Microsoft

Maximize Ransomware Resiliency with Azure and Microsoft 365

October 2021

Acknowledgements

Author

Charles Iheagwara, Principal Program Manager

Contributors

Mark Simos, Director of Business Strategy

Jack Richins, Principal Program Manager

Joe Davies, Senior Technical Writer

Michele Myauo, Principal Engineering Manager

Gladys Rodriguez, Principal Cybersecurity Engineer

Terry Lanfear, Principal Content Developer

Table of Contents

1 Executive Summary

Ransomware and extortion are a high profit, low-cost business which has a debilitating impact on targeted organizations, national security, economic security, and public health and safety. What started as simple single-PC ransomware has grown to include a variety of extortion techniques directed at all types of corporate networks and cloud platforms.

This combination of real-time intelligence and broader criminal tactics, techniques and procedures has maximized the impact of these attacks and driven the level of profits from these attacks to levels that were hard to imagine a few years ago. To put it in perspective, the publicly reported profits from ransomware/extortion attacks gives these attackers a budget that would likely rival the budgets of nation state attack organizations (without even counting the profits from attacks that never made the headlines).

To ensure customers using Microsoft products are protected against ransomware attacks, this white paper addresses strategies to maximize ransomware resiliency using Microsoft security solutions. It includes recommended defensive best practices that when implemented ensures an organization maximizes both preventive and defensive capabilities to defeat ransomware attacks.

Microsoft offers a unique approach that empowers security professionals with both security information event management and extended detection and response (XDR) tools from a single vendor with an emphasis on integration so that defenders get the best of both worlds – end-to-end visibility across all of your resources, and intelligent alerts built with a deep understanding of individual resources and filtered with artificial intelligence.

Microsoft Azure Sentinel, a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution 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 Defender is an XDR that manifests itself in two tailored experiences, Azure Defender and Microsoft 365 Defender. Azure Defender protects Azure and hybrid environments and ensures cloud infrastructure resources are protected from common threats such as brute-forcing virtual machines, or attacking storage or SQL injection, or even mitigating threats against containers, the key management service or IoT devices.

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across devices (endpoints), identities, email, and applications to provide integrated protection against sophisticated attacks.

Our Azure native anti-lockout technologies ensure there is no ransomware lock up of the entire cloud portfolio. Advanced enterprise protection is also extended to all other Microsoft assets including collaboration, messaging, and Microsoft 365.

By implementing the best practices recommended in this white paper, you are taking measures that ensure your organization is optimally positioned to prevent, protect, and detect potential ransomware attacks targeted at your assets.

2 Introduction

The rise in popularity of ransomware—and its subsequent rise in fame—has led to a cybersecurity narrative that focuses on the intricacies of the ransomware payload itself and the novelty of encryption methods utilized. When successful, ransomware attacks can cripple a business core IT infrastructure and capacity and cause destruction that could have a debilitating impact on the physical, economic security or safety of a business. Ransomware attacks are targeted to businesses of all types. This requires that all businesses take preventive measures to ensure protection.

Successful ransomware usually exploits weaknesses or vulnerabilities in organizations' IT systems or infrastructure. The attacks are so obvious that it doesn't take much investigation to confirm that an organization has been attacked or to declare an incident. The exception might be a spam email that demands ransom in exchange for supposedly compromising materials. These types of incidents should be dealt with as spam, unless the email contains very specific information.

Recent trends on the number of attacks are quite alarming. While 2020 was not a good year for ransomware attacks on businesses, 2021 started on a bad trajectory. On May 7, the Colonial Pipeline (Colonial) attack temporarily shutdown services such as pipeline transportation of diesel, gasoline, and jet fuel. Colonial shut the critical fuel network supplying the populous eastern states.

Historically, cyberattacks were seen as a sophisticated set of actions targeting particular industries, which left the remaining industries believing they were outside the scope of cybercrime, and without context about which cybersecurity threats they should prepare for. Ransomware represents a major shift in this threat landscape, and it's made cyberattacks a very real and omnipresent danger for everyone. Encrypted and lost files and threatening ransom notes have now become the top-of-mind fear for most executive teams.

Ransomware's economic model capitalizes on the misperception that a ransomware attack is solely a malware incident, whereas in reality, ransomware is a breach involving human adversaries attacking a network.

For many organizations, the cost to rebuild from scratch after a ransomware incident far outweighs the original ransom demanded. With a limited understanding of the threat landscape and how ransomware operates, paying the ransom seems like the better business decision to return to operations. However, the real damage is often done when the cybercriminal exfiltrates files for release or sale, while leaving backdoors in the network for future criminal activity—and these risks persist whether or not the ransom is paid.

2.1 Infection process

A ransomware attack involves a threat actor deploying malware that infects a computer and restricts a user's access to the infected system or specific files in order to extort them for money. After the target system has been compromised, it typically locks out most interaction and displays an on-screen alert, usually stating that the system has been locked or that all files have been encrypted. It then demands a substantial ransom be paid before the system is released or files decrypted. In some cases, rather than just encrypt a victim's files and request a ransom in exchange for the decryption key, the attackers also exfiltrate sensitive data before deploying the ransomware. This prevents victims from disengaging from negotiations and raises the victim's (reputational) costs of not paying the ransom as the attackers likely will not only leave the victim's data encrypted but also leak sensitive information.

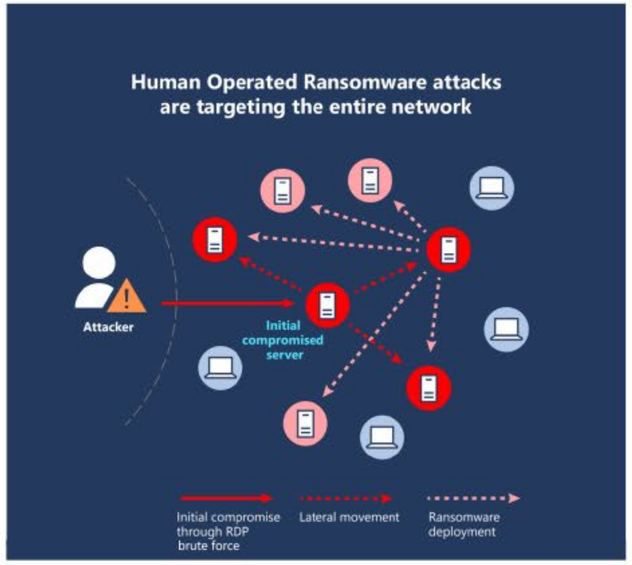


Figure 1: Typical infection chain

2.2 Common entry techniques

There are several ways an organization can be compromised by ransomware; the most common are through e-mail phishing attacks, web hosted malvertising, vulnerable network services and Remote Desktop Protocol (RDP) brute-force or stolen credentials.

- **Executing ransomware content within direct phishing emails** Such email includes a malicious attachment and a convincingly legitimate appearance to lure the recipient to open the attachment. Once the user opens the attachment, a binary executes and drops the ransomware on the system. Depending on the variant, it may then operate independently to lock out the system or securely communicate with a command-and-control service to receive further instructions before execution.
- **Connecting to a malicious web hosted malvertising or compromised site used to deliver ransomware.** Either the attacker sets up a malicious server or compromises a weak web server to deliver ransomware. Victims are then either actively directed to the site (for example, via a phishing or spear phishing attack) or casually (for example, via compromised web ad delivery). Their systems download the ransomware and execute it.
- **Compromising vulnerable network services.** In some cases, ransomware may be part of a larger, multipartite attack that leverages a worm attack on vulnerable networked services to insert the ransomware on the victim's device.
- **RDP brute-force or stolen credentials**. Most ransomware attacks involve brute-force or using lost or stolen credentials. Attackers use several methods to obtain the credentials. Quite often they have access to a large number of credentials amassed from past data breaches and leaked password lists over an extended period of time.

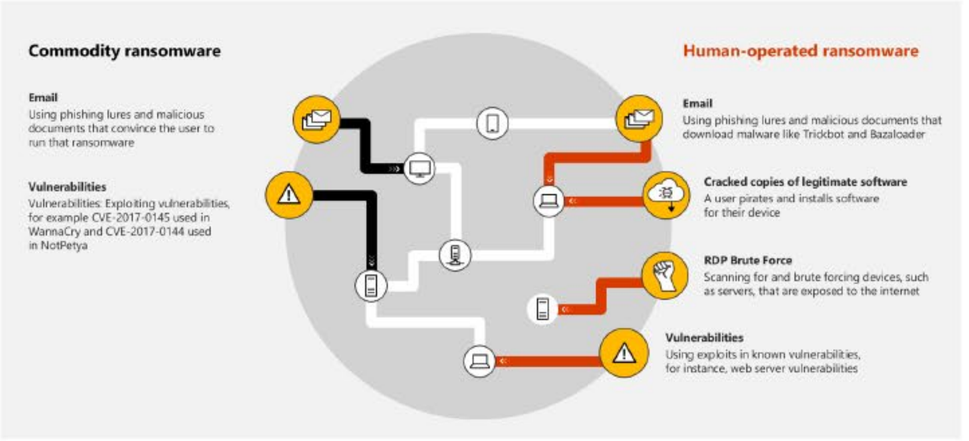


Figure 2: Example of known entry techniques into an organization

2.3 Command and control

The process of ransomware attack involves back and forth command and control (C2) callback methods for obtaining encryption keys and payment messaging. C2 communication is a vital stage in the kill chain during which time attackers issue commands to their payload. Encryption key management and payment messaging are typical use cases. Different ransomware variants use different communication methods. Some of the most prevalent ransomware variants resolve a domain name to an IP address to initiate this callback. Others use the other known methods such as DNS and TOR. For example, the SamSam variant uses a built-in encryption key that does not require a C2 callback, while other variants use Tor-based Onion Routing or IP-only callbacks that avoid DNS.

2.4 Kill chain

Understanding a bad actor's techniques is key to successful ransomware defense. In ransomware lexicon, the term "kill chain" refers to the ability to block an attack at any of these specific stages if the correct capabilities are deployed. The application of the kill chain concept helps organizations to deploy the capabilities that disrupts attack stages and ultimately the attack.

The cyber-attack lifecycle (first articulated by Lockheed Martin as the "kill chain") is a framework used to better understand and anticipate the moves of cyber adversaries at each stage of an attack.

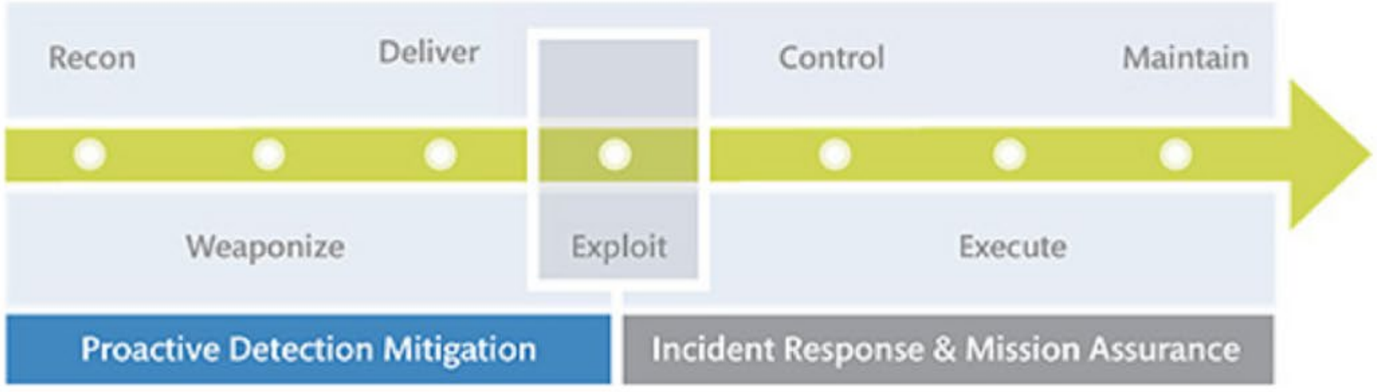


Figure 3: Cyber-attack lifecycle [source MITRE]

The following is a brief description of the stages as they are commonly understood across the security industry:

- **Reconnaissance:** Attackers gather information on their target
- **Weaponization:** Attackers develop their attack payload
- **Delivery:** Attackers launch their intrusion
- **Exploitation:** Attackers compromise their target
- **Installation:** Attackers gain persistence on their target
- **Command and control:** Attackers issue commands to their payload
- **Actions on objectives:** Attackers complete their end goal

2.5 Disrupting the kill chain

The application of the Kill Chain concept helps organizations to deploy the capabilities that disrupts attack step and the attack.

A holistic solution for ransomware may not detect each variant entry vector, but must detect, prevent, and respond to patterns used in ransomware. Detecting the conditions that lead up to compromise is important, but too broad. Detecting the behaviors that almost certainly lead to a system being ransomed is a discrete detection from the vulnerability.

To effectively defend against the kill chain, specific capabilities are necessary to build the appropriate layers of defense. Table 1 lists the functional description of the capabilities with select Microsoft solutions that fulfill the functions.

Microsoft's end-to-end ransomware protection solutions are intended to:

- Prevent ransomware from getting into the enterprise wherever possible
- Stop ransomware at the system level before it gains command and control
- Detect when ransomware is present and spreading in the network
- Work to contain ransomware from expanding to additional systems and network areas
- Performs incident response to fix the vulnerabilities and areas that were attacked

Table 1: Microsoft end-to-end capability

Capability (Focuses on Function rather than product)	Function	Microsoft solutions
Intrusion Prevention	lock attacks, exploitation, and intelligence gathering	Microsoft Defender Azure Firewall
Identity-based Firewall segmentation	Identity-based Firewall segmentation Authenticate access, separate traffic based on role and policy	Azure Active Directory Azure Firewall Azure WAF
Threat Intelligence	Knowledge of existing ransomware and communication vectors and learned knowledge in new threats	Sentinel Defender Azure Security Center Azure Network Watch
DNS Security	Block known malicious domains and break the command-and-control callback	DNS Sinkhole DNS resolver with dynamic deny list/allow list capability Azure DNS, if customer is using our Server
Email Security	Block ransomware attachments and links	Microsoft 365 Defender
Web Security	Block web communication to infected sites and files	WAF Azure Defender MCAS (Microsoft Cloud Application Security)
Network Antimalware	Enable antimalware protection to analyze all files that reach user systems, servers, and encrypted communications	Microsoft Antimalware for Azure
Client Security	Inspect files for ransomware and viruses, and then quarantine and remove	Azure Antimalware Azure Advanced Threat Protection
Network Monitoring	Monitor infrastructure communications using flow-based analytics – Identify and alert on abnormal traffic flows	Azure Monitor Network Watcher ExpressRoute Monitor Sentinel

3 Microsoft's Technologies are Engineered to Break the Kill Chain

The ransomware threat landscape is becoming more complex with increasing sophistication of attacks and wider attack surfaces. Security teams struggle to manage this environment with multiple solutions that are often not integrated. This results in serious ransomware threats avoiding detection due to data being collected and analyzed in silos, as well as security teams suffering from alert fatigue. Further pressure on resources is felt from a worldwide shortage of skilled security practitioners. Ransomware actors exploit vulnerabilities in infrastructures to gain a foothold. The kill chain can be disrupted with Microsoft solutions. Microsoft's Secure and Productive Enterprise is a suite of product offerings that have been purposely built to disrupt this cyber-attack kill chain while still ensuring an organization's employees remain productive.

Your organization needs intelligent, automated, integrated security to close the gaps, providing visibility and proactive response across the organization. Microsoft has invested in native security capabilities and building guidance for organizations to defend against ransomware attacks (and drive-up attacker cost).

Microsoft offers a unique solution architecture approach that empowers security professionals with both SIEM and extended detection and response (XDR) tools from a single vendor with an emphasis on integration so that cyber defenders get the best of both worlds – end-to-end visibility across all of your resources, and intelligent alerts built with a deep understanding of individual resources and filtered with AI.

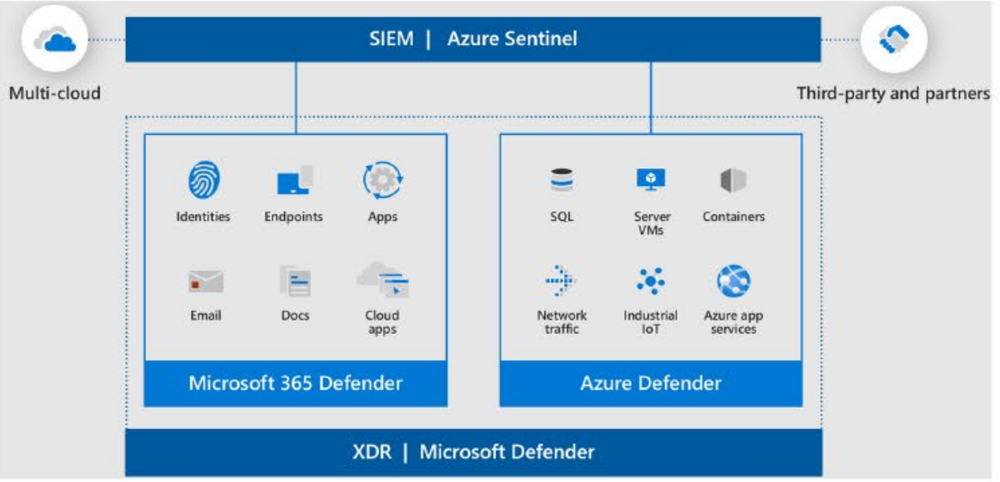


Figure 4: Integrated threat protection for your enterprise

With the combination of SIEM and XDR, security professionals and defenders can now focus on what's important, namely mitigating threats, armed with more context than ever, and spend less time on infrastructure, or the large volume of low fidelity signals.

Azure Sentinel -a cloud-native SIEM, delivers intelligent security analytics for your entire organization. You can connect to any of your security sources using built-in connectors and industry standards and then take advantage of artificial intelligence to correlate multiple low fidelity signals spanning multiple sources to create a complete view of a ransomware kill chain and prioritized alerts so that defenders can accelerate their time to evict adversaries.

Two of the key inputs to any SIEM for many customers are Microsoft 365 security data spanning users, devices (endpoints), applications, and infrastructure data from Microsoft Azure and hybrid environments including virtual machines, storage, or SQL databases.

Unlike other vendors that only have a SIEM and require defenders to filter through volumes of low fidelity data, Microsoft has complementary XDR capabilities in Microsoft Defender that have a detailed understanding of the Microsoft 365 and Microsoft Azure, apply artificial intelligence and automation at a resource level and filter out the most important alerts to surface in the SIEM. That capability we call Microsoft Defender delivers the broadest resource coverage of any XDR on the market today spanning users, devices, applications, virtual machines, SQL databases, IoT and much more all from a single vendor.

Microsoft Defender is an XDR that manifests itself in two tailored experiences, Azure Defender and Microsoft 365 Defender, so that security professionals cannot just identify issues but address them directly in the experiences they use every day.

Azure Defender protects Azure and hybrid environments and ensures your cloud infrastructure resources are protected from ransomware and other threats such as brute-forcing virtual machines, attacking storage or SQL injection, or even mitigating threats against containers, the key management service, or IoT devices. Azure Defender delivers protection for all these resources from directly within the Azure experience and extends protection to on-premises and multi-cloud virtual machines and SQL databases using Azure Arc. In addition, we have continued to enhance the threat protection capabilities with XDR now available for SQL on-premises and enhancements to container threat protection.

Microsoft Defender for Office 365 – This technology is designed to disrupt the "initial compromise" stage and raise the cost of successfully using phishing attacks. Most ransomware attackers leverage phishing emails containing malicious attachments or links pointing to watering hole sites. Microsoft Defender for Office 365 provides protection against both known and unknown malware and viruses in email, provides real-time (time-of-click) protection against malicious URLs, as well as enhanced reporting and trace capabilities. Messages and attachments are not only scanned against signatures powered by multiple antimalware engines and intelligence from Microsoft's Intelligent Security Graph, but are also routed to a special detonation chamber, run, and the results analyzed with machine learning and advanced analysis techniques for signs of malicious behavior to detect and block threats. Enhanced reporting capabilities also make it possible for security teams to quickly identify and respond to email-based attacks when they occur.

With the combination of SIEM and XDR, defenders can use the breadth of resource coverage of a SIEM coupled with the depth of understanding from XDR all in one seamlessly integrated and yet open package. Security operations teams are now empowered to spend less time on setting up and maintaining security systems, less time working through false alarms. You can now quickly identify threats – even never-before seen attacks – streamline threat investigation, and automate remediation. Now your team can focus on what matters, even as the threat landscape evolves.

Integrated Threat Protection Portfolio – Microsoft's best-in-breed threat protection portfolio includes point products to cover security for the critical components of the modern workplace. We have technologies that are integrated to disrupt the lateral movement phase by detecting lateral movement attack techniques early, allowing for rapid response. If an attacker still manages to get through the above defenses, compromise credentials, and moves laterally, other solutions provide a robust set of capabilities to detect this stage of an attack. Advance threat analytics is embedded Defender for Identity which uses both detection of known attack techniques as well as user-based analytics that learns what is "normal" for your environment so it can spot anomalies that indicate an attack.

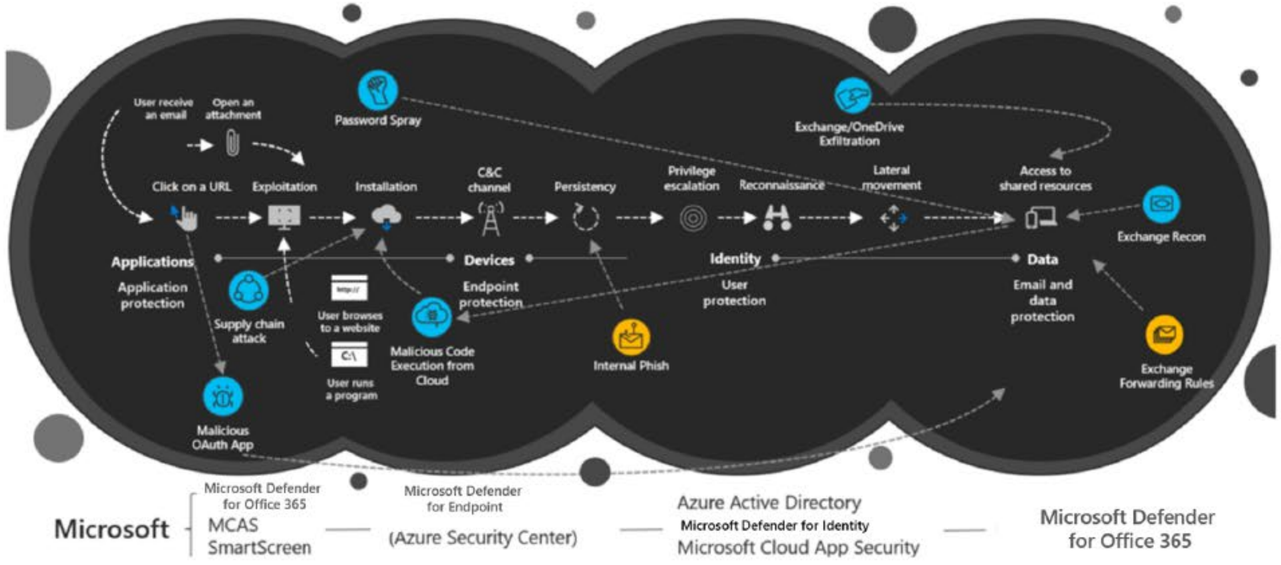


Figure 5: Integrated Microsoft security solutions

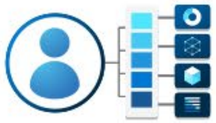
As shown in the Figure 5 above, each technology is designed to work seamlessly with other Microsoft security technologies together and provide security teams with visibility across the entire kill chain.

4 What Microsoft is Doing to Protect You

Microsoft as a security leader is continuously enhancing our products, services, and industry guidance to support customers to be ransomware resilient.

Products

Implementing ransomware alerting, mitigations, and resiliency into our products



Services

Global Team supporting customers with proactive ransomware mitigations and rapid ransomware recovery

Industry Guidance

Providing step-by-step ransomware readiness guidance to support customers

4.1 Approach

Microsoft's approach to ransomware protection is built around three primary axioms:

1. Protect Microsoft

Under this approach, we have maximized ransomware resiliency on our Azure infrastructure, Microsoft 365 platforms and other assets ensuring resilient capabilities for disaster recovery (for storage), isolation (for compute), and detection + response (for both):

- **Protecting storage** with disaster recovery
  - We store multiple copies of metadata and content in geo-distribution regions
  - If metadata is corrupted in Azure SQL we can restore for up to 30 days
  - We do not give capacity units the ability to overwrite or delete content in Azure Storage, only to create new blobs
- **Protecting compute** with isolation
  - It is an explicit design goal to prevent malware from being able to break out of a capacity unit to broadly impact our customers
  - There exist no credentials on a given capacity unit VM that can be used to move laterally to another VM within same the capacity unit
  - Likewise, there exist no credentials on a given capacity unit that can be used to move laterally to another capacity unit
- **Defending storage and compute** with detection and incident response
  - We have dedicated intrusion detection systems for metadata storage (Azure SQL), content storage (in Azure storage), and compute
  - These intrusion detection systems operate in near-real-time and are designed to detect unauthorized access, tampering, or deletion of content
  - These capabilities are exercised yearly by the Microsoft 365 pen-test team

2. Protect Microsoft customers

- Provide the tools & guidance for customers to protect themselves

3. Monitor and limit attackers

- Every person and organization has the right to expect the technology they use is secure and delivered by a company they can trust.
- Microsoft Threat Intelligence Center (MSTIC) works with Microsoft's Digital Crimes Unit to disrupt infrastructure and payment systems that enable ransomware attacks, including eliminating abuse of Microsoft cloud services by ransomware-affiliated threat actors. The response often includes immediate blocking and suspension as a trustworthy cloud provider and - in many cases - follow-up criminal investigations for legal action and law enforcement referrals
- Microsoft Detection and Response Team (DART) engages with customers globally to identify risks and provide reactive incident response and proactive security investigation services to help our customers manage their cyber-risk, especially in today's dynamic threat environment.

4.2 Ransomware lockup protection

Microsoft has implemented stringent measures that ensures there is no ransomware lock up of the entire cloud portfolio using the isolation, backup and defensive techniques:

1. Isolation – across offerings, services, data centers, and region.

- Azure actively tracks critical services and secrets to ensure isolation and partitioning to regional granularity.
- We strive to partition Azure with Business Continuity and Disaster Recovery (BCDR) to ensure failure in one region does not result in a global impact.
- Azure Infrastructure Identity has an isolated Identity tenant (AME) and isolated token service (dSTS) for infrastructure layers.
- Microsoft 365 isolates capacity unites with unique credentials

2. Backup – ensure critical systems are backed up and backups are protected against deliberate attacker erasure/encryption.

- Azure backs up critical data stores and performs disaster recovery drills for services
- Microsoft 365 stores multiples copies of metadata and content in geo-distribution regions, 30-day backups of metadata in SQL, and uses append only design for data in Azure Storage.

3. Defend – with detection and incident response

- Intrusion detection systems at all layers across Azure and Microsoft 365
- Pen testing done frequently
- MSTIC tracks adversaries in collaborations with M365, Azure, MTE, and Defender.
- MSTIC Threat Intelligence flows to our EPP/EDR products (Defender, Microsoft Defender for Endpoint) to protect our customers

4.3 Key vault protection

We have implemented effective measures to prevent any instance of Key Vault compromise:

- Key Vault, Storage, and Azure Backup support soft delete, meaning deletions can be recovered for some window (90 days by default for Key Vault)
- Key Vaults have 30 days of offline backups. As a best practice, critical services which persist service data such as Key Vault and Azure Active Directory (Azure AD) have offline backups
- When possible, services are designed to be stateless and can simply be redeployed

4.4 Hunt and evict

Microsoft has deployed all available resources to ensure no bad actor is allowed entry or stay on our platforms and infrastructure:

- Microsoft would leverage its Blue teams and detection pipelines to hunt intrusions and completely evict the adversary. Microsoft regularly practices such activity cross-company.
- Microsoft also practices cert and credential rotations to support evictions if necessary

4.5 Recovery

- Redeploy stateless systems - when possible, services are designed to be stateless and can simply be redeployed.
- Leverage soft delete recovery when possible (Key Vault, Azure Backup, and Azure Storage support soft-delete which can simply be reverted)
- Restore stateful systems without soft delete from Azure Archival Storage and other offline backups. Key Vault and Azure AD, for example, have 30 day offline backups)

Microsoft performs hundreds of compromise recoveries and has a tried-and-true methodology. Not only will it get you to a more secure position, but it also affords you the opportunity to consider your long-term strategy rather than reacting to the situation.

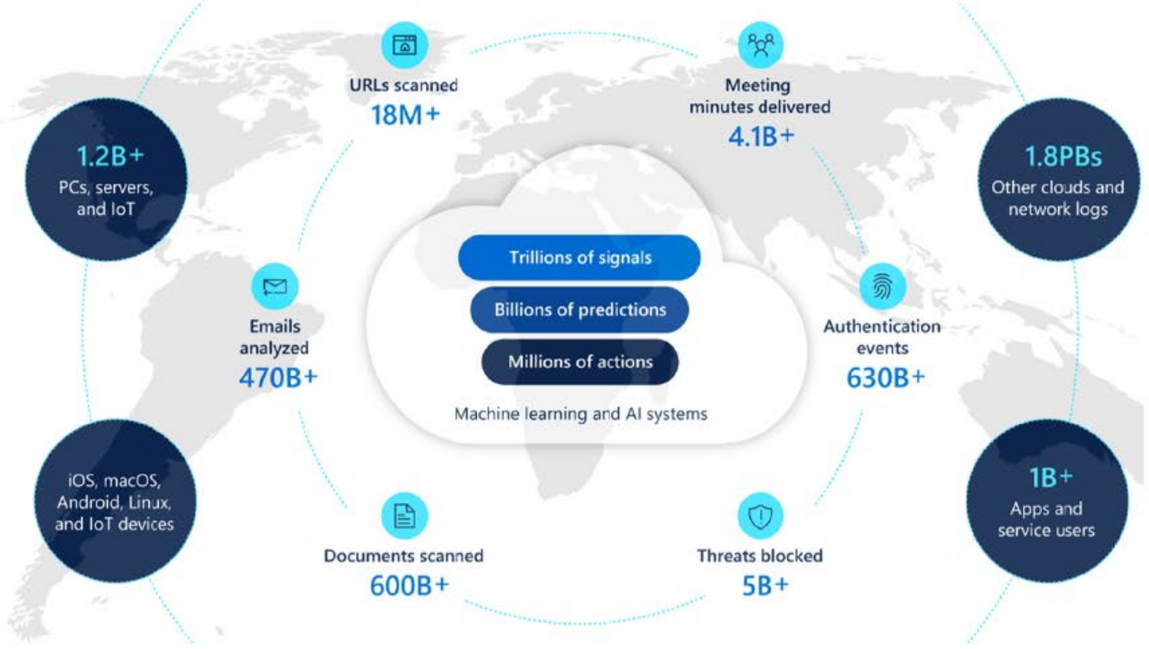


Figure 6: Monthly volume and diversity of signals used by Microsoft security operations

Because Microsoft serves billions of customers globally, we're able to aggregate security data from a broad and diverse spectrum of companies, organizations, and consumers, and this also means that we have a very unique vantage point. The unique insights informed by trillions of signals helps us stay ahead of attacks.

5 Azure Native Ransomware Protections

Microsoft has invested in native security capabilities that make Azure resilient against ransomware attacks. These controls help organizations defeat both high-volume, everyday commodity ransomware attacks and sophisticated targeted attacks.

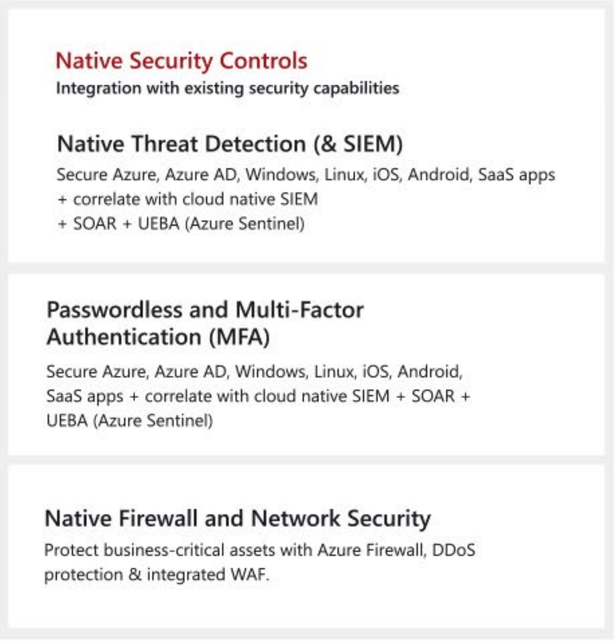
Native security controls

Key capabilities include:

- **Native threat detection:** Azure Defender provides high-quality threat detection and response capabilities called Extended Detection and Response (XDR). With XDR, you avoid using scarce security resources to build custom alerts using raw activity logs. Ensuring effective security monitoring can enable security teams to rapidly approve use of Azure services.
- **Passwordless and multi-factor authentication (MFA):** Azure MFA, Azure AD Authenticator App, and Windows Hello provide passwordless and MFA capabilities. These capabilities help protect accounts against common password attacks, which account for 99.9% of the identity attacks in Azure AD. While no security is perfect, eliminating password-only attack vectors dramatically lowers the ransomware attack risk to Azure resources.
- **Native firewall and network security:** Microsoft built native distributed denial of service (DDoS) attack mitigations, firewall, web application firewall, and many other controls into Azure. These "security as a service" controls help simplify security configuration and implementation. Organizations have the choice to use native Azure services or virtual appliance versions of familiar vendor capabilities to simplify their Azure security.

Microsoft Cloud App Security

Cloud App Security has anomaly detection policies, that include looking for Ransomware activity: [Create anomaly detection policies in Cloud App Security]



The Azure platform provides backup and recovery options through Azure Backup, as well as built into other data services and workloads.

6 Microsoft 365 Native Ransomware Protections

To help protect our customers from ransomware attacks, Microsoft has introduced capabilities in Microsoft 365 to prevent, detect, protect and disrupt a ransomware kill chain. New protection capabilities have also been added for file recovery from malicious attacks like ransomware, tools to help keep your information secure and private, and advanced protection from viruses and cybercrime.

6.1 Distinct capabilities

Detection and response

- Microsoft 365 engages in continuous security monitoring of its systems to detect and respond to threats to Microsoft 365 Services.
- Centralized logging collects and analyzes log events for activities that might indicate a security incident. Log data is analyzed as it gets uploaded to our alerting system and produces alerts in near real time.
- Cloud-based tools allow us to respond rapidly to detected threats. These tools enable remediation using automatically triggered actions.
- When automatic remediation is not possible, alerts are sent to the appropriate on-call engineers, who are equipped with a set of tools that enable them to act in real time to mitigate detected threats.

Ransomware detection & recovery — Office 365 can now detect ransomware attacks and help you restore your OneDrive to a point before files were compromised, so you don't have to submit to cybercriminal demands.

Files Restore — Files Restore allows you to restore your entire OneDrive to a previous point in time within the last 30 days. You can use this feature to recover from an accidental mass delete, file corruption, ransomware, or another catastrophic event.

Password protected sharing links — With the additional security option for links you share in OneDrive, you will now be able to set and require a password to access a shared file or folder. This prevents others from accessing your files if your intended recipient accidentally forwards or shares the link.

Email encryption — Email encryption in Outlook.com offers an added layer of protection and ensures end-to-end encryption of your email. Unlike Outlook.com, some email providers don't encrypt their connection, making it easy for hackers to intercept and read your communication.

As cybercriminals resort to tricking people into giving away their sign-in credentials or downloading viruses through malicious emails and links, we have added advanced protections to help keep Office 365 Home and Office 365 Personal subscribers safe with enterprise-grade security.

Advanced link checking in Word, Excel, and PowerPoint — With this feature, links you click in Word, Excel, and PowerPoint will also be checked in real-time to determine if the destination website is likely to download malware onto your computer or if it's related to a phishing scam. If the link is suspicious, you will be redirected to a warning screen recommending you don't access the site.

6.2 Domain level Protection

Microsoft has built in defenses and controls it uses to mitigate the risks of a ransomware attack against your organization and its assets. Assets can be organized by domain with each domain having its own set of risk mitigations.

6.2.1 Domain 1: Tenant level controls

The first domain is the people that make up your organization and the infrastructure and services owned and controlled by your organization. The following features in Microsoft 365 are on by default, or can be configured, to help mitigate the risk and recover from a successful compromise of the assets in this domain.

6.2.1.1 Exchange Online

- With single item recovery and mailbox retention, customers can recover items in a mailbox upon inadvertent or malicious premature deletion. Customers can rollback mail messages deleted within 14 days by default, configurable up to 30 days.
- Additional customer configurations of these retention policies within the Exchange Online service allow for:
  - configurable retention to be applied (1 year/10 year+)
  - copy on write protection to be applied
  - the ability for the retention policy to be locked such that immutability can be achieved
- Exchange Online Protection scans incoming email and attachments in real-time both entering and exiting the system. This is enabled by default and has filtering customizations available. Messages containing ransomware or other known or suspected malware are deleted. You can configure admins to receive notifications when this occurs.

6.2.1.2 SharePoint Online and OneDrive for Business Protection

SharePoint Online and OneDrive for Business Protection have built in features that help protect against ransomware attacks.

Versioning: As versioning retains a minimum of 500 versions of a file by default and can be configured to retain more, if the ransomware edits and encrypts a file, a previous version of the file can be recovered.

Recycle bin: If the ransomware creates a new encrypted copy of the file, and deletes the old file, customers have 93 days to restore it from the recycle bin.

Preservation Hold library: Files stored in SharePoint or OneDrive sites can be retained by applying retention settings. When a document with versions is subject to retention settings, versions get copied to the Preservation Hold library and exist as a separate item. If a user suspects their files have been compromised, they can investigate file changes by reviewing the retained copy. File Restore can then be used to recover files within the last 30 days.

6.2.1.3 Teams

Teams chats are stored within Exchange Online user mailboxes and files are stored in either SharePoint Online or OneDrive for Business. Microsoft Teams data is protected by the controls and recovery mechanisms available in these services.

6.2.2 Domain 2: Service level controls

The second domain is the people that make up Microsoft the organization, and the corporate infrastructure owned and controlled by Microsoft to execute the organizational functions of a business.

Microsoft's approach to securing its corporate estate is Zero Trust, implemented using our own products and services with defenses across our digital estate. You can find more details about the principles of Zero Trust here: Zero Trust Architecture.

Additional features in Microsoft 365 extend the risk mitigations available in domain 1 to further protect the assets in this domain.

6.2.2.1 SharePoint Online and OneDrive for Business Protection

Versioning: If ransomware encrypted a file in place, as an edit, the file can be recovered up to the initial file creation date using version history capabilities managed by Microsoft.

Recycle bin: If the ransomware created a new encrypted copy of the file, and deleted the old file, customers have 93 days to restore it from the recycle bin. After 93 days, there is a 14-day window where Microsoft can still recover the data. After this window, the data is permanently deleted.

6.2.2.2 Exchange Online

Database availability groups (DAG) help provide protection against corruption of mailbox data in Exchange Online. Exchange Online has 4 database availability groups, 4 active and 1 lagged by 14 days of delayed transaction logs.

If a ransomware attack affects the mailbox server that hosts the active copy of a mail transaction, failover to another active DAG takes place, transparent to customers. All three copies of a mail transaction in the active databases would have to be affected by the ransomware attack to fall back on the lagged DAG. Failure isolation mechanisms reduce the blast radius of a ransomware attack.

6.2.2.3 Teams

The risks mitigations for Teams outlined in domain 1 also apply to domain 2.

6.2.3 Domain 3: Developers & service infrastructure

The third domain is the people who develop and operate the Microsoft 365 service, the code, and infrastructure that delivers the service, and the storage and processing of your data.

Microsoft investments that secure the Microsoft 365 platform and mitigate the risks in this domain focus on these areas:

- Continuous assessment and validation of the security posture of the service
- Building tools and architecture that protect the service from compromise
- Building the capability to detect and respond to threats if an attack does occur

6.2.3.1 Continuous assessment and validation of the security posture

- Microsoft mitigates the risks associated with the people who develop and operate the Microsoft 365 service using the principle of **least privilege.** This means access and permissions to resources are limited to only what is necessary to perform a needed task.
- A Just-In-Time (JIT), Just-Enough-Access (JEA) model is used to provide Microsoft engineers with temporary privileges.
- Engineers must submit a request for a specific task to acquire elevated privileges.
- Requests are managed through Lockbox, which uses Azure role-based access control (RBAC) to limit the types of JIT elevation requests engineers can make

- In addition to the above, all Microsoft candidates are pre-screened prior to beginning employment at Microsoft. Employees who maintain Microsoft online services in the United States must undergo a Microsoft Cloud Background Check as a prerequisite for access to online services systems.
- All Microsoft employees are required to complete basic security awareness training along with Standards of Business Conduct training.

7 Ransomware Defensive Best Practices

Implementing ransomware resiliency requires you deploy the right tools and techniques and optimize systems configurations across the organization. In this Section, we outline nine ransomware protection strategies that ensures your organization maximizes both preventive and defensive capabilities to defeat ransomware attacks.

7.1 Email/Collaboration security

Implement best practices for email and collaboration solutions to make it more difficult for attackers to abuse them, while allowing internal users to easily and safely access external content.

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 for these attack vectors.

- **Enable** AMSI for Office VBA to detect Office macro attacks with endpoint tools like Defender for Endpoint
- **Implement advanced email security** using Defender for Office 365 or a similar solution
- Enable attack surface reduction (ASR) rules to block common attack techniques including
  - **Endpoint abuse** - Credential theft, ransomware activity, and suspicious use of PsExec and WMI
  - **Weaponized Office document** activity including advanced macro activity, executable content, process creation, and process injection initiated by Office applications.
- **Audit and monitor** – to find and fix deviations from baseline and potential attacks (see Detection and Response Plan)

7.2 Endpoint security

Implement relevant security features and rigorously follow software maintenance best practices for computers 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 provide attackers access to the organization's assets. Prioritize blocking common operating system and application with preventive controls to slow or stop them from executing the next stages.

Apply these best practices to all Windows, Linux, MacOS, Android, iOS, and other endpoints (as available):

Block known threats – with Attack surface reduction rules, tamper protection, and block at first site
Apply Security Baselines - to harden internet-facing Windows Servers, Windows Clients, and Office Applications
Maintain software – to avoid missing/neglecting manufacturer protections

- **Updated** - Rapidly deploy critical security updates for OS, browser, & email
- **Supported** – Update operating systems and software to currently support versions

Isolate, disable, or retire insecure systems and protocols – including unsupported operating systems and legacy protocols

Block unexpected traffic – using host-based firewall and network defenses
Audit and Monitor – to find and fix deviations from baseline and potential attacks

7.3 Remote access security

Follow zero trust security best practices for remote access solutions to internal organizational resources.

Attackers frequently use the organization's remote access solutions for the initial entry into the environment and for ongoing operations to damage internal resources.

- **Maintain software/Appliance** – to avoid missing/neglecting manufacturer protections (security updates, supported status)
- **Configure Azure AD** – for existing remote access, including enforcing zero trust user + device validation with Conditional Access (so that infected remote machines and compromised user accounts cannot communicate with the corporate network)
    - **Existing 3rd party VPN** – 3rd party VPNs (Cisco AnyConnect, Palo Alto Networks GlobalProtect & Captive Portal, Fortinet FortiGate SSL VPN, Citrix NetScaler, Zscaler Private Access (ZPA), and more)
    - **Azure VPN gateway**
- **Publish remote desktop** with Azure Active Directory Application Proxy
- **Move beyond VPN** by publishing apps with Azure AD Application Proxy
- **Secure access to Azure resources** - using Azure Bastion
- **Audit and monitor** – to find and fix deviations from baseline and potential attacks

7.4 Privileged access

Implement a comprehensive strategy to reduce risk of privileged access compromise. Build a multi-part strategy using the guidance at https://aka.ms/SPA including:

- **Enforce End-to-end session security** – to explicitly validate trust of users and workstations before allowing access to administrative interfaces (using Azure AD Conditional Access).
- **Protect & monitor identity systems** against privilege escalation attacks including Directories, Identity Management, Admin Accounts and groups, Consent grant configuration.
- **Mitigate lateral traversal** to ensure that compromising a single device will not immediately lead to control of many or all other devices using local account passwords, service account passwords, or other secrets
- **Ensure rapid threat response** to limit adversary access and time in the environment

All other security controls can easily be invalidated by an attacker with privileged access in your environment. Ransomware attack operators use privileged access as a quick path to control all critical assets in the organization for their extortion.

7.5 Accounts protection

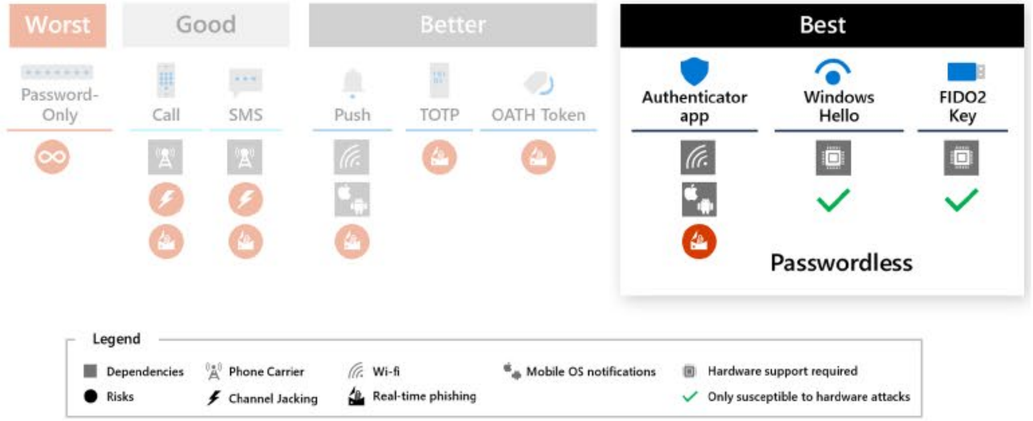
Starting with critical impact admins, rigorously follow best practices for account security including using passwordless or multi-factor authentication (MFA).

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 MFA was once a burdensome extra step, Passwordless approaches today improve the logon experience using biometric approaches that don't require you to remember or type a password. Additionally, zero trust approaches remember trusted devices, which reduce prompting for annoying out of band MFA actions.

- **Enforce Strong MFA or Passwordless logon** – for all users starting with administrators using one or more of:
  - **Passwordless Authentication** with Windows Hello or Authenticator App
  - Azure Multi-Factor Authentication (MFA)
  - **Third-party MFA** solution
- **Increase password security**
  - **Azure AD accounts** – Use Azure AD Identity Protection to block the use of known weak and custom passwords.
  - **On-Premises Active Directory Domain Services (AD DS) accounts** - Extend Azure AD Password Protection to your on-premises AD DS
- **Audit and monitor** – to find and fix deviations from baseline and potential attacks

Strong Multi-Factor Authentication

The best options aren't that difficult



7.6 Data protection

Implement data protection to ensure rapid and reliable recovery from a ransomware attack + block some techniques.

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.

- **Designate** Protected Folders – to make it more difficult for unauthorized applications to modify the data in these folders.
- **Review permissions** – to reduce risk from broad access enabling ransomware
  - **Discover broad write/delete permissions** on fileshares, SharePoint, and other solutions
  - **Reduce broad permissions** while meeting business collaboration requirements
  - **Audit and monitor** to ensure broad permissions don't reappear
- **Migrate your organization to the cloud:**
  - 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

7.7 Secure backups

Ensure critical systems are backed up and backups are protected against deliberate attacker erasure/encryption.

Ransomware attacks focus on crippling your organization's ability to respond without paying, frequently targeting backups and key documentation required for recovery (e.g., SolarWinds diagrams) to force organizations into paying extortion demands. Most organizations don't protect backup and restoration procedures against this level of intentional targeting.

- **Backup** all critical systems automatically on a regular schedule
- **Ensure rapid recovery** of business operations by regularly exercising business continuity / disaster recovery (BC/DR) plan
- **Protect backups** against deliberate erasure and encryption
  - **Strong protection** – Require out of band steps (like MUA/MFA) before modifying online backups (e.g. Azure Backup)
  - **Strongest protection** – Isolate backups from online/production workloads to enhance the protection of backup data.
- **Protect supporting documents** required for recovery such as restoration procedure documents, CMDB, and network diagrams

7.8 Detection and response plan

Ensure rapid detection and remediation of common attacks on endpoint, Web applications, and identity.

Minutes matter. Rapidly remediating common attack entry points to limit attacker's time to laterally traverse & do damage.

- **Prioritize common entry points** – Ransomware (and other) operators favor Endpoint/Email/Identity + RDP
  - **Integrated XDR** - Use integrated Extended Detection and Response (XDR) tools like Azure Defender and Microsoft 365 Defender to provide high quality alerts and minimize friction and manual steps during response
  - **Brute-force** - Monitor for brute-force attempts like password spray
- **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)
  - **Don't ignore commodity malware** - Ransomware attackers regularly purchase access to target organizations from dark markets
  - **Integrate outside experts** – into processes to supplement expertise, such as Microsoft Detection and Response Team (DART)
  - **Rapidly isolate** compromised computers using Defender for Endpoint

7.9 Incident handling process

To prepare for potential ransomware incidents, ensure your organization undertakes activities that roughly follow the incident response steps and guidance described in the US National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (Special Publication 800-61r2).

A proactive incident handling process entails instituting a multi phased approach specifically designed to contain a ransomware attack and assist in the return to service.

These steps include:

1. **Preparation:** This stage describes the measures to implement before an incident. Measures include both technical preparations, such as implementing suitable security controls and other technologies, and non-technical preparations, such as preparing processes and procedures.

2. **Triggers and detection:** This stage describes how ransomware might be detected, and the available triggers to initiate either further investigation or the declaration of an incident. Triggers are generally separated into high-confidence and low-confidence triggers.

3. **Investigation and analysis:** This stage describes the activities to undertake to investigate and analyze available data when it's not clear whether an incident has occurred. The goal is either confirming that an incident should be declared, or concluding that an incident has not occurred.

4. **Incident declaration:** This stage covers the steps to declare an incident. Incident declaration usually involves raising a ticket within the enterprise incident management ticketing system, and directing the ticket to the appropriate personnel for evaluation and action.

5. **Containment and mitigation:** This stage covers the steps that the SOC or others can take to contain, mitigate, or stop the incident, or limit the effects of the incident by using available tools, techniques, and procedures.

6. **Remediation and recovery:** This stage covers the steps to remediate or recover from damage the incident caused before it was contained and mitigated.

7. **Post-incident activity:** This stage covers the activities to perform once the incident has been closed. These activities can include capturing the final narrative associated with the incident and identifying lessons learned.

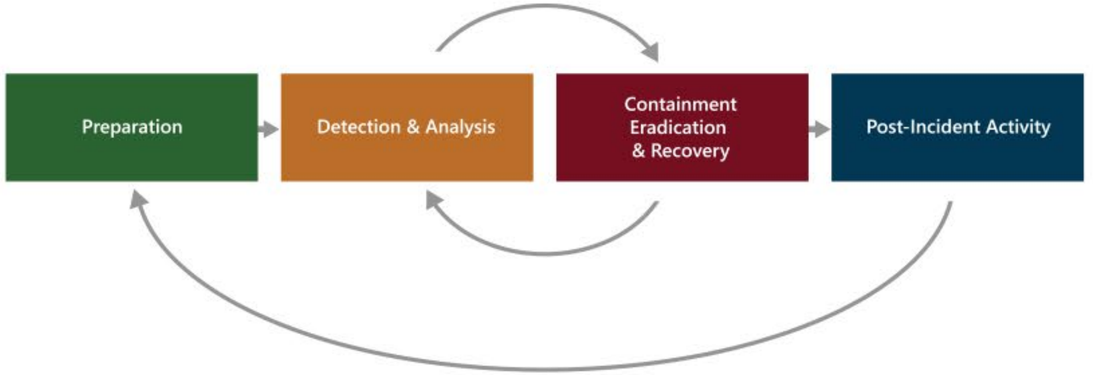


Figure 7: NIST SP 800-61r2 Computer Security Incident Response Life Cycle

8 Summary and Conclusion

The ransomware threat landscape is becoming more complex with increasing sophistication of attacks and wider attack surfaces. Security teams are struggling to manage this environment with multiple solutions that are often not integrated. This results in several ransomware threats avoiding detection due to data being collected and analyzed in silos, as well as security teams suffering from alert fatigue. Additional pressure on resources is felt from a worldwide shortage of skilled security practitioners.

Every organization needs intelligent, automated, integrated security to close the gaps, providing visibility and proactive response across the organization. Microsoft offers a unique approach that empowers security professionals with both SIEM and extended detection and response (XDR) tools from a single vendor with an emphasis on integration so that your cyber defenders get the best of both worlds – end-to-end visibility across all of your resources, and intelligent alerts built with a deep understanding of individual resources and filtered with Artificial Intelligence. With the combination of SIEM and XDR, security professionals can now focus on what's important, namely mitigating threats armed with more context than ever, and spending less time on infrastructure or the large volume of low fidelity signals.

With Azure Sentinel, a cloud-native SIEM, you can connect to any of your security sources using built-in connectors and industry standards and then take advantage of artificial intelligence to correlate multiple low fidelity signals spanning multiple sources to create a complete view of a ransomware kill chain and prioritized alerts so that defenders can accelerate their time to evict adversaries. Microsoft 365 Defender brings these best-of-breed products - Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Cloud App Security, Microsoft Defender for Office 365 - together into one powerful cross-domain full protection stack, deeply integrating signals and capabilities for an e nd-to-end experience protecting your organization's network.

Azure Defender, the integrated cloud workload protection platform of Azure Security Center allows you to detect and quickly respond to threats across hybrid cloud workloads. A new ransomware detection feature (connector) allows you to stream your Azure Defender security alerts from Azure Security Center into Azure Sentinel, so you can view, analyze, and respond to Defender alerts, and the incidents they generate, in a broader organizational threat context.

Microsoft as a leader in cybersecurity embraces the responsibility to make the world a safer place. This is reflected in our comprehensive approach to ransomware prevention and detection in our security framework, designs, products, legal efforts, industry partnerships, and services. We look forward to partnering with you in addressing ransomware in a holistic approach.

9 Resources

Microsoft Cloud Adoption Framework for Azure

Build great solutions with the Microsoft Azure Well-Architected Framework

Azure Top Security Best Practices

Security Baselines

Resource Center | Microsoft Azure

Azure Migration Guide

Security Compliance Management

Azure Security Control – Incident Response

Zero Trust Guidance Center

Azure Web Application Firewall

Azure VPN Gateway

Azure Multi-Factor Authentication (MFA)

Azure AD Identity Protection

Azure AD Conditional Access

The growing threat of ransomware, Microsoft On the Issues blog post on July 20, 2021

Human-operated ransomware

Rapidly protect against ransomware and extortion

The latest Microsoft Security Intelligence Report (see pages 22-24)

Deploy ransomware protection for your Microsoft 365 tenant

Recover from a ransomware attack

Protect your Windows 10 PC from ransomware

Handling ransomware in SharePoint Online

Find ransomware with advanced hunting

To report a ransomware breach, contact the FBI at:

IC3 Complaint Referral Form

Connect with us!

- AskAzureSecurity@microsoft.com
- https://www.microsoft.com/services
- https://sip.security.microsoft.com/homepage