SC-900: Microsoft Security, Compliance, and Identity Fundamentals

Cybersecurity Introduction:

A cyberattack is commonly defined as an attempt to gain illegal access to a computer or computer system to cause damage or harm.

A cybercriminal is anyone who carries out a cyberattack.

Cybersecurity refers to technologies, processes, and training that help protect systems, networks, programs, and data from cyberattacks, damage, and unauthorized access.

Cybersecurity enables you to achieve the following goals:

1. **Confidentiality**: Information should only be visible to the right people.
2. **Integrity**: Information should only be changed by the right people or processes.
3. **Availability**: Information should be visible and accessible whenever needed.

This is commonly referred to as the *Confidentiality, Integrity, Availability* (CIA) model in the context of cybersecurity.

An *attack vector* is an entry point or route for an attacker to gain access to a system.

Any attack that results in someone gaining unauthorized access to devices, services, or networks is considered a *Security breach*.

Malware:

Malware comes from the combination of the words malicious and software. It's a piece of software used by cybercriminals to infect systems and carry out actions that will cause harm. This could include stealing data or disrupting normal usage and processes.

Malware has two main components:

1. Propagation mechanism

Propagation is how the malware spreads itself across one or more systems. Here are a few examples of common propagation techniques:

- Virus
- Worm
- Trojan

2. Payload

The payload is the action that a piece of malware performs on an infected device or system. Here are some common types of payloads:

- Ransomware
- Spyware
- Backdoors
- Botnet

A **Mitigation strategy** is a measure or collection of steps that an organization takes to prevent or defend against a cyberattack.

Cryptography:
cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

Plaintext (Normal data) → ciphertext (encrypted/secured data)
The plaintext message to be transformed into ciphertext. The mechanism that enables this is called ***encryption***.

Hashing uses an algorithm, also known as a **hashing function**, to convert the original text to a unique fixed-length value. This is called a hash value. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data. *Secure Hash Algorithm (SHA)* one of the more commonly used SHAs is SHA-256 which produces a hash value that is 256 bits long.

A digital certificate is a credential issued by a **certificate authority** (CA) that can be used to verify the identity of an individual or entity to whom the certificate is issued, referred to as the subject. In this sense, a digital certificate is like a passport or other identity credential issued by a trusted authority or government agency, it's used to verify an identity. The data in a certificate includes information about the subject, the subject's public key from their public/private key pair, and has been verified by the CA.

Authentication is the process of proving that a person is who they say they are.
When you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called *Authorization*.

A network is a grouping of interconnected physical components that work together to provide a seamless backbone for all your devices to communicate.

Typosquatting is a type of browser-based attack where a cybercriminal obtains deliberately misspelled domain names.
A zero-day vulnerability is any flaw that is previously unknown to the application owner and unpatched.

Cloud service types

Infrastructure as a service (IaaS): In an IaaS model, the cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical security. You're responsible for everything else: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on.

Platform as a service (PaaS): In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet. They also maintain the operating systems, middleware, development tools, and business intelligence services that make up a cloud solution.

Software as a service (SaaS): Software as a service (SaaS) is the most complete cloud service model from a product perspective. With SaaS, you're essentially renting or using a fully developed application. Email, financial software, messaging applications, and connectivity software are all common examples of a SaaS implementation.

Cloud computing

Cloud computing is the delivery of computing services over the internet. Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking. Cloud services also expand the traditional IT offerings to include things like Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI).

Types of cloud:

Private cloud: A private cloud is, in some ways, the natural evolution from a corporate datacentre. It's a cloud (delivering IT services over the internet) that's used by a single entity. Private cloud provides much greater control for the company and its IT department. However, it also comes with greater cost and fewer of the benefits of a public cloud deployment. Finally, a private cloud may be hosted from your onsite datacentre. It may also be hosted in a dedicated datacentre offsite, potentially even by a third party that has dedicated that datacentre to your company.

Public cloud: A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources. The general public availability is a key difference between public and private clouds.

Hybrid cloud: A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources.

Multi-cloud: In a multi-cloud scenario, you use multiple public cloud providers. Maybe you use different features from different cloud providers. Or maybe you started your cloud

journey with one provider and are in the process of migrating to a different provider. Regardless, in a multi-cloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments.

Azure Arc is a set of technologies that helps manage your cloud environment. Azure Arc can help manage your cloud environment, whether it's a public cloud solely on Azure, a private cloud in your datacentre, a hybrid configuration, or even a multi-cloud environment running on multiple cloud providers at once.

Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability.

High availability focuses on ensuring maximum availability, regardless of disruptions or events that may occur.

Scalability refers to the ability to adjust resources to meet demand. Scaling generally comes in two varieties: vertical and horizontal.

Vertical scaling is focused on increasing or decreasing the capabilities of resources(such as CPUs and RAMs).

Horizontal scaling is adding or subtracting the number of resources(such as virtual machines or containers).

Reliability is the ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework.

Predictability in the cloud lets you move forward with confidence. Predictability can be focused on performance predictability or cost predictability. Both performance and cost predictability are heavily influenced by the Microsoft Azure Well-Architected Framework.

Shared responsibility model:

The *shared responsibility model* identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer.

Zero Trust model: The Zero Trust model operates on the principle of "**trust no one, verify everything.**"

The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

Compliance concepts:

Data residency - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.

Data sovereignty - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed. This can add a layer of complexity when it comes to compliance because the same piece of data can be collected in one location, stored in another, and processed in still another; making it subject to laws from different countries/regions.

Data privacy - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations. Personal data means any information relating to an identified or identifiable natural person. Privacy laws previously referenced "PII" or "personally identifiable information" but the laws have expanded the definition to any data that is directly linked or indirectly linkable back to a person. Organizations are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy.

Modern authentication:

With modern authentication, all services, including all authentication services, are supplied by a central identity provider. Information that's used to authenticate the user with the server is stored and managed centrally by the identity provider.

When the identity (which can be a user or an application) has been verified, the identity provider issues a *security token* that the client sends to the server.

The server validates the security token through its *trust relationship* with the identity provider. By using the security token and the information that's contained within it,

the user or application accesses the required resources on the server. In this scenario, the token and the information it contains is stored and managed by the identity provider. The centralized identity provider is supplying the authentication service.

Microsoft Azure Active Directory is an example of a cloud-based identity provider. Other examples include Twitter, Google, Amazon, LinkedIn, and GitHub.

A directory service stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks.

The best-known service of this kind is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

AD DS is a central component in organizations with on-premises IT infrastructure. AD DS gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. AD DS doesn't, however, natively support mobile devices, SaaS applications, or line of business apps that require *modern authentication* methods.

Azure Active Directory is the next evolution of identity and access management solutions. It provides organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

Azure Active Directory: Azure AD is used by IT admins to control access to corporate apps and resources, based on business requirements. Azure AD also provides APIs that allow developers to build personalized app experiences using existing organizational data.

Azure AD is available in four editions: Free, Office 365 Apps, Premium P1, and Premium P2.

1. **Azure Active Directory Free**. The free version allows you to administer users and create groups, synchronize with on-premises Active Directory, create basic reports, configure self-service password change for cloud users, and enable single sign-on across Azure, Microsoft 365, and many popular SaaS apps. The free edition is included with subscriptions to Office 365, Azure, Dynamics 365, Intune, and Power Platform.
2. **Office 365 Apps**. The Office 365 Apps edition allows you to do everything included in the free version, plus self-service password reset for cloud users,

and device write-back, which offers two-way synchronization between on-premises directories and Azure AD. The Office 365 Apps edition of Azure Active Directory is included in subscriptions to Office 365 E1, E3, E5, F1, and F3.

3. **Azure Active Directory Premium P1**. The Premium P1 edition includes all the features in the free and Office 365 apps editions. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
4. **Azure Active Directory Premium P2**. P2 offers all the Premium P1 features, and Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data. P2 also gives you Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources, and to provide just-in-time access when needed.

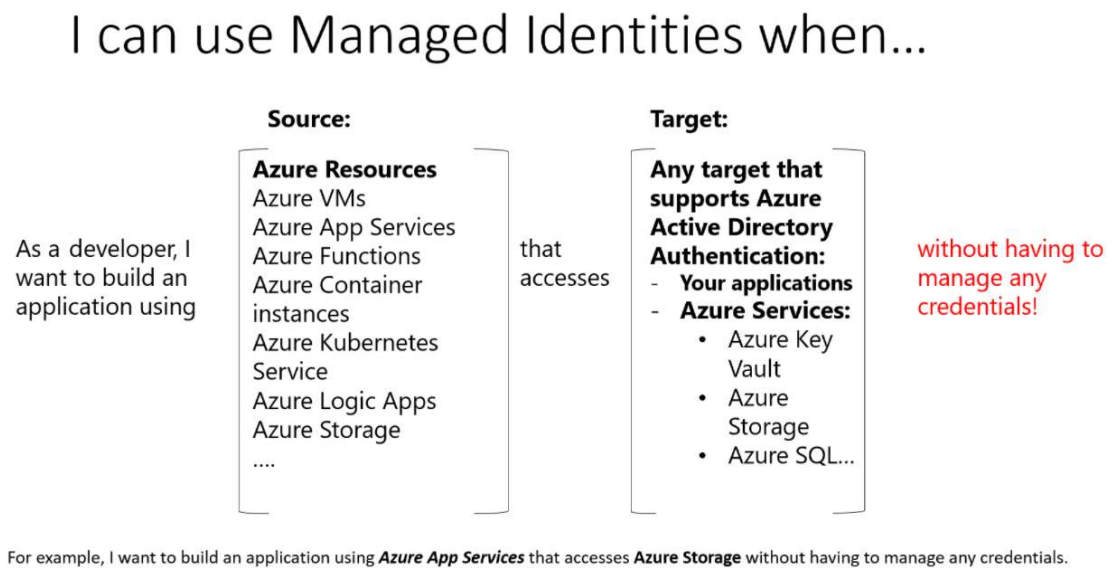
Azure AD identities:

A ***User*** identity is a representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD. If you have several users with the same access needs, you can create a group. You use groups to give access permissions to all members of the group, instead of having to assign access rights individually.

Azure AD business-to-business (B2B) collaboration, a feature within External Identities, includes the capability to add guest users. With B2B collaboration, an organization can securely share applications and services with guest users from another organization.

A ***Service principal*** is, essentially, an identity for an application. For an application to delegate its identity and access functions to Azure AD, the application must first be registered with Azure AD to enable its integration. Once registered, a service principal is created in each Azure AD tenant where the application is used. The service principal enables core features such as authentication and authorization of the application to resources that are secured by the Azure AD tenant.

Managed identities are a type of service principal that are automatically managed in Azure AD and eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to Azure resources that support Azure AD authentication and can be used without any extra cost.



There are two types of managed identities: system-assigned and user-assigned.

System-assigned. Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity, an identity is created in Azure AD that's tied to the lifecycle of that service instance. When the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.

User-assigned. You may also create a managed identity as a standalone Azure resource. Once you create a user-assigned managed identity you can assign it to one or more instances of an Azure service. With user-assigned managed identities, the identity is managed separately from the resources that use it.

A ***Device*** is a piece of hardware, such as mobile devices, laptops, servers, or printers. A device identity gives administrators information they can use when making access or configuration decisions. Device identities can be set up in different ways in Azure AD.

- **Azure AD registered devices**. The goal of Azure AD registered devices is to provide users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization's resources using a personal device. Azure AD registered devices register to Azure AD without requiring an organizational account to sign in to the device. Supported operating systems for Azure AD registered devices include Windows 10 and above, iOS, Android, and macOS.

- **Azure AD joined**. An Azure AD joined device is a device joined to Azure AD through an organizational account, which is then used to sign in to the device. Azure AD joined devices are generally owned by the organization. Supported operating systems for Azure AD joined devices include Windows 10 or greater (except Home edition) and Windows Server 2019 Virtual Machines running in Azure.
- **Hybrid Azure AD joined devices**. Organizations with existing on-premises Active Directory implementations can benefit from the functionality provided by Azure AD by implementing hybrid Azure AD joined devices. These devices are joined to your on-premises Active Directory and Azure AD requiring organizational account to sign in to the device.

Azure AD External Identities is a set of capabilities that enable organizations to allow access to external users, such as customers or partners. Your customers, partners, and other guest users can "bring their own identities" to sign in.

There are two different Azure AD External Identities: B2B and B2C.

- B2B collaboration allows you to share your apps and resources with external users.
- B2C is an identity management solution for consumer and customer facing apps.

Azure AD External Identities is a feature of Premium P1 and P2 Azure AD editions, and pricing is based on Monthly Active Users.

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this **hybrid identity**.

When it comes to authentication of hybrid identities, Microsoft offers several ways to authenticate.

- Azure AD Password hash synchronization.
    - The Active Directory domain service (AD DS) stores passwords in the form of a hash value representation, of the actual user password. With Azure AD password hash synchronization, the password hash is extracted from the on-premises Active Directory instance using Azure AD Connect.
- Azure AD Pass-through authentication
    - Azure AD pass-through authentication allows users to sign in to both on-premises and cloud-based applications using the same passwords, like password hash synch. A key difference, however, is when users sign in using Azure AD, pass-through authentication validates users' passwords directly against your on-premises Active Directory.

Password validation doesn't happen in the cloud. This can be an important factor for organizations wanting to enforce their on-premises Active Directory security and password policies.

- Federated authentication
    - In federated authentication, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. This sign-in method ensures that all user authentication occurs on-premises.
    - Organizations that decide to use Federation with Active Directory Federation Services (AD FS), can optionally set up password hash synchronization as a backup in case their AD FS infrastructure fails.

Azure AD offers different methods of authentication:

1. *Passwords* are the most common form of authentication, but they have many problems, especially if used in single-factor authentication, where only one form of authentication is used.
2. Azure AD supports two options for phone-based authentication.

    - Short message service (SMS) used in mobile device text messaging can be used as a primary form of authentication.
    - Users can use voice calls as a secondary form of authentication, to verify their identity, during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication.

3. OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP is implemented using either software or hardware to generate the codes.
4. Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This two-factor authentication is a combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics).
5. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources using an external security key or a platform key built into a device, eliminating the need for a username and password.
6. As a passwordless authentication method, the Microsoft Authenticator app can be used as a primary form of authentication to sign in to any Azure AD account or as an additional verification option during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication events.

Conditional Access is a feature of Azure AD that provides an extra layer of security before allowing authenticated users to access data or other assets.

Azure AD roles control permissions to manage Azure AD resources.

Managing access using roles is known as **role-based access control (RBAC)**. Azure AD built-in and custom roles are a form of RBAC in that Azure AD roles control access to Azure AD resources. This is referred to as Azure AD RBAC.

Azure AD RBAC - Azure AD roles control access to Azure AD resources such as users, groups, and applications.
Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.

Azure AD Privileged Identity Management (PIM) provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Azure AD, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources. PIM is a feature of Azure AD Premium P2.

Entitlement management is an identity governance feature that enables organizations to manage the identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.

Entitlement management includes the following capabilities to address these challenges:

- Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.
- Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

Azure Active Directory (AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.
Azure AD terms of use allow information to be presented to users, before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.
Conditional Access policies are used to require a terms of use statement being displayed, and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined.

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These include resources in Azure AD, Azure, and other Microsoft online services such as Microsoft 365 or Microsoft Intune. PIM mitigates the risks of excessive, unnecessary, or misused access permissions. It requires justification to understand why users want permissions and enforces multifactor authentication to activate any role.

Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. Sign-in risk can be calculated in real-time or calculated offline using Microsoft's internal and external threat intelligence sources.

Identity Protection provides organizations with three reports that they can use to investigate identity risks in their environment. These reports are the **risky users**, **risky sign-ins**, and **risk detections**. Investigation of events is key to understanding and identifying any weak points in your security strategy.

Distributed Denial of Service (DDoS) attacks: The aim of a Distributed Denial of Service (DDoS) attack is to overwhelm the resources on your applications and servers, making them unresponsive or slow for genuine users. A DDoS attack will usually target any public-facing device that can be accessed through the internet.

The three most frequent types of DDoS attack are:

- **Volumetric attacks**: These are volume-based attacks that flood the network with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through. These types of attacks are measured in bits per second.
- **Protocol attacks**: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. These types of attacks are typically measured in packets per second.
- **Resource (application) layer attacks**: These attacks target web application packets, to disrupt the transmission of data between hosts.

The *Azure DDoS Protection service* is designed to help protect your applications and servers by analysing network traffic and discarding anything that looks like a DDoS attack.

Azure DDoS Protection comes in three tiers:

- **Default DDoS infrastructure protection** (previously referred to as Basic): The default DDoS infrastructure protection service is automatically enabled for every property in Azure, at no extra cost, as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.
- **DDoS Network Protection**: The DDoS Network Protection service (available as a SKU), combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It's automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes. DDoS Network Protection has several advantages over the default infrastructure-level DDoS protection, including logging, alerting, and telemetry. See DDoS Protection overview for more details.
- **DDoS IP Protection**: DDoS IP Protection is a pay-per-protected IP model. DDoS IP Protection contains the same core engineering features as DDoS Network Protection, but will differ in the following value-added services: DDoS rapid response support, cost protection, and discounts on WAF.

Azure Firewall is a managed, cloud-based network security service that protects your Azure virtual network (VNet) resources from attackers.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.

Segmentation is about dividing something into smaller pieces. Network segmentation also supports the Zero Trust model and a layered approach to security that is part of a defense in depth strategy.

Network segmentation can secure interactions between perimeters. This approach can strengthen an organization's security posture, contain risks in a breach, and stop attackers from gaining access to an entire workload.

Azure Virtual Network (VNet) is the fundamental building block for your organization's private network in Azure. Additional benefits of Azure's infrastructure such as scale, availability, and isolation compared to traditional network.

Azure VNet enables organizations to segment their network. Organizations can create multiple VNets per region per subscription, and multiple smaller networks (subnets) can be created within each VNet.

VNets provide network level containment of resources with no traffic allowed across VNets or inbound to the VNet, by default. Communication needs to be explicitly provisioned. This enables more control over how Azure resources in a VNet communicate with other Azure resources, the internet, and on-premises networks.

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine. An NSG consists of rules that define how the traffic is filtered. You can associate only one network security group to each virtual network subnet and network interface in a virtual machine. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

An NSG is made up of inbound and outbound security rules. NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. By default, Azure creates a series of rules, three inbound and three outbound rules, to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Each rule specifies one or more of the following properties:

- **Name**: Every NSG rule needs to have a unique name that describes its purpose. For example, AdminAccessOnlyFilter.
- **Priority**: Rules are processed in priority order, with lower numbers processed before higher numbers. When traffic matches a rule, processing stops. This means that any other rules with a lower priority (higher numbers) won't be processed.
- **Source or destination**: Specify either individual IP address or an IP address range, service tag (a group of IP address prefixes from a given Azure service), or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- **Protocol**: What network protocol will the rule check? The protocol can be any of: TCP, UDP, ICMP or Any.
- **Direction**: Whether the rule should be applied to inbound or outbound traffic.
- **Port range**: You can specify an individual or range of ports. Specifying ranges enables you to be more efficient when creating security rules.
- **Action**: Finally, you need to decide what will happen when this rule is triggered.

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. Azure Bastion provides secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Key features of Azure Bastion

The following features are available:

- **RDP and SSH directly in Azure portal**: You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.
- **Remote session over TLS and firewall traversal for RDP/SSH**: From the Azure portal, a connection to the VM, will open an HTML5 based web client that is automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely. The connection is made secure by using the Transport Layer Security (TLS) protocol to establish encryption.
- **No Public IP required on the Azure VM**: Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.
- **No hassle of managing NSGs**: A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.
- **Protection against port scanning**: Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.
- **Hardening in one place to protect against zero-day exploits**: Azure Bastion is a fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don't need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

Just-in-time (JIT) access allows lock down of the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT requires Microsoft Defender for servers to be enabled on the subscription.

Espionage, data theft, and data exfiltration are a real threat to any company.

Encryption on Azure

Microsoft Azure provides many different ways to secure your data, each depending on the service or usage required.

- **Azure Storage Service Encryption** helps to protect data at rest by automatically encrypting before persisting it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and decrypts the data before retrieval.
- **Azure Disk Encryption** helps you encrypt 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 data disks.
- **Transparent data encryption (TDE)** helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Azure Key Vault is a centralized cloud service for storing your application secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities.

- **Secrets management**. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
- **Key management**. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- **Certificate management**. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for Azure, and internally connected, resources more easily.
- **Store secrets backed by hardware security modules (HSMs)**. The secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Cloud security posture management (CSPM) is a relatively new class of tools designed to improve your cloud security management. It assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud environment to monitor and prioritize security enhancements and features.

CSPM uses a combination of tools and services:

- **Zero Trust-based access control**: Considers the active threat level during access control decisions.
- **Real-time risk scoring**: To provide visibility into top risks.
- **Threat and vulnerability management (TVM)**: Establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.
- **Discover risks**: To understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.
- **Technical policy**: Apply guardrails to audit and enforce the organization's standards and policies to technical systems.
- **Threat modeling systems and architectures**: Used alongside other specific applications.

Microsoft Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

Microsoft Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- **Continuously assess** - Know your security posture, identify and track vulnerabilities.
- **Secure** - Harden all connected resources and services.
- **Defend** - Detect and resolve threats to resources, workloads, and services.

The features of Microsoft Defender for Cloud, that deliver on these requirements, cover two broad pillars of cloud security: cloud security posture management and cloud workload protection.

In Microsoft Defender for Cloud, the posture management features provide:

- Visibility - to help you understand your current security situation
- Hardening guidance - to help you efficiently and effectively improve your security

Through cloud workload protection capabilities, Microsoft Defender for Cloud is able to detect and resolve threats to resources, workloads, and services. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads.

Microsoft Defender for Cloud is offered in two modes:

- Microsoft Defender for Cloud (Free) - Microsoft Defender for Cloud is enabled for free on all your Azure subscriptions. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.
- Microsoft Defender for Cloud with enhanced security features - Enabling enhanced security extends the capabilities of the free mode to workloads running in Azure, hybrid, and other cloud platforms, providing unified security management and threat protection across your workloads. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads.

Microsoft Defender for Cloud plans you can select from are:

- **Microsoft Defender for servers** adds threat detection and advanced defenses for your Windows and Linux machines.
- **Microsoft Defender for App Service** identifies attacks targeting applications running over App Service.
- **Microsoft Defender for Storage** detects potentially harmful activity on your Azure Storage accounts.
- **Microsoft Defender for SQL** secures your databases and their data wherever they're located.
- **Microsoft Defender for Kubernetes** provides cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.
- **Microsoft Defender for container registries** protects all the Azure Resource Manager based registries in your subscription.
- **Microsoft Defender for Key Vault** is advanced threat protection for Azure Key Vault.
- **Microsoft Defender for Resource Manager** automatically monitors the resource management operations in your organization.
- **Microsoft Defender for DNS** provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
- **Microsoft Defender for open-source relational protections** brings threat protections for open-source relational databases.

Microsoft cloud security benchmark is the successor of Azure Security Benchmark (ASB), which was rebranded in October 2022. It is currently in public preview.

The Microsoft cloud security benchmark and security baselines for Azure, which are closely related, help organizations secure their cloud solutions on Azure.

Some of the key pieces of information in MCSB are:

- ID - Each line item in the MCSB has an identifier that maps to a specific recommendation.
- Control domain - A control is a high-level description of a feature or activity that needs to be addressed and isn't specific to a technology or implementation. MCSB control domains include network security, data protection, identity management, privileged access, incident response, endpoint security to name just a few.
- Mapping to industry frameworks - The recommendations included in the MCSB map to existing industry frameworks such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standards (PCI DSS) frameworks. This makes security and compliance easier for customer applications running on Azure services.
- Recommendation - For each control domain area there can be many distinct recommendations. Each recommendation captures specific functionality associated with the control domain area and is itself a control. For example, the "Network Security" control domain in MCSB v1 has 10 distinct recommendations identified as NS-1 through NS-10. Each of these recommendations describes a specific control under network security. The recommendation identified as NS-1 is to establish network segmentation boundaries.
- Security principle - Each recommendation lists a "Security Principle" that explains the "what" for the control at the technology-agnostic level. For the recommendation to establish network segmentation boundaries, one of the points included in the security principle is that any workload that could incur higher risk for the organization should be in isolated virtual networks.
- Azure Guidance - Azure Guidance is focused on the "how", elaborating on the relevant technical features and ways to implement the controls in Azure. Continuing with the example of NS-1, the Azure guidance includes information regarding creating a virtual network (VNet), using network security groups (NSG), and using an application security group (ASG).
- AWS Guidance - The AWS guidance is focused on the "how" specific to AWS, explaining the AWS technical features and implementation basics.

Mapping to industry frameworks

ID	Control Domain	CIS Controls v7.1 ID(s)	CIS Controls v8 ID(s)	NIST SP800-53 r4 ID(s)	PCI-DSS v3.2.1 ID(s)	Recommendation	Security Principle	Azure Guidance	Implementation and additional context	AWS Guidance
NS-1	Network Security	9.2 - Ensure Only Approved Ports, Protocols and Services Are Running 9.4 - Apply Host-Based Firewalls or Port Filtering 12.3 - Deny	3.12 - Segment Data Processing and Storage Based on Sensitivity 13.4 - Perform Traffic Filtering Between Network	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Establish network segmentation boundaries	Ensure that your virtual network deployment aligns to your enterprise segmentation strategy defined in the GS-2 security control. Any workload that could incur higher risk for the organization should be in isolated virtual networks.	Create a virtual network (VNet) as a fundamental segmentation approach in your Azure network, so resources such as VMs can be deployed into the VNet within a network boundary. To further segment the network, you can create subnets inside VNet for smaller sub-networks.	Azure Virtual Network concepts and best practices: https://docs.microsoft.com/azure/virtual-network/concepts-and-best-practices Add, change, or delete a virtual network subnet: https://docs.microsoft.com/	Create a Virtual Private Cloud (VPC) as a fundamental segmentation approach in yo AWS network, so resources such as EC2 instances can be deployed into the VPC wit a network boundary. To further segment th network, you can create subnets inside VPC smaller sub-networks. For EC2 instances, use Security Groups, as a
NS-2	Network Security	14.1 - Segment the Network Based on Sensitivity	3.12 - Segment Data Processing and Storage Based on Sensitivity 4.4 - Implement and Manage a	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING	1.1 1.2 1.3	Secure cloud native services with network controls	Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access from public network when possible.	Deploy private endpoints for all Azure resources that support the Private Link feature, to establish a private access point for the resources. Using Private Link will keep the private connection from routing through the public network.	Understand Azure Private Link: https://docs.microsoft.com/azure/private-link/private-link-overview	Deploy VPC PrivateLink for all AWS resourc that support the PrivateLink feature, to allo private connection to the supported AWS services or services hosted by other AWS accounts (VPC endpoint services). Using PrivateLink will keep the private connectior from routing through the public network.

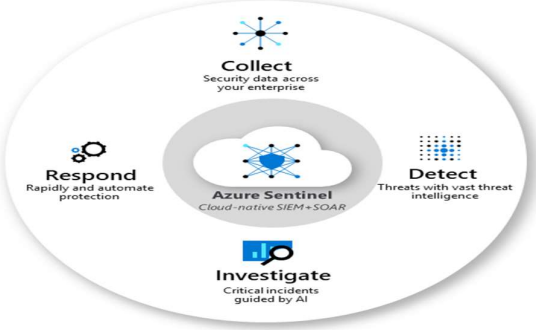
Security baselines are standardized documents for Azure product offerings, describing the available security capabilities and the optimal security configurations to help you strengthen security through improved tooling, tracking, and security features. Service baselines are currently only available for Azure.

- **Control ID**: The Microsoft cloud security benchmark ID that corresponds to the control (recommendation) in the Microsoft cloud security benchmark.
- **Feature**: Security feature(s) that can help you meet that control requirement.
- **Feature Description**: A high-level description of the feature and how it fits into the product offering.
- **Supported**: A true/false value indicating if this feature is supported to secure this product offering.
- **Enabled by Default**: A true/false value indicating if this feature is enabled in a default deployment by Microsoft.
- **Configuration Responsibility**: Who is responsible for implementing the configuration guidance (where possible scenarios are Customer responsibility, Microsoft responsibility or Shared responsibility).
- **Configuration Guidance**: Actionable guidance to implement the configurations.
- **Microsoft Defender for Cloud monitoring Note**: Microsoft Defender for Cloud policy / monitoring information. (Note: If a feature is not monitored by Microsoft Defender for Cloud for the service, this section is omitted.)
- **Reference**: A reference link to dive deeper into how to implement the configuration guidance.

A *Security information event management (SIEM)* system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

A *Security orchestration automated response (SOAR)* system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

Microsoft Sentinel is a scalable, cloud native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.



Microsoft Sentinel helps enable end-to-end security operations, in a modern Security Operations Centre (SOC). Listed below are some of the key features of Microsoft Sentinel.

Connect Sentinel to your data: Microsoft sentinel has built in own connecters for Microsoft tools like Azure AD, Office 365, etc. And Microsoft Sentinel GitHub repository or by following generic deployment procedures for how to connect your data source to Microsoft Sentinel for data sources outside the Microsoft tools.

Workbooks: After you connect data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks. You'll see a canvas for data analysis and the creation of rich visual reports within the Azure portal. Through this integration, Microsoft Sentinel allows you to create custom workbooks across your data. It also comes with built-in workbook templates that allow quick insights across your data as soon as you connect a data source.

Analytics: Microsoft Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve.

Manage incidents in Microsoft Sentinel: Incident management allows you to manage the lifecycle of the incident. View all related alerts that are aggregated into an incident. You can also triage and investigate.

Security automation and orchestration: You can use Microsoft Sentinel to automate some of your security operations and make your security operations center (SOC) more productive. Microsoft Sentinel integrates with Azure Logic Apps, so you can create automated workflows, or playbooks, in response to events. A security playbook is a collection of procedures that can help SOC engineers and analysts of all tiers to automate and simplify tasks and orchestrate a response. Playbooks work best with single, repeatable tasks, and require no coding knowledge.

Investigation: Microsoft Sentinel's deep investigation tools help you to understand the scope of a potential security threat and find the root cause.

Hunting: Use Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework (a global database of adversary tactics and techniques), to proactively hunt for security threats across your organization’s data sources, before

an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.

While hunting, you can bookmark interesting events. Bookmarking events enables you to return to them later, share them with others, and group them with other correlating events to create a compelling incident for investigation.

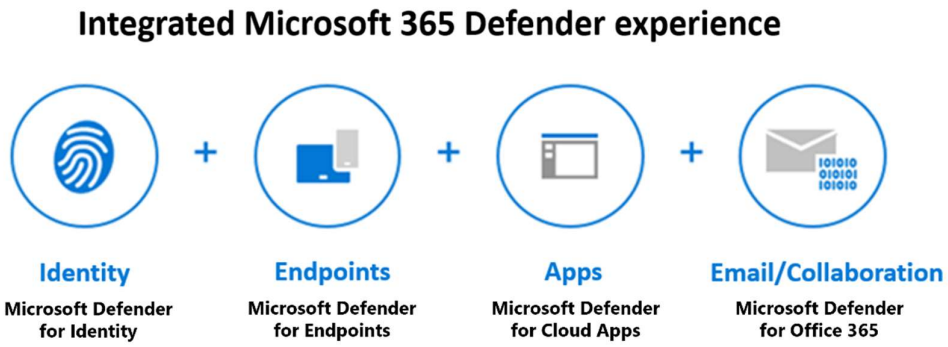
Notebooks: Microsoft Sentinel supports Jupyter notebooks. Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. You can use Jupyter notebooks in Microsoft Sentinel to extend the scope of what you can do with Microsoft Sentinel data.

Community: The Microsoft Sentinel community is a powerful resource for threat detection and automation. Microsoft security analysts constantly create and add new workbooks, playbooks, hunting queries, and more, posting them to the community for you to use in your environment.

Microsoft Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Billing is based on the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace. There are two ways to pay for the Microsoft Sentinel service: Capacity Reservations and Pay-As-You-Go.

- **Capacity Reservations**: With Capacity Reservations, you're billed a fixed fee based on the selected tier, enabling a predictable total cost for Microsoft Sentinel.
- **Pay-As-You-Go**: With Pay-As-You-Go pricing, you're billed per gigabyte (GB) for the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace.

Microsoft 365 Defender is an enterprise defense suite that protects against sophisticated cyberattacks. With Microsoft 365 Defender, you can natively coordinate the detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications.



Microsoft 365 Defender suite protects:

- **Identities with Microsoft Defender for Identity and Azure AD Identity Protection** - Microsoft Defender for Identity uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- **Endpoints with Microsoft Defender for Endpoint** - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.
- **Applications with Microsoft Defender for Cloud Apps** - Microsoft Defender for Cloud Apps is a comprehensive cross-SaaS solution that brings deep visibility, strong data controls, and enhanced threat protection to your cloud apps.
- **Email and collaboration with Microsoft Defender for Office 365** - Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Microsoft Defender for Office 365 covers these key areas:

- **Threat protection policies**: Define threat protection policies to set the appropriate level of protection for your organization.
- **Reports**: View real-time reports to monitor Microsoft Defender for Office 365 performance in your organization.
- **Threat investigation and response capabilities**: Use leading-edge tools to investigate, understand, simulate, and prevent threats.
- **Automated investigation and response capabilities**: Save time and effort investigating and mitigating threats.

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and detection tools for your Office 365 suite:

- **Safe Attachments**: Checks email attachments for malicious content.
- **Safe Links**: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.
- **Safe Attachments for SharePoint, OneDrive, and Microsoft Teams**: Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.
- **Anti-phishing protection**: Detects attempts to impersonate your users and internal or custom domains.
- **Real-time detections**: A real-time report that allows you to identify and analyze recent threats.

Microsoft Defender for Office 365 Plan 2

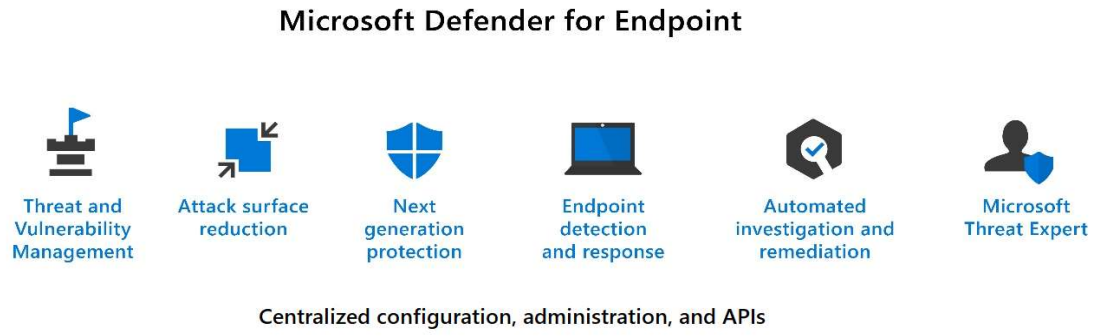
This plan includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite:

- **Threat Trackers**: Provide the latest intelligence on prevailing cybersecurity issues, and allow an organization to take countermeasures before there's an actual threat.
- **Threat Explorer**: A real-time report that allows you to identify and analyze recent threats.
- **Automated investigation and response (AIR)**: Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.
- **Attack Simulator**: Allows you to run realistic attack scenarios in your organization to identify vulnerabilities. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.
- **Proactively hunt for threats with advanced hunting in Microsoft 365 Defender**: Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities.
- **Investigate alerts and incidents in Microsoft 365 Defender**: Microsoft Defender for Office 365 P2 customers have access to Microsoft 365 Defender integration to efficiently detect, review, and respond to incidents and alerts.

Microsoft Defender for Office 365 is included in certain subscriptions, such as Microsoft 365 E5, Office 365 E5, Office 365 A5, and Microsoft 365 Business Premium.

If your subscription doesn't include Defender for Office 365, you can purchase it as an add-on. Use Microsoft Defender for Office 365 to protect your organization's collaboration tools and messages.

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints. It does so by preventing, detecting, investigating, and responding to advanced threats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and Microsoft cloud services.



Microsoft Defender for Endpoint includes:

- **Threat and vulnerability management**: A risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. It uses sensors on devices to avoid the need for agents or scans, and prioritizes vulnerabilities.
- **Attack surface reduction**: The attack surface reduction set of capabilities provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs; helping prevent apps from accessing dangerous locations
- **Next generation protection**: Brings together machine learning, big data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices in your enterprise organization.
- **Endpoint detection and response**: Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.
- **Automated investigation and remediation**: The automated investigation feature uses inspection algorithms and processes used by analysts (such as playbooks) to examine alerts and take quick remediation action to resolve breaches. This process significantly reduces the volume of alerts that must be investigated individually.
- **Microsoft Threat Experts**: A managed threat hunting service that provides Security Operation Centers (SOCs) with monitoring and analysis tools to ensure critical threats don't get missed.
- **Management and APIs**: Provides APIs to integrate with other solutions.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB). It's a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the cloud provider. Microsoft Defender for Cloud Apps provides rich visibility to your

cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Use this service to gain visibility into Shadow IT by discovering the cloud apps being used. You can control and protect data in the apps after you sanction them to the service.

A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use, wherever they're located, and regardless of the device they're using. CASBs help organizations protect their environment by providing a wide range of capabilities across the following pillars:

- **Visibility** - Detect cloud services and app use and provide visibility into Shadow IT.
- **Threat protection** - Monitor user activities for anomalous behaviors, control access to resources through access controls, and mitigate malware.
- **Data security** - Identify, classify and control sensitive information, protecting against malicious actors.
- **Compliance** - Assess the compliance of cloud services.

These capability areas represent the basis of the Defender for Cloud Apps framework described below.

The Defender for Cloud Apps framework

Microsoft Defender for Cloud Apps is built on a framework that provides the following capabilities:

- **Discover and control the use of Shadow IT**: Identify the cloud apps, and IaaS and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks.
- **Protect against cyberthreats and anomalies**: Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage, and remediate automatically to limit risks.
- **Protect your sensitive information anywhere in the cloud**: Understand, classify, and protect the exposure of sensitive information at rest. Use out-of-the-box policies and automated processes to apply controls in real time across all your cloud apps.
- **Assess your cloud apps' compliance**: Assess if your cloud apps meet relevant compliance requirements, including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.

Microsoft Defender for Cloud Apps functionality

Defender for Cloud Apps Security delivers on the components of the framework through an extensive list of features and functionality. Listed below are some examples.

- **Cloud Discovery** maps and identifies your cloud environment and the cloud apps your organization uses. Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps being used.
- **Sanctioning and unsanctioning apps** in your organization by using the Cloud apps catalog that includes over 25,000 cloud apps. The apps are ranked and scored based on industry standards. You can use the cloud app catalog to rate the risk for your cloud apps based on regulatory certifications, industry standards, and best practices.
- Use **App connectors** to integrate Microsoft and non-Microsoft cloud apps with Microsoft Defender for Cloud Apps, extending control and protection. Defender for Cloud Apps queries the app for activity logs, and it scans data, accounts, and cloud content that can be used to enforce policies, detect threats and provide governance actions to resolve issues.
- **Conditional Access** App Control protection provides real-time visibility and control over access and activities within your cloud apps. Avoid data leaks by blocking downloads before they happen, setting rules to require data stored in and downloaded from the cloud to be protected with encryption, and controlling access from non-corporate or risky networks.
- Use **policies** to detect risky behavior, violations, or suspicious data points and activities in your cloud environment. You can use policies to integrate remediation processes to achieve risk mitigation.

Office 365 Cloud App Security is a subset of Microsoft Defender for Cloud Apps that provides enhanced visibility and control for Office 365. Office 365 Cloud App Security includes threat detection based on user activity logs, discovery of Shadow IT for apps with similar functionality to Office 365 offerings, control app permissions to Office 365, and apply access and session controls.

Azure Active Directory Premium P1 includes Azure Active Directory Cloud App Discovery at no extra cost. This feature is based on the Microsoft Defender for Cloud Apps Cloud Discovery capabilities that provide deeper visibility into cloud app usage in your organization.

Microsoft Defender for Identity is a cloud-based security solution. It uses your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user.

For hybrid environments in which Active Directory Federation Services (AD FS) is present, Defender for Identity protects the AD FS by detecting on-premises attacks and providing visibility into authentication events generated by the AD FS.

Assets might include sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill-chain:

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance

Microsoft 365 Defender natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. The Microsoft 365 Defender portal brings this functionality together into a central place that is designed to meet the needs of security teams and emphasizes quick access to information, simpler layouts. Through the Microsoft 365 Defender portal you can view the security health of your organization.
The Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day-to-day jobs.

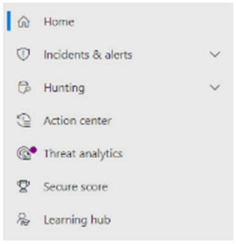
The cards fall into these categories:

- Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors.
- Data - Help track user activity that could lead to unauthorized data disclosure.
- Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.
- Apps - Gain insight into how cloud apps are being used in your organization.

You must be assigned an appropriate role, such as Global Administrator, Security Administrator, Security Operator, or Security Reader in Azure Active Directory to access the Microsoft 365 Defender portal.

The Microsoft 365 Defender portal allows admins to tailor the navigation pane to meet daily operational needs. Admins can customize the navigation pane to show or hide functions and services based on their specific preferences. Customization is specific to the individual admin, so other admins won't see these changes.

The left navigation pane provides security professionals easy access to the email and collaboration capabilities of Microsoft Defender for Office 365 and the capabilities for Microsoft Defender for Endpoint which were described in the previous units. Listed below we describe a few of the other capabilities accessible from the left navigation bar in the Microsoft 365 Defender portal.



Secure score in Microsoft Defender for Cloud is a measure of the security posture of your Azure subscriptions. Secure score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

The Service Trust Portal (STP) is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored whitepapers that provide details on how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

The Service Trust Portal landing page includes content that is organized into the following categories:

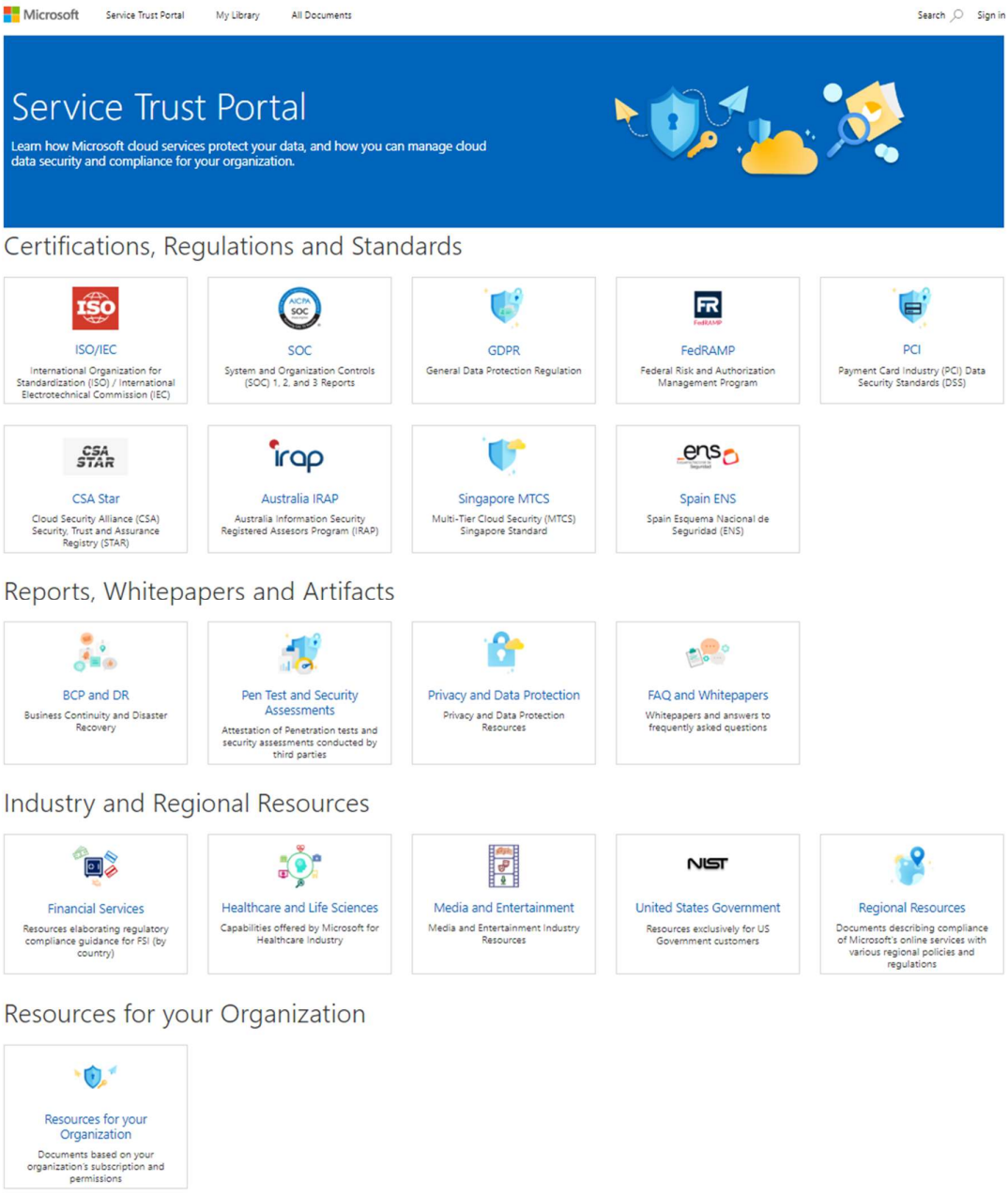
- Certifications, Regulations, and Standards
- Reports, Whitepapers, and Artifacts
- Industry and Regional Resources
- Resources for your Organization

Microsoft's approach to privacy is built on the following six principles: Control, Transparency, Security, Strong legal protections, No content based targeting, Benefits to you.

Microsoft Priva helps you meet these challenges so you can achieve your privacy goals. Priva's capabilities are available through two solutions: **Priva Privacy Risk Management**, which provides visibility into your organization's data and policy templates for reducing risks; and **Priva Subject Rights Requests**, which provides automation and workflow tools for fulfilling data requests.

Priva evaluates your organization's data stored in the following Microsoft 365 services within your Microsoft 365 tenant:

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams



The Microsoft Purview compliance portal is the portal for organizations to manage their compliance needs using integrated solutions for information protection, information governance, insider risk management, auditing, and more.

The compliance portal is available to customers with a Microsoft 365 SKU with one of the following roles:

- Global administrator
- Compliance administrator
- Compliance data administrator

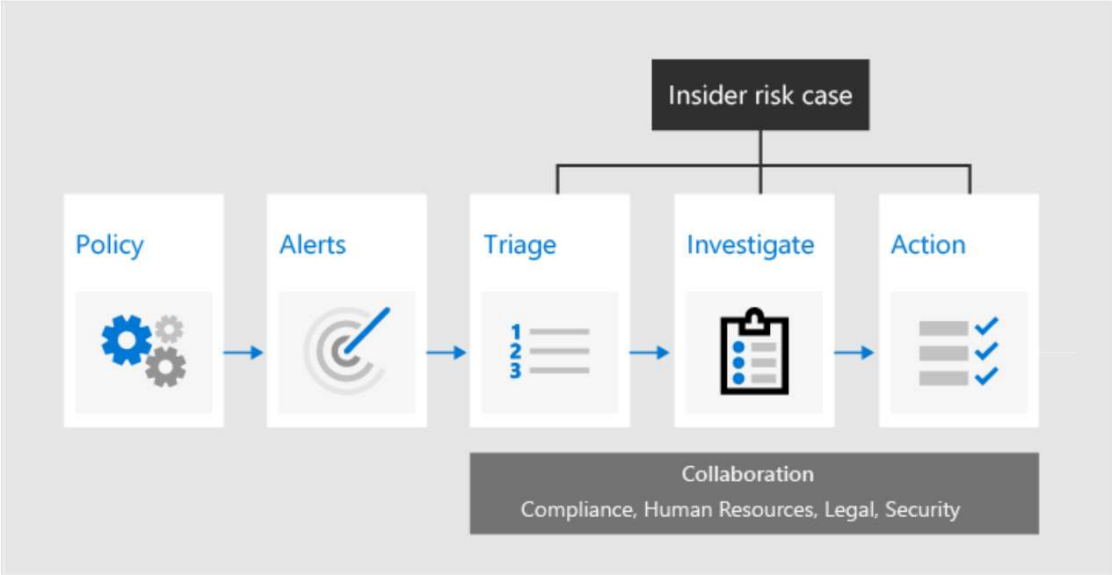
Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps admins to manage an organization's compliance requirements with greater ease and convenience.

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in the Microsoft Purview compliance portal.

Insider risk management is centered around the following principles:

- **Transparency**: Balance user privacy versus organization risk with privacy-by-design architecture.
- **Configurable**: Configurable policies based on industry, geographical, and business groups.
- **Integrated**: Integrated workflow across Microsoft Purview solutions.
- **Actionable**: Provides insights to enable user notifications, data investigations, and user investigations.



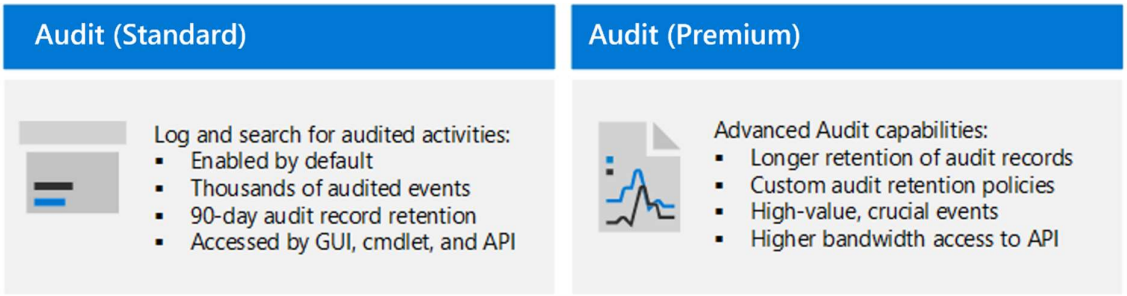
Communication compliance in the Microsoft Purview compliance portal helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages.

Microsoft Purview Information Barriers is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).

Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium).



Azure Policy is designed to help enforce standards and assess compliance across your organization. Azure Policy is designed to help enforce standards and assess compliance across your organization.

Azure Policy evaluates all resources in Azure and Arc enabled resources (specific resource types hosted outside of Azure).

Azure Policy evaluates whether the properties of resources match with business rules. These business rules are described using JSON format, and referred to as policy definitions. For simplified management, you can group together multiple business rules to form a single policy initiative. After business rules have been formed, you can assign the policy definition, or policy initiative, to any scope of resources that are supported, such as management groups, subscriptions, resource groups, or individual resources.

Azure Blueprints provide a way to define a repeatable set of Azure resources. Azure Blueprints enable development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance requirements. Teams can also provision Azure resources across several subscriptions simultaneously, meaning they can achieve shorter development times and quicker delivery.

Azure Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Microsoft Purview governance portal provides a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data.