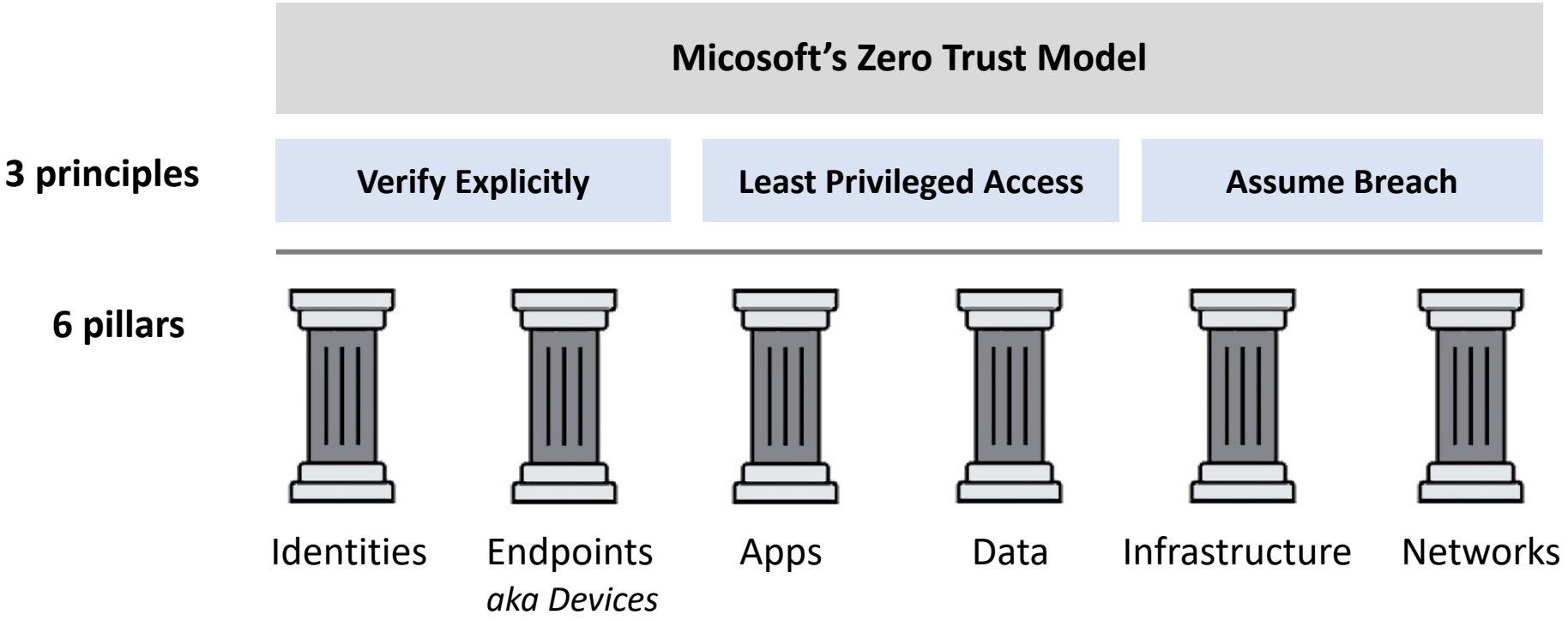
Zero-Trust Methodologies

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

Malicious actors being able to by-pass conventional **access controls** demonstrates traditional security measures are no long sufficient



Zero-Trust Methodologies – Principles

Verify explicitly
Always authenticate and authorize based on all available data points.

Least privileged access / Principle of Least Privilege (PoLP)
Limit user access with **Just-In-Time** and **Just-Enough-Access** (JIT/JEA), risk-based adaptive policies, and data protection.

Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Zero-Trust Methodologies – Pillars

Identities
Verify and secure each identity with strong authentication across your entire digital estate.

- Identity Access and Management (IAM)
- Azure Active Directory
- Single Sign On
- Multi-Factor Authentication
- Passwordless Authentication
- Risk-based policies
- Identity Secure Score

Endpoints (Devices)
Gain visibility into devices accessing the network. Ensure compliance and health status before granting access.

- Register devices to your IpD (Azure AD device management)
- Microsoft Intune (MDM and MAM)
- Microsoft Endpoint Manager
- Microsoft Defender for Endpoints
- Data Loss Prevention (DLP) Policies

Apps
Discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, and monitor and control user actions.

- Policy-based access controls
- Microsoft Cloud App Security (MCAS)
- Azure AD Application Proxy
- Cloud Discovery
- JIT VM access

Zero-Trust Methodologies – Pillars

Data
Move from perimeter-based data protection to data-driven protection. Use intelligence to classify and label data. Encrypt and restrict access based on organizational policies.

- Sensitivity Labels
- Microsoft Information Protection
- Data Classification
- Azure Information Protection (AIP) scanner
- decision-based policies
- Data Loss Prevention (DLP) Policies

Infrastructure
Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior, and employ least privilege access principles.

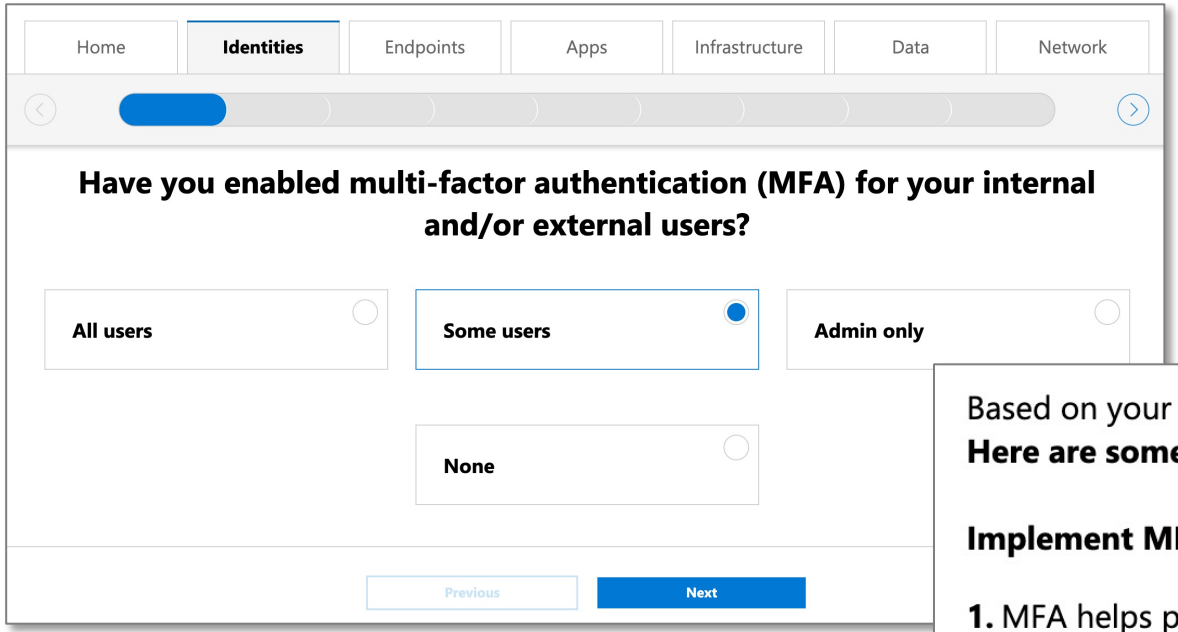
- Azure Security Center
- Azure AD Managed Identities
- User and resource segmentation
- VNeTs
- Peering rules
- Privileged Identity Management
- Network Security Groups (NSG)
- Application Security Groups (ASG)
- Azure Firewall
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Azure Sentinel

Network
Ensure devices and users aren't trusted just because they're on an internal network. Encrypt all internal communications, limit access by policy, and employ microsegmentation and real-time threat detection.

- Network Segmentation
- Azure Ddos Protection Service
- Azure Firewall
- Azure Web Application Firewall (WAF)
- Azure VPN
- Azure AD Proxy
- Azure Bastion
- SSL/TLS

Zero-Trust Assessment Tool

A free tool to assess your organization degree of adoption toward a Zero-Trust model and suggests to improve your current security implementations



Based on your responses, you are in the **traditional** Zero Trust Identity stage.
Here are some recommendations on how you can continue on your Zero Trust journey.

Implement MFA

1. MFA helps protect your applications by using a second source of validation, (something they are and something they have) like a phone or token, to verify identity before granting access.

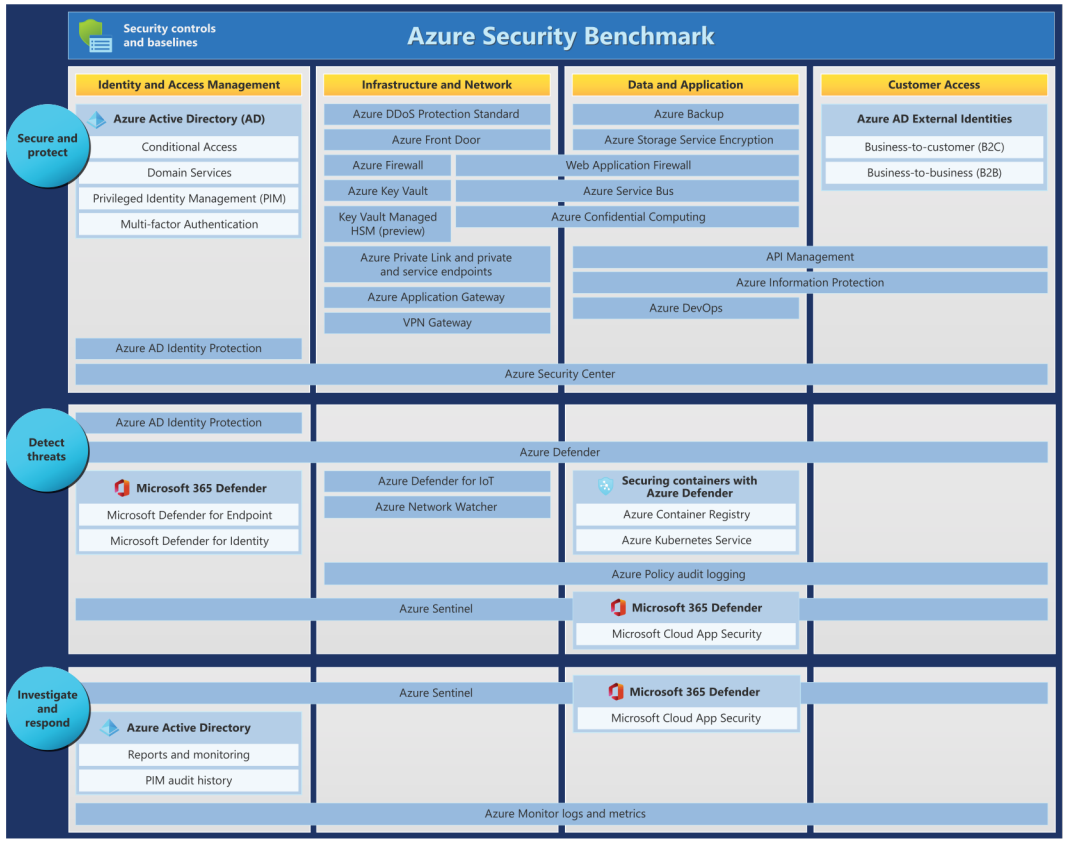
2. Azure Active Directory (Azure AD) can help you enable multi-factor authentication for free.

3. Already have Azure AD? Start deploying today

Microsoft Security Services Map (MSSM)

Microsoft Security Services Map is a **tabular visualization** to **introduce you to the security services** in Azure

- **columns** — Resources we want to protect
- **rows** — Services used to protect resources



Services are grouped into 3 categories:

Secure and protect
Services that let you implement a layered, **defense in-depth** strategy across identity, hosts, networks, and data. This collection of security services and capabilities provides a way to understand and improve your **security posture** across your Azure environment.

Detect threats
Services that identify suspicious activities and facilitate mitigating the threat.

Investigate and respond
Services that pull logging data so you can assess a suspicious activity and respond.

MSSM – Secure and Protect

IAM

- Azure AD
  - Conditional Access
  - Domain Services
  - PIM
  - MFA
- Azure AD Identity Protection

Infra. and Network

- Azure DDOS Protection Standard
- Azure Front Door
- Azure Firewall
- Azure Application Firewall
- Azure Key Vault
- Azure Service Bus
- Azure Key Managed HSM
- Azure Confidential Computing
- Azure Private Links
- Azure Application Gateway
- VPN Gateway

Data and Apps

- Azure Backup
- Azure Storage Service Encryption
- API Management
- Azure Information Protection
- Azure DevOps

Customer Access

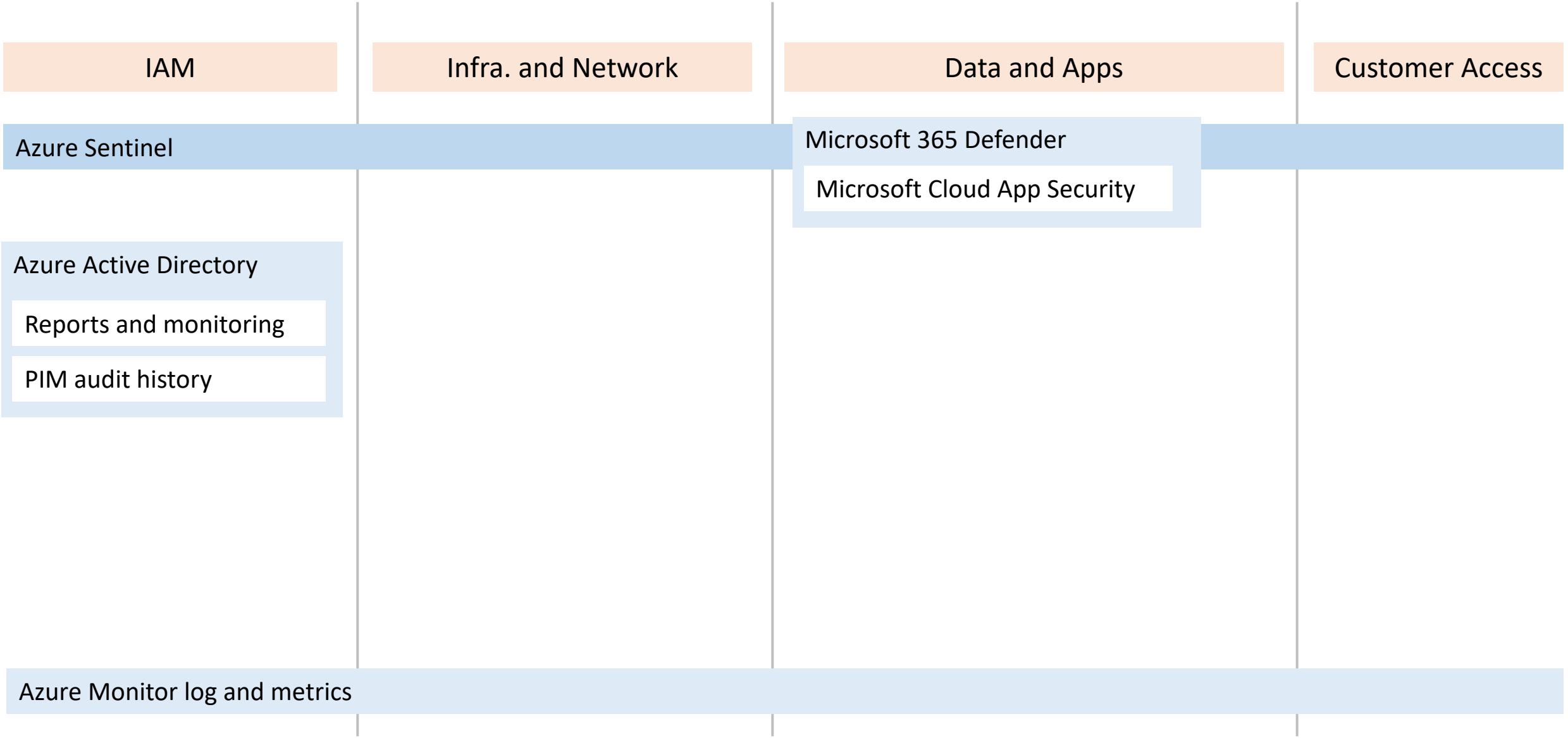
- Azure AD External Identities
  - B2C
  - B2B

Azure Security Center

MSSM – Detect Threats

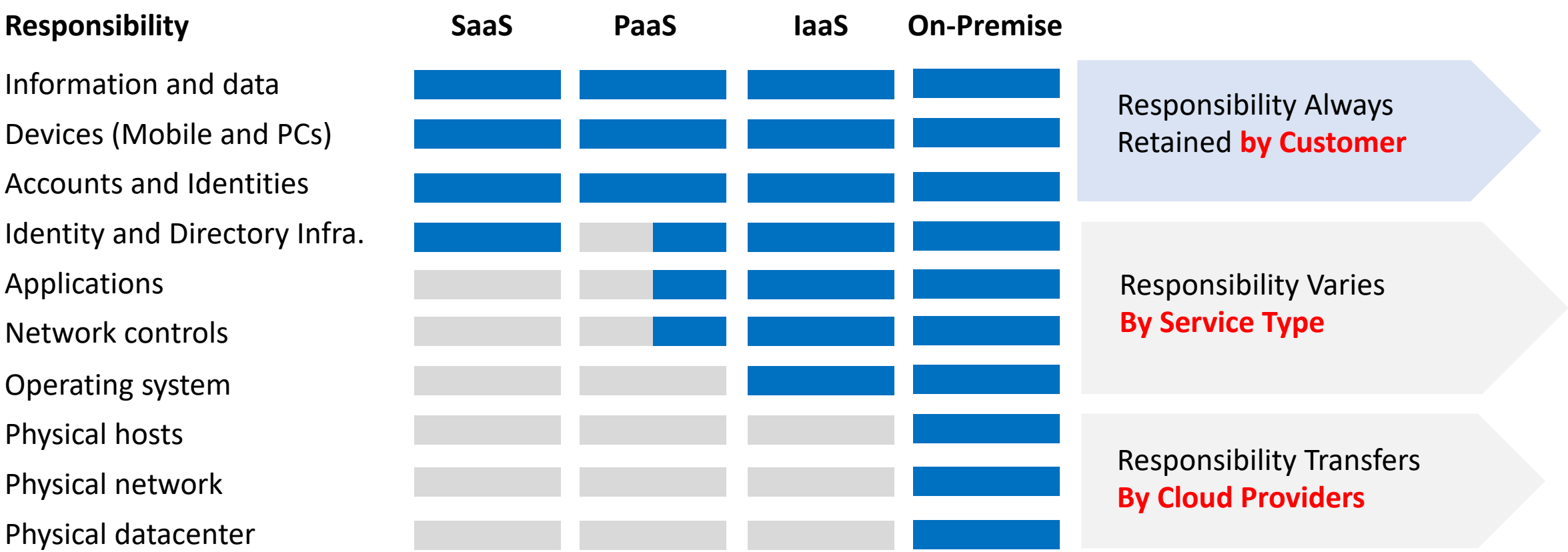
IAM	Infra. and Network	Data and Apps	Customer Access
Azure AD Identity Protection			
Azure Defender			
Microsoft 365 Defender Defender for Endpoints Defender for Identity	Azure Defender for IoT Azure Network Watcher	Securing Containers (Azure Defender) Azure Container Registry Azure Kubernetes Service	
	Azure Policy Audit Logging		
Azure Sentinel		Microsoft 365 Defender Microsoft Cloud App Security	

MSSM – Investigate and Respond



Shared Responsibility Model

Shared Responsibility Model describes what the Customer and Azure is responsible for related to cloud resources



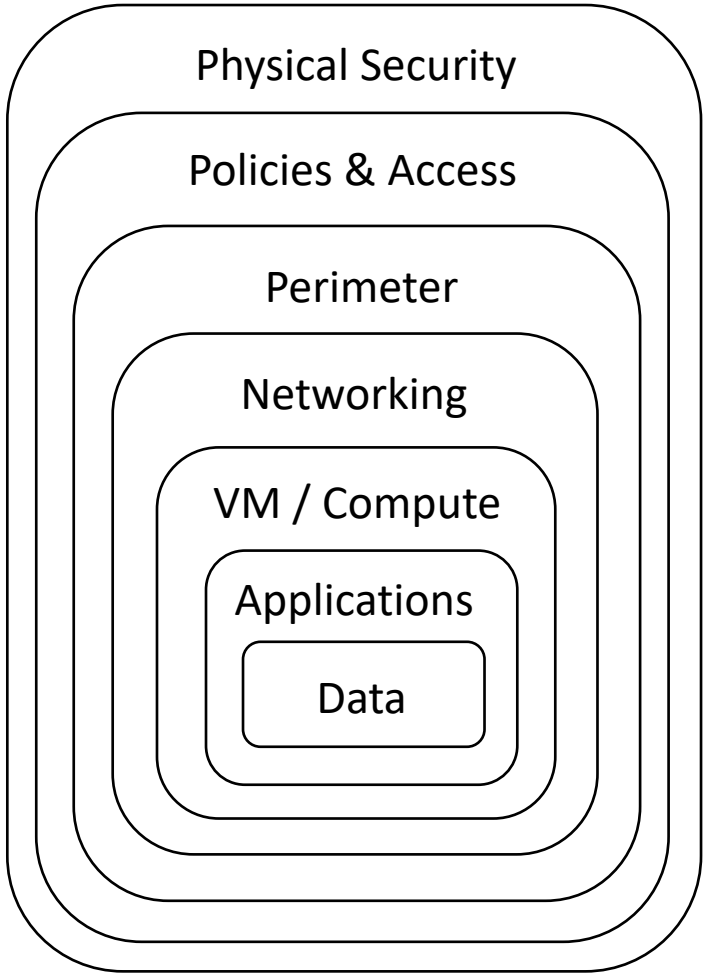
Software as a Service (SaaS) — software that use in the cloud eg. Microsoft 365, Skype, Dynamics CRM
Platform as a Service (PaaS) — deploy apps without worrying about underlying infrastructure. Azure App Services
Infrastructure as a Service (IaaS) — basic building blocks of cloud IT eg. Storage, Compute, Databases, Networking
On-Premise — datacenter owned, operated and maintained by customer

Shared Responsibility Model

Regardless of the type of deployment, the following responsibilities are always retained by you:

- **Data**
- **Endpoints**
- **Account**
- **Access management**

Defense in Depth



The 7 Layers of Security

1. Data
access to business and customer data, and encryption to protect data.

2. Application
applications are secure and free of security vulnerabilities.

3. Compute
Access to virtual machines (ports, on-premise, cloud)

4. Network
limit communication between resources using segmentation and access controls.

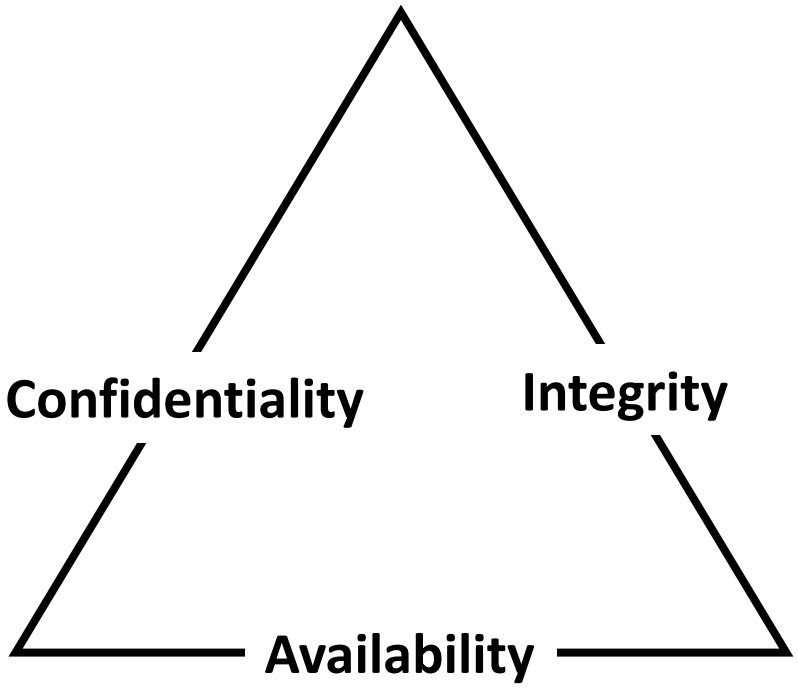
5. Perimeter
distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

6. Identity and access
controlling access to infrastructure and change control.

7. Physical
limiting access to a datacenter to only authorized personnel.

Confidentiality, Integrity, Availability (CIA)

Confidentiality, Integrity, and Availability (CIA) triad is a model describing the foundation to security principles and their trade-off relationship.



Confidentiality
confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. In practice this can be using cryptographic keys to encrypt our data, and using keys to encrypt our keys (envelope encryption)

Integrity
maintaining and assuring the accuracy and completeness of data over its entire lifecycle. In Practice utilizing ACID compliant databases for valid transactions. Utilizing tamper-evident or tamper proof Hardware security modules. (HSM)

Availability
information needs to be made be available when needed
In Practice: High Availability, Mitigating DDoS, Decryption access

The CIA triad was first mentioned in a **NIST publication from 1977.**
There have been efforts to expand and modernize or suggest alternatives to CIA triad:

- (1998) Six Atomic Elements of Information eg. confidentiality, possession, integrity, authenticity, availability, and utility
- (2004) NIST Engineering Principles for Information Technology Security — 33 security principles

Common Threats

What is a Threat?
A threat in cloud security is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application

Azure wants you to know the following **4 types** of threats

Dictionary Attack
Attacker attempts to steal an identity by brute forcing into a target accounts by enumerating over a large number of known passwords.

Disruptive attacks
An attack which attempts to disrupt a computer system or computer network for various reasons: DDoS, coin miners, rootkits, trojans, worms etc….

Ransomware
A type of malicious software (malware) that when installed holds data, workstation or a network hostage until the ransom has been paid.

Data Breach
When a malicious actor gains unauthorized access to a system in order to extract private data.

Vulnerabilities

What is a vulnerability?
a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

Allowing Domains or Accounts to Expire
Buffer Overflow
Business logic vulnerability
CRLF Injection
CSV Injection
Catch NullPointerException
Covert storage channel
Deserialization of untrusted data
Directory Restriction Error
Doubly freeing memory
Empty String Password
Expression Language Injection
Full Trust CLR Verification issue
Heartbleed Bug
Improper Data Validation
Improper pointer subtraction
Information exposure through query strings
Injection problem
Insecure Compiler Optimization
Insecure Randomness
Insecure Temporary File
Insecure Third Party Domain Access
Insecure Transport
Insufficient Entropy
Insufficient Session-ID Length
Least Privilege Violation
Memory leak
Missing Error Handling
Missing XML Validation
Multiple admin levels
Null Dereference
OWASP .NET Vulnerability Research
Overly Permissive Regular Expression
PHP File Inclusion
PHP Object Injection
PRNG Seed Error
Password Management Hardcoded Password
Password Plaintext Storage
Poor Logging Practice
Portability Flaw
Privacy Violation
Process Control
Return Inside Finally Block
Session Variable Overloading
String Termination Error
Unchecked Error Condition
Unchecked Return Value Missing Check against Null
Undefined Behavior
Unreleased Resource
Unrestricted File Upload
Unsafe JNI
Unsafe Mobile Code
Unsafe function call from a signal handler
Unsafe use of Reflection
Use of Obsolete Methods
Use of hard-coded password
Using a broken or risky cryptographic algorithm
Using freed memory
Vulnerability template
XML External Entity (XXE) Processing

Encryption

What is cryptography?
The practice and study of techniques for secure communication in the presence of third parties called adversaries

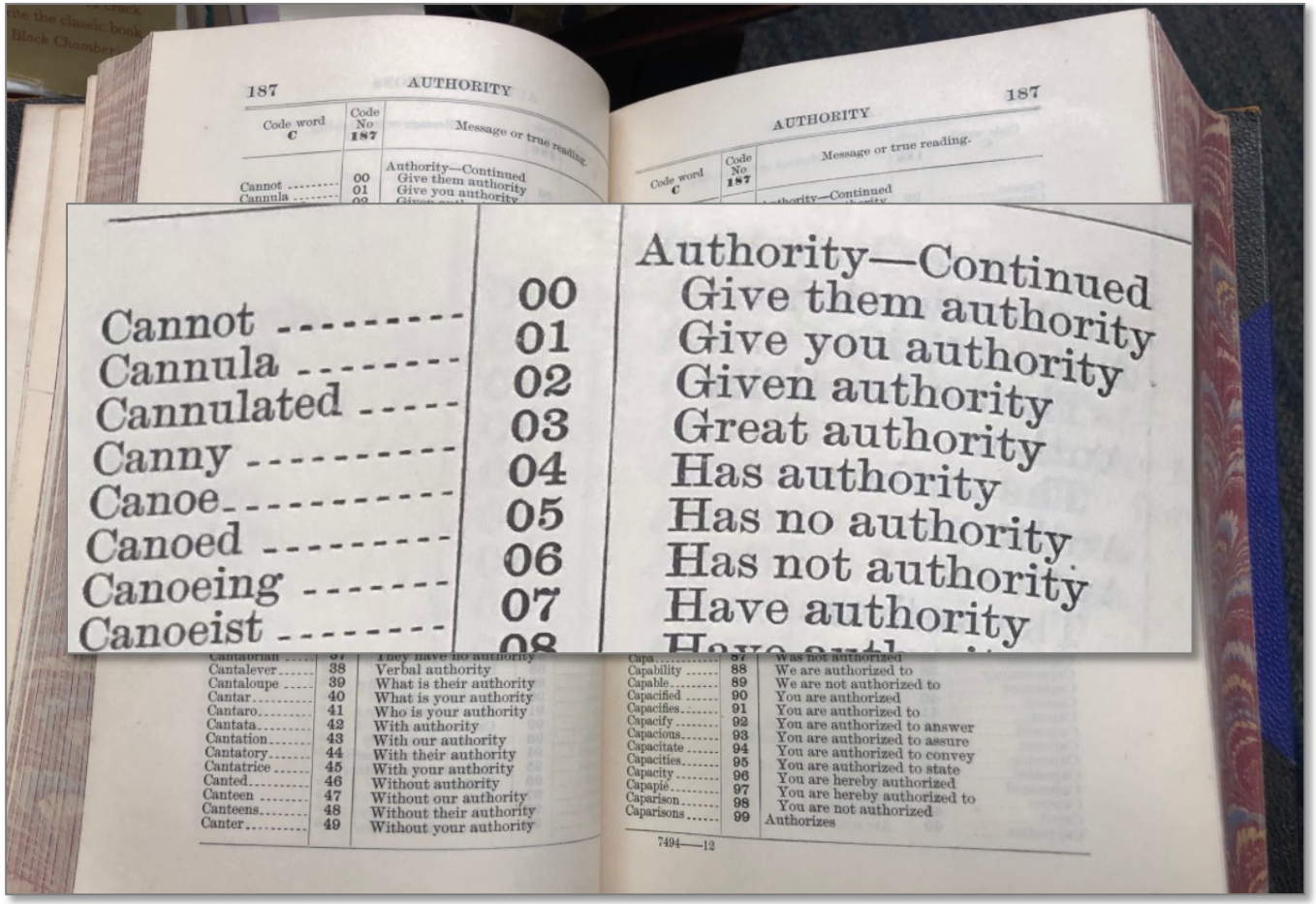
What is encryption?
The process of encoding (scrabbling) information **using** a **key** and a **cypher** to store sensitive data in an unintelligible format as a means of protection. An encryption takes in plaintext and produces **ciphertext**.

The **enigma machine** was used during WW2. A different key for each day was used to set the position of the rotors. It relied on simple cypher substitution.

Cyphers

What is a cypher?
An algorithm that performs encryption or decryption. Cipher is synonymous with “code”

What is ciphertext
Ciphertext is the result of encryption performed on plaintext via an algorithm

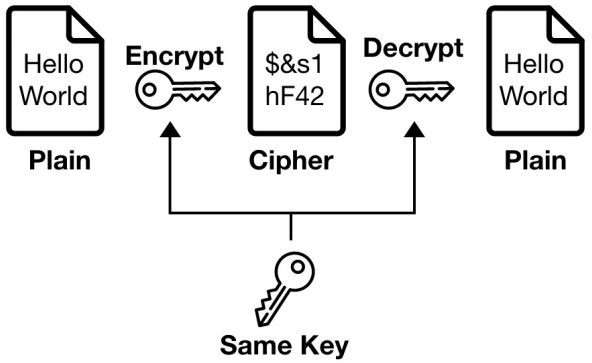


A **codebook** is a type of document used for gathering and storing cryptography codes

Cryptographic Keys

What is a cryptographic key?

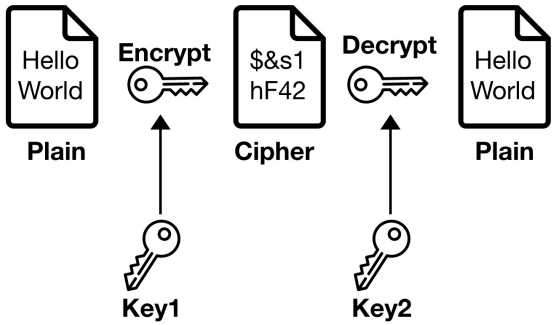
A key is a variable used in conjunction with an encryption algorithm in order to encrypt or decrypt data.



What is symmetric encryption?

The same key is used for encoding and decoding.

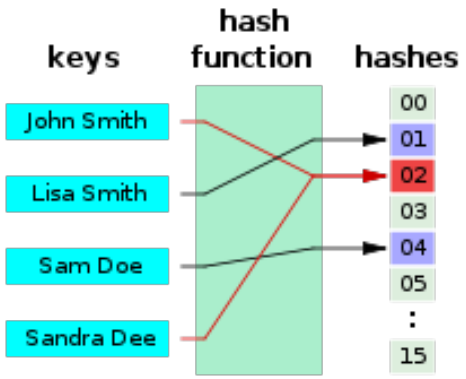
eg **Advanced Encryption Standard (AES)**



What is asymmetric encryption?

Two keys are used. One to encode and one to decode eg. **Rivest–Shamir–Adleman (RSA)**

Hashing and Salting



What is hashing function?
A function that accepts arbitrary size value and maps it to a fixed-size data structure. Hashing can reduce the size of the store value.

Hashing is a **one-way process** and is **deterministic**
A deterministic function always returns the same output for the same input.

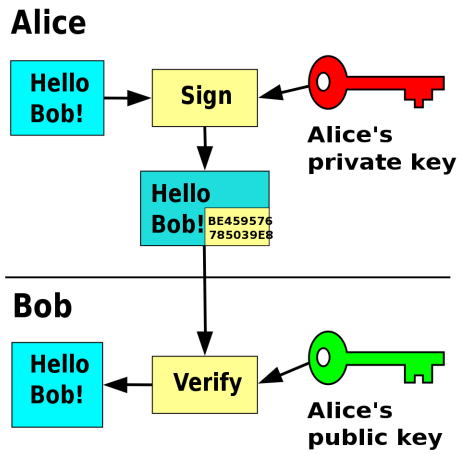
Hashing Passwords
Hashing functions are used to store passwords in database so that a password does not reside in a plaintext format.

To authenticate a user, when a user inputs their password, it is hashed, and the hash is compared to the store hashed. If they match then the user has successful logged in.

Popular hashing functions are **MD5, SHA356 and Bcrypt**
If an attacker knowns what function you are using and stole your database, they could enumerate a dictionary of password to determine the password.

Salting Passwords
A salt is a random string not known to the attacker that the hash function accepts to mitigate the deterministic nature of hashing functions

Digital Signatures and Signing



What is a digital signature
A mathematical scheme for verifying the authenticity of digital messages or documents.

A Digital signature gives us **tamper-evidence** .

- Did someone mess (modify) the data?
- Is this data is not from the expected sender?

There are three algorithms to digital signatures:

- **Key generation** – generates a public and private key.
- **Signing** - the process of generating a digital signature with a **private key** and inputted message
- **Signing verification –** verify the authenticity of the message with a **public key**

```
ssh-keygen -t rsa
```

SSH uses a public and private key to authorize remote access into a remote machine e.g. Virtual Machine. It is common to use RSA
ssh-keygen is a **well known command** to generate a public and private key

What is Code Signing?
When you use a digital signature to ensure **computer code** has not been tampered

In-Transit vs At-Rest Encryption

Encryption In-Transit
Data that is secure when moving between locations
Algorithms: **TLS, SSL**

Encryption At-Rest
Data that is secure when residing on storage or within a database
Algorithms: **AES, RSA**

Transport Layer Security (TLS)
An encryption protocol for data integrity between two or more communicating computer application. TLS is Deprecated in favour of SSL

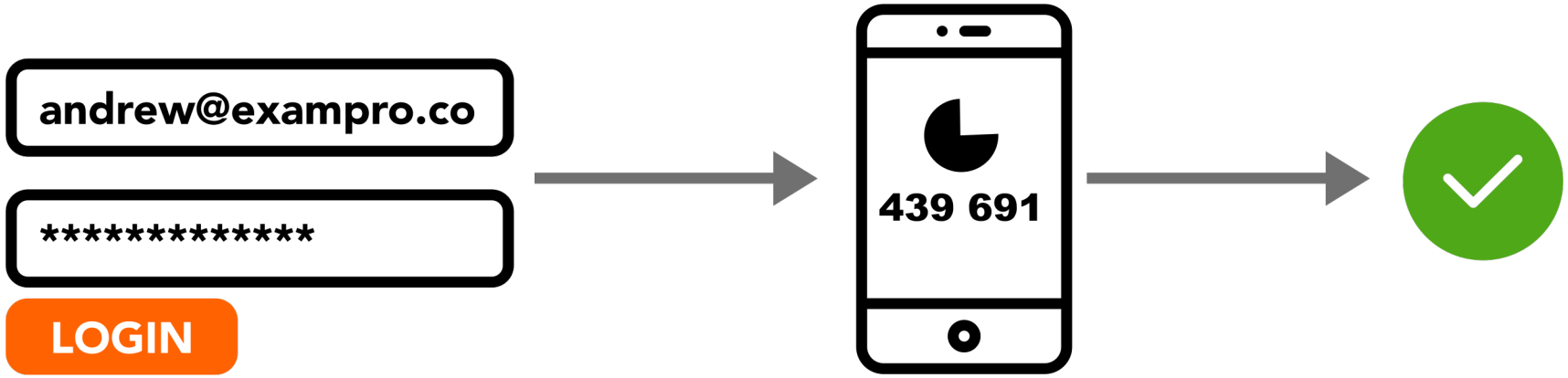
Secure Sockets Layers (SSL)
An encryption protocol for data integrity between two or more communicating computer application

Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?
A security control where after you fill in your username/email and password **you have to use a second device** such as a phone to confirm that its you logging in.

MFA **protects** against people who have stolen your password.

MFA is an option in most cloud providers and even social media websites such as Facebook.



Security information and event management (SIEM)

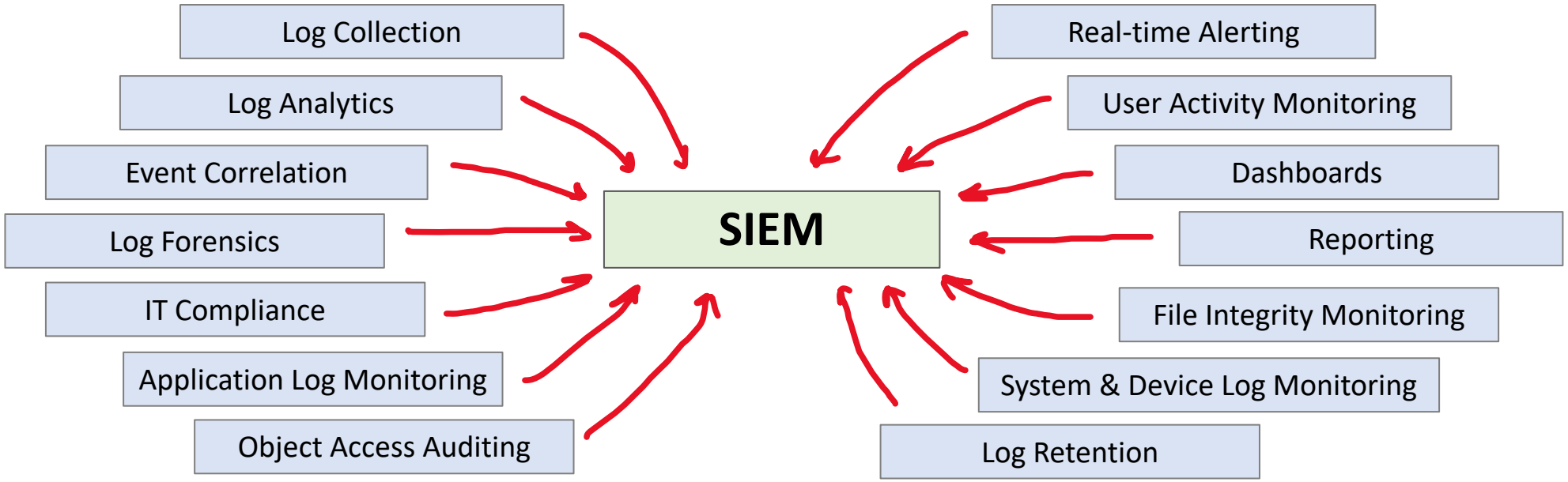
What is Log Management?
Focus on simple collection and storage of log messages and **audit trails**

What are event logs?
systems and applications generate events which are kept in **event logs**. Lists of activities that occurred, with records of new events being appended to the end of the logs as they occur.

What is Security information management (SIM)?
Long-term storage as well as analysis and reporting of log data.

What is security event management (SEM)?
Real-time monitoring, correlation of events, notifications and console views

What is Security information and event management (SIEM)?
Combines SIM and SEM to **provides real-time analysis of security alerts** generated by network hardware and applications



Security Orchestration Automated Response (SOAR)

A **Security Orchestration Automated Response (SOAR)** **collects data about security threats** and **respond to security events** without human assistance.

The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue

Security Orchestration
Connects various internal or external security tools via built-in or custom integrations.

Possible Connected sources:

- Vulnerability scanners
- Endpoint Protection
- End-User Behavior Analytics
- Firewalls
- Intrusion Detection/ Protection Systems (IDs/IPs)
- Security Information and Event Management (SIEM)
- Threat Intelligence Feeds

Security Automation
Analyzes the injected data to create **Playbooks** (repeatable, automated processes to replace manual processes) eg:

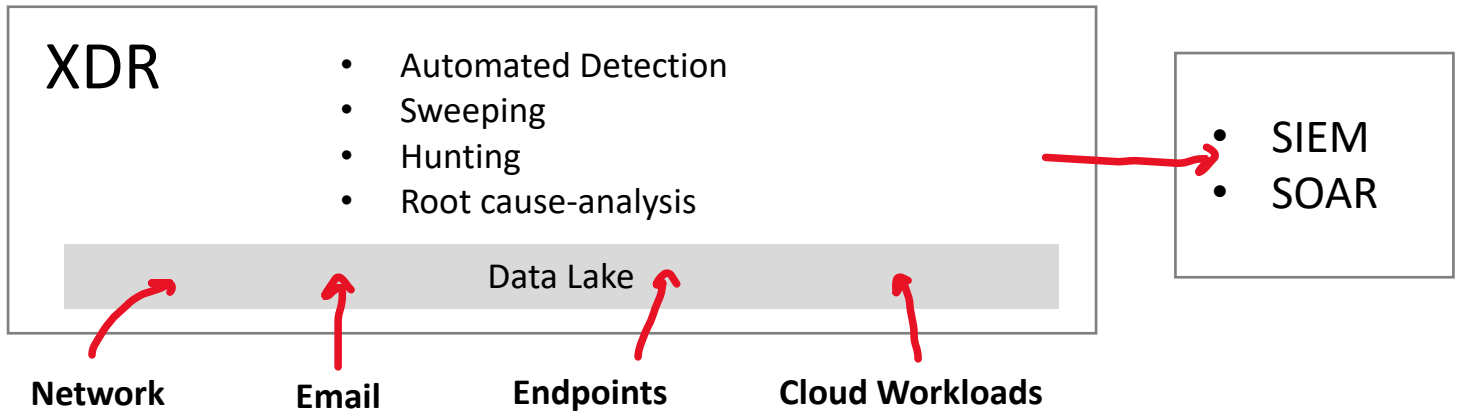
- Vulnerability scanning
- Log analysis
- Ticket checking
- Auditing

SOARS can **use AI and ML** to provide recommendations and further automate responses

Extended Detection and Response (XDR)

Extended detection and response (XDR) is cross-layered detection and response security system

XDR uses a **holistic approach** to detect and respond to threats that would normally evade detection in a single-vector solution **by collaborating multiple data sources into a multi-vector solution**.



Endpoint Detection and Response (EDR)

Endpoint detection and response (EDR) combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

EDPs are designed to detect APTs

What is an Advanced Persist Threat (APT)?

An Advanced Persistent Threat will breach a security perimeter and take up residence within a network to steal as much data as it can over a long period of time. APT are threat actors that engineer malware engineered for a particular target. APTs are slow **acting and stealthy**. Common targets for APTs are:

- Tier-one manufacturer
- Defense contractors
- Government agencies

EDR

Detection	Response	Investigation
• Behavior analysis • Advanced detection techniques • IoC scan	• Automated response on discovery • Quick response during the investigation • Multiple response options	• Root cause • Attack Visualizations • Enriched Alert data

Cloud access security brokers (CASB)

Cloud access security broker sits between cloud service users and cloud applications, and **monitors all activity and enforces security policies**

- Remote Workforce
- Corporate Office

CASB
- Control and Monitoring (Visibility)
- Compliance Management
- Data Security
- Threat Protection

Cloud Services
1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

Features of a CASB:
- monitoring user activity
- warning administrators about potentially hazardous actions
- enforcing security policy compliance
- automatically preventing malware.
- Restricts unauthorized access

- Identifies account takeovers
- Uncovers shadow cloud IT
- Cloud data loss prevention (DLP)
- Internal and external data access controls
- Records an audit trail of risky behavior
- Cloud phishing and malware threats
- Continuous monitoring for new cloud risks

Security Posture

Malicious Actors *aka Threat Actor, Attacker*
a person, machine or entity for an event or incident that impacts, or has the potential to impact, the safety or security of another entity

Inventory
up-to-date list of assets (software and hardware) for your organization can be accompanied with additional metadata
Perimeter assets — assets exposed to the internet (public-facing)
Core assets — assets within your private network (private-facing)

Attack Vectors
the method that a malicious actor uses to breach or infiltrate your network
They could target infrastructure or a human for weakness

Attack Surface
The sum of the attack vectors.
The larger the inventory generally increases the amount of attack vectors
The larger the attack surface the more difficult it is to mitigate attacks.

Security Controls
Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks

Security Posture
A formula to determine the overall effectiveness of a companies security overall defense

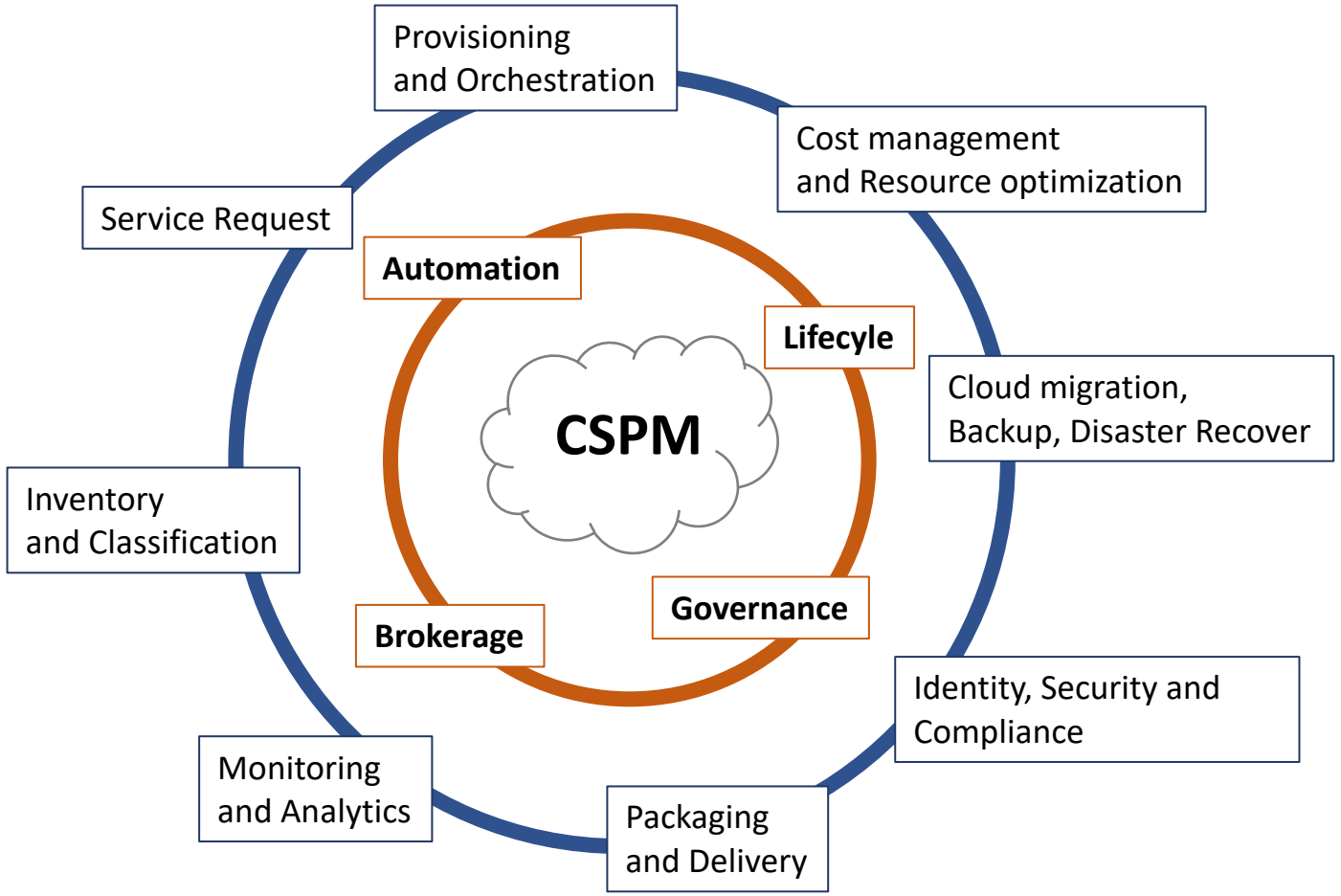
Security Posture

How to evaluate / Assess Security Posture:

1. Collect information by asking common questions
    - What data do we collect?
    - How and where are we storing this data?
    - How do we protect and document the data?
    - How long do we keep data?
    - Who has access internally and externally to the data?
    - Is the place we are storing the data properly secured?
2. Security ratings aka Security scores
    - data-driven, objective, and dynamic measurement of an organization's security posture
        - created by a trusted, independent security rating platform

Cloud Security Posture Management (CSPM)

CSPM identify and remediate risks through **security assessments and automated compliance** monitoring



Cloud Security Posture Management (CSPM)

A CSPM assesses your systems and **automatically alerts security staff** in your IT department when a vulnerability is found.

CSPM provides various security tools:

- Zero Trust-based access control
- Real-time risk scoring
- Threat and vulnerability management (TVM)
- Discover sharing risks
- Technical policy
- Threat modeling systems and architectures

Teams that would use a CSPM:

- Threat intelligence team
- Information technology
- Compliance and risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

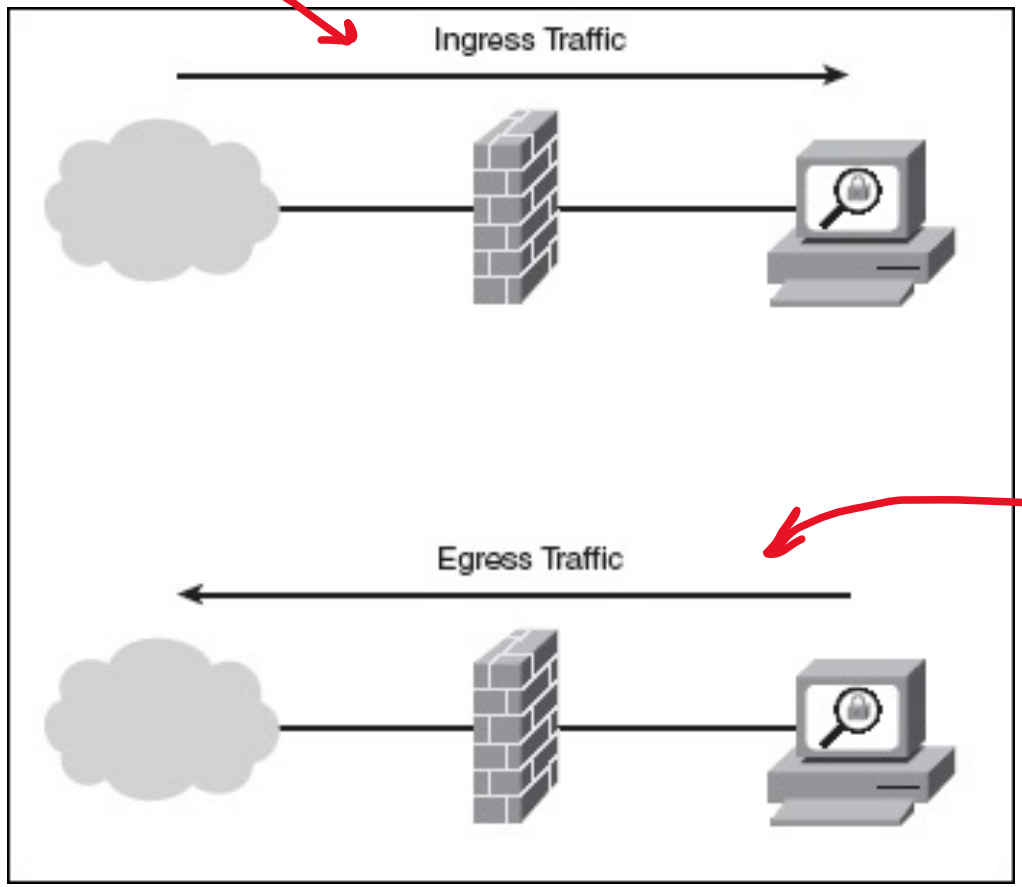
Just-in-Time/ Just Enough Privilege

Just-in-time (JIT)
giving access to resources only during the time when needed
reducing the surface attack based on range of time access

Just Enough Privilege (JeP)
giving access to only the specific actions (API calls)
reducing the surface attack by providing least-permissive permissions

Ingress vs Egress

Ingress traffic
traffic that is entering a network boundary



Egress traffic
traffic that is exiting a network boundary

Ingress: Latin ingressus "an advance; walking; an entry

Shadow IT

Shadow IT is a **business agility process** where **departments can purchase and provision their own IT resources** *without the approval* of the organization centralized IT department

The **advantage** of Shadow IT systems allows organizations to innovate and quickly prototype future solutions

The **disadvantage** of Shadow IT systems increase risks with organizational requirements for:

- security control
- compatibility with compliance programs
- loss of data, or unexpected data exposure
- documentation
- reliability

Automated Investigation and Remediation (AIR)

What is an investigation?
gathering evidence from digital systems to **uncover malicious intent** or reduction in a security posture

What is an remediation?
the action of remedying something **to prevent or revert a disaster**
the act of changing a resource back to the desired state or a state that does not causes problems
In the context of cloud security, a cloud resource is being remediated to stay compliant with our expected security controls
eg. preventing: Turn this VM off if port 22 is exposed
eg. reverting: Turn back on encryption if a disk encryption is disabled

What is Automated Investigation
a service which uses an inspection algorithms that **triggers an alert** which in turn creates an incident

What is Automated Remediation?
a service which **watches for types of incidents and matches it with a remediation action** eg. shut off server

What is Automated Investigation and Remediation (AIR)?
AIR is a unified service that does both Automated Investigation and Remediation

Threat Analysis

Threat analysis is the **practice of mitigating possible threats** via threat modeling

What is threat modelling?

A structured process for identifying attackers and cataloging possible threats

Threat modelling methodologies

Numerous threat modeling methodologies are available for implementation

STRIDE — developed by Microsoft in 1999

PASTA — Process for Attack Simulation and Threat Analysis, seven-step, risk-centric methodology

Trike — open source threat modeling process

MAL — Meta Attack Language, a domain-specific language used for used for threat modeling and attack simulations

STRIDE Methodology

STRIDE categorizes different threats as the following:

- **S**poofing — illegally accessing and then using another user's authentication information
- **T**ampering — malicious modification of data
- **R**epudiation — llegal operation in a system that lacks the ability to trace the prohibited operation
- **I**nformation Disclosure — exposure of information to individuals who are not supposed to have access to it
- **D**enial of Service — deny service to valid users
- **E**levation of Privilege — unprivileged user gains privileged access

Microsoft Security Development Lifecycle uses **STRIDE**
and provides a **tool to assist** with this process

Microsoft Threat Modeling Tool
makes threat modeling easier for all developers through a standard notation
for visualizing system components, data flows, and security boundaries

Intrusion Detection and Protection

What is an IDS?
Intrusion Detection System (IDS) **monitors** a network or system for malicious activity or policy violations

What is an IPS?
Intrusion Protection System (IPS) **restricts** access to a network or systems mitigate malicious activity or policy violations

What is IDS/IPS?
Intrusion Detection System and Intrusion Protection System (IDS/IPS) is the combination of an IDS and IPS.

How does an IDS detect incidents?

- **Signature-Based Detection** (simple technique)
  - A **signature** is a set of rules that an **IDS** and an **IPS** use to detect typical intrusive activity
  - compares signatures against observed events to identify possible incidents
- **Anomaly-Based Detection** (advanced technique)
  - compares definitions of what is considered normal activity with observed events in order to identify significant deviations
- **Stateful Protocol Analysis** (profile technique)
  - compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations

MITRE ATT&CK Framework

What is MITRE?
MITRE is a not-for-profit organization supporting various U.S. government agencies in the aviation, defense, healthcare, homeland security, and cybersecurity fields

What is MITRE ATT&CK?
globally-accessible **knowledge base of adversary tactics and techniques** based on real-world observations

https://attack.mitre.org

The ATT&CK knowledge base is used as a foundation for the **development of specific threat models and methodologies** in the private sector, in government, and in the cybersecurity product and service community

Microsoft Privacy Principles

Microsoft has 6 privacy principles

1. Control
We will put you in control of your privacy with easy-to-use tools and clear choices.

2. Transparency
We will be transparent about data collection and use so you can make informed decisions.

3. Security
We will protect the data you entrust to us through strong security and encryption.

4. Strong legal protections
We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

5. No content-based targeting
We will not use your email, chat, files or other personal content to target ads to you.

6. Benefits to you
When we do collect data, we will use it to benefit you and to make your experiences better.

Microsoft Privacy

Control your data

- Your data belongs to you
  - access, modify, or delete it at any time
- Your control of your data
  - reinforced by Microsoft compliance
    - GDPR, ISO 27018
- Independent audit reports
- Data processing only with consent
  - neither shared nor mined for market research and advertising
- Subcontractors data restrictions
  - aka subprocessors
  - can perform only the functions that Microsoft has hired them to provide, and they are bound by the same contractual privacy commitments that Microsoft makes to you

Control data location

You choose where your data is located

- Choices for datacenters
- Choices for data residency
  - data remaining within a country or geographic boundaries

Securing your data

- data-at-rest — AES-256 encryption
- Data-in-transit — SSL and TLS
- Encryption keys — Azure Key Vault

Defending your data

- Responding to data requests
  - will not disclose data to a government or law enforcement agency
    - unless required by law
- Law enforcement requests
  - direct the requesting party to seek the data directly from the customer
- Our contractual commitments
  - using the courts to challenge government demands that are inconsistent with the rule of law
- GDPR compliance
  - disclose their data in response to a government request in violation of the EU's GDPR

Primary Security Perimeter

What is a security perimeter?
barriers or built fortifications to either keep intruders out or to keep captives contained within the area the boundary surrounds.

A datacenter would have physical fence as its security perimeter
A cloud network would have a protocol, software and or hardware as its security perimeter

What is an Entrypoint?
The point of entry to cross a security perimeter

What are Access Controls (AC)?
The security mechanism at the point of access that that allows or denies access
Permission to access a resource is called **authorization**.

What is the Primary Security Perimeter?
Traditional security focused on firewalls and VPNs since there were few employees or workstations outside the office
Bring-your-own-device, remote workstations is much more common now access controls via Zero-trust model are being adopted eg. MFA and we see a shift towards **user identity management** becoming the primary perimeter for security

Azure Active Directory is the most common tool to protect against tool in an Azure or Microsoft workloads.

Identity Providers (IpD)

Identity Provider (IdP) a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to applications within a **federation** or distributed network.
A trusted provider of your user identity that lets you use authenticate to access other services.
Identity Providers could be: **Facebook, Amazon, Google, Twitter, Github, LinkedIn**

Federated identity is a method of linking a user's identity across multiple separate identity management systems

OpenID
open standard and decentralized authentication protocol. Eg be able to login into a different social media platform using a Google or Facebook account
OpenID is about providing who are you

OAuth2.0
industry-standard protocol for authorization OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers.
Oauth is about granting access to functionality

SAML
Security Assertion Markup Language is an open standard for exchanging authentication and authorization between an identity provider and a service provider.
An important use case for SAML is Single-Sign-On via web browser.

Introduction to Azure AD

Azure Active Directory (Azure AD) is Microsoft's cloud-based **identity and access management service**, which helps your employees sign in and access resources

External Resources

- Microsoft Office 365
- Azure Portal
- SaaS applications

Internal Resources

- Applications within your internal networking
- Access to workstations on-premise

Use Azure AD to implement **Single-Sign On (SSO)**

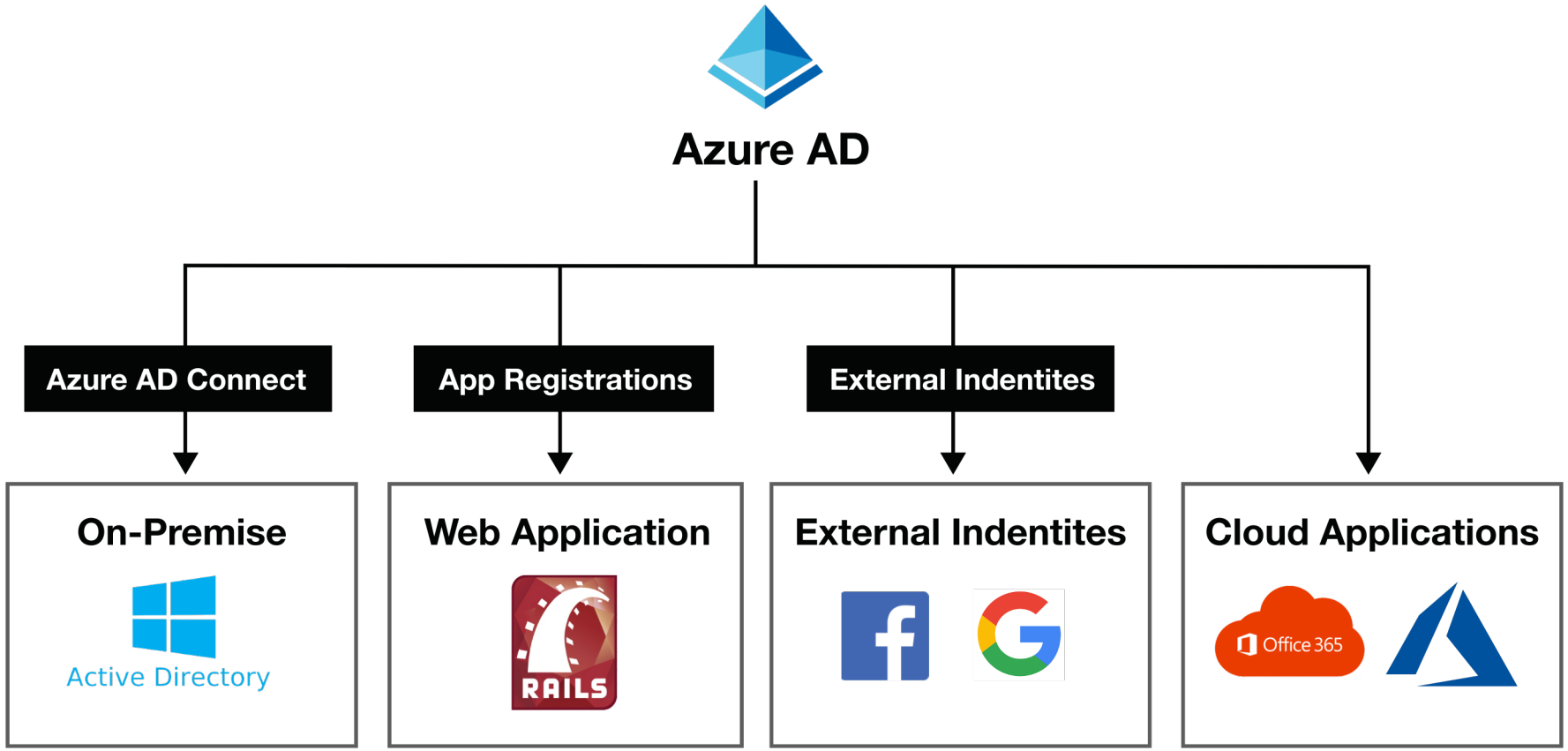
Azure Active Directory comes in four editions

1. **Free** MFA, SSO, Basic Security and Usage Reports, User Management
2. **Office 365 Apps** Company Branding, SLA, Two-Sync between On-Premise and Cloud
3. **Premium 1** Hybrid Architecture, Advanced Group Access, Conditional Access
4. **Premium 2** Identity Protection, Identity Governance

Azure AD – Use Case

Azure AD can **authorize** and **authenticate** to multiple sources.

- To your on-premise AD
- To your web-application
- Allow users to login with their IpD eg. Facebook or Google
- To Microsoft 365 or **Microsoft Azure**



Active Directory vs Azure Active Directory

Microsoft introduced **Active Directory** Domain Services in **Windows 2000** to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

Azure AD takes this approach to the next level by providing organizations with an **Identity as a Service (IDaaS)** solution for all their apps **across cloud and on-premises**.

Both versions are still used today

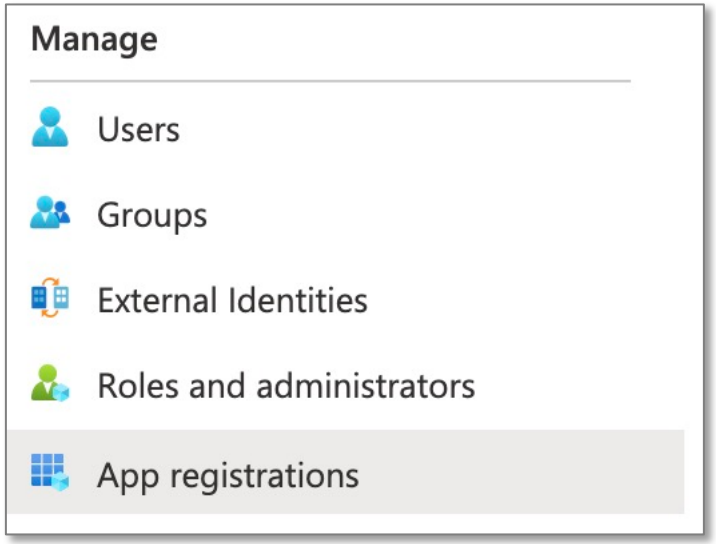
Active Directory
The **on-premise** version

Azure AD
The **cloud** version

Azure AD – App Registrations

App Registrations allows developers to integrate web-applications to use Azure AD authenticate users and request access to user resources such as email, calendar, and documents

This allows you to implement **Single Sign-On** into your web-applications



Azure AD – External Identities

External Identities in Azure AD, allow people outside your organization to access your apps and resources, while letting them sign in using whatever identity they prefer.

Your partners, distributors, suppliers, vendors, and other guest users can **"bring their own identities"**.

Supports Logins from **Google** and **Facebook**

- Share apps with external users (B2B collaboration).
- Develop apps intended for other Azure AD tenants (single-tenant or multi-tenant)
- Develop white-labeled apps for consumers and customers (Azure AD B2C)

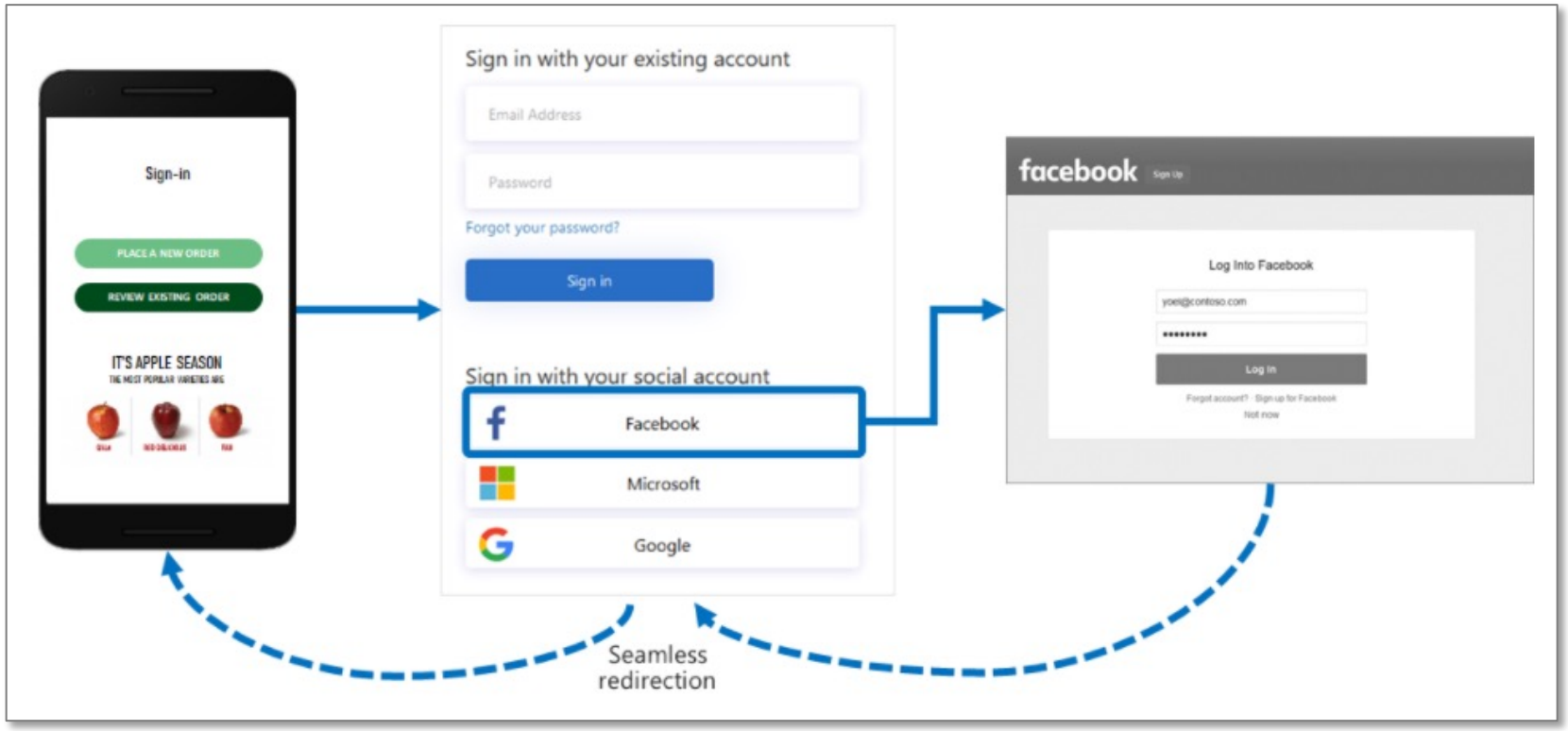
There are two types of External Identities for Azure AD

- **B2B** allows external businesses to authenticate with your app
- **B2C** allows customers to authenticate with your app
  - customer identity access management (CIAM) solution.

Azure AD BC2 Identity Providers

Azure AD BC2 IpD Support

- AD FS
- Amazon
- Apple
- Azure AD (Single-tenant)
- Azure AD (Multi-tenant)
- Azure AD B2C
- eBay
- Facebook
- Generic identity provider
- GitHub
- ID.me
- Google
- LinkedIn
- Microsoft Account
- QQ
- Salesforce
- Salesforce (SAML protocol)
- Twitter
- WeChat
- Weibo



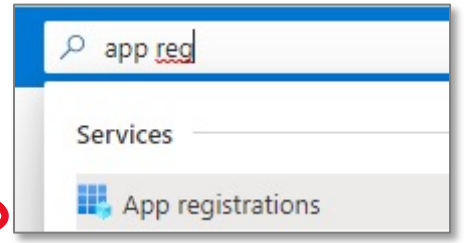
External Identities B2B vs B2C

	B2B	B2C
Scenario	Collaboration using Microsoft applications	IAM for modern SaaS or custom-developed applications
Intended	Collaborating with business partners from external organizations	Customers of your product
IpD Suport	work accounts, school accounts, any email address, SAML and WS-Fed based identity providers, Gmail, and Facebook	local application, social identities, and users with corporate and gov-issued identities via SAML/WS-Fed based IpD federation.
External User Management	managed in the same directory as employees	managed separately from the organization's employee and partner directory
SSO	SSO to all Azure AD-connected apps is supported.	SSO to customer owned apps within the Azure AD B2C tenants is supported
Policy and Compliance	Managed by the host/inviting organization	Managed by the organization via Conditional Access and Identity Protection
Branding	Host/inviting organization's brand is used	Fully customizable branding per application or organization.
Billing model	Based on monthly active users **(MAU)**	

Azure AD – Service Principle

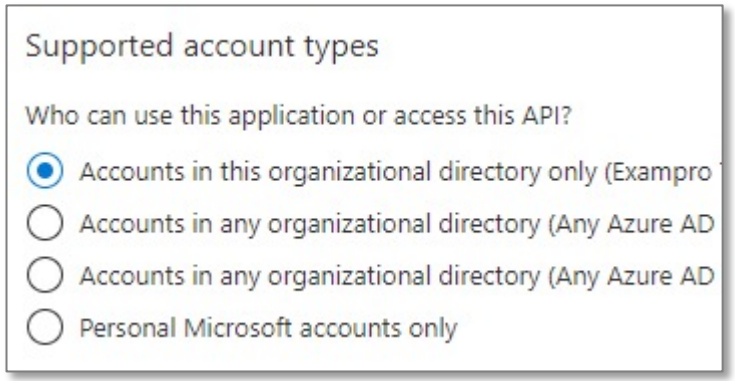
A service principal is a **security identity** used by applications or services to **access specific Azure resource**

A service principal is created when a user from that tenant has consented to the application's or API's use.

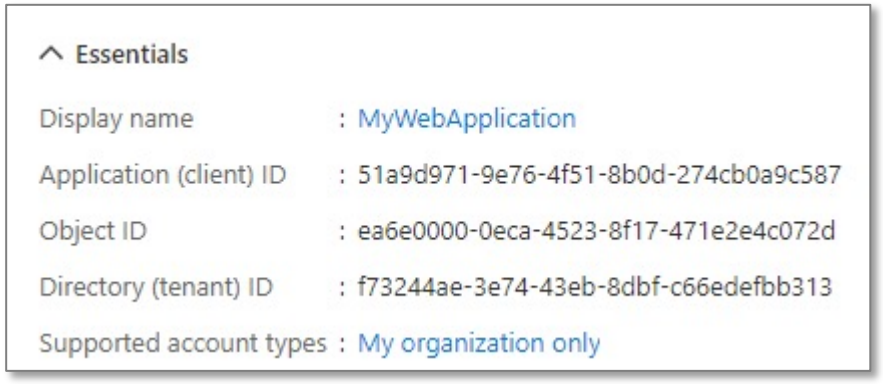


Service principals define:

- who **can access the application**
- what resources the application can access



A service principal is created in each tenant where the application is used and references the **globally unique application object**



The **ApplicationID** represents the global application across all tenants
The **ObjectID** is a unique value for an application object

Azure AD – Managed Identity

Managed identities are used to manage the credentials for authenticating a cloud application with an Azure service

Using a managed identity, you can **authenticate to any service** that supports Azure AD authentication **without having credentials in your code**.

There are two types of managed Identities

System-assigned
An identity in Azure AD tied to the lifecycle of a service instance
When the resource is deleted so is the system-assigned managed identity

Used-Assigned
An identity assigned to one or more instances of services. The identity is managed separately from the resource. When a resource is deleted the identity remains

Managed Identity System vs User Assigned

	System-assigned	User-assigned
Creation	Created as part of an Azure resource	Created as a standalone Azure resource
Lifecycle	Shared lifecycle with the Azure resource.	Independent life cycle.
Deletion	When resource deletes so does the identity	Must be explicitly deleted
Sharing across Azure resources	Cannot be shared. Associated with a single Azure resource.	Can be shared Can be associated with more than one Azure resource.

Azure AD – Device Management

What is Device identity management?
The management of **physical devices** such as **phones, tablets, laptops and desktop** computers, that are granted access to company resources such as Printers, Cloud Resources via **device-based Conditional Access**.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Complia...	Registered	Activity
DESKTOP-J1KCQ...	Yes	Windows	10.0.18362.0	Azure AD registered	Miles O'Brien	None	N/A	2020-07-12, 10:05:4...	2021-03-22, 9:
DESKTOP-00B6Q...	Yes	Windows	10.0.19042.867	Azure AD registered	Sonya Gomez	None	N/A	2020-08-24, 4:43:28 ...	2021-03-13, 7:
LAPTOP-HIELPOBE	No	Windows	10.0.19041.388	Azure AD registered	Reginald Barclay	None	N/A	2020-08-07, 2:57:31 ...	2020-09-19, 7:
DESKTOP-P9TM...	Yes	Windows	10.0.19041.867	Azure AD registered	Alyssa Ogawa	None	N/A	2021-03-31, 8:00:10 ...	2021-03-31, 8:

For companies with a distributed workforce, that allows remote employees and employees who Are allowed you use their own personal equipment eg. **Bring Your Own Device (BYOD).**

A company needs a way to protect their organization's assets such as access to cloud resources across these devices where they have less control over the physical securities of the work environment

Azure AD – Device Management

There are **3 ways** to get devices into Azure AD

1. Azure AD Registered

- **personally** owned or mobile devices,
- And signed in with a **personal** Microsoft or local account

- Windows 10
- iOS
- Android
- MacOS

2. Azure AD Joined

- owned by an **organization**
- And signed in with an Azure AD account belonging to the organization.
- They exist **only in the cloud**.

- Windows 10
- Windows Server 2019 VMs running in Azure (Server core is not supported)

3. Hybrid Azure AD Joined

- owned by an **organization**
- And are signed in with an Active Directory Domain Services account belonging to that organization
- They exist **in the cloud and on-premises**

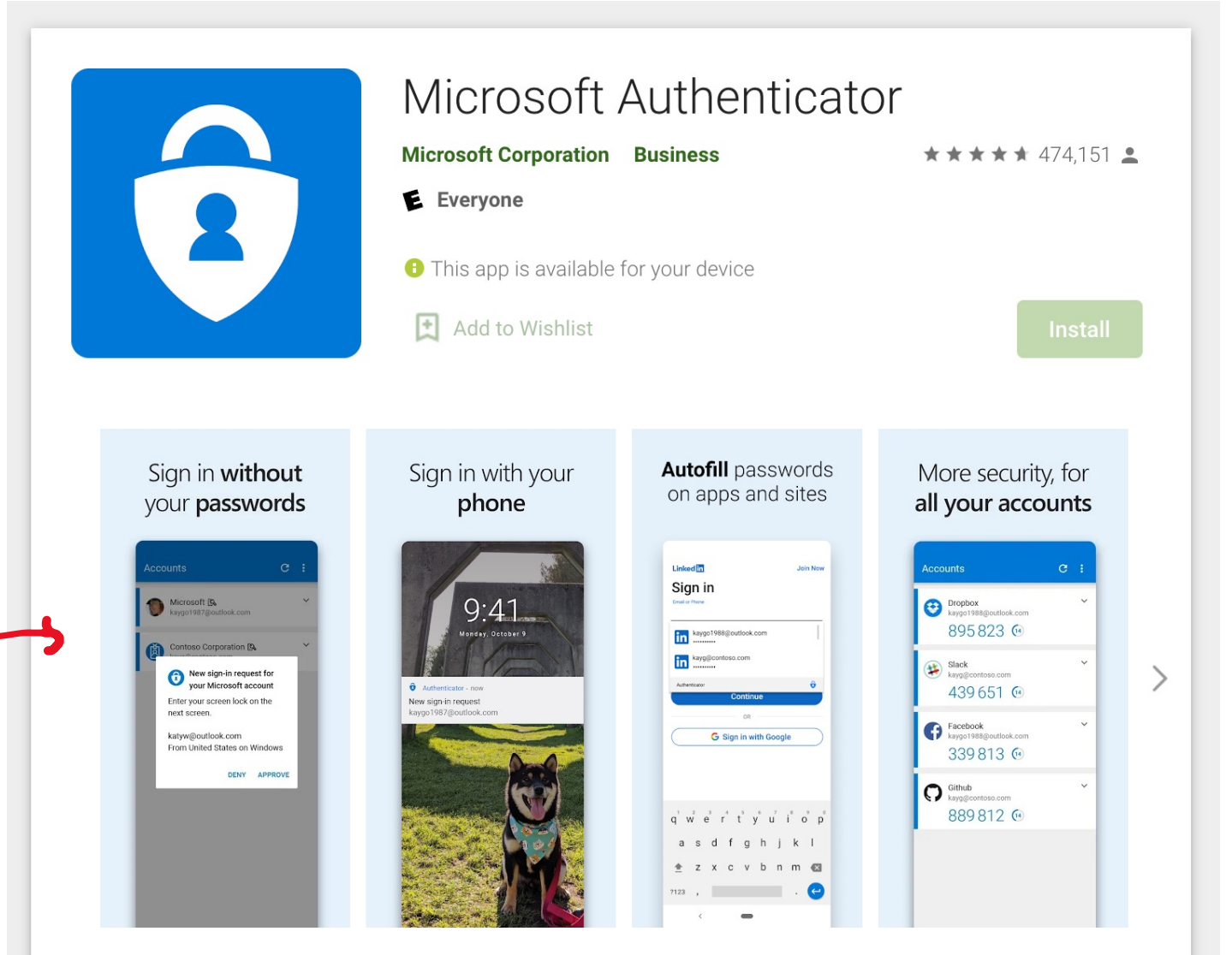
- Windows 7, 8.1, or 10
- Windows Server 2008 or newer

Microsoft Authenticator

secure sign-ins for all your online accounts using:

- multi-factor authentication
- Passwordless
- password autofill

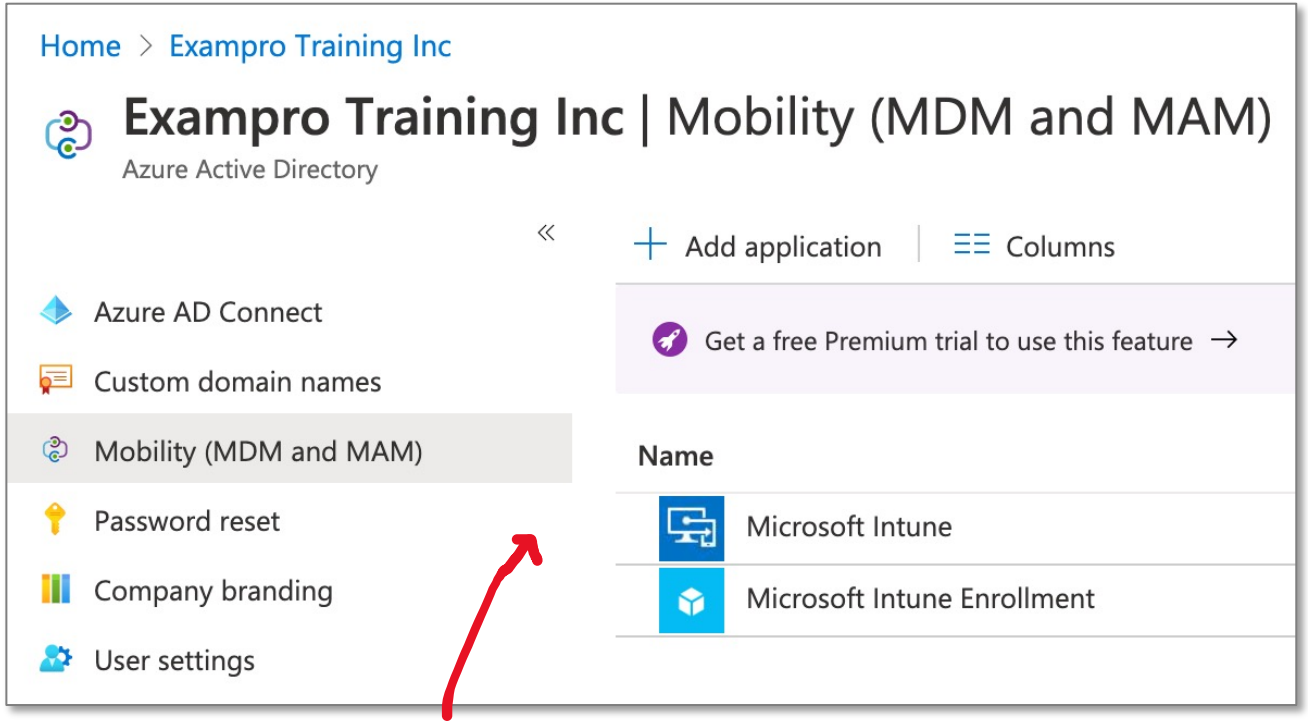
You can download from the **Apple App Store** or **Google Play**



MDM and MAM

Mobile Device Management (MDM)
control the entire device, can wipe data from it, and also reset it to factory settings

Mobile Application Management (MAM)
Publish, push, configure, secure, monitor, and update mobile apps for your users



MDM and MAM is found in Azure AD

MDM and MAM is managed via **Microsoft Intune**
To use Microsoft Intune you have to upgrade to **Azure AD Premium 2**
Microsoft Intune is part of **Microsoft Endpoint Manager**
Microsoft Endpoint Manager and Intune are part of **Microsoft Enterprise Mobility + Security (EMS)**
Intune = Endpoint Manager = EMS *Yes, I am confused too by all these names…*

Microsoft Intune

Windows Hello

Windows Hello
Gives Windows 10 users **an alternative way** to log into their devices and applications using:

- fingerprint
- iris scan
- facial recognition

Authenticate types with Windows Hello:

- A Microsoft account.
- Active Directory account.
- Azure AD account
- IpD Services
- Relying Party Services that support FIDO2.0

Windows Hello PIN is backed by a Trusted Platform Module (TPM) chip

- multiple physical security mechanisms to make it tamper resistant

Windows Hello PIN is more secure than a standard PIN because it is tied to a specific device.

- The PIN is for that device and only that device

Windows Hello vs Windows Hello for Business

Windows Hello

individuals/consumer devices

Uses a PIN backed by hashing

Windows Hello for Business

Business owned devices

can be configured by Group Policies (GPO) or MDM

uses a PIN backed by asymmetric (public/private key) or certificate-based authentication

Azure AD Connect

Azure AD Connect is a **hybrid service** to **connect your on-premise Active Directory to your Azure Account**

Azure AD Connect allows for seamless **Single Sign On** from your on-premise workstation to Microsoft Azure

Azure AD Connect has the following features:

- **Password hash synchronization** — sign-in method, synchronizes a hash of a users on-premises AD password with Azure AD
- **Pass-through authentication** — sign-in method, allows users to use the same password on-premises and in the cloud
- **Federation integration** — hybrid environment using an on-premises AD FS infrastructure, for certificate renewal
- **Synchronization** — Responsible for creating users, groups, and other objects, ensures on-prem and cloud data matches
- **Health Monitoring** — robust monitoring and provide a central location in the Azure portal to view this activity

Azure AD Connect Health

Self-Service Password Reset (SSPR)

Self-service password reset (SSPR) allows users to **change or reset their password, without the help from an administrator**,

Free up your help desk support requests, add an additional layer of security, keep users more productive

Self-service password scenarios:

- **Password change**
  - when a user knows their password but wants to change it to something new.
- **Password reset**
  - when a user can't sign in, such as when they forget the password, and want to reset it.
- **Account unlock**
  - when a user can't sign in because their account is locked out.

Authentication methods for SSRP:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Azure AD Password Protection

What is Password Spraying?
A type of brute force dictionary attack. Identity systems mitigate traditional brute force attacks by having lockout after an amount of attempts and lockout ends after short waiting period. Password Spraying circumvents lockout by spraying the same password across multiple accounts before trying another password while lockout time cools down.

Azure AD Password Protection is a feature of Azure AD to protect your passwords from identity attacks such as **password spray attacks**.

Global banned password list
password list with known weak passwords is automatically updated and enforced by Microsoft.

Custom banned password lists
Admins can also create custom banned password lists to support specific business security needs.

Banned password lists are a feature of **Azure AD Premium 1 or 2.**

Hybrid security
Azure AD Password Protection can be integrated to on-premise Active Directory environments

Azure identity management best practices

Azure identity management and access control security best practices

- Treat identity as the primary security perimeter
- Centralize identity management
- Manage connected tenants
- Enable single sign-on
- Turn on Conditional Access
- Plan for routine security improvements
- 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
- Use Azure AD for storage authentication

Emergency Access and Break Glass

Emergency access **accounts prevent admins from being accidentally locked** out of Azure AD

You can mitigate the impact of accidental lack of administrative access by creating **two or more** emergency access accounts in your organization

Emergency access accounts are

- highly privileged, and they are not assigned to specific individuals
- are limited to emergency or **"break glass"' scenarios** where normal administrative accounts can't be used.

recommend to maintain a goal of restricting emergency account use to only the times when it is absolutely necessary

These accounts should be:

- cloud-only accounts that use the *.onmicrosoft.com domain
- not federated or synchronized from an on-premises environment.

Exclude at least one account from phone-based multi-factor authentication

Exclude at least one account from Conditional Access policies

Store account credentials safely

Monitor sign-in and audit logs

Authentication Methods

Azure Active Directory multi-factor authentication methods

SMS
A text message is sent to your phone with a PIN

Voice call
A phone call from a synthesized voice speaks a PIN

Microsoft Authenticator app
You press a button in the app and it authorizes you

OATH Hardware token
You touch your security key and it authorize you by generating and entering a PIN

Biometrics

Biometrics are body measurements and calculations related to human characteristics

Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control.

Physiological characteristics

- **Fingerprint**
- Palm veins
- Face recognition
- DNA
- Palm print
- Hand geometry
- **Iris recognition**
- Retina
- Odor/scent

Behavioral characteristics

- typing rhythm
- Gait
- Keystroke
- Signature
- behavioral profiling
- voice

FIDO2.0

Fast Identity Online (FIDO) Alliance
An open industry association whose mission is to **develop and promote authentication standards** that **help reduce the world's over-reliance on passwords**

FIDO Alliance has published three sets of **open specifications** for simpler, stronger user authentication:

- FIDO Universal Second Factor (FIDO U2F)
- FIDO Universal Authentication Framework (FIDO UAF)
- Client to Authenticator Protocols (CTAP)
- CTAP is complementary to the W3C's Web Authentication (WebAuthn) specification; together, they are known as **FIDO2**

Security Keys

What is a Security Key?
A secondary device used as second step in authentication process to gain access to a device, workstation or application.

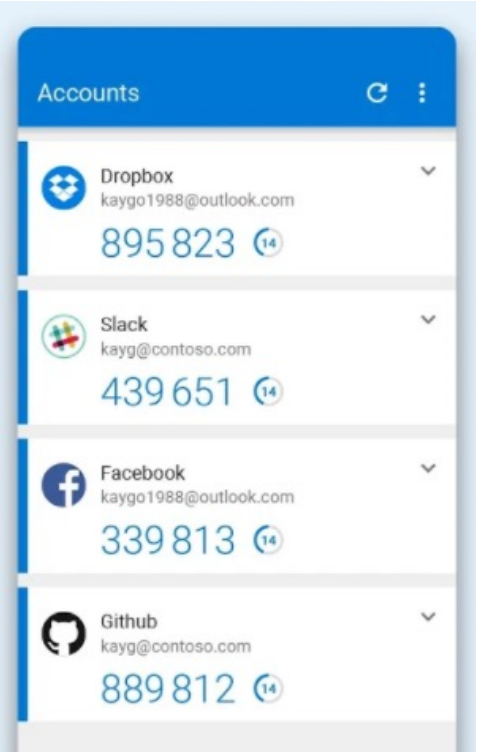
A popular brand of security key is an Yubikey

A security key can resemble a memory stick.
When your finger makes contact with a button
er exposed metal on the device it will generate
And autofill a security token.

- Works out of the box with Gmail, Facebook, and hundreds more
- Supports **FIDO2**/WebAuthn, U2F
- Waterproof and crush resistant
- USB-A and NFC dual connectors on a single key

Open Authentication

Open Authentication (OATH*) not to be confused with Oauth* is an open standard that specifies how time-based, one-time password (TOTP) codes are generated



Time-based One-time Password (TOTP) is a computer algorithm that generates a one-time password (OTP) which uses the current time as a source of uniqueness

OATH TOTP is implemented using either software or hardware to generate the codes

Software OATH would be generated from Authenticator apps e.g. Microsoft Authenticator
Hardware OATH would be generated from a security key e.g. Yubikey

Passwordless Authentication

Passwordless authentication is **a less frustrating authentication method** than MFA

Passwordless authentication methods are more convenient because the password is removed and replaced with:

- **something you have** + **something you are** or **something you know**

Something you have:

- Windows 10 Device, Phone, Security Key

Something you are:

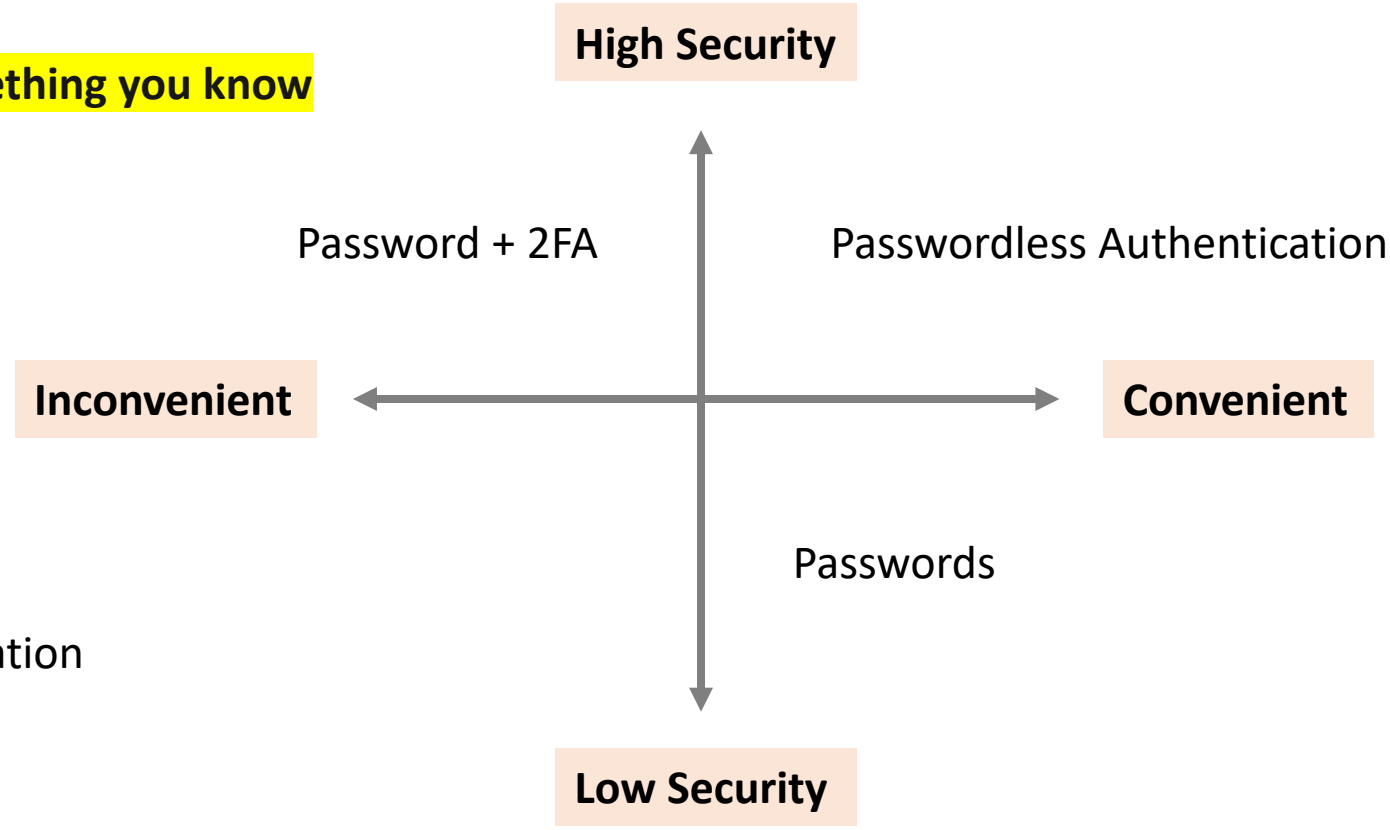
- Biometric, Fingerprint

Something you know:

- PIN

Solutions for Passwordless Authentication include:

- Windows Hello for business
- Microsoft Authenticator App
- FIDO2 Security Keys



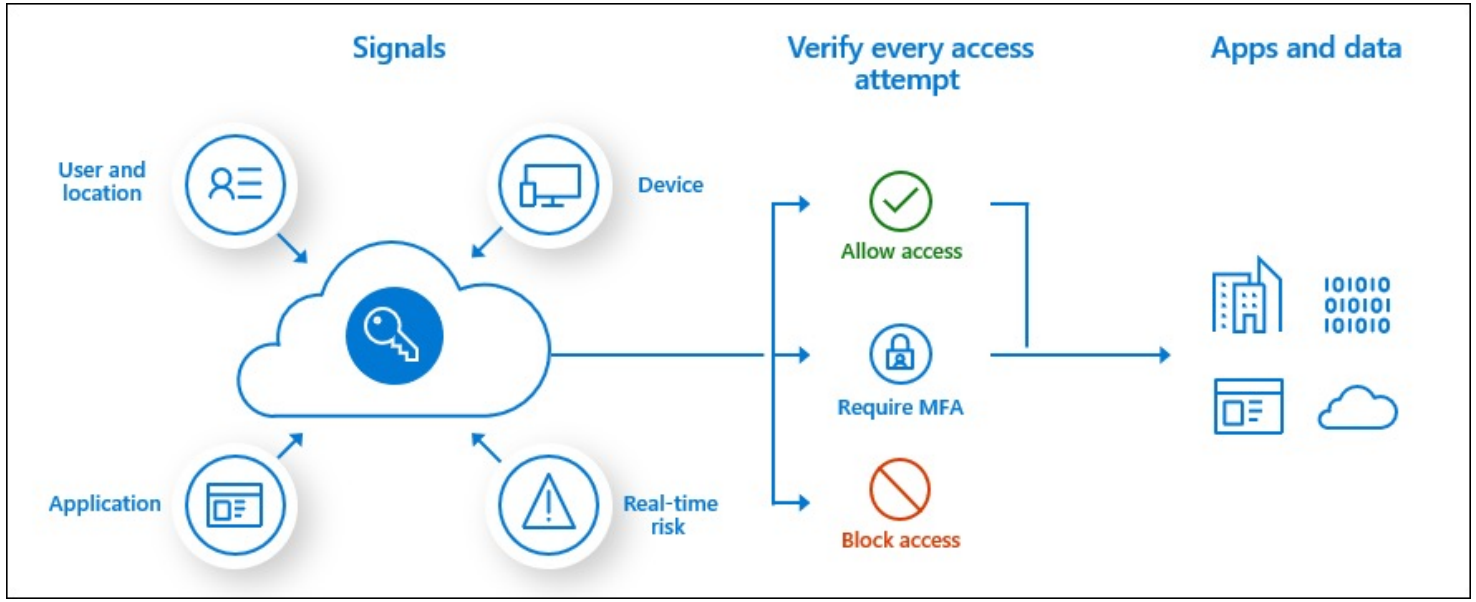
Azure AD Conditional Access

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

Conditional Access is implemented through **Conditional Access policies**

Conditional Access policy analyses:

- **Signals**
  - user, location, device, application, real-time- risk
- and Verifies every access attempt via **Access Controls**
  - Require MFA, Block, Allow



Conditional Access – Signals

Signals is metadata associated with an identity attempting to gain access

User or group membership.
Policies target specific users and groups (including admin roles), giving admins fine-grained control over access
Named location information / IP Location Information
IP address ranges, used when making policy decisions.
Admins can opt to block or allow traffic from an entire country's IP range.
Device
Users with devices of specific platforms or marked with a specific state can be used
Application
Users attempting to access specific applications can trigger different Conditional Access policies.
Real-time sign-in risk detection.
Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multifactor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
Cloud apps or actions.
Cloud apps or actions can include or exclude cloud applications or user actions that will be subject to the policy.
User risk
For customers with access to Identity Protection, user risk can be evaluated as part of a Conditional Access policy. User risk represents the probability that a given identity or account is compromised. User risk can be configured for high, medium, or low probability.

Conditional Access – Common Decisions

Common decisions define the access controls that **that decide what level of access** based on Signal information

Block access

- Most restrictive decision

Grant access

- Least restrictive decision, still require one or more of the following options:
  - Require multi-factor authentication
  - Require device to be marked as compliant
  - Require Hybrid Azure AD joined device
  - Require approved client app
  - Require app protection policy (preview)

Azure Role-Based Access Control (RBAC)

A Security Principal represents the identities requesting access to an Azure resource such as:

User An individual who has a profile in Azure Active Directory

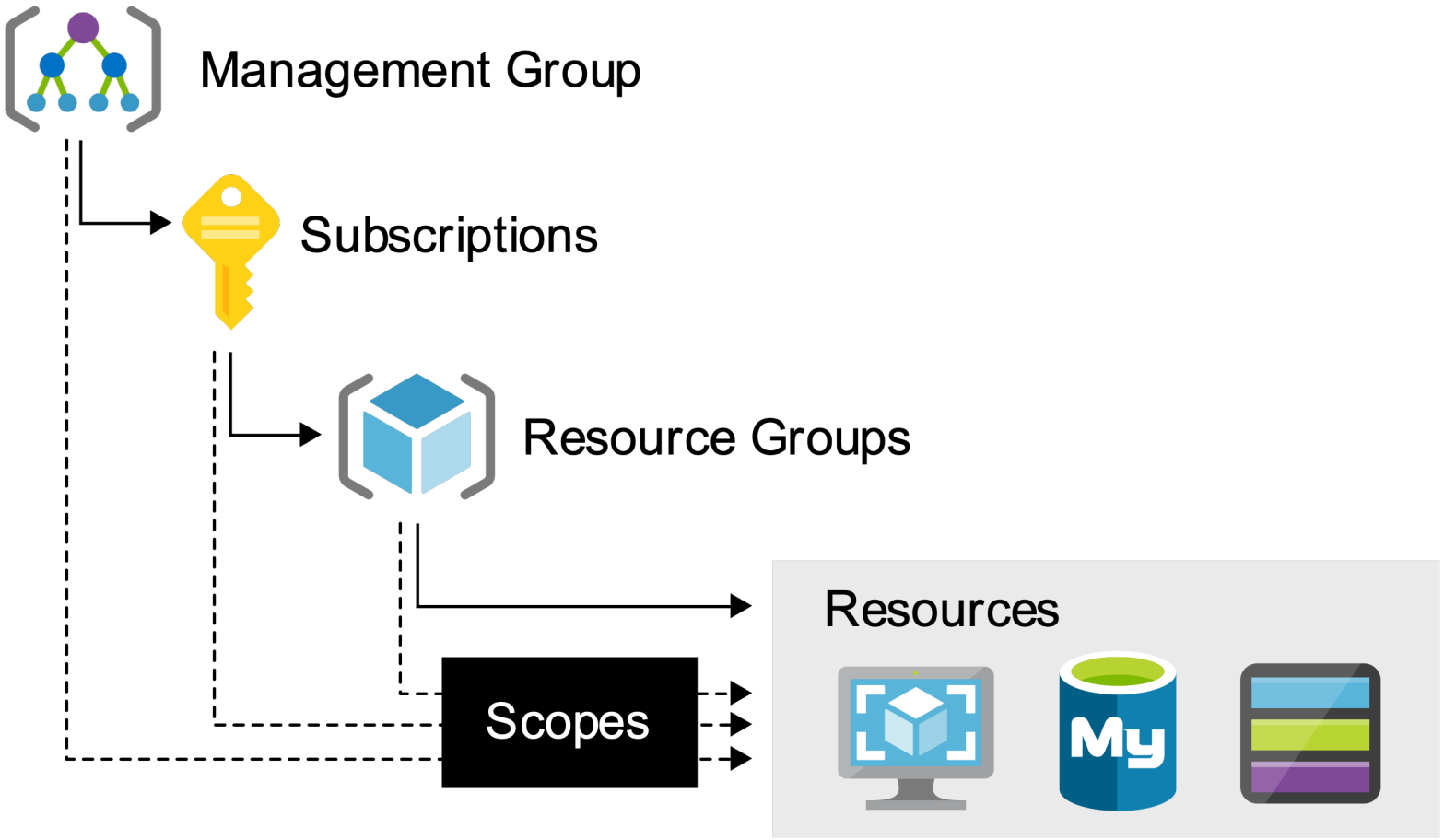
Group A set of users created in Azure Active Directory.

Service Principal A security identity used by applications or services to access specific Azure resources.

Managed identity An identity in Azure Active Directory that is automatically managed by Azure.

Azure Role-Based Access Control (RBAC)

Scope is the **set of resources** that access for the Role Assignment applies to.
Scope Access Controls at the Management, Subscription or Resource Group level.



Azure Role-Based Access Control (RBAC)

A Role Definition is a collection of permissions.
A role definition lists the operations that can be performed, such as **read, write, and delete**.
Roles can be high-level, like owner, or specific, like virtual machine reader.

Azure has **built-in roles** and you can define **custom roles**

	Read	Grant	Create, Update, Delete
Owner			
Contributor			
Reader			
User Access Administrator			

These are the four fundamental built-in role

Azure AD Roles

Azure AD roles are used to **manage Azure AD resources** in a directory such as:

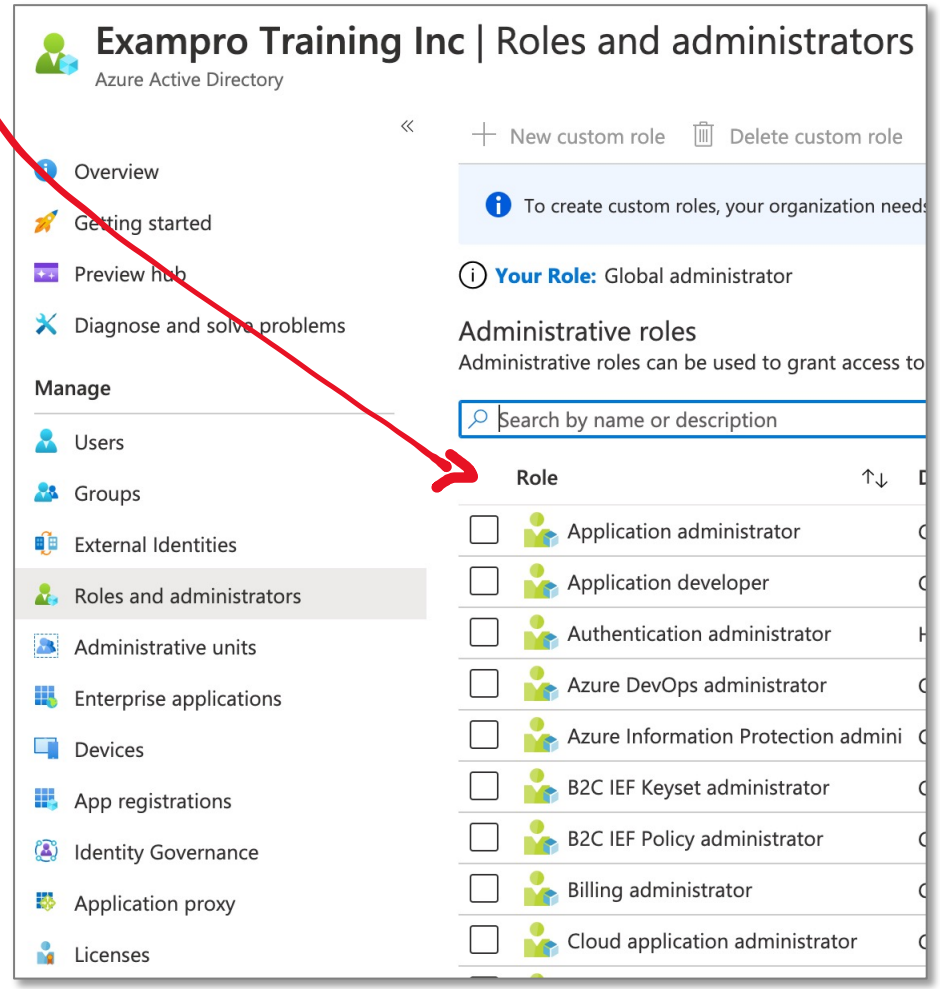
- create or edit users
- assign administrative roles to others
- reset user passwords
- manage user licenses
- manage domains.

A few important Built-In Azure AD roles you should know:

- **Global Administrator** Full access to everything
- **User Administrator** Full access to create and manage users
- **Billing Administrator** Make purchases, manage subscriptions and support tickets

<u>You can create custom roles</u> but you need to purchase either:

- Azure AD Premium P1 or P2



Identity Governance

Azure AD allows to **govern identities** to balance and organization security vs employee productivity

Ensure that the right people have the right access to the right resources.

Azure AD and Enterprise Mobility + Security features allows you to mitigate access risk by protecting, monitoring, and auditing access to critical assets

Identity Governance give organizations the ability to do the following:

- Govern the identity lifecycle
- Govern access lifecycle
- Secure privileged access for administration

Identity Governance address these 4 questions:

- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?

Human Capital Management

What is human capital management (HCM)?
The practice of managing people as resources within an organization.

What is an HCM system?
An application that provide **administrative** and **strategic** support around human resources

Administration:
- Payroll
- Benefits
- Employee self-service portal

Strategic:
- Workforce planning
- Competency management
- Performance management
- Time and expense management
- Education and training)
- Recruitment
- Onboarding
- Organization visualization

HCM systems:

successfactors™ An SAP Company

SAP HCM

workday.

ORACLE E-BUSINESS SUITE

ORACLE PeopleSoft

sage People

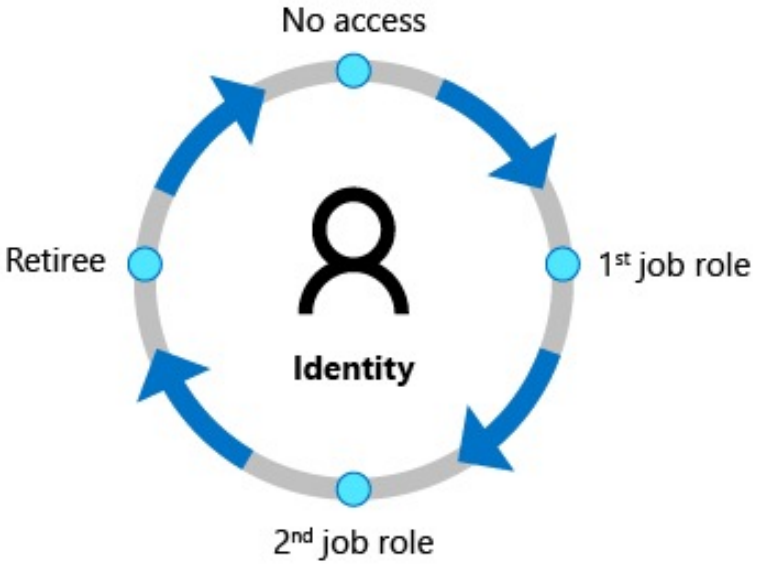
UZIO

Identity Governance – Identity Lifecycle

Identity lifecycle management is the **foundation** for Identity Governance
The goal is to achieve a balance between **productivity** and **security**

Productivity
How quickly can a person have access to the resources they need, such as when they join my organization?

Security
How should their access change over time, such as due to changes to that person's employment status?



Azure AD Premium automatically maintains user identities for people represented in **Workday** and **SAP SuccessFactors** in both Active Directory and Azure Active Directory,

Azure AD Premium also includes Microsoft Identity Manager

- can import records from on-premises HCM systems such as SAP HCM, Oracle eBusiness, and Oracle PeopleSoft.

Azure AD B2B collaboration enables you to securely share your organization's applications and services with guest users and external partners from any organization, while maintaining control over your own corporate data

Azure AD entitlement management enables you to select which organization's users are allowed to request access and be added as B2B guests to your organization's directory, and ensures that these guests are removed when they no longer need access.

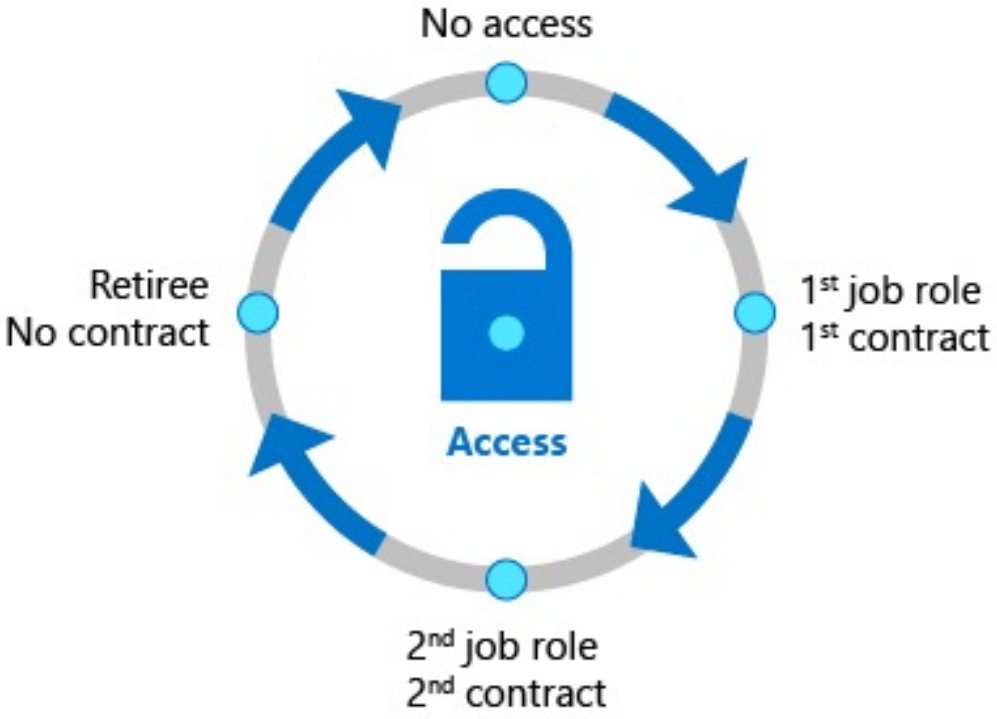
Identity Governance – Access Lifecycle

Access lifecycle is the process of managing user access throughout their lifecycle in an organization

Azure AD Dynamic Groups determine group membership based on **user** or device properties

Azure AD access reviews enforce review on a regular basis to make sure only the right people have continued access

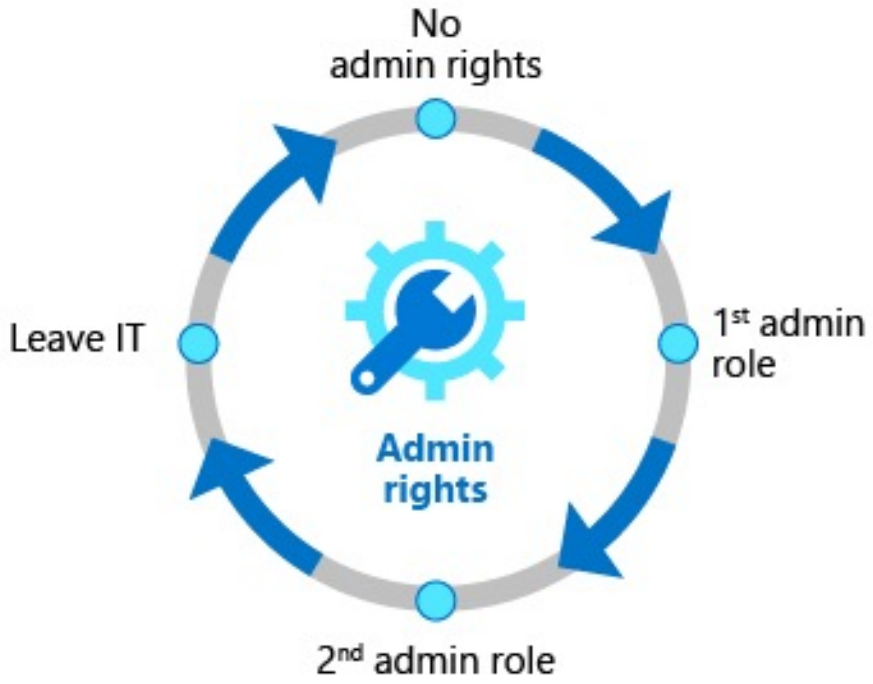
Azure AD entitlement management enables you to define how users request access across packages of group and team memberships, application roles, and SharePoint Online roles



Identity Governance – Privileged Access Lifecycle

Privileged Access Lifecycle is the management of fine-grade permissions over the life-cycle of a user within an organization.

Azure AD Privileged Identity Management (PIM) provides additional controls to securing access rights for resources, across Azure AD, Azure, and other Microsoft Online Services



Entitlement Management

Azure Active Directory (Azure AD) **entitlement management** is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating: **access request workflows, access assignments, reviews, expiration**

Entitlement management is a feature of **Azure AD Premium 2**.

Take a bunch of resources, bundled it into an access package, then apply it to internal or external users that for a specific range of time. **Just-in-Time Access**
You accomplish this by creating a project, catalog and access packages

Project – A logical container for your catalog and access packages
Catalog – resources that are assigned to the project

- Groups and teams, Applications, Sharepoint Sites

Access package

An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task.
Access packages are used to govern access for your internal employees, and also users outside your organization.
Access packages also include one or more policies. A policy defines the rules or guardrails for assignment to access package.

Access Packages can manage:

- Group memberships
- Cloud app access and access rights
- SharePoint online sites
- Organizational and technical roles

Privileged Identity Management (PIM)

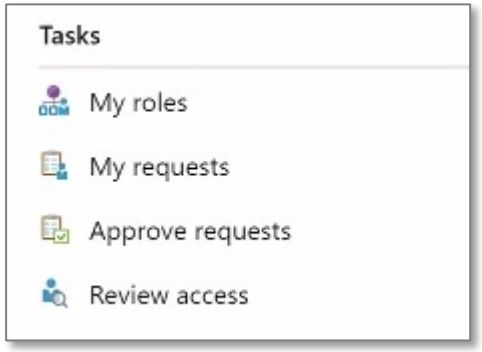
Privileged Identity Management (PIM) is an Azure AD service enabling you to **manage, control, and monitor access to** important resources in your organization

You can manage resources from:

- Azure AD
- Azure
- Microsoft 365
- Microsoft Intune
- And more!

Key features:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit



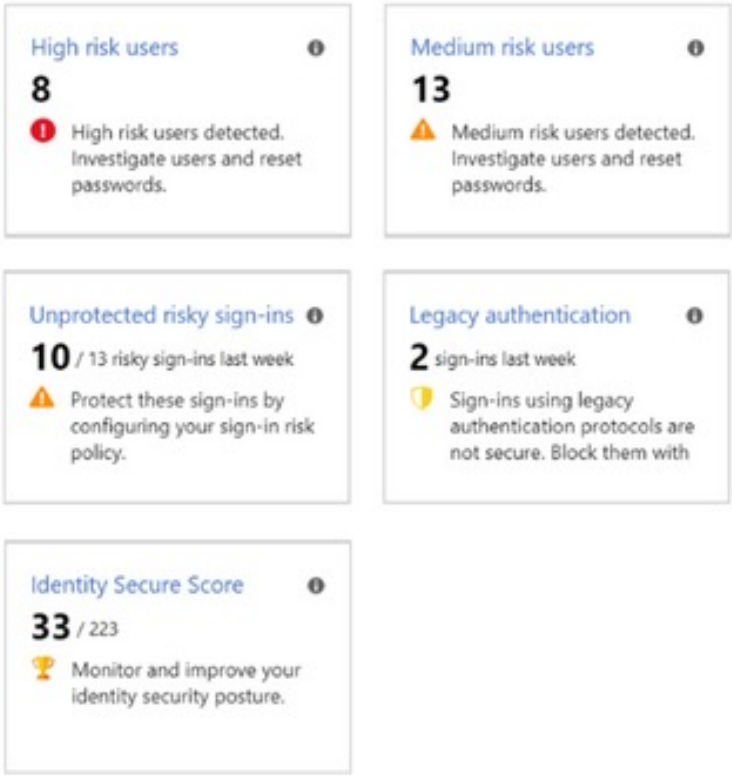
Privileged Identity Management is a feature of **Azure AD Premium 2**

Azure AD Identity Protection

Identity Protection is an Azure AD that's you to **detect, investigate, remediate and export** for future analysis **identity-based risks**.

Microsoft analyses 6.5 trillion signals per day to identify and protect customers from threats.

Identity Protection notices:
Risky Users
Risky Sign-ins
Risk Detections



Identity Protection – Detection and Remediation

Identity Protection identifies for the following risks:

Anonymous IP address Sign in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

Atypical travel Sign in from an atypical location based on the user's recent sign-ins

Malware linked IP address Sign in from a malware linked IP address

Unfamiliar sign-in properties Sign in with properties we've not seen recently for the given user

Leaked Credentials Indicates that the user's valid credentials have been leaked

Password spray multiple usernames being attacked using common passwords in a unified, brute-force manner

Azure AD threat intelligence Microsoft's internal and external threat intelligence sources have identified a known attack pattern

New country This detection is discovered by Microsoft Cloud App Security (MCAS)

Activity from anonymous IP address This detection is discovered by Microsoft Cloud App Security (MCAS)

Suspicious inbox forwarding This detection is discovered by Microsoft Cloud App Security (MCAS)

The **risk signals** can **trigger remediation efforts** such as requiring users:
Azure AD Multi-Factor Authentication, reset their password using self-service password reset,
or blocking until an administrator takes action

Identity Protection – Investigation

Identity Protection categorizes risk into three tiers: **low, medium, and high**.

Key reports that admin use for investigations in Identity Protection **Risky users**, **Risky sign-ins**, **Risk detections**

Risky users

- Details about detections
- History of all risky sign-ins
- Risk history

Risky sign-ins

- Which sign-ins are classified as at risk, confirmed compromised, confirmed safe, dismissed, or remediated.
- Real-time and aggregate risk levels with sign-in attempts.
- Detection types triggered
- Conditional Access policies applied
- MFA details
- Device, Application, Location information

Risk detections

contains filterable data for up to the past 90 days

- Information about each risk detection including type.
- Other risks triggered at the same time
- Sign-in attempt location
- Link out to more detail from MCAS

Admin follow up actions:

- Reset the user password
- Confirm user compromise
- Dismiss user risk
- Block user from signing in
- Investigate further using Azure ATP

Network Security Groups (NSG)

Network security group (NSG) **filter network traffic** to and from Azure resources in a VNet

An NSG is composed of many **Security Rules**

Each Security Rule has the following properties:

Name — A unique name within the network security group.

Source or destination — An IP Address or CIDR block, Service Tag or Application Security Group

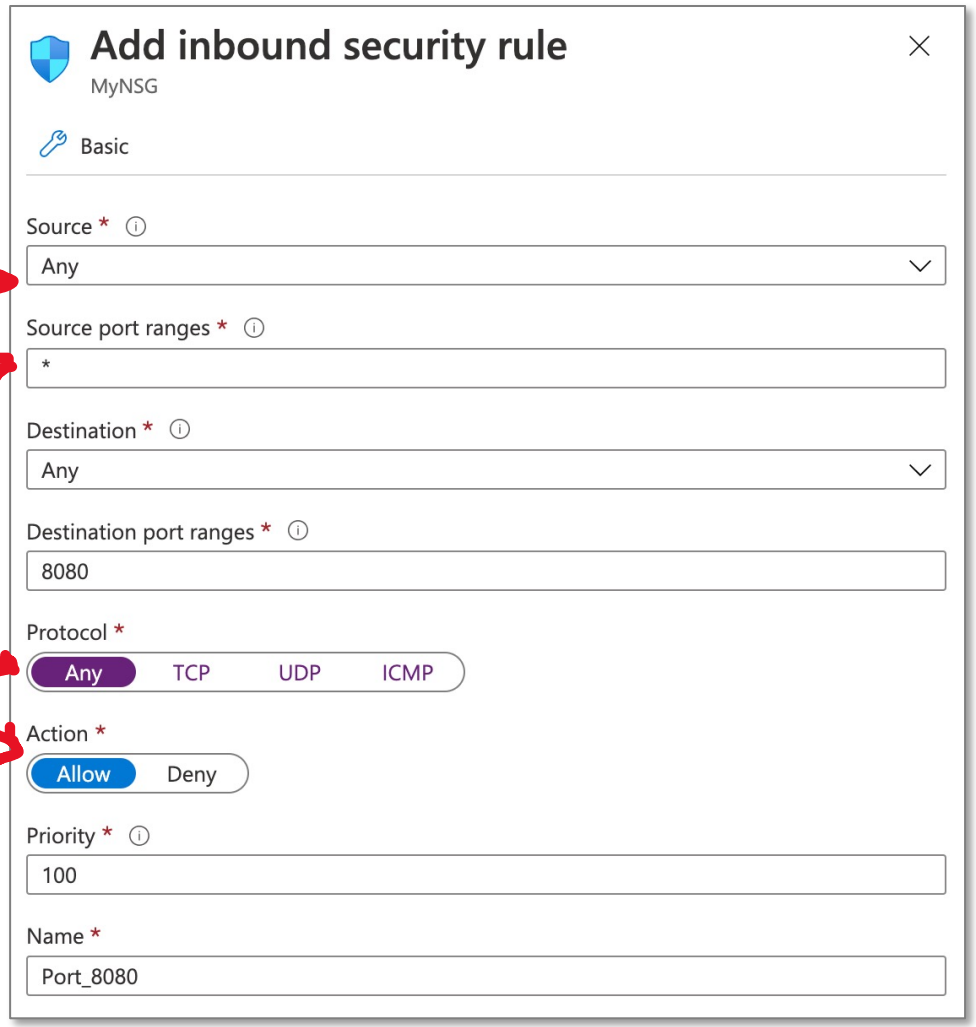
Port Range — Specify a single or range of ports. eg. 80 or 10000-10005

Protocol — TCP, UDP, ICMP or ANY

Action — Allor or Deny

Priority — A number between 100 and 4096 (lower number higher priority)

- **Inbound Rules** apply to traffic ***entering*** the NSG
- **Outbound Rules** apply to traffic ***leaving*** the NSG



NSG – Default Security Rules

Azure sets the following **default security rules** when you create an NSG:

Outbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Inbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

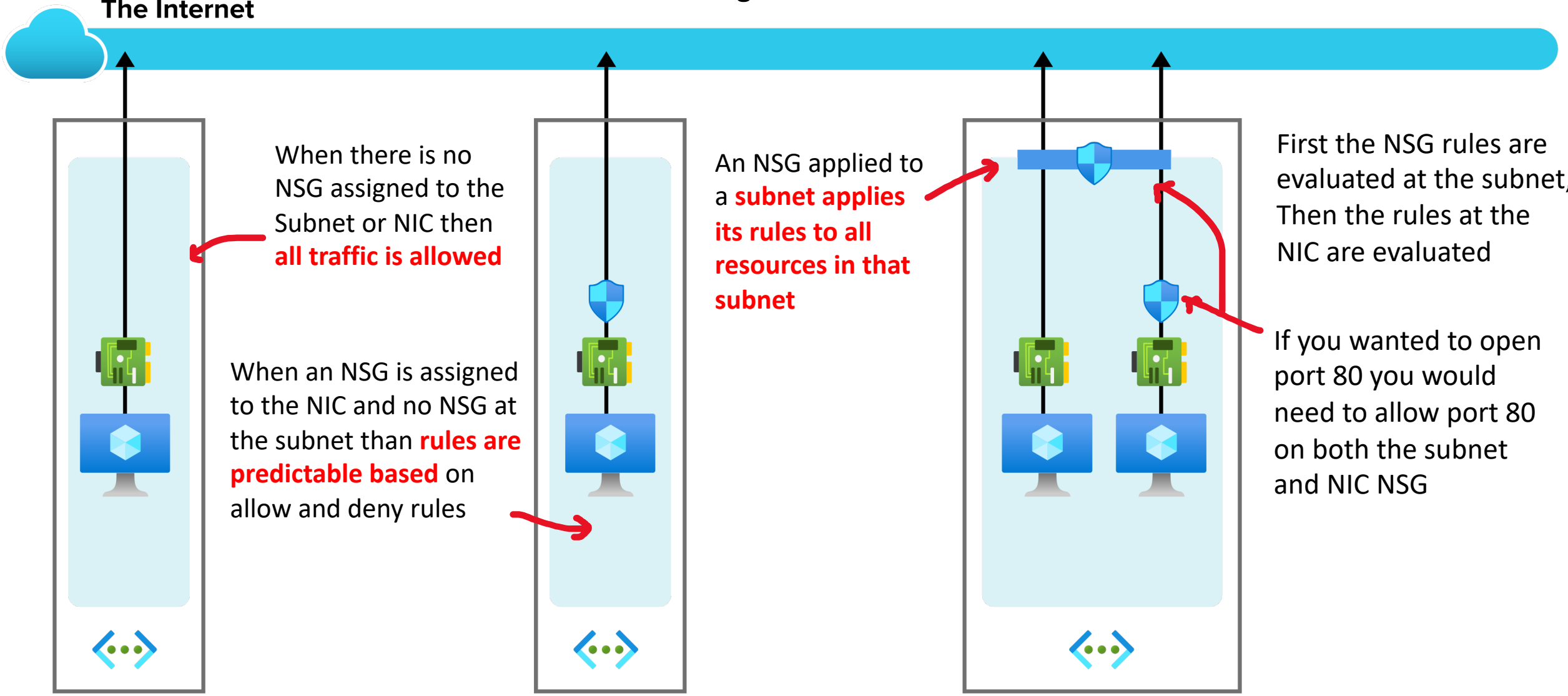
NSG – Security Rules Logic

Security Rules has **a lot of logic** to determine how to apply its rules

- You may not create two security rules with the same priority and direction.
- You can have 5000 NSG per subscription, 1000 NSG rules per NSG
- **Priority**
  - Rules are processed in priority order, with lower numbers processed before higher number
  - Network security group security rules are evaluated by priority using the 5-tuple information to allow or deny traffic: 1] source 2] source port 3] Destination 4] destination port 5] protocol
- **Flow Records**
  - The flow record allows a network security group to be stateful.
  - A flow record is created for existing connections
  - Communication is allowed or denied based on the connection state of the flow record.
- **Statefulness**
  - If you specific an outbound security port you don't need to set the inbound port since it will be set for you.
  - You only need to specify an inbound security rule if communication is initiated externally.
  - The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.
- **Interruption**
  - Existing connections may not be interrupted when you remove a security rule that enabled the flow.
  - Traffic flows are interrupted when connections are stopped and no traffic is flowing in either direction, for at least a few minutes.

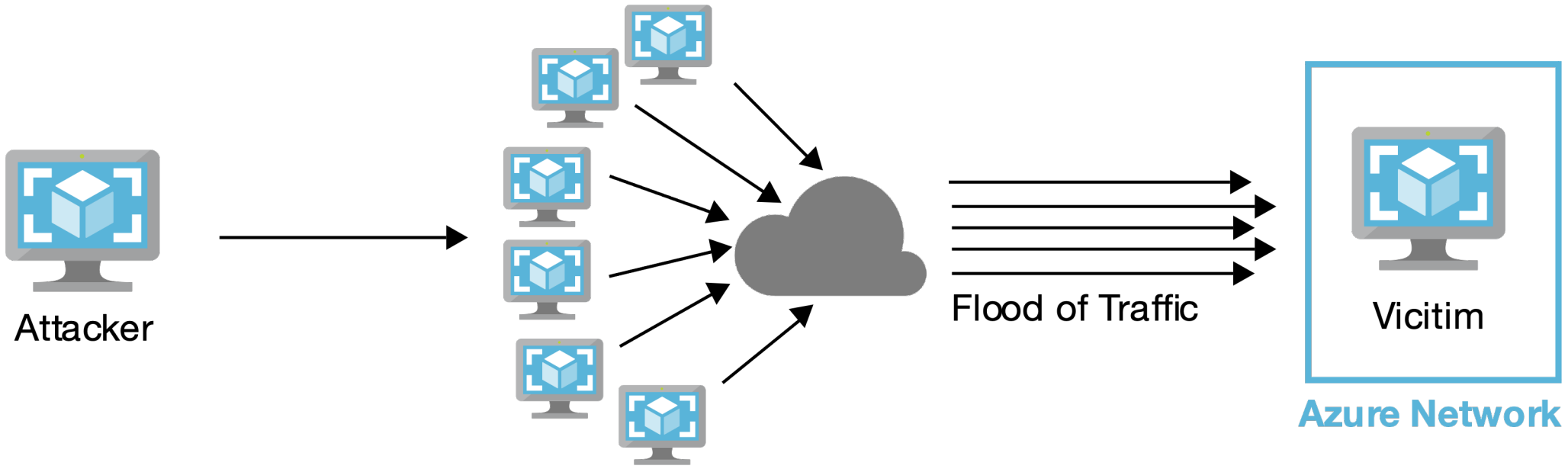
Network Security Groups (NSG)

Let's look at how rules changed based on NSG attached



Azure DDoS Protection

What is a DDoS (Distributed Denial of Service) Attack?
A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic.



Azure DDoS Protection

Most frequent types of DDoS attack:

- **Volumetric attacks**
  - Volume-based attacks that flood the network with legitimate looking traffic
  - Exhausts available bandwidth
  - Legitimate uses cannot access website
  - Measured in Bits per second (bps)
- **Protocol attacks**
  - exhausting server resources with false protocol requests that exploit weaknesses
    - UDP and TCP flooding on Layer 3 and 4
  - Measured in packages per second (psp)
- **Application layer attacks**
  - Attacks that occurs at the application layer (Layer 7)
  - HTTP floods, SQL injections, cross-site scripting (XSS) , parameter tampering, Sowloris attacks
  - Web Application Firewalls (WAFs) are used as means of protection

Azure DDoS Protection

Azure offers **two tiers** of DDoS Protection

DDoS Protection Basic

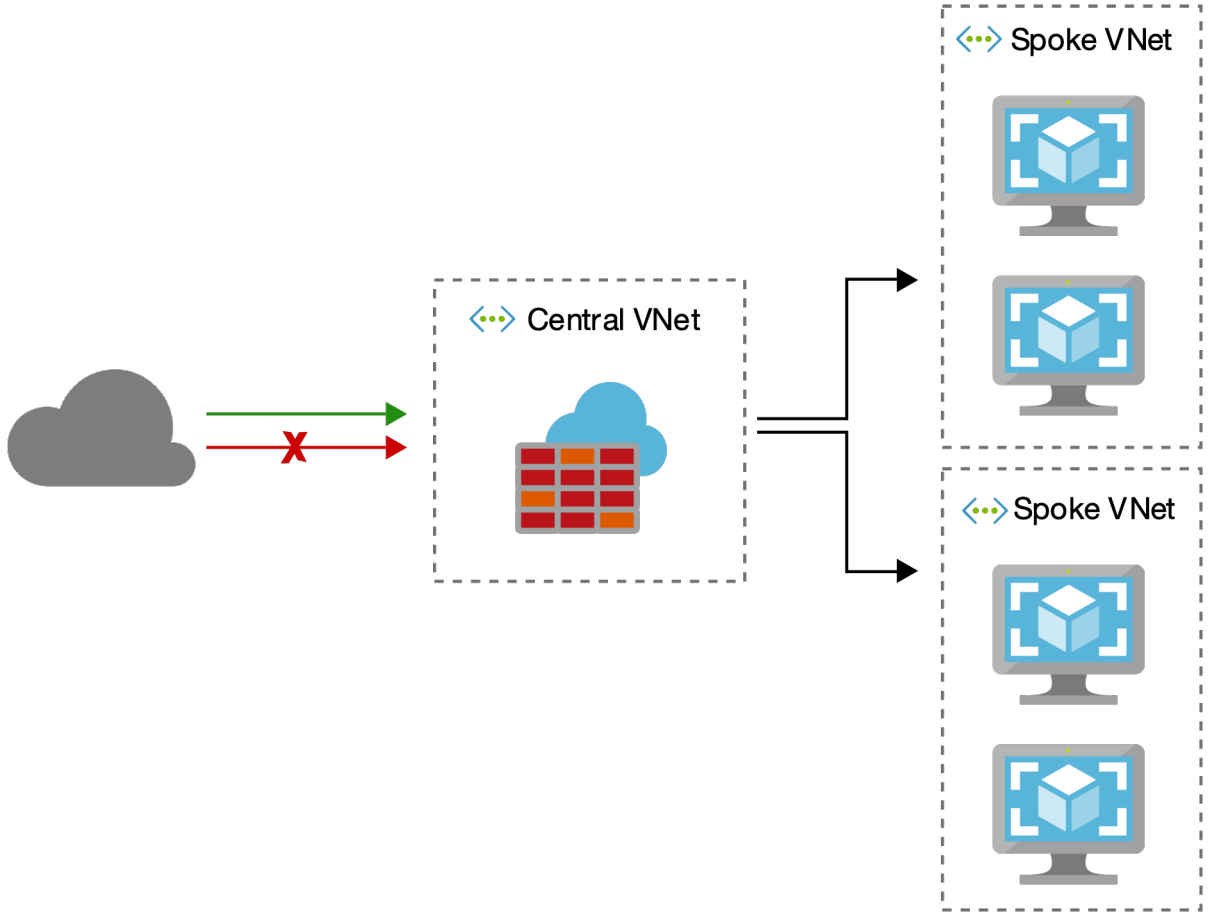
- Free
- Already turned on protect Azure‘s global network

DDoS Protection Standard

- Starting at $2,994/month
- Metrics, Alerts, Reporting
- DDoS Expert Support
- Application and Cost Protection SLAs

Azure Firewall

Azure Firewall is a managed, **cloud-based network security service** that protects your Azure Virtual Network resources.



Azure Firewall

Azure Firewall Features

- Centrally create, enforce, and log application and network connectivity policies **across subscriptions** and virtual networks.
- Uses a **static public IP address** for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network
- High availability is built in**, no additional load balancers are required**
- Can configure during deployment to **span multiple AZs for increased availability**.
- There's **no additional cost** for a firewall deployed in an Availability Zone (AZ)
- There are **additional costs for inbound and outbound data transfers** associated with AZs

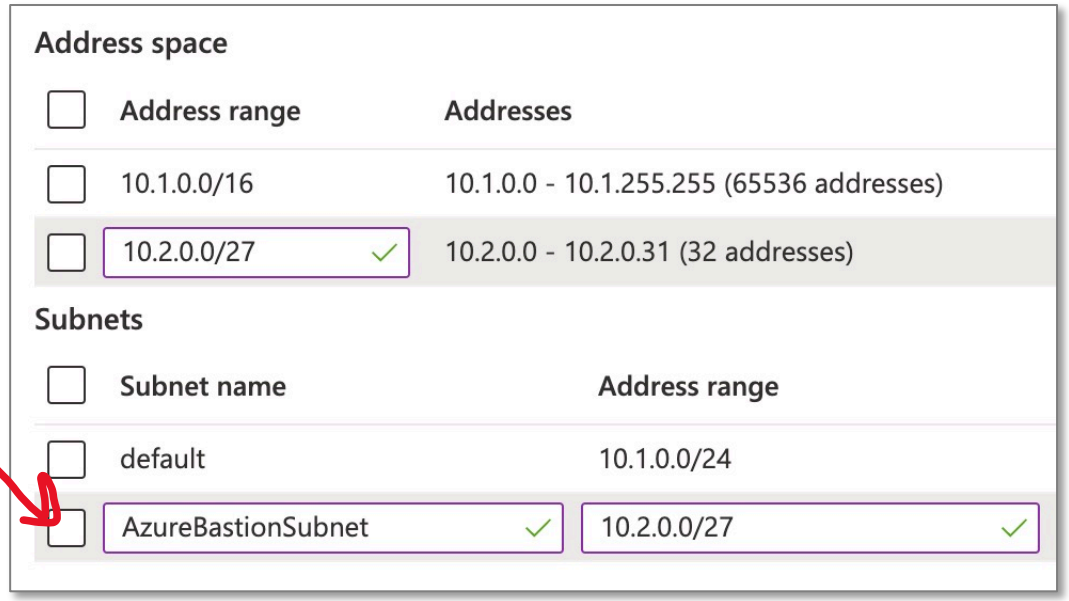
Azure Bastion

Azure Bastion is an **intermediate harden instance** you can use to connect to your target server via SSH or RDP
It will provision a web-based RDP client or SSH Terminal

A bastion is also known as a **jump box**.

Some devices cannot run an RDP Client such **as Google Chromebook**
and so Azure Bastion is one of the only ways to allow you to do that

When you create an Azure Bastion
You need to add a Subnet to your VNet
called **AzureBastionSubet** with at least a
size of /27 (32 addreses)

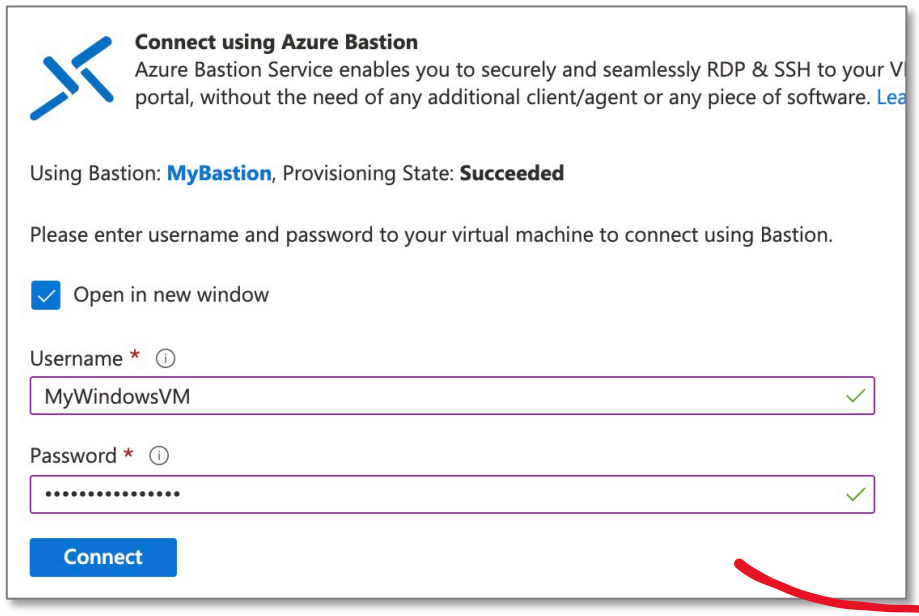


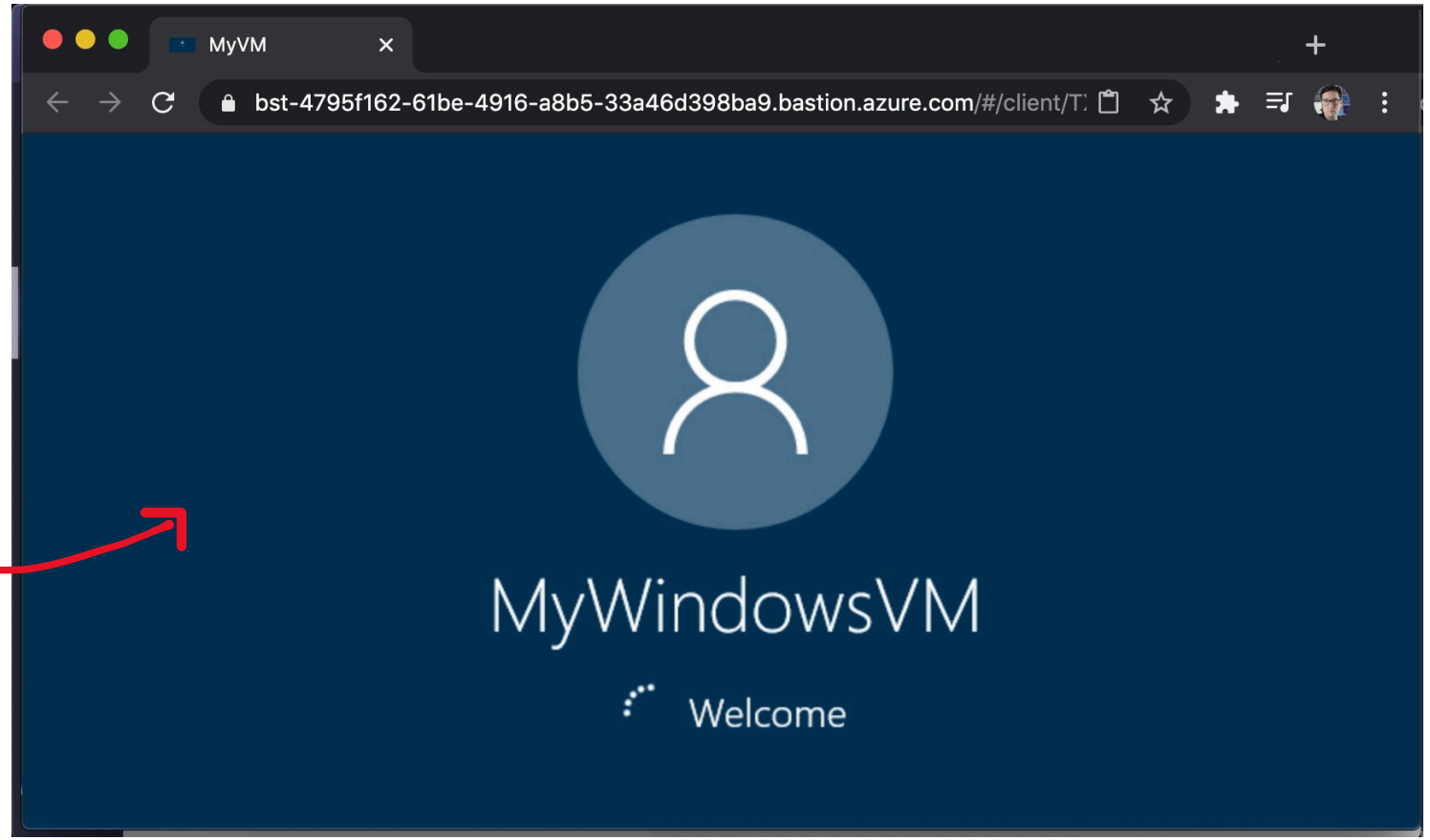
Key Features

- RDP and SSH directly in Azure portal
- Remote Session over TLS and firewall traversal for RDP/SSH:
- No Public IP required on the Azure VM
- No hassle of managing NSGs
- Protection against port scanning
- Protect against zero-day exploits. Hardening in one place only

Azure Bastion

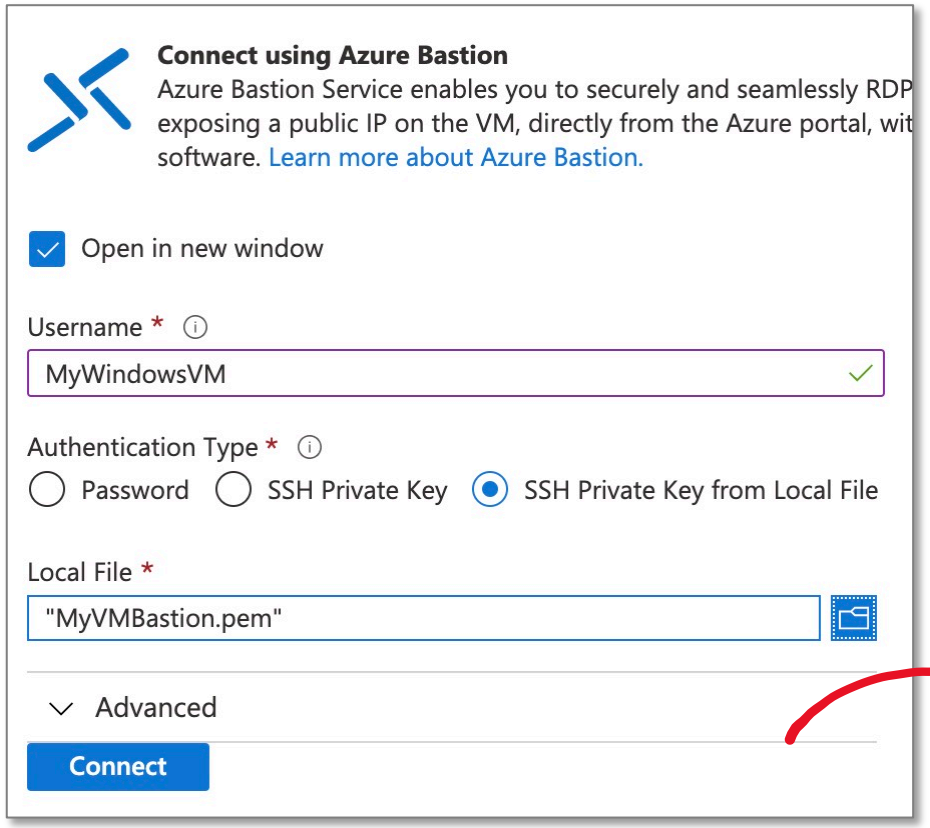
If you have a Windows Server which requires RDP, and have a Bastion in the same VNet
You just enter in your Username and Password as you normally would

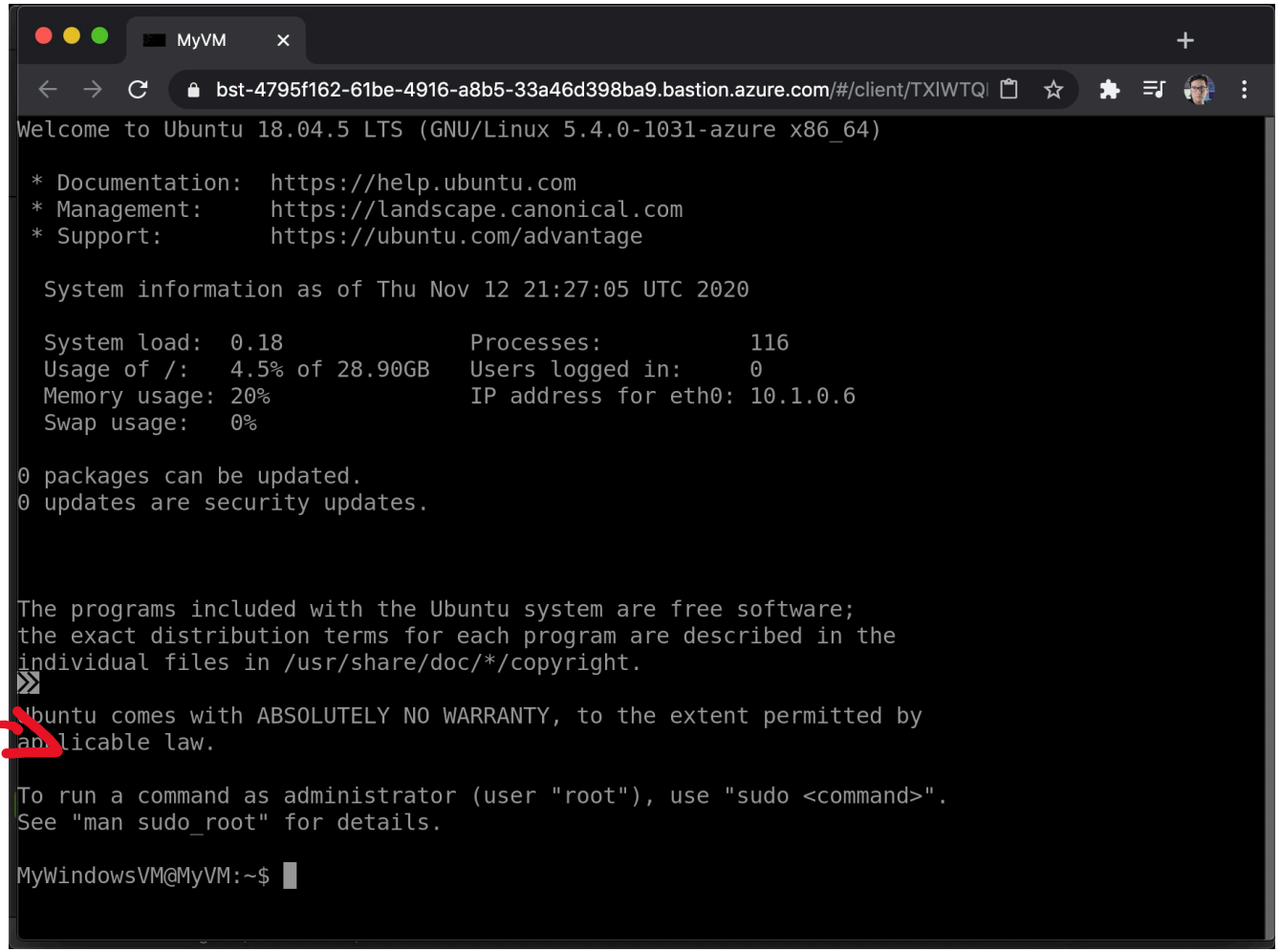




Azure Bastion

If you have a Linux server you can SSH with the Bastion.
You can use SSH Private Key or Password that you set when you created your VM





Azure Web Application Firewall

What is a WAF?
A Web Application Firewall is service that protects web-applications communication on the application layer (layer 7) by **analyzing incoming HTTP requests**.
WAFs for cloud providers are generally attached to Load Balancers, API Gateways or CDNs.

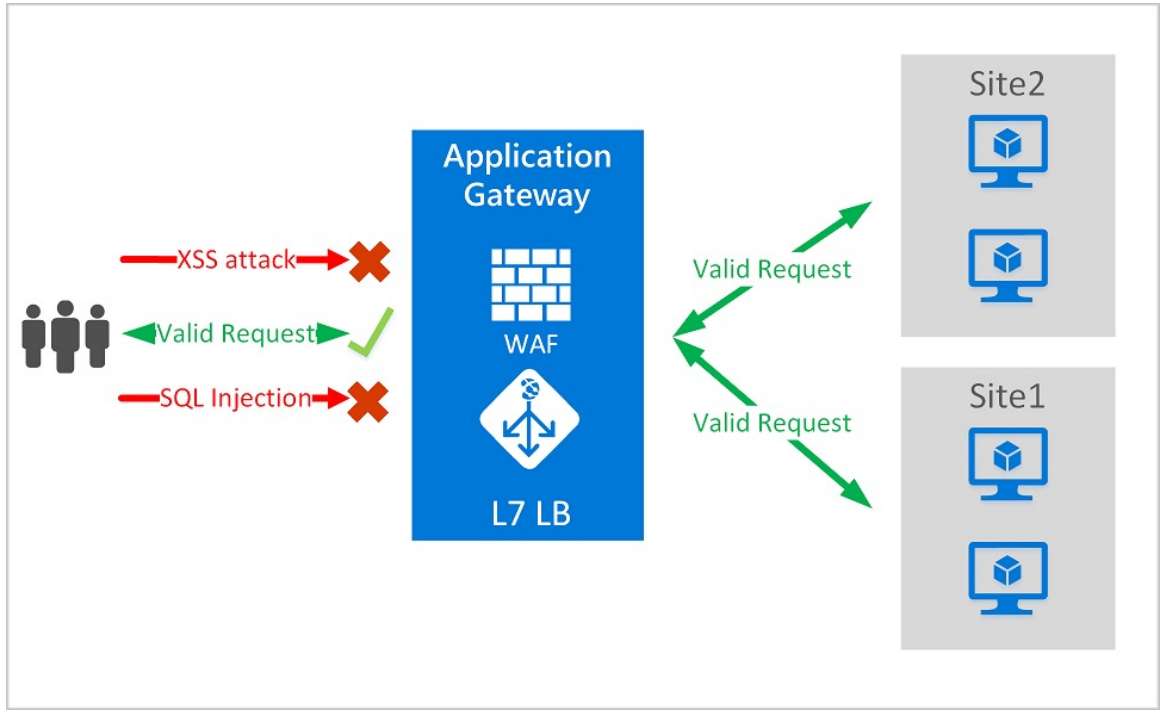
Azure WAF can be attached to:

- Azure Application Gateway (an application load balancer)
- Azure Front Door (CDN)
- Azure Content Delivery Network (CDN)

Azure WAF uses the **Core Rules Set (CRS)** by **OWASP** to protection against common vulnerabilities

A WAF Policy allows you to apply:

- Managed Rules (Azure-managed OWASP rules)
- Custom Rules



Azure Encryption Overview

Azure provides a variety of encryption methods:

- **Azure Storage Service Encryption (SSE)**
  - protect data at rest by automatically encrypting before persisting it to:
    - Azure-managed disks
    - Azure Blob Storage
    - Azure Files
    - Azure Queue Storage
  - It also is used to decrypt data on retrieval
- **Azure Disk Encryption**
  - encrypt Windows and Linux IaaS virtual machine disks
  - Uses BitLocker feature on Windows or DM-Crypt on Linux
- **Transparent data encryption (TDE)**

Azure Disks Encryption

Azure Managed Disks supports 2 types of encryption:

- Server Side Encryption (SSE)
- Azure Disk Encryption (ADE)

Server Side Encryption (SSE)

provides encryption-at-rest and safeguards your data to meet your organizational security and compliance commitments.

enabled **by default** for all managed disks, snapshots, and images

Temporary disk are not encrypted by server-side encryption unless you enable encryption at host

Keys can be managed two ways:

1. Platform-managed keys — Azure manages your keys
2. Customer-managed keys — You manage your keys

Azure Disk Encryption (ADE)

allows you to **encrypt the OS and Data** disks used by an IaaS Virtual Machine

- For Windows encryption is done by **BitLocker**
- For Linux encryption is done by **DM-Crypt**

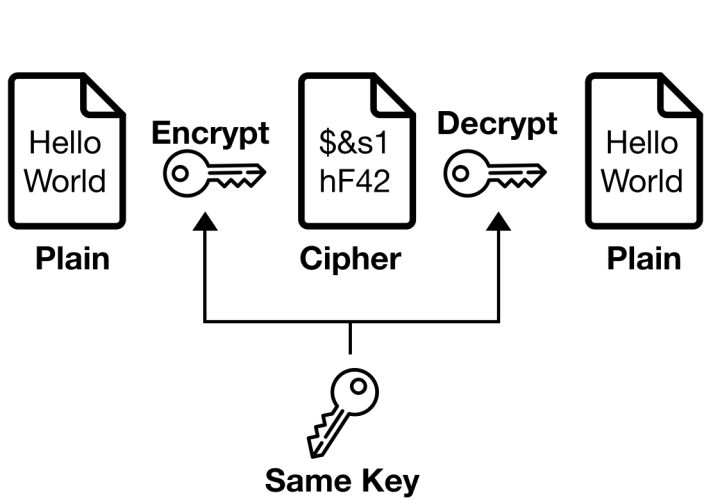
Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) **encrypts data-at-rest** for Microsoft Databases

TDE can be applied to:

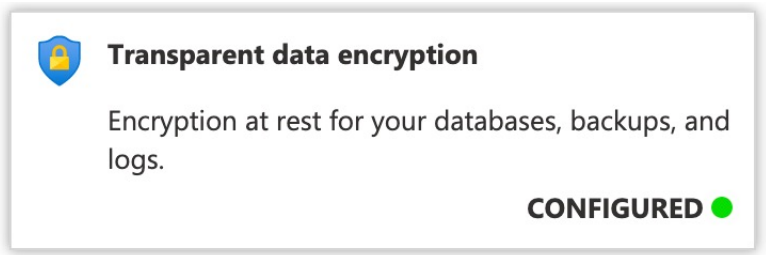
- SQL Server
- Azure SQL Database
- Azure Synapse Analytics

- TDE does real-time I/O encryption and decryption of data and log files
- encryption uses a database encryption key (DEK)
- database boot record stores the key for availability during recovery
- The DEK is a **symmetric key** (same cryptographic **keys** for both the **encryption** of plaintext and the decryption of ciphertext.)



Steps to apply TDE to a database:

- Create Database Master Key
- Create a Certificate to support TDE
- Create Database Encryption Key
- **Enable TDE on Database**



Key Vault

Azure Key Vault helps you **safeguard** **cryptographic keys and other secrets** used by cloud apps and services.

Secrets Management
store and tightly control access to **tokens, passwords, certificates, API keys, and other secrets**

Key Management
create and control the **encryption keys** used to encrypt your data

Certificate Management
easily provision, manage, and deploy public and private **SSL certificates** for use with Azure and internal connected resources.

Hardware Security Module
secrets and keys can be protected either by software or **FIPS 140-2 Level 2** validated HSMs

Key Vault

An HSM is a **Hardware Security Module**.
Its a piece of hardware designed to store encryption keys.

Federal Information Processing Standard (FIPS) 140-2
US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

HSM's that are **multi-tenant** are **FIPS 140-2 Compliant**
(multiple customers virtually isolated on an HSM)

HSM's that are **single-tenant** are **FIPS 140-3 Compliant**
(single customer on a dedicated HSM)

Azure Security Benchmark

Azure Security Benchmark includes a collection of high-impact security recommendations you can use to help secure the services you use in Azure.
It includes **Security Controls** and **Service Baselines**

The Azure Security Benchmark holistic security guidance is influenced by :

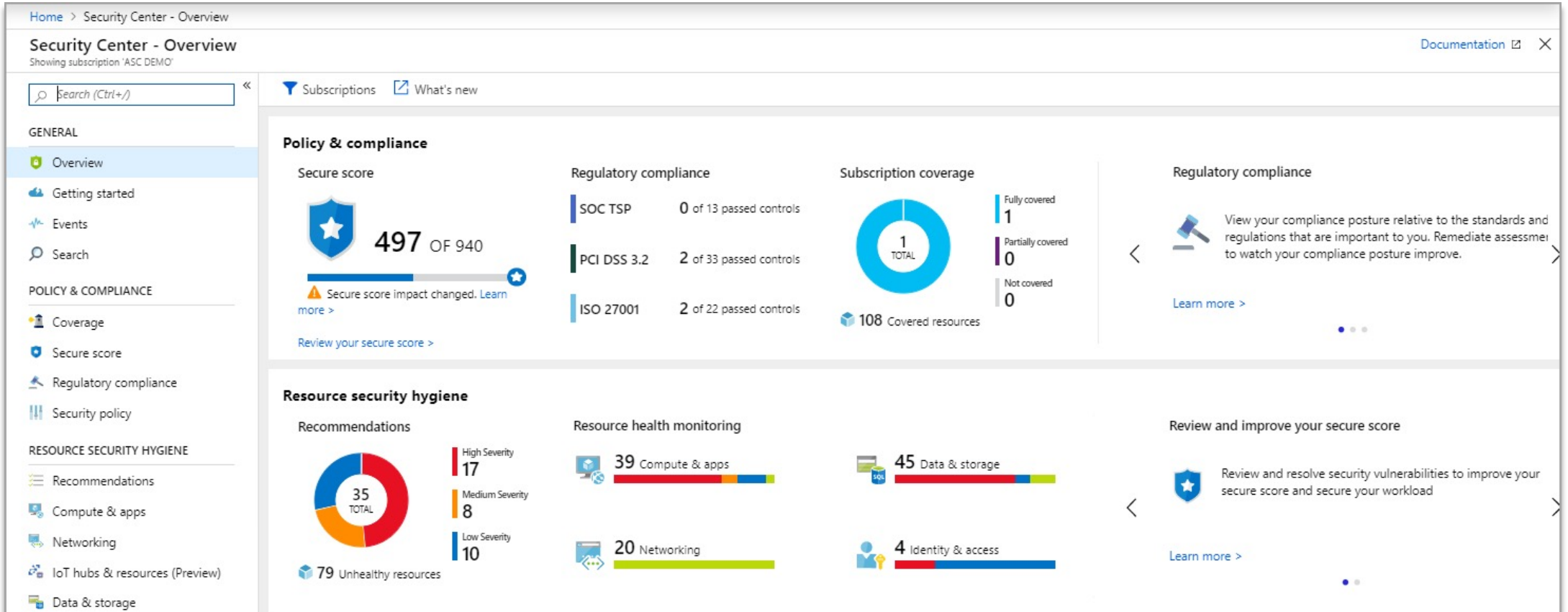
- Cloud Adoption Framework
- Azure Well-Architected Framework
- Microsoft Security Best Practices

Security controls
These recommendations are generally applicable across your Azure tenant and Azure services. Each recommendation identifies a list of stakeholders that are typically involved in planning, approval, or implementation of the benchmark.

Service baselines
These apply the controls to individual Azure services to provide recommendations on that service's security configuration.

Azure Security Center

Azure Security Center is a **unified infrastructure security management system**
It strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud.

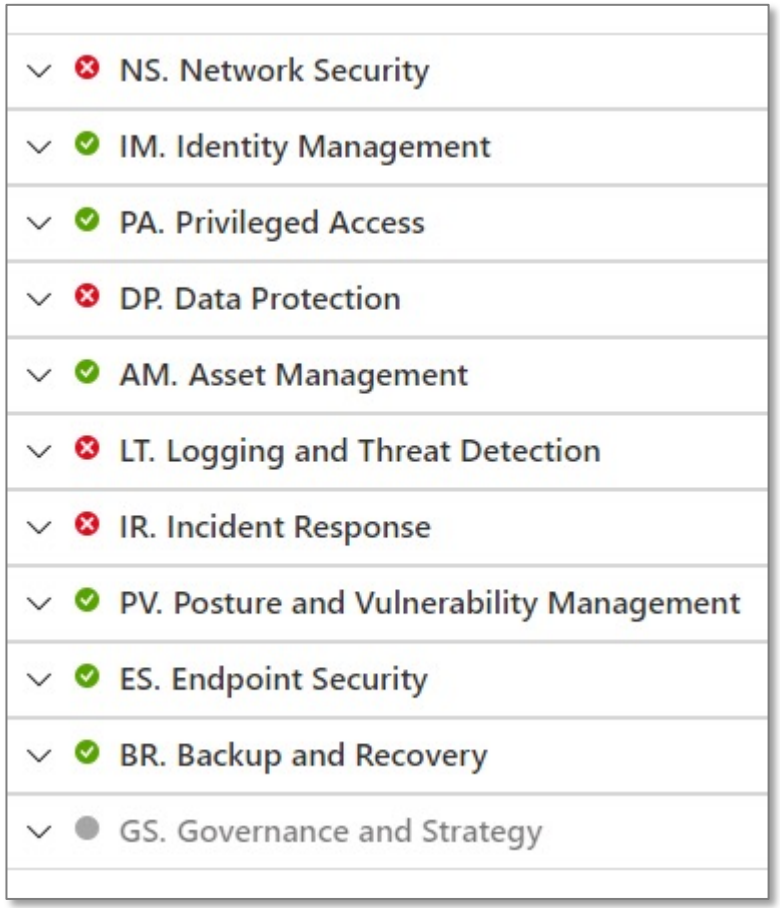


Azure Security Center – Regulatory Compliance

Regulatory Compliance Dashboard shows you your **compliance posture** for a set of supported standards and regulations, based on continuous assessments of your Azure environment

Compliance policies currently supported for the dashboard

- **Azure Security Benchmark**
- PCI DSS 3.2.1
- ISO 27001
- SOC TSP



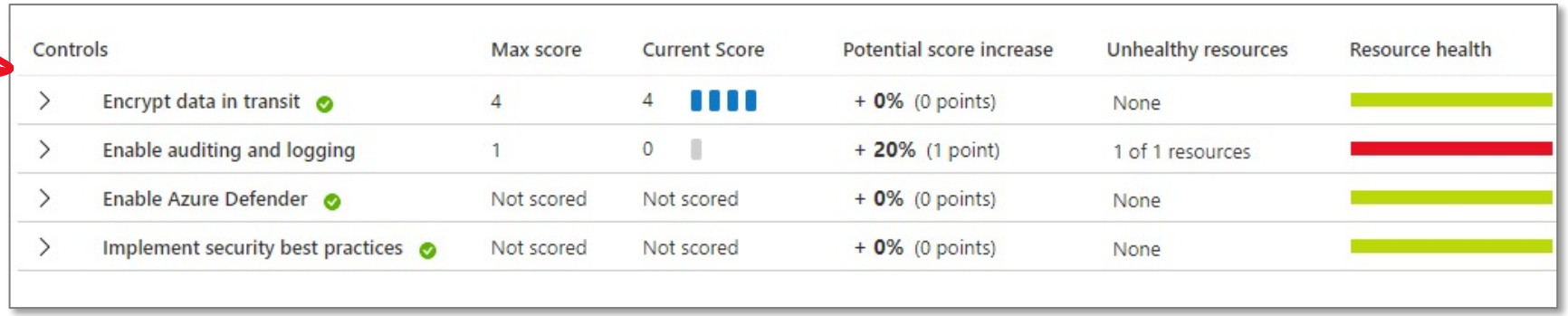
Azure Security Center – Secure Score

Security Center continually assesses your resources, subscriptions, and organization for security issues.
It then aggregates all the findings into a **single score** so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

The Security Score helps with:

- understanding your current security situation
- efficiently and effectively improve your security

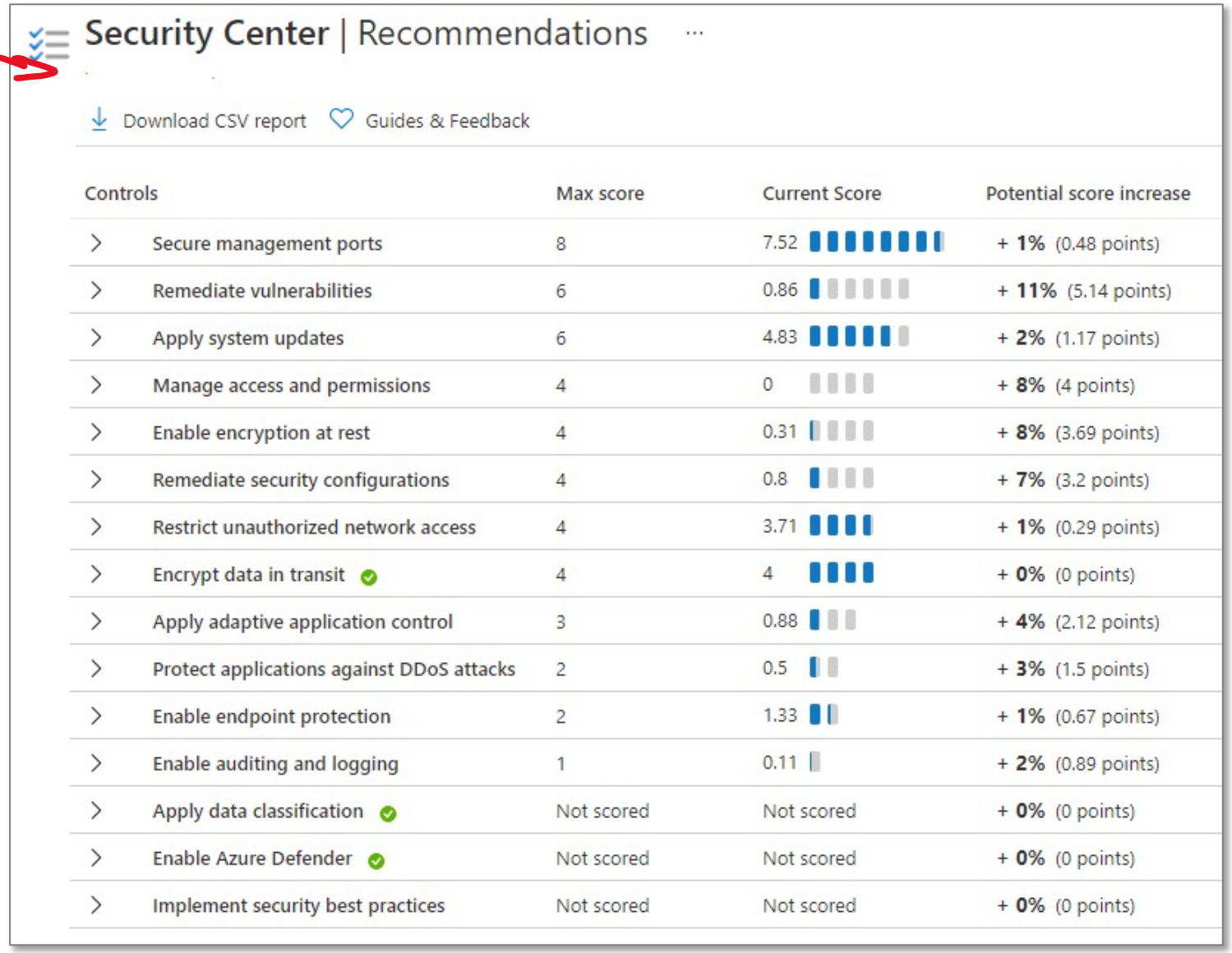
The **security controls** within Azure Security Center are used to calculate the overall score



Controls	Max score	Current Score	Potential score increase	Unhealthy resources	Resource health
Encrypt data in transit	4	4	+ 0% (0 points)	None	
Enable auditing and logging	1	0	+ 20% (1 point)	1 of 1 resources	
Enable Azure Defender	Not scored	Not scored	+ 0% (0 points)	None	
Implement security best practices	Not scored	Not scored	+ 0% (0 points)	None	

Azure Security Center – Secure Controls

Security controls are **recommendations** of actionable security items that will help improve your overall security score.

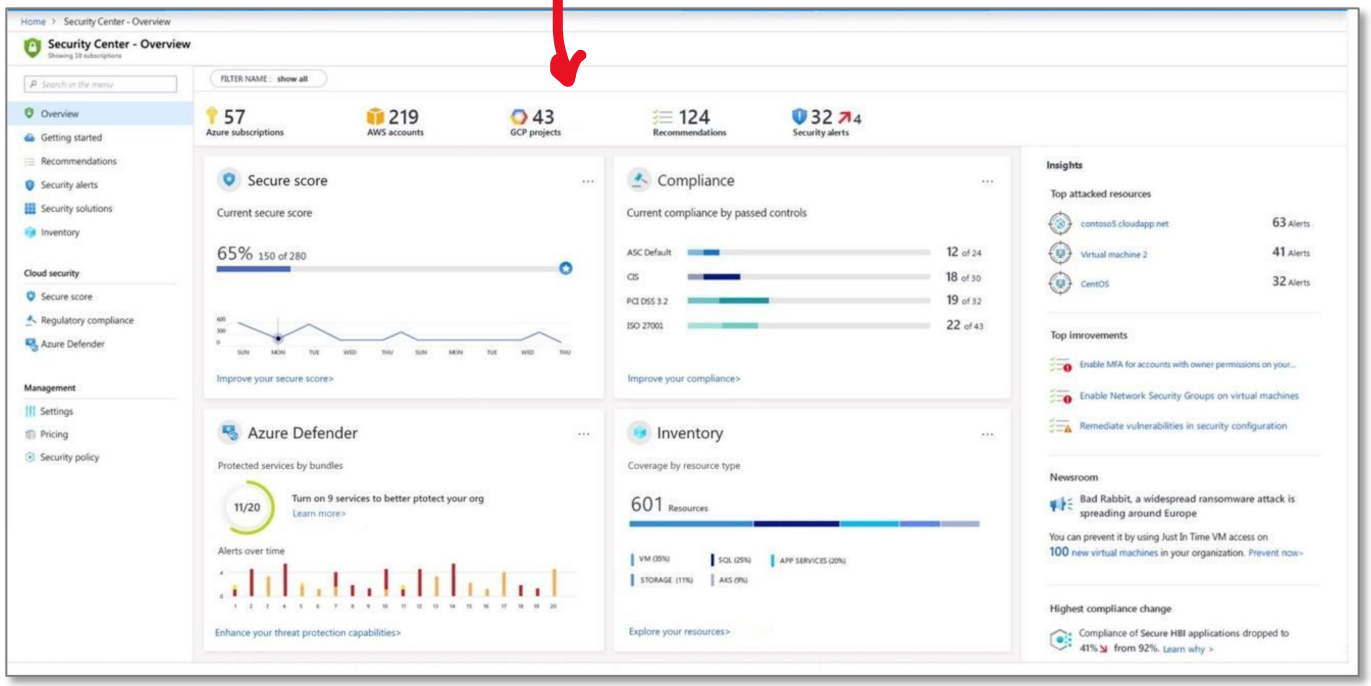


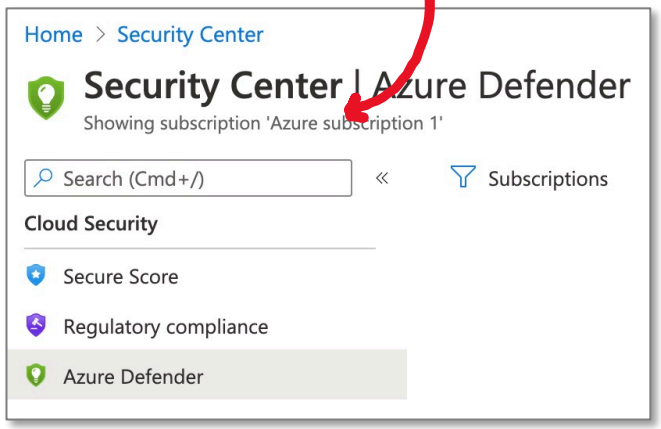
Controls	Max score	Current Score	Potential score increase
Secure management ports	8	7.52	+ 1% (0.48 points)
Remediate vulnerabilities	6	0.86	+ 11% (5.14 points)
Apply system updates	6	4.83	+ 2% (1.17 points)
Manage access and permissions	4	0	+ 8% (4 points)
Enable encryption at rest	4	0.31	+ 8% (3.69 points)
Remediate security configurations	4	0.8	+ 7% (3.2 points)
Restrict unauthorized network access	4	3.71	+ 1% (0.29 points)
Encrypt data in transit	4	4	+ 0% (0 points)
Apply adaptive application control	3	0.88	+ 4% (2.12 points)
Protect applications against DDoS attacks	2	0.5	+ 3% (1.5 points)
Enable endpoint protection	2	1.33	+ 1% (0.67 points)
Enable auditing and logging	1	0.11	+ 2% (0.89 points)
Apply data classification	Not scored	Not scored	+ 0% (0 points)
Enable Azure Defender	Not scored	Not scored	+ 0% (0 points)
Implement security best practices	Not scored	Not scored	+ 0% (0 points)

Azure Defender

Azure Defender provides **advanced protection** for your Azure and on-premise workloads

Azure Defender can be found in the **Azure Security Center**



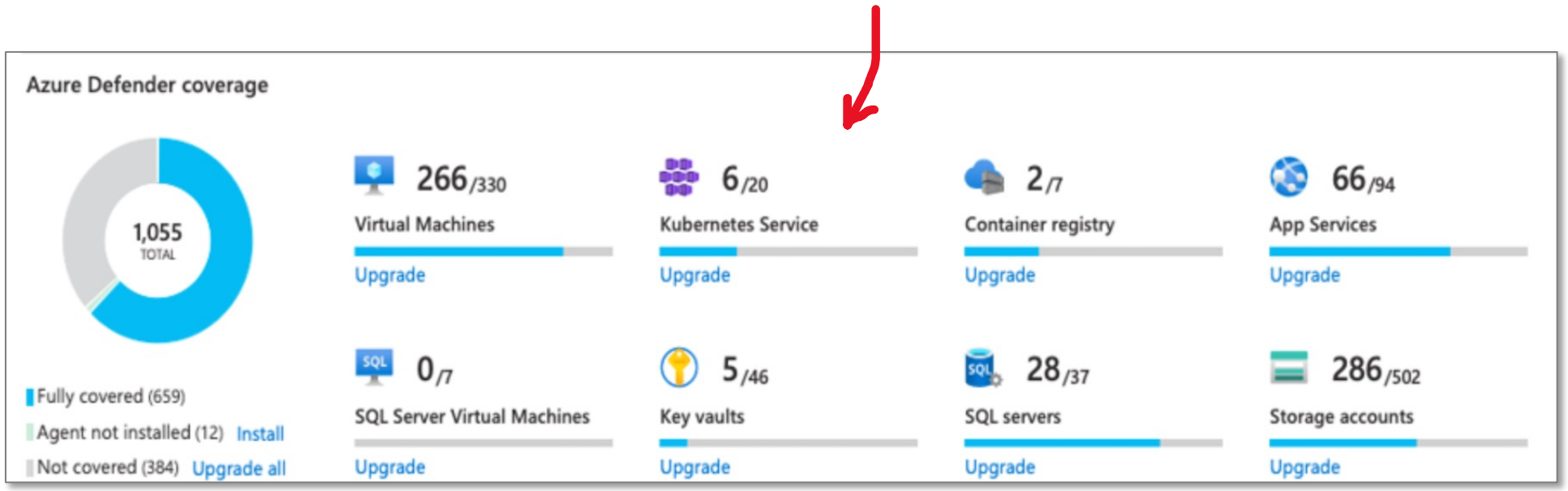


Azure Defender is composed of:

- Coverage
- Security Alerts
- Insights
- Advanced Protection

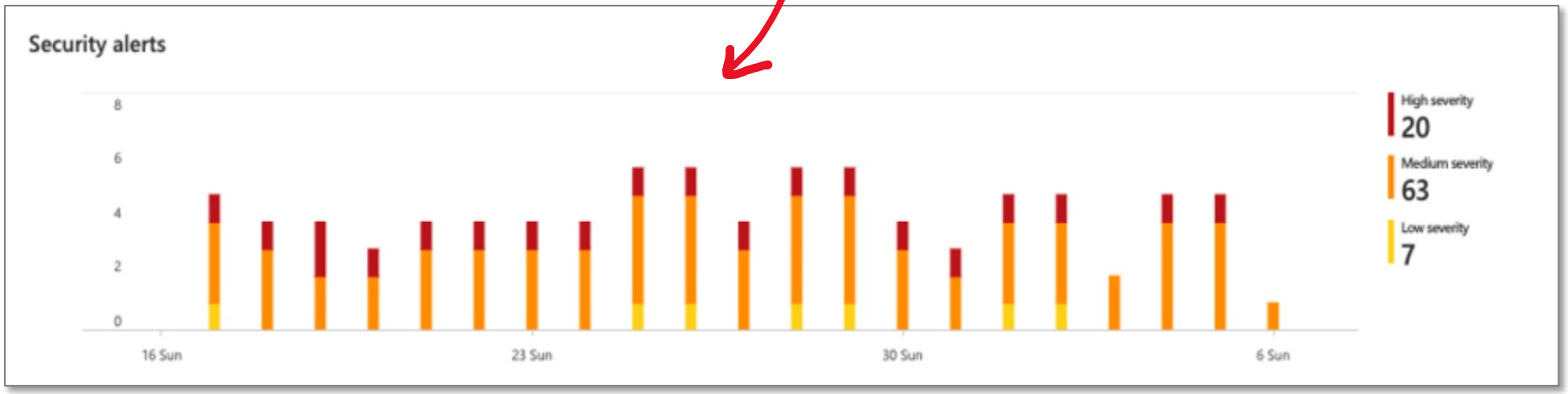
Azure Defender – Coverage

Coverage lets **see the resources types** that are in your subscription and eligible for protection by Azure Defender



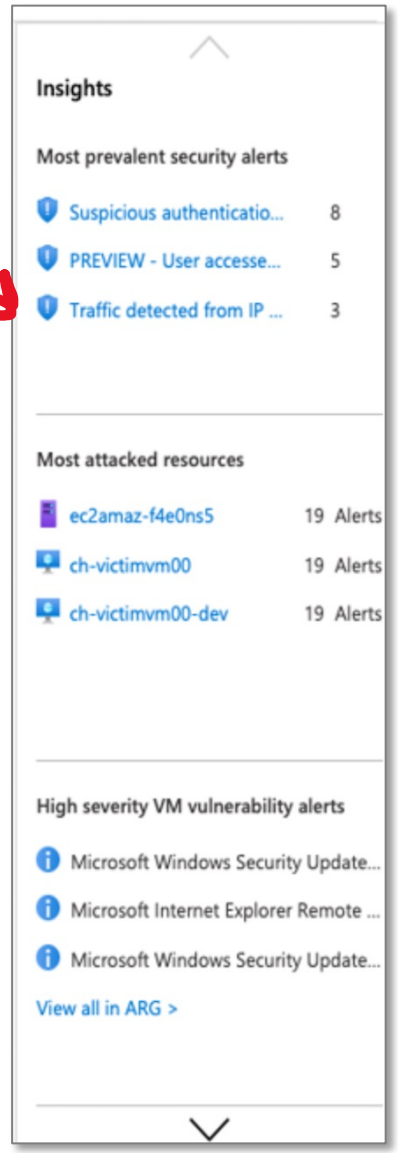
Azure Defender – Security Alerts

Security Alerts describe **details of the affected resources**, suggested **remediation** steps, and in some cases an option to trigger a logic app in response



Azure Defender – Insights

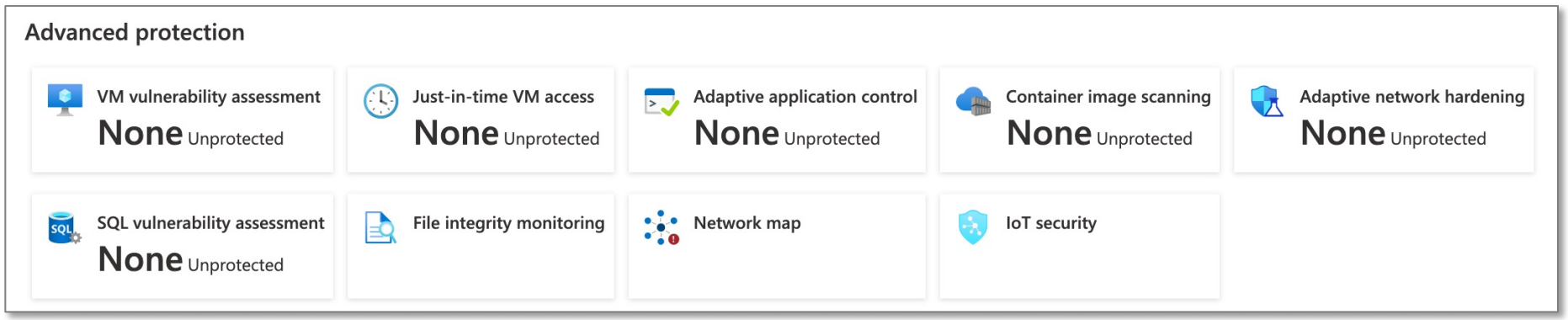
Insights is a **rolling pane of news**, suggested reading, and **high priority alerts** gives Security Center's insights into pressing security matters that are relevant to you and your subscription



Azure Defender – Advanced Protection

Advanced Protection within Defender are additional security features that is driven by analytics

- VM vulnerability assessment
- Just-in-time VM access
- Adaptative application control
- Container image scanning
- Adaptative network hardening
- SQL vulnerability assessment
- File integrity monitoring
- Network map
- IoT Security



Scope of Azure Defender

Azure Defender has **many plans** for specific Azure resources:

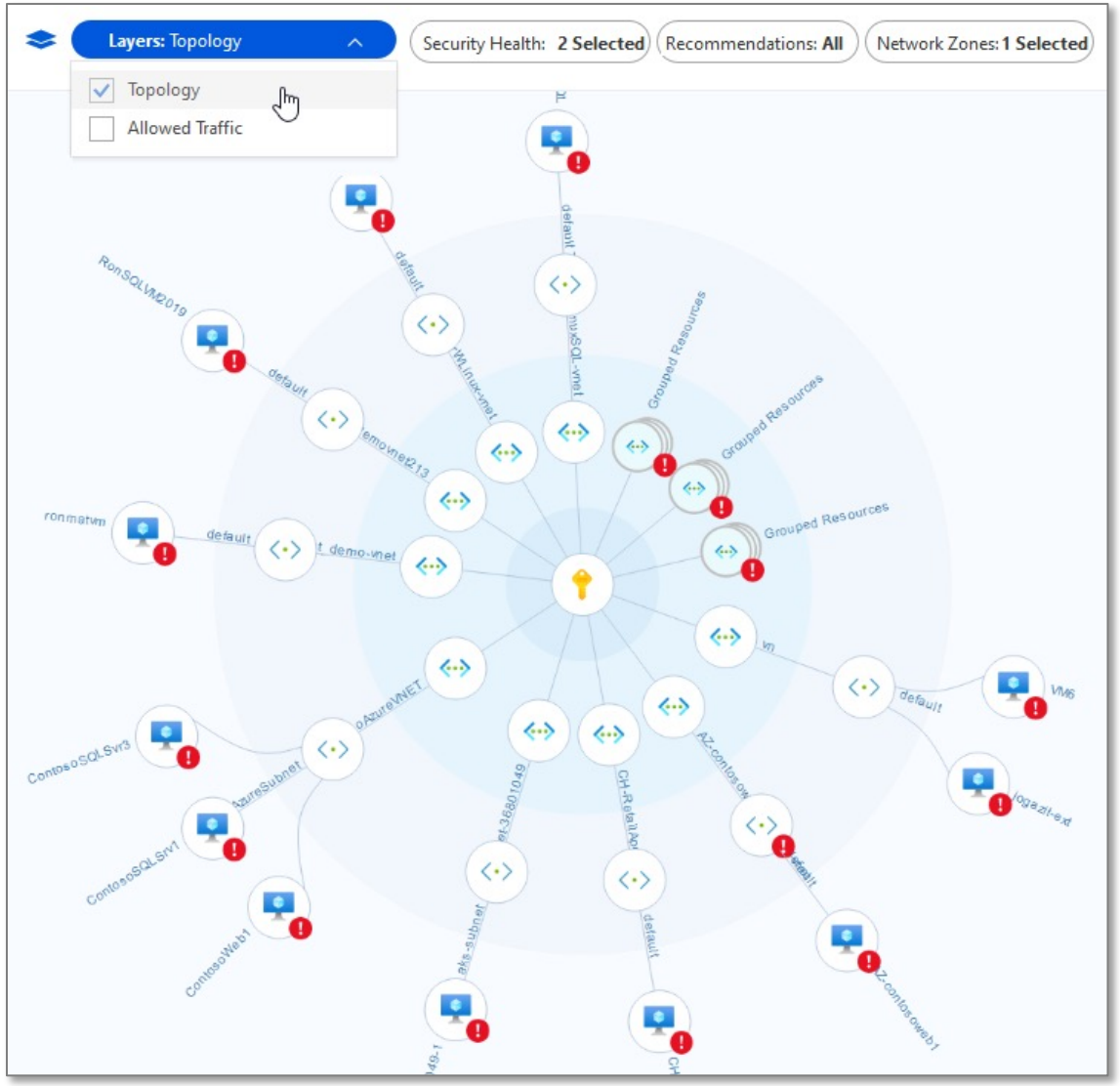
- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for container registries
- Azure Defender for Key Vault
- Azure Defender for Resource Manager
- Azure Defender for DNS
- Azure Defender for open-source relational databases

When you turn on Azure Defender **all plans are activated**

Azure Defender – Network Map

Network map provides a graphical view with security overlays giving you recommendations and insights for hardening your network resources

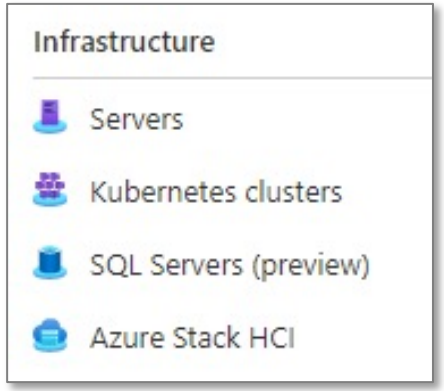
Using the map you can see the network topology of your Azure workloads, connections between your virtual machines and subnets, and the capability to drill down from the map into specific resources and the recommendations for those resources.



Azure Defender – Hybrid Cloud Protection

Azure Defender can protect virtual machines residing in other cloud service providers e.g. Amazon Web Services (AWS) and Google Cloud Platform (GCP) via **Azure Arc**

Azure Arc is a **control plane** that can manage **compute resources** across cloud service providers, on-premise and at the edge.



Azure Security Benchmark

What is a Security baseline?
A security baseline is a set of **minimum security controls** defined for:

- low-impact information system
- moderate-impact information system
- high-impact information system

Security baselines for Azure focus on cloud-centric control areas and these controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS)

The **Azure Security Benchmark (ASB)** is a security baseline for Azure.

benchmark is part of a set of holistic security guidance that also includes:

- Azure Cloud Adoption Framework
- Azure Well-Architected Framework
- Microsoft Security Best Practices

Azure Security Benchmark

The Azure Security Benchmark has the following controls (group of recommendations):

- Network security (NS)
- Identity Management (IM)
- Privileged Access (PA)
- Data Protection (DP)
- Asset Management (AM)
- Logging and Threat Detection (LT)
- Incident Response (IR)
- Posture and Vulnerability Management (PV)
- Endpoint Security (ES)
- Backup and Recovery (BR)
- Governance and Strategy (GS)

The Azure Security Benchmark can be downloaded as **Excel Spreadsheet**

A recommendation will have the following fields:

- Azure Control
- Azure ID
- Recommendation
- Guidance
- Responsibility
- Azure Security Monitoring Center
  - Whether the Azure Security Center monitors this control

Azure Security Benchmark

Generic Guidance

Ensure security teams are granted Security Reader permissions in your Azure tenant and subscriptions so they can monitor for security risks using Azure Security Center.

Depending on how security team responsibilities are structured, monitoring for security risks could be the responsibility of a central security team or a local team. That said, security insights and risks must always be aggregated centrally within an organization.

Security Reader permissions can be applied broadly to an entire tenant (Root Management Group) or scoped to management groups or specific subscriptions.

Note: Additional permissions might be required to get visibility into workloads and services.

Overview of Security Reader Role:
https://docs.microsoft.com/azure/role-based-access-control/built-in-roles#security-reader

Overview of Azure Management Groups:
https://docs.microsoft.com/azure/governance/management-groups/overview

Azure Control
Asset Management

Azure ID
AM-1

CIS Controls v7.1 ID(s)
1.1: Utilize an Active Discovery Tool
1.2: Use a Passive Asset Discovery Tool

NIST SP800-53 r4 ID(s)
CM-8: INFORMATION SYSTEM COMPONENT INVENTORY
PM-5: INFORMATION SYSTEM INVENTORY

Benchmark Recommendation
Ensure security team has visibility into risks for assets

Responsibility
Customer

Customer Stakeholders
Infrastructure and endpoint security:
/organize/cloud-security-infrastructure-endpoint (cloud-adoption-framework)
Security Compliance Management:
organize/cloud-security-compliance-management (cloud-adoption-framework)

Azure Sentinel

Azure Sentinel is a scalable, cloud-native:

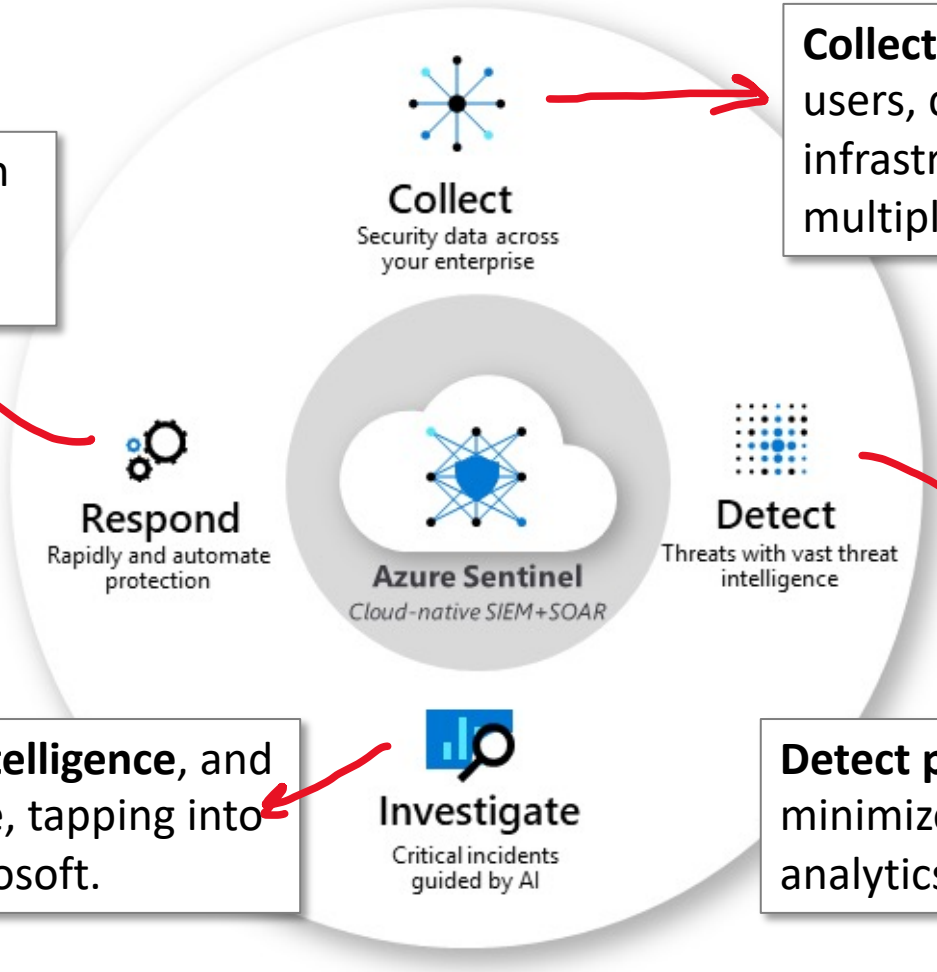
- **security information event management (SIEM)**
- **security orchestration automated response (SOAR)**

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for:

- alert detection
- threat visibility
- proactive hunting
- threat response

Azure Sentinel

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.



Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

Azure Sentinel – Data Sources

Azure Sentinel comes with a number of connectors for Microsoft solutions:

- Microsoft 365 Defender
- Office 365
- Azure AD
- Microsoft Defender for Identity
- Microsoft Cloud App Security

Use common event formats:

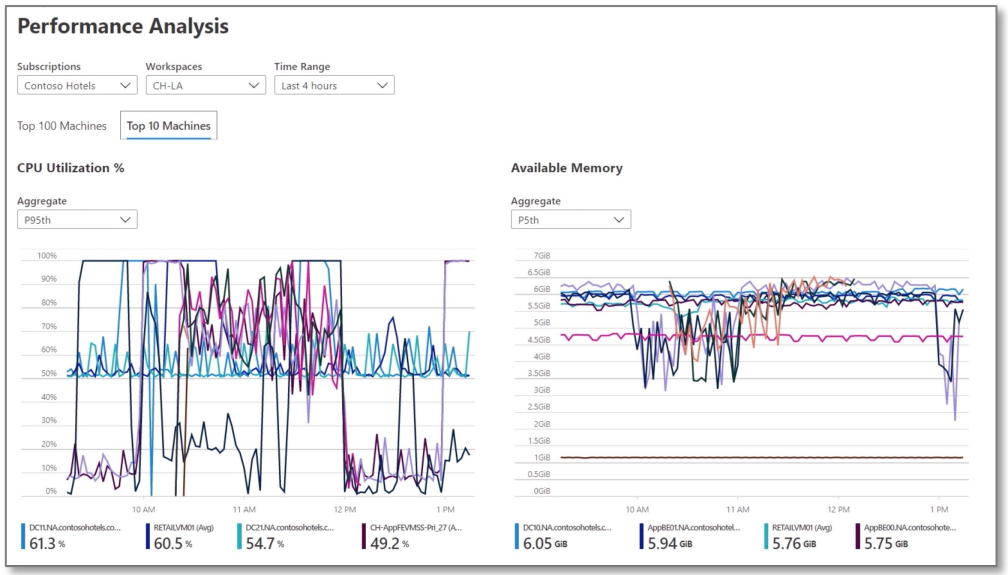
- Syslog
- REST-API
- Windows Event Logs
- Common Event Format (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII)

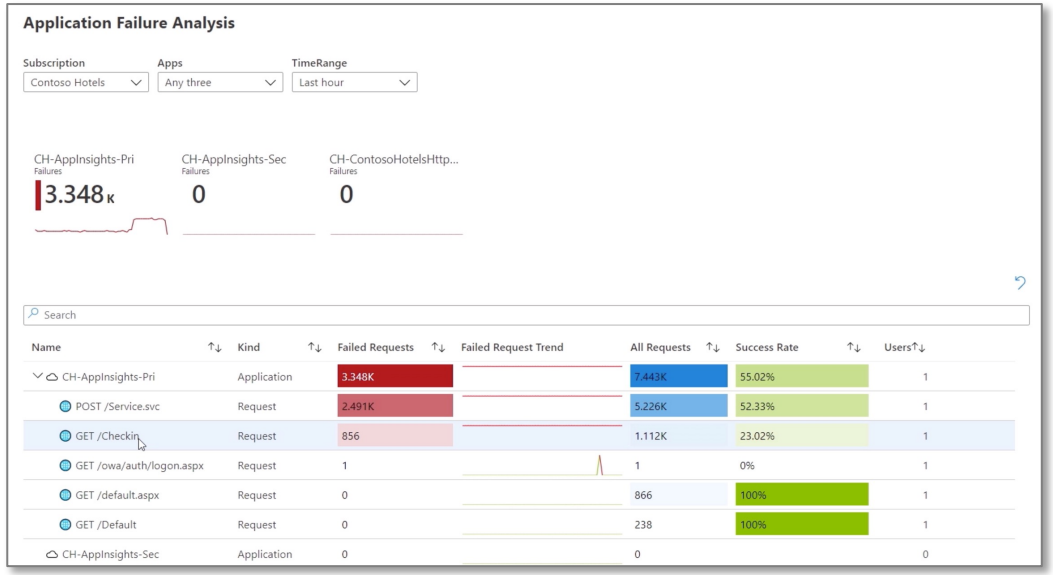
Azure Sentinel - Azure Workbooks

From Azure Sentinel you can create Azure Monitor Workbooks

Workbooks provide a flexible **canvas for data analysis** and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences.

It tells a **story** about the performance and availability about your applications and services.



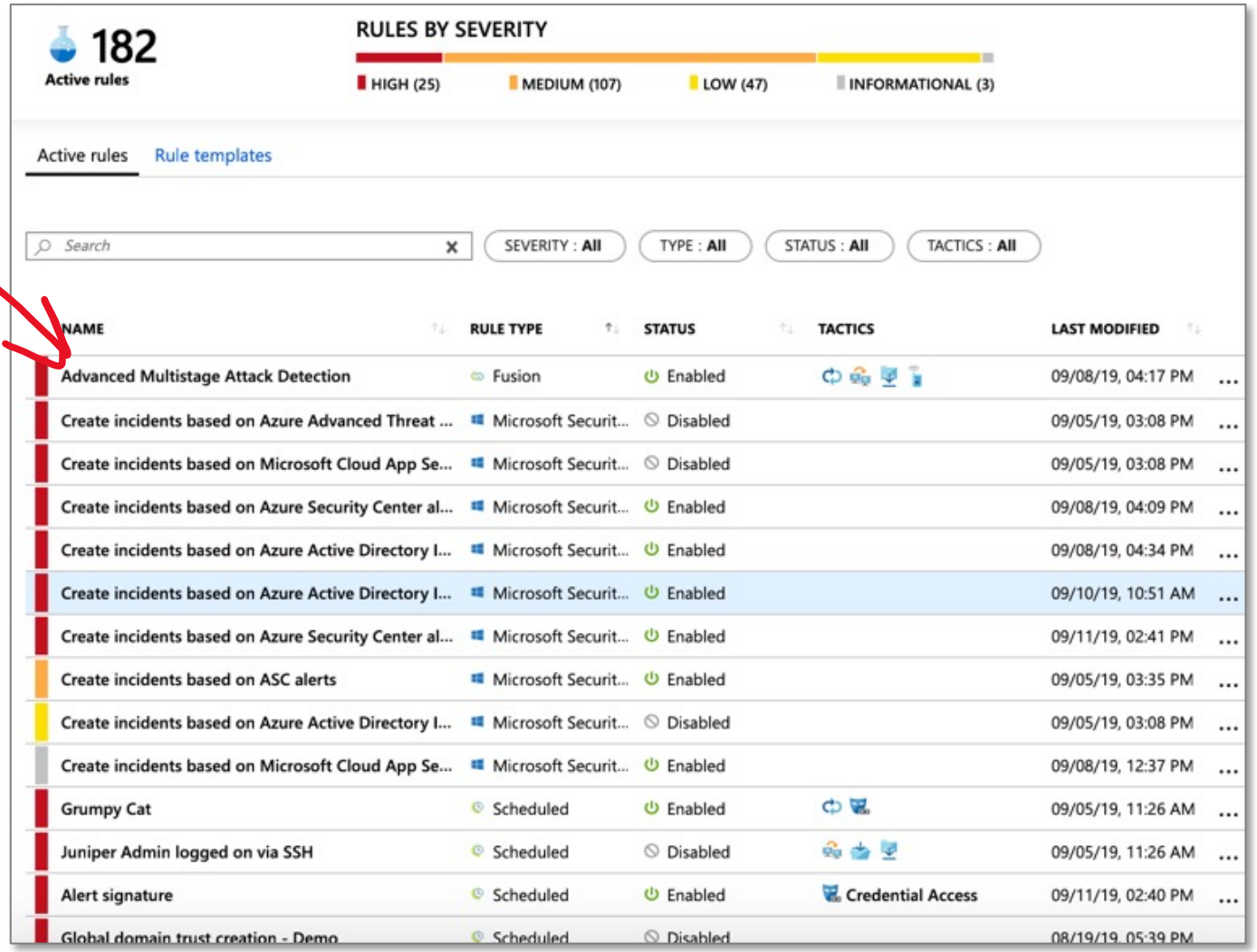


Workbooks are temporary workspaces to define a document-like format with visualization intertwined to help investigate and discuss performance.

Azure Sentinel – Analytics

Azure 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

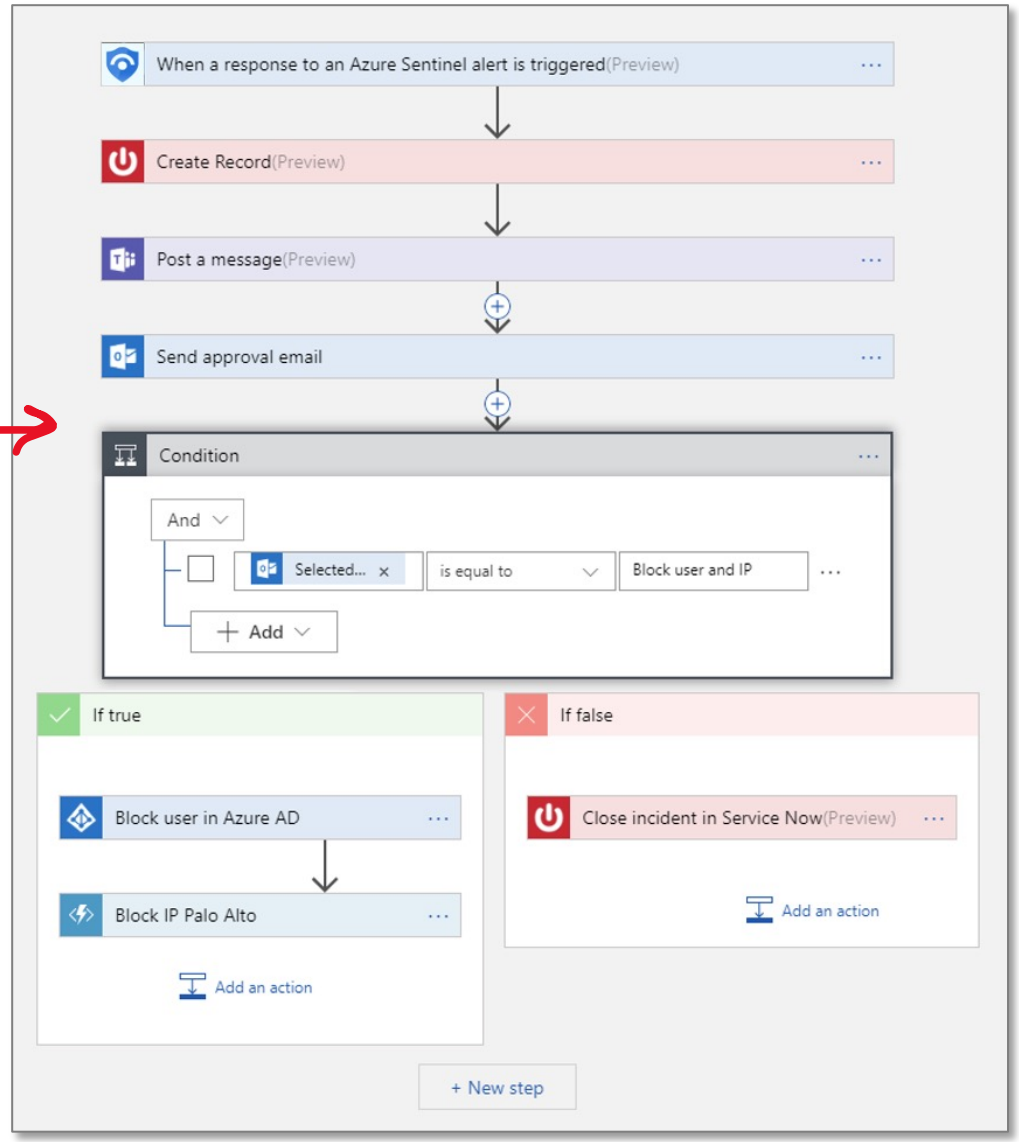


Azure Sentinel – Automation and Orchestration

Azure Sentinel's automation and orchestration solution provides a highly-extensible architecture that enables scalable automation as new technologies and threats emerge

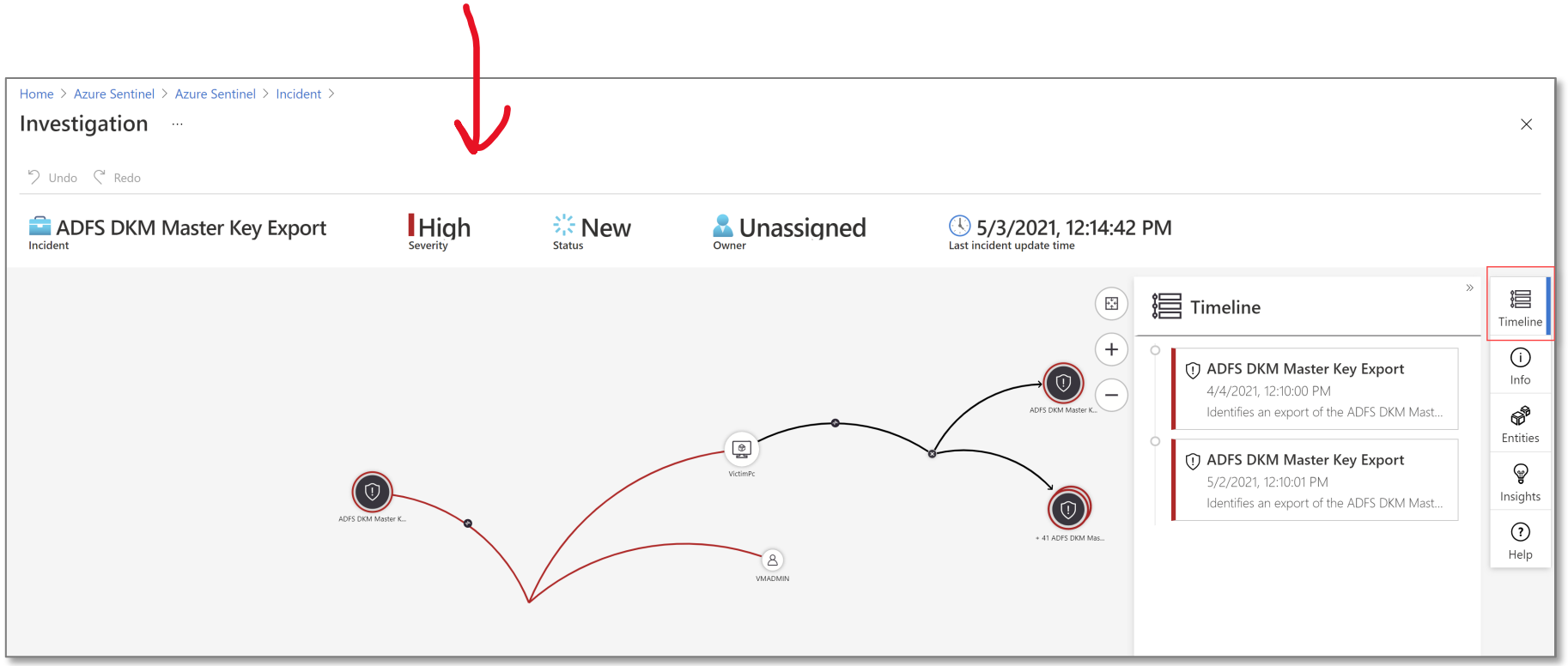
Built on the foundation of **Azure Logic Apps**

include 200+ connectors for services



Azure Sentinel – Investigation

Azure Sentinel deep **investigation tools** help you to understand the scope and find the root cause, of a potential security threat. You can choose an entity on the interactive graph to ask interesting questions for a specific entity, and drill down into that entity and its connections to get to the root cause of the threat.

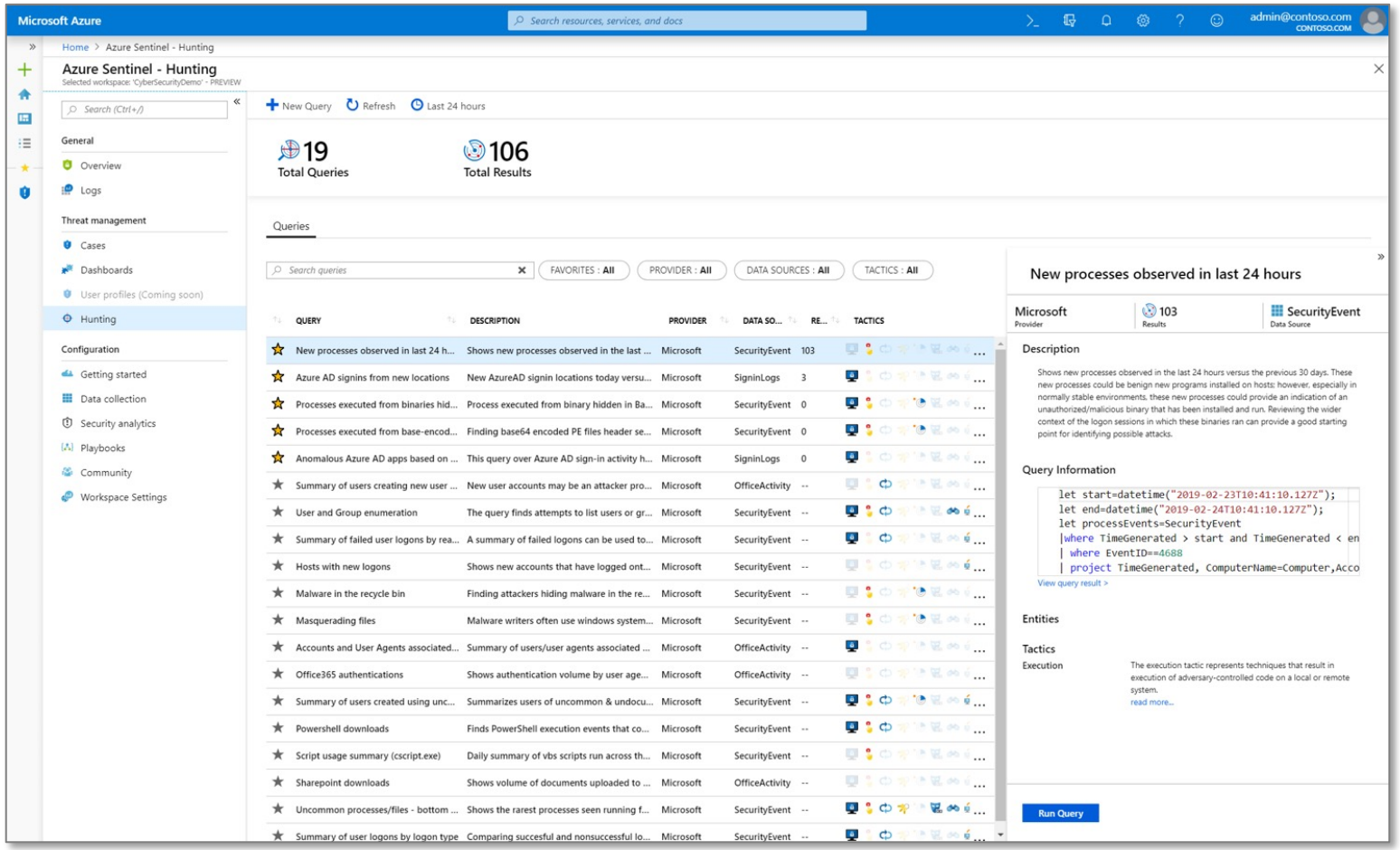


Azure Sentinel – Hunting

Azure Sentinel's powerful **hunting search-and-query tools**, based on the **MITRE framework**, which enable you 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 create bookmarks for interesting events, enabling you to return to them later, share them with others, and group them with other correlating events to create a compelling incident for investigation.



Azure Sentinel – Pricing

Azure Sentinel has **two different pricing models**

Capacity Reservations:
billed a fixed fee based on the selected tier, enabling a predictable total cost for Azure Sentinel.

Pay-As-You-Go:
billed per gigabyte (GB) for the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace.

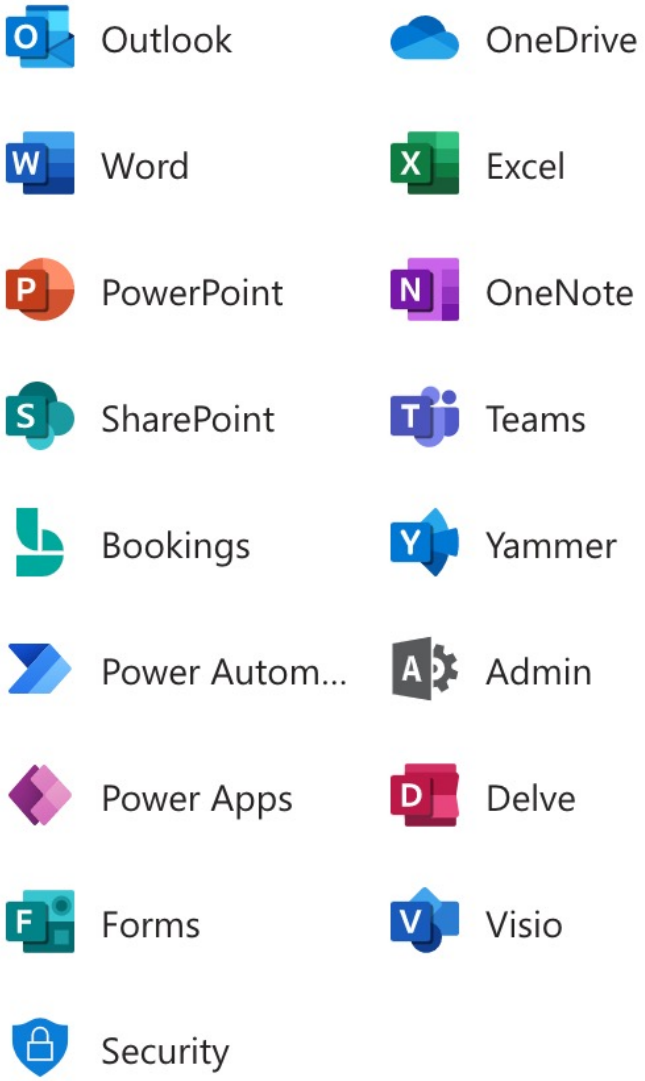
Microsoft 365

Microsoft 365 *(formally Office 365)* is a **suite of business software** packaged a as SaaS offering

You access Microsoft 365 via **https://portal.office.com**

Most notable services:

- SharePoint — site collaboration, shared company document drive
- Outlook — email service
- Word — word processor
- PowerPoint — Slide shows
- Excel — spreadsheets
- Teams —collaboration app for your organization *(similar to Slack)*



Microsoft 365 Defender

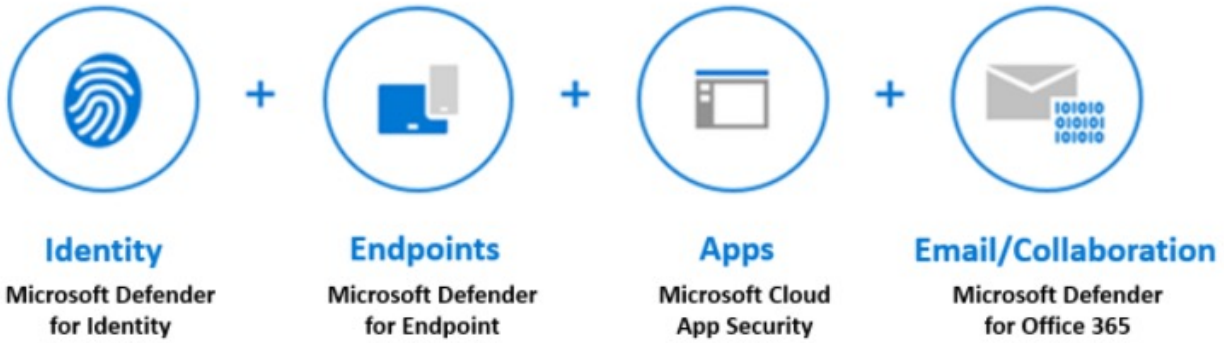
Microsoft 365 Defender is a **unified pre- and post-breach enterprise defense suite** that natively coordinates

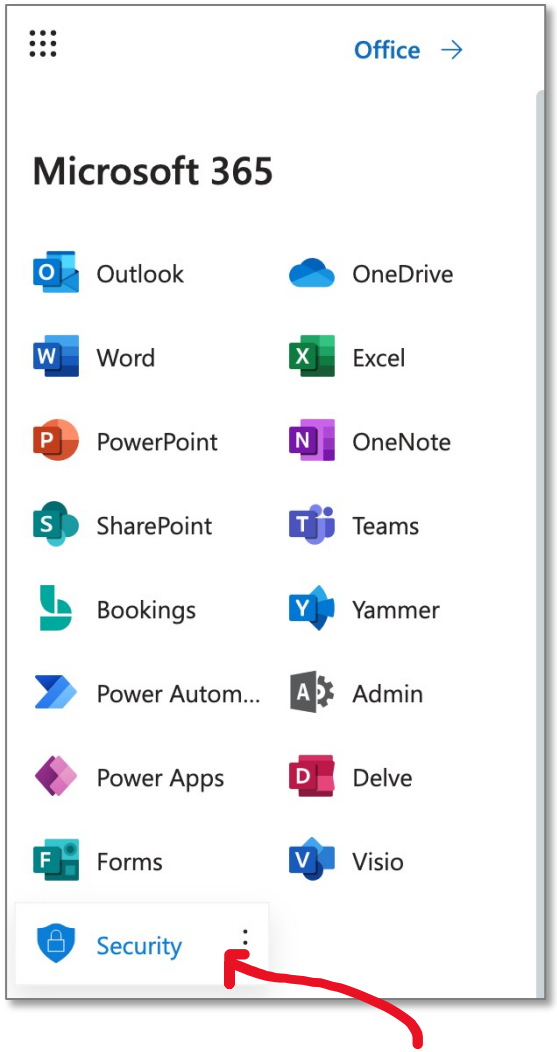
- responses: **detection, prevention, investigation**
- across: **endpoints, identities, email, applications**

to provide integrated protection against sophisticated attacks.

Microsoft Defender is composed of the following services:

- Microsoft Secure Score
- **Microsoft Defender for Endpoint**
- **Microsoft Defender for Office 365**
- **Microsoft Defender for Identity**
- **Microsoft Cloud App Security**



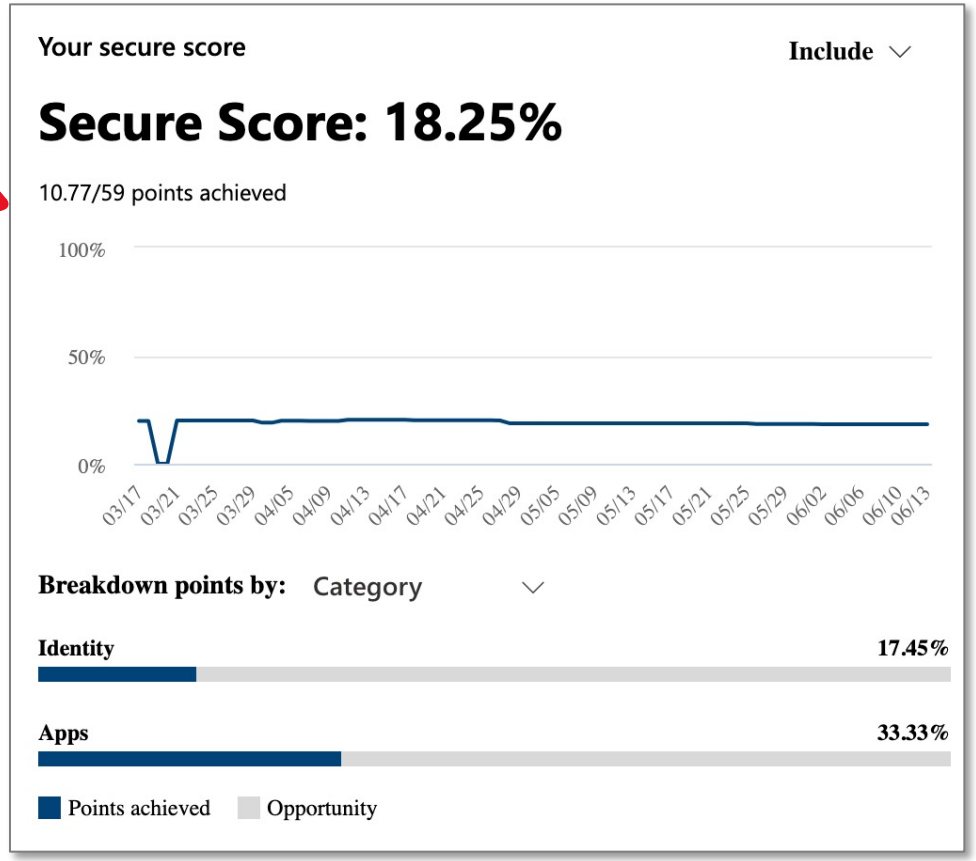


founder under **Security**

Microsoft 365 Defender – Secure Score

Microsoft Secure Score is a representation of your organization's **security posture**, and your opportunity to improve it via **Improvement Actions**

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for ...	+15.25%	0.77/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on sign-in risk policy	+11.86%	0/7
5	Turn on user risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Restrict anonymous users from joining meetings	+1.69%	0/1



Microsoft 365 – Endpoints

Microsoft 365 Endpoints are the set of destination IP addresses, DNS domain names, and URLs for Microsoft 365 traffic on the Internet

To optimize performance to Microsoft 365 cloud-based services, these endpoints need special handling by your client browsers and the devices in your edge network. These devices include firewalls, SSL Break and Inspect and packet inspection devices, and data loss prevention systems.

```
outlook.office.com, outlook.office365.com
13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22,
23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14,
131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22,
204.79.197.215/32, 2603:1006::/40, 2603:1016::/36,
2603:1026::/36, 2603:1036::/36, 2603:1046::/36,
2603:1056::/36, 2603:1096::/38, 2603:1096:400::/40,
2603:1096:600::/40, 2603:1096:a00::/39, 2603:1096:c00::/40,
2603:10a6:200::/40, 2603:10a6:400::/40, 2603:10a6:600::/40,
2603:10a6:800::/40, 2603:10d6:200::/40, 2620:1ec:4::152/128,
2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128,
2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46,
2620:1ec:900::/46, 2620:1ec:a92::152/128,
2620:1ec:a92::153/128, 2a01:111:f400::/48
```

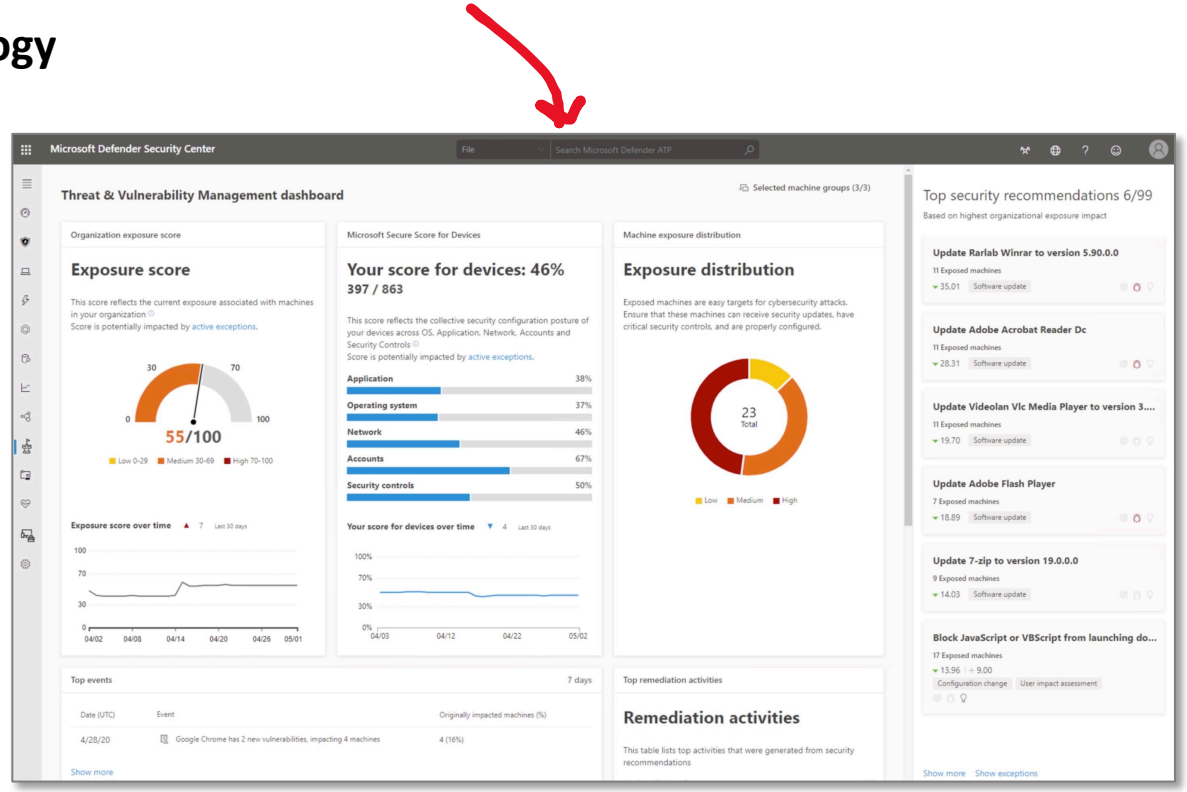
endpoints are grouped into four service areas:

- **Exchange Online**
- SharePoint Online and OneDrive for Business
- Skype for Business Online and Microsoft Teams
- Microsoft 365 Common and Office Online

Microsoft 365 Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks **prevent, detect, investigate, and respond** to **advanced threats**

Defender for Endpoint uses the **following combination of technology** built into **Windows 10 and Microsoft cloud service**



Endpoint behavioral sensors
Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint

Cloud security analytics
Leveraging big-data, device-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.

Threat intelligence
Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data

Microsoft 365 – Security Reports

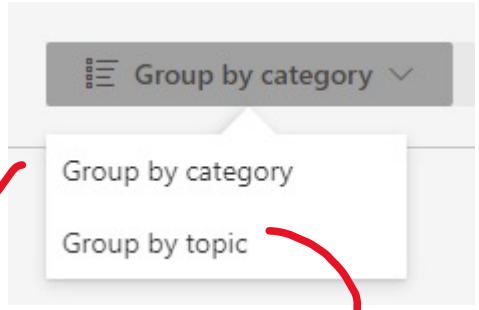
Security report is **a general security dashboard** about **security trends for M365 Identities, devices and Apps**

Information is organized as “cards” on the dashboard

Identities
- **Users at risk**
- Global admins

Devices
- Devices at risk
- Device compliance
- Devices with active malware
- Types of malware on devices
- Malware on devices
- Devices with malware detection
- Users with malware detections

Apps
- Risk levels

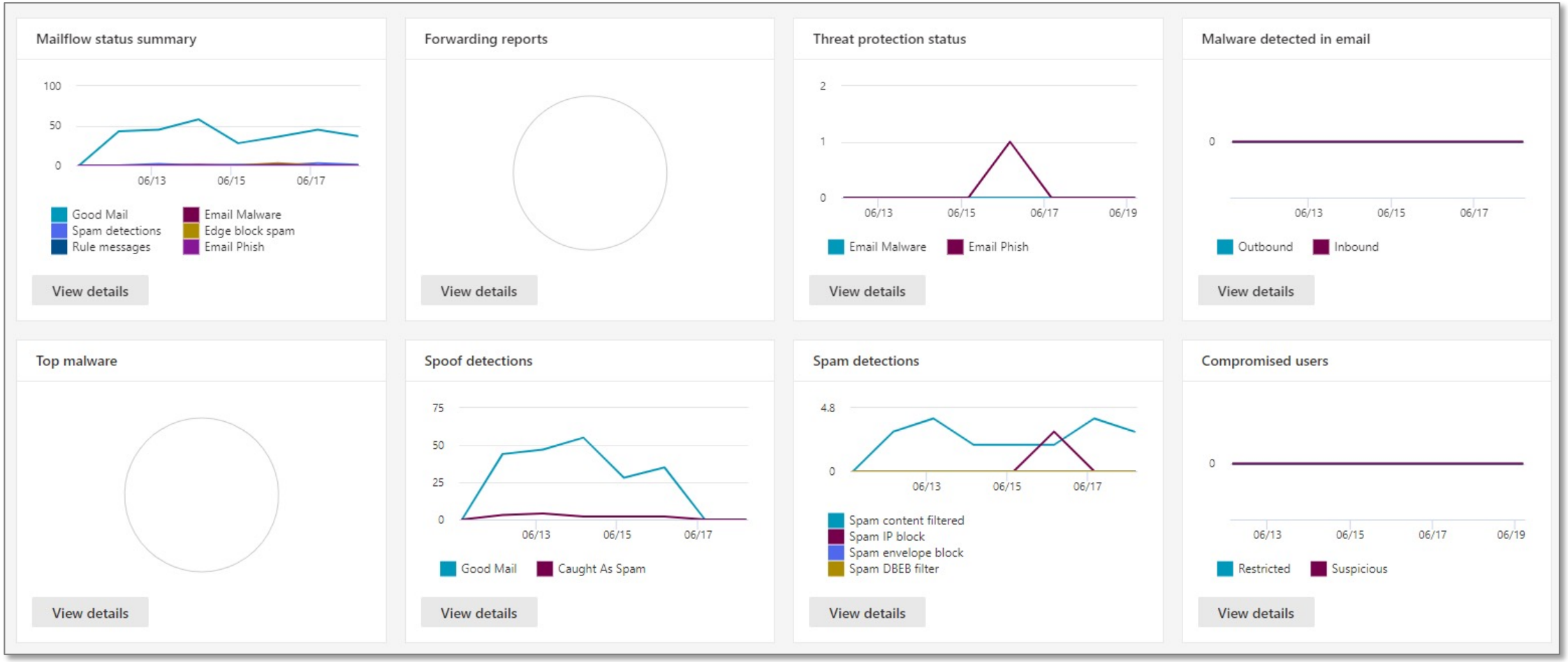


Group by **Category**:
- Identities
- Devices
- Apps

Group by **Topic**:
- Risk
- Detection trends
- Configuration and health

Microsoft 365 – Email Collaboration Reports

Security Reports for Office 365 Exchange (mail server)



Microsoft 365 Defender for Identity

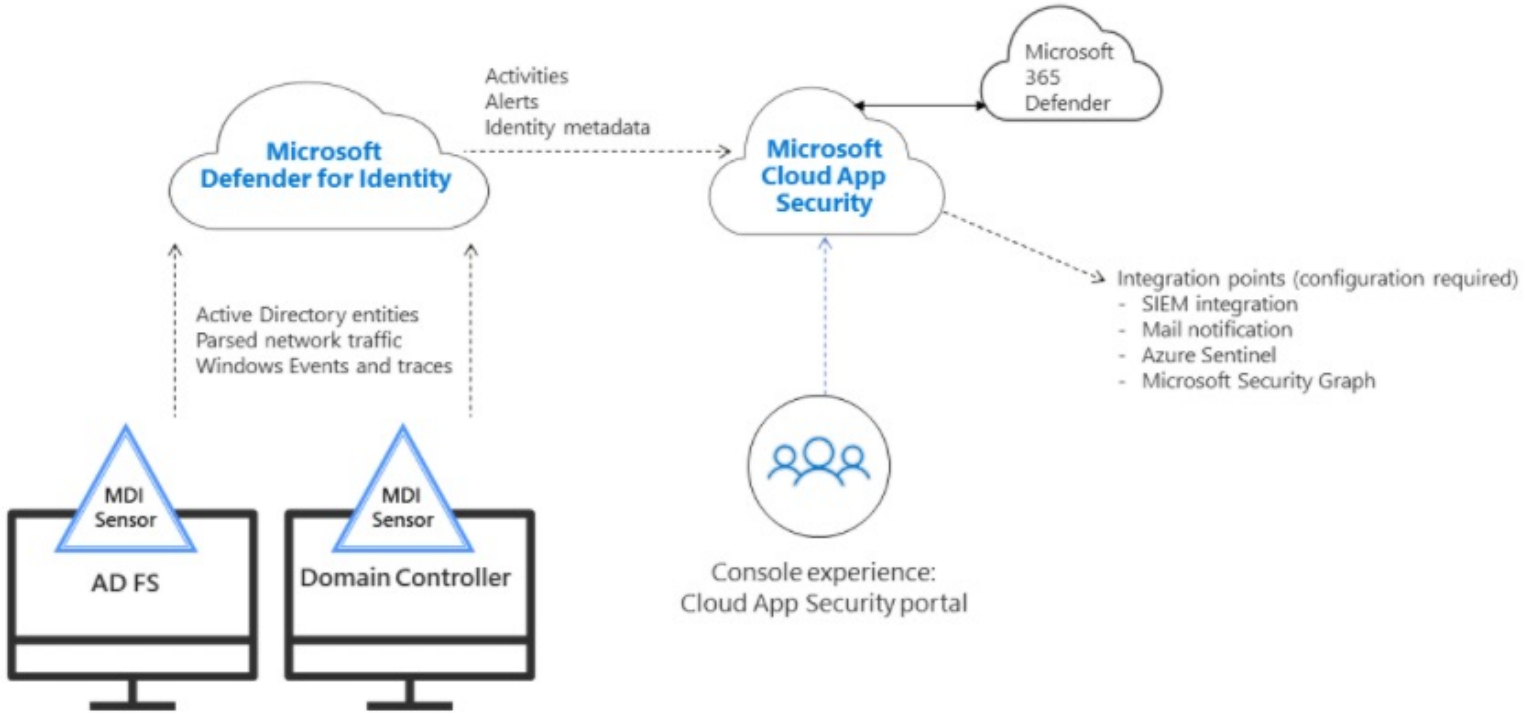
Microsoft 365 Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals **to identify, detect, and investigate** advanced threats, compromised identities, and malicious insider actions directed at your organization

detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Microsoft 365 Defender for Identity

Microsoft Defender for Identity monitors your domain controllers by capturing and parsing network traffic and leveraging Windows events directly from your domain controllers, then analyzes the data for attacks and threats.



Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Defender for Identity learns about your network, enables detection of anomalies, and warns you of suspicious activities.

Microsoft 365 Defender for Office 365

Microsoft Defender for Office 365 protects against advanced threats by email messages, links (URLs), and Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients

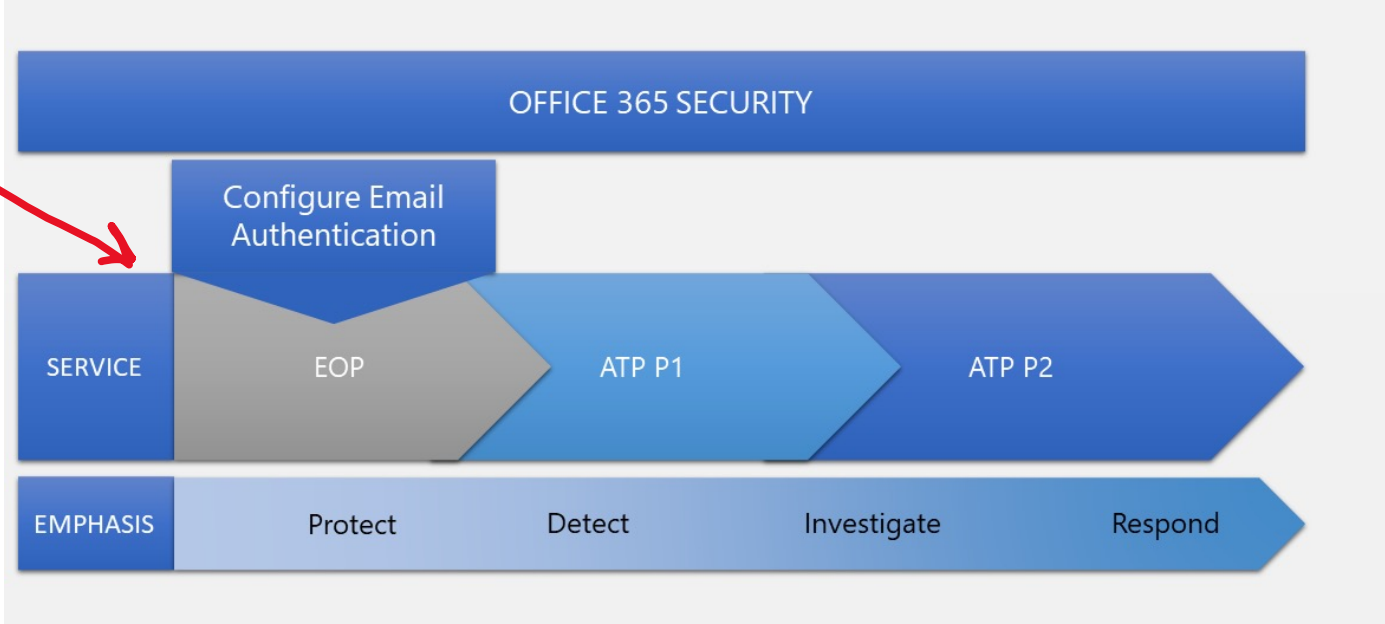
Protection is provided via:

- Reports
- Threat Investigation
- Thread Response
- Threat protection policies

There three available subscriptions:

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365 Plan 1 (Defender for Office P1)
- Microsoft Defender for Office 365 Plan 2 (Defender for Office P2)

Office 365 security builds on the **core protections** offered by EOP.
EOP is present in any subscription where Exchange Online mailboxes can be found



Microsoft 365 Defender for Office 365

Exchange Online Protection (EOP)

- cloud-based filtering service that protects your organization against spam, malware, and other email threats

Defender for Office P1

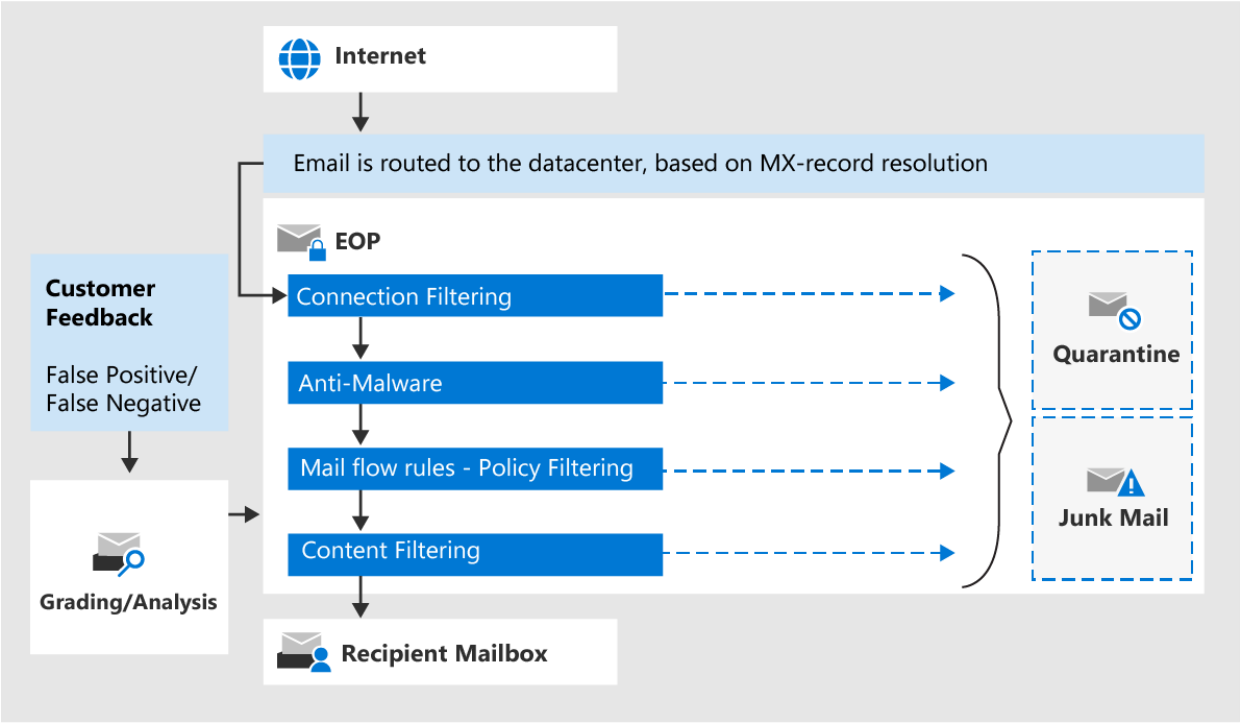
- **Safe Attachments**: Checks email attachments for malicious content
- **Safe Links**: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked
- **Protection for SharePoint, OneDrive, and Microsoft Teams**:
  - identifies and blocks malicious files in team 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

Defender for Office P2

- *Includes Defender Office 1 features*
- **Threat Trackers**: latest intelligence on cybersecurity issues, take countermeasures before an actual threat.
- **Threat Explorer**: real-time report that allows you to identify and analyze recent threats.
- **Automated investigation and response (AIR)**:
  - a set of security playbooks that can be launched automatically
    - start an automated investigation, provide detailed results, recommend actions security team can approve
- **Attack Simulator**: run realistic attack scenarios in your organization to identify vulnerabilities.

Exchange Online Protection

Exchange Online Protection (EOP) is cloud-based filtering service that protects your organization **against spam, malware, and other email threats**



EOP features:

- Anti-malware
- Inbound anti-spam
- Outbound anti-spam
- Connection filtering
- Anti-phishing
- Anti-spoofing protection
- Zero-hour auto purge (ZAP) for delivered malware, spam, and phishing messages
- Preset security policies
- Tenant Allow/Block List
- Allow/Block lists for message senders
- Directory Based Edge Blocking (DBEB)
- Mail flow rules
- Accepted domains
- Message training
- And *more (seriously! there is a lot of features)*

Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS) is **a Cloud Access Security Broker (CASB)** that sits **between the user and the cloud service provider** to gatekeep access in real-time to cloud resources.

MCAS is built on-top of the **4 principles** of the **Microsoft Cloud App Security Framework**:

1. Discover and control the use of Shadow IT
Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

2**. Protect your sensitive information anywhere in the cloud**
Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.

3. 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 the risk to your organization.

4. Assess the compliance of your cloud apps
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 Cloud App Security

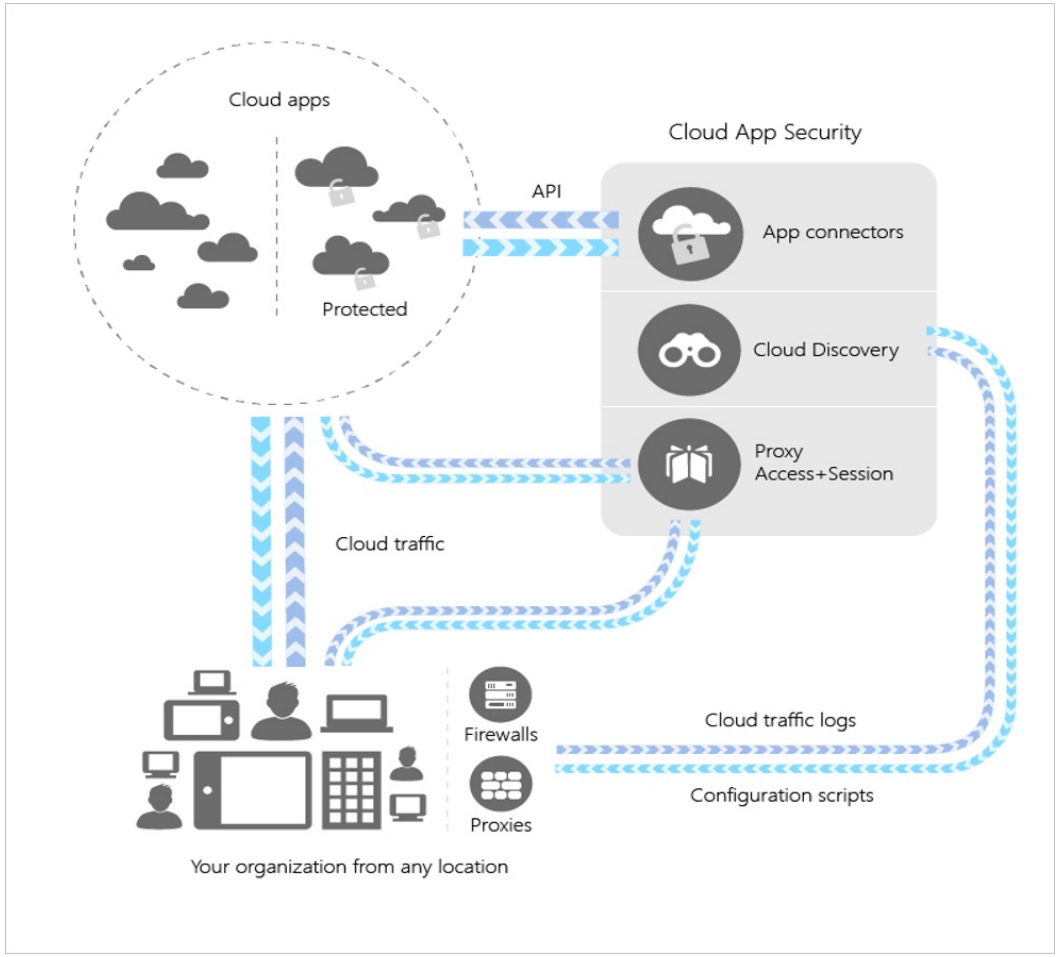
Cloud App Security integrates visibility with your cloud by:

- Using Cloud Discovery to map and identify your cloud environment and the cloud apps your organization is using.
- Sanctioning and unsanctioning apps in your cloud.
- Using easy-to-deploy app connectors that take advantage of provider APIs, for visibility and governance of apps that you connect to.
- Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps.
- Helping you have continuous control by setting, and then continually fine-tuning, policies.

Office 365 Cloud App Security is a subset of Microsoft Cloud App Security

- threat detection based on user activity logs, discovery of Shadow IT for apps with similar functionality to Office 365 offerings

Azure AD Premium P1 includes Azure Active Directory Cloud App Discovery at no extra cost.



Microsoft Endpoint Manager

Microsoft Intune and **Configuration Manager** was merged into a single service called **Microsoft Endpoint Manager**

Microsoft Intune
Used for managing the security of mobile devices

Configuration Manager
Used to manage desktops, servers and laptops

The services are managed via the **Microsoft Endpoint Manager Admin Center**
https://endpoint.microsoft.com

Microsoft Intune

Micorosft Intune is a **mobile device and mobile application manager (MDM and MAM)** found within Microsoft Endpoint Manager

Microsoft Intune can:

- Manage devices
- Manage security baselines
- Use policies to manage device security
- Use device compliance policy
- Configure conditional access
- Integration with Microsoft Defender for Endpoint
- Role-based access controls

Microsoft Intune integrates with:

- Azure AD
- Mobile Threat Defenders
- ADMX templates
- Win32
- Custom LOB apps
- And more!

Microsoft Intune can be used to manage on-premise infrastructure via **Intune connectors**

- Intune Connector for Active Directory
- Intune certificate connector

Regulatory Compliance

What is compliance?
conforming to a rule, such as a **specification, policy, standard or law**

What is regulatory compliance?
an organization that take effort to comply with relevant **laws, policies, and regulations**

Regulatory compliance can vary at the following levels:

- federal — Canada
- state (provincial) — Ontario
- political and economic union — European Union (EU)
- international organization
  - International Organization of Standards (ISO)

Why Regulatory Compliance?
Governments want to protect its citizens data that that is collected by companies and organization

What are Compliance controls?
internal control mechanisms that need to be in place to detect, prevent, and correct compliance issues eg.

- Published Standards and Policies
- Documented Procedures
- Training
- Monitoring
- Internal audit

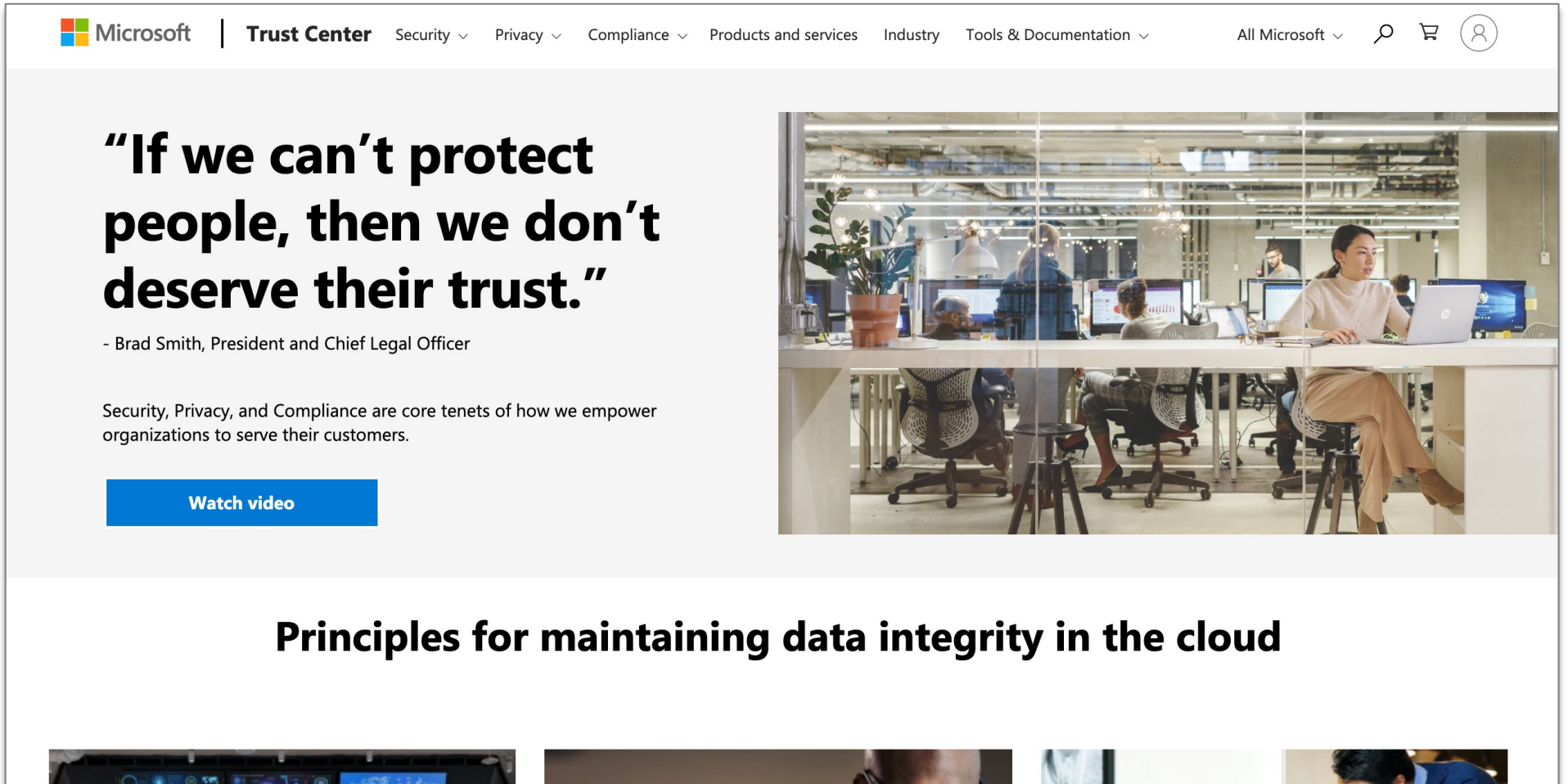
Regulatory Compliance

Examples of measures that regulatory compliance can enforce:

- citizens the right to access their data at any time.
- citizens the right to correct or delete data if needed.
- retention periods that for the a minimum or maximum time data should be stored.
- enabling governments and regulatory agencies the right to access and examine data when necessary
- defining rules for what data can be processed and how that should be done.

Azure Trust Center

A public-facing website portal providing easy access to **privacy** and **security** and **regulatory compliance** information.



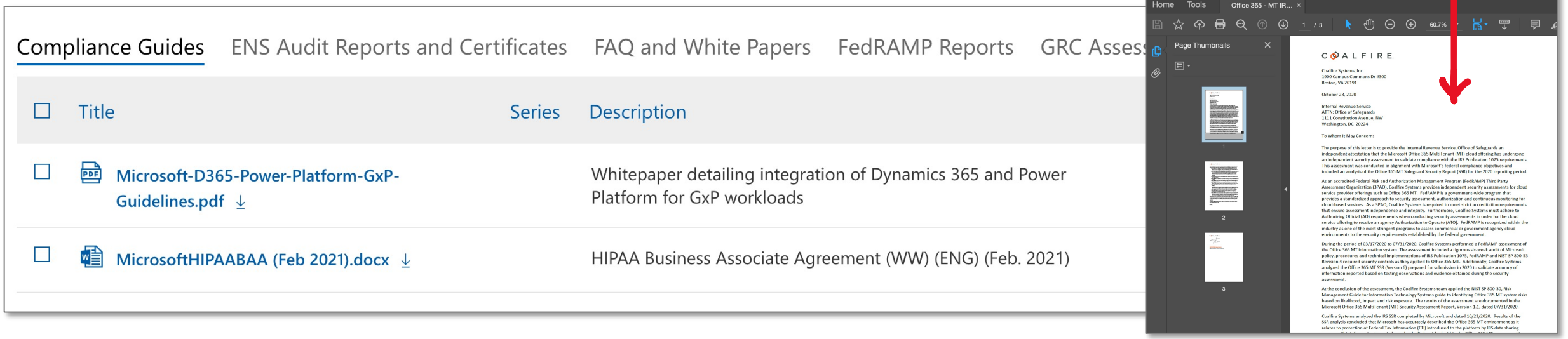
Service Trust Provider – Audit Reports

Audit Reports independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements

Audit reports for:

- International Organization for Standardization (ISO)
- Service Organization Controls (SOC)
- National Institute of Standards and Technology (NIST)
- Federal Risk and Authorization Management Program (FedRAMP)
- General Data Protection Regulation (GDPR)

Downloadable PDFs



Compliance Manager

At-a-glance summary of the shared responsibility model for Microsoft and your Organization

- Microsoft Trust Center – Compliance Manager (Classic)
- M365 Compliance Center – Compliance Manger

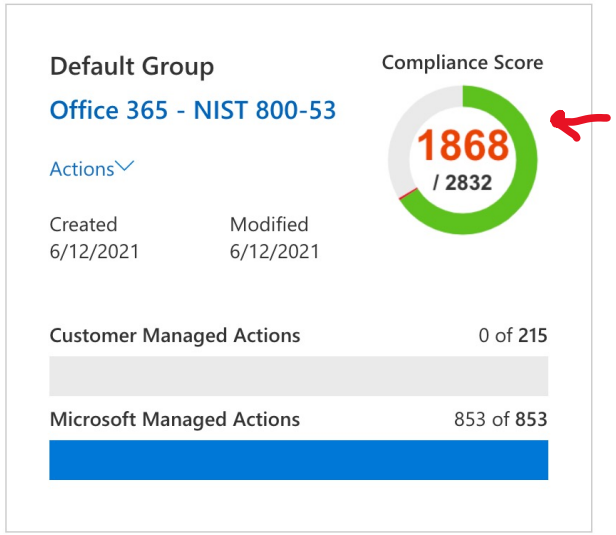
Risk assessment workflow and management tools
provide task assignment and verification to help Governance, Risk & Compliance teams and IT departments work together to streamline internal compliance activities.

Intelligent tracking
understands common and similar compliance activities across multiple standards and regulations to reduce your organizations costs and efforts from regulation to audit by applying a single activity to multiple Assessments or controls

Each assessed control will be labeled:

- Preventive, Detective, or Corrective and
- Mandatory or Discretionary

Assessments for:
Office 365 – GDPR
Office 365 - NIST 800-53
Office 365 - ISO 27001:2013
Azure – GDPR
Azure - ISO 27018:2014
Azure - ISO 27001:2013
HIPPA



Compliance score
figure out what actions you can take to improve your organization's compliance posture.

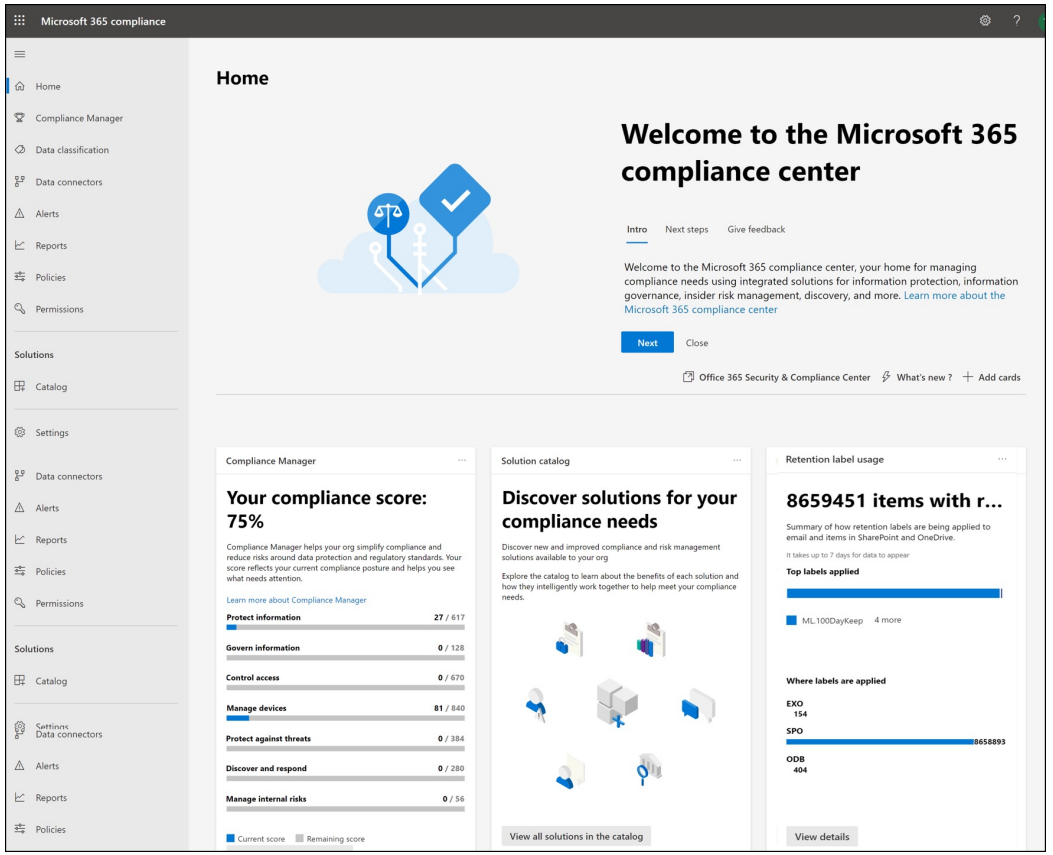
Service Trust Provider – Compliance Manager

Clicking into an assessment will give you a detailed list of actionable controls

Microsoft 365 Compliance Center

Microsoft 365 compliance center provides easy access to the data and tools you need to manage to your organization's compliance needs.

Access the Compliance Center at compliance.microsoft.com



Features of M365 Compliance Center

- Compliance Score
- Audits
- Activity Alerts
- Solution Catalog
- Data Classification
- eDiscovery
- Insider Risk Management
- Records Management

The following roles have access to compliance center:

- Global administrator
- Compliance administrator
- Compliance data administrator

Compliance Programs

Criminal Justice Information Services (CJIS)
Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.

cloud CSA security alliance®

Cloud Security Alliance (CSA) STAR Certification
Independent third-party assessment of a cloud provider's security posture

General Data Protection Regulation (GDPR)
A European privacy law. Imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

EU Model Clauses
Contractual guarantees around transfers of personal data outside of the EU

Compliance Programs

Health Insurance Portability and Accountability Act (HIPAA).
US federal law that regulates patient Protected Health Information

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27018.
Code of practice, covering the processing of personal information by cloud service providers.

Multi-Tier Cloud Security (MTCS) Singapore.
Operational Singapore security management Standard. A common standard that cloud service providers (CSPs) can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services.

Service Organization Controls (SOC) 1, 2, and 3.
independent third-party examination reports that demonstrate how the company achieves key compliance controls and objectives

Compliance Programs

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
Voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks.

UK Government G-Cloud.
Cloud computing certification for services used by government entities in the United Kingdom

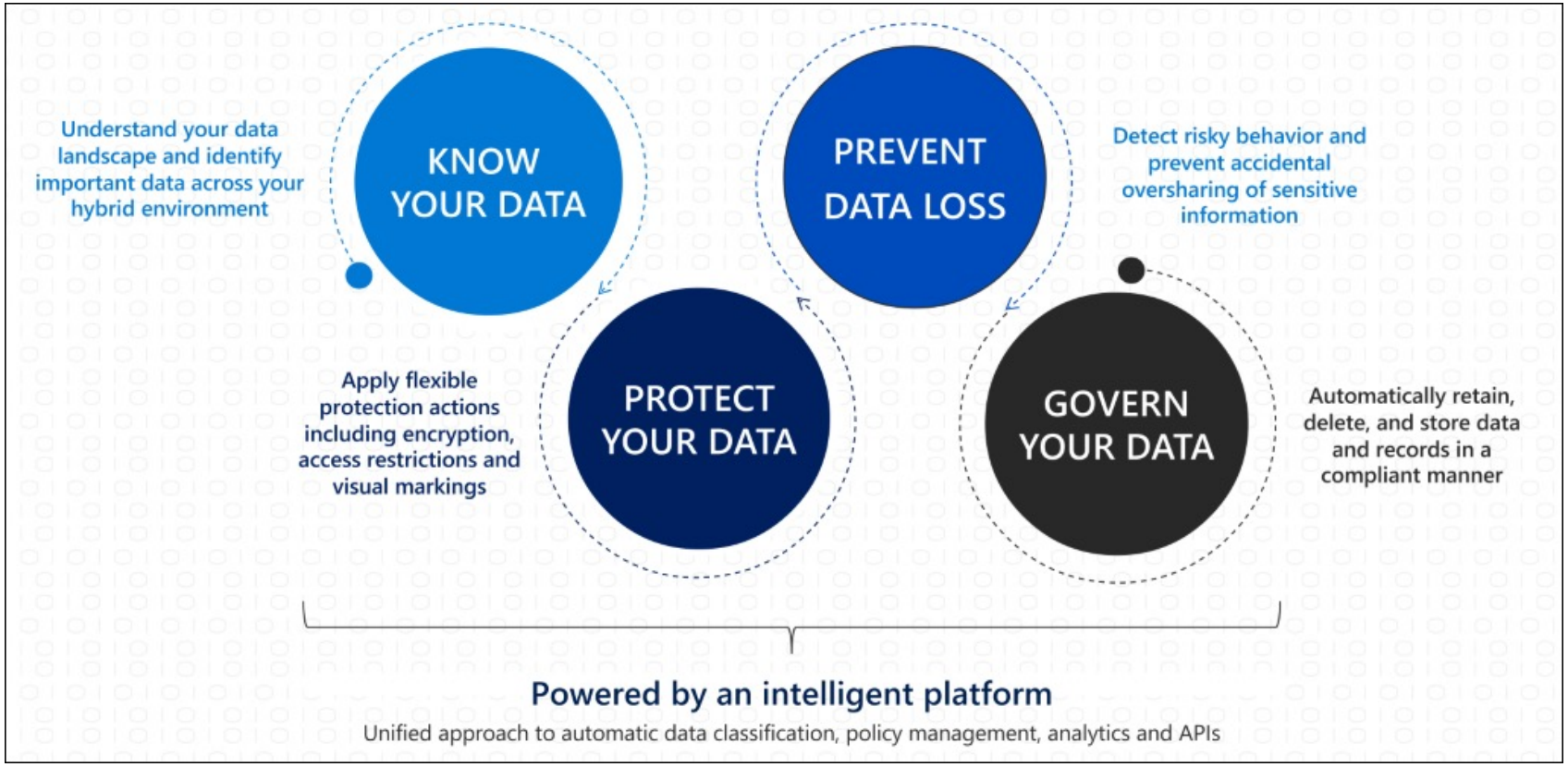
Federal Information Processing Standard (FIPS) 140-2
US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

Microsoft Information Protection

Microsoft Information Protection (MIP) is a collection of features within M365 Compliance to help **you discover, classify, and protect** sensitive information wherever it lives or travels.

MIP capabilities:

- Know your data
- Protect your data
- Prevent Data Loss
- Govern your Data*
  - GIP



MIP – Know your data

Know your data

Understand your **data landscape** and identify important data across your hybrid environment

Sensitive information types

Identifies sensitive data by using **built-in or custom regular expressions** or a function. Corroborative evidence includes keywords, confidence levels, and proximity.

- Built-in sensitive labels

Trainable classifiers

Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.

- Trainable classifiers

Data classification

A **graphical identification of items** in your organization that have a sensitivity label, a retention label, or have been classified. You can also use this information to gain insights into the actions that your users are taking on these items.

- Content explorer
- Activity explorer

MIP – Protect your data

Protect your data

apply **flexible protection** actions that include encryption, access restrictions, and visual markings

- Sensitivity labels
- Azure Information Protection unified labeling client
- Double Key Encryption
- Office 365 Message Encryption (OME)
- Service encryption with Customer Key
- SharePoint Information Rights Management (IRM)
- Rights Management connector
- Azure Information Protection unified labeling scanner
- Microsoft Cloud App Security
- Microsoft Information Protection SDK

MIP – Prevent data loss

Prevent data loss

prevent **accidental oversharing** of sensitive information

- Data loss prevention (DLP)
- Endpoint data loss prevention
- Microsoft Compliance Extension – Chrome Extension
- Microsoft 365 data loss prevention on-premises scanner
- Protect sensitive information in Microsoft Teams chat and channel messages

MIG – Govern Your Data

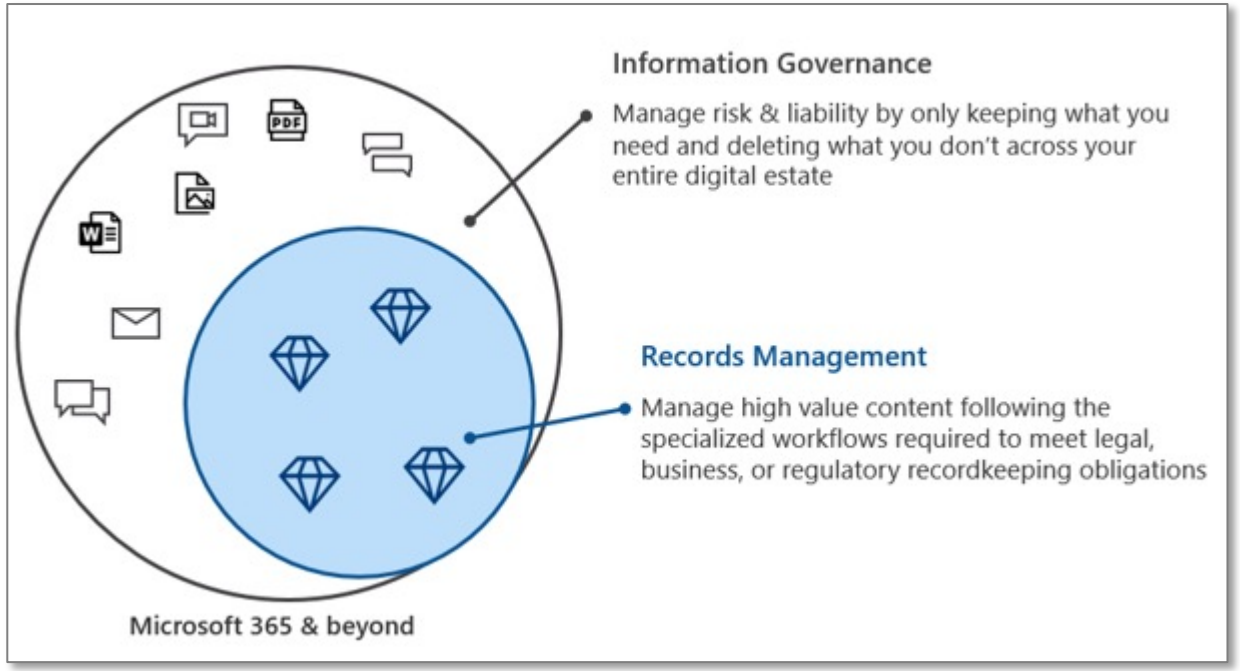
Microsoft Information Governance (MIG) a collection of features to **govern your data for compliance** or regulatory

Information governance

- Retention policies and retention labels
- Import service
- Archive third-party data
- Inactive mailboxes

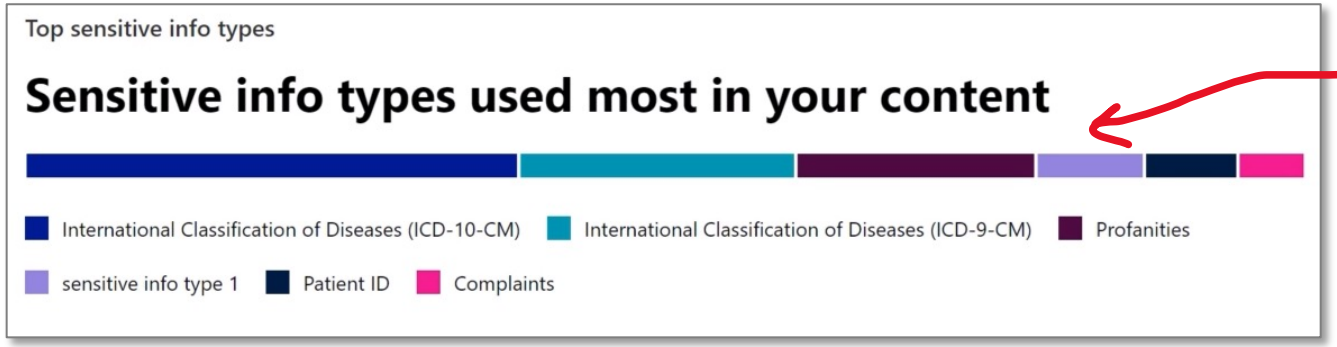
Records management

A single solution for email and documents that incorporates retention schedules and requirements into a file plan that supports the full lifecycle of your content with records declaration, retention, and disposition



Sensitive Information Types

Sensitive Information types **are classifications (categories) of data by sensitivity**

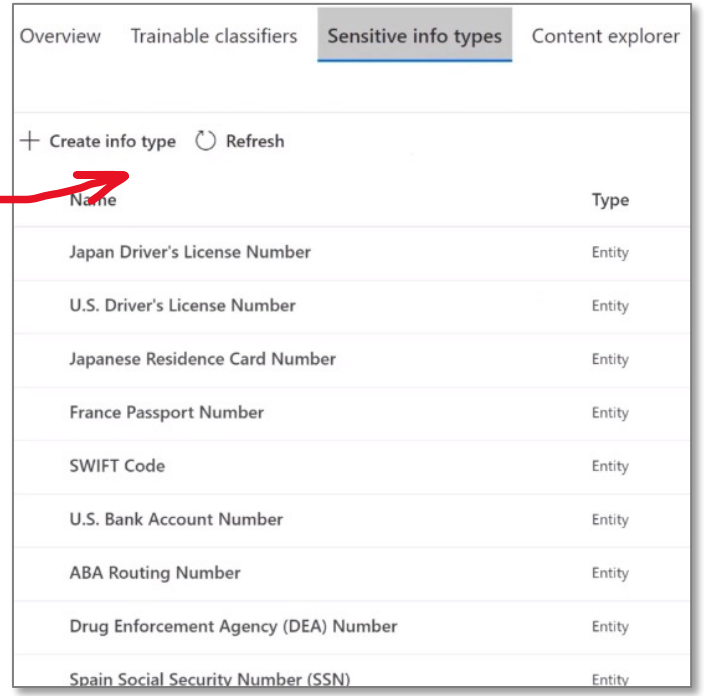


Within M365 Compliance Data Classification you get a **breakdown** of the distribution of sensitive info types

Types identified based on on regular expression (regex) or a function.
There are hundreds of built-in Information types: eg.

- IP address
- EU passport number
- Credit card number
- Azure storage account key
- ABA routing number
- Canada health service number
- Latvia driver's license number
- Netherlands tax identification number

You can create your own info types



Sensitive information types are used in

- Data loss prevention policies
- Sensitivity labels
- Retention labels
- Insider risk management
- Communication compliance
- Auto-labelling policies

Trainable Classifiers

What is a Classifier?

A Classifier is a machine learning model that **can take records of data and classify (categorized) by applying a label** from a predetermine list of categories

What is training?

Training is the **act of teaching a machine learning model how to learn** by providing it large amounts of data that is already labeled. It uses the labeled data to tell if its predictions are similar to the ones provided.

M365 Compliance center has two kinds of Trainable Classifiers

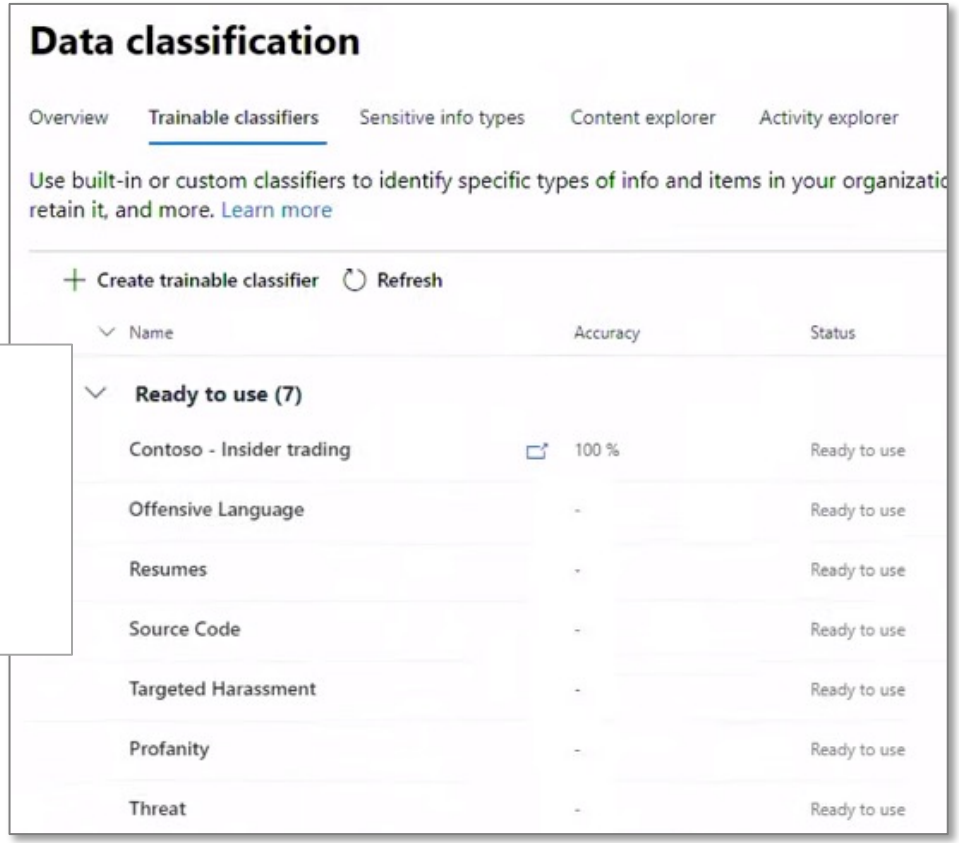
Pre-Trained Classifiers

Ready to use classifiers **with five pretrained classifiers**.
You don't need to provide any data used for training
Meets many general use cases

1. Resumes
2. Source Code
3. Harassment
4. Profanity
5. Threat

Custom Trainable Classifiers

When you have your own kind of documents.
When you have specific business documents.
You'll have to provide training data.

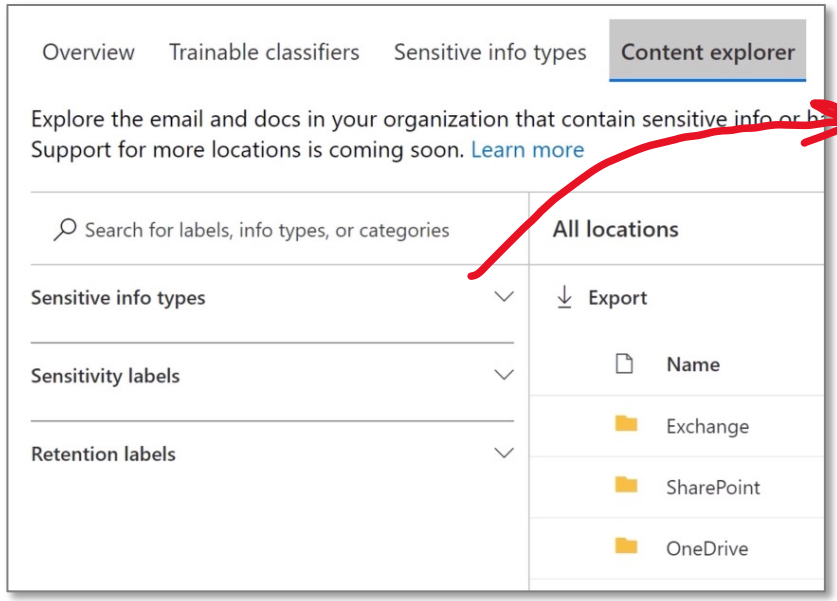


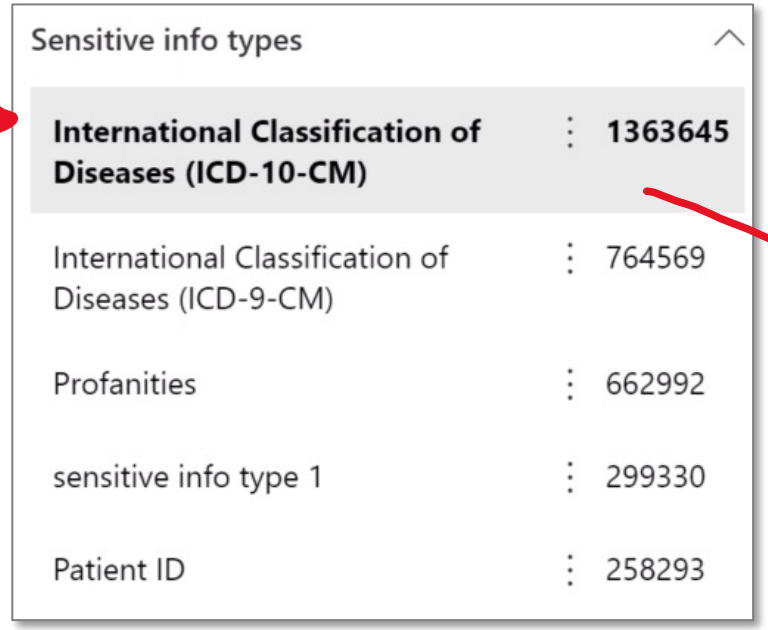
Content Explorer

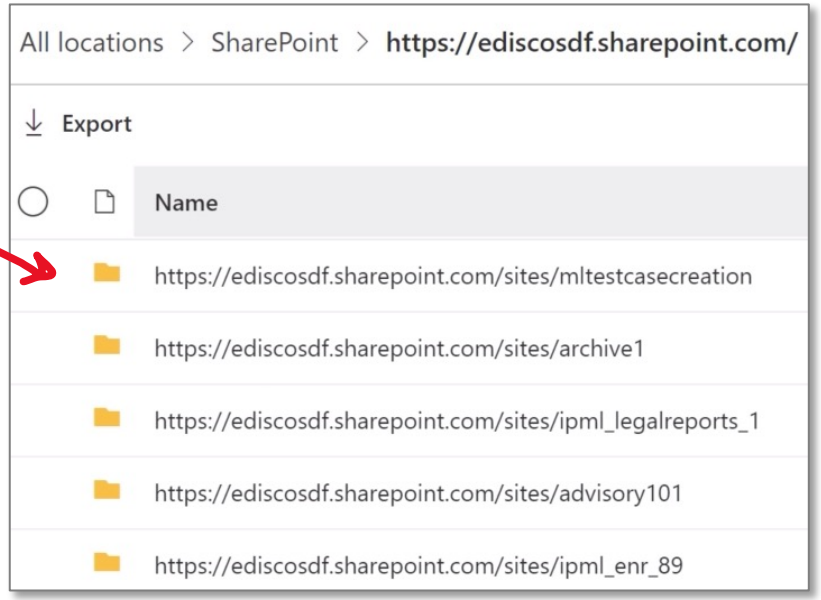
Context Explorer

Drill down to find emails (Microsoft Exchange) and documents (OneDrive and SharePoint) that's been labeled based on

- Sensitive info types
- Sensitivity labels
- Retention labels







Activity Explorer

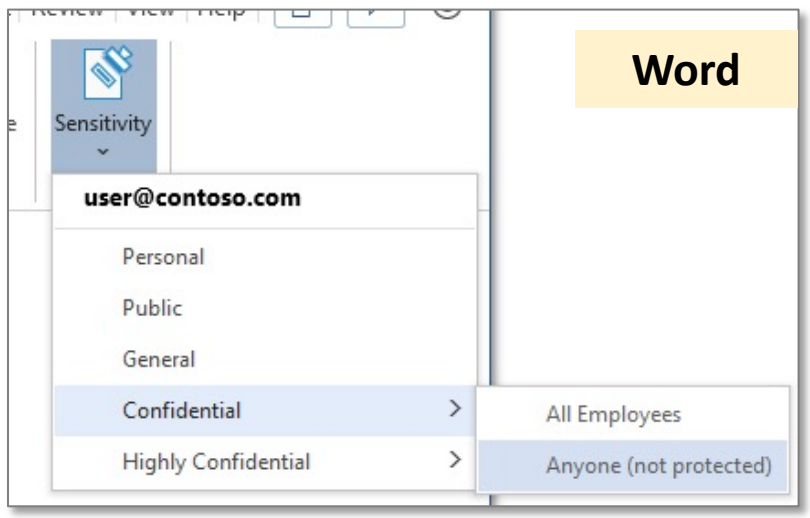
Activity Explorer

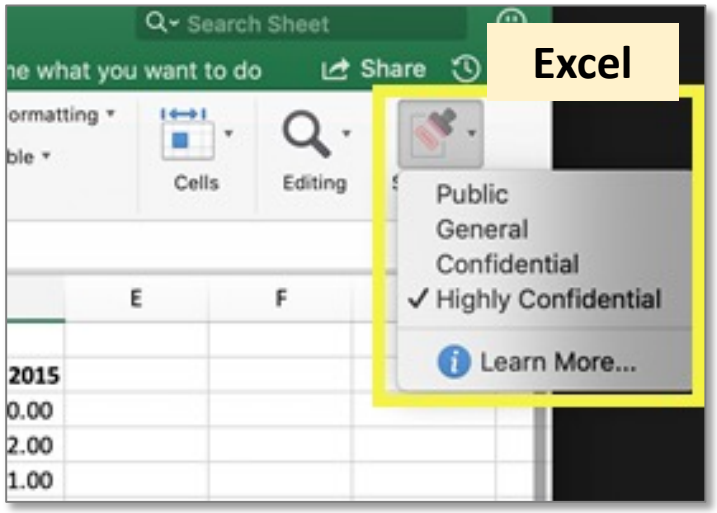
Helps discover **which file labels were changed**, and **which files were modified**.

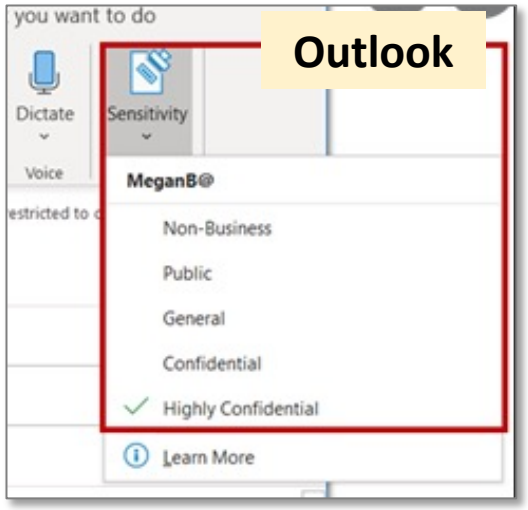
Monitors label activity across Exchange, SharePoint, OneDrive and endpoint devices

Sensitivity Labels

Sensitivity Labels allow you to **apply a label to your documents or emails**,
The most common way is via built-in dropdown within Office 365 products







Sensitivity Labels

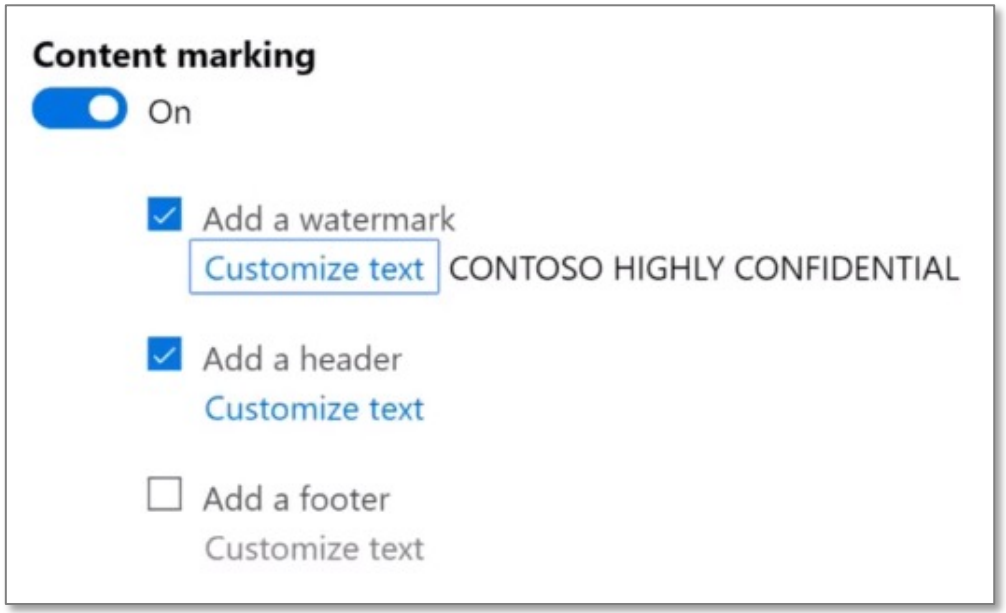
Sensitivity labeling makes it easy to apply to do **Content marking** and **Encryption**

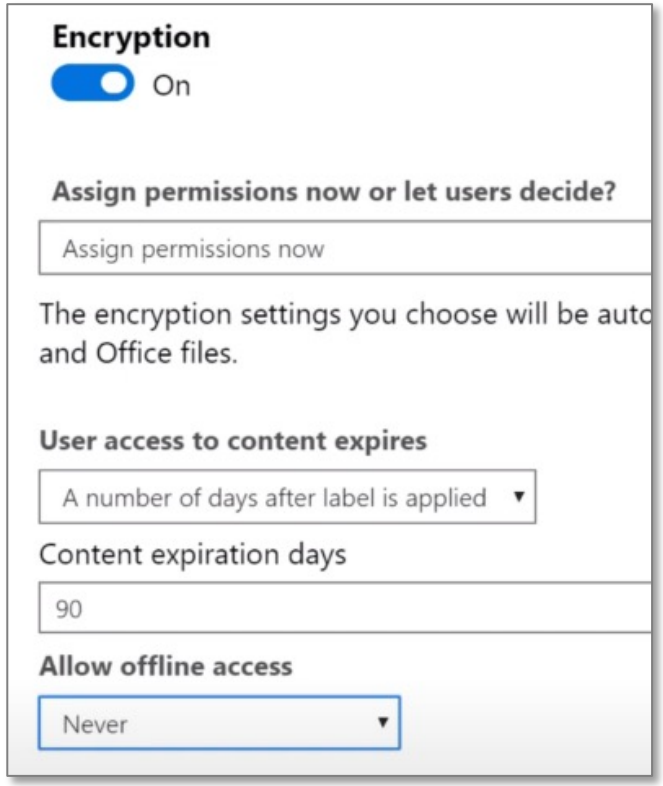
Content markings

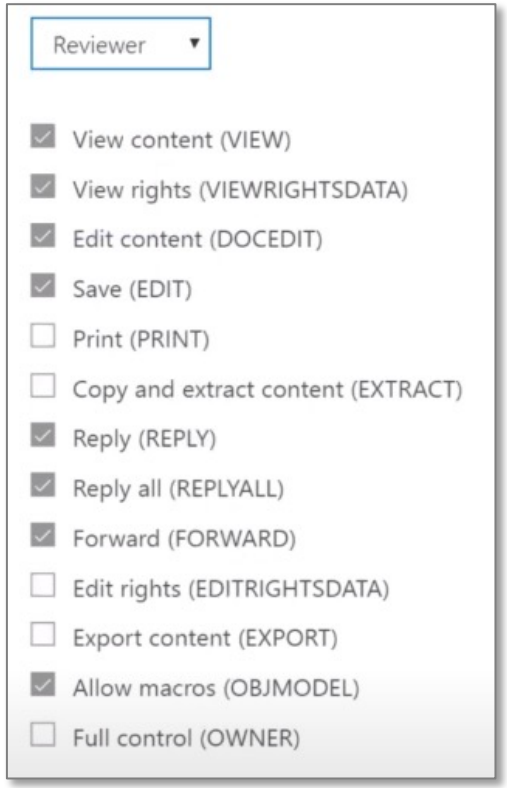
watermarks, warnings are applied to the header and footer of a document e.g. “Highly Confidential”

Encryption

Apply encryption and specific which users and groups may decrypt and other fine-tune permissions

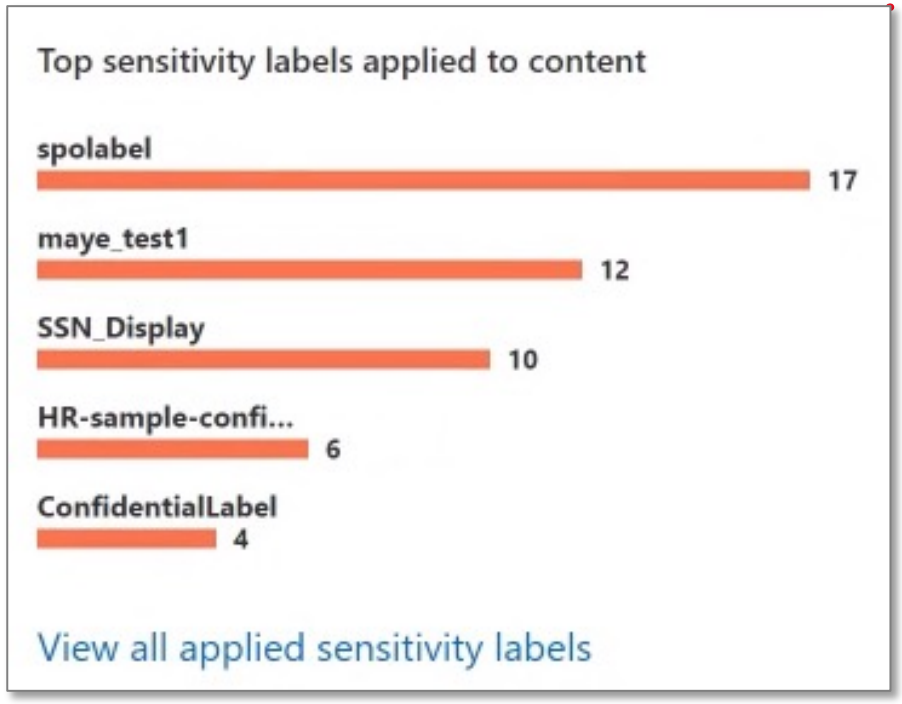


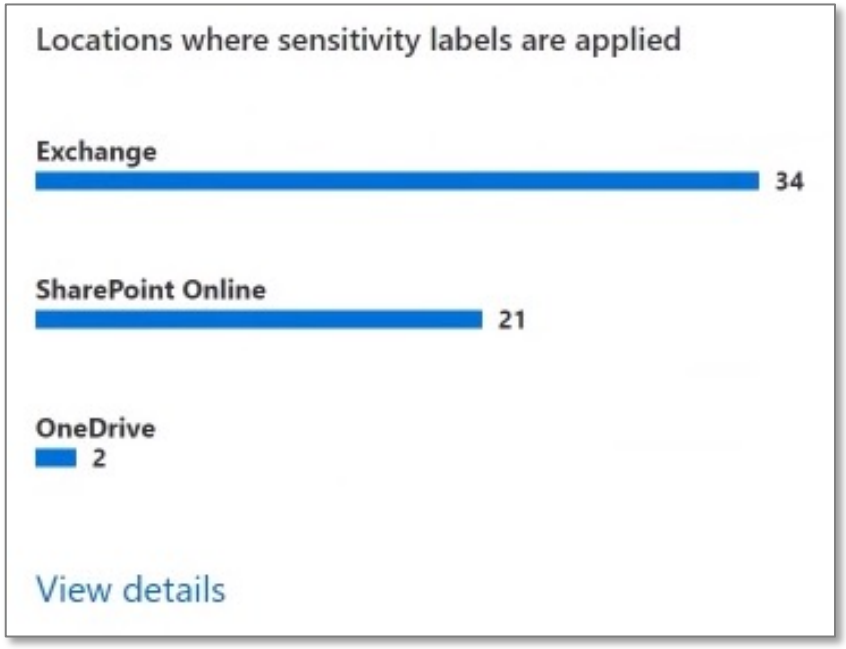




Sensitivity Labels

Within M365 Compliance Center under classification you can see the distribution of sensitive labels applied to documents and emails or based on location





Sensitivity Labels

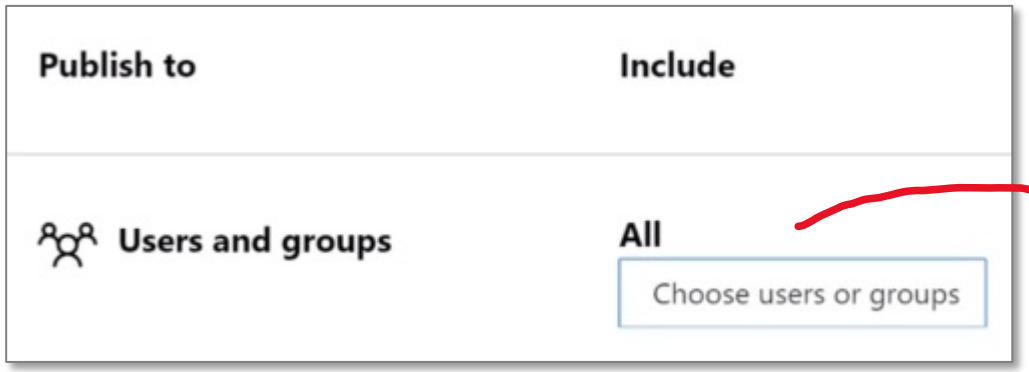
Sensitivity Labels can be used in:

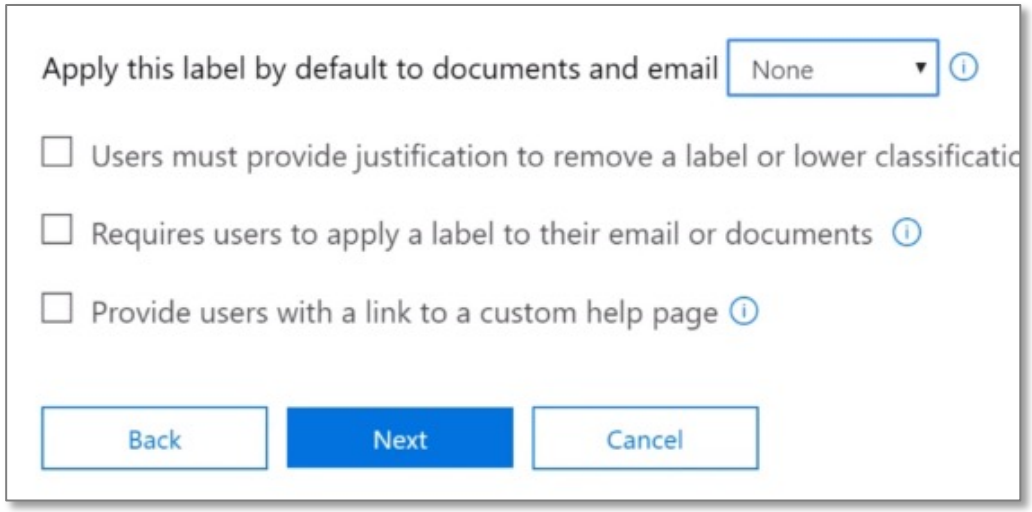
- Provide protection settings that include encryption and content markings
- Protect content in Office apps across different platforms and devices
- Protect content in third-party apps and services
- Protect containers
- Extend sensitivity labels to Power BI
- Extend sensitivity labels to assets in Azure
- Extend sensitivity labels to third-party apps and services
- Classify content without using any protection settings

Sensitivity Labels – Label Policies

In order to use Sensitivity labels they need to be **published** along with a **label policy**

A label Policy determines who can use the labels and other conditions





Sensitivity Labels – Label Policies

Choose the users and groups that can see labels.
Labels can be published to specific users, distribution groups, Microsoft 365 groups in Azure Active Directory, and more.

Apply a default label to all new emails and documents that the specified users and groups create. Users can always change the default label if they believe the document or email has been mislabeled.

Require justifications for label changes. If a user wants to remove a label or replace it, admins can require the user to provide a valid justification to complete the action. The user will be prompted to provide an explanation for why the label should be changed.

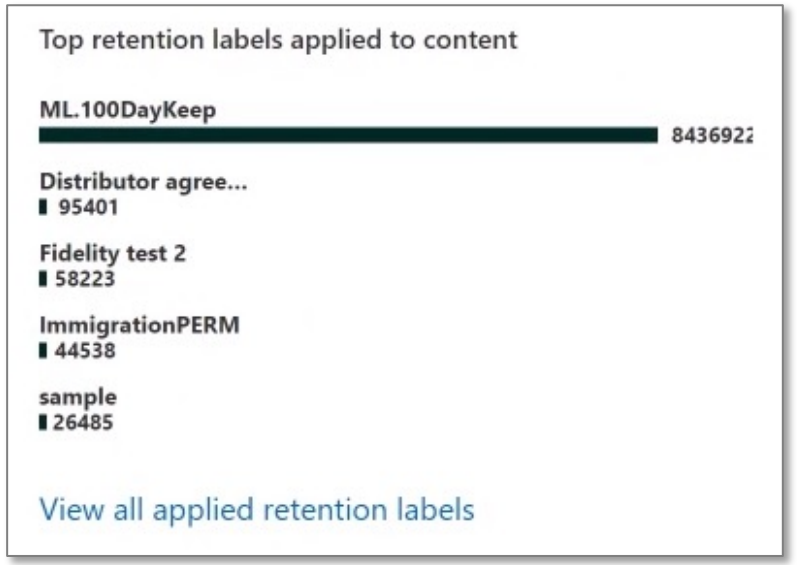
Require users to apply a label (mandatory labeling). It ensures a label is applied before users can save their documents, send emails, or create new sites or groups.

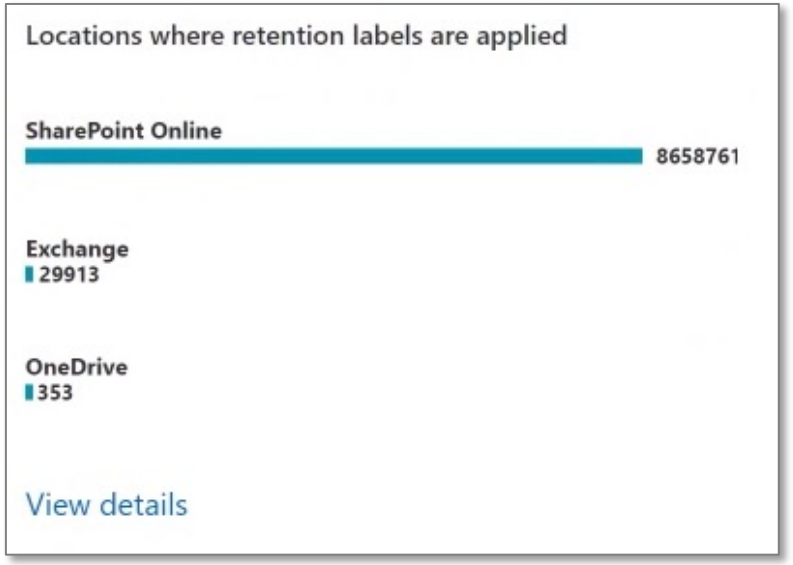
Link users to custom help pages. It helps users to understand what the different labels mean and how they should be used.

Retention

Retention Labels ensures **data is held for a specific duration** to meet a regulatory compliance or industry best practices.

Retention Policies are used to **assign the same retention settings to content at a site level or mailbox level**





Records Management

What is Records Management?

An organizations process of managing an organization's information throughout its life cycle.

Record management helps organization meeting regulatory compliance (legal requirements)

Lifecycle of a record

A **record** represents labeled information or content and its lifecycle will be managed

M365 Record Management enabled you to:

- Labeling content as a record.
- Migrating and managing retention plans with file plan manager.
- Establishing retention and deletion policies within the record label.
- Triggering event-based retention.
- Reviewing and validating disposition.
- Proof of records deletion.
- Exporting information about disposed items.
- Setting specific permissions for record manager functions in the organization.

Label content applys the following controls:

- Restrictions are put in place to block certain activities.
- Activities are logged.
- Proof of disposition is kept at the end of the retention period.

Data Loss Prevention

M365 Compliance Center Data Loss Protection (DLP) policies prevent data loss

DLP policies allows you to:

- Identify, monitor, and automatically protect sensitive information in M365
- Help users learn how compliance works
- View DLP reports

DLP polices are composed of:

- **Conditions**
  - Matching content before rule is enforced
- **Actions**
  - What actions to take when the condition is found
- **Locations**
  - Where the policy should be applied

Insider Risk Management

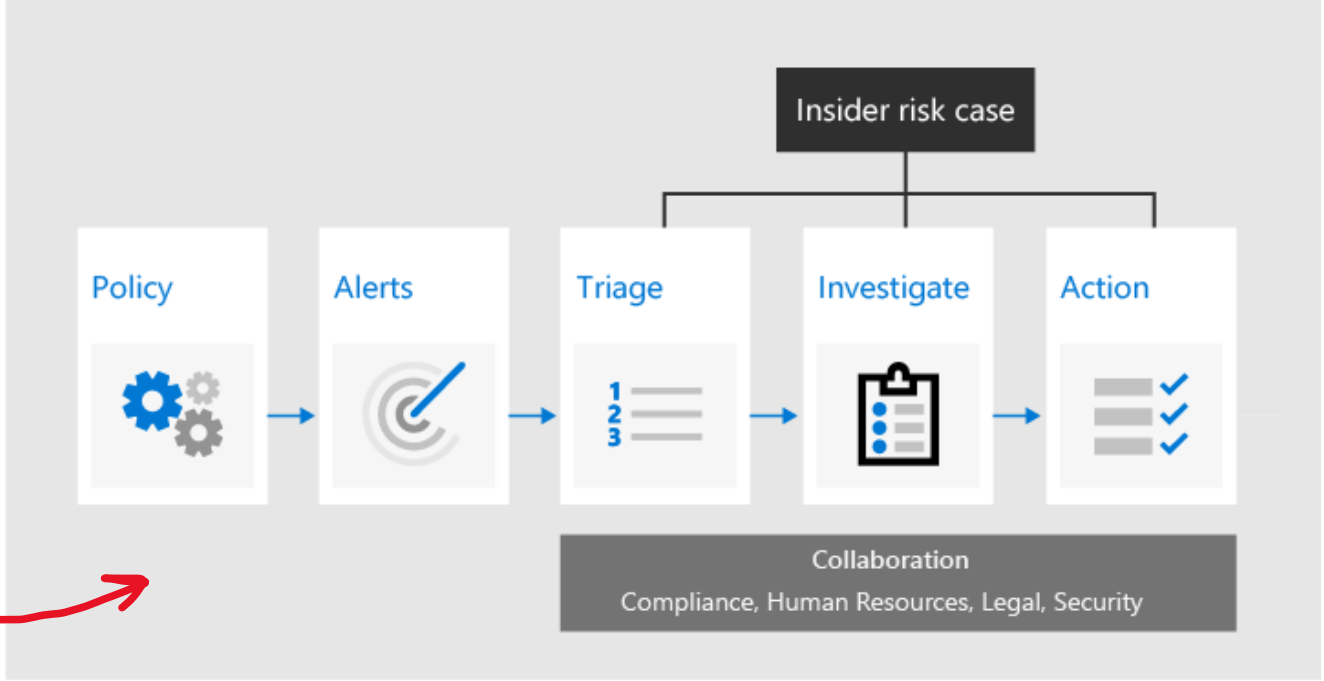
M365 Insider Risk Management minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization

Define the types of risks to identify and detect in your organization, including acting on cases and escalating cases to Microsoft Advanced eDiscovery if needed.

Insider Risk Management is looking to detect:

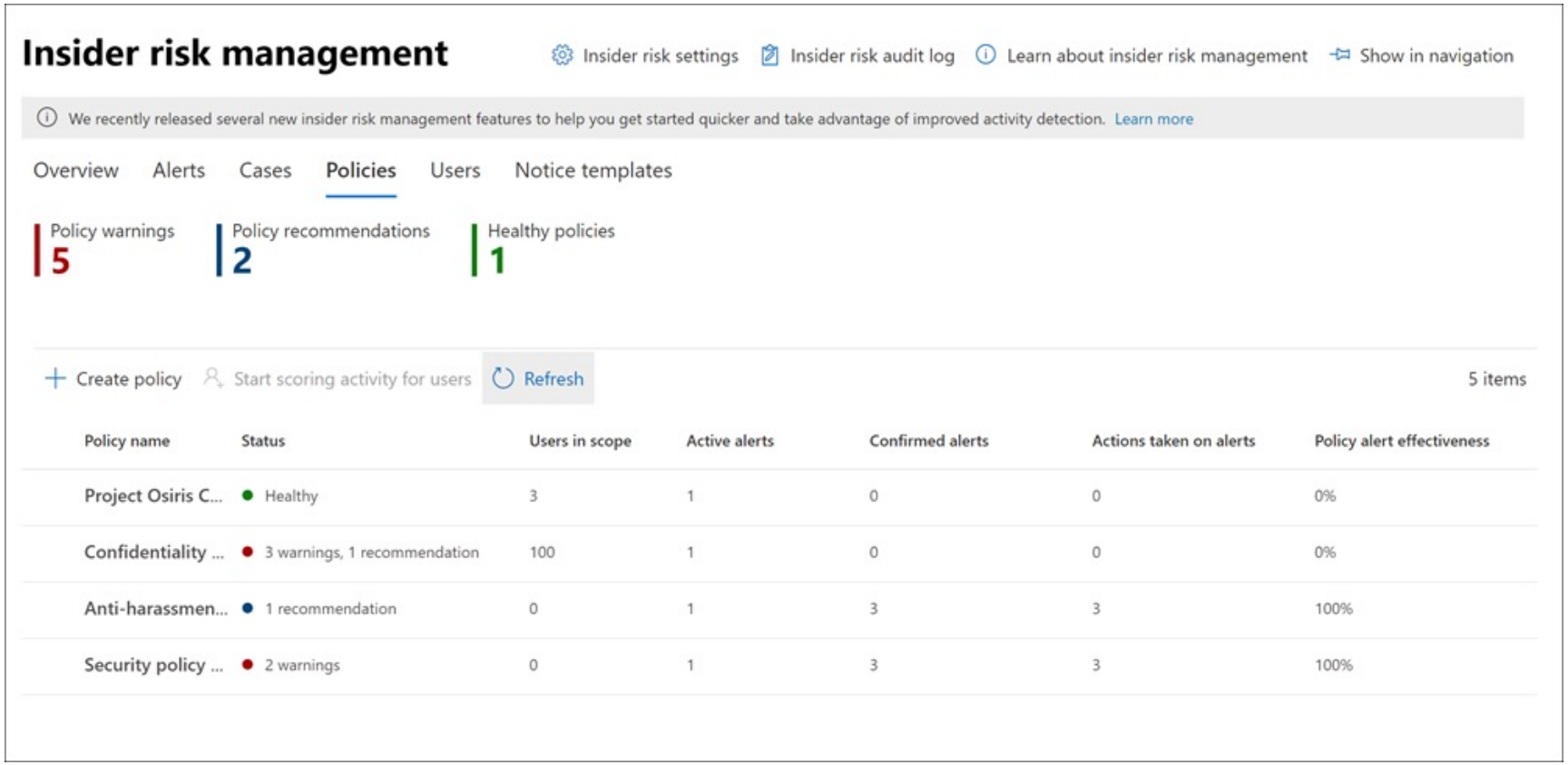
- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

M365 Insider Risk Management uses the following workflow



Insider Risk Management – Policies

Policies
pre-defined templates and policy conditions that define what triggering events and risk indicators are examined in your organization

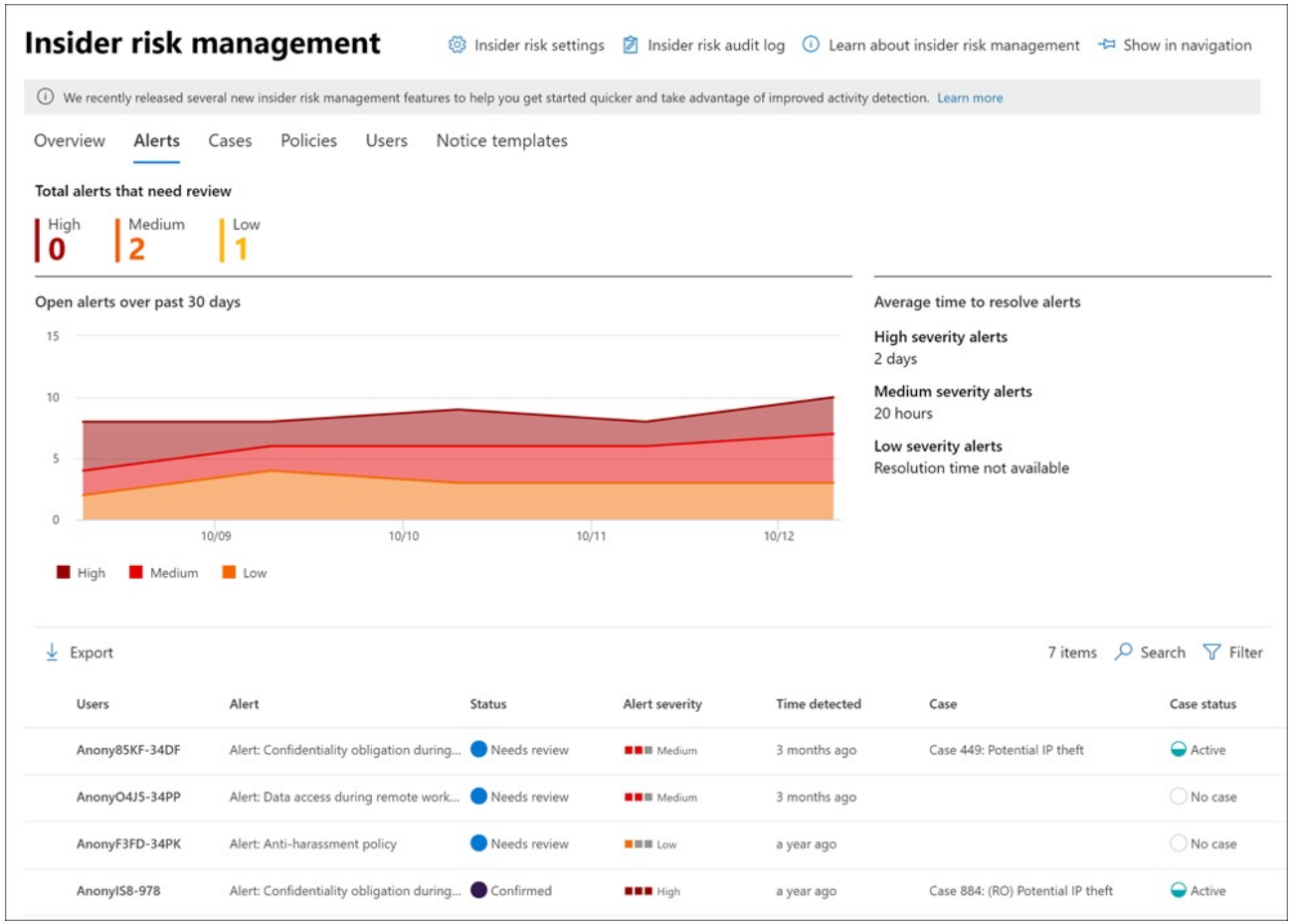


Insider Risk Management – Alerts

Alerts
Automatically generated by risk indicators that match policy conditions and are displayed in the Alerts dashboard

Identify the status of existing alerts and new alerts that need action:

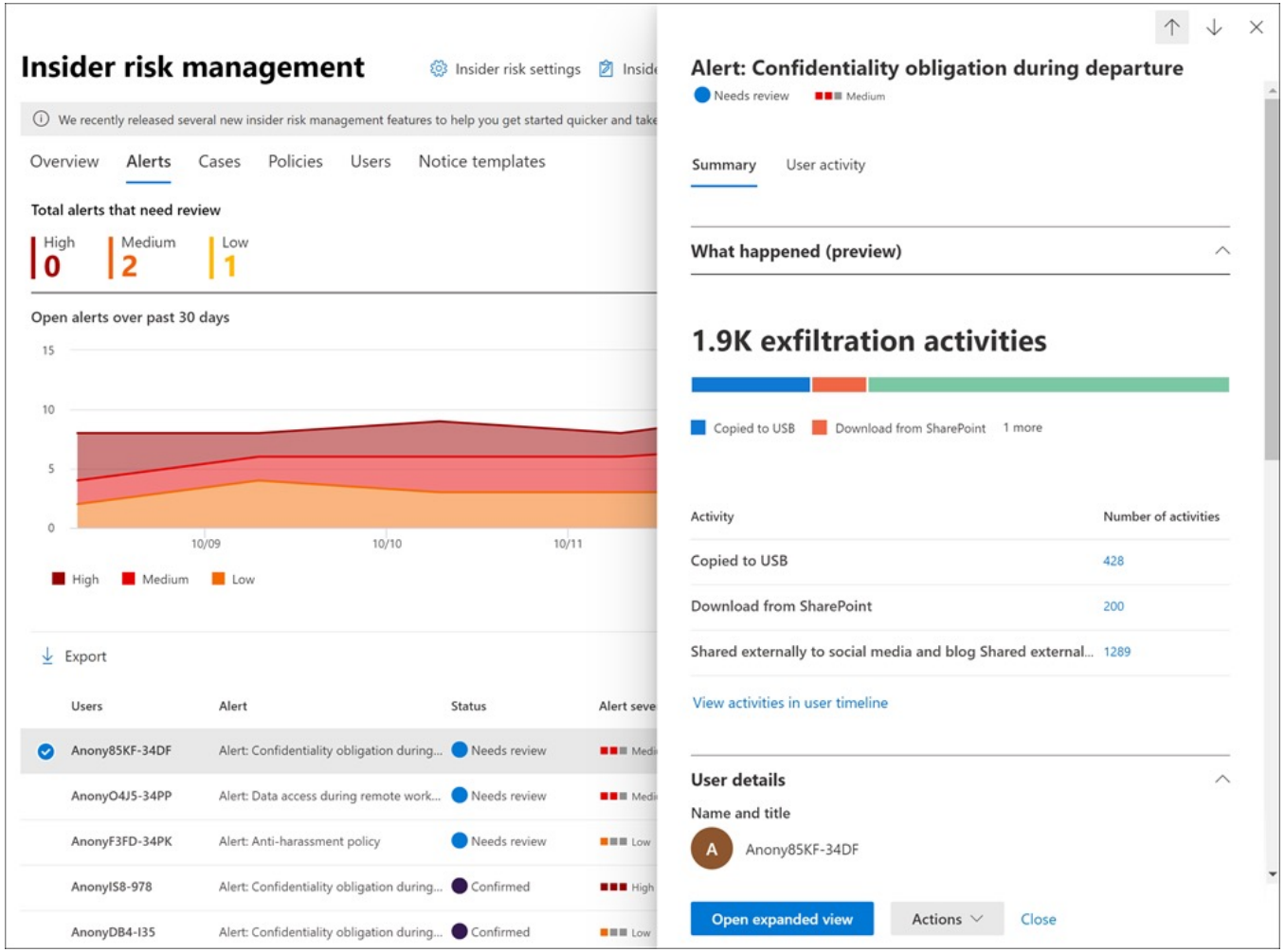
- Status
- Severity
- Time detected
- Case
- Case status



Insider Risk Management – Triage

Triage

reviewers can view alert details for the activities identified by the policy, view user activity associated with the policy match, see the severity of the alert, and review user profile information.



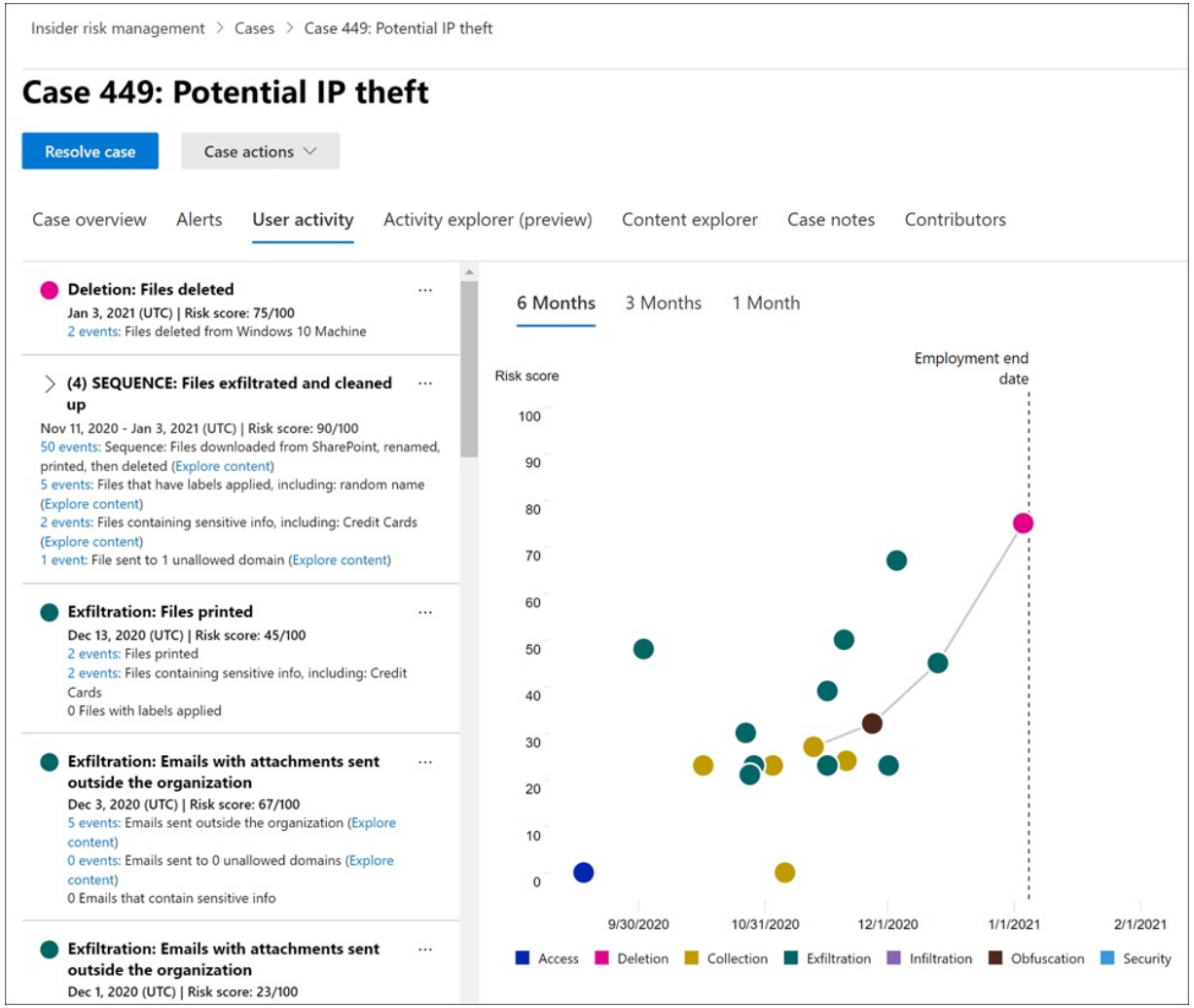
Insider Risk Management – Investigate

Investigate
Case dashboard provides an all-up view of all active cases, open cases over time, and case statistics for your organization. Reviewers can quickly filter cases by status, the date the case was opened, and the date the case was last updated.

Cases are created for alerts that require deeper review and investigation of the activity details and circumstances around the policy match.

primary investigation tools are

- User Activity
- Activity Explorer
- Content Explorer
- Case Notes



Communication Compliance

Microsoft 365 Communication Compliance that helps **minimize communication risks** by helping you detect, capture, and act on inappropriate messages in your organization.

Pre-defined and custom policies allow you to scan internal and external communications for policy matches so they can be examined by designated reviewers.

Reviewers can investigate scanned email, Microsoft Teams, Yammer, or third-party communications in your organization and take appropriate actions to make sure they're compliant with your organization's message standards.

Communication Compliance can

- Scanning increasing types of communication channels
- The increasing volume of message data
- Regulatory enforcement and the risk of fines

Scenarios for Communication Compliance:

- **Corporate polices**
  - acceptable use, ethical standards
  - avoid harassment or the use of inappropriate or offensive language
- **Risk management**
  - manage potential legal exposure and risk
  - unauthorized communications and conflicts of interest about confidential projects such as upcoming acquisitions, mergers, earnings disclosures, reorganizations, or leadership team changes
- **Regulatory compliance**
  - supervisory or oversight process for messaging that is appropriate for their industry
  - Regulatory Authority (FINRA) Rule 311

Communication Compliance

Configure
identify your compliance requirements and configure applicable communication compliance policies.

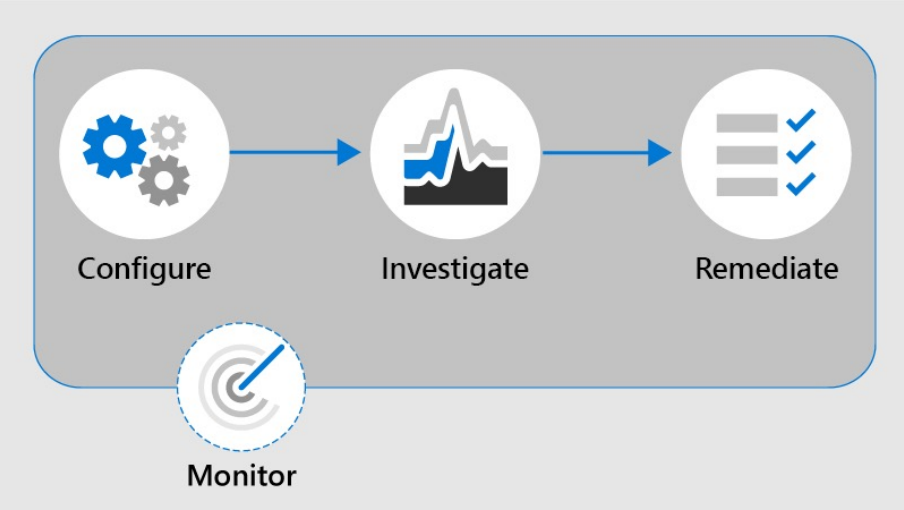
- Offensive or threatening language
- Sensitive information
- Regulatory compliance
- Conflict of interest
- Custom policy

Investigate
issues detected as matching your communication compliance policies

- Alerts
- Issue Management
- Document Review
- Reviewing User Activity History
- Filters

Remediate
remediate communication compliance issues you've investigated

- Resolve
- Tag a message
- Notify the user
- Escalate to another reviewer
- Mark as a false positive
- Remove message in Teams
- Escalate for investigation



Monitor and report
communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs to continually evaluate and improve your compliance posture

Information Barriers

Information Barriers are policies that admins can configure to
prevent individuals or groups from communicating with each other

Information Barriers can be applied to:

- Microsoft Teams
- OneDrive for Business
- SharePoint Online
- And more…

Information Barriers only support
two-way restrictions.

Information barriers in Microsoft Teams
information barrier policies can restrict the following

- Searching for a user
- Adding a member to a team
- Starting a chat session with someone
- Starting a group chat
- Inviting someone to join a meeting
- Sharing a screen
- Placing a call
- Sharing a file with another user
- Access to file through sharing link

Use cases:

- Education
  - A student cant view details of student of other schools
- Legal
  - A lawyers cannot obtain client data from another lawyer in the firm

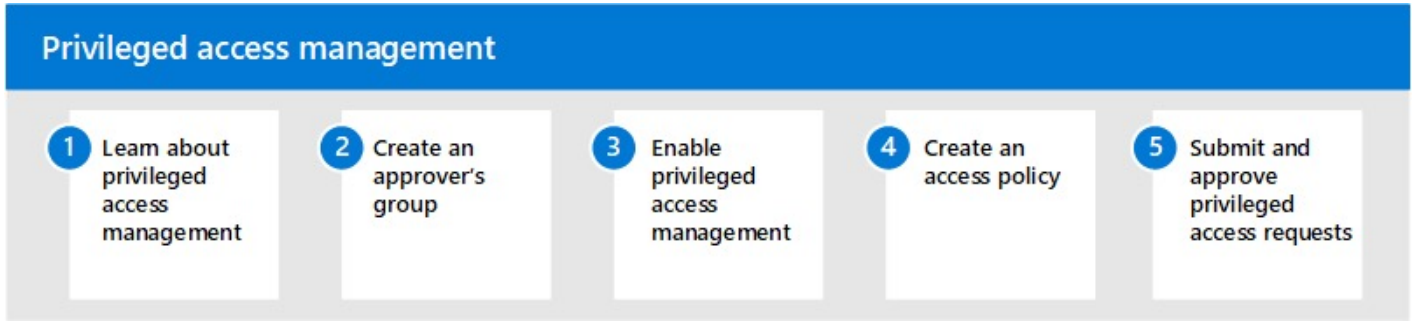
Privileged Access Management

M365 Privileged Access Management protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration setting

just-in-time access rules are implemented for tasks that need elevated permissions and lets an organization operate with **zero standing access**

Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

- Create an approver's group
- Enable privileged access management
- Create an access policy
- Submit/approve privileged access requests



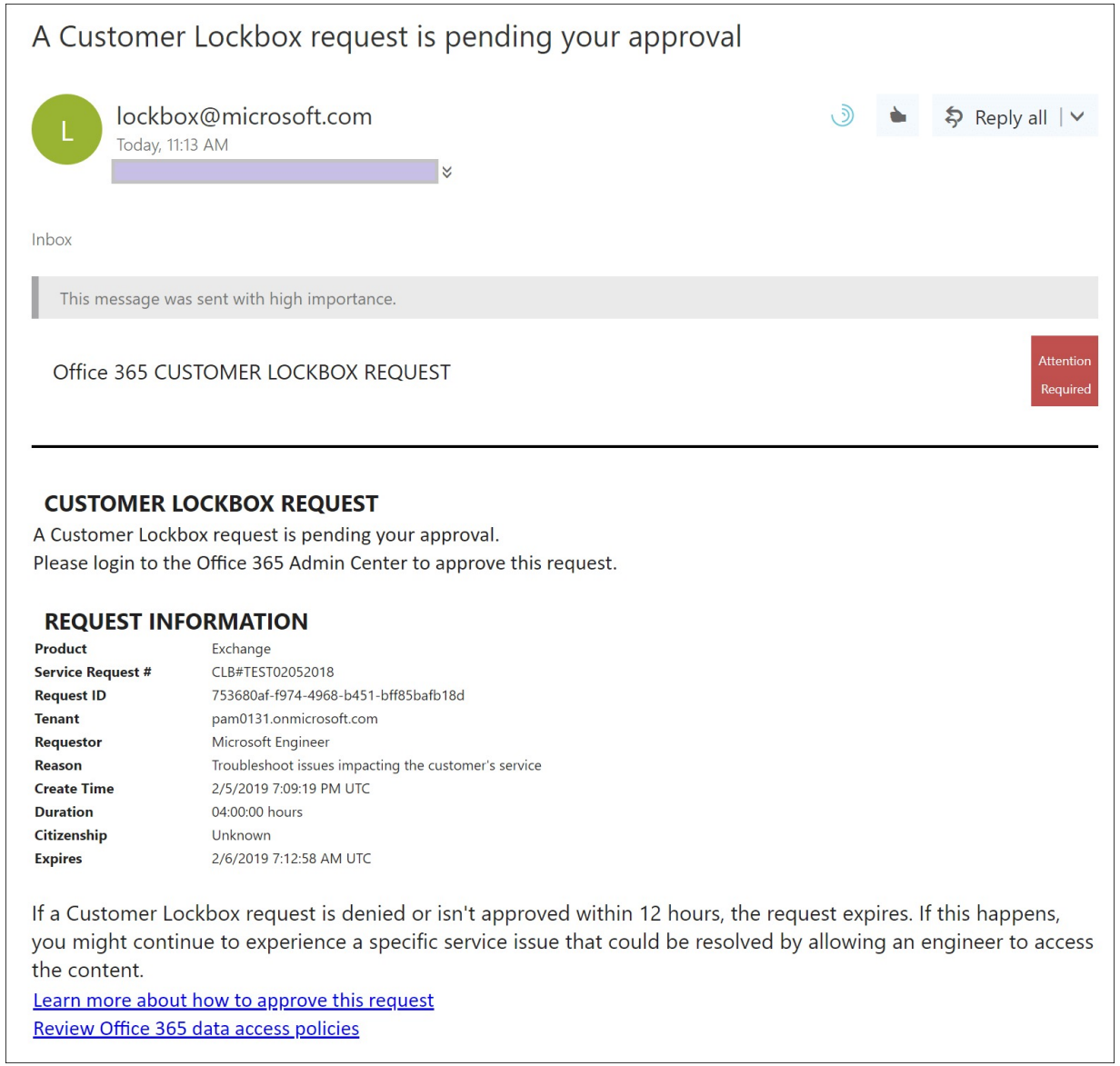
Customer Lockbox

Customer Lockbox **protects sensitive data when working with Microsoft Support Engineers** by enforcing a **request system** to view custom private information to resolve a M365 related issue.

Customer Lockbox supports requests to access data for:

- Exchange Online
- SharePoint Online
- OneDrive for Business.

- You need to turn on Customer Lockbox
- Support Engineer must make an email request and approved before access
- Support Engineer only has access for the minimum amount of time
- An audit trail of access is maintained



A Customer Lockbox request is pending your approval

L lockbox@microsoft.com
Today, 11:13 AM

Reply all

Inbox

This message was sent with high importance.

Office 365 CUSTOMER LOCKBOX REQUEST

Attention Required

CUSTOMER LOCKBOX REQUEST

A Customer Lockbox request is pending your approval.
Please login to the Office 365 Admin Center to approve this request.

REQUEST INFORMATION

Product	Exchange
Service Request #	CLB#TEST02052018
Request ID	753680af-f974-4968-b451-bff85bafb18d
Tenant	pam0131.onmicrosoft.com
Requestor	Microsoft Engineer
Reason	Troubleshoot issues impacting the customer's service
Create Time	2/5/2019 7:09:19 PM UTC
Duration	04:00:00 hours
Citizenship	Unknown
Expires	2/6/2019 7:12:58 AM UTC

If a Customer Lockbox request is denied or isn't approved within 12 hours, the request expires. If this happens, you might continue to experience a specific service issue that could be resolved by allowing an engineer to access the content.

Learn more about how to approve this request
Review Office 365 data access policies

eDiscorvey

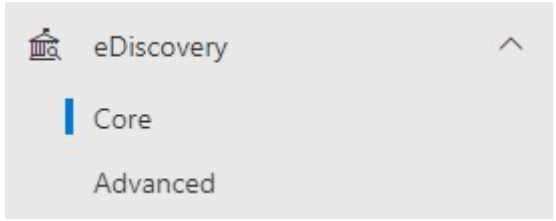
Electronic discovery (eDiscovery)
the process of identifying and delivering electronic information that can be used as evidence in legal cases.

eDiscovery tools in Microsoft 365 to search for content in:

- Exchange Online mailboxes
- Microsoft 365 Groups
- Microsoft Teams
- SharePoint Online
- OneDrive for Business sites
- Skype for Business conversations
- Yammer teams

Microsoft 365 provides the following eDiscovery tools:

- **Content search** – running a search across content
- **Core eDiscovery** – A workflow to search and export content
- **Advanced eDiscovery** - end-to-end workflow to preserve, collect, review, analyze, and export content for internal or external investigation

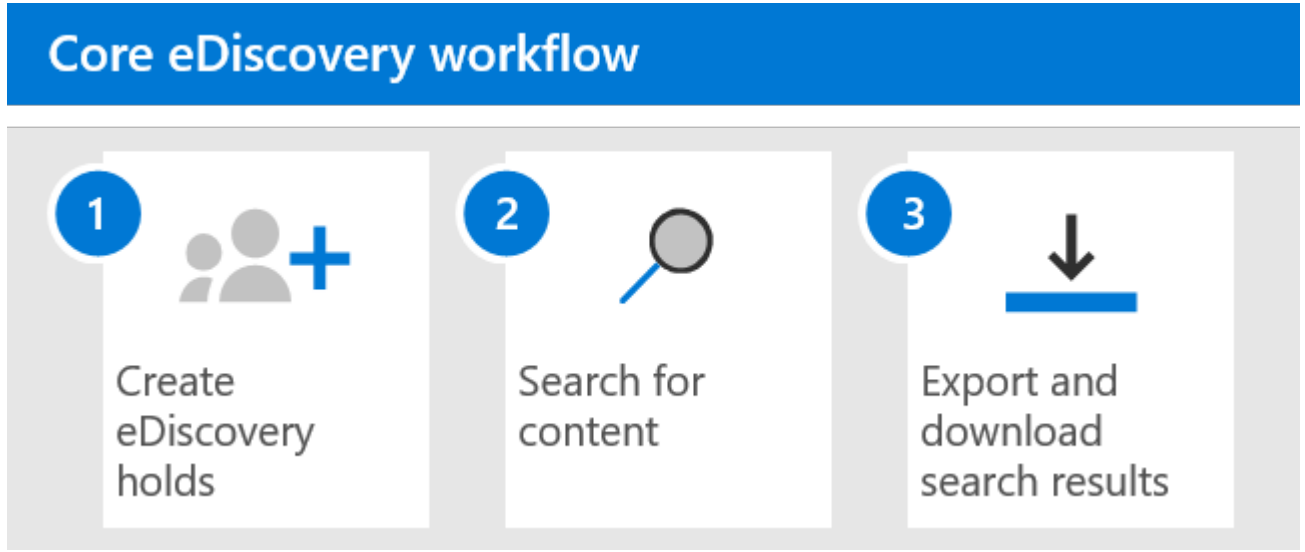


Core eDiscovery Workflow

Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organizations can use to search and export content in Microsoft 365 and Office 365.

You can also use Core eDiscovery to place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams.

Nothing is needed to deploy Core eDiscovery, but there are some prerequisite tasks that an IT admin and eDiscovery manager have to **complete** before your organization can start using Core eDiscovery to search, export, and preserve content.

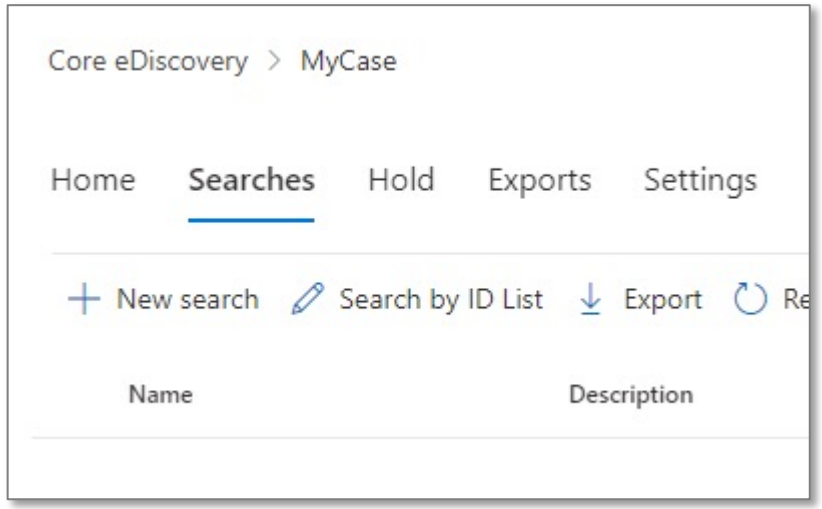


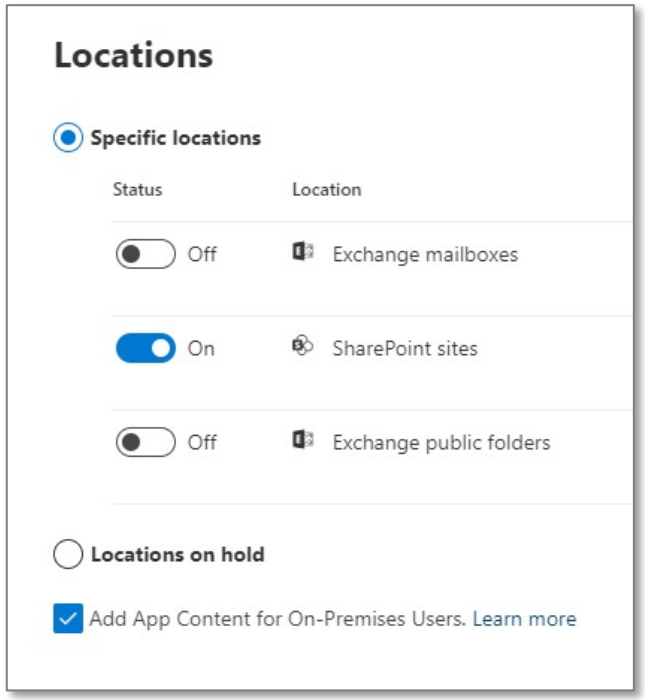
Initial Setup
- Verify and assign appropriate licenses
- Assign eDiscovery permissions
- Create a Core eDiscovery case

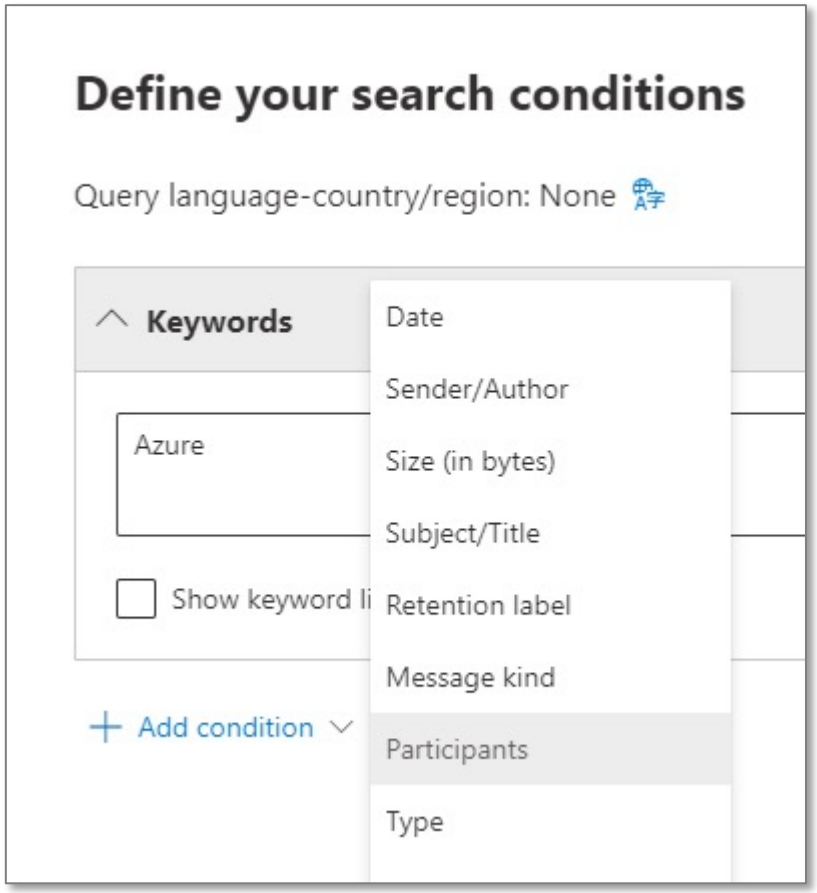
Use
- Create a eDiscovery Hold
- Search for content
- Export and download search results

Content Search

To perform a content search, create a new search, specific the locations and provide keywords and conditions.
Leaving keywords blank will return all items with the conditions.





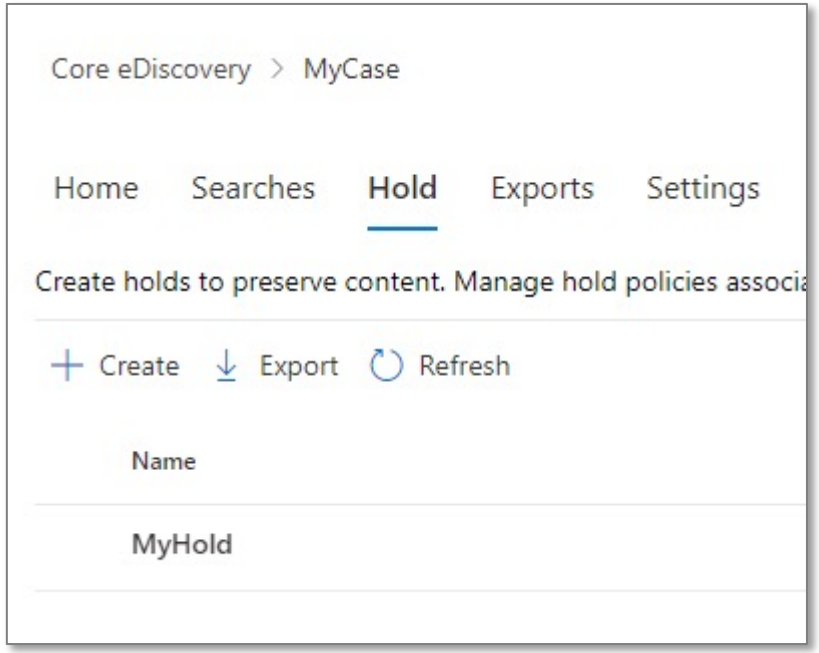


Core eDiscovery Hold

An **eDiscovery Hold** preserves content that might be relevant to a specific eDiscovery case

You can place a hold in:

- Exchange mailboxes
- OneDrive for Business
- Microsoft Teams
- Office 365 Groups
- Yammer Groups



Content is preserved until you remove the content location from the hold or until you delete the hold.

After you create an eDiscovery hold, it may take up to 24 hours for the hold to take effect

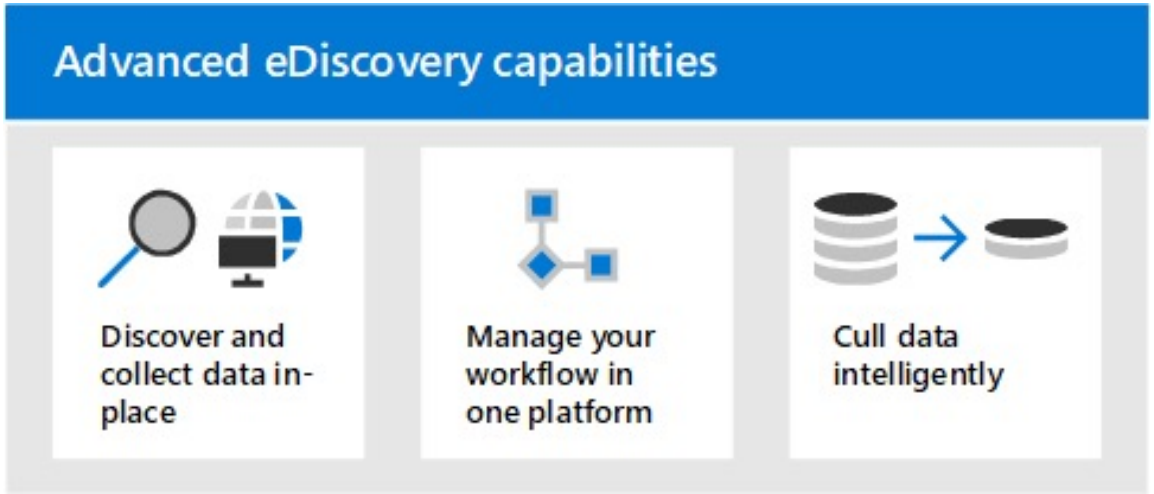
Advanced eDiscovery Worklfow

Advanced eDiscovery workflow builds on the existing Core eDiscovery workflow. Advanced eDiscovery **is end-to-end workflow** to **preserve, collect, review, analyze, and export** content that's relevant to your organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case.

The built-in workflow of Advanced eDiscovery aligns with the **Electronic Discovery Reference Model (EDRM),**

- a framework that outlines standards for recovery and discovery of digital data.

- Add custodians to a case
- Search custodial data sources for data relevant to the case
- Add data to a review set
- Review and analyze data in a review set
- Export and download case data



M365 Audit

What is an audit?

The investigating of a security events, forensic investigations, internal investigations, and compliance obligations

An audit would involve **capturing, recording and retaining** a unified audit log

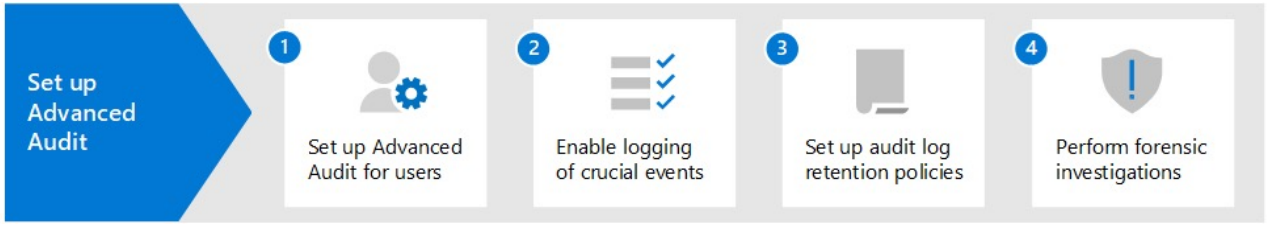
M365 has two auditing solutions

Basic Audit

- Enabled by default
- Thousands of searchable audit events
- 90-day audit record retention
- Export audit records to a CSV file
- Audit search tool in the Microsoft 365 compliance center
- Access to audit logs via Office 365 Management Activity API.
- Search-UnifiedAuditLog cmdlet

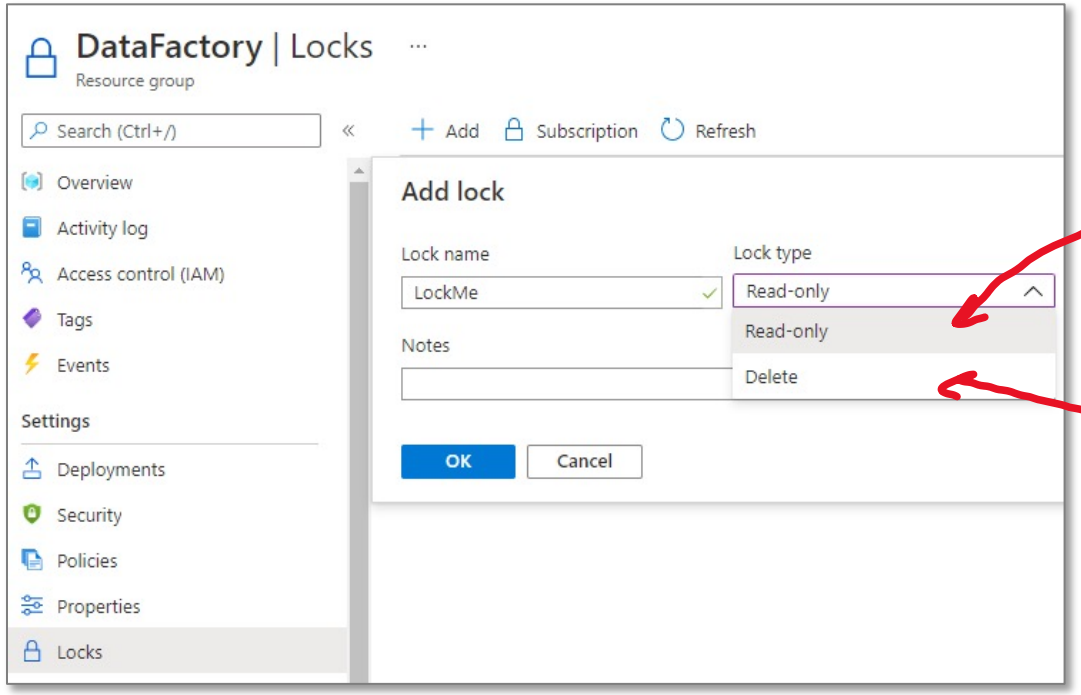
Advanced Audit

- *Includes all the Basic Audit features*
- Audit log retention policies
- Longer retention of audit records
- High-value, crucial events
- Higher bandwidth to the Office 365 Management Activity API



Resource Locks

As an admin, you may need to **lock a subscription, resource group, or resource** to **prevent other users from accidentally deleting or modifying critical resources.**



ReadOnly (Read-only)
authorized users can read a resource, but they can't delete or update the resource

CanNotDelete (Delete)
authorized users can still read and modify a resource, but they can't delete the resource.

Resource Tags

A tag is a **key and value pair** that you can assign to azure resources.

Tag Examples
Dept = Finance
Status = Approved
Team = Compliance
Environment = Production
Project = Enterprise
Location = West US

Tags allow you to organize your resources in the following ways:

- **Resource management**
  - specific workloads, environments eg. Developer Environments
- **Cost management and optimization**
  - Cost tracking, Budgets, Alerts
- **Operations management**
  - Business commitments and SLA operations eg. Mission-Critical Services
- **Security**
  - Classification of data and security impact
- **Governance and regulatory compliance**
- **Automation**
- **Workload optimization**

Azure Blueprints

Azure Blueprints enable **quick creation** of **governed subscriptions**.
Compose artifacts based on common or organization-based patterns into re-usable blueprints.
The service is designed to help with *environment setup*

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 Azure Blueprints service is backed by the globally distributed **Azure Cosmos DB**
Blueprint objects are replicated to multiple Azure regions.

ARM Templates vs Azure Blueprints

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template.

ARM Template

- ARM templates are stored either locally or in source control.
- There's no active connection or relationship to the ARM template

Azure Blueprints

- relationship between the blueprint definition (what *should be* deployed) and the blueprint assignment (what *was* deployed)
- can also upgrade several subscriptions at once that are governed by the same blueprint

Azure Blueprints supports **improved tracking and auditing of deployments**

Introduction to Azure Policies

Azure Policy enforce organizational standards and to assess **compliance** at-scale
Policies do not restrict access, they only observe for compliance.

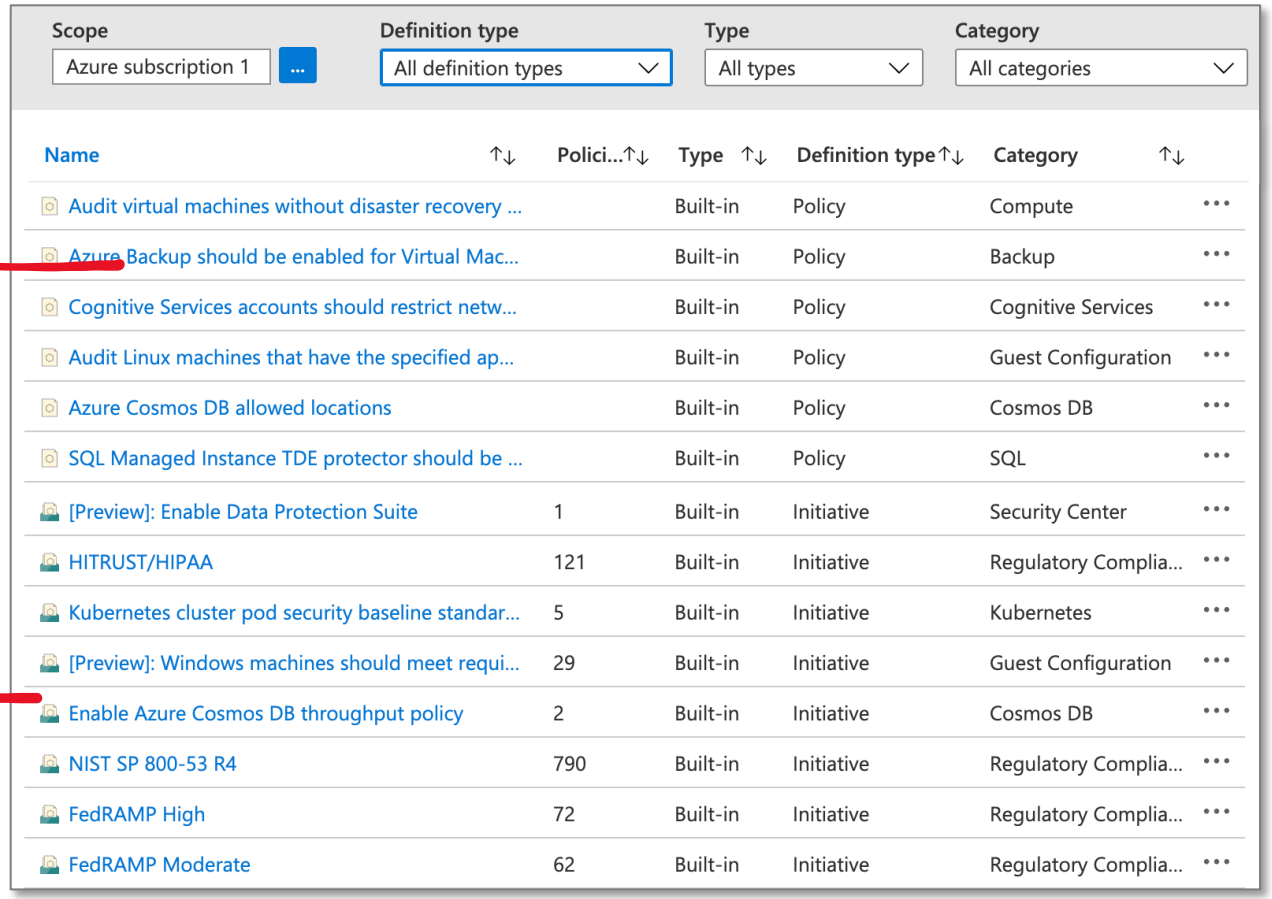
Azure has "built-in" policies you can used right away

Policy Definitions
A policy definition is a **JSON** file used to describe business rules to control access to resources.

Policy Assignment
The scope of a policy can effect. Assigned to a user, a resource group or management group.

Policy Parameters
Values you can pass into your Policy definition so your Policies are more flexible for re-use.

Initiative Definitions
An initiative definition is a collection of policy definitions, that you can assign. eg. A group of policies to enforce **PCI-DSS compliance**

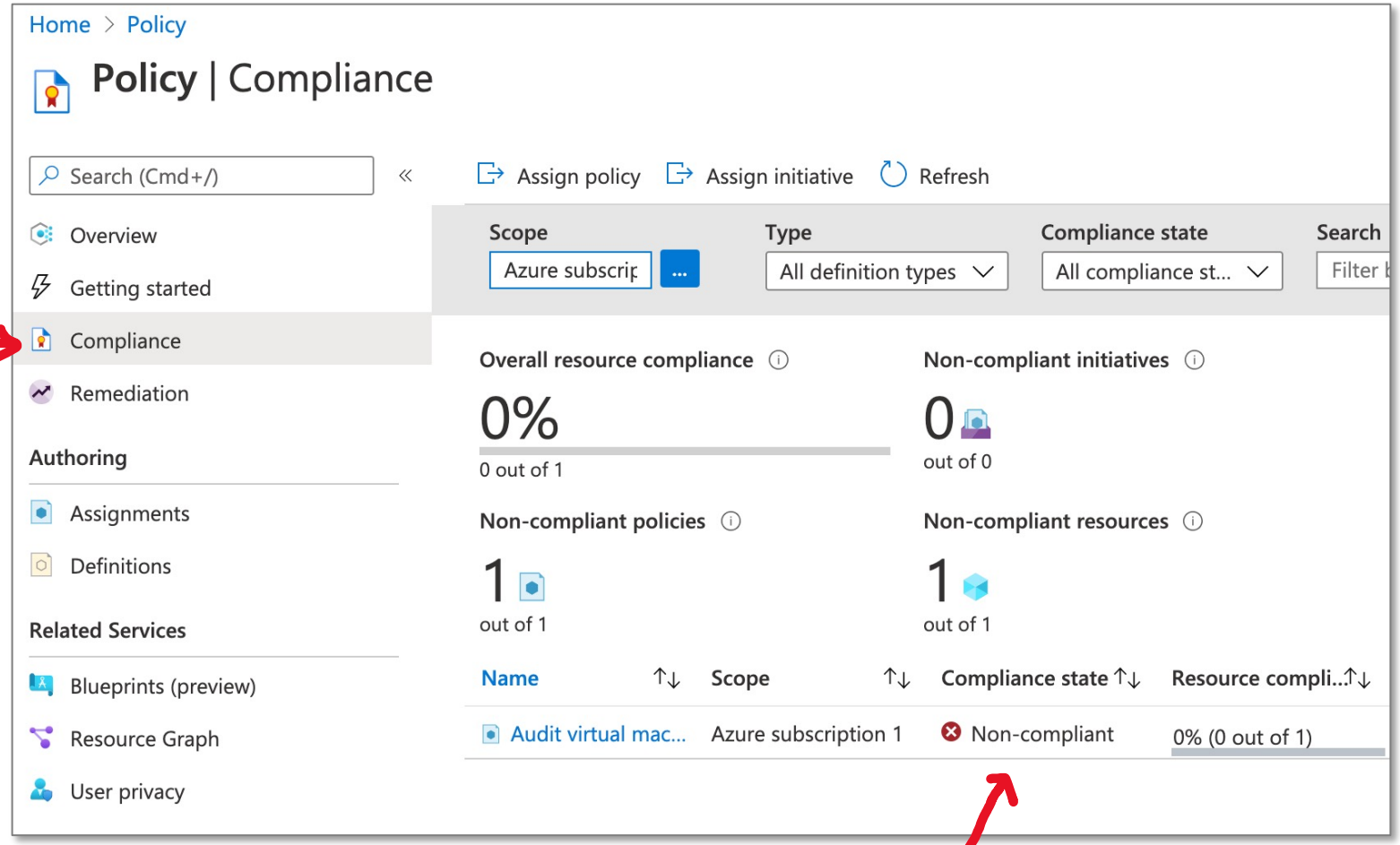


Name	Polici...	Type	Definition type	Category
Audit virtual machines without disaster recovery ...		Built-in	Policy	Compute
Azure Backup should be enabled for Virtual Mac...		Built-in	Policy	Backup
Cognitive Services accounts should restrict netw...		Built-in	Policy	Cognitive Services
Audit Linux machines that have the specified ap...		Built-in	Policy	Guest Configuration
Azure Cosmos DB allowed locations		Built-in	Policy	Cosmos DB
SQL Managed Instance TDE protector should be ...		Built-in	Policy	SQL
[Preview]: Enable Data Protection Suite	1	Built-in	Initiative	Security Center
HITRUST/HIPAA	121	Built-in	Initiative	Regulatory Complia...
Kubernetes cluster pod security baseline standar...	5	Built-in	Initiative	Kubernetes
[Preview]: Windows machines should meet requi...	29	Built-in	Initiative	Guest Configuration
Enable Azure Cosmos DB throughput policy	2	Built-in	Initiative	Cosmos DB
NIST SP 800-53 R4	790	Built-in	Initiative	Regulatory Complia...
FedRAMP High	72	Built-in	Initiative	Regulatory Complia...
FedRAMP Moderate	62	Built-in	Initiative	Regulatory Complia...

Viewing Non-Compliant Resources

Once a policy is assigned it will evaluate for the compliance state periodically

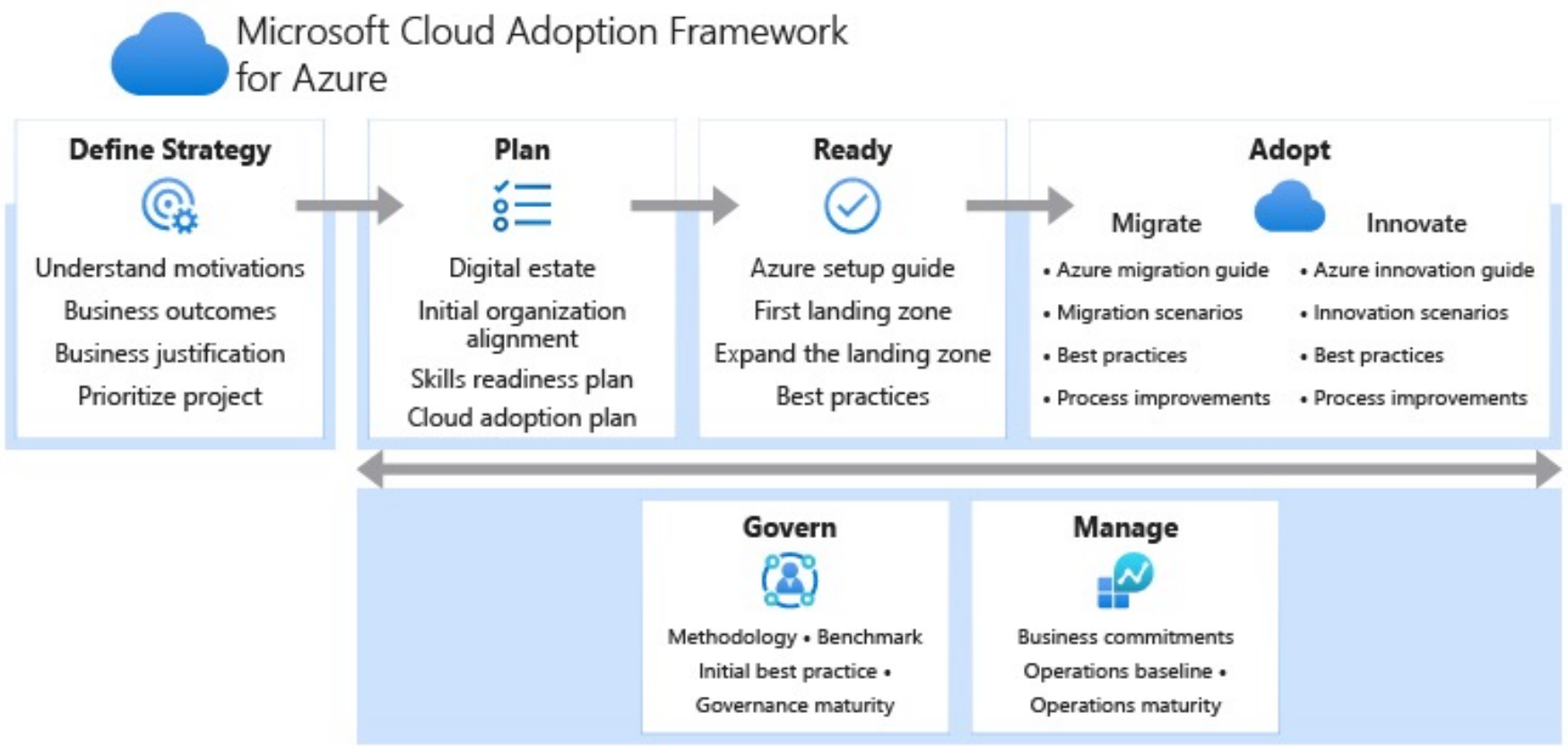
We can see how compliant we Are on the **Compliance tab**



eg. VMs should have Disaster Recovery

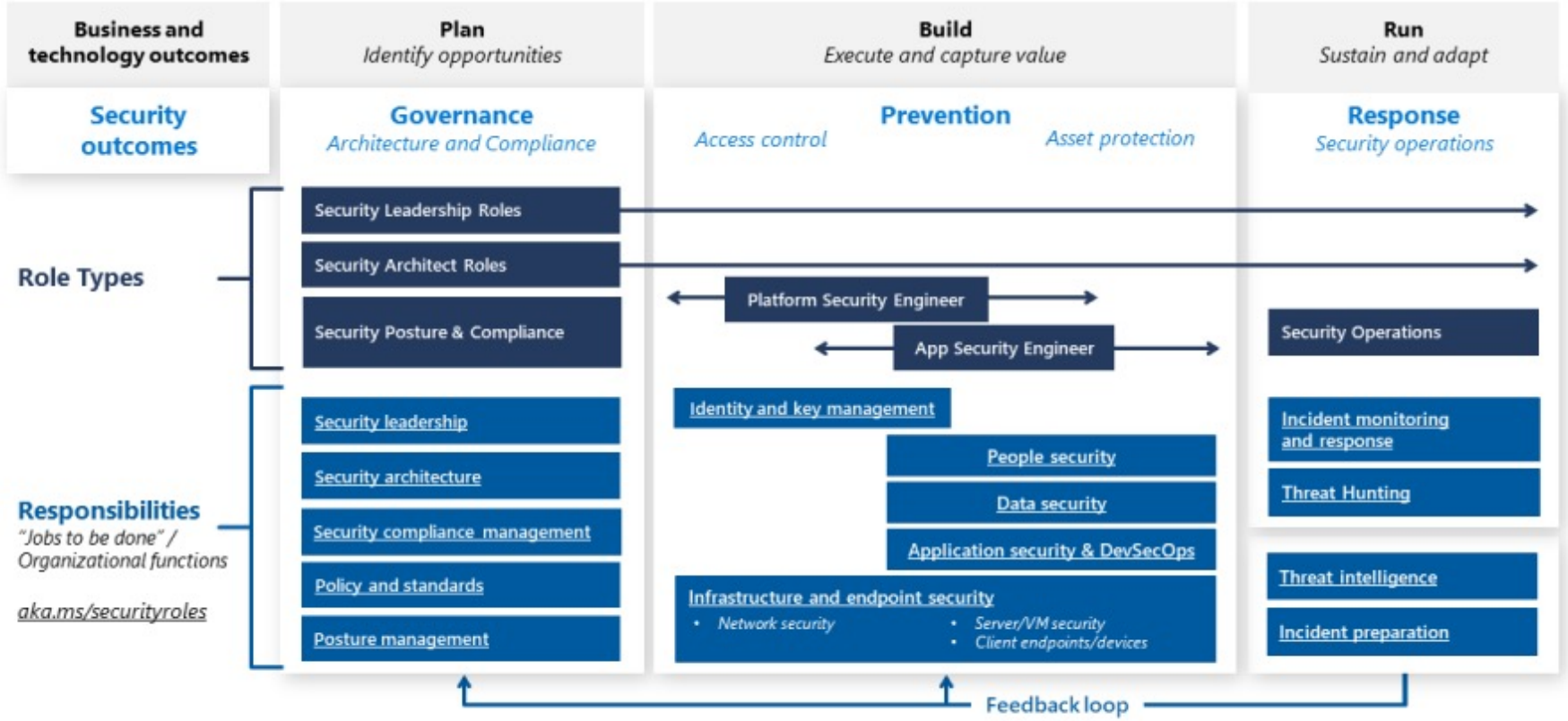
Azure Cloud Adoption Framework

Cloud Adoption Framework is a whitepaper that is a **step by step process** to help organizations plan and migrate their workloads to Azure



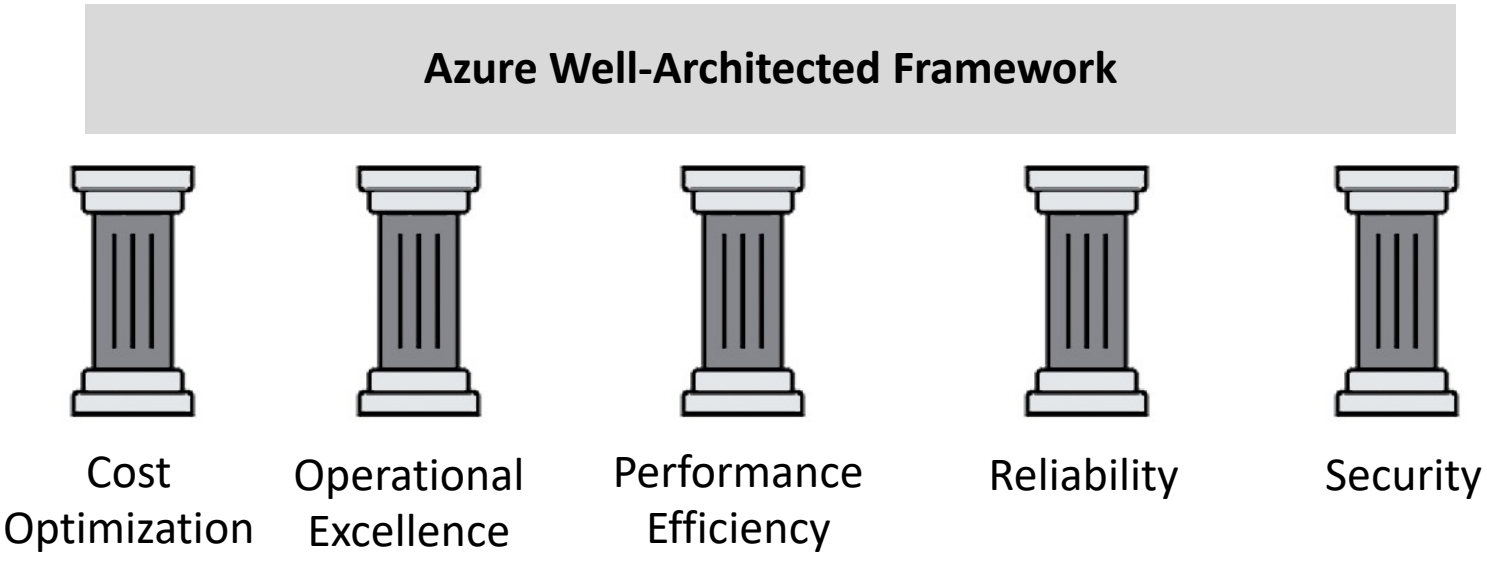
Azure Cloud Adoption Framework

Security Roles and Responsiblities



Azure Well-Architected Framework

Azure Well-Architected Framework describe **best practices for building workloads** on Azure **categorized into 5 pillars**



Cost Optimization — Managing costs to maximize the value delivered.
Operational Excellence — Operations processes that keep a system running in production.
Performance Efficiency — The ability of a system to adapt to changes in load.
Reliability — The ability of a system to recover from failures and continue to function.
Security — Protecting applications and data from threats.

Azure Well-Architected Framework – Security Pillar

These are the topics covered in the **security pillar**

- Role of security
- Security design principles
- Regulatory compliance
- Reduce organizational risk
- Administration
- Application and Services
- Governance, risk, and compliance
- Identity and access management
- Network security and containment
- Security Operations

Azure Well-Architected Framework – Security Pillar

These are the topics we cover in the security pillar

Role of security

security of complex systems depends on understanding the

- Business context
- Social context
- Technical context

- Specialization
  - instead of developing deep expertise for security leverage cloud security offering
- Shared Responsibility Model

Key Strategies:

- Establish a Modern Perimeter
- Modernize Infrastructure Security
- “Trust but Verify” each cloud provider

Security design principles

list of security design principles:

- Align Security Priorities to Mission
- Build a Comprehensive Strategy
- Drive Simplicity
- Design for Attackers
- Leverage Native Controls
- Use Identity as Primary Access Control
- Accountability
- Embrace Automation
- Focus on Information Protection
- Design for Resilience
- Baseline and Benchmark
- Drive Continuous Improvement
- Assume Zero Trust
- Educate and Incentivize Security

Azure Well-Architected Framework – Security Pillar

Types of attacks to resist

What types of attack should the architecture resist? should both resist attacks and recover rapidly from disruption to the security assurances of confidentiality, integrity, and availability. (CIA triad)

critical to discover and prioritize risks based on the mission of the organization via:

- Experience and data
  - leverage existing data in production that could be used in attack to gain experience and prioritize security investment
- Threat modeling
  - new apps don't have real-world data, so you need to model a threat to mitigate possible attachs

Regulatory compliance

recommend working with your regulators and carefully reviewing the standards to understand both the intent and the literal wording

Reduce organizational risk

Three key strategic directions to reducing risk:

1. Building **resilience** into your cybersecurity strategy
   - Identify/Protect
   - Detect/Respond/Recover
2. Strategically **increasing attacker cost**
   - Investment criteria
   - Attack simulation goals
3. Tactically **containing attacker access**.
   - Limit Time in Environment (JIT)
   - Limit Privilege (JeP)
     - Preventive controls
     - Detection/response/recovery

Azure Well-Architected Framework – Security Pillar

Administration

practice of monitoring, maintaining, and operating IT systems

Core strategy for administrative to reduce risk:

- Reduce risk exposure (scope and time)
  - **Scope** – *Just Enough Access (JEA)*
  - **Time** – *Just in Time (JIT)*
  - **Mitigate the remaining risks**
    - eg isolating admin accounts
- Minimize number of critical impact admins
  - Assign at least two accounts to the privileged group for business continuity
  - When two or more accounts are required, provide justification for each member including the original two
  - Regularly review membership & justification for each group member
- Managed and Separate accounts for admins
- No standing access / Just in Time privileges
  - **Just in Time —** Enable Azure AD Privileged Identity Management (PIM)
  - **Break glass —** For rarely used accounts, follow an emergency access process to gain access to the accounts
- Emergency access or 'Break Glass' accounts
- Admin workstation security
- Passwordless or multi-factor authentication for admins
- Enforce conditional access for admins - Zero Trust
- Avoid granular and custom permissions
- Use built-in roles
- Establish lifecycle management for critical impact accounts
- Attack simulation for critical impact accounts

Azure Well-Architected Framework – Security Pillar

Governance, risk, and compliance

Governance: How is org security going to be monitored, audited, and reported?
Risk: What types of risks does the organization face protecting PIIs?
Compliance: Is there a industry, gov, or regulatory requirement org must meet?

- Design/Improve/Sustain
- Prioritize security best practices investments
- Improve and Monitor Secure Score
- Clear lines of responsibility
- Enterprise segmentation strategy
- Security team visibility
- Establish segmentation with management groups
- Use root management group carefully
- Assign privileges for managing the environment
- Segment reference permissions
- Virtual Machine (VM) security updates and strong passwords
- Remove Virtual Machine (VM) direct internet connectivity
- Assign incident notification contact
- Regularly review critical access
- Discover and remediate common risks
- Increase automation with Azure Blueprints
- Evaluate security using benchmarks
- Audit and enforce policy compliance
- Monitor identity Risk
- Penetration testing
- Discover & replace insecure protocols
- Elevated security capabilities

Applications and Service

- Application security considerations
- Application classification
- Threat analysis
- Securing PaaS deployments
- Compliance requirements
- Configuration and dependencies

Storage, data, and encryption

- Use Identity based storage access controls
- Encrypt virtual disk files
- Enable platform encryption services
- Encrypt data in transit

Identity and access management (IAM)

Define clear lines of responsibility and separation of duties for each function. Restrict access based on a need-to-know basis and least privilege security principles.
Assign permissions to users, groups, and applications at a certain scope through Azure RBAC. Use built-in roles when possible.
Prevent deletion or modification of a resource, resource group, or subscription through management locks.

Azure Well-Architected Framework – Security Pillar

Identity and access management (IAM)

- How are you managing the identity for your workload?
  - Define clear lines of responsibility and separation of duties for each function. Restrict access based on a need-to-know basis and least privilege security principles.
  - Assign permissions to users, groups, and applications at a certain scope through Azure RBAC. Use built-in roles when possible.
  - Prevent deletion or modification of a resource, resource group, or subscription through management locks.
  - Use Managed Identities to access resources in Azure.
  - Support a single enterprise directory. Keep the cloud and on-premises directories synchronized, except for critical-impact accounts.
  - Set up Azure AD Conditional Access. Enforce and measure key security attributes when authenticating all users, especially for critical-impact accounts.
  - Have a separate identity source for non-employees.
  - Preferably use passwordless methods or opt for modern password methods.
  - Block legacy protocols and authentication methods.

Azure Well-Architected Framework – Security Pillar

Network security and containment

- Centralize network management and security
- Align network segmentation with enterprise segmentation strategy
- Evolve security beyond network controls
- Build a security containment strategy
- Define an internet edge strategy
- Use of legacy network security technology
  Design virtual network subnet security
- Mitigate DDoS attacks
- Decide upon an internet ingress/egress policy
- Enable enhanced network visibility

Security operations

maintain and restores the security assurances of the system as live adversaries attack it

NIST Cybersecurity Framework functions :

- **Detect** — must detect the presence of adversaries in the system
- **Respond** — rapidly investigate to identify whether it is an actual attack (true positive) or a false alarm (false positive)
- **Recover** — preserve or restore the security assurances (confidentiality, integrity, availability) of business services

- Objective and metrics
- Hybrid enterprise view
- Leverage native detections and controls
- Prioritize alert and log integration

Microsoft Security Best Practices

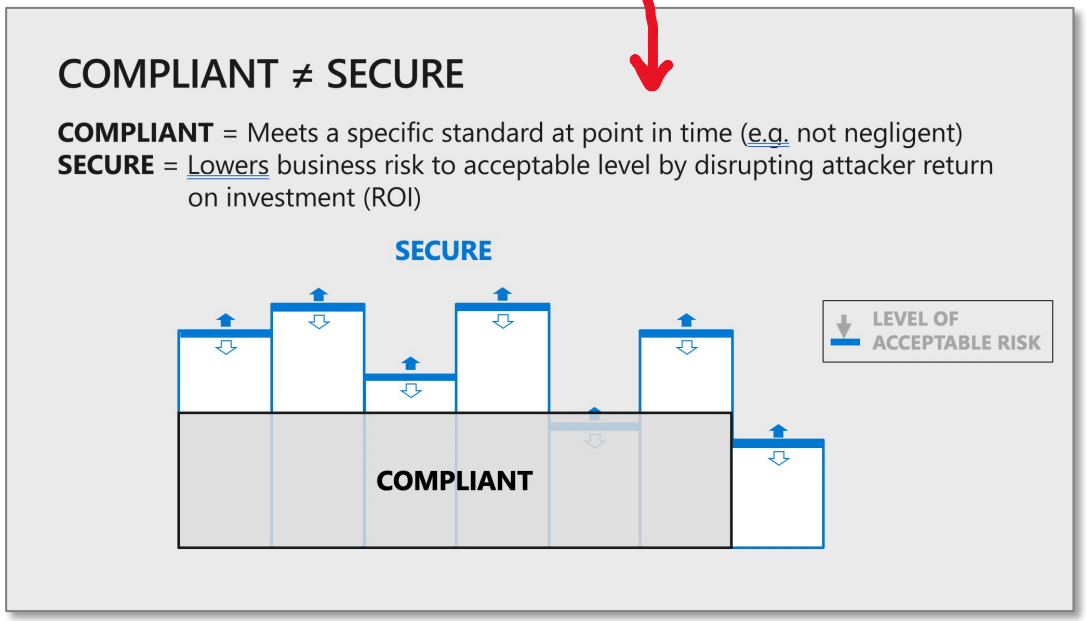
Microsoft Security Best Practices is a collection of best practices that provide clear actionable guidance for security related decisions.

Previously known as Azure Security Compass

The best practices are packaged into a a **series or videos** or you can download all the **power point slides**

The best practices covers the following:

- Governance, risk, and compliance
- Security operations
- Identity and access management
- Network security and containment
- Information protection and storage
- Applications and services



~150 slides

Shared Access Signatures

A shared access signature (SAS) is a URI that grants restricted access rights to **Azure Storage** resources.
Share the URI to grant clients temporary access to specific set of permissions

Types of shared access signatures

Account-level SAS
- access to resources in **one or more** of the storage services

Service-level SAS
- access to single the storage account by using the storage account key

User delegation SAS
- Access to storage account using Azure AD credentials
- Limited only to Blob and Containers
- Microsoft considers this method best practice for accessing via SAS

A shared access signature comes into different formats:

Ad hoc SAS
- the start time, expiry time, and permissions are part of the URI
- Any type of SAS can be an ad hoc SAS

Service SAS with stored access policy:
- A stored access policy is defined on a resource container (limited to blob container, table, queue, or file share)
- The stored access policy can be associated to multiple SAS to manage constraints

Shared Access Signatures

The URI Format itself:

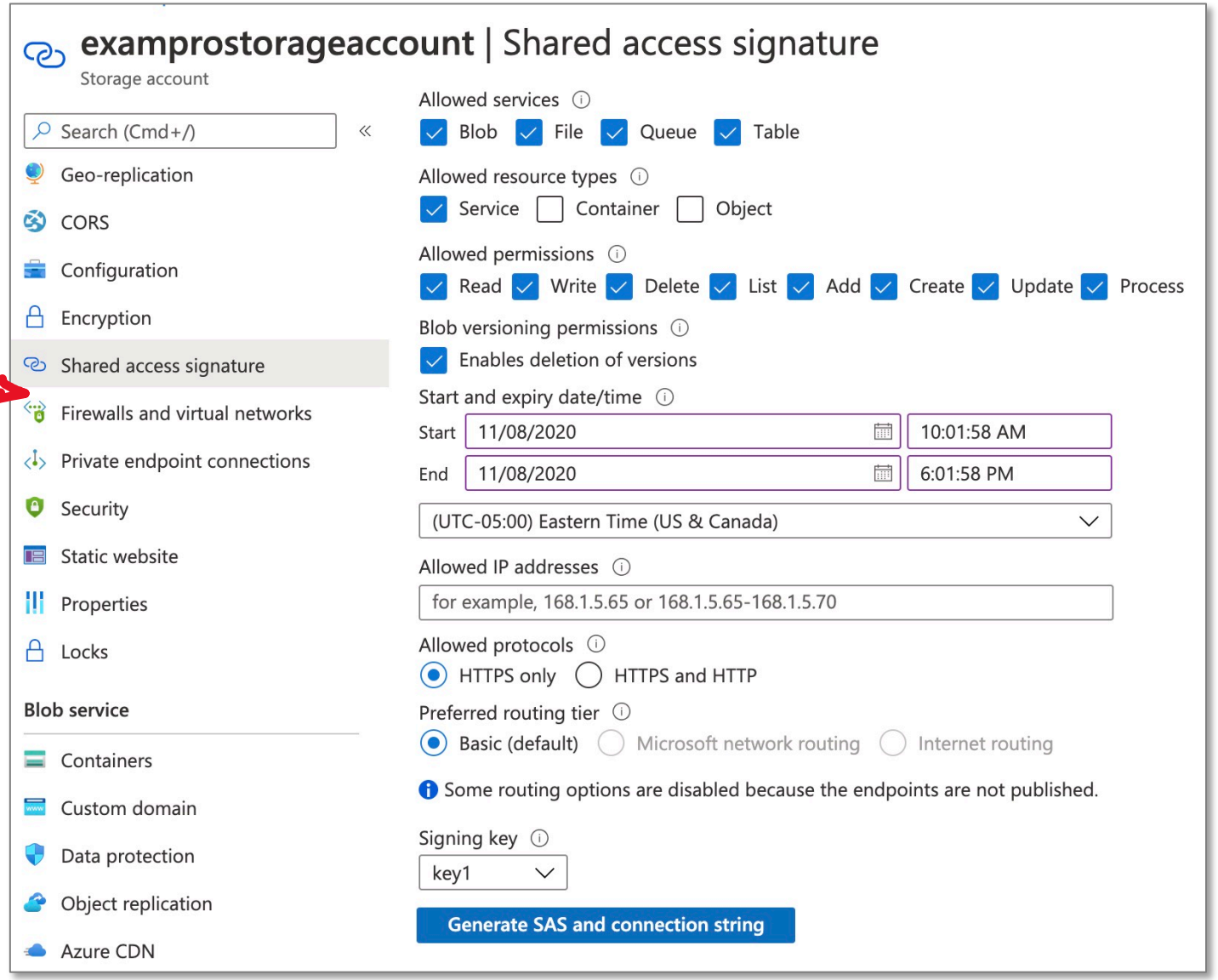
- **Blob URI:** https://myaccount.blob.core.windows.net/mycontainer/myblob.txt
- **sv (Storage services version)** which version of the storage services to use
- **st (Start Time)** the time the SAS becomes valid
- **se (Expiration Time)** the time when the SAS becomes invalid eg. Container (c) or Blob (b)
- **sr (Storage Resource)** if the resource is a blob, queue
- **sp (Permissions)** what operations can be performed against the storage resource eg. Read (r) and Write (w)
- **sig (Signature)** used to authenticate access a SHA256 algorithm

```
https://myaccount.blob.core.windows.net/mycontainer/myblob.txt
?sv=2014-02-14
&st=2014-12-23T22%3A18%3A26Z
&se=2014-12 23T22%3A23%3A26Z
&sr=b
&sp=rw
&sig=Za7816bf8X01cfea414%40We5dae2Y23b00361a39617%a9c
```

Shared Access Signatures

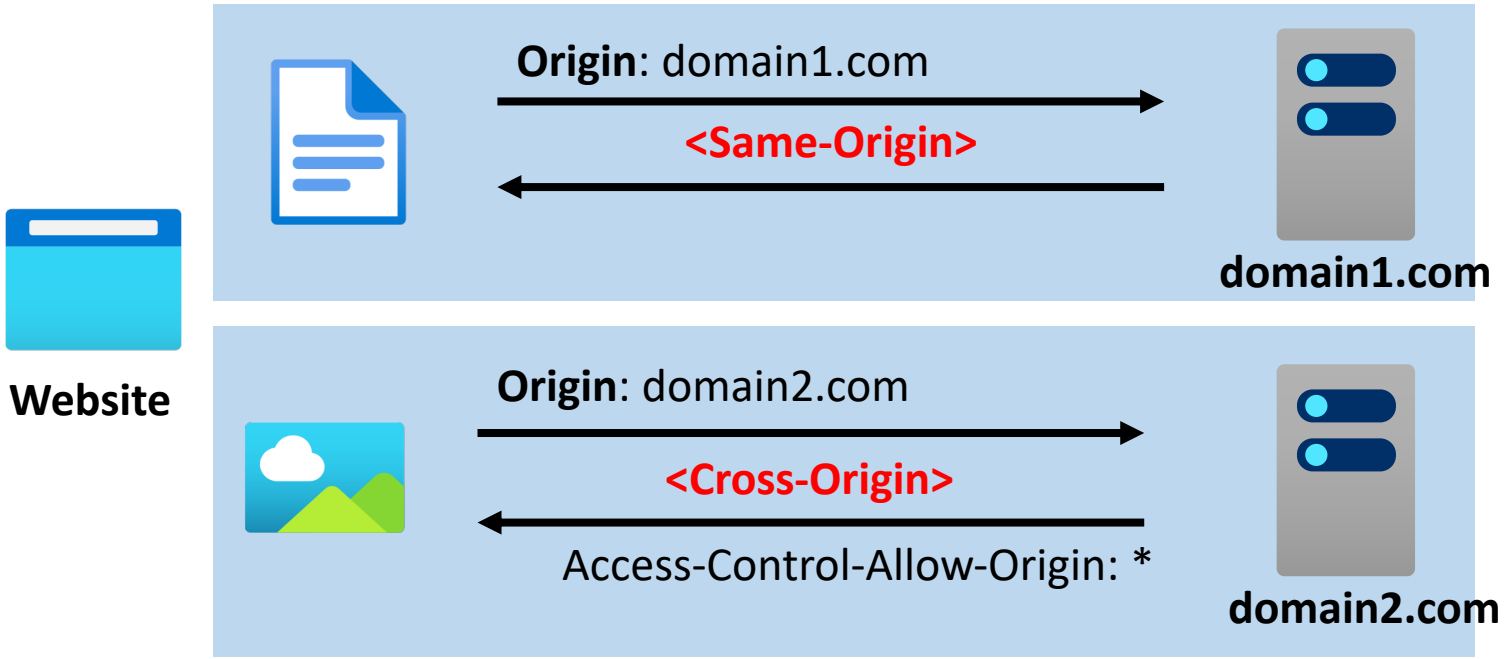
You can **generate** SAS via

- Azure SDK
- Azure **Portal**



Cross-Origin Resource Sharing (CORS)

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any other origins (domain, scheme, or port) than its own from which a browser should permit loading of resources



CORS restrict which websites may access data to be loaded onto its page

Access is controlled via HTTP headers

Request Headers

- Origin
- Access-Control-Request-Method
- Access-Control-Request-Headers

Response Headers

- Access-Control-Allow-Origin
- Access-Control-Allow-Credentials
- Access-Control-Expose-Headers
- Access-Control-Max-Age
- Access-Control-Allow-Methods
- Access-Control-Allow-Headers

Microsoft Security Development Lifecycle (SDL)

Microsoft Security Development Lifecycle (SDL) is an **industry-leading software security assurance process**.

A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture.

Building security into each **SDL phase** of the development lifecycle helps you catch issues early, and it helps you reduce your development costs.

SDL Phases