Overview

October 24, 2021 6:40 PM

Is this exam for you?

Candidates for this exam should have subject matter expertise implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

From <https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>

Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code, security operations processes, cloud capabilities, and Azure services.

From <https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>

Objectives

October 24, 2021 6:52 PM

Clipped from:
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

Exam AZ-500: Microsoft Azure Security Technologies – Skills Measured

This exam was updated on September 29, 2021. Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that were made to the exam on that date.

NOTE: Passing score: 700. Learn more about exam scores here.

Audience Profile

Candidates for this exam should have subject matter expertise implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

Responsibilities for an Azure Security Engineer include managing the security posture, identifying and remediating vulnerabilities, performing threat modeling, implementing threat protection, and responding to security incident escalations.

Azure Security Engineers often serve as part of a larger team to plan and implement cloud-based management and security.

Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code, security operations processes, cloud capabilities, and Azure services.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Manage identity and access (30-35%)

Manage Azure Active Directory (Azure AD) identities

- create and manage a managed identity for Azure resources
- manage Azure AD groups
- manage Azure AD users
- manage external identities by using Azure AD
- manage administrative units

Manage secure access by using Azure AD

- configure Azure AD Privileged Identity Management (PIM)
- implement Conditional Access policies, including multifactor authentication
- implement Azure AD Identity Protection
- implement passwordless authentication
- configure access reviews

Manage application access

- integrate single sign-on (SSO) and identity providers for authentication
- create an app registration
- configure app registration permission scopes
- manage app registration permission consent
- manage API permissions to Azure subscriptions and resources
- configure an authentication method for a service principal

Manage access control

- configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- interpret role and resource permissions
- assign built-in Azure AD roles
- create and assign custom roles, including Azure roles and Azure AD roles

Implement platform protection (15-20%)

Implement advanced network security

- secure the connectivity of hybrid networks
- secure the connectivity of virtual networks
- create and configure Azure Firewall
- create and configure Azure Firewall Manager
- create and configure Azure Application Gateway
- create and configure Azure Front Door
- create and configure Web Application Firewall (WAF)
- configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure App Service
- configure network isolation for Web Apps and Azure Functions
- implement Azure Service Endpoints
- implement Azure Private Endpoints, including integrating with other services
- implement Azure Private Links
- implement Azure DDoS Protection

Configure advanced security for compute

- configure Azure Endpoint Protection for virtual machines (VMs)
- Implement and manage security updates for VMs
- configure security for container services
- manage access to Azure Container Registry
- configure security for serverless compute
- configure security for an Azure App Service
- configure encryption at rest
- configure encryption in transit

Manage security operations (25-30%)

Configure centralized policy management

- configure a custom security policy
- create a policy initiative
- configure security settings and auditing by using Azure Policy

Configure and manage threat protection

- configure Azure Defender for Servers (not including Microsoft Defender for Endpoint)
- evaluate vulnerability scans from Azure Defender
- configure Azure Defender for SQL
- use the Microsoft Threat Modeling Tool

Configure and manage security monitoring solutions

- create and customize alert rules by using Azure Monitor
- configure diagnostic logging and log retention by using Azure Monitor
- monitor security logs by using Azure Monitor
- create and customize alert rules in Azure Sentinel
- configure connectors in Azure Sentinel
- evaluate alerts and incidents in Azure Sentinel

Secure data and applications (25–30%)

Configure security for storage

- configure access control for storage accounts
- configure storage account access keys
- configure Azure AD authentication for Azure Storage and Azure Files
- configure delegated access

Configure security for data

- enable database authentication by using Azure AD
- enable database auditing
- configure dynamic masking on SQL workloads
- implement database encryption for Azure SQL Database
- implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB

Configure and manage Azure Key Vault

- create and configure Key Vault
- configure access to Key Vault
- manage certificates, secrets, and keys
- configure key rotation
- configure backup and recovery of certificates, secrets, and keys

The exam guide below shows the changes that were implemented on September 29, 2021. Note that the audience profile has been updated.

Audience Profile

Candidates for this exam should have subject matter expertise implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure~~and threat protection, managing identity and access, and protecting data, applications, and networks~~.

Responsibilities for an Azure Security Engineer include ~~maintaining~~ managing the security posture, identifying and remediating vulnerabilities, performing threat modeling ~~by using a variety of security tools~~, implementing threat protection, and responding to security incident escalations.

Azure Security Engineers often serve as part of a larger team to plan and implement cloud-based management and security ~~dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure~~.

~~A c~~Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code, ~~and~~ security operations processes, cloud capabilities, and Azure services~~. The Azure Security Engineer should have a strong familiarity with~~be familiar with scripting and automation, ~~and should have a deep understanding of networking and virtualization. A candidate should also have a strong familiarity with cloud capabilities, Azure products and services, and other Microsoft products and services~~.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Manage identity and access (30-35%)

Manage Azure Active Directory (Azure AD) identities

- create and manage a managed identity for Azure resources~~Configure security for service principals~~
- manage Azure AD ~~directory~~groups
- manage Azure AD users
- manage external identities by using Azure AD
- manage administrative units
- ~~configure password writeback~~
- ~~configure authentication methods including password hash and Pass-Through Authentication (PTA), OAuth, and passwordless~~
- ~~transfer Azure subscriptions between Azure AD tenants~~

Manage~~Configure~~ secure access by using Azure AD

- ~~monitor privileged access for Azure AD Privileged Identity Management (PIM)~~
- ~~configure Access Reviews~~
- configure Azure AD Privileged Identity Management (PIM)
- implement Conditional Access policies, including multifactor authentication
- implement~~Configure~~ Azure AD Iidentity Pprotection
- implement passwordless authentication
- configure access reviews

Manage application access

- integrate single sign-on (SSO) and ~~multiple~~ identity providers for authentication
- create an aApp rRegistration
- configure aApp rRegistration permission scopes
- manage aApp rRegistration permission consent
- manage API permissions~~access~~ to Azure subscriptions and resources
- configure an authentication method for a service principal

Manage access control

- configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- ~~configure subscription and resource permissions~~
- ~~configure resource group permissions~~
- ~~configure custom RBAC roles~~
- ~~identify the appropriate role~~
- interpret role and resource permissions
- assign built-in Azure AD roles
- create and assign custom roles, including Azure roles and Azure AD roles

Implement platform protection (15-20%)

Implement advanced network security

- secure the connectivity of ~~virtual~~ hybrid networks ~~(VPN authentication, Express Route encryption)~~
- secure the connectivity of virtual networks~~Configure Network Security Groups (NSGs) and Application Security Groups (ASGs)~~
- create and configure Azure Firewall
- create and configure ~~Implement~~ Azure Firewall Manager
- create and configure Azure ~~Configure Azure Front Door service as an~~ Application Gateway
- create and configure Azure Front Door
- create and configure ~~a~~ Web Application Firewall (WAF) ~~on Azure Application Gateway~~
- ~~configure Azure Bastion~~
- configure a resource firewall, including ~~on a~~ storage account, Azure SQL, Azure Key Vault, or Azure App Service
- configure network isolation for Web Apps and Azure Functions
- implement Azure Service Endpoints
- implement Azure Private Endpoints, including integrating with other services
- implement Azure Private Links
- implement Azure DDoS P~~p~~rotection

Configure advanced security for compute

- configure Azure E~~e~~ndpoint P~~p~~rotection for virtual machines (VMs)
- ~~configure and monitor system~~Implement and manage security updates for VMs
- ~~configure authentication for Azure Container Registry~~
- configure security for ~~different types of~~ container services
- manage access to Azure Container Registry
- configure security for serverless compute
- configure security for an Azure App Service
- configure encryption at rest

- configure encryption in transit
- ~~implement Azure Disk Encryption~~
- ~~configure authentication and security for Azure App Service~~
  - ~~configure SSL/TLS certs~~
  - ~~configure authentication for Azure Kubernetes Service~~
  - ~~configure automatic updates~~

Manage security operations (25-30%)

Configure centralized policy management

- configure a custom security policy
- create a policy initiative
- configure security settings and auditing by using Azure Policy

~~Monitor security by using Azure Monitor~~

- ~~create and customize alerts~~
- ~~monitor security logs by using Azure Monitor~~
- ~~configure diagnostic logging and log retention~~

Configure and manage threat protection~~Monitor security by using Azure Security Center~~

- configure Azure Defender for Servers (not including Microsoft Defender for Endpoint)
- evaluate vulnerability scans from Azure ~~Security Center~~Defender
- configure Azure Defender for SQL
- use the Microsoft Threat Modeling Tool
- ~~configure centralized policy management by using Azure Security Center~~
- ~~configure compliance policies and evaluate for compliance by using Azure Security Center~~
- ~~configure workflow automation by using Azure Security Center~~

Configure and manage security monitoring solutions~~Monitor security by using Azure Sentinel~~

- create and customize alert rules by using Azure Monitor
- configure diagnostic logging and log retention by using Azure Monitor
- monitor security logs by using Azure Monitor
- create and customize alert rules in Azure Sentinel
- configure ~~data sources to~~connectors in Azure Sentinel
- evaluate ~~results from~~alerts and incidents in Azure Sentinel
- ~~configure a playbook~~

~~Configure security policies~~

- ~~configure security settings by using Azure Policy~~
- ~~configure security settings by using Azure Blueprint~~

Secure data and applications (2~~5~~0–30~~2~~5%)

Configure security for storage

- configure access control for storage accounts
- configure ~~key management for~~ storage account access keys
- configure Azure AD authentication for Azure Storage and Azure Files
- ~~configure Azure AD Domain Services authentication for Azure Files~~
- configure delegated access
- ~~configure Storage Service Encryption~~
- ~~configure Azure Defender for Storage~~

Configure security for data~~bases~~

- enable database authentication by using Azure AD
- enable database auditing
- configure dynamic masking on SQL workloads
- ~~configure Azure Defender for SQL~~
- implement database encryption for Azure SQL Database
- implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB

Configure and manage Azure Key Vault

- create and configure Key Vault
- configure ~~Manage~~ access to Key Vault
- ~~manage permissions to secrets, certificates, and keys~~
  - ~~configure RBAC usage in Azure Key Vault~~
- manage certificates, secrets, and keys
- ~~manage secrets~~
- configure key rotation
- configure ~~B~~backup and recovery of certificates, secrets, and keys~~restore of Key Vault items~~
- ~~configure Azure Defender for Key Vault~~

Links

October 25, 2021 9:21 AM

MS Distro https://github.com/microsoft/CBL-Mariner

Learning Path https://docs.microsoft.com/en-us/learn/browse/?terms=az-500

Certification Poster Become Microsoft Certified

ESI Program Enterprise Skills Initiative: Welcome (microsoft.com)

GitHub labs MicrosoftLearning/AZ500-AzureSecurityTechnologies: Microsoft Azure Security Technologies (github.com)

Azure Security Architecture Diagrams Browse Azure Architecture - Azure Architecture Center | Microsoft Docs

shell.azure.com

https://docs.microsoft.com/en-us/learn/modules/azure-well-architected-security/

Manage Azure Active Directory (Azure AD) identities

October 24, 2021 6:51 PM

What is Azure Active Directory? - Azure Active Directory | Microsoft Docs
Compare Active Directory to Azure Active Directory | Microsoft Docs

Does not support legacy authentication ie Kerberos, NTLM

Pricing Pricing - Azure Active Directory | Microsoft Azure - know the tiers and what is in included in each tier Azure AD Multi-Factor Authentication versions and consumption plans | Microsoft Docs

SCIM https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/sync-scim

Azure AD Roles vs Azure Roles What's the difference between Azure roles and Azure AD roles? - Microsoft Tech Community

AD DS
Azure AD built-in roles - Azure Active Directory | Microsoft Docs
Manage emergency access admin accounts - Azure AD | Microsoft Docs

Conditional Access - Require MFA for administrators - Azure Active Directory | Microsoft Docs
Management concepts for Azure AD Domain Services | Microsoft Docs

- create and manage a managed identity for Azure resources

  Create & delete Azure AD B2C consumer user accounts in the Azure portal | Microsoft Docs
  Overview of user accounts in Azure Active Directory B2C | Microsoft Docs
  What is hybrid identity with Azure Active Directory? | Microsoft Docs

  > **Note**
  >
  > Not all Microsoft services are available in all locations. Before a license can be assigned to a user, you must specify the **Usage location**. You can set this value in the **Azure Active Directory** > **Users** > **Profile** > **Settings** area in Azure AD. Any user whose usage location is not specified inherits the location of the Azure AD organization.

- manage Azure AD groups
  Manage app & resource access using groups - Azure AD | Microsoft Docs
  Use Azure AD groups to manage role assignments - Azure Active Directory | Microsoft Docs
  Create a basic group and add members - Azure Active Directory | Microsoft Docs
  Change static group membership to dynamic - Azure AD | Microsoft Docs
  Create or edit a dynamic group and get status - Azure AD | Microsoft Docs
  Rules for dynamically populated groups membership - Azure AD | Microsoft Docs = max 5

- manage Azure AD users
  Add or delete users - Azure Active Directory | Microsoft Docs

- manage external identities by using Azure AD

- manage administrative units ****
  Administrative units in Azure Active Directory | Microsoft Docs
  Add and remove administrative units - Azure Active Directory | Microsoft Docs
  Assign and list roles with administrative unit scope - Azure Active Directory | Microsoft Docs

Passwordless
Azure Active Directory passwordless sign-in | Microsoft Docs
Passwordless sign-in with the Microsoft Authenticator app - Azure Active Directory | Microsoft Docs
Passwordless security key sign-in - Azure Active Directory | Microsoft Docs

Other links outside of scope of this course
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Azure Virtual Desktop documentation | Microsoft Docs
Microsoft Authentication Library Learn about MSAL - Microsoft identity platform | Microsoft Docs

Manage secure access by using Azure AD

October 25, 2021 9:23 AM

Azure Active Directory Connect

- What is Azure AD Connect and Connect Health. | Microsoft Docs
- Azure AD Connect: Prerequisites and hardware | Microsoft Docs
- Azure AD Connect: Supported topologies | Microsoft Docs

Azure AD Connect Cloud Sync

- What is Azure AD Connect cloud sync. | Microsoft Docs
- Azure AD Connect cloud sync deep dive - how it works | Microsoft Docs
- Azure AD Connect sync: Understanding the architecture - Azure | Microsoft Docs

- Azure AD Connect sync: Understand and customize synchronization | Microsoft Docs
- Azure AD Connect cloud sync FAQ | Microsoft Docs

Authentication

- What is password hash synchronization with Azure AD? | Microsoft Docs
- Azure AD Connect: Pass-through Authentication | Microsoft Docs
- What is federation with Azure AD? | Microsoft Docs
- Decision Tree Authentication for Azure AD hybrid identity solutions - Active Directory | Microsoft Docs
- Architecture Authentication for Azure AD hybrid identity solutions - Active Directory | Microsoft Docs

Password WriteBack

- Enable Azure Active Directory password writeback | Microsoft Docs
- Enable Azure Active Directory self-service password reset | Microsoft Docs

Azure AD MFA

Azure AD Multi-Factor Authentication overview | Microsoft Docs
Deployment considerations for Azure AD Multi-Factor Authentication | Microsoft Docs
Azure AD Multi-Factor Authentication versions and consumption plans | Microsoft Docs
Azure AD Multi-Factor Authentication versions and consumption plans | Microsoft Docs

MFA for Free & Security Defaults

Azure Active Directory security defaults | Microsoft Docs + Authenticator App

Extra information
https://github.com/Identity-Deployment-Guides/Identity-Deployment-Guides/tree/master/ADFS%20to%20AzureAD%20App%20Migration

Zero Trust
Learn Module Explore the Zero Trust security model - Learn | Microsoft Docs
2 Day Learning https://www.microsoft.com/en-ie/training-days/

configure Azure AD Privileged Identity Management (PIM)

Zero Trust Model - Modern Security Architecture | Microsoft Security

What is Privileged Identity Management? - Azure AD | Microsoft Docs
License requirements to use Privileged Identity Management - Azure Active Directory | Microsoft Docs
Start using PIM - Azure Active Directory | Microsoft Docs
Configure Azure AD role settings in PIM - Azure AD | Microsoft Docs

implement Conditional Access policies, including multifactor authentication

If This Then That
Configure the MFA registration policy - Azure Active Directory Identity Protection | Microsoft Docs
What is Conditional Access in Azure Active Directory? | Microsoft Docs
Conditional Access require terms of use - Azure Active Directory | Microsoft Docs
Conditional Access - Require MFA for administrators - Azure Active Directory | Microsoft Docs
Conditional Access - Require MFA for Azure management - Azure Active Directory | Microsoft Docs
Conditional Access - Require MFA for all users - Azure Active Directory | Microsoft Docs

Require MFA from untrusted networks - Azure Active Directory | Microsoft Docs
What is Conditional Access report-only mode? - Azure Active Directory | Microsoft Docs
The Conditional Access What If tool - Azure Active Directory | Microsoft Docs

implement Azure AD Identity Protection

What is Azure Active Directory Identity Protection? | Microsoft Docs
What is risk? Azure AD Identity Protection | Microsoft Docs
Risk policies - Azure Active Directory Identity Protection | Microsoft Docs
What is risk? Azure AD Identity Protection | Microsoft Docs
User Risk= User Behaviour
Sign-in Risk= Authentication request isn't authorized ie bot.

Configure the MFA registration policy - Azure Active Directory Identity Protection | Microsoft Docs
Azure AD Identity Protection policies | Microsoft Docs
What is risk? Azure AD Identity Protection | Microsoft Docs
Azure Active Directory Identity Protection notifications | Microsoft Docs
FAQs for Identity Protection in Azure Active Directory | Microsoft Docs

implement passwordless authentication

Azure Active Directory passwordless sign-in | Microsoft Docs
Passwordless sign-in with the Microsoft Authenticator app - Azure Active Directory | Microsoft Docs
Passwordless security key sign-in - Azure Active Directory | Microsoft Docs

configure access reviews

What are access reviews? - Azure Active Directory | Microsoft Docs
P2 License
Create an access review of Azure resource and Azure AD roles in PIM - Azure AD | Microsoft Docs
To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.

From <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review?toc=/azure/active-directory/governance/toc.json>

Manage application access

October 25, 2021 9:24 AM

- integrate single sign-on (SSO) and identity providers for authentication
- create an app registration
- configure app registration permission scopes
- manage app registration permission consent
- manage API permissions to Azure subscriptions and resources
- configure an authentication method for a service principal

Manage access control

October 25, 2021 9:24 AM

Shared Responsibility Model Shared responsibility in the cloud - Microsoft Azure | Microsoft Docs
Cloud Security Advantages Shared responsibility in the cloud - Microsoft Azure | Microsoft Docs

- configure Azure role permissions for management groups, subscriptions, resource groups, and resources

  Azure Hierarchy
  Organize your Azure resources effectively - Cloud Adoption Framework | Microsoft Docs

  Azure Policy
  Overview of Azure Policy - Azure Policy | Microsoft Docs
  Policy definitions for tagging resources - Azure Resource Manager | Microsoft Docs
  Tutorial: Manage tag governance - Azure Policy | Microsoft Docs
  Tutorial: Build policies to enforce compliance - Azure Policy | Microsoft Docs
  Assignments Overview of Azure Policy - Azure Policy | Microsoft Docs
  Understand how effects work - Azure Policy | Microsoft Docs

  Modelling
  Subscription decision guide - Cloud Adoption Framework | Microsoft Docs

  Azure Management Groups
  Organize your resources with management groups - Azure Governance - Azure governance | Microsoft Docs

  Classic subscription administrator roles, Azure roles, and Azure AD roles | Microsoft Docs
  What is Azure role-based access control (Azure RBAC)? | Microsoft Docs

  Azure subscription limits and quotas - Azure Resource Manager | Microsoft Docs
  Troubleshoot Azure RBAC | Microsoft Docs

  RBAC and Policy Overview of Azure Policy - Azure Policy | Microsoft Docs

  Transfer billing ownership of an Azure subscription | Microsoft Docs

- interpret role and resource permissions
  List Azure AD role assignments | Microsoft Docs
  List Azure role assignments using the Azure portal - Azure RBAC | Microsoft Docs
  Understand Azure deny assignments - Azure RBAC | Microsoft Docs

- assign built-in Azure AD roles
  Azure AD built-in roles - Azure Active Directory | Microsoft Docs
  Best practices for Azure AD roles - Azure Active Directory | Microsoft Docs

- create and assign custom roles, including Azure roles and Azure AD roles
  Create custom roles in Azure AD role-based access control | Microsoft Docs

Azure BluePrints (Preview as of Oct 25)
Overview of Azure Blueprints - Azure Blueprints | Microsoft Docs
Tutorial: Protect new resources with locks - Azure Blueprints | Microsoft Docs

Quotas
Check Azure resource usage against limits | Microsoft Docs

Resource Locks
Lock resources to prevent changes - Azure Resource Manager | Microsoft Docs
To create or delete management locks, you must have access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions.

From <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#who-can-create-or-delete-locks>

Azure Security Best Practices.pdf

Monday, October 25, 2021 2:34 PM

Clipped from:
https://azure.microsoft.com/mediahandler/files/resourcefiles/security-best-practices-for-azure-solutions/Azure%20Security%20Best%20Practices.pdf

Security best practices for Azure solutions

April 2019

Disclaimer

This document is for informational purposes only. MICROSOFT MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this white paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Executive summary

This paper is a collection of security best practices to use when you're designing, deploying, and managing your cloud solutions by using Microsoft Azure. These best practices come from our experience with Azure security and the experiences of customers like you.

This paper is intended to be a resource for IT pros. This might include designers, architects, developers, and testers who build and deploy secure Azure solutions.

For each best practice, our goal is to describe:

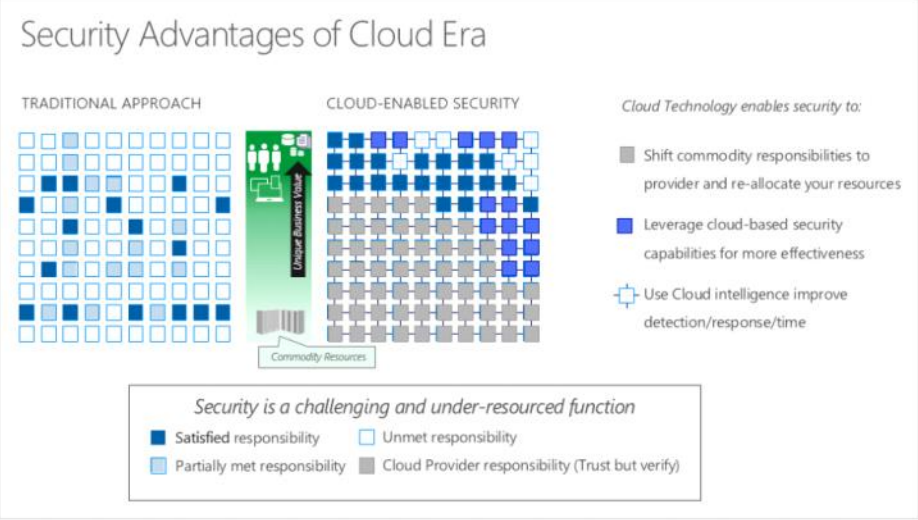
- What the practice is
- Why you want to enable it
- What might be the result if you don't enable it
- How you can learn to enable it
- Where to find detailed information

Table of Contents

Overview

Most consider the cloud to be more secure than corporate datacenters, as shown in the following figure. Organizations face many challenges with securing their datacenters, including recruiting and keeping security experts, using many security tools, and keeping pace with the volume and complexity of threats.

Azure is uniquely positioned to help organizations with these challenges. Azure helps protect business assets while reducing security costs and complexity. Built-in security controls and intelligence help admins easily identify and respond to threats and security gaps, so organizations can rapidly improve their security posture. By shifting responsibilities to Azure, organizations can get more security coverage—which enables them to move security resources and budget to other business priorities.

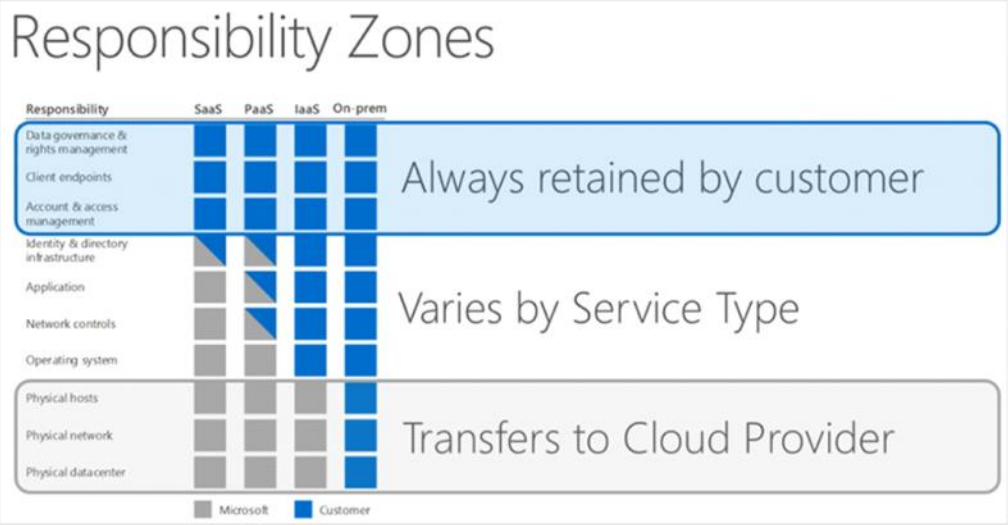


Understand the shared responsibility model for the cloud

It's important to understand the division of responsibility between you and Microsoft. On-premises, you own the whole stack. But as you move to the cloud, some responsibilities transfer to Microsoft.

Microsoft provides a secure foundation across physical, infrastructure, and operational security. Physical security refers to how Microsoft takes a multilayered approach to protect its datacenters. Network infrastructure, firmware and hardware, and continuous testing and monitoring make up the Azure infrastructure. Operational security consists of different security teams at Microsoft that work to mitigate risks across the security landscape.

The following figure shows the areas of the stack on-premises and in a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) deployment that you and Microsoft are responsible for.



For all cloud deployment types, you are responsible for protecting the security of your data, identities, on-premises resources, and the cloud components that you control (which vary by service type). Responsibilities that you always keep, regardless of the type of deployment, are:

- Data
- Endpoints
- Account
- Access management

Be sure that you understand the division of responsibility between you and Microsoft in a SaaS, PaaS, and IaaS deployment. For more details on the division of responsibility, see Shared Responsibilities for Cloud Computing.

Classify your data for cloud readiness

Classifying your data and identifying your data protection needs help you select the right cloud solution for your organization. Classifying (categorizing) stored data by sensitivity and business impact helps organizations determine the risks associated with the data. After the process is completed, organizations can manage their data in ways that reflect its value to them instead of treating all data the same way. Data classification enables organizations to find optimizations that might not be possible when all data is assigned the same value.

Data classification can yield benefits like compliance efficiencies, improved ways to manage the organization's resources, and facilitation of migration to the cloud. It's also worth noting that an organization must address data classification rules for data retention when moving to the cloud, and that cloud solutions can help mitigate risk. Some data protection technologies—such as encryption, rights management, and data loss prevention solutions—have moved to the cloud and can help mitigate cloud risks.

The downloadable white paper Data classification for cloud readiness provides guidance on classifying data.

Shared responsibility for compliance

Microsoft provides resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards. Because Azure has more certifications than any other cloud provider, you can deploy your critical workloads to Azure with confidence.

Recommended resources to help you stay compliant with regulatory standards are:

- Microsoft Azure Blueprints. Provides an automated way to deploy and govern cloud environments in a repeatable manner. A blueprint includes an industry-specific overview and industry-specific guidance, a customer responsibilities matrix, reference architectures with threat models, control implementation matrices, and automation to deploy reference architectures.
- Compliance Manager (in preview). Helps your organization by providing a holistic view of your data protection and compliance posture when you're using Microsoft cloud services. Compliance Manager helps you perform risk assessments and simplifies your compliance process by providing recommended actions, evidence gathering, and audit preparedness. Key features of Compliance Manager are:
    - Risk assessment capabilities, so you can assess your organization's Azure compliance posture for ISO 27001:2013 , HIPAA, and others.
    - Recommended actions that provide rich insight and direction to improve your data protection capabilities and compliance posture.
    - Simplified compliance that streamlines your organization's compliance and auditing workflow with built-in control management and audit-ready reporting tools.

Top security best practices to do now

We understand that you're busy and may not be able to immediately read this entire document. To help you get started fast, here are the top security best practices you can do now to secure your Azure solution:

- Upgrade your Azure subscription to Azure Security Center Standard. Security Center's Standard tier helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack.
- Store your keys and secrets in Azure Key Vault (and not in your source code). Key Vault is designed to support any type of secret: passwords, database credentials, API keys and, certificates.
- Install a web application firewall. Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities.
- Enforce multi-factor verification for users, especially your administrator accounts. Azure Multi-Factor Authentication (Azure MFA) helps administrators protect their organizations and users with additional authentication methods.

- Encrypt your virtual hard disk files to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.
- Connect Azure virtual machines and appliances to other networked devices by placing them on Azure virtual networks. Virtual machines connected to an Azure virtual network can connect to devices on the same virtual network, different virtual networks, the internet, or your own on-premises networks.
- Mitigate and protect against DDoS. Distributed denial of service (DDoS) is a type of attack that tries to exhaust application resources. Azure has two DDoS service offerings that help protect your network from attacks. DDoS Protection Basic is automatically enabled as part of the Azure platform. DDoS Protection Standard provides additional mitigation capabilities—beyond those of the Basic service tier—that are tuned specifically to Azure Virtual Network resources.

Strong operational security practices to implement every day are:

- Manage your VM updates. Azure VMs, like all on-premises VMs, are meant to be user managed. Azure doesn't push Windows updates to them. Ensure you have solid processes in place for important operations such as patch management and backup.
- Enable password management and use appropriate security policies to prevent abuse.
- Review your Security Center dashboard regularly to get a central view of the security state of all of your Azure resources and take action on the recommendations.

Optimize identity and access management

Things you can do to optimize identity and access management include:

- Treat identity as the primary security perimeter
- Centralize identity management
- Enable single sign-on
- Turn on conditional access
- Enable password management
- Enforce multi-factor verification for users
- Use role-based access control
- Lower exposure of privileged accounts
- Control locations where resources are located

Treat identity as the primary security perimeter

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defense can't be as effective as it was before the explosion of BYOD devices and cloud applications.

Azure Active Directory (Azure AD) is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access management, and identity protection into a single solution.

The following sections list best practices for identity and access security using Azure AD.

Centralize identity management

In a hybrid identity scenario, we recommend that you integrate your on-premises and cloud directories. Integration enables your IT team to manage accounts from one location, regardless of where an account is created. Integration also helps your users be more productive by providing a common identity for accessing both cloud and on-premises resources.

Best practice	Solution
Establish a single Azure AD instance. Consistency and a single authoritative source will increase clarity and reduce security risks from human errors and configuration complexity.	Designate a single Azure AD directory as the authoritative source for corporate and organizational accounts.
Integrate your on-premises directories with Azure AD.	Use Azure AD Connect to synchronize your on-premises directory with your cloud directory. **Note:** There are factors that affect the performance of Azure AD Connect. Ensure Azure AD Connect has enough capacity to keep underperforming systems from impeding security and productivity. Large or complex organizations (organizations provisioning more than 100,000 objects) should follow the recommendations to optimize their Azure AD Connect implementation.
Don't synchronize accounts to Azure AD that have high privileges in your existing Active Directory instance.	Don't change the default Azure AD Connect configuration that filters out these accounts. This configuration mitigates the risk of adversaries pivoting from cloud to on-premises assets (which could create a major incident).

Turn on password hash synchronization.	Password hash synchronization is a feature used to sync user password hashes from an on-premises Active Directory instance to a cloud-based Azure AD instance. This sync helps to protect against leaked credentials being replayed from previous attacks. Even if you decide to use federation with Active Directory Federation Services (AD FS) or other identity providers, you can optionally set up password hash synchronization as a backup in case your on-premises servers fail or become temporarily unavailable. This sync enables users to sign in to the service by using the same password that they use to sign in to their on-premises Active Directory instance. It also allows Identity Protection to detect compromised credentials by comparing synchronized password hashes with passwords known to be compromised, if a user has used the same email address and password on other services that aren't connected to Azure AD. For more information, see Implement password hash synchronization with Azure AD Connect sync.
For new application development, use Azure AD for authentication.	Use the correct capabilities to support authentication: ○ Azure AD for employees ○ Azure AD B2B for guest users and external partners ○ Azure AD B2C to control how customers sign up, sign in, and manage their profiles when they use your applications

Organizations that don't integrate their on-premises identity with their cloud identity can have more overhead in managing accounts. This overhead increases the likelihood of mistakes and security breaches.

Note: You need to choose which directories critical accounts will reside in and whether the admin workstation used is managed by new cloud services or existing processes. Using existing management and identity provisioning processes can decrease some risks but can also create the risk of an attacker compromising an on-premises account and pivoting to the cloud. You might want to use a different strategy for different roles (for example, IT admins vs. business unit admins). Your options are:

- Create Azure AD Accounts that aren't synchronized with your on-premises Active Directory instance. Join your admin workstation to Azure AD, which you can manage and patch by using Microsoft Intune.
- Use existing admin accounts by synchronizing to your on-premises Active Directory instance. Use existing workstations in your Active Directory domain for management and security.

Manage connected tenants

Your security organization needs visibility to assess risk and to determine whether the policies of your organization, and any regulatory requirements, are being followed. You should ensure that your security organization has visibility into all subscriptions connected to your production environment and network (via Azure ExpressRoute or site-to-site VPN). A Global Administrator/Company Administrator in Azure AD can elevate their access to the User Access Administrator role and see all subscriptions and managed groups connected to your environment.

See elevate access to manage all Azure subscriptions and management groups to ensure that you and your security group can view all subscriptions or management groups connected to your environment. You should remove this elevated access after you've assessed risks.

Enable single sign-on

In a mobile-first, cloud-first world, you want to enable single sign-on (SSO) to devices, apps, and services from anywhere so your users can be productive wherever and whenever. When you have multiple identity solutions to manage, this becomes an administrative problem not only for IT but also for users who have to remember multiple passwords.

By using the same identity solution for all your apps and resources, you can achieve SSO. And your users can use the same set of credentials to sign in and access the resources that they need, whether the resources are located on-premises or in the cloud.

Best practice	Solution
Enable SSO.	Azure AD extends on-premises Active Directory to the cloud. Users can use their primary work or school account for their domain-joined devices, company resources, and all of the web and SaaS applications that they need to get their jobs done. Users don't have to remember multiple sets of usernames and passwords, and their application access can be automatically provisioned (or deprovisioned) based on their organization group memberships and their status as an employee. And you can control that access for gallery apps or for your own on-premises apps that you've developed and published through the Azure AD Application Proxy.

Use SSO to enable users to access their SaaS applications based on their work or school account in Azure AD. This is applicable not only for Microsoft SaaS apps, but also other apps, such as Google Apps and Salesforce. You can configure your application to use Azure AD as a SAML-based identity provider. As a security control, Azure AD does not issue a token that allows users to sign into the application unless they have been granted access through Azure AD. You can grant access directly, or through a group that users are a member of.

Organizations that don't create a common identity to establish SSO for their users and applications are more exposed to scenarios where users have multiple passwords. These scenarios increase the likelihood of users reusing passwords or using weak passwords.

Turn on conditional access

Users can access your organization's resources by using a variety of devices and apps from anywhere. As an IT admin, you want to make sure that these devices meet your standards for security and compliance. Just focusing on who can access a resource isn't sufficient anymore.

To balance security and productivity, you need to think about how a resource is accessed before you can make a decision about access control. With Azure AD conditional access, you can address this requirement. With conditional access, you can make automated access control decisions—based on conditions—for accessing your cloud apps.

Best practice	Solution
Manage and control access to corporate resources.	Configure Azure AD conditional access based on a group, location, and application sensitivity for SaaS apps and Azure AD–connected apps.
Block legacy authentication protocols.	Attackers exploit weaknesses in older protocols every day, particularly for password spray attacks. Configure conditional access to block legacy protocols. See the video Azure AD: Do's and Don'ts for more information.

Enable password management

If you have multiple tenants or you want to enable users to reset their own passwords, it's important that you use appropriate security policies to prevent abuse.

Best practice	Solution
Set up self-service password reset (SSPR) for your users.	Use the Azure AD self-service password reset feature.
Monitor how or if SSPR is really being used.	Monitor the users who are registering by using the Azure AD Password Reset Registration Activity report. The reporting feature that Azure AD provides helps you answer questions by

Best practice	Solution
	using prebuilt reports. If you're appropriately licensed, you can also create custom queries.
Extend cloud-based password policies to your on-premises infrastructure.	Enhance password policies in your organization by performing the same checks for on-premises password changes as you do for cloud-based password changes. Install Azure AD password protection for Windows Server Active Directory agents on-premises to extend banned password lists to your existing infrastructure. Users and admins who change, set, or reset passwords on-premises are required to comply with the same password policy as cloud-only users.

Enforce multi-factor verification for users

We recommend that you require two-step verification for all of your users. This includes administrators and others in your organization who can have a significant impact if their account is compromised (for example, financial officers).

There are multiple options for requiring two-step verification. The best option for you depends on your goals, the Azure AD edition you're running, and your licensing program. See How to require two-step verification for a user to determine the best option for you. See the Azure AD and Azure Multi-Factor Authentication pricing pages for more information about licenses and pricing.

The following table describes options and benefits for enabling two-step verification:

Option	Benefits
Option 1: Enable Multi-Factor Authentication by changing user state	This is the traditional method for requiring two-step verification. It works with both Azure Multi-Factor Authentication in the cloud and Azure Multi-Factor Authentication Server. Using this method requires users to perform two-step verification every time they sign in and overrides conditional access policies. To determine where Multi-Factor Authentication needs to be enabled, see Which version of Azure MFA is right for my organization?.
Option 2: Enable Multi-Factor Authentication with conditional access policy	This option allows you to prompt for two-step verification under specific conditions by using conditional access. Specific conditions can be user sign-in from different locations, untrusted

Option	Benefits
	devices, or applications that you consider risky. Defining specific conditions where you require two-step verification enables you to avoid constant prompting for your users, which can be an unpleasant user experience. This is the most flexible way to enable two-step verification for your users. Enabling a conditional access policy works only for Azure Multi-Factor Authentication in the cloud and is a premium feature of Azure AD. You can find more information on this method in Deploy cloud-based Azure Multi-Factor Authentication.
Option 3: Enable Multi-Factor Authentication with conditional access policies by evaluating user and sign-in risk of Azure AD Identity Protection	This option enables you to: • Detect potential vulnerabilities that affect your organization's identities. • Configure automated responses to detected suspicious actions that are related to your organization's identities. • Investigate suspicious incidents and take appropriate action to resolve them. This method uses the Azure AD Identity Protection risk evaluation to determine if two-step verification is required based on user and sign-in risk for all cloud applications. This method requires Azure Active Directory P2 licensing. You can find more information on this method in Azure Active Directory Identity Protection.

Note: Option 1, enabling Multi-Factor Authentication by changing the user state, overrides conditional policies. Because options 2 and 3 use conditional access policies, you cannot use option 1 with them.

Organizations that don't add extra layers of identity protection, such as two-step verification, are more susceptible for credential theft attack. A credential theft attack can lead to data compromise.

Use role-based access control

Access management for cloud resources is critical for any organization that uses the cloud. Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Designating groups or individual roles responsible for specific functions in Azure helps avoid confusion that can lead to human and automation errors that create security risks. Restricting access

based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.

Your security team needs visibility into your Azure resources in order to assess and remediate risk. If the security team has operational responsibilities, they need additional permissions to do their jobs.

You can use RBAC to assign permissions to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource.

Best practices for using RBAC to manage access to your cloud resources are:

Best practice	Solution
Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only certain actions at a particular scope.	Use built-in RBAC roles in Azure to assign privileges to users. **Note:** Specific permissions create unneeded complexity and confusion, accumulating into a "legacy" configuration that's difficult to fix without fear of breaking something. • Avoid resource-specific permissions. Instead, use management groups for enterprise-wide permissions and resource groups for permissions within subscriptions. • Avoid user-specific permissions. Instead, assign access to groups in Azure AD.
Grant security teams with Azure responsibilities access to see Azure resources so they can assess and remediate risk.	Grant security teams the RBAC Security Reader role. You can use the root management group or the segment management group, depending on the scope of responsibilities: • **Root management group** for teams responsible for all enterprise resources • **Segment management group** for teams with limited scope (commonly because of regulatory or other organizational boundaries)
Grant the appropriate permissions to security teams that have direct operational responsibilities.	Review the RBAC built-in roles for the appropriate role assignment. If the built-in roles don't meet the specific needs of your organization, you can create custom roles for Azure resources. As with built-in roles, you can assign custom roles to users, groups, and service principals at subscription, resource group, and resource scopes.
Grant Azure Security Center access to security roles that need it. Security Center allows	Add security teams with these needs to the RBAC Security Admin role so they can view

Best practice	Solution
security teams to quickly identify and remediate risks.	security policies, view security states, edit security policies, view alerts and recommendations, and dismiss alerts and recommendations. You can do this by using the root management group or the segment management group, depending on the scope of responsibilities.

Organizations that don't enforce data access control by using capabilities like RBAC might be giving more privileges than necessary to their users. This can lead to data compromise by allowing users to access types of data (for example, high business impact) that they shouldn't have.

Lower exposure of privileged accounts

Securing privileged access is a critical first step to protecting business assets. Minimizing the number of people who have access to secure information or resources reduces the chance of a malicious user getting access, or an authorized user inadvertently affecting a sensitive resource.

Privileged accounts are accounts that administer and manage IT systems. Cyber attackers target these accounts to gain access to an organization's data and systems. To secure privileged access, you should isolate the accounts and systems from the risk of being exposed to a malicious user.

We recommend that you develop and follow a roadmap to secure privileged access against cyber attackers. For information about creating a detailed roadmap to secure identities and access that are managed or reported in Azure AD, Microsoft Azure, Office 365, and other cloud services, review Securing privileged access for hybrid and cloud deployments in Azure AD.

Best practices for lowering exposure to privileged accounts are:

Best practice	Solution
Manage, control, and monitor access to privileged accounts.	Turn on Azure AD Privileged Identity Management. After you turn on Privileged Identity Management, you'll receive notification email messages for privileged access role changes. These notifications provide early warning when additional users are added to highly privileged roles in your directory.
Ensure all critical admin accounts are managed Azure AD accounts.	Remove any consumer accounts from critical admin roles (for example, Microsoft accounts like @hotmail.com, @live.com, and @outlook.com).
Ensure all critical admin roles have a separate account for administrative tasks in order to	Create a separate admin account that's assigned the privileges needed to perform the administrative tasks. Block the use of these

Best practice	Solution
avoid phishing and other attacks to compromise administrative privileges.	administrative accounts for daily productivity tools like Microsoft Office 365 email or arbitrary web browsing.
Identify and categorize accounts that are in highly privileged roles.	After turning on Azure AD Privileged Identity Management, view the users who are in the global administrator, privileged role administrator, and other highly privileged roles. Remove any accounts that are no longer needed in those roles, and categorize the remaining accounts that are assigned to admin roles: • Individually assigned to administrative users, and can be used for non-administrative purposes (for example, personal email) • Individually assigned to administrative users and designated for administrative purposes only • Shared across multiple users • For emergency access scenarios • For automated scripts • For external users
Implement "just in time" (JIT) access to further lower the exposure time of privileges and increase your visibility into the use of privileged accounts.	Azure AD Privileged Identity Management lets you: • Limit users to only taking on their privileges JIT. • Assign roles for a shortened duration with confidence that the privileges are revoked automatically.
Define at least two emergency access accounts.	Emergency access accounts help organizations restrict privileged access in an existing Azure Active Directory environment. These accounts are highly privileged and are not assigned to specific individuals. Emergency access accounts are limited to scenarios where normal administrative accounts can't be used. Organizations must limit the emergency account's usage to only the necessary amount of time. Evaluate the accounts that are assigned or eligible for the global admin role. If you don't see any cloud-only accounts by using the

Best practice	Solution
	*.onmicrosoft.com domain (intended for emergency access), create them. For more information, see Managing emergency access administrative accounts in Azure AD.
Have a "break glass" process in place in case of an emergency.	Follow the steps in Securing privileged access for hybrid and cloud deployments in Azure AD.
Require all critical admin accounts to be password-less (preferred), or require Multi-Factor Authentication.	Use the Microsoft Authenticator app to sign in to any Azure AD account without using a password. Like Windows Hello for Business, the Microsoft Authenticator uses key-based authentication to enable a user credential that's tied to a device and uses biometric authentication or a PIN. Require Azure Multi-Factor Authentication at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global Administrator, Privileged Role Administrator, Exchange Online Administrator, and SharePoint Online Administrator. Enable Multi-Factor Authentication for your admin accounts and ensure that admin account users have registered.
For critical admin accounts, have an admin workstation where production tasks aren't allowed (for example, browsing and email). This will protect your admin accounts from attack vectors that use browsing and email and significantly lower your risk of a major incident.	Use an admin workstation. Choose a level of workstation security: • Highly secure productivity devices provide advanced security for browsing and other productivity tasks. • Privileged Access Workstations (PAWs) provide a dedicated operating system that's protected from internet attacks and threat vectors for sensitive tasks.
Deprovision admin accounts when employees leave your organization.	Have a process in place that disables or deletes admin accounts when employees leave your organization.
Regularly test admin accounts by using current attack techniques.	Use Office 365 Attack Simulator or a third-party offering to run realistic attack scenarios in your organization. This can help you find vulnerable users before a real attack occurs.

Best practice	Solution
Take steps to mitigate the most frequently used attacked techniques.	Identify Microsoft accounts in administrative roles that need to be switched to work or school accounts Ensure separate user accounts and mail forwarding for global administrator accounts Ensure that the passwords of administrative accounts have recently changed Turn on password hash synchronization Require Multi-Factor Authentication for users in all privileged roles as well as exposed users Obtain your Office 365 Secure Score (if using Office 365) Review the Office 365 security and compliance guidance (if using Office 365) Configure Office 365 Activity Monitoring (if using Office 365) Establish incident/emergency response plan owners Secure on-premises privileged administrative accounts

If you don't secure privileged access, you might find that you have too many users in highly privileged roles and are more vulnerable to attacks. Malicious actors, including cyber attackers, often target admin accounts and other elements of privileged access to gain access to sensitive data and systems by using credential theft.

Control locations where resources are created

Enabling cloud operators to perform tasks while preventing them from breaking conventions that are needed to manage your organization's resources is very important. Organizations that want to control the locations where resources are created should hard code these locations.

You can use Azure Resource Manager to create security policies whose definitions describe the actions or resources that are specifically denied. You assign those policy definitions at the desired scope, such as the subscription, the resource group, or an individual resource.

Note: Security policies are not the same as RBAC. They actually use RBAC to authorize users to create those resources.

Organizations that are not controlling how resources are created are more susceptible to users who might abuse the service by creating more resources than they need. Hardening the resource creation process is an important step to securing a multitenant scenario.

Actively monitor for suspicious activities

An active identity monitoring system can quickly detect suspicious behavior and trigger an alert for further investigation. The following table lists two Azure AD capabilities that can help organizations monitor their identities:

Best practice	Solution
Have a method to identify: • Attempts to sign in without being traced. • Brute force attacks against a particular account. • Attempts to sign in from multiple locations. • Sign-ins from infected devices. • Suspicious IP addresses.	Use Azure AD Premium anomaly reports. Have processes and procedures in place for IT admins to run these reports on a daily basis or on demand (usually in an incident response scenario).
Have an active monitoring system that notifies you of risks and can adjust risk level (high, medium, or low) to your business requirements.	Use Azure AD Identity Protection, which flags the current risks on its own dashboard and sends daily summary notifications via email. To help protect your organization's identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level is reached.

Organizations that don't actively monitor their identity systems are at risk of having user credentials compromised. Without knowledge that suspicious activities are taking place through these credentials, organizations can't mitigate this type of threat.

Use Azure AD for storage authentication

Azure Storage supports authentication and authorization with Azure AD for Blob storage and Queue storage. With Azure AD authentication, you can use Azure role-based access control to grant specific permissions to users, groups, and applications—down to the scope of an individual blob container or queue.

We recommend that you use Azure AD for authenticating access to storage.

Use strong network controls

You can connect Azure virtual machines (VMs) and appliances to other networked devices by placing them on Azure virtual networks. That is, you can connect virtual network interface cards to a virtual network to allow TCP/IP-based communications between network-enabled devices. Virtual machines connected to an Azure virtual network can connect to devices on the same virtual network, different virtual networks, the internet, or your own on-premises networks.

As you plan your network and the security of your network, we recommend that you centralize:

- Management of core network functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.
- Governance of network security elements, such as network virtual appliance functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.

If you use a common set of management tools to monitor your network and the security of your network, you get clear visibility into both. A straightforward, unified security strategy reduces errors because it increases human understanding and the reliability of automation.

The following sections describe best practices for network security.

Logically segment subnets

Azure virtual networks are similar to LANs on your on-premises network. The idea behind an Azure virtual network is that you create a network, based on a single private IP address space, on which you can place all your Azure virtual machines. The private IP address spaces available are in the Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16) ranges.

Best practices for logically segmenting subnets include:

Best practice	Solution
Don't assign allow rules with broad ranges (for example, allow 0.0.0.0 through 255.255.255.255).	Ensure troubleshooting procedures discourage or ban setting up these types of rules. These allow rules lead to a false sense of security and are frequently found and exploited by red teams.
Segment the larger address space into subnets.	Use CIDR-based subnetting principles to create your subnets.
Create network access controls between subnets. Routing between subnets happens automatically, and you don't need to manually configure routing tables. By default, there are no network access controls between the subnets that you create on an Azure virtual network.	Use a network security group to protect against unsolicited traffic into Azure subnets. Network security groups are simple, stateful packet inspection devices that use the 5-tuple approach (source IP, source port, destination IP, destination port, and layer 4 protocol) to create allow/deny rules for network traffic. You allow or deny traffic to and from a single IP address, to and from multiple IP addresses, or to and from entire subnets. When you use network security groups for network access control between subnets, you can put resources that belong to the same security zone or role in their own subnets.
Avoid small virtual networks and subnets to ensure simplicity and flexibility.	Most organizations add more resources than initially planned, and re-allocating addresses is labor intensive. Using small subnets adds limited security value, and mapping a network

Best practice	Solution
	security group to each subnet adds overhead. Define subnets broadly to ensure that you have flexibility for growth.
Simplify network security group rule management by defining Application Security Groups.	Define an Application Security Group for lists of IP addresses that you think might change in the future or be used across many network security groups. Be sure to name Application Security Groups clearly so others can understand their content and purpose.

Adopt a Zero Trust approach

Perimeter-based networks operate on the assumption that all systems within a network can be trusted. But today's employees access their organization's resources from anywhere on a variety of devices and apps, which makes perimeter security controls irrelevant. Access control policies that focus only on who can access a resource are not enough. To master the balance between security and productivity, security admins also need to factor in *how* a resource is being accessed.

Networks need to evolve from traditional defenses because networks might be vulnerable to breaches: an attacker can compromise a single endpoint within the trusted boundary and then quickly expand a foothold across the entire network. Zero Trust networks eliminate the concept of trust based on network location within a perimeter. Instead, Zero Trust architectures use device and user trust claims to gate access to organizational data and resources. For new initiatives, adopt Zero Trust approaches that validate trust at the time of access.

Best practices are:

Best practice	Solution
Give conditional access to resources based on device, identity, assurance, network location, and more.	Azure AD conditional access lets you apply the right access controls by implementing automated access control decisions based on the required conditions. For more information, see Manage access to Azure management with conditional access.
Enable port access only after workflow approval.	You can use just-in-time VM access in Azure Security Center to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Grant temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.	Use just-in-time access in Azure AD Privileged Identity Management or in a third-party solution to grant permissions to perform privileged tasks.

Zero Trust is the next evolution in network security. The state of cyberattacks drives organizations to take the "assume breach" mindset, but this approach shouldn't be limiting. Zero Trust networks protect corporate data and resources while ensuring that organizations can build a modern workplace by using technologies that empower employees to be productive anytime, anywhere, in any way.

Control routing behavior

When you put a virtual machine on an Azure virtual network, the VM can connect to any other VM on the same virtual network, even if the other VMs are on different subnets. This is possible because a collection of system routes enabled by default allows this type of communication. These default routes allow VMs on the same virtual network to initiate connections with each other, and with the internet (for outbound communications to the internet only).

Although the default system routes are useful for many deployment scenarios, there are times when you want to customize the routing configuration for your deployments. You can configure the next-hop address to reach specific destinations.

We recommend that you configure user-defined routes when you deploy a security appliance for a virtual network. We talk about this in a later section titled secure your critical Azure service resources to only your virtual networks.

Note: User-defined routes are not required, and the default system routes usually work.

Use virtual network appliances

Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the OSI model. But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.

Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- Firewalling
- Intrusion detection/intrusion prevention
- Vulnerability management
- Application control
- Network-based anomaly detection
- Web filtering
- Antivirus
- Botnet protection

To find available Azure virtual network security appliances, go to the Azure Marketplace and search for "security" and "network security."

Deploy perimeter networks for security zones

A perimeter network (also known as a DMZ) is a physical or logical network segment that provides an additional layer of security between your assets and the internet. Specialized network access control devices on the edge of a perimeter network allow only desired traffic into your virtual network.

Perimeter networks are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. A perimeter network is where you typically enable distributed denial of service (DDoS) prevention, intrusion detection/intrusion prevention systems (IDS/IPS), firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.

Although this is the basic design of a perimeter network, there are many different designs, like back-to-back, tri-homed, and multi-homed.

Based on the Zero Trust concept mentioned earlier, we recommend that you consider using a perimeter network for all high security deployments to enhance the level of network security and access control for your Azure resources. You can use Azure or a third-party solution to provide an additional layer of security between your assets and the internet:

- **Azure native controls**. Azure Firewall and the web application firewall in Application Gateway offer basic security with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration.
- Third-party offerings. Search the Azure Marketplace for next-generation firewall (NGFW) and other third-party offerings that provide familiar security tools and significantly enhanced levels of network security. Configuration might be more complex, but a third-party offering might allow you to use existing capabilities and skill sets.

Avoid exposure to the internet with dedicated WAN links

Many organizations have chosen the hybrid IT route. With hybrid IT, some of the company's information assets are in Azure, and others remain on-premises. In many cases, some components of a service are running in Azure while other components remain on-premises.

In a hybrid IT scenario, there's usually some type of cross-premises connectivity. Cross-premises connectivity allows the company to connect its on-premises networks to Azure virtual networks. Two cross-premises connectivity solutions are available:

- **Site-to-site VPN**. It's a trusted, reliable, and established technology, but the connection takes place over the internet. Bandwidth is constrained to a maximum of about 200 Mbps. Site-to-site VPN is a desirable option in some scenarios. It's discussed further in the Disable RDP/SSH access to virtual machines section of this white paper.
- **Azure ExpressRoute**. We recommend that you use ExpressRoute for your cross-premises connectivity. ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services like Azure, Office 365, and Dynamics 365. ExpressRoute is a dedicated WAN link between your on-premises location or a Microsoft Exchange hosting provider. Because this is a telco connection, your data doesn't travel over the internet, so it isn't exposed to the potential risks of internet communications.

  The location of your ExpressRoute connection can affect firewall capacity, scalability, reliability, and network traffic visibility. You'll need to identify where to terminate ExpressRoute in existing (on-premises) networks. You can:

- Terminate outside the firewall (the perimeter network paradigm) if you require visibility into the traffic, if you need to continue an existing practice of isolating datacenters, or if you're solely putting extranet resources on Azure.
- Terminate inside the firewall (the network extension paradigm). This is the default recommendation. In all other cases, we recommend treating Azure as an *n*th datacenter.

Optimize uptime and performance

If a service is down, information can't be accessed. If performance is so poor that the data is unusable, you can consider the data to be inaccessible. From a security perspective, you need to do whatever you can to make sure that your services have optimal uptime and performance.

A popular and effective method for enhancing availability and performance is load balancing. Load balancing is a method of distributing network traffic across servers that are part of a service. For example, if you have front-end web servers as part of your service, you can use load balancing to distribute the traffic across your multiple front-end web servers.

This distribution of traffic increases availability because if one of the web servers becomes unavailable, the load balancer stops sending traffic to that server and redirects it to the servers that are still online. Load balancing also helps performance, because the processor, network, and memory overhead for serving requests is distributed across all the load-balanced servers.

We recommend that you employ load balancing whenever you can, and as appropriate for your services. The following table lists scenarios at both the Azure virtual network level and the global level, along with load-balancing options for each.

Scenario	Load-balancing option
You have an application that: • Requires requests from the same user/client session to reach the same back-end virtual machine. Examples of this are shopping cart apps and web mail servers. • Accepts only a secure connection, so unencrypted communication to the server is not an acceptable option. • Requires multiple HTTP requests on the same long-running TCP connection to be routed or load balanced to different back-end servers.	Use Azure Application Gateway, an HTTP web traffic load balancer. Application Gateway supports end-to-end SSL encryption and SSL termination at the gateway. Web servers can then be unburdened from encryption and decryption overhead and traffic flowing unencrypted to the back-end servers.
You need to load balance incoming connections from the internet among your servers located in an Azure virtual network. Scenarios are when you:	Use the Azure portal to create an external load balancer that spreads incoming requests across multiple VMs to provide a higher level of availability.

Scenario	Load-balancing option
• Have stateless applications that accept incoming requests from the internet. • Don't require sticky sessions or SSL offload. Sticky sessions is a method used with Application Load Balancing, to achieve server-affinity.	
You need to load balance connections from VMs that are not on the internet. In most cases, the connections that are accepted for load balancing are initiated by devices on an Azure virtual network, such as SQL Server instances or internal web servers.	Use the Azure portal to create an internal load balancer that spreads incoming requests across multiple VMs to provide a higher level of availability.
You need global load balancing because you: • Have a cloud solution that is widely distributed across multiple regions and requires the highest level of uptime (availability) possible. • Need the highest level of uptime possible to make sure that your service is available even if an entire datacenter becomes unavailable.	Use Azure Traffic Manager. Traffic Manager makes it possible to load balance connections to your services based on the location of the user. For example, if the user makes a request to your service from the EU, the connection is directed to your services located in an EU datacenter. This part of Traffic Manager global load balancing helps to improve performance because connecting to the nearest datacenter is faster than connecting to datacenters that are far away.

Disable RDP/SSH access to virtual machines

It's possible to reach Azure virtual machines by using Remote Desktop Protocol (RDP) and the Secure Shell (SSH) protocol. These protocols enable the management VMs from remote locations and are standard in datacenter computing.

The potential security problem with using these protocols over the internet is that attackers can use brute force techniques to gain access to Azure virtual machines. After the attackers gain access, they can use your VM as a launch point for compromising other machines on your virtual network or even attack networked devices outside Azure.

We recommend that you disable direct RDP and SSH access to your Azure virtual machines from the internet. After direct RDP and SSH access from the internet is disabled, you have other options that you can use to access these VMs for remote management.

Scenario	Option
Enable a single user to connect to an Azure virtual network over the internet.	Point-to-site VPN is another term for a remote access VPN client/server connection. After the point-to-site connection is established, the user can use RDP or SSH to connect to any VMs located on the Azure virtual network that the user connected to via point-to-site VPN. This assumes that the user is authorized to reach those VMs. Point-to-site VPN is more secure than direct RDP or SSH connections because the user has to authenticate twice before connecting to a VM. First, the user needs to authenticate (and be authorized) to establish the point-to-site VPN connection. Second, the user needs to authenticate (and be authorized) to establish the RDP or SSH session.
Enable users on your on-premises network to connect to VMs on your Azure virtual network.	A site-to-site VPN connects an entire network to another network over the internet. You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet.
Use a dedicated WAN link to provide functionality similar to the site-to-site VPN.	Use ExpressRoute. It provides functionality similar to the site-to-site VPN. The main differences are: • The dedicated WAN link doesn't traverse the internet. • Dedicated WAN links are typically more stable and perform better.

Secure your critical Azure service resources to only your virtual networks

Use virtual network service endpoints to extend your virtual network private address space, and the identity of your virtual network to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your virtual network to the Azure service always remains on the Microsoft Azure backbone network.

Service endpoints provide the following benefits:

- **Improved security for your Azure service resources**: With service endpoints, Azure service resources can be secured to your virtual network. Securing service resources to a virtual network provides improved security by fully removing public internet access to resources, and allowing traffic only from your virtual network.
- **Optimal routing for Azure service traffic from your virtual network**: Any routes in your virtual network that force internet traffic to your on-premises and/or virtual appliances, known as forced tunneling, also force Azure service traffic to take the same route as the internet traffic. Service endpoints provide optimal routing for Azure traffic.

  Endpoints always take service traffic directly from your virtual network to the service on the Azure backbone network. Keeping traffic on the Azure backbone network allows you to continue auditing and monitoring outbound internet traffic from your virtual networks,

through forced tunneling, without affecting service traffic. Learn more about user-defined routes and forced tunneling.

- **Simple to set up with less management overhead**: You no longer need reserved, public IP addresses in your virtual networks to secure Azure resources through an IP firewall. There are no NAT or gateway devices required to set up the service endpoints. Service endpoints are configured through a simple click on a subnet. There is no additional overhead to maintain the endpoints.

To learn more about service endpoints and the Azure services and regions that service endpoints are available for, see Virtual network service endpoints.

Lock down and secure VM and computer operating systems

In most IaaS scenarios, Azure virtual machines are the main workload for organizations that use cloud computing. This fact is evident in hybrid scenarios where organizations want to slowly migrate workloads to the cloud. In such scenarios, follow the general security considerations for IaaS, and apply security best practices to all your VMs.

The following sections describe security best practices for VMs and operating systems.

Protect VMs by using authentication and access control

For the topics of identity and access, we discussed using strong authentication and authorization to protect data and resources. The first step in protecting your VMs is to ensure that only authorized users can set up new VMs and access VMs.

Note: To improve the security of Linux VMs on Azure, you can integrate with Azure AD authentication. When you use Azure AD authentication for Linux VMs, you centrally control and enforce policies that allow or deny access to the VMs.

Best practice	Solution
Control VM access.	Use Azure policies to establish conventions for resources in your organization and create customized policies. Apply these policies to resources, such as resource groups. VMs that belong to a resource group inherit its policies. If your organization has many subscriptions, you might 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 management groups (containers) and apply your governance conditions to those groups. All subscriptions within a management group automatically inherit the conditions applied to the group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.

Best practice	Solution
Reduce variability in your setup and deployment of VMs.	Use Azure Resource Manager templates to strengthen your deployment choices and make it easier to understand and inventory the VMs in your environment.
Secure privileged access.	Use a least privilege approach and built-in Azure roles to enable users to access and set up VMs: • Virtual Machine Contributor: Can manage VMs, but not the virtual network or storage account to which they are connected. • Classic Virtual Machine Contributor: Can manage VMs created by using the classic deployment model, but not the virtual network or storage account to which the VMs are connected. • Security Manager: Can manage security components, security policies, and VMs. • DevTest Labs User: Can view everything and connect, start, restart, and shut down VMs. **Note:** Your subscription admins and coadmins can change this setting, making them administrators of all the VMs in a subscription. Be sure that you trust all of your subscription admins and coadmins to log in to any of your machines.

Note: We recommend that you consolidate VMs with the same lifecycle into the same resource group. By using resource groups, you can deploy, monitor, and roll up billing costs for your resources.

Organizations that control VM access and setup improve their overall VM security.

Use multiple VMs for better availability

If your VM runs critical applications that need to have high availability, we strongly recommend that you use multiple VMs. For better availability, use an availability set.

An availability set is a logical grouping that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they're deployed in an Azure datacenter. Azure ensures that the VMs you place in an availability set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or Azure software failure occurs, only a subset of your VMs are affected, and your overall application continues to be available to your customers. Availability sets are an essential capability when you want to build reliable cloud solutions.

Protect against malware

You should install antimalware protection to help identify and remove viruses, spyware, and other malicious software. You can install Microsoft Antimalware or a Microsoft partner's endpoint protection solution (Trend Micro, Symantec, McAfee, Windows Defender, and System Center Endpoint Protection).

Microsoft Antimalware includes features like real-time protection, scheduled scanning, malware remediation, signature updates, engine updates, samples reporting, and exclusion event collection. For environments that are hosted separately from your production environment, you can use an antimalware extension to help protect your VMs and cloud services.

You can integrate Microsoft Antimalware and partner solutions with Azure Security Center for ease of deployment and built-in detections (alerts and incidents).

Best practice	Solution
Install an antimalware solution to protect against malware.	Install a Microsoft partner solution or Microsoft Antimalware
Integrate your antimalware solution with Security Center to monitor the status of your protection.	Manage endpoint protection issues with Security Center

Manage your VM updates

Azure VMs, like all on-premises VMs, are meant to be user managed. Azure doesn't push Windows updates to them. You need to manage your VM updates.

Best practice	Solution
Keep your VMs current.	Use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers that are deployed in Azure, in on-premises environments, or in other cloud providers. You can quickly assess the status of available updates on all agent computers and manage the process of installing required updates for servers. Computers that are managed by Update Management use the following configurations to perform assessment and update deployments: • Microsoft Monitoring Agent (MMA) for Windows or Linux • PowerShell Desired State Configuration (DSC) for Linux • Automation Hybrid Runbook Worker • Microsoft Update or Windows Server Update Services (WSUS) for Windows computers

Best practice	Solution
	Note: If you use Windows Update, leave the automatic Windows Update setting enabled.
Ensure at deployment that images you built include the most recent round of Windows updates.	Check for and install all Windows updates as a first step of every deployment. This measure is especially important to apply when you deploy images that come from either you or your own library. Although images from the Azure Marketplace are updated automatically by default, there can be a lag time (up to a few weeks) after a public release.
Periodically redeploy your VMs to force a fresh version of the OS.	Define your VM with an Azure Resource Manager template so you can easily redeploy it. Using a template gives you a patched and secure VM when you need it.
Rapidly apply security updates to VMs	Enable Azure Security Center (Free tier or Standard tier) to identify missing security updates and apply them.
Deploy and test a backup solution.	A backup needs to be handled the same way that you handle any other operation. This is true of systems that are part of your production environment extending to the cloud. Test and dev systems must follow backup strategies that provide restore capabilities that are similar to what users have grown accustomed to, based on their experience with on-premises environments. Production workloads moved to Azure should integrate with existing backup solutions when possible. Or, you can use Azure Backup to help address your backup requirements.

Organizations that don't enforce software-update policies are more exposed to threats that exploit known, previously fixed vulnerabilities. To comply with industry regulations, companies must prove that they are diligent and using correct security controls to help ensure the security of their workloads located in the cloud.

Software-update best practices for a traditional datacenter and Azure IaaS have many similarities. We recommend that you evaluate your current software update policies to include VMs located in Azure.

Manage your VM security posture

Cyberthreats are evolving. Safeguarding your VMs requires a monitoring capability that can quickly detect threats, prevent unauthorized access to your resources, trigger alerts, and reduce false positives.

To monitor the security posture of your Windows and Linux VMs, use Azure Security Center. In Security Center, safeguard your VMs by taking advantage of the following capabilities:

- Apply OS security settings with recommended configuration rules.
- Identify and download system security and critical updates that might be missing.
- Deploy recommendations for endpoint antimalware protection.
- Validate disk encryption.
- Assess and remediate vulnerabilities.
- Detect threats.

Security Center can actively monitor for threats, and potential threats are exposed in security alerts. Correlated threats are aggregated in a single view called a security incident.

Security Center stores data in Azure Log Analytics. Log Analytics provides a query language and analytics engine that gives you insights into the operation of your applications and resources. Data is also collected from Azure Monitor, management solutions, and agents installed on virtual machines in the cloud or on-premises. This shared functionality helps you form a complete picture of your environment.

Organizations that don't enforce strong security for their VMs remain unaware of potential attempts by unauthorized users to circumvent security controls.

Monitor VM performance

Resource abuse can be a problem when VM processes consume more resources than they should. Performance issues with a VM can lead to service disruption, which violates the security principle of availability. This is particularly important for VMs that are hosting IIS or other web servers, because high CPU or memory usage might indicate a denial of service (DoS) attack. It's imperative to monitor VM access not only reactively while an issue is occurring, but also proactively against baseline performance as measured during normal operation.

We recommend that you use Azure Monitor to gain visibility into your resource's health. Azure Monitor features:

- Resource diagnostic log files: Monitors your VM resources and identifies potential issues that might compromise performance and availability.
- Azure Diagnostics extension: Provides monitoring and diagnostics capabilities on Windows VMs. You can enable these capabilities by including the extension as part of the Azure Resource Manager template.

Organizations that don't monitor VM performance can't determine whether certain changes in performance patterns are normal or abnormal. A VM that's consuming more resources than normal might indicate an attack from an external resource or a compromised process running in the VM.

Encrypt your virtual hard disk files

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.

Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.

The following table lists best practices for using Azure Disk Encryption:

Best practice	Solution
Enable encryption on VMs.	Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. Create an Azure AD application for this purpose. For authentication purposes, you can use either client secret-based authentication or client certificate-based Azure AD authentication.
Use a key encryption key (KEK) for an additional layer of security for encryption keys. Add a KEK to your key vault.	Use the Add-AzureKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises hardware security module (HSM) for key management. For more information, see the Key Vault documentation. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault. Keeping an escrow copy of this key in an on-premises key management HSM offers additional protection against accidental deletion of keys.
Take a snapshot and/or backup before disks are encrypted. Backups provide a recovery option if an unexpected failure happens during encryption.	VMs with managed disks require a backup before encryption occurs. After a backup is made, you can use the **Set-AzureRmVMDiskEncryptionExtension** cmdlet to encrypt managed disks by specifying the *-skipVmBackup* parameter. For more information about how to back up and restore encrypted VMs, see the Azure Backup article.
To make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the key vault and the VMs to be located in the same region.	Create and use a key vault that is in the same region as the VM to be encrypted.

When you apply Azure Disk Encryption, you can satisfy the following business needs:

- IaaS VMs are secured at rest through industry-standard encryption technology to address organizational security and compliance requirements.
- IaaS VMs start under customer-controlled keys and policies, and you can audit their usage in your key vault.

Restrict direct internet connectivity

Monitor and restrict VM direct internet connectivity. Attackers constantly scan public cloud IP ranges for open management ports and attempt "easy" attacks like common passwords and known unpatched vulnerabilities. The following table lists best practices to help protect against these attacks:

Best practice	Solution
Prevent inadvertent exposure to network routing and security.	Use RBAC to ensure that only the central networking group has permission to networking resources.
Identify and remediate exposed VMs that allow access from "any" source IP address.	Use Azure Security Center. Security Center will recommend that you restrict access through internet-facing endpoints if any of your network security groups has one or more inbound rules that allow access from "any" source IP address. Security Center will recommend that you edit these inbound rules to restrict access to source IP addresses that actually need access.
Restrict management ports (RDP, SSH)	Just-in-time (JIT) VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. When JIT is enabled, Security Center locks down inbound traffic to your Azure VMs by creating a network security group rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the JIT solution.

Protect data

To help protect data in the cloud, you need to account for the possible states in which your data can occur, and what controls are available for that state. Best practices for Azure data security and encryption relate to the following data states:

- **At rest**: This includes all information storage objects, containers, and types that exist statically on physical media, whether magnetic or optical disk.
- **In transit**: When data is being transferred between components, locations, or programs, it's in transit. Examples are transfer over the network, across a service bus (from on-premises to

cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process.

The following sections describe security best practices for protecting data.

Choose a key management solution

Protecting your keys is essential to protecting your data in the cloud.

Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data. Developers can create keys for development and testing in minutes, and then migrate them to production keys. Security administrators can grant (and revoke) permission to keys, as needed.

You can use Key Vault to create multiple secure containers, called vaults. These vaults are backed by HSMs. Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Key vaults also control and log the access to anything stored in them. Azure Key Vault can handle requesting and renewing Transport Layer Security (TLS) certificates. It provides features for a robust solution for certificate lifecycle management.

Azure Key Vault is designed to support application keys and secrets. Key Vault is not intended to be a store for user passwords.

The following table lists security best practices for using Key Vault:

Best practice	Solution
Grant access to users, groups, and applications at a specific scope.	Use RBAC's predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role Key Vault Contributor to this user at a specific scope. The scope in this case would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can define your own roles.
Control what users have access to.	Access to a key vault is controlled through two separate interfaces: management plane and data plane. The management plane and data plane access controls work independently. Use RBAC to control what users have access to. For example, if you want to grant an application access to use keys in a key vault, you only need to grant data plane access permissions by using key vault access policies, and no management plane access is needed for this application. Conversely, if you want a user to be able to read vault properties and tags but not have any access to keys, secrets, or certificates, you can

Implement advanced network security

October 25, 2021 9:25 AM

Defense in Depth Defense in depth (computing) - Wikipedia
OSI OSI model - Wikipedia

- secure the connectivity of hybrid networks
  - Express Route https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction
  - Azure ExpressRoute: Connectivity models | Microsoft Docs
  - Azure ExpressRoute: Routing requirements | Microsoft Docs
  - FAQ - Azure ExpressRoute | Microsoft Docs
  - Pricing – ExpressRoute | Microsoft Azure
  - About ExpressRoute virtual network gateways - Azure | Microsoft Docs
  - About Azure ExpressRoute Direct | Microsoft Docs

- secure the connectivity of virtual networks
  - UDR and Network Virtual Appliances Azure virtual network traffic routing | Microsoft Docs
  - VPN Forced Tunneling Configure forced tunneling for Site-to-Site connections - Azure VPN Gateway | Microsoft Docs
  - Deploy highly available NVAs - Azure Architecture Center | Microsoft Docs
  - Implement a secure hybrid network - Azure Architecture Center | Microsoft Docs
  - Hub-spoke network topology in Azure - Azure Reference Architectures | Microsoft Docs

- create and configure Azure Firewall
  - What is Azure Firewall? | Microsoft Docs
  - Tutorial: Deploy & configure Azure Firewall and policy using the Azure portal | Microsoft Docs
  - Azure Firewall Samples | Microsoft Docs
  - Azure Firewall Samples | Microsoft Docs
  - Azure Firewall Premium features | Microsoft Docs TLS, IDPS, URL Filtering, Web Categories

- create and configure Azure Firewall Manager
  - What is Azure Firewall Manager? | Microsoft Docs
  - Tutorial: Secure your virtual hub using Azure Firewall Manager | Microsoft Docs
  - Tutorial: Secure your virtual hub using Azure PowerShell | Microsoft Docs
  - Azure Firewall Manager policy overview | Microsoft Docs
  - What is a secured virtual hub? | Microsoft Docs

- create and configure Azure Application Gateway
  - What is Azure Application Gateway | Microsoft Docs
  - Quickstart: Direct web traffic using the portal - Azure Application Gateway | Microsoft Docs
  - Quickstart: Direct web traffic using PowerShell - Azure Application Gateway | Microsoft Docs
  - Tutorial: Configure TLS termination in portal - Azure Application Gateway | Microsoft Docs
  - Review the other tutorials
  - Azure Application Gateway features | Microsoft Docs

- create and configure Azure Front Door
  - Azure Front Door | Microsoft Docs
  - Tutorial - Configure HTTPS on a custom domain for Azure Front Door | Microsoft Docs
  - Review the other tutorials
  - Quickstart: Set up high availability with Azure Front Door Service - Azure portal | Microsoft Docs
  - Azure Front Door - Frequently asked questions | Microsoft Docs

- create and configure Web Application Firewall (WAF)
  - What is Azure Web Application Firewall on Azure Application Gateway? - Azure Web Application Firewall | Microsoft Docs
  - What is Azure web application firewall on Azure Front Door? | Microsoft Docs
  - Tutorial: Create using portal - Web Application Firewall | Microsoft Docs

- configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure App Service
  - Secure a database - Azure SQL Database | Microsoft Docs
  - Secure your Azure Storage account - Learn | Microsoft Docs
  - Security recommendations for Blob storage - Azure Storage | Microsoft Docs
  - Best Practices to use Key Vault - Azure Key Vault | Microsoft Docs
  - Azure Key Vault security overview | Microsoft Docs
  - Security recommendations - Azure App Service | Microsoft Docs
  - Security - Azure App Service | Microsoft Docs

- configure network isolation for Web Apps and Azure Functions
  - Azure Functions networking options | Microsoft Docs

- implement Azure Service Endpoints
  - Azure virtual network service endpoints | Microsoft Docs

- implement Azure Private Endpoints, including integrating with other services
  - What is an Azure Private Endpoint? | Microsoft Docs

- implement Azure Private Links
  - What is Azure Private Link? | Microsoft Docs
  - Review the QuickStarts
  - What is an Azure Private Endpoint? | Microsoft Docs

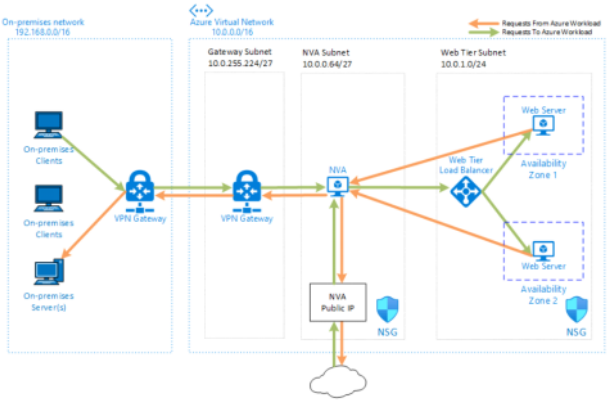
- implement Azure DDoS Protection
  - Azure DDoS Protection Standard Overview | Microsoft Docs
  - Manage Azure DDoS Protection Standard using the Azure portal | Microsoft Docs
  - Create and configure an Azure DDoS Protection plan using Azure PowerShell | Microsoft Docs
  - Azure DDoS Protection fundamental best practices | Microsoft Docs
  - Azure DDoS Protection features | Microsoft Docs
  - DDOS is at the network level not subnet

VPN Forced Tunneling
- Configure forced tunneling for Site-to-Site connections - Azure VPN Gateway | Microsoft Docs

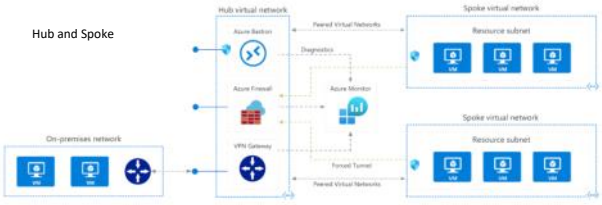
Network Security Groups
- Azure network security groups overview | Microsoft Docs
- Network security group - how it works | Microsoft Docs
- Introduction to Effective security rules view in Azure Network Watcher | Microsoft Docs
- Diagnose a virtual machine network traffic filter problem | Microsoft Docs

Application Security Groups
- Azure application security groups overview | Microsoft Docs

Network Virtual Appliance Workflow



Hub and Spoke



Configure advanced security for compute

October 25, 2021 9:25 AM

configure Azure Endpoint Protection for virtual machines (VMs)
- Endpoint Protection (microsoft.com)
- Endpoint protection recommendations in Azure Security Centers | Microsoft Docs

Implement and manage security updates for VMs
- Enable Azure Automation Update Management from the Azure portal | Microsoft Docs
- Manage updates and patches for your VMs in Azure Automation | Microsoft Docs
- How to create alerts for Azure Automation Update Management | Microsoft Docs
- Configure Windows Update settings for Azure Automation Update Management | Microsoft Docs

configure security for container services
- Serverless containers in Azure - Azure Container Instances | Microsoft Docs
- Azure security baseline for Container Instances | Microsoft Docs
- Security considerations for container instances - Azure Container Instances | Microsoft Docs
- Containers vs. virtual machines | Microsoft Docs
- Scenarios to use a virtual network - Azure Container Instances | Microsoft Docs

https://www.microsoft.com/security/blog/2021/07/21/the-evolution-of-a-matrix-how-attck-for-containers-was-built/

https://github.com/docker/docker-bench-security#:~:text=Docker%20Bench%20for%20Security%20The%20Docker%20Bench%20for,are%20based%20on%20the%20CIS%20Docker%20Benchmark%20v1.3.1.
- Registry authentication options - Azure Container Registry | Microsoft Docs

manage access to Azure Container Registry
- Quickstart - Create registry in portal - Azure Container Registry | Microsoft Docs
- Managed container registries - Azure Container Registry | Microsoft Docs

AKS
- Introduction to Azure Kubernetes Service - Azure Kubernetes Service | Microsoft Docs
- Azure Kubernetes Service (AKS) design - Azure Architecture Center | Microsoft Docs
- Azure security baseline for Azure Kubernetes Service | Microsoft Docs
- Concepts - Security in Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs
- Azure Policy Regulatory Compliance controls for Azure Kubernetes Service (AKS) - Azure Kubernetes Service | Microsoft Docs
- Best practices for Azure Kubernetes Service (AKS) - Azure Kubernetes Service | Microsoft Docs
- Concepts - Kubernetes basics for Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs
- Concepts - Networking in Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs
- Concepts - Storage in Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs
- Integrate Azure Active Directory with Azure Kubernetes Service (legacy) - Azure Kubernetes Service | Microsoft Docs
- Service principals for Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs
- Use managed identities in Azure Kubernetes Service - Azure Kubernetes Service | Microsoft Docs
- Configure Azure CNI networking in Azure Kubernetes Service (AKS) - Azure Kubernetes Service | Microsoft Docs

configure security for serverless compute

configure security for an Azure App Service

configure encryption at rest
- Enable Azure Disk Encryption for Windows VMs - Azure Virtual Machines | Microsoft Docs
- Enable Azure Disk Encryption for Linux VMs - Azure Virtual Machines | Microsoft Docs
- Creating and configuring a key vault for Azure Disk Encryption - Azure Virtual Machines | Microsoft Docs

configure encryption in transit

Privileged Access Workstations
- Why are privileged access devices important | Microsoft Docs
- Securing privileged access overview | Microsoft Docs
- Developing a privileged access strategy | Microsoft Docs
- Securing privileged access accounts | Microsoft Docs
- Rapidly modernize your security infrastructure | Microsoft Docs

Virtual Machine Templates
- Templates overview - Azure Resource Manager | Microsoft Docs
- Best practices for templates - Azure Resource Manager | Microsoft Docs

Azure Resource Manager Template Toolkit

From <https://github.com/azure/arm-ttk>
- Azure Quickstart Templates (microsoft.com)

Remote Access Management
Bastion https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
- Quickstart: Configure Bastion from VM settings - Azure Bastion | Microsoft Docs

Azure ARC Azure Arc overview - Azure Arc | Microsoft Docs - outside of scope
Windows Admin Center Configuring Azure Integration | Microsoft Docs

Microsoft Defender for Endpoint
- Manage Windows Defender Credential Guard (Windows) - Windows security | Microsoft Docs
- Microsoft Defender for Endpoint - Configuration Manager | Microsoft Docs
- How to manage Windows Defender Application Control - Configuration Manager | Microsoft Docs

Azure Security Benchmark
- Azure Security Benchmark | Microsoft Docs

Azure Advisor
- Introduction to Azure Advisor - Azure Advisor | Microsoft Docs
- Azure security baseline for Azure Advisor | Microsoft Docs
- Make resources more secure with Azure Advisor - Azure Advisor | Microsoft Docs

Azure Security Center
- What is Azure Security Center? | Microsoft Docs
- Azure Security Center's asset inventory | Microsoft Docs

Defense_In_Depth_Enterprise Mobility_and_Security_61517.pdf

Tuesday, October 26, 2021 9:06 AM

Clipped from: http://info.microsoft.com/rs/157-GQE-382/images/Defense_In_Depth_Enterprise%20Mobility_and_Security_61517.pdf

My grandfather was a Welsh Guardsman. You may know them as the guys in the bearskin hats and red coats who guard Buckingham Palace (though they are more than that).

Having family in North Wales has allowed me to study the castles built there in the 13th century. Even in their weathered state, now abandoned to tourism, they are awesome to behold. The pinnacle of military technology in their day, they allowed a small garrison to hold off hordes of attackers, due in part to their rings of defense.

Defensive rings map well to the cybersecurity principle of "defense in depth," the idea of building multiple redundant defenses into systems. We build each ring to be effective, but if the barbarians manage to cross the moat, it's great if we can retreat to the walls and defend from there. If a bad guy gets through one ring, the next one can catch him.

Microsoft Enterprise Mobility + Security has similar defensive rings:

- **Azure Active Directory (Azure AD) Identity Protection Security Reports**, like watchmen in the towers, allow you to see configuration vulnerabilities, which are session and user risk signals that our machine learning, heuristic, and research systems detect.
- **Azure Active Directory Risk-Based Conditional Access**, like guards at the gate, allows you to put those risk signals to work, automatically intercepting bad sign-ins and deactivating compromised passwords.
- **Microsoft Cloud Application Security**, like a security escort, allows you to monitor and control activity between an app and the user.
- **Advanced Threat Analytics**, like a watchman in the treasury, provides deep forensic insights into what's happening in your on-premises environment, allowing you to see precisely how a hacker acted in your environment so you can provide a rapid response.
- **Azure Active Directory Privileged Identity Management**, like a keeper of keys, ensures that you have the minimum possible administrative attack surface by giving you just-in-time and just-enough administrative access.
- **Azure Information Protection**, like guards who protect treasure in transit, allows you to protect data with strong encryption and access policies regardless of where it goes.
- **Microsoft Intune Mobile Device Management and Mobile Application Management**, like a protector of the armory, help you ensure that devices and apps used in your organization are secure and healthy, again protecting data on these devices against device loss, malware, or other threats.

Let's garrison the castle and briefly talk about how these technologies work together to create a Secure Productive Enterprise. With the realities of shrinking IT budgets and increasing attacks it's a good time to learn how even a small garrison can hold off hordes of attackers.

Azure AD Identity Protection Security Reports: *the watchmen in the tower*

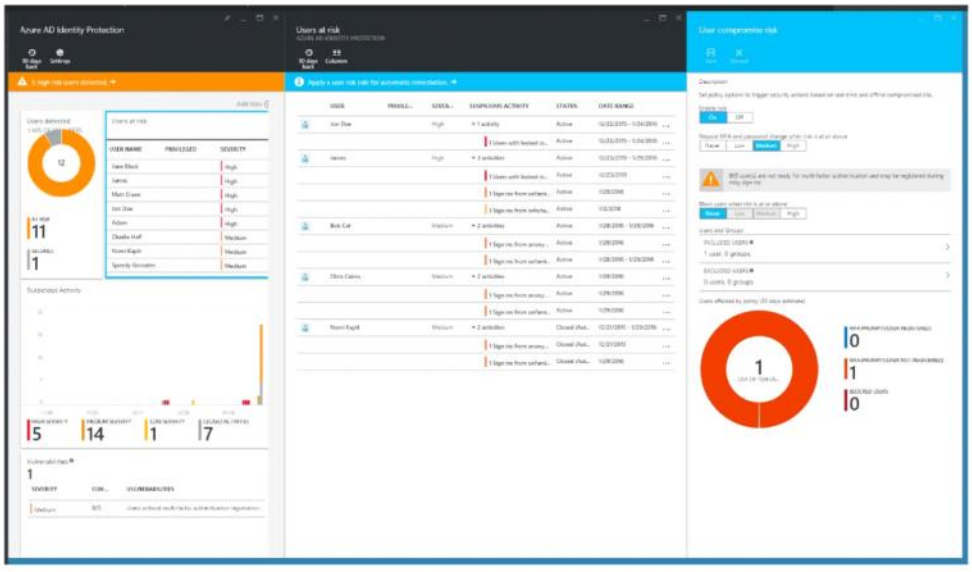
In addition to single sign-on for millions of companies and thousands of SaaS and on-premises applications (including, of course, Office 365), Microsoft's Identity Division also provides Microsoft account, our consumer-facing IdP, which supports Xbox, Outlook, OneDrive, Skype, and more. The combined data from these services—more than 10TB every day—gives us tremendous insight into what's normal behavior and, critically, what deviates from normal and indicates risk. This is our strongest signal source for Azure AD Identity Protection.

We get even more signal sources from other data in the Microsoft Intelligent Security Graph—botnet infections from the Digital Crimes Unit, data contributions, security research, and threat reports from the Microsoft Security Response Center, as well as SaaS specific data from services like Office 365 Exchange (for example, a good user started sending spam)—providing great triangulation on the signal from our identity services.

Security reports fall into three broad categories:

- Cases where a sign-in is anomalous and associated with some level of risk that it is an attempt at unauthorized access.
- Cases with significant indication that a user's credentials have been compromised, because they are showing up frequently in risky sign-ins, or because we have discovered them in criminal hands.
- Cases where your security posture could be improved, that is, vulnerabilities in your defenses that configuration changes can mitigate.

Azure AD Identity Protection Security Reports provide you all of this information, either in the Azure AD Portal or programmatically (so you can integrate it into your SIEM or ticketing system).



Azure AD Identity Protection Security Reports display risky users and sign-ins.

Learn more about Azure AD Identity Protection Security Reports here.

Like the watchmen posted high atop the castle tower, Azure AD Identity Protection Security Reports give you insights into what's happening in your environment so you can take action.

Now, imagine the watchmen see a problem and call down to the guards at the gate to give them warning...

Azure AD Conditional Access: *the guards at the gate*

One critical aspect of good security is that it's nearly invisible to most users. Excessive friction inhibits productivity, and clever users will find ways to work around things that block their productivity, which can create risk. While we could challenge every user at every sign-in, ideally, we maximize productivity by allowing users to get their work done with minimal interruption, while stopping the bad guys in their tracks.

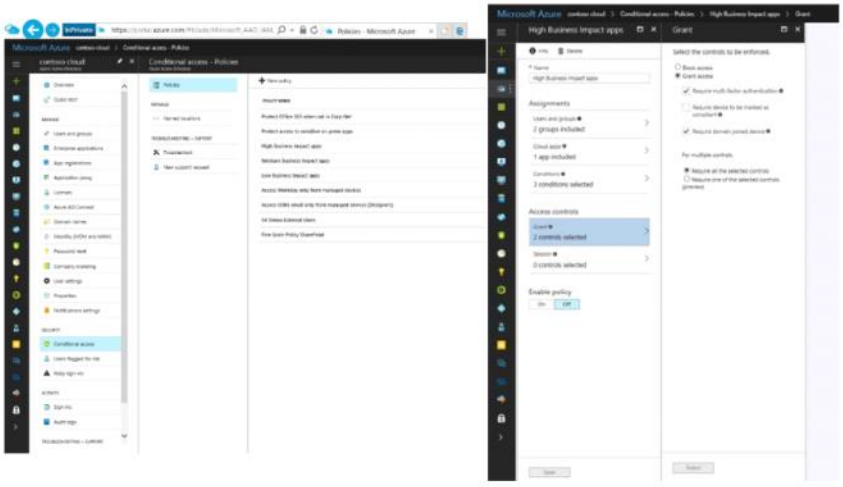
Azure AD Conditional Access allows us to do just that. Previously, you might've had to say, "No access from off the corporate network" or "No access from a personal device," but Azure AD Conditional Access allows you to say, effectively, "Yes, but there are conditions." For example, instead of blocking access to work email from a personal device, you can say one of the following:

- Yes, but you must be on a secure, compliant device (using Intune).
- Yes, but you must first pass a Multi-Factor Authentication challenge.
- Yes, but you won't be allowed to print, save, or download documents.

These are just a few examples. Azure AD Conditional Access provides a powerful framework for regulating access in governance, risk, and compliance scenarios. When combined with the information from AADIP, it gains even more power, allowing you to say, effectively, one of the following:

- Yes, unless there is risk in your session.
- Yes, but because your credentials are at risk you must first change your password.
- Yes, but we will monitor your session because of security concerns.

Adding Azure AD Identity Protection risk assessments to Azure AD Conditional Access allows you to relax challenges and friction in cases where no risk is present. It also allows you to have an "umbrella policy"—whatever else your corporate policies dictate, you can issue challenges in cases of unanticipated risks that the Intelligent Security Graph has detected in the sign-in, ensuring you stay secure in the face of evolving threats (this is by far the most important thing you can do to protect against compromised credentials!).



Azure AD Conditional Access allows good users to get their work done with minimal interruption.

In our castle analogy, you can think of Azure AD Conditional Access as the guards at the gate, welcoming good citizens into the castle while challenging others to confirm their identities, and denying entry to the riskiest.

Or perhaps we'll let them pass, but assign a security escort...

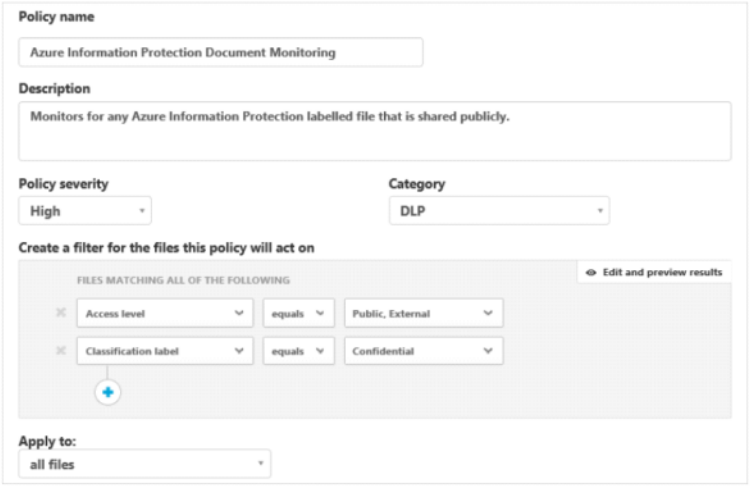
Microsoft Cloud App Security: *the security escort*

The primary role of Azure AD is to provide secure, reliable single sign-on for users across all applications, ensuring that only authorized users gain access. Effectively, it allows users to access all the critical resources they need to be productive once they've been authenticated.

But what if the authorized user does something wrong? What if they are no longer loyal to the organization, or are under duress? Or some malware is riding along in their session? Once Azure AD grants a user access, Azure AD can't see the specifics of what they do during their interactions with the application, making in-session anomalies invisible to Azure AD.

That's where Microsoft Cloud App Security comes in. Cloud App Security provides a mechanism to observe and manage what happens inside sessions between users and the applications they access. For example, Cloud App Security can tell you if a large volume of data is being accessed, apply specific API level restrictions based on configured policies, or even shut down a session if behavior become anomalous.

Together with Azure AD Conditional Access, Cloud App Security allows you to apply this enhanced monitoring and control when your policy requires it, and to protect yourself from session hijack, rogue users, and other session anomalies while ensuring good users can access resources with specific download or action restrictions to mitigate session risks.



Microsoft Cloud App Security helps you observe and manage sessions between users and the apps they access.

You can think of Microsoft Cloud App Security as the security escort, going along to ensure the user doesn't do—or come to—any harm.

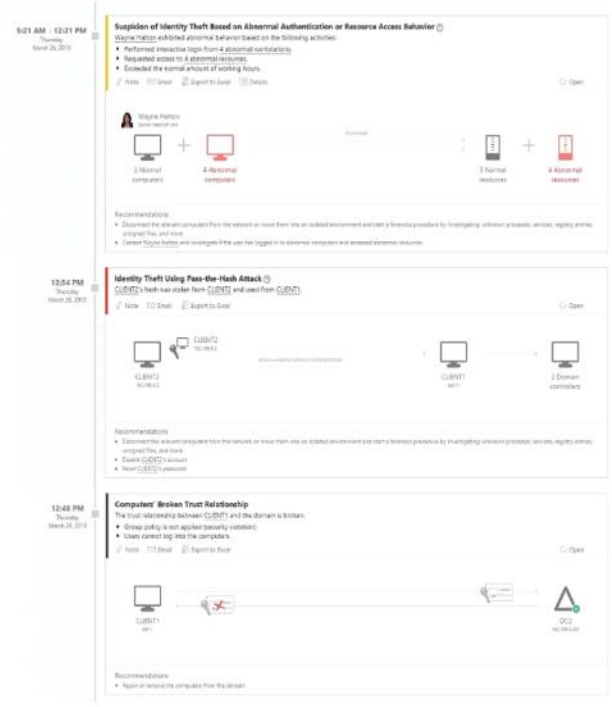
Microsoft Advanced Threat Analytics: *the watcher in the treasury*

The layers of defense described above provide very effective protection for your organization. Unfortunately, user behavior (e.g. falling for phishing attacks or re-using credentials on insecure sites), vulnerabilities of traditional on-premises infrastructure (e.g. VPNs), and clever attacks sometimes allow an attacker to get through.

Attackers move incredibly quickly once they gain access to a working credential, often VPN'ing into a corporate network and using log files, memory resident tokens, unencrypted files, and a host of other mechanisms to dig in and elevate privilege until, before you know it, they are domain admins and nearly impossible to get rid of.

Worse, where on-premises attacks are concerned, the network boundaries you relied on to keep you safe actually make it impossible for our cloud-based intelligence and protection mechanisms like Azure AD Identity Protection, Azure AD Conditional Access, and Cloud App Security to keep you safe.

Most companies have a great many legacy applications and resources running in their on-premises networks, so the hybrid environment is a reality for the foreseeable future. Unfortunately, these on-premises resources are often the most vulnerable when they have both inadequate security capabilities and valuable data.



Microsoft Advanced Threat Analytics helps you rapidly detect penetration of your on-premises environment.

The reality is that, as of this writing, if an attacker establishes a foothold in your on-premises environment, they will maintain it for an average of 140 days before you can begin to remove them—if you can remove them.

Luckily, Microsoft Advanced Threat Analytics gives you a tool to rapidly detect penetration of your on-premises environment so you can get attackers out before they dig in.

Advanced Threat Analytics quietly:

- builds a profile of what normal behavior looks like in your environment, and then
- notes any activity which differs from normal behavior, and then
- alerts you to these anomalies, along with an explanation of what attack the anomaly maps to, which resources are affected, and any recommended remediation.

Advanced Threat Analytics can you give you the rapid warning you need to respond before lateral movement or data exfiltration begin.

If your on-premises environment is like the royal treasury, Microsoft Advanced Threat Analytics is like the watcher hidden in the room, ready to sound the alarm if an attacker has broken in.

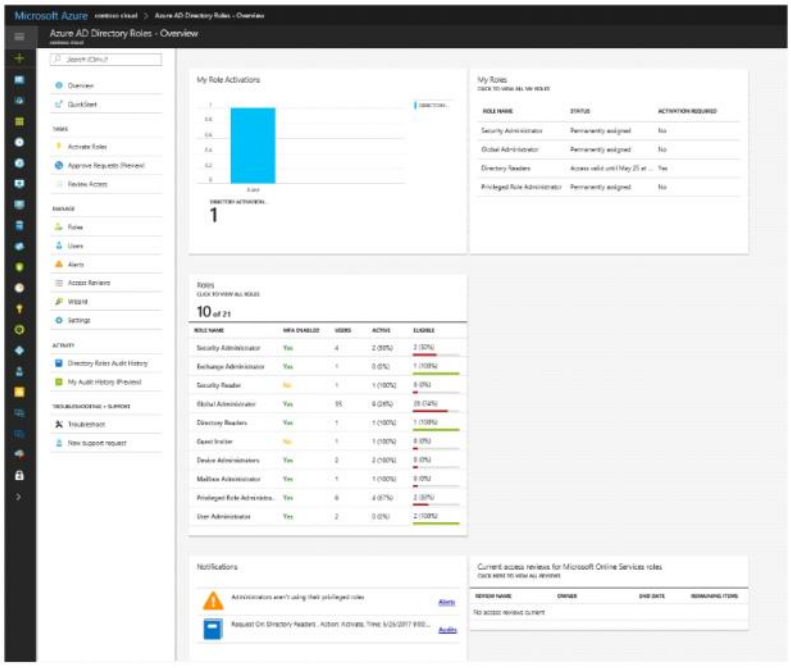
Azure AD Privileged Identity Management: *the keeper of keys*

The harsh reality is that with phishing, malware, breach, weak passwords, and lack of conditional access policies, determined attackers have a chance. Detection isn't always in real time, and sometimes false negatives occur. Since account compromise remains a possibility, the best way to minimize risk to your organization is to assume breach has happened or will happen.

While any compromised account is bad, a compromised admin account is catastrophic. If you assume some number of your organization's accounts will eventually be breached, it's critical to minimize the probability that those accounts have admin privileges.

Azure AD Privileged Identity Management gives you the tool you need to do just that. It empowers you to ensure you have the smallest possible number of admin-privileged users:

- It analyzes your environment to help identify whether you have admin privileges that are going unused or an excessive number of privileged users relative to your industry, allowing you to remove privileges from users who no longer need them.
- It helps you set up policies to grant admin access only when needed, on for as long as needed, and only in compliance with your elevation policies.



Azure AD Privileged Identity Management helps you minimize the number of admin-privileged users.

Most users who need to do privileged tasks only do so for a small fraction of their day. Using Azure AD Privileged Identity Management, you can set up a policy so that, for example, privileged access is only granted with manager approval, and only within a multi-factor authentication session, and only lasts for 60 minutes. In other words, policies are configurable to whatever makes most sense for your organization.

In this way, Azure AD Privileged Identity Management acts as a keeper of the keys, helping ensure that if a user is compromised, the most critical assets remain safe.

Microsoft Intune: *protect treasure in transit (part one)*

Even when we're sure an identity isn't compromised, there's always a chance a user will download content onto an unhealthy device, such as one that's unencrypted and missing PIN protection.

For example, if a user is synchronizing corporate mail onto a mobile phone which is not PIN locked, then anyone picking up that phone has unfettered access to everything in their mailbox. If a user has downloaded a spreadsheet full of key contract information onto their personal laptop and that laptop is stolen, so is the contract information.

Many devices act as a trust factor for user authentication or have active sessions, making unhealthy devices a threat to online resources as well. And malware, leaking user credentials every time the user does an interactive sign-in, is a real threat.

The age of Bring Your Own Device is here, but we must acknowledge the reality that bad things happen to good devices, whether malware, theft, or loss. Microsoft Intune can ensure that devices are safely in compliance and as resistant as possible to issues like malware and device theft.

In some cases, it may also make sense to ensure that only properly configured and approved applications are used to access sensitive data. Intune also supports mobile application management, ensuring that the application and its configuration is approved by your organization.

You can think of Intune as ensuring the integrity of the treasure chest and its locks, helping guarantee the security of what's inside.

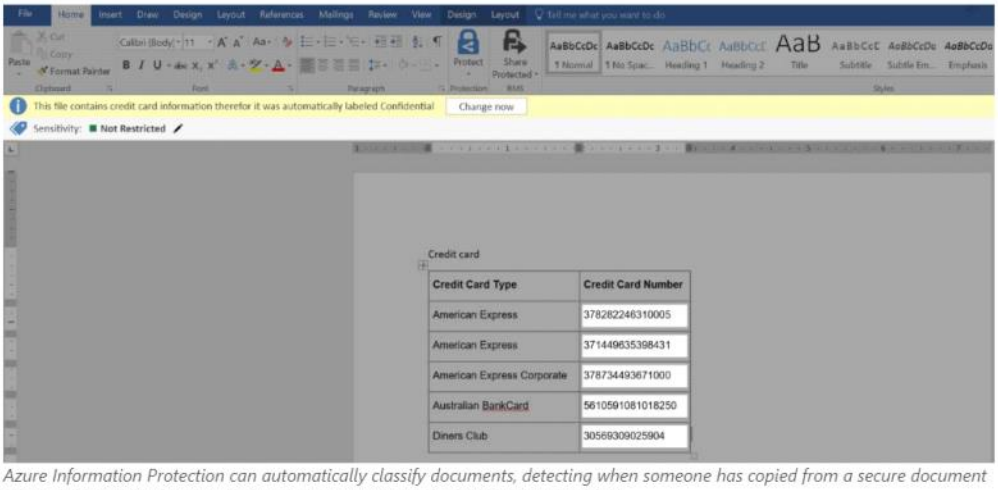
Azure Information Protection: *protect treasure in transit (part two)*

Even when we're able to ensure that the user accessing a resource in our environment is who they say they are and is well-behaved and in a healthy environment, the risk remains that they'll share a document with someone who's not, or become compromised after they've downloaded the content.

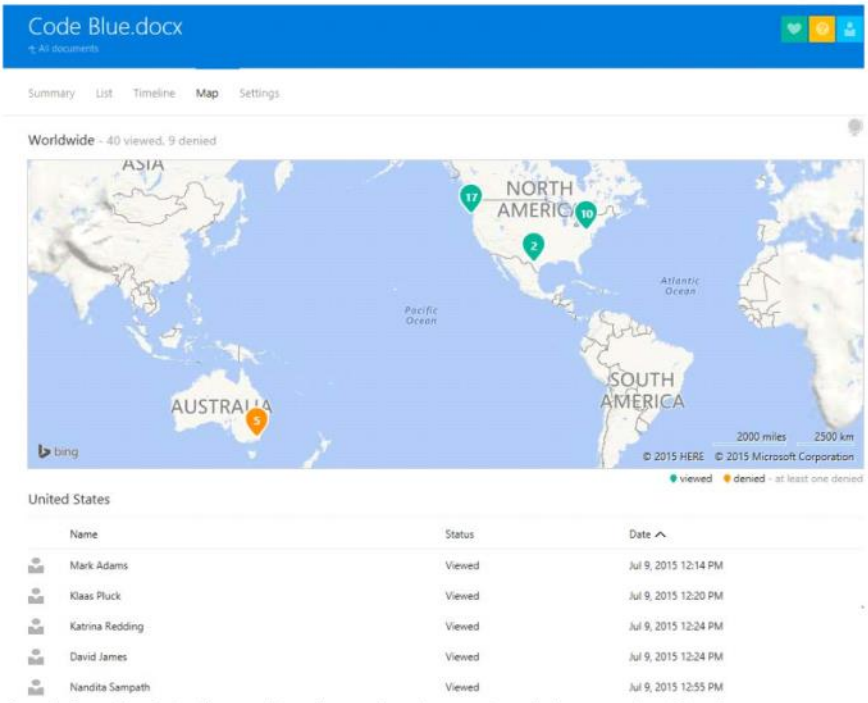
Azure Information Protection allows you to encrypt documents to ensure that even if the document is transmitted to an insecure environment, only authorized users, as defined by your policies, can access the document.

Better still, it can do the following:

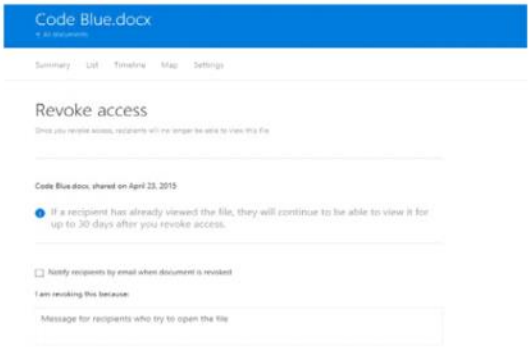
- Automatically classify documents, detecting when someone has copied from a secure document or is typing sensitive data, such as social security numbers or credit card numbers.
- Show you where documents are being opened, and by whom.
- Allow you to revoke all copies of a document, making it unreadable wherever it has gone.



Azure Information Protection can automatically classify documents, detecting when someone has copied from a secure document or is typing sensitive data, such as social security numbers or credit card numbers.



Azure Information Protection can let you know where documents are being opened, and by whom.



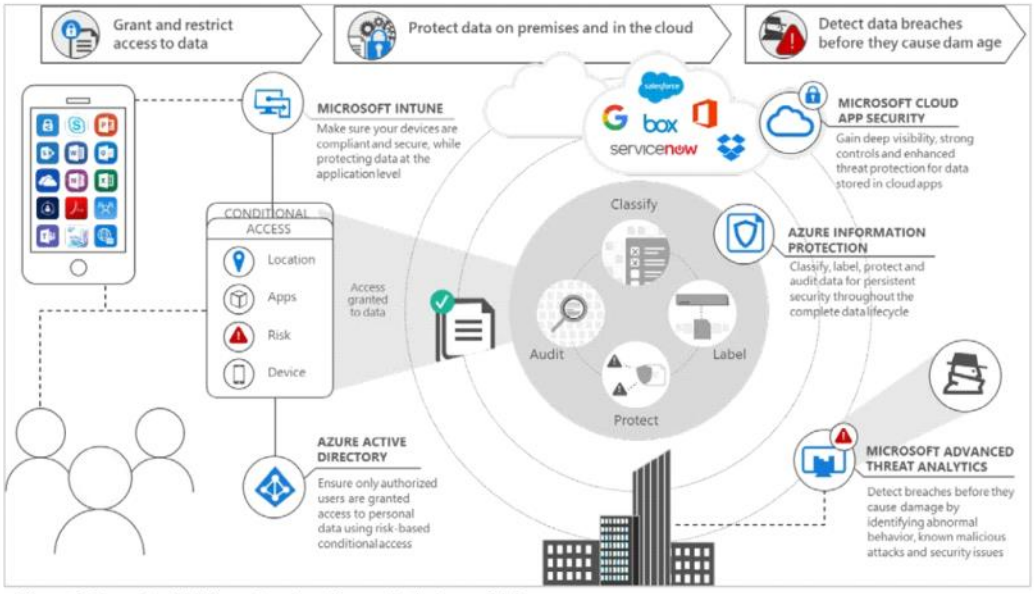
Azure Information Protection gives you the power to protect data in transit—wherever your data goes, you can be sure that only authorized people can read it.

In our castle analogy, Azure Information Protection is a bit of sorcery, ensuring the treasure turns to dust if it falls into the wrong hands.

Azure Information Protection allows you to revoke all copies of a document, making it unreadable wherever it has gone.

Putting it together: *defense in depth and EMS*

Now that you've toured the rings of defense, here's a map and table that summarize them:



Microsoft Enterprise Mobility + Security offers multiple rings of defense.

Feature	Capabilities	Threats Mitigated	Because
Azure AD Identity Protection Reports	Insights into risky sign-in attempts and users whose credentials are compromised	Undetected intrusion, highly vulnerable users	Criminals attempt almost 100M fraudulent sign-ins every day, and you should know if one impacts you.
Azure AD Conditional Access	Automated sign-in challenge (with multi-factor) or block based on governance, compliance, or risk factors	Attempted malicious sign-in, vulnerable users	You can intercept the clear majority of attacks before they can cause harm by having policy-based risk response to disrupt criminals.
Microsoft Cloud App Security	In-session monitoring and control	Rogue users, malware on machine	Sometimes an authorized user does unauthorized things—or their machine does.
Microsoft Advanced Threat Analytics	On-premises behavior analysis and anomaly detection, detection of bad actors in your organizational network	Undetected inside attackers or undetected attackers using stolen credentials via VPN	Your on-premises environment represents your greatest risk, making rapid response to intrusion your best hope.
Azure AD Privileged Identity Management	Detection and mitigation of excess administrative privilege, just-enough and just-in-time access for privileged tasks	Compromise of privileged accounts	Every admin account represents substantial risk if the account is compromised. For privileged access, less is more.
Microsoft Intune	Enforcement of device compliance with policies to ensure device health and safety, including PIN lock, encryption, and current malware protection	Data loss due to lost or stolen devices, infected devices	Machines get lost or stolen and malware can exfiltrate data.
Azure Information Protection	Securing of data in transit with encryption, document tracking, and auto-classification	Data loss due to non-compliant opening of documents	Documents get emailed outside of your span of control (to users and machines that may be insecure).

Summary

The brutal truth is that the rate and sophistication of attacks are increasing. Leaks of highly sophisticated attacks mated to old fashioned malware create new intersections of capabilities, while old techniques find new targets in governments and industry. The enemy is at the gates.

In a hostile environment with sophisticated attackers, we must assume breach—no one defense will suffice. Using the technologies and techniques above will help you establish a defensible fortress to protect your organization's integrity and operations.

And a guard in a bearskin hat can't hurt.

This paper explored the defense-in-depth capabilities of EMS. There are advanced security features in many Microsoft products, such as Windows Defender Advanced Threat Protection, the Microsoft Azure Security Center, or advanced security features in Windows Server. To learn more about these, please visit http://www.microsoft.com/security

Configure centralized policy management

October 25, 2021 9:26 AM

Overview of Azure Policy - Azure Policy | Microsoft Docs

- configure a custom security policy
  - Create custom security policies in Azure Security Center | Microsoft Docs
  - Azure security baseline for Azure Policy | Microsoft Docs
- create a policy initiative
  - Tutorial: Build policies to enforce compliance - Azure Policy | Microsoft Docs
  - Tutorial: Create a custom policy definition - Azure Policy | Microsoft Docs
  - Details of the initiative definition structure - Azure Policy | Microsoft Docs
- configure security settings and auditing by using Azure Policy

Configure and manage threat protection

October 25, 2021 9:26 AM

Overview of Azure Defender and the available plans | Microsoft Docs

- configure Azure Defender for Servers (not including Microsoft Defender for Endpoint)
  Azure Defender for servers - the benefits and features | Microsoft Docs

- evaluate vulnerability scans from Azure Defender
  Use Microsoft Defender for Endpoint's threat and vulnerability management capabilities with Azure Security Center | Microsoft Docs

- configure Azure Defender for SQL
  Azure Defender for SQL - the benefits and features | Microsoft Docs

- use the Microsoft Threat Modeling Tool
  Microsoft Security Development Lifecycle Threat Modelling
  Getting Started - Microsoft Threat Modeling Tool - Azure | Microsoft Docs

Configure and manage security monitoring solutions

October 25, 2021 9:26 AM

- create and customize alert rules by using Azure Monitor
  - Azure Monitor overview - Azure Monitor | Microsoft Docs
  - What is monitored by Azure Monitor - Azure Monitor | Microsoft Docs
  - Azure Monitor FAQ - Azure Monitor | Microsoft Docs
  - Tutorial - Create a metrics chart in Azure Monitor - Azure Monitor | Microsoft Docs
  - Azure Monitor best practices - Alerts and automated actions - Azure Monitor | Microsoft Docs
  - Azure Sentinel data connectors | Microsoft Docs
- configure diagnostic logging and log retention by using Azure Monitor
  - Send Azure Activity log to Log Analytics workspace using Azure portal - Azure Monitor | Microsoft Docs
  - Collect resource logs from an Azure Resource and analyze with Azure Monitor - Azure Monitor | Microsoft Docs
  - Tutorial - Create a metrics chart in Azure Monitor - Azure Monitor | Microsoft Docs
- monitor security logs by using Azure Monitor
  - What is Azure Sentinel? | Microsoft Docs
  - Best practices for Azure Sentinel | Microsoft Docs
- create and customize alert rules in Azure Sentinel
  - Create custom analytics rules to detect threats with Azure Sentinel | Microsoft Docs
  - Create incidents from alerts in Azure Sentinel | Microsoft Docs
- configure connectors in Azure Sentinel
  - Best practices for data collection in Azure Sentinel | Microsoft Docs
  - Find your Azure Sentinel data connector | Microsoft Docs
- evaluate alerts and incidents in Azure Sentinel
  - Investigate incidents with Azure Sentinel | Microsoft Docs
  - Use playbooks with automation rules in Azure Sentinel | Microsoft Docs
  - Hunting capabilities in Azure Sentinel | Microsoft Docs

KQL quick reference | Microsoft Docs
Kusto Query overview- Azure Data Explorer | Microsoft Docs
Manage usage and costs for Azure Monitor Logs - Azure Monitor | Microsoft Docs
Sources of data in Azure Monitor - Azure Monitor | Microsoft Docs

Azure Monitor ITSM Connector for ServiceNow ITOM with Secure Export | Azure updates | Microsoft Azure
Connect ServiceNow with IT Service Management Connector - Azure Monitor | Microsoft Docs

General Availability of Azure Sentinel Threat Intelligence in Public and Azure Government cloud - Microsoft Tech Community

Security Center

October 28, 2021 9:11 AM

What is Azure Security Center? | Microsoft Docs
Upgrade to Azure Defender - Azure Security Center | Microsoft Docs
Create a security automation for specific security alerts by using an Azure Resource Manager template (ARM template) | Microsoft Docs
Azure Security Benchmark | Microsoft Docs
Working with security policies | Microsoft Docs
Built-in policy definitions for Azure Security Center | Microsoft Docs
Reference table for all Azure Security Center recommendations | Microsoft Docs

Just-in-time virtual machine access in Azure Security Center | Microsoft Docs
Secure score in Azure Security Center | Microsoft Docs

Integrate security solutions in Azure Security Center | Microsoft Docs

Azure Security Center free vs Azure Defender enabled | Microsoft Docs
Enable Azure Security Center's integrated workload protections | Microsoft Docs
Auto-deploy agents for Azure Security Center | Microsoft Docs

Configure security for storage

October 25, 2021 9:27 AM

Security recommendations for Blob storage - Azure Storage | Microsoft Docs
Azure security baseline for Azure Storage | Microsoft Docs
Enabling Data Residency and Data Protection in Microsoft Azure Regions
Data Residency in Azure | Microsoft Azure
Require secure transfer to ensure secure connections - Azure Storage | Microsoft Docs
Time-based retention policies for immutable blob data - Azure Storage | Microsoft Docs
Legal holds for immutable blob data - Azure Storage | Microsoft Docs
Data redundancy - Azure Storage | Microsoft Docs
Ensure business continuity & disaster recovery using Azure Paired Regions | Microsoft Docs

Define a stored access policy - Azure Storage | Microsoft Docs

Azure Storage encryption for data at rest | Microsoft Docs

Create an account SAS - Azure Storage | Microsoft Docs
Service SAS examples - Azure Storage | Microsoft Docs

- configure access control for storage accounts
  - Authorize requests to Azure Storage (REST API) | Microsoft Docs
  - Configure anonymous public read access for containers and blobs - Azure Storage | Microsoft Docs

- configure storage account access keys
  - Authorize with Shared Key (REST API) - Azure Storage | Microsoft Docs

- configure Azure AD authentication for Azure Storage and Azure Files
  - Authorize with Azure Active Directory (REST API) - Azure Storage | Microsoft Docs

- configure delegated access
  - Delegate access with a shared access signature - Azure Storage | Microsoft Docs
  - Review the topics listed in the Delegate access link above

Enable infrastructure encryption for double encryption of data - Azure Storage | Microsoft Docs

NFS file shares (preview) in Azure Files | Microsoft Docs

Configure security for data

October 25, 2021 9:28 AM

Security Overview - Azure SQL Database & Azure SQL Managed Instance | Microsoft Docs

Azure Policy Regulatory Compliance controls for Azure SQL Database - Azure SQL Database | Microsoft Docs

Azure Policy Regulatory Compliance controls for Azure SQL Database - Azure SQL Database | Microsoft Docs
Playbook for addressing common security requirements - Azure SQL Database & Azure SQL Managed Instance | Microsoft Docs

IP firewall rules - Azure SQL Database and Azure Synapse Analytics | Microsoft Docs

Data Discovery & Classification - Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse | Microsoft Docs

Azure Defender for SQL - Azure SQL Database | Microsoft Docs

SQL vulnerability assessment - Azure SQL Database & SQL Managed Instance & Azure Synapse Analytics | Microsoft Docs

Configure Advanced Threat Protection - Azure SQL Database | Microsoft Docs

 enable database authentication by using Azure AD
Authorize server and database access using logins and user accounts - Azure SQL Database & SQL Managed Instance & Azure Synapse Analytics | Microsoft Docs
Azure Active Directory authentication - Azure SQL Database | Microsoft Docs

 enable database auditing
Azure SQL Auditing for Azure SQL Database and Azure Synapse Analytics - Azure SQL Database | Microsoft Docs

 configure dynamic masking on SQL workloads
Dynamic data masking - Azure SQL Database | Microsoft Docs

 implement database encryption for Azure SQL Database
Always Encrypted documentation - Azure SQL Database | Microsoft Docs
Transparent data encryption - Azure SQL Database & SQL Managed Instance & Azure Synapse Analytics | Microsoft Docs

 implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB

Configure and manage Azure Key Vault

October 25, 2021 9:28 AM

- create and configure Key Vault
  - Azure Key Vault Overview - Azure Key Vault | Microsoft Docs
  - Azure Key Vault Keys, Secrets, and Certificates Overview | Microsoft Docs
  - Azure Key Vault logging | Microsoft Docs
  - Azure Key Vault logging | Microsoft Docs
  - Get started with Key Vault certificates | Microsoft Docs
  - About Azure Key Vault Certificates access control | Microsoft Docs
  - Pricing Details - Key Vault | Microsoft Azure
  - Get started with Key Vault certificates | Microsoft Docs

- configure access to Key Vault
  - Manage secrets in your server apps with Azure Key Vault - Learn | Microsoft Docs
  - Configure encryption with customer-managed keys stored in Azure Key Vault - Azure Storage | Microsoft Docs
  - Azure Managed HSM Overview - Azure Managed HSM | Microsoft Docs

- manage certificates, secrets, and keys
  - Rotation tutorial for resources with one set of authentication credentials stored in Azure Key Vault | Microsoft Docs

- configure key rotation
  - Tutorial - Updating certificate auto-rotation frequency in Key Vault | Microsoft Docs

- configure backup and recovery of certificates, secrets, and keys
  - Back up a secret, key, or certificate stored in Azure Key Vault | Microsoft Docs
  - Azure Key Vault soft-delete | Microsoft Docs

Use the Secrets Store CSI driver for Azure Kubernetes Service secrets - Azure Kubernetes Service | Microsoft Docs
https://docs.microsoft.com/en-us/azure/aks/developer-best-practices-pod-security
https://hackerone.com/reports/694931

Application Security

October 27, 2021 10:59 AM

Assign an Azure Key Vault access policy (CLI) | Microsoft Docs

Microsoft Identity Platform

- Microsoft identity platform overview - Azure - Microsoft identity platform | Microsoft Docs
- Best practices for the Microsoft identity platform | Microsoft Docs

Azure AD App Scenarios

- Microsoft identity platform authentication flows & app scenarios | Microsoft Docs

App Registration

- Authentication and authorization basics for Microsoft Graph - Microsoft Graph | Microsoft Docs

Microsoft Graph Permissions

- Authentication and authorization basics for Microsoft Graph - Microsoft Graph | Microsoft Docs

Managed Identities

- Managed identities for Azure resources | Microsoft Docs
- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-manage-ua-identity-portal
- How managed identities for Azure resources work with with Azure virtual machines | Microsoft Docs

Web App Certificates

- Configure TLS mutual authentication - Azure App Service | Microsoft Docs