule (including backup of critical dependencies like Active Directory).	Allows you to recover data up to the last backup.
Validate that your backup is good as your backup is created.	

Task	Detail
Protect (or print) supporting documents and systems required for recovery such as restoration procedure documents, CMDB, network diagrams, and SolarWinds instances.	Attackers deliberately target these resources because it impacts your ability to recover.
Ensure you have well-documented procedures for engaging any third-party support, particularly support from threat intelligence providers, antimalware solution providers, and from the malware analysis provider. Protect (or print) these procedures.	Third-party contacts may be useful if the given ransomware variant has known weaknesses or decryption tools are available.
<p>Ensure backup and recovery strategy includes:</p> <p>Ability to back up data to a specific point in time.</p> <p>Multiple copies of backups are stored in isolated, offline (air-gapped) locations.</p> <p>Recovery time objectives that establish how quickly backed up information can be retrieved and put into production environment.</p> <p>Rapid restore of back up to a production environment/sandbox.</p>	<p>Backups are essential for resilience after an organization has been breached. Apply the 3-2-1 rule for maximum protection and availability: 3 copies (original + 2 backups), 2 storage types, and 1 offsite or cold copy.</p>

Task	Detail
Protect backups against deliberate erasure and encryption:	Backups that are accessible by attackers can be rendered unusable for business recovery.
Store backups in offline or off-site storage and/or immutable storage.	Offline storage ensures robust transfer of backup data without using any network bandwidth. Azure Backup supports offline backup , which transfers initial backup data offline, without the use of network bandwidth. It provides a mechanism to copy backup data onto physical storage devices. The devices are then shipped to a nearby Azure datacenter and uploaded onto a Recovery Services vault .
Require out of band steps (such as MFA or a security PIN) before permitting an online backup to be modified or erased.	Online immutable storage (such as Azure Blob) enables you to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval.
Create private endpoints within your Azure Virtual Network to securely back up and restore data from your Recovery Services vault.	Multifactor authentication (MFA) should be mandatory for all admin accounts and is strongly recommended for all users. The preferred method is to use an authenticator app rather than SMS or voice where possible. When you set up Azure Backup you can configure your recovery services to enable MFA using a security PIN generated in the Azure portal. This ensures that a security pin is generated to perform critical operations such as updating or removing a recovery point.
Designate protected folders .	Makes it more difficult for unauthorized applications to modify the data in these folders.
Review your permissions:	Reduces risk from broad access-enabling ransomware activities.
Discover broad write/delete permissions on file shares, SharePoint, and other solutions. Broad is defined as many users having write/delete permissions for business-critical data.	
Reduce broad permissions while meeting business collaboration requirements.	
Audit and monitor to ensure broad permissions don't reappear.	

Task	Detail
Protect against a phishing attempt:	The most common method used by attackers to infiltrate an organization is phishing attempts via email. Exchange Online Protection (EOP) is the cloud-based filtering service that protects your organization against spam, malware, and other email threats. EOP is included in all Microsoft 365 organizations with Exchange Online mailboxes.
Conduct security awareness training regularly to help users identify a phishing attempt and avoid clicking on something that can create an initial entry point for a compromise.	An example of a security filtering control for email is Safe Links . Safe Links is a feature in Defender for Office 365 that provides scanning and rewriting of URLs and links in email messages during inbound mail flow, and time-of-click verification of URLs and links in email messages and other locations (Microsoft Teams and Office documents). Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in EOP. Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.
Apply security filtering controls to email to detect and minimize the likelihood of a successful phishing attempt.	Learn more about anti-phishing protection.

What to do during an attack

If you are attacked, your prioritized back up list becomes your prioritized restore list. Before you restore, validate again that your backup is good. You may be able to look for malware inside the backup.

Steps to take during an attack

Apply these best practices during an attack.

Task	Detail
------	--------

Task	Detail
<p>Early in the attack, engage third-party support, particularly support from threat intelligence providers, antimalware solution providers and from the malware analysis provider.</p>	<p>These contacts may be useful if the given ransomware variant has a known weakness or decryption tools are available.</p> <p>Microsoft Detection and Response Team (DART) can help protect you from attacks. The DART engages with customers around the world, helping to protect and harden against attacks before they occur, as well as investigating and remediating when an attack has occurred.</p> <p>Microsoft also provides Rapid Ransomware Recovery services. Services are exclusively delivered by the Microsoft Global Compromise Recovery Security Practice (CRSP). The focus of this team during a ransomware attack is to restore authentication service and limit the impact of ransomware.</p> <p>DART and CRSP are part of Microsoft's Industry Solutions Delivery security service line.</p>
<p>Contact your local or federal law enforcement agencies.</p>	<p>If you are in the United States, contact the FBI to report a ransomware breach using the IC3 Complaint Referral Form.</p>
<p>Take steps to remove malware or ransomware payload from your environment and stop the spread.</p> <p>Run a full, current antivirus scan on all suspected computers and devices to detect and remove the payload that's associated with the ransomware.</p> <p>Scan devices that are synchronizing data, or the targets of mapped network drives.</p>	<p>You can use Windows Defender or (for older clients) Microsoft Security Essentials.</p> <p>An alternative that will also help you remove ransomware or malware is the Malicious Software Removal Tool (MSRT).</p>
<p>Restore business-critical systems first. Remember to validate again that your backup is good before you restore.</p>	<p>At this point, you don't need to restore everything. Focus on the top five business-critical systems from your restore list.</p>
<p>If you have offline backups, you can probably restore the encrypted data after you've removed the ransomware payload (malware) from your environment.</p>	<p>To prevent future attacks, ensure ransomware or malware is not on your offline backup before restoring.</p>

Task	Detail
Identify a safe point-in-time backup image that is known not to be infected.	To prevent future attacks, scan backup for ransomware or malware before restoring.
If you use Recovery Services vault, carefully review the incident timeline to understand the right point-in-time to restore a backup.	
Use a safety scanner and other tools for full operating system restore as well as data restore scenarios.	Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers. Simply download it and run a scan to find malware and try to reverse changes made by identified threats.
Ensure that your antivirus or endpoint detection and response (EDR) solution is up to date. You also need to have up-to-date patches.	An EDR solution, such as Microsoft Defender for Endpoint , is preferred.
After business-critical systems are up and running, restore other systems.	Telemetry data should help you identify if malware is still on your systems.
As systems get restored, start collecting telemetry data so you can make formative decisions about what you are restoring.	

Post attack or simulation

After a ransomware attack or an incident response simulation, take the following steps to improve your backup and restore plans as well as your security posture:

1. Identify lessons learned where the process did not work well (and opportunities to simplify, accelerate, or otherwise improve the process)
2. Perform root cause analysis on the biggest challenges (at enough detail to ensure solutions address the right problem — considering people, process, and technology)
3. Investigate and remediate the original breach (engage the [Microsoft Detection and Response Team \(DART\)](#) ↗ to help)
4. Update your backup and restore strategy based on lessons learned and opportunities — prioritizing based on highest impact and quickest implementation steps first

Next steps

In this article, you learned how to improve your backup and restore plan to protect against ransomware. For best practices on deploying ransomware protection, see [Rapidly protect against ransomware and extortion](#).

Key industry information:

- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)

Microsoft Azure:

- [Help protect from ransomware with Microsoft Azure Backup](#) (26 minute video)
- [Recovering from systemic identity compromise](#)
- [Advanced multistage attack detection in Microsoft Sentinel](#)

Microsoft 365:

- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)
- [Protect your Windows 10 PC from ransomware](#)
- [Handling ransomware in SharePoint Online](#)

Microsoft 365 Defender:

- [Find ransomware with advanced hunting](#)

Microsoft Security team blog posts:

- [Becoming resilient by understanding cybersecurity risks: Part 4, navigating current threats \(May 2021\)](#). See the Ransomware section
- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#). Includes attack chain analysis of actual human-operated ransomware attacks
- [Ransomware response — to pay or not to pay? \(December 2019\)](#)
- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#)

Microsoft DART ransomware approach and best practices

Article • 02/01/2023 • 16 minutes to read

[Human-operated ransomware](#) is not a malicious software problem—it's a human criminal problem. The solutions used to address commodity problems aren't enough to prevent a threat that more closely resembles a nation-state threat actor who:

- Disables or uninstalls your antivirus software before encrypting files
- Disables security services and logging to avoid detection
- Locates and corrupts or deletes backups before sending a ransom demand

These actions are commonly done with legitimate programs that you might already have in your environment for administrative purposes. In criminal hands, these tools are used maliciously to carry out attacks.

Responding to the increasing threat of ransomware requires a combination of modern enterprise configuration, up-to-date security products, and the vigilance of trained security staff to detect and respond to the threats before data is lost.

The [Microsoft Detection and Response Team \(DART\)](#) responds to security compromises to help customers become cyber-resilient. DART provides onsite reactive incident response and remote proactive investigations. DART leverages Microsoft's strategic partnerships with security organizations around the world and internal Microsoft product groups to provide the most complete and thorough investigation possible.

This article describes how DART handles ransomware attacks for Microsoft customers so that you can consider applying elements of their approach and best practices for your own security operations playbook.

See these sections for the details:

- [How DART uses Microsoft security services](#)
- [The DART approach to conducting ransomware incident investigations](#)
- [DART recommendations and best practices](#)

Note

This article content was derived from the [A guide to combatting human-operated ransomware: Part 1](#) and [A guide to combatting human-operated ransomware:](#)

How DART uses Microsoft security services

DART relies heavily on data for all investigations and uses existing deployments of Microsoft security services such as [Microsoft Defender for Office 365](#), [Microsoft Defender for Endpoint](#), [Microsoft Defender for Identity](#), and [Microsoft Defender for Cloud Apps](#).

Defender for Endpoint

Defender for Endpoint is Microsoft's enterprise endpoint security platform designed to help enterprise network security analysts prevent, detect, investigate, and respond to advanced threats. Defender for Endpoint can detect attacks using advanced behavioral analytics and machine learning. Your analysts can use Defender for Endpoint for attacker behavioral analytics.

Here's an example of an alert in Microsoft Defender for Endpoint for a pass-the-ticket attack.

The screenshot shows the Microsoft Defender Security Center interface. The left sidebar has a tree view with nodes like 'janetl pc.ftpdemons.net' and 'Alerts > Pass-the-ticket attack'. The main pane displays a detailed alert for a 'Pass-the-ticket attack' on 'janetl pc.ftpdemons.net'. The alert is categorized as 'High' risk and 'New'. It includes sections for 'Alert story' (listing processes like 'nttakm.exe', 'smss.exe', 'smss.exe (92999999 00000004)', 'wminit.exe', 'services.exe', and 'PSXEXSVCE.exe'), 'Details' (showing incident details, detection source as EDR, and detection status as Detected), and 'Alert description' (mentioning a kerberos ticket file was created). A status bar at the bottom right says 'A kerberos ticket file, a known file extension for Kerberos tickets containing long-lived encrypted users credentials, was observed being created on the machine. T'.

Your analysts can also perform advanced hunting queries to pivot off indicators of compromise (IOCs) or search for known behavior if they identify a threat actor group.

Here's an example of how advanced hunting queries can be used to locate known attacker behavior.

The screenshot shows the Microsoft Defender Security Center interface. On the left, the 'Advanced hunting' pane is open, displaying a schema tree for 'Devices' and 'Functions'. Under 'Functions', there are entries for 'FileProfile', 'AssignedIPAddresses', and 'DeviceFromIP'. Below these are 'Queries' sections for 'Shared queries', 'Community', 'Campaigns', 'Collection', and 'Command and Control'. In the center, a PowerShell query editor window is open with the following script:

```
// Finds PowerShell execution events that could involve a download.
DeviceProcessEvents
| where FileLineIn -in ("powershell.exe", "powershell_lse.exe")
| where ProcessCommandLine has ".Net.WebClient"
| or ProcessCommandLine has "DownloadofFile"
| or ProcessCommandLine has "Invoke-WebRequest"
| or ProcessCommandLine has "Invoke-Shellcode"
| or ProcessCommandLine has "Http"
| or ProcessCommandLine has "Start-FileTransfer"
| or ProcessCommandLine has "InvokeUnexec"
| or ProcessCommandLine has "PowerShell"

```

Below the query editor is a table showing event details like Timestamp, DeviceID, DeviceName, and Action. On the right, the 'Inspect record' pane is open, showing asset details for a machine named 'annette-pc' with a risk level of 'High' and exposure level 'High'. It also displays a process tree for 'powershell.exe' under 'WINWORD.EXE', showing its execution time (Aug 12, 2021, 11:44:29.897 PM) and path (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe). A detailed view of the process is shown on the far right.

In Defender for Endpoint, you have access to a real-time expert-level monitoring and analysis service by Microsoft Threat Experts for ongoing suspected actor activity. You can also collaborate with experts on demand for additional insights into alerts and incidents.

Here's an example of how Defender for Endpoint shows detailed ransomware activity.

The screenshot shows an 'Alerts > Ransomware activity detected on 4 devices' page. The main section is titled 'Ransomware activity detected on 4 devices' and shows two affected hosts: 'HOST01' and 'HOST01\administrator'. Below this is a 'What happened' summary and an 'Executive summary' which states: 'Microsoft Threat Experts are tracking a threat in your environment related to ransomware activity on 4 devices. These behaviors may have resulted in credential dumping, credential commands via Windows Management Interface (WMI), launch new commands via PowerShell, delete or move generated artifacts on a host system, use tools to persist on systems, disable security tools, attempt to cover their tracks, launch processes through remote file copy, automated collection, creation of an account to allow persistence, adding a program to a startup folder or referencing it with a Registry run key, command and control, using a remote access tool, data encryption for impact and inhibition of system recovery. In ransomware attacks, threat actors encrypt data on target systems to create an interruption in business operations which they then leverage for monetary gain.' It also mentions immediate action steps and a follow-up alert.

The 'Timeline of observed events' table lists specific malicious activities:

Date/Time	Actions
2021-05-08T12:20:54.872Z	T1003: OS Credential Dumping mimikatz.exe loaded crypt32.dll library
2021-05-08T12:20:59.368Z	lazagne.exe process executed command: lsAzoGiczzl
2021-05-08T12:21:02.646Z	T1003: OS Credential Dumping cmd.exe process executed command: reg.exe save hklm\system c:\users\<USER_NAME>\appdata\local\temp\qjgmyhuf
2021-05-08T12:41:34.827Z	T1490: Inhibit System Recovery cmd.exe process executed command: wmic SHADOWCOPY Delete

The 'Impacted device(s)' section lists the four devices involved. To the right, the 'Details' pane shows the alert status as 'Resolved', classification as 'True alert', and determination as 'Malware'. It also lists the detection source as 'Threat Experts', category as 'Ransomware', and techniques used, including T1003, T1113, T1114, T1115, T1116, T1117, T1118, T1119, and T1121.

Defender for Identity

You use Defender for Identity to investigate known compromised accounts and to find potentially compromised accounts in your organization. Defender for Identity sends alerts for known malicious activity that actors often use such as DC Sync attacks, remote

code execution attempts, and pass-the-hash attacks. Defender for Identity enables you to pinpoint suspect activity and accounts to narrow down the investigation.

Here's an example of how Defender for Identity sends alerts for known malicious activity related to ransomware attacks.

Alerts									
Export		1 Week	Manage alerts						
Filters: Service sources: Microsoft Defender for Identity									
Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last activity ↓
Security principal reconnaissance (LDAP)	Medium	Unsupported OS	Resolved	Discovery	MDI	HOST01	Aug 15, 2021 2:45 AM	Aug 15, 2021 2:48 AM	
Remote code execution attempt	Medium	Unsupported alert type	Resolved	Execution	MDI	3 Hosts	Aug 13, 2021 9:32 AM	Aug 14, 2021 9:12 AM	
Security principal reconnaissance (LDAP)	Medium	Resolved	Discovery	MDI	HOST02	Aug 12, 2021 8:18 PM	Aug 13, 2021 5:03 PM		
User and group membership reconnaissance ...	Medium	Resolved	Discovery	MDI	HOST03	5 Acc... Aug 12, 2021 9:26 PM	Aug 12, 2021 9:26 PM		
Suspicious additions to sensitive groups	Medium	Unsupported alert type	Resolved	Persistence	MDI	HOST04	2 Acc... Aug 10, 2021 11:41 PM	Aug 10, 2021 11:41 PM	

Defender for Cloud Apps

Defender for Cloud Apps (previously known as Microsoft Defender for Cloud Apps) allows your analysts to detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications. Defender for Cloud Apps is Microsoft's cloud access security broker (CASB) solution that allows for monitoring of cloud services and data access in cloud services by users.

Here's an example of the Defender for Cloud Apps dashboard, which allows analysis to detect unusual behavior across cloud apps.

Dashboard

Filter by app: All apps

<h4>Alerts</h4> <p>7 open alerts Over the last 30 days</p>  <p>Low severity Medium severity High severity</p> <p>Recent alerts:</p> <table><thead><tr><th>Alert</th><th>Date</th></tr></thead><tbody><tr><td>HVT Login from Non-Corporate</td><td>Aug 16, 2021</td></tr><tr><td>Impossible travel activity</td><td>Aug 16, 2021</td></tr><tr><td>Risky sign-in: Unfamiliar sign-i...</td><td>Aug 16, 2021</td></tr></tbody></table> <p>View all alerts</p>	Alert	Date	HVT Login from Non-Corporate	Aug 16, 2021	Impossible travel activity	Aug 16, 2021	Risky sign-in: Unfamiliar sign-i...	Aug 16, 2021	<h4>Discovered apps</h4> <p>No discovered apps Over the last 30 days Updated on Aug 16, 2021, 1:57 PM View all discovered apps</p>	<h4>Top users to investigate</h4> <p>1000+ users to investigate Investigation priority is calculated by the user's alerts and activities over the past 7 days</p> <table border="1"><thead><tr><th>Name</th><th>Investigation priority score</th></tr></thead><tbody><tr><td>MEGHAN BOWERS</td><td>250</td></tr><tr><td>JEFF LEATHERMAN</td><td>184</td></tr><tr><td>MIKE JONES</td><td>176</td></tr><tr><td>JOHN WOOD</td><td>171</td></tr><tr><td>JIM BOB</td><td>166</td></tr><tr><td>KAREN SMITH</td><td>146</td></tr><tr><td>HELP DESK</td><td>138</td></tr></tbody></table> <p>View all users to investigate</p>	Name	Investigation priority score	MEGHAN BOWERS	250	JEFF LEATHERMAN	184	MIKE JONES	176	JOHN WOOD	171	JIM BOB	166	KAREN SMITH	146	HELP DESK	138
Alert	Date																									
HVT Login from Non-Corporate	Aug 16, 2021																									
Impossible travel activity	Aug 16, 2021																									
Risky sign-in: Unfamiliar sign-i...	Aug 16, 2021																									
Name	Investigation priority score																									
MEGHAN BOWERS	250																									
JEFF LEATHERMAN	184																									
MIKE JONES	176																									
JOHN WOOD	171																									
JIM BOB	166																									
KAREN SMITH	146																									
HELP DESK	138																									

Microsoft Secure Score

The set of Microsoft 365 Defender services provides live remediation recommendations to reduce the attack surface. Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating that more improvement actions have been taken. See the [Secure Score](#) documentation to find out more about how your organization can leverage this feature to prioritize remediation actions that are based on their environment.

The DART approach to conducting ransomware incident investigations

You should make every effort to determine how the adversary gained access to your assets so that vulnerabilities can be remediated. Otherwise, it is highly likely that the same type of attack will take place again in the future. In some cases, the threat actor takes steps to cover their tracks and destroy evidence, so it is possible that the entire chain of events may not be evident.

The following are three key steps in DART ransomware investigations:

Step	Goal	Initial questions
1. Assess the current situation	Understand the scope	What initially made you aware of a ransomware attack? What time/date did you first learn of the incident? What logs are available and is there any indication that the actor is currently accessing systems?
2. Identify the affected line-of-business (LOB) apps	Get systems back online	Does the application require an identity? Are backups of the application, configuration, and data available? Are the content and integrity of backups regularly verified using a restore exercise?
3. Determine the compromise recovery (CR) process	Remove attacker control from the environment	N/A

Step 1. Assess the current situation

An assessment of the current situation is critical to understanding the scope of the incident and for determining the best people to assist and to plan and scope the investigation and remediation tasks. Asking the following initial questions is crucial in helping to determine the situation.

What initially made you aware of the ransomware attack?

If the initial threat was identified by IT staff—such as noticing backups being deleted, antivirus alerts, endpoint detection and response (EDR) alerts, or suspicious system changes—it is often possible to take quick decisive measures to thwart the attack, typically by disabling all inbound and outbound Internet communication. This may temporarily affect business operations, but that would typically be much less impactful than an adversary deploying ransomware.

If the threat was identified by a user call to the IT helpdesk, there may be enough advance warning to take defensive measures to prevent or minimize the effects of the attack. If the threat was identified by an external entity (like law enforcement or a financial institution), it is likely that the damage is already done, and you will see evidence in your environment that the threat actor has already gained administrative control of your network. This can range from ransomware notes, locked screens, or ransom demands.

What date/time did you first learn of the incident?

Establishing the initial activity date and time is important because it helps narrow the scope of the initial triage for quick wins by the attacker. Additional questions may include:

- What updates were missing on that date? This is important to understand what vulnerabilities may have been exploited by the adversary.
- What accounts were used on that date?
- What new accounts have been created since that date?

What logs are available, and is there any indication that the actor is currently accessing systems?

Logs—such as antivirus, EDR, and virtual private network (VPN)—are an indicator of suspected compromise. Follow-up questions may include:

- Are logs being aggregated in a Security Information and Event Management (SIEM) solution—such as [Microsoft Sentinel](#), Splunk, ArcSight, and others—and

current? What is the retention period of this data?

- Are there any suspected compromised systems that are experiencing unusual activity?
- Are there any suspected compromised accounts that appear to be actively used by the adversary?
- Is there any evidence of active command and controls (C2s) in EDR, firewall, VPN, web proxy, and other logs?

As part of assessing the current situation, you might need an Active Directory Domain Services (AD DS) domain controller that was not compromised, a recent backup of a domain controller, or a recent domain controller taken offline for maintenance or upgrades. Also determine whether [multifactor authentication \(MFA\)](#) was required for everyone in the company and if [Azure Active Directory \(Azure AD\)](#) was used.

Step 2. Identify the LOB apps that are unavailable due to the incident

This step is critical in figuring out the quickest way to get systems back online while obtaining the evidence required.

Does the application require an identity?

- How is authentication performed?
- How are credentials such as certificates or secrets stored and managed?

Are tested backups of the application, configuration, and data available?

- Are the contents and integrity of backups regularly verified using a restore exercise? This is particularly important after configuration management changes or version upgrades.

Step 3. Determine the compromise recovery process

This step may be necessary if you have determined that the control plane, which is typically AD DS, has been compromised.

Your investigation should always have a goal of providing output that feeds directly into the CR process. CR is the process that removes attacker control from an environment and tactically increase security posture within a set period. CR takes place post-security breach. To learn more about CR, read the Microsoft Compromise Recovery Security Practice team's [CRSP: The emergency team fighting cyber attacks beside customers](#) blog article.

Once you have gathered the responses to the questions above, you can build a list of tasks and assign owners. A key factor in a successful incident response engagement is thorough, detailed documentation of each work item (such as the owner, status, findings, date, and time), making the compilation of findings at the end of the engagement a straightforward process.

DART recommendations and best practices

Here are DART's recommendations and best practices for containment and post-incident activities.

Containment

Containment can only happen once the analysis has determined what needs to be contained. In the case of ransomware, the adversary's goal is to obtain credentials that allow administrative control over a highly available server and then deploy the ransomware. In some cases, the threat actor identifies sensitive data and exfiltrates it to a location they control.

Tactical recovery will be unique for your organization's environment, industry, and level of IT expertise and experience. The steps outlined below are recommended for short-term and tactical containment steps your organization can take. To learn more about for long-term guidance, see [securing privileged access](#). For a comprehensive view of ransomware and extortion and how to prepare and protect your organization, see [Human-operated ransomware](#).

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

- Which user accounts were compromised?
- Which devices are affected?
- Which applications are affected?

Step 2: Preserve existing systems

- Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.
- Isolate compromised systems from the network, but do not shut them off.

- Isolate at least one known good domain controller in every domain—two is even better. Either disconnect them from the network or shut them down entirely. The object here is to stop the spread of ransomware to critical systems—identity being among the most vulnerable. If all your domain controllers are virtual, ensure that the virtualization platform's system and data drives are backed up to offline external media that is not connected to the network, in case the virtualization platform itself is compromised.
- Isolate critical known good application servers, for example SAP, configuration management database (CMDB), billing, and accounting systems.

These two steps can be done concurrently as new threat vectors are discovered. Disable those threat vectors and then try to find a known good system to isolate from the network.

Other tactical containment actions can include:

- [Reset the krbtgt password](#), twice in rapid succession. Consider using a [scripted, repeatable process ↗](#). This script enables you to reset the krbtgt account password and related keys while minimizing the likelihood of Kerberos authentication issues being caused by the operation. To minimize potential issues, the krbtgt lifetime can be reduced one or more times prior to the first password reset so that the two resets are done quickly. Note that all domain controllers that you plan to keep in your environment must be online.
- Deploy a Group Policy to the entire domain(s) that prevents privileged login (Domain Admins) to anything but domain controllers and privileged administrative-only workstations (if any).
- Install all missing security updates for operating systems and applications. Every missing update is a potential threat vector that adversaries can quickly identify and exploit. Microsoft Defender for Endpoint's [Threat and Vulnerability Management](#) provides an easy way to see exactly what is missing—as well as the potential impact of the missing updates.
 - For Windows 10 (or higher) devices, confirm that the current version (or n-1) is running on every device.
 - Deploy [attack surface reduction \(ASR\) rules](#) to prevent malware infection.
 - Enable all [Windows 10 security features](#).
- Check that every external facing application, including VPN access, is protected by multifactor authentication, preferably using an authentication application that is running on a secured device.

- For devices not using Defender for Endpoint as their primary antivirus software, run a full scan with [Microsoft Safety Scanner](#) on isolated known good systems before reconnecting them to the network.
- For any legacy operating systems, upgrade to a supported OS or decommission these devices. If these options are not available, take every possible measure to isolate these devices, including network/VLAN isolation, Internet Protocol security (IPsec) rules, and login restrictions, so they are only accessible to the applications by the users/devices to provide business continuity.

The riskiest configurations consist of running mission critical systems on legacy operating systems as old as Windows NT 4.0 and applications, all on legacy hardware. Not only are these operating systems and applications insecure and vulnerable, if that hardware fails, backups typically cannot be restored on modern hardware. Unless replacement legacy hardware is available, these applications will cease to function. Strongly consider converting these applications to run on current operating systems and hardware.

Post-incident activities

DART recommends implementing the following security recommendations and best practices after each incident.

- Ensure that best practices are in place for [email and collaboration solutions](#) to make it more difficult for attackers to abuse them while allowing internal users to access external content easily and safely.
- Follow [Zero Trust](#) security best practices for remote access solutions to internal organizational resources.
- Starting with critical impact administrators, follow best practices for account security including using [passwordless authentication](#) or MFA.
- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
 - For cloud and forest/domain administrative access, use Microsoft's [privileged access model \(PAM\)](#).
 - For endpoint administrative management, use the [local administrative password solution \(LAPS\)](#).
- Implement data protection to block ransomware techniques and to confirm rapid and reliable recovery from an attack.

- Review your critical systems. Check for protection and backups against deliberate attacker erasure or encryption. It's important that you periodically test and validate these backups.
- Ensure rapid detection and remediation of common attacks on endpoint, email, and identity.
- Actively discover and continuously improve the security posture of your environment.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

PAM

Using the [PAM](#) (formerly known as the tiered administration model) enhances Azure AD's security posture. This involves:

- Breaking out administrative accounts in a "planed" environment—one account for each level, usually four:
- Control Plane (formerly Tier 0): Administration of domain controllers and other crucial identity services, such as Active Directory Federation Services (ADFS) or Azure AD Connect. This also includes server applications that require administrative permissions to AD DS, such as Exchange Server.
- The next two planes were formerly Tier 1:
 - Management Plane: Asset management, monitoring, and security.
 - Data/Workload Plane: Applications and application servers.
- The next two planes were formerly Tier 2:
 - User Access: Access rights for users (such as accounts).
 - App Access: Access rights for applications.
- Each one of these planes will have a *separate administrative workstation for each plane* and will only have access to systems in that plane. Other accounts from other planes will be denied access to workstations and servers in the other planes through user rights assignments set to those machines.

The net result of the PAM is that:

- A compromised user account will only have access to the plane to which it belongs.
- More sensitive user accounts will not be logging into workstations and servers with a lower plane's security level, thereby reducing lateral movement.

LAPS

By default, Microsoft Windows and AD DS have no centralized management of local administrative accounts on workstations and member servers. This usually results in a common password that is given for all these local accounts, or at the very least in groups of machines. This enables would-be attackers to compromise one local administrator account, and then use that account to gain access to other workstations or servers in the organization.

Microsoft's [LAPS](#) mitigates this by using a Group Policy client-side extension that changes the local administrative password at regular intervals on workstations and servers according to the policy set. Each of these passwords are different and stored as an attribute in the AD DS computer object. This attribute can be retrieved from a simple client application, depending on the permissions assigned to that attribute.

LAPS requires the AD DS schema to be extended to allow for the additional attribute, the LAPS Group Policy templates to be installed, and a small client-side extension to be installed on every workstation and member server to provide the client-side functionality.

You can get LAPS from the [Microsoft Download Center](#).

Incident response playbooks

Examine guidance for identifying and investigating these types of attacks:

- [Phishing](#)
- [Password spray](#)
- [App consent grant](#)

Incident response resources

- [Overview](#) for Microsoft security products and resources for new-to-role and experienced analysts
- [Planning](#) for your Security Operations Center (SOC)
- [Process](#) for incident response process recommendations and best practices

- Microsoft 365 Defender incident response
- Microsoft Defender for Cloud (Azure)
- Microsoft Sentinel incident response

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021
- [Human-operated ransomware](#)
- [Rapidly protect against ransomware and extortion](#)
- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat](#) threat analytics report in the Microsoft 365 Defender portal
- [Microsoft DART ransomware case study](#)

Microsoft 365:

- [Deploy ransomware protection for your Microsoft 365 tenant](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)
- [Protect your Windows 10 PC from ransomware](#)
- [Handling ransomware in SharePoint Online](#)
- [Threat analytics reports for ransomware](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- [Find ransomware with advanced hunting](#)

Microsoft Azure:

- [Azure Defenses for Ransomware Attack](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Backup and restore plan to protect against ransomware](#)
- [Help protect from ransomware with Microsoft Azure Backup](#) (26-minute video)
- [Recovering from systemic identity compromise](#)
- [Advanced multistage attack detection in Microsoft Sentinel](#)
- [Fusion Detection for Ransomware in Microsoft Sentinel](#)

Microsoft Defender for Cloud Apps:

- [Create anomaly detection policies in Defender for Cloud Apps](#)

Microsoft Security team blog posts:

- [3 steps to prevent and recover from ransomware \(September 2021\)](#) ↗
- [A guide to combatting human-operated ransomware: Part 1 \(September 2021\)](#) ↗

Key steps on how Microsoft's DART conducts ransomware incident investigations.

- [A guide to combatting human-operated ransomware: Part 2 \(September 2021\)](#) ↗

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#) ↗

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#) ↗

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#) ↗

- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#) ↗

Microsoft DART ransomware case study

Article • 08/26/2022 • 7 minutes to read

Human-operated ransomware continues to maintain its position as one of the most impactful cyberattack trends world-wide and is a significant threat that many organizations have faced in recent years. These attacks take advantage of network misconfigurations and thrive on an organization's weak interior security. Although these attacks pose a clear and present danger to organizations and their IT infrastructure and data, they are a [preventable disaster](#).

The [Microsoft Detection and Response Team \(DART\)](#) responds to security compromises to help customers become cyber-resilient. DART provides onsite reactive incident response and remote proactive investigations. DART leverages Microsoft's strategic partnerships with security organizations around the world and internal Microsoft product groups to provide the most complete and thorough investigation possible.

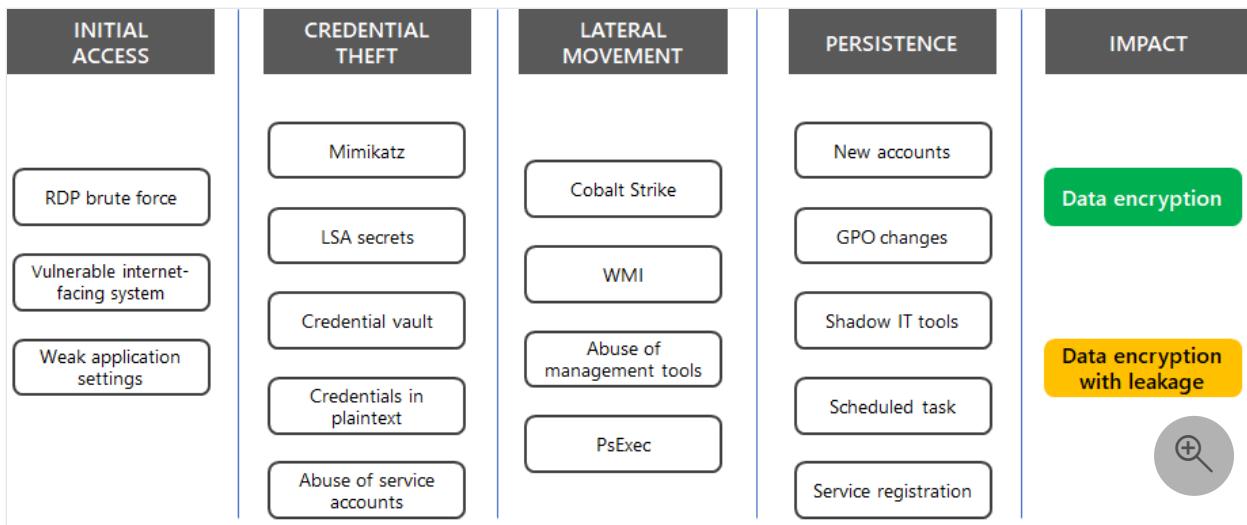
This article describes how DART investigated a recent ransomware incident with details on the attack tactics and detection mechanisms.

See [Part 1](#) and [Part 2](#) of DART's guide to combatting human-operated ransomware for more information.

The attack

DART leverages [incident response tools and tactics](#) to identify threat actor behaviors for human operated ransomware. Public information regarding ransomware events focuses on the end impact, but rarely highlights the details of the operation and how threat actors were able to escalate their access undetected to discover, monetize, and extort.

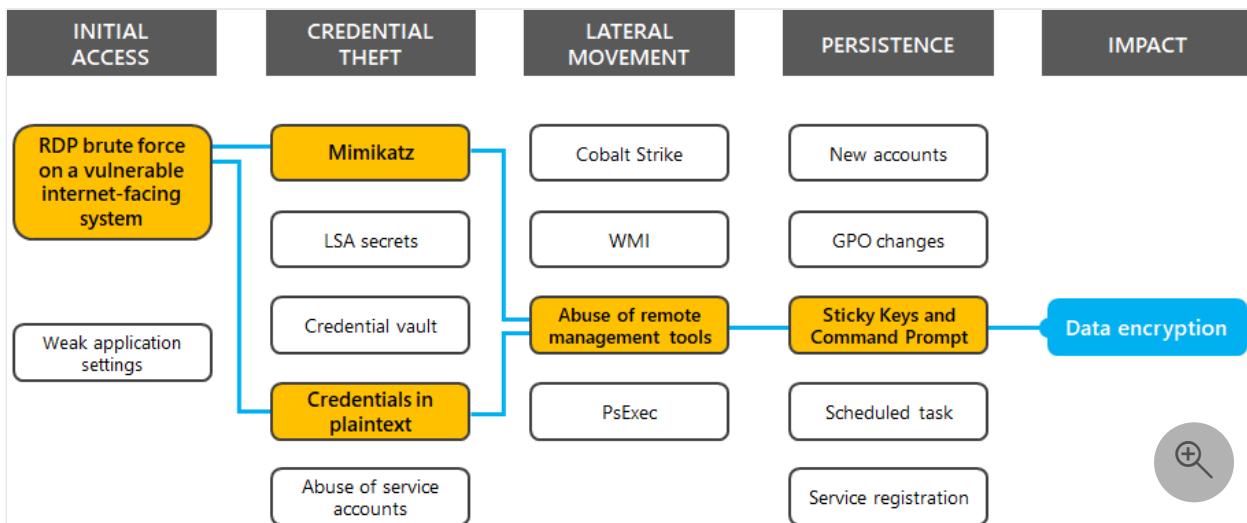
Here are some common techniques that attackers use for ransomware attacks based on [MITRE ATT&CK tactics](#).



DART used Microsoft Defender for Endpoint to track the attacker through the environment, create a story depicting the incident, and then eradicate the threat and remediate. Once deployed, Defender for Endpoint began detecting successful logons from a brute force attack. Upon discovering this, DART reviewed the security data and found several vulnerable Internet-facing devices using the Remote Desktop Protocol (RDP).

After initial access was gained, the threat actor used the Mimikatz credential harvesting tool to dump password hashes, scanned for credentials stored in plaintext, created backdoors with Sticky Key manipulation, and moved laterally throughout the network using remote desktop sessions.

For this case study, here is the highlighted path that the attacker took.



The following sections describe additional details based on the MITRE ATT&CK tactics and include examples of how the threat actor activities were detected with the Microsoft 365 Defender portal.

Initial access

Ransomware campaigns use well-known vulnerabilities for their initial entry, typically using phishing emails or weaknesses in perimeter defense such as devices with the enabled Remote Desktop service exposed on the Internet.

For this incident, DART was able to locate a device that had TCP port 3389 for RDP exposed to the Internet. This allowed threat actors to perform a brute-force authentication attack and gain the initial foothold.

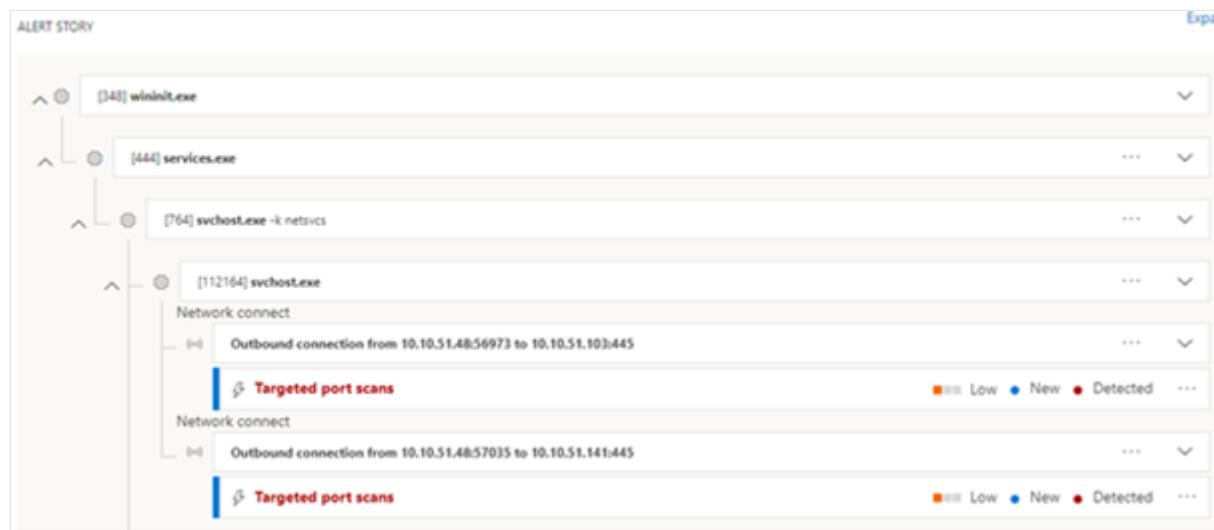
Defender for Endpoint used threat intelligence to determine that there were numerous sign-ins from known brute-force sources and displayed them in the Microsoft 365 Defender portal. Here's an example.

Reconnaissance

Once the initial access was successful, environment enumeration and device discovery began. These activities allowed the threat actors to identify information about the organization's internal network and target critical systems such as domain controllers, backup servers, databases, and cloud resources. After the enumeration and device discovery, the threat actors performed similar activities to identify vulnerable user accounts, groups, permissions, and software.

The threat actor leveraged Advanced IP Scanner, an IP address scanning tool, to enumerate the IP addresses used in the environment and perform subsequent port scanning. By scanning for open ports, the threat actor discovered devices that were accessible from the initially compromised device.

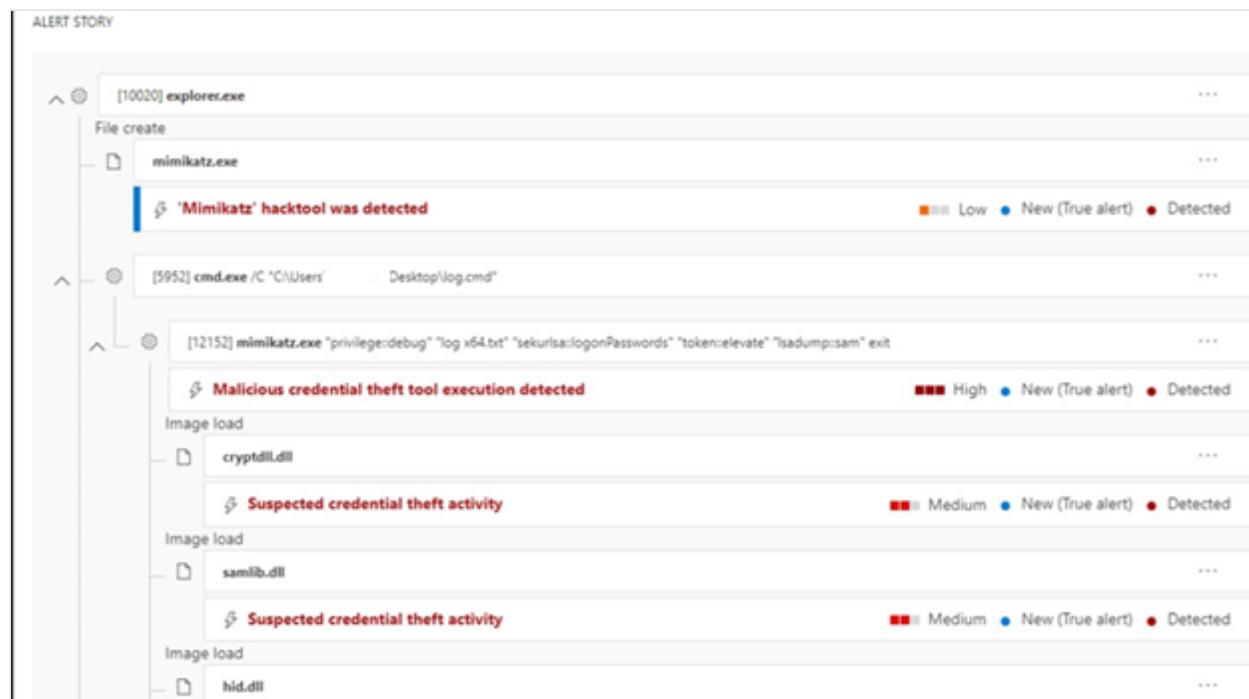
This activity was detected in Defender for Endpoint and used as an indicator of compromise (IoC) for further investigation. Here's an example.



Credential theft

After gaining initial access, the threat actors performed credential harvesting using the Mimikatz password retrieval tool and by searching for files containing “password” on initially compromised systems. These actions enabled the threat actors to access additional systems with legitimate credentials. In many situations, threat actors use these accounts to create additional accounts to maintain persistence after the initial compromised accounts are identified and remediated.

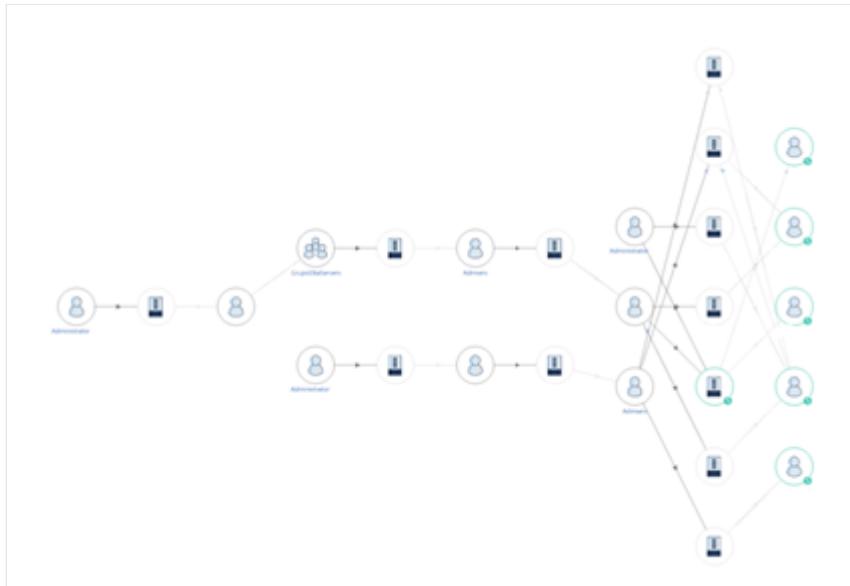
Here's an example of the detected use of the Mimikatz in the Microsoft 365 Defender portal.



Lateral movement

Movement across endpoints can vary between different organizations, but threat actors commonly use different varieties of remote management software that already exists on the device. By utilizing methods of remote access that the IT department commonly uses in their day-to-day activities, threat actors can fly under the radar for extended periods of time.

Using Microsoft Defender for Identity, DART was able to map out the path that the threat actor took between devices, displaying the accounts that were used and accessed. Here's an example.



Defense evasion

To avoid detection, the threat actors used defense evasion techniques to avoid identification and achieve their objectives throughout the attack cycle. These techniques include disabling or tampering with anti-virus products, uninstalling or disabling security products or features, modifying firewall rules, and using obfuscation techniques to hide the artifacts of an intrusion from security products and services.

The threat actor for this incident used PowerShell to disable real-time protection for Microsoft Defender on Windows 11 and Windows 10 devices and local networking tools to open TCP port 3389 and allow RDP connections. These changes decreased the chances of detection in an environment because they modified system services that detect and alert on malicious activity.

Defender for Endpoint, however, cannot be disabled from the local device and was able to detect this activity. Here's an example.

[143232] cmd.exe /C "C:\Users\...\Documents\rd.bat"	...
[47684] powershell.exe powershell Set-MpPreference -DisableRealtimeMonitoring \$true	...
↳ A suspicious file was observed	■■■ Medium ● New ● Detected ...
↳ Suspicious behavior by cmd.exe was observed	■■■ Medium ● New ● Detected ...
[136704] netsh.exe netsh advfirewall firewall add rule name="allow RemoteDesktop" dir=in protocol=TCP localport=3390 action=allow	...
↳ Suspicious behavior by cmd.exe was observed	■■■ Medium ● New ● Detected ...
↳ Suspicious Security Software Discovery	■■■■ Low ● New ● Detected ...
cmd.exe process performed Security Software Discovery by invoking netsh.exe	...
↳ Suspicious Security Software Discovery	■■■■ Low ● New ● Detected ...

Persistence

Persistence techniques include actions by threat actors to maintain consistent access to systems after efforts are made by security staff to regain control of compromised systems.

The threat actors for this incident used the Sticky Keys hack because it allows for remote execution of a binary inside the Windows operating system without authentication. They then used this capability to execute a Command Prompt and perform further attacks.

Here's an example of the detection of the Sticky Keys hack in the Microsoft 365 Defender portal.

[17996] explorer.exe	...
File create	...
zam.exe	...
↳ A suspicious file was observed	■■■ Medium ● New ● Detected ...
↳ Suspicious sequence of exploration activities	■■■■ Low ● New ● Detected ...
↳ Suspicious behavior by cmd.exe was observed	■■■ Medium ● New ● Detected ...
[112432] zam.exe	...
[81488] cmd.exe "cmd" /c "C:\Users\...\AppData\Local\Temp\AFBBtmp\8142tmp\8153.bat C:\Users\...\Documents\zam.exe"	...
↳ Suspicious behavior by cmd.exe was observed	■■■ Medium ● New ● Detected ...
[122228] reg-exe REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HelpPane.exe" /f /v Debugger /t REG_...	...
↳ Sticky Keys binary hijack detected	■■■ Medium ● New ● Detected ...

Impact

Threat actors typically encrypt files using applications or features that already exist within the environment. The use of PsExec, Group Policy, and Microsoft Endpoint Configuration Management are methods of deployment that allow an actor to quickly reach endpoints and systems without disrupting normal operations.

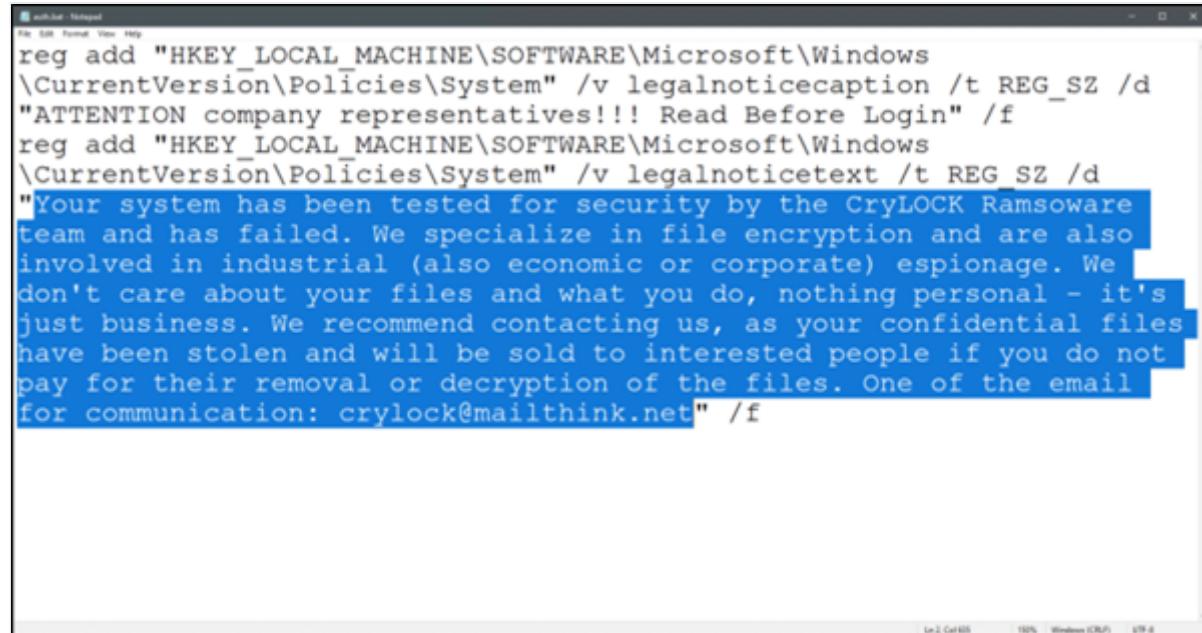
The threat actor for this incident leveraged PsExec to remotely launch an interactive PowerShell Script from various remote shares. This attack method randomizes distribution points and makes remediation more difficult during the final phase of the ransomware attack.

Ransomware execution

Ransomware execution is one of the primary methods that a threat actor uses to monetize their attack. Regardless of the execution methodology, distinct ransomware frameworks tend to have a common behavioral pattern once deployed:

- Obfuscate threat actor actions
- Establish persistence
- Disable windows error recovery and automatic repair
- Stop a list of services
- Terminate a list of processes
- Delete shadow copies and backups
- Encrypt files, potentially specifying custom exclusions
- Create a ransomware note

Here's an example of a ransomware note.



A screenshot of a Windows Notepad window titled "mof.bat - Notepad". The window contains the following text:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticecaption /t REG_SZ /d "ATTENTION company representatives!!! Read Before Login" /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticetext /t REG_SZ /d "Your system has been tested for security by the CryLOCK Ramsoware team and has failed. We specialize in file encryption and are also involved in industrial (also economic or corporate) espionage. We don't care about your files and what you do, nothing personal - it's just business. We recommend contacting us, as your confidential files have been stolen and will be sold to interested people if you do not pay for their removal or decryption of the files. One of the email for communication: crylock@mailthink.net" /f
```

Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021

- Human-operated ransomware
- Rapidly protect against ransomware and extortion
- 2021 Microsoft Digital Defense Report ↗ (see pages 10-19)
- Ransomware: A pervasive and ongoing threat ↗ threat analytics report in the Microsoft 365 Defender portal
- Microsoft DART ransomware approach and best practices

Microsoft 365:

- Deploy ransomware protection for your Microsoft 365 tenant
- Maximize Ransomware Resiliency with Azure and Microsoft 365 ↗
- Recover from a ransomware attack
- Malware and ransomware protection
- Protect your Windows 10 PC from ransomware ↗
- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware ↗ in the Microsoft 365 Defender portal

Microsoft 365 Defender:

- Find ransomware with advanced hunting

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Azure:

- Azure Defenses for Ransomware Attack ↗
- Maximize Ransomware Resiliency with Azure and Microsoft 365 ↗
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup ↗ (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel ↗

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021) ↗
- A guide to combatting human-operated ransomware: Part 1 (September 2021) ↗

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021) ↗

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#) ↗

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#) ↗

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#) ↗
- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#) ↗

Microsoft Security Best Practices module: Information protection and storage

Article • 06/08/2022 • 2 minutes to read

Intellectual property that is valuable to the organization (or its customers/constituents) requires security protection appropriate to its value.

See the [Storage, data, and encryption](#) and [Capabilities](#) topics for more information.

The following videos provide guidance on information protection and storage. You can also download the [PowerPoint slides](#) associated with these videos.

For more information about information protection capabilities across Microsoft 365 and SQL databases, see [CISO Workshop Module 5: Information Protection](#) and [Information protection and storage capabilities](#).

Part 1: Introduction (13:39)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4qm6e?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4qm6e?postJs||Msg=true)

Part 2: Storage and Encryption Best Practices (03:30)

[https://www.microsoft.com/en-us/videoplayer/embed/RE4q9Eg?postJs||Msg=true ↗](https://www.microsoft.com/en-us/videoplayer/embed/RE4q9Eg?postJs||Msg=true)

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Storage, data, and encryption

Article • 06/08/2022 • 3 minutes to read

Protecting data at rest is required to maintain confidentiality, integrity, and availability assurances across all workloads. Storage in a cloud service like Azure is [architected and implemented](#) quite differently than on premises solutions to enable massive scaling, modern access through REST APIs, and isolation between tenants.

Granting access to Azure storage is possible through Azure Active Directory (Azure AD) as well as key based authentication mechanisms (Symmetric Shared Key Authentication, or Shared Access Signature (SAS))

Storage in Azure includes a number of native security design attributes

- All data is encrypted by the service
- Data in the storage system cannot be read by a tenant if it has not been written by that tenant (to mitigate the risk of cross tenant data leakage)
- Data will remain only in the region you choose
- The system maintains three synchronous copies of data in the region you choose.
- Detailed activity logging is available on an opt-in basis.

Additional security features can be configured such as a storage firewall to provide an additional layer of access control as well as storage threat protection to detect anomalous access and activities.

Encryption is a powerful tool for security, but it's critical to understand its limits in protecting data. Much like a safe, encryption restricts access to only those with possession of a small item (a mathematical key). While it's easier to protect possession of keys than larger datasets, it is imperative that you provide the appropriate protections for the keys. Protecting cryptographic keys is not a natural intuitive human process (especially because electronic data like keys can be copied perfectly without a forensic evidence trail), so it is often overlooked or implemented poorly.

While encryption is available in many layers in Azure (and often on by default), we have identified the layers that are most important to implement (high potential for data to move to another storage medium) and are easiest to implement (near zero overhead).

Use Identity based storage access controls

Cloud service providers make multiple methods of access control over storage resources available. Examples include shared keys, shared signatures, anonymous access, and identity provider-based methods.

Identify provider methods of authentication and authorization are the least liable to compromise and enable more fine-grained role-based access controls over storage resources.

We recommend that you use an identity-based option for storage access control.

An example of this is [Azure Active Directory Authentication to Azure blob and queue services](#).

Encrypt virtual disk files

Virtual machines use virtual disk files as virtual storage volumes and exist in a cloud service provider's blob storage system. These files can be moved from on-premises to cloud systems, from cloud systems to on-premises, or between cloud systems. Due to the mobility of these files, you need to make sure the files and their contents are not accessible to unauthorized users.

Authentication-based access controls should be in place to prevent potential attackers from downloading the files to their own systems. In the event of a flaw in the authentication and authorization system or its configuration, you want to have a backup mechanism to secure the virtual disk files.

You can encrypt the virtual disk files to help prevent attackers from gaining access to the contents of the disk files in the event that an attacker is able to download the files. When attackers attempt to mount an encrypted disk file, they will not be able to because of the encryption.

We recommend that you enable virtual disk encryption.

An example of virtual disk encryption is [Azure Disk Encryption](#).

Enable platform encryption services

All public cloud service providers enable encryption that is done automatically using provider-managed keys on their platform. In many cases, this is done for the customer and no user interaction is required. In other cases, the provider makes this an option that the customer can choose to use or not to use.

There is almost no overhead in enabling this type of encryption as it's managed by the cloud service provider.

We recommend that for each service that supports service provider encryption that you enable that option.

An example of service-specific service provider encryption is [Azure Storage Service encryption](#).

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

Information protection and storage capabilities

Article • 06/07/2022 • 3 minutes to read

This article lists the capabilities that can help with information protection and storage.

Capabilities that work with Microsoft 365

Microsoft 365 and Office 365 include capabilities that can be applied to specific types of data to protect information across Microsoft 365 tools, including OneDrive, SharePoint Online, and mail. Some capabilities, like sensitive information types, can be used with Microsoft Defender for Cloud Apps to protect information across other SaaS apps in your environment.

Capability	More information
Sensitivity labels	<p>With sensitivity labels you can classify and help protect your sensitive content. Protection options include labels, watermarks, and encryption. Sensitivity labels use Azure Information Protection. If you are using Azure Information Protection labels, for now we recommend that you avoid creating new labels in other admin centers until after you've completed your migration. See Azure Information Protection migration.</p> <p>Retention labels are different than sensitivity labels. Retention labels help you retain or delete content based on policies that you define. These help organizations comply with industry regulations and internal policies.</p>
Data loss prevention (DLP)	<p>With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.</p>
Sensitive information types	<p>Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels. Sensitive information types can also be used with the Azure Information Protection scanner to classify and protect files on premises. Sensitive information types define how the automated process recognizes specific information types such as health service numbers and credit card numbers.</p>
Office 365 Message Encryption (OME)	<p>With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.</p>

Capability	More information
Azure Information Protection	<p>Azure Information Protection (sometimes referred to as AIP) helps an organization to classify, label, and optionally, protect documents and emails. Administrators can automatically apply labels by defining rules and conditions. Users can manually apply labels to files and mail. You can also give users recommendations about when to apply labels.</p> <p>If you're using sensitivity labels or Office Message Encryption, you're already using classification and protection capabilities. If you haven't yet migrated Azure Information Protection labels to Office 365, continue to manage these in Azure Information Protection.</p> <p>You can run the Azure Information Protection scanner on premises to classify and protect files on Windows Server, network shares, and SharePoint Server sites and libraries. This can be a first step toward identifying data to migrate to Office 365.</p>
Azure Information Protection with customer managed encryption key	<p>Some organizations have a business need or compliance requirement to retain control of an encryption key. This is not common. Azure Information Protection allows organizations to bring your own key (BYOK) to the service. For more information, see Bring your own key (BYOK) for Azure Information Protection.</p> <p>Another more complex option is offered for customers who have a requirement to retain an encryption key on premises, referred to as hold your own key (HYOK). For more information, see Hold your own key (HYOK) for Azure Information Protection.</p>

Azure storage and encryption

Capability	Description	More information
Azure Storage	Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables.	Azure Storage documentation
Azure encryption	Azure encryption options include encryption at rest, encryption in flight, and key management with Azure Key Vault	Azure encryption overview

Azure SQL Database

Capability	Description	More information
Azure SQL Database	Azure SQL Database is a general-purpose relational database, provided as a managed service. With it, you can create a highly available and high-performance data storage layer for the applications and solutions in Azure.	Azure SQL Database documentation

Capability	Description	More information
Azure SQL Database security capabilities	Security capabilities for data include Always encrypted and Transparent Data Encryption (TDE)	An overview of Azure SQL Database security capabilities

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).

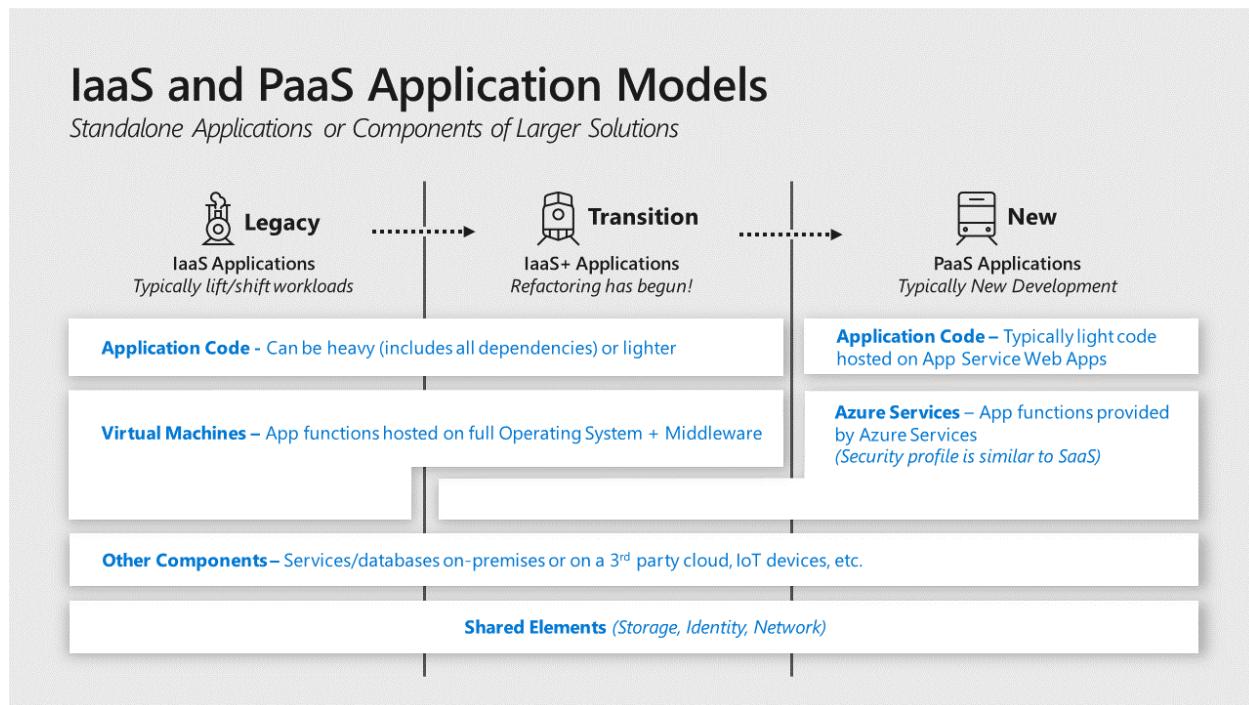
Applications and services

Article • 06/08/2022 • 16 minutes to read

Applications and the data associated with them ultimately act as the primary store of business value on a cloud platform. While the platform components like identity and storage are critical elements of the security environment, applications play an outsize role in risks to the business because:

- **Business Processes** are encapsulated and executed by applications and services need to be available and provided with high integrity
- **Business Data** is stored and processed by application workloads and requires high assurances of confidentiality, integrity, and availability.

This section focuses on applications written by your organization or by others on behalf of your organization vs. SaaS or commercially available applications installed on IaaS VMs.



Modern cloud platforms like Azure can host both legacy and modern generations of applications

- **Legacy** applications are hosted on Infrastructure as a Service (IaaS) virtual machines that typically include all dependencies including OS, middleware, and other components.
- **Modern** Platform as a Service (PaaS) applications don't require the application owner to manage and secure the underlying server operating systems (OSes) and

are sometimes fully "Serverless" and built primarily using functions as a service.

Notes: Popular forms of modern applications are application code hosted on Azure App Services and containerized applications (though containers can also be hosted on IaaS VMs or on-premises as well).

- **Hybrid** – While hybrid applications can take many forms, the most common is an "IaaS plus" state where legacy applications are transitioning to a modern architecture with modern services replacing legacy components or being added a legacy application.

Securing an application requires security assurances for three different component types:

- **Application Code** – This is the logic that defines the custom application that you write. The security of this code is the application owners' responsibility in all generations of application architecture including any open-source snippets or components included in the code. Securing the code requires identifying and mitigating risks from the design and implementation of the application as well as assessing supply chain risk of included components. Note that the evolution of applications into [microservices architectures](#) will break various aspects of application code into smaller services vs. a single monolithic codebase.
- **Application Services** – These are the various standardized components that the application uses such as databases, identity providers, event hubs, IoT device management, and so on. For cloud services this is a shared responsibility:
 - **Cloud Provider** - The security of the underlying service is the responsibility of the cloud provider
 - **Application Owner** - The application owner is responsible for security implications of the configuration and operation of the service instance(s) used by the application including any data stored and processed on the service.
- **Application Hosting Platform** – This is the computing environment where the application actually executes and runs. In an enterprise with applications hosted on premises, in Azure and in third-party clouds like Amazon Web Services (AWS), this could take many forms with significant variations on who is responsible for security:
 - **Legacy Applications** typically require a full operating system (and any middleware) hosted on physical or virtualized hardware. The virtual hardware can be hosted on premises or on Infrastructure as a Service (IaaS) VMs. This operating system and installed middleware/other components are operated and

secured by the application owner or their infrastructure team(s).

The responsibility for the physical hardware and OS virtualization components (virtualization hosts, operating systems, and management services) varies:

- **On premises** - The application owner or their organization is responsible for maintenance and security.
- **IaaS** – The cloud provider is responsible for maintenance and security of the underlying infrastructure and the application owner's organization is responsible for the VM configuration, operating system, and any components installed on it.
- **Modern Applications** are hosted on Platform as a Service (PaaS) environments such as an Azure application service. In most application service types, the underlying operating system is abstracted from the application owner and secured by the cloud provider. Application owners are responsible for the security of the application service configurations that are provided to them.
- **Containers** are an application packaging mechanism in which applications are abstracted from the environment in which they run. These containerized applications fit into either the legacy or modern models above depending on whether they are run on a container service by the cloud provider (Modern Applications) or on a server managed by the organization (on premises or in IaaS). See the [container security section](#) below for more details.

Identify and classify business critical applications

Ensure you have identified and classified the applications in your portfolio that are critical to business functions.

Enterprise organizations typically have a large application portfolio, so prioritizing where to invest time and effort into manual and resource-intensive tasks like threat modeling can increase the effectiveness of your security program.

Identify applications that have a high potential impact and/or a high potential exposure to risk.

- **High potential impact** – Identify application that would a significant impact on the business if compromised. This could take the form of one or more of:
 - **Business critical data** – Applications that process or store information, which would cause significant negative business or mission impact if an assurance of

confidentiality, integrity, or availability is lost.

- **Regulated data** – Applications that handle monetary instruments and sensitive personal information regulated by standards. For example, payment card industry (PCI) and Health Information Portability and Accountability Act (HIPAA).
- **Business critical availability** – Applications whose functionality is critical to organizations business mission such as production lines generating revenue, devices, or services critical to life and safety, and other critical functions.
- **Significant Access** – Applications which have access to systems with a high potential impact through technical means such as
 - *Stored Credentials* or keys/certificates that grant access to the data/service
 - *Permissions* granted via access control lists or other means
- **High exposure to attacks** – Applications that are easily accessible to attackers such as web applications on the open internet. Legacy applications can also be higher exposure as attackers and penetration testers frequently target them because they know these legacy applications often have vulnerabilities that are difficult to fix.

Adopt the DevOps approach

Organizations should shift from a 'Waterfall' development cycle to DevOps lifecycle of continuous integration, continuous delivery (CI/CD) for applications as fast as is practical. DevOps is the union of people, processes, and tools that enable continuous delivery of value to end users. The contraction of Dev and Ops refers to combining the development and operations disciplines into multi-disciplinary teams that work together with shared and efficient practices and tools.

The DevOps model increases the organization's ability to rapidly address security concerns without waiting for a longer planning and testing cycle of a waterfall model.

Follow DevOps security guidance

Organizations should leverage guidance and automation for securing applications on the cloud rather than starting from zero.

Using resources and lessons learned by external organizations that are early adopters of these models can accelerate the improvement of an organization's security posture with less expenditure of effort and resources.

- Microsoft has released a toolkit for Secure DevOps on Azure –
<https://azsk.azurewebsites.net/>
- Organization for Web App Security Project (OWASP) has published guidance
DevOps Pipeline security
https://www.owasp.org/index.php/OWASP_AppSec_Pipeline#tab=Main

Use Cloud services instead of custom implementations

Developers should use services available from your cloud provider for well-established functions like databases, encryption, identity directory, and authentication instead of writing custom versions of them.

These services provide better security, reliability, and efficiency because cloud providers operate and secure them with dedicated teams with deep expertise in those areas.

Using these services also frees your developer resources from reinventing the proverbial wheel so that they can focus development time on your unique requirements for your business. This practice should be followed to avoid risk during new application development as well as to reduce risk in existing applications either during planned update cycle or with a security-focused application update.

Several capabilities that should be prioritized first because of potential security impact:

- **Identity** – User directories and other authentication functions are complex to develop and critically important to security assurances. Avoid using homegrown authentication solutions and favor mature capabilities like Azure Active Directory ([Azure AD](#)), [Azure AD B2B](#), [Azure AD B2C](#), or third-party solutions to authenticate and grant permission to users, partners, customers, applications, services, and other entities.
- **Data Protection** – Developers should use established capabilities from cloud providers such as native encryption in cloud services to encrypt and protect data. The security world is littered with examples of failed attempts to protect data or passwords that didn't stand up to real world attacks. If direct use of cryptography is required, developers should call well-established cryptographic algorithms and not attempt to invent their own.
- **Key management** – Ideally use identity for authentication rather than directly handling keys (see [Prefer Identity Authentication over Keys](#)). For situations where accessing services that require access to keys, leverage a key management service like [Azure Key Vault](#) or AWS [Key Management Service](#) to manage and secure

these keys rather than attempting to safely handle keys in application code. You can use [CredScan](#) to discover potentially exposed keys in your application code.

- **Application Configurations** – Inconsistent configurations for applications can create security Risks. Azure App Configuration provides a service to centrally manage application settings and feature flags, which helps mitigate this risk.

Use Native Security capabilities in application services

Use native security capabilities built into cloud services instead of adding external security components (for data encryption, network traffic filtering, threat detection, and other functions).

Native security controls are maintained and supported by the service provider, eliminating or reducing effort required to integrate external security tooling and update those integrations over time. Cloud services evolve rapidly, which greatly increases the burden of maintaining an external tool and increases risk of losing security visibility and protections from these tools if the tool doesn't keep up with the cloud service.

- List of Azure Services
<https://azure.microsoft.com/services/>
- Native security capabilities of each service
</azure/security/common-security-attributes>

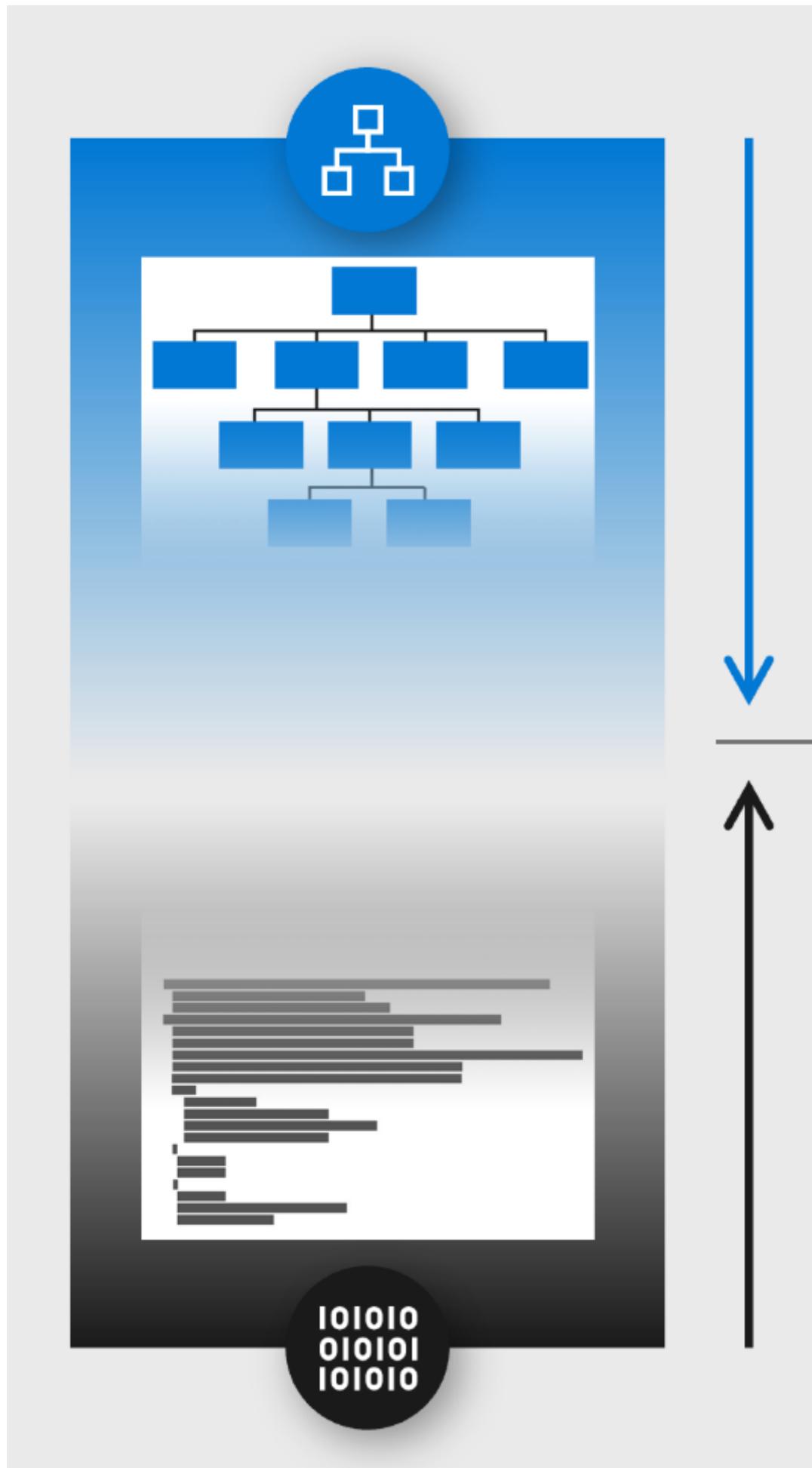
Prefer Identity Authentication over Keys

Always authenticate with identity services rather than cryptographic keys when available.

Managing keys securely with application code is difficult and regularly leads to mistakes like accidentally publishing sensitive access keys to code repositories like GitHub. Identity systems offer secure and usable experience for access control with built-in sophisticated mechanisms for key rotation, monitoring for anomalies, and more. Most organizations also have skilled teams dedicated to managing identity systems and few (if any) people actively managing key security systems.

For services that offer the Azure AD authentication like [Azure Storage](#), [Azure App Service](#), [Azure Backup](#), use it for authentication and authorization. To further simplify using identities for developers, you can also take advantage of [managed identities](#) to assign identities to resources like VMs and App Services so that developers don't have to manage identities within the application.

Bottom-up approach to reduce security bug volume and impact

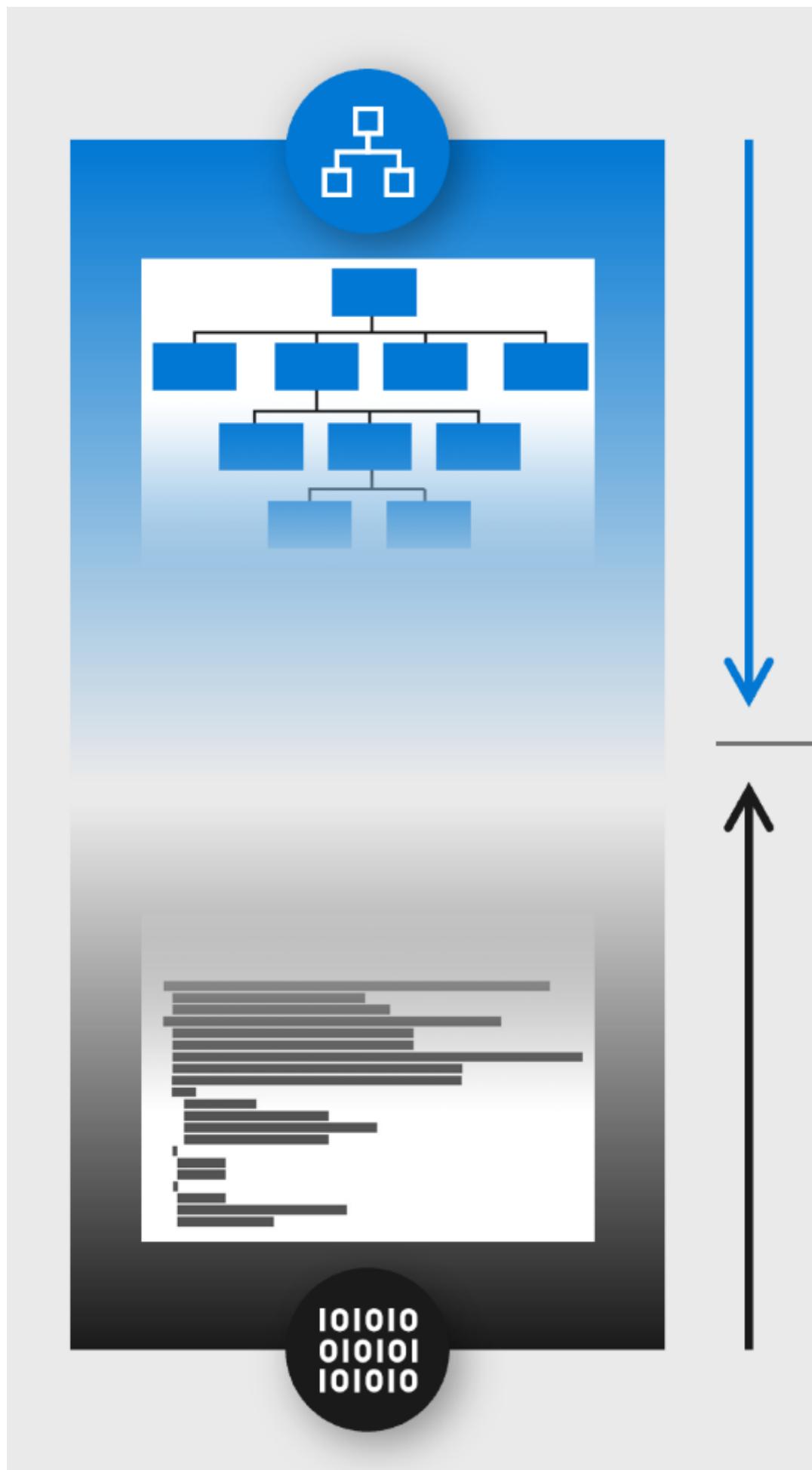


Reduce the count and potential severity of security bugs in your application by implementing security practices and tools during the development lifecycle.

Security bugs can result in an application disclosing confidential data, allowing criminals to alter data/records, or the data/application becoming unavailable for use by customers and employees. Applications will always have some logic errors that can result in security risk, so it is important to discover, evaluate, and correct them to avoid damage to the organization's reputation, revenue, or margins. It is easier and cheaper to resolve these earlier in the development lifecycle than it is to correct them after application has completed testing, is in production use, or has been breached frequently called "shift left" or "push left" principle.

Mitigating application risk is achieved by integrating security practices and tools into the development lifecycle, often called a secure development lifecycle (SDL or SDLC). Microsoft has published a number of recommendations in a whitepaper entitled [Develop Secure Apps on Azure](#) based on Microsoft's [Security Development Lifecycle](#) to mitigate common risks with input and output validation, perform fuzz testing, attack surface reviews, and more.

Top-down approach through threat modeling



Perform threat modeling on your business-critical applications to discover and mitigate potential risks to your organization.

Threat modeling identifies risks to the application itself as well as risks that application may pose to your enterprise particularly when evaluating individual applications in a larger system.

Threat modeling can be used at any stage of application development or production, but it is uniquely effective for the design stages of new functionality because no real-world data yet exists for that application.

Because threat modeling is a skill intensive exercise, we recommend taking measures to minimize time investment while maximizing security value:

1. **Prioritize by risk** - Apply threat modeling first to business-critical applications that would have an outsize impact on the business if compromised
2. **Limit Scope** - Perform threat modeling in progressive stages of detail to quickly identify quick wins and actionable mitigations before spending a lot of manual effort:
 - a. **Start with simple questions** method (See [Simple questions method](#)) documented below to quickly get insight into risks and whether basic protections are in place
 - b. **Progressively evaluate Application Design** – as resource and expertise are available, move to a more advanced analysis using the STRIDE method [Advanced threat modeling techniques](#) or another similar one already used by your team. Start with the architecture level design and progressively increase detail as time and resources allow:
 - i. **System level design** – includes applications and how they interact with each other
 - ii. **Application level** – includes components of the application and how they interact with each other
 - iii. **Component level** – includes how the individual component is composed and how each element of it interacts with each other
3. **Align with Development lifecycle** – Optimize your efforts by aligning threat modeling activities with your application development lifecycles.
 - a. **Waterfall** – ensure major projects should include threat modeling during the design process and during significant updates to the application.
 - b. **DevOps** – Trigger threat modeling activities at a frequency that adds security value without over-burdening the development teams. Good integration points

are during the introduction of significant features or changes to the application and a regular recurring calendar schedule for example, every quarter for business-critical applications.

- c. **Legacy applications** – These applications typically lack support, source code access, and/or expertise in the organization, so perform threat modeling on a best effort basis with what application knowledge/expertise you have available.

Simple questions method

This simple questioning method is designed to get security professionals and developers started on threat modelling before moving on to a more advanced method like STRIDE or OWASP's method (see, [Top-down approach through threat modeling](#)).

For each application or component, ask and answer these questions

- Are you authenticating connections using Azure AD, TLS (with mutual authentication), or another modern security protocol approved by your security team? This protects against unauthorized access to the application and data
 - Between users and the application (if applicable)
 - Between different application components and services (if applicable)
- Do you limit which accounts have access to write or modify data in the application to only those required to do so? This reduces risk of unauthorized data tampering/alteration
- Is the application activity logged and fed into a Security Information and Event Management (SIEM) via Azure Monitor or a similar solution? This helps the security team detect attacks and quickly investigate them.
- Is business-critical data protected with encryption that has been approved by the security team? This helps protect against unauthorized copying of data while at rest.
- Is inbound and outbound network traffic encrypted using TLS? This helps protect against unauthorized copying of data while in transit.
- Is the application protected against Distributed Denial of Service (DDoS) attacks using services like Azure DDoS protection, Akamai, or similar? This protects against attacks designed to overload the application so it can't be used

- Does the application store any sign in credentials or keys to access other applications, databases, or services? This helps identify whether an attack can use your application to attack other systems.
- Do the application controls allow you to fulfill security and privacy requirements for the localities you operate in? (This helps protect user's private data and avoid compliance fines)

Important: Security is a complex topic and the potential risks are limited only by the imagination of smart motivated attackers. These questions are designed to help identify readily discoverable gaps that are easily exploited by attackers. As you develop comfort and competencies with this method, you can look to grow your ability to threat model by progressing to advanced threat modelling techniques.

Advanced threat modeling techniques

A more comprehensive threat model can identify more potential risks, two popular techniques are STRIDE and OWASP

- **Microsoft** Security Development Lifecycle has documented a process of threat modeling in and released a free tool to assist with this process
 - This method evaluates application components and connections/relationships against potential risks, which map to the STRIDE mnemonic:
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Privilege Elevation
 - This method can be applied to any level of the design from the high level architectural specific application components.
- **OWASP** – The Open Web Application Security Project (OWASP) has documented a threat modeling approach for applications, which refers to STRIDE and other methods [https://www.owasp.org/index.php/Application_Threat_Modeling ↗](https://www.owasp.org/index.php/Application_Threat_Modeling)

Use Web Application Firewalls

Web application firewalls (WAFs) mitigate the risk of an attacker being able to exploit commonly seen security vulnerabilities for applications. While not perfect, WAFs provide a basic minimum level of security for web applications.

WAFs are an important mitigation as attackers target web applications for an ingress point into an organization similar to a client endpoint. WAFs are appropriate for both

- Organizations without a strong application security program as it's a critical safety measure(much like a parachute in a plane. Note that this shouldn't be the only planned safety mechanism to reduce the volume and severity of security bugs in your applications. For details, see [Reduce security bug volume and impact](#).
- Organizations who have invested in application security as WAFs provide a valuable additional defense in-depth mitigation. WAFs in this case act as a final safety mechanism in case a security bug was missed by security practices in the development lifecycle.

Microsoft includes WAF capabilities in [Azure Application Gateway](#) and many vendors offer these capabilities as standalone security appliances or as part of next generation firewalls.

Follow best practices for container security

Applications hosted in containers should follow general application best practices as well as some specific guidelines to manage this new application architecture type

Containerized applications face the same risks as any application and also adds new requirements to securely the hosting and management of the containerized applications.

Application containers architectures introduced a new layer of abstraction and management tooling (typically Kubernetes) that have increased developer productivity and adoption of DevOps principles.

While this is an emerging space that is evolving rapidly, several key lessons learned and best practices have become clear:

- **Use a Kubernetes managed service instead of installing and managing Kubernetes**
Kubernetes is a very complex system and still has a number of default settings that are not secure and few Kubernetes security experts in the marketplace. While this

has been improving in recent years with each release, there are still a lot of risks that have to be mitigated.

- **Validate container + container supply chain**

Just as you should validate the security of any open-source code added to your applications, you should also validate containers you add to your applications.

- Ensure that the practices applied to building the container are validated against your security standards like application of security updates, scanning for unwanted code like backdoors and illicit crypto coin miners, scanning for security vulnerabilities, and application of secure development practices.
- Regularly scan containers for known risks in the container registry, before use, or during use.

- **Set up registry of known good containers**

This allows developers in your organization to use containers validated by security rapidly with low friction. Additionally, build a process for developer to request and rapidly get security validation of new containers to encourage developers to use this process vs. working around it.

- **Don't run containers as root or administrator unless explicitly required**

Early versions of containers required root privileges (which makes attacks easier), but this is no longer required with current versions.

- **Monitor containers**

Ensure you deploy security monitoring tools that are container aware to monitor for anomalous behavior and enable investigation of incidents.

Next steps

For additional security guidance from Microsoft, see [Microsoft security documentation](#).