# Introduction: summary of knowledge

https://docs.microsoft.com/en-us/learn/certifications/exams/sc-900

1. Describe the concepts of security, compliance, and identity (10-15%)
   1.1. Describe security and compliance concepts & methodologies
      1.1.1. describe the Zero-Trust methodology
      1.1.2. describe the shared responsibility model
      1.1.3. define defense in depth
      1.1.4. describe common threats
      1.1.5. describe encryption
      1.1.6. describe cloud adoption framework
   1.2. Define identity concepts
      1.2.1. define identity as the primary security perimeter
      1.2.2. define authentication
      1.2.3. define authorization
      1.2.4. describe what identity providers are
      1.2.5. describe what Active Directory is
      1.2.6. describe the concept of Federated services
      1.2.7. define common Identity Attacks

2. Describe the capabilities of Microsoft identity and access management solutions (30-35%)
   2.1. Describe the basic identity services and identity types of Azure AD
      2.1.1. describe what Azure Active Directory is
      2.1.2. describe Azure AD identities (users, devices, groups, service principals/applications)
      2.1.3. describe what hybrid identity is
      2.1.4. describe the different external identity types (Guest Users)
   2.2. Describe the authentication capabilities of Azure AD
      2.2.1. describe the different authentication methods
      2.2.2. describe self-service password reset
      2.2.3. describe password protection and management capabilities
      2.2.4. describe Multi-factor Authentication
      2.2.5. describe Windows Hello for Business
   2.3. Describe access management capabilities of Azure AD
      2.3.1. describe what conditional access is
      2.3.2. describe uses and benefits of conditional access
      2.3.3. describe the benefits of Azure AD roles
   2.4. Describe the identity protection & governance capabilities of Azure AD
      2.4.1. describe what identity governance is
      2.4.2. describe what entitlement management and access reviews is
      2.4.3. describe the capabilities of PIM
      2.4.4. describe Azure AD Identity Protection
3. Describe the capabilities of Microsoft security solutions (35-40%)
   3.1. Describe basic security capabilities in Azure
      3.1.1. describe Azure Network Security groups

- 3.1.2. describe Azure DDoS protection
- 3.1.3. describe what Azure Firewall is
- 3.1.4. describe what Azure Bastion is
- 3.1.5. describe what Web Application Firewall is
- 3.1.6. describe ways Azure encrypts data

3.2. Describe security management capabilities of Azure
- 3.2.1. describe the Azure Security center
- 3.2.2. describe Azure Secure score
- 3.2.3. describe the benefit and use cases of Azure Defender - previously the cloud workload
- 3.2.4. protection platform (CWPP)
- 3.2.5. describe Cloud security posture management (CSPM)
- 3.2.6. describe security baselines for Azure

3.3. Describe security capabilities of Azure Sentinel
- 3.3.1. define the concepts of SIEM, SOAR, XDR
- 3.3.2. describe the role and value of Azure Sentinel to provide integrated threat protection

3.4. Describe threat protection with Microsoft 365 Defender
- 3.4.1. describe Microsoft 365 Defender services
- 3.4.2. describe Microsoft Defender for Identity (formerly Azure ATP)
- 3.4.3. describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- 3.4.4. describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- 3.4.5. describe Microsoft Cloud App Security

3.5. Describe security management capabilities of Microsoft 365
- 3.5.1. describe the Microsoft 365 Defender portal
- 3.5.2. describe how to use Microsoft Secure Score
- 3.5.3. describe security reports and dashboards
- 3.5.4. describe incidents and incident management capabilities

3.6. Describe endpoint security with Microsoft Intune
- 3.6.1. describe what Intune is
- 3.6.2. describe endpoint security with Intune
- 3.6.3. describe the endpoint security with the Microsoft Endpoint Manager admin center

4. Describe the capabilities of Microsoft compliance solutions (25-30%)

4.1. Describe the compliance management capabilities in Microsoft
- 4.1.1. describe the offerings of the Service Trust portal
- 4.1.2. describe Microsoft's privacy principles
- 4.1.3. describe the compliance center
- 4.1.4. describe compliance manager
- 4.1.5. describe use and benefits of compliance score

4.2. Describe information protection and governance capabilities of Microsoft 365
- 4.2.1. describe data classification capabilities
- 4.2.2. describe the value of content and activity explorer
- 4.2.3. describe sensitivity labels
- 4.2.4. describe Retention Polices and Retention Labels
- 4.2.5. describe Records Management
- 4.2.6. describe Data Loss Prevention

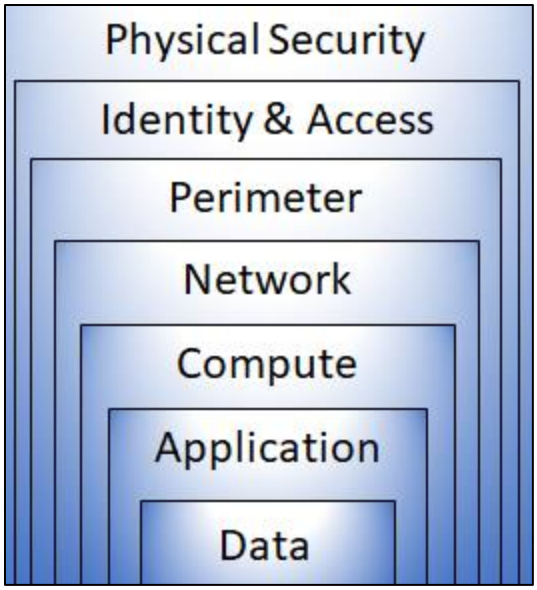
4.3. Describe insider risk capabilities in Microsoft 365
- 4.3.1. describe Insider risk management solution

4.3.2. describe communication compliance
4.3.3. describe information barriers
4.3.4. describe privileged access management
4.3.5. describe customer lockbox
4.4. Describe the eDiscovery and audit capabilities of Microsoft 365
4.4.1. describe the purpose of eDiscovery
4.4.2. describe the capabilities of the content search tool
4.4.3. describe the core eDiscovery workflow
4.4.4. describe the advanced eDiscovery workflow
4.4.5. describe the core audit capabilities of M365
4.4.6. describe purpose and value of Advanced Auditing
4.5. Describe resource governance capabilities in Azure
4.5.1. describe the use of Azure Resource locks
4.5.2. describe what Azure Blueprints is
4.5.3. define Azure Policy and describe its use cases

# 1. Describe the Concepts of Security, Compliance, and Identity

## 1.1. Describe Security and Compliance Concepts & Methodologies

### 1.1.1. Defense in depth




#### 1.1.1.1. Physical Security

1. Data center access

#### 1.1.1.2. Identity and Access Management (IAM)

1. MFA
2. Azure Active directory

3. Conditional Access
4. Azure Identity Protection
5. PIM

#### 1.1.1.3. Perimeter

1. DDoS
2. Azure Firewall

#### 1.1.1.4. Network

1. Network security group

#### 1.1.1.5. Compute

layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.

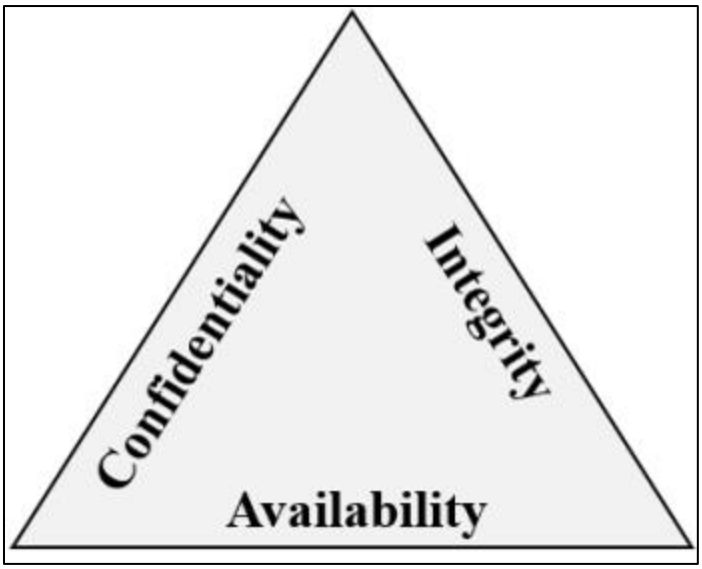
#### 1.1.1.6. Application

layer security to ensure applications are secure and free of security vulnerabilities.

#### 1.1.1.7. Data

layer security including controls to manage access to business and customer data and encryption to protect data.

### 1.1.2. CIA



#### 1.1.2.1. C: Confidentiality

Preserving the access control and disclosure restriction on information guarantying that no one will be breaking the rules of personal privacy and proprietary information.

#### 1.1.2.2. I: Integrity

Integrity is avoiding the unauthorized information modification or destruction and ensuring the non-repudiation and information authenticity

#### 1.1.2.3. A: Availability

Ensure that the information must be available to be accessed and used all the time, that means a reliable access

### 1.1.3. Threats

#### 1.1.3.1. Data Breach (Data)

A data breach is when data is stolen, and this includes personal data. Personal data means any information related to an individual that can be used to identify them directly or indirectly.

Common security threats that can result in a breach of personal data include phishing, spear phishing, tech support scams, SQL injection, and malware designed to steal passwords or bank details.

#### 1.1.3.2. Dictionary Attack Brute force (Identity)

A dictionary attack is a type of identity attack where a hacker attempts to steal an identity by trying a large number of known passwords. Each password is automatically tested against a known username. Dictionary attacks are also known as brute force attacks.

#### 1.1.3.3. Phishing Attack (Identity)

#### 1.1.3.4. Spear Phishing (Identity)

#### 1.1.3.5. Ransomware (Availability)

Malware is the term used to describe malicious applications and code that can cause damage and disrupt normal use of devices. Malware can give attackers unauthorized access, which allows them to use system resources, lock you out of your computer, and ask for ransom.

Ransomware is a type of malware that encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from victims, usually in the form of cryptocurrencies, in exchange for the decryption key.

Cybercriminals that distribute malware are often motivated by money and will use infected computers to launch attacks, obtain banking credentials, collect information that can be sold, sell access to computing resources, or extort payment from victims.

#### 1.1.3.6. Disruptive

##### 1.1.3.6.1. Distributed Denial of Service (DDoS)

(DDoS) attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

##### 1.1.3.6.2. Coin miners

Cybercriminals are always looking for new ways to make money. With the rise of digital currencies, also known as cryptocurrencies, criminals see a unique opportunity to infiltrate an organization and secretly mine for coins by reconfiguring malware.

Mining is the process of running complex mathematical calculations necessary to maintain the blockchain ledger. This process generates coins but requires significant computing resources.

Coin miners aren't inherently malicious. Some individuals and organizations invest in hardware and electric power for legitimate coin mining operations. However, others look for alternative sources of computing power and try to find their way into corporate networks. These coin miners aren't wanted in enterprise environments because they eat up precious computing resources.

##### 1.1.3.6.3. Rootkits

Rootkits intercept and change standard operating system processes. After a rootkit infects a device, you can’t trust any information that the device reports about itself.

##### 1.1.3.6.4. Trojans

Trojans are a common type of malware which can’t spread on their own. This means they either have to be downloaded manually or another malware needs to download and install them. Trojans often use the same file names as real and legitimate apps so it's easy to accidentally download a trojan thinking that it is legitimate.

##### 1.1.3.6.5. Worms

A worm is a type of malware that can copy itself and often spreads through a network by exploiting security vulnerabilities. It can spread through email attachments, text messages, file-sharing programs, social networking sites, network shares, removable drives, and software vulnerabilities.

#### 1.1.3.6.6. Exploits and exploit kits.

Exploits take advantage of vulnerabilities in software. A vulnerability is a weakness in your software that malware uses to get onto your device. Malware exploits these vulnerabilities to bypass your computer's security safeguards and infect your device.

### 1.1.4. Zero Trust

We assume that the network is compromise

#### 1.1.4.1. Verify explicitly

Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.

##### 1.1.4.1.1. Authenticate
##### 1.1.4.1.2. Authorize

#### 1.1.4.2. Least privileged access

Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.

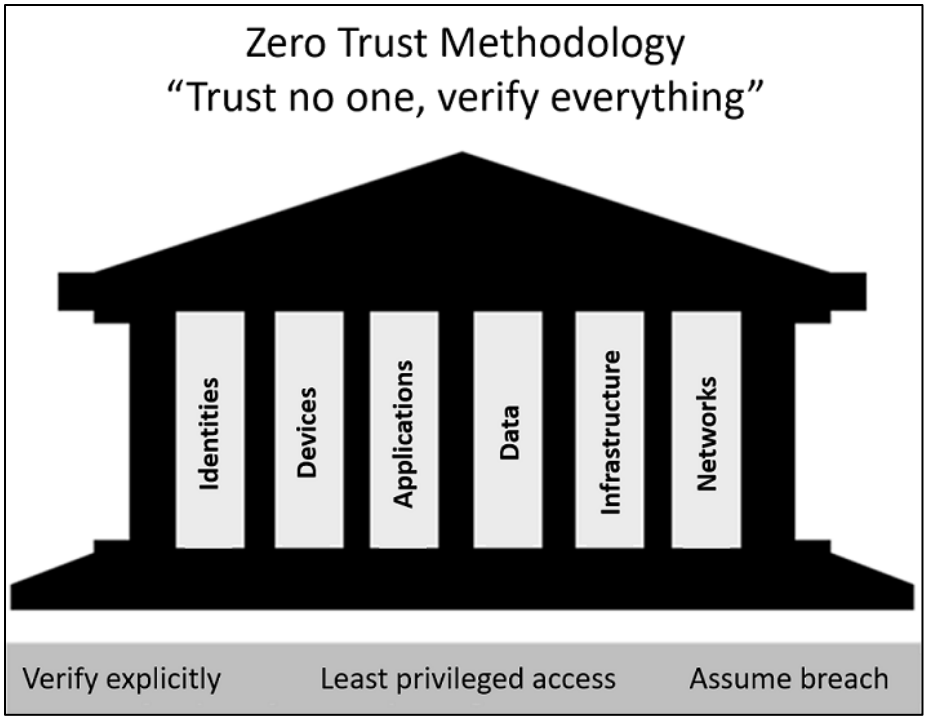
##### 1.1.4.2.1. JIT: Just in time
##### 1.1.4.2.2. JEA: just enough Access

#### 1.1.4.3. Assume breach

Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

##### 1.1.4.3.1. Segmentation Network
##### 1.1.4.3.2. Encryption
##### 1.1.4.3.3. Detect Threats

#### 1.1.4.4. Six Foundational Pillars




#### 1.1.4.4.1. Identities

Identities may be:

- Users
- Services
- devices.

When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.

#### 1.1.4.4.2. Devices

Devices create a large attack surface as data flows from devices to on-premises workloads and the cloud.

Monitoring devices for health and compliance is an important aspect of security.

#### 1.1.4.4.3. Applications

Applications are the way that data is consumed.

This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally.

This pillar also includes managing permissions and access.

#### 1.1.4.4.4. Data

Data based on his attributes should be:

- Classified
- labeled,
- encrypted

Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.

#### 1.1.4.4.5. Infrastructure

Infrastructure whether on-premises or cloud based, represents a threat vector.

To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies.

This allows you to automatically block or flag risky behavior and take protective actions.

#### 1.1.4.4.6. Networks

Networks should be segmented, including deeper in-network micro segmentation.

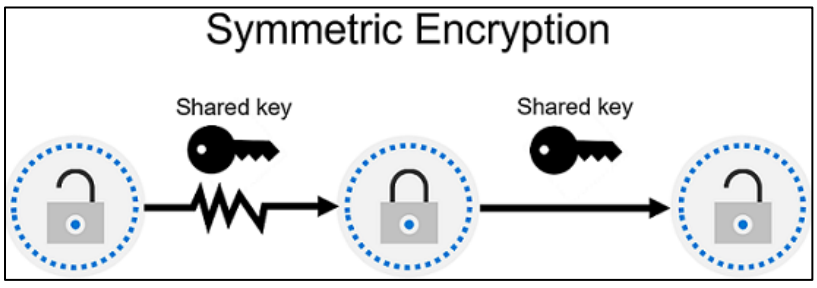
Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

## 1.1.5. Encryption

### 1.1.5.1. Encryption types

#### 1.1.5.1.1. Symmetric

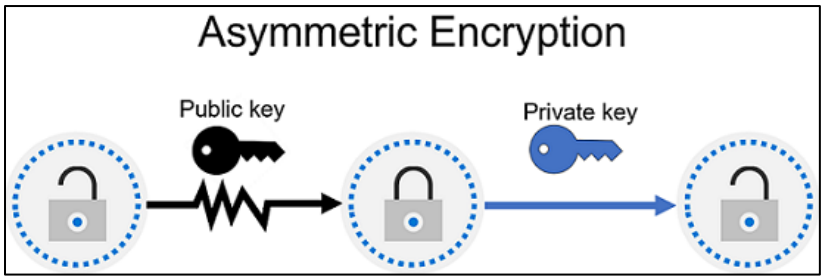
Symmetric encryption uses the same key to encrypt and decrypt the data.



#### 1.1.5.1.2. Asymmetric

Asymmetric encryption uses a public key and private key pair.

Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, you need a paired key. Asymmetric encryption is used for things like Transport Layer Security (TLS), such as the HTTPS protocol, and data signing. Encryption may protect data at rest, or in transit.




### 1.1.5.2. Encryption at Rest

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

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

### 1.1.5.3. Encryption in transit

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

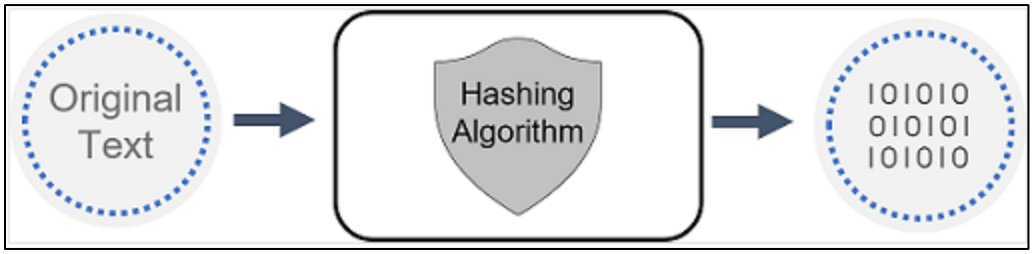
Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

### 1.1.5.4. Hashing (integrity)

Hashing uses an algorithm to convert the original text to a unique fixed-length hash value. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

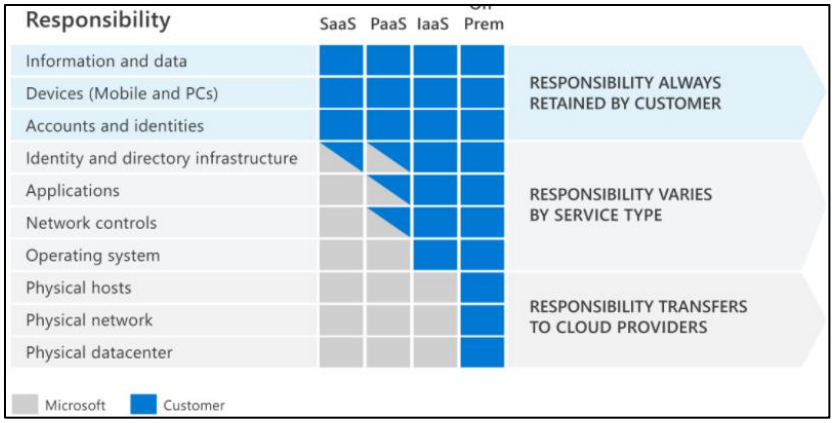
Hashing is used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. To mitigate this risk, passwords are often "salted". This refers to adding a fixed-length random value to the input of hash functions to create unique hashes for every input. As hackers can't know the salt value, the hashed passwords are more secure.




### 1.1.6. Shared Responsibility Model

The responsibilities vary depending on where the workload is hosted:

| Responsibility | On-premises | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Data governance and Rights Management | Customer | Customer | Customer | Customer |
| Client endpoints | Customer | Customer | Customer | Customer |
| Account and access management | Customer | Customer | Customer | Customer |
| Identity and directory Infrastructure | Customer | Customer | Microsoft/ Customer | Microsoft/ Customer |
| Application | Customer | Customer | Microsoft/ Customer | Microsoft |
| Network controls | Customer | Customer | Microsoft/ Customer | Microsoft |
| Operating system | Customer | Customer | Microsoft | Microsoft |
| Physical hosts | Customer | Microsoft | Microsoft | Microsoft |
| Physical network | Customer | Microsoft | Microsoft | Microsoft |
| Physical datacenter | Customer | Microsoft | Microsoft | Microsoft |




### 1.1.6.1. Hosted Application Types

#### 1.1.6.1.1. Software as a Service (SaaS)

SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics CRM Online are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources.

In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

#### 1.1.6.1.2. Platform as a Service (PaaS)

PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

#### 1.1.6.1.3. Infrastructure as a Service (IaaS)

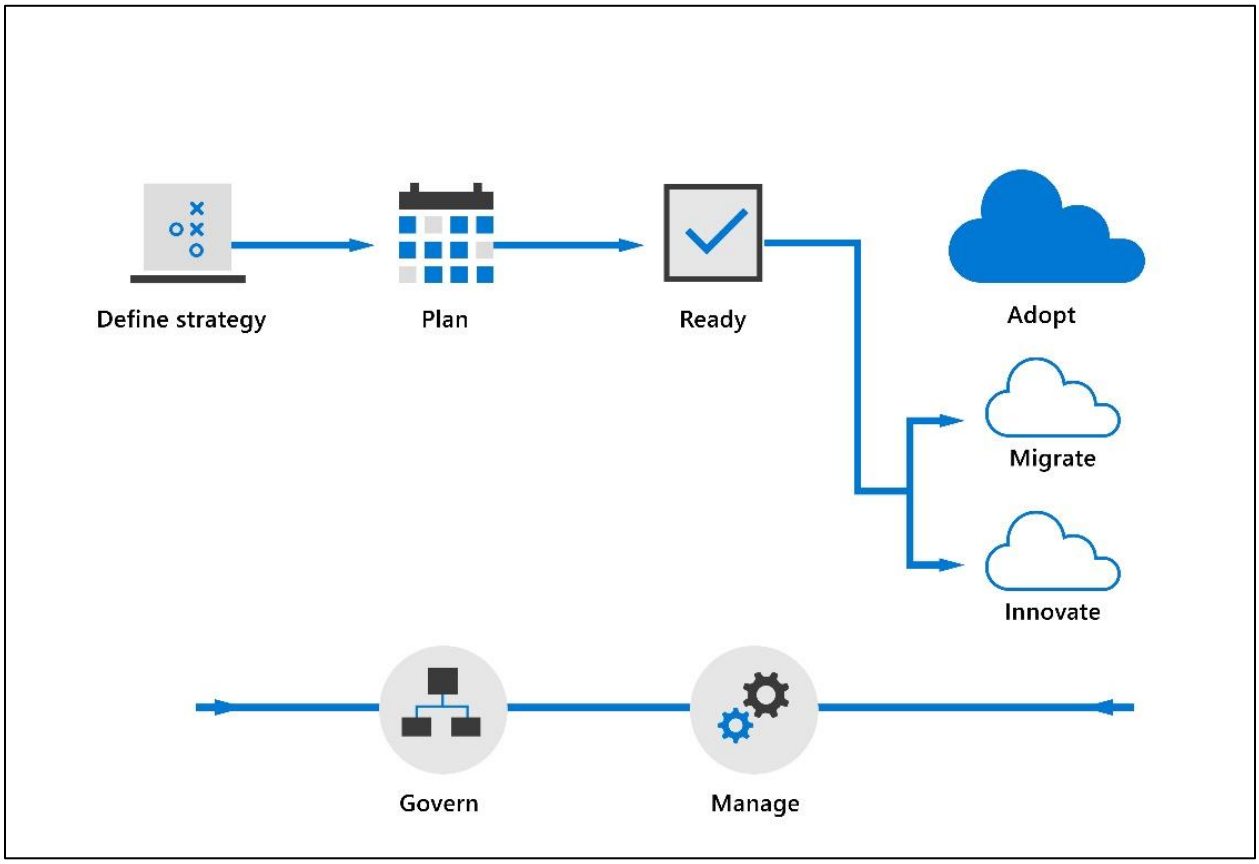
Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider's computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers and the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components such as operating systems, network controls, applications, and protecting data.

#### 1.1.6.1.4. On-premises datacenter (On-prem)

In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.

### 1.1.7. Cloud Adoption Framework (CAF)

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/




#### 1.1.7.1. Strategy

Strategy: define business justification and expected outcomes of adoption.

#### 1.1.7.2. Plan

Plan: align actionable adoption plans to business outcomes.

#### 1.1.7.3. Ready

Ready: Prepare the cloud environment for the planned changes.

#### 1.1.7.4. Adopt

##### 1.1.7.4.1. Migrate

Migrate and modernize existing workloads.

##### 1.1.7.4.2. Innovate

Develop new cloud-native or hybrid solutions.

#### 1.1.7.5. Govern

Govern the environment and workloads.

#### 1.1.7.6. Manage

Manage: Operations management for cloud and hybrid solutions.

# 2. Describe the Capabilities of Microsoft identity and access management solutions

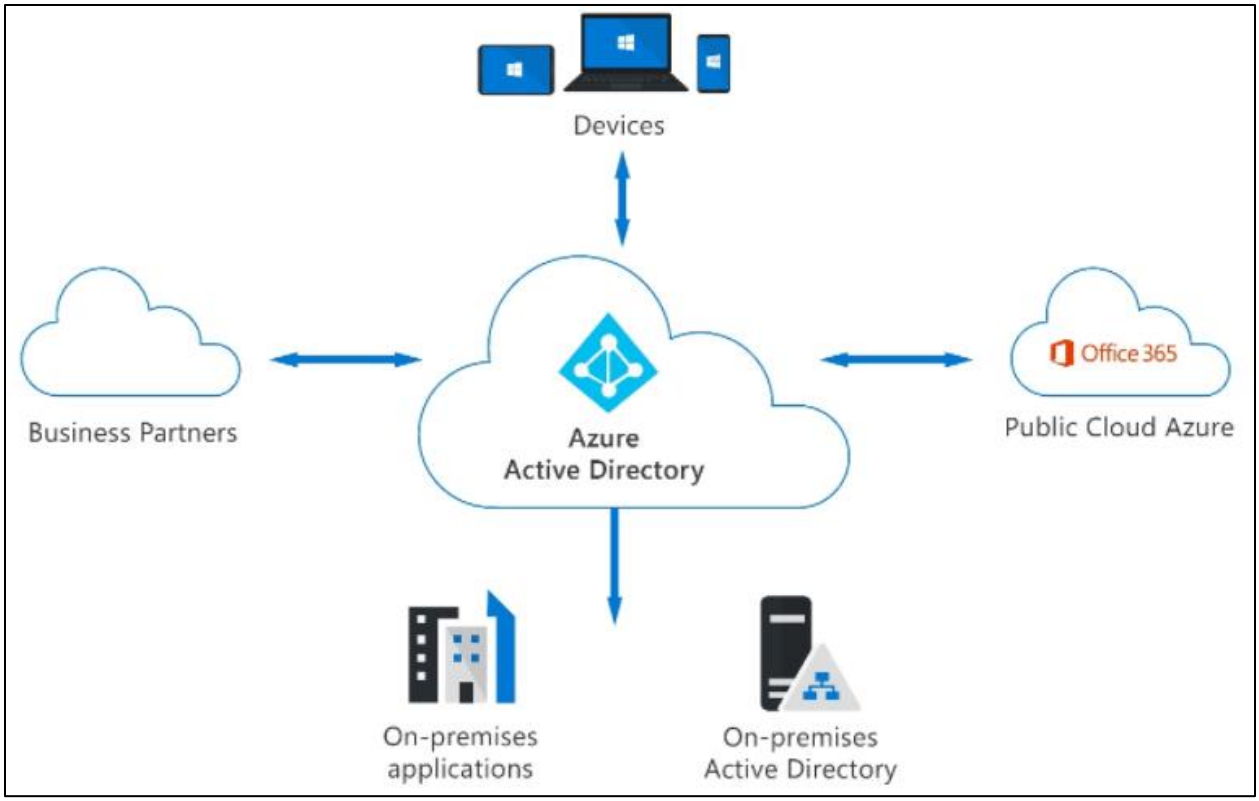
## 2.1. Azure Active Directory (IdP)

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Organizations use Azure AD to enable their employees, guests, and others to sign in and access the resources they need, including:

- Internal resources, such as apps on your corporate network and intranet, and cloud apps developed by your own organization.
- External services, such as Microsoft Office 365, the Azure portal, and any SaaS applications used by your organization.

Azure AD simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications. Azure AD can be synchronized with your existing on-premises Active Directory, synchronized with other directory services, or used as a standalone service.

Azure AD also allows organizations to securely enable the use of personal devices, such as mobiles and tablets, and enable collaboration with business partners and customers.




Developers use Azure AD as a standards-based approach for adding single sign-on (SSO) to their apps, so that users can sign in with their pre-existing credentials. Azure AD also provides APIs that allow developers to build personalized app experiences using existing organizational data.

### 2.1.1. Azure Active Directory Pricing options

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

| Purchase Method | Premium P1 | Premium P2 | Free | Office 365 apps |
|---|---|---|---|---|
| Microsoft Representative | Included with Microsoft 365 | Included with Microsoft 365 | Included with Microsoft 365 | Included with Microsoft 365 |
| Online | $6 user/month* | $9 user/month* | Included with Microsoft 365 | Included with Microsoft 365 |

| | | Free | Office 365 Apps | Premium P1 | Premium P2 |
|---|---|---|---|---|---|
| CORE IDENTITY AND ACCESS MANAGEMENT (IAM) | Directory Objects[1] | 500,000 Object Limit | No Object Limit | No Object Limit | No Object Limit |
| | Single sign-on (SSO) (unlimited)[2] | ✔ | ✔ | ✔ | ✔ |
| | User provisioning | ✔ | ✔ | ✔ | ✔ |
| | Federated authentication (AD Federation Services or third-party identity provider) | ✔ | ✔ | ✔ | ✔ |
| | User and group management (add/update/delete) | ✔ | ✔ | ✔ | ✔ |
| | Device registration | ✔ | ✔ | ✔ | ✔ |
| | Cloud authentication (pass-through authentication, password hash synchronization, seamless SSO) | ✔ | ✔ | ✔ | ✔ |
| | Azure AD Connect sync (extend on-premises directories to Azure AD) | ✔ | ✔ | ✔ | ✔ |
| | Self-service password change for cloud users | ✔ | ✔ | ✔ | ✔ |
| | Azure AD Join: desktop SSO and administrator BitLocker recovery | ✔ | ✔ | ✔ | ✔ |
| | Password protection (global banned password) | ✔ | ✔ | ✔ | ✔ |
| | Multifactor authentication (MFA)[3] | ✔ | ✔ | ✔ | ✔ |
| | Basic security and usage reports | ✔ | ✔ | ✔ | ✔ |
| EXTERNAL IDENTITIES | Secure and manage customers and partners* | No charge for first 50,000 monthly active users. | No charge for first 50,000 monthly active users. | No charge for first 50,000 monthly active users; then $0.00325 per monthly active user. | No charge for first 50,000 monthly active users; then $0.01625 per monthly active user. |

| | | | | | |
|---|---|---|---|---|---|
| IAM FOR OFFICE 365 APPS | Company branding (customization of login and logout pages, access panel) | | ✔ | ✔ | ✔ |
| | Self-service password reset for cloud users | | ✔ | ✔ | ✔ |
| | Service-level agreement | | ✔ | ✔ | ✔ |
| | Device write-back (device objects two-way synchronization between on-premises directories and Azure) | | ✔ | ✔ | ✔ |
| PREMIUM FEATURES | Password protection (custom banned password) | | | ✔ | ✔ |
| | Password protection for Windows Server Active Directory (global and custom banned password) | | | ✔ | ✔ |
| | Self-service password reset/change/unlock with on-premises write-back | | | ✔ | ✔ |
| | Group access management | | | ✔ | ✔ |
| | Microsoft Cloud App Discovery[4] | | | ✔ | ✔ |
| | Azure AD Join: mobile device management auto enrollment and local admin policy customization | | | ✔ | ✔ |
| | Azure AD Join: self-service BitLocker recovery, enterprise state roaming | | | ✔ | ✔ |
| | Advanced security and usage reports | | | ✔ | ✔ |
| HYBRID IDENTITIES | Application Proxy | | | ✔ | ✔ |
| | Microsoft Identity Manager user Client Access License[5] | | | ✔ | ✔ |
| | Connect Health[6] | | | ✔ | ✔ |
| ADVANCED GROUP ACCESS MANAGEMENT | Dynamic groups | | | ✔ | ✔ |
| | Group creation permission delegation | | | ✔ | ✔ |
| | Group naming policy | | | ✔ | ✔ |
| | Group expiration | | | ✔ | ✔ |
| | Usage guidelines | | | ✔ | ✔ |
| | Default classification | | | ✔ | ✔ |

| | | | | | |
|---|---|---|---|---|---|
| CONDITIONAL ACCESS | Conditional access based on group, location and device status | | | ✔ | ✔ |
| | Azure Information Protection integration | | | ✔ | ✔ |
| | SharePoint limited access | | | ✔ | ✔ |
| | Terms of Use (set up for specific access) | | | ✔ | ✔ |
| | MFA with conditional access | | | ✔ | ✔ |
| | Microsoft Cloud App Security integration | | | ✔ | ✔ |
| | Third-party identity governance partners integration | | | ✔ | ✔ |
| IDENTITY PROTECTION | Vulnerabilities and risky accounts detection | | | | ✔ |
| | Risk events investigation | | | | ✔ |
| | Risk-based conditional access policies | | | | ✔ |
| IDENTITY GOVERNANCE | Privileged Identity Management | | | | ✔ |
| | Access reviews | | | | ✔ |
| | Entitlement management | | | | ✔ |
| PRICE | | Free | O365 E1, E3, E5, F3 | $6 per user, per month | $9 per user, per month |

#### 2.1.1.1. Azure Active Directory Free.

The free version allows you to:

1. Administer users create groups
2. Synchronize with on-premises Active Directory
3. Create basic reports
4. Configure self-service password change for cloud users
5. Enable single sign-on across Azure, Microsoft 365, and many popular SaaS apps.

The free edition is included with subscriptions to Office 365, Azure, Dynamics 365, Intune, and Power Platform.

#### 2.1.1.2. Office 365 Apps.

The Office 365 Apps edition allows you to do everything included in the free version, plus:

1. Self-service password reset for cloud users
2. Devices write-back
   2.1. which offers two-way synchronization between on-premises directories and Azure AD.

The Office 365 Apps edition of Azure Active Directory is included in subscriptions to Office 365 E1, E3, E5, F1, and F3.

#### 2.1.1.3. P1 Azure Active Directory Premium P1.

The Premium P1 edition includes all the features in the free and Office 365 apps editions. It also supports:

Advanced administration such as:

1. Dynamic groups
2. self-service group management
3. Microsoft Identity Manager
   3.1. an on-premises identity and access management suite
4. Cloud write-back capabilities
   4.1. which allow self-service password reset for your on-premises users.
5. Microsoft Cloud App Discovery

#### 2.1.1.4. P2 Azure Active Directory Premium P2.

P2 offers all the Premium P1 features, and:

1. Azure Active Directory Identity Protection
   1.1. This help provide risk-based Conditional Access to your apps and critical company data.

2. Access review
3. Privileged Identity Management PIM
    3.1.1. Discover
    3.1.2. Restrict
    3.1.3. Monitor administrators and their access to resources,
    3.1.4. Provide just-in-time (JIT)access when needed.

#### 2.1.1.5. "Pay as you go" feature licenses.

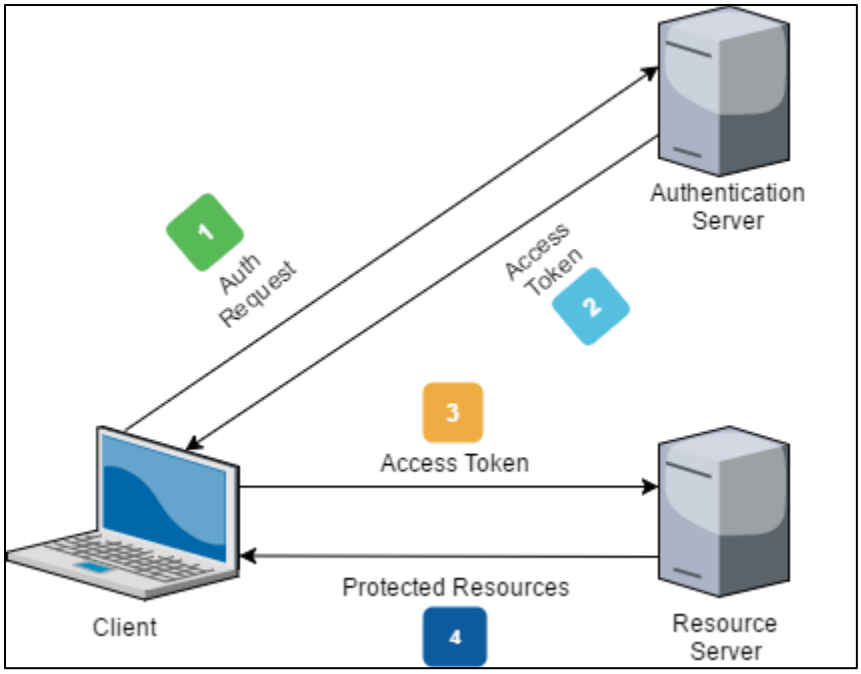
You can get other feature licenses separately, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps.

### 2.1.2. Modern Authentication

*Modern Authentication* is a method of identity management that offers more secure user authentication and authorization.

Modern authentication is an umbrella term for a combination of authentication and authorization methods between a client (for example, your laptop or your phone) and a server, as well as some security measures that rely on access policies that you may already be familiar with. It includes:

- **Authentication methods**: Multi-factor authentication (MFA); smart card authentication; client certificate-based authentication
- **Authorization methods**: Microsoft's implementation of Open Authorization (OAuth) (token issuance)
- **Conditional access policies**: Mobile Application Management (MAM) and Azure Active Directory (Azure AD) Conditional Access




#### 2.1.2.1. Identity Protocols

The identity provider keeps users' identity records. For example, it can be Windows Active Directory in a business setting, or a social media site such as Facebook, Google, or Twitter for consumer applications.

Identity protocols supply information about a user — such as a persistent identifier, phone or email address — that may be used for long-term identification of that user to your system and hence for authenticating the user and authorizing access to resources.

In the same way that someone must show their driver's license in order to enter a bar, an identity provider uses a set of instructions to verify users' digital identity to a service provider so they can gain entrance into a specific system or application. With standardized protocols to assure interoperability when exchanging information, authentication protocols help organizations centralize authentication, while enabling users to access the resources they need without having to memorize numerous usernames and passwords.

##### 2.1.2.1.1. OpenID Connect: OIDC

an identity layer that sits on top of OAuth 2 and allows for easy verification of the user's identity, as well as the ability to get basic profile information from the identity provider.

For authenticating consumer websites and mobile applications, OIDC may be the right choice because of its lightweight, easy-to-implement JSON security tokens.

OIDC is a simple identity layer on top of 0Auth 2.0, an authorization framework managed by the OpenID Foundation. The protocol uses RESTful API communication to transmit JSON web tokens

between the identity provider and service provider, which contain common claims such as the user's name, email address, birth date, picture, and other personal data. The tokens are digitally signed and can be encrypted as needed.

OIDC is easy to integrate with simple apps, but also provides security options that adhere to rigorous enterprise requirements. OIDC's easy-to-consume tokens support a broad spectrum of signature and encryption algorithms.

OIDC is easy to implement with lightweight data processing requirements, which makes it the preferred authentication standard for mobile games, social media integrations, and other mobile applications.

OIDC benefits from the use of JSON and the simpler use by mobile apps, compared to SAML

#### 2.1.2.1.2. SAML2.0 Security Assertion Markup Language

an open-standard, XML-based data format that allows businesses to communicate user authentication and authorization information to partner companies and enterprise applications their employees may use.

For authenticating enterprise applications, SAML has a long track record of secure data exchange and may be the preferred standard.

It uses XML language as its identity data format and simple HTTP and SOAP for its data transport mechanisms.

SAML provides communication between identity providers and service providers using encrypted, digitally signed XML-based certificates. When a user is authenticated, a package of user identity data, known as the "SAML Assertion" is issued from the identity provider to the service provider and can include attributes such as a name, phone number, and email address. As an XML-based protocol, SAML is a feature-rich, versatile standard that can be used on nearly every platform.

It is widely used for Software-as-a-Service (SaaS) solutions and in single-sign on (SSO) applications, particularly in business settings where users need to unlock their computer screens or log in to the corporate intranet and several enterprise applications using a single username and password.

Where strong security is a requirement, SAML is generally a good choice. All aspects of the exchange between the RP and IdP can be digitally signed and verified by both parties. This provides high assurance that each party is communicating with the correct counterpart and not an imposter. In addition, the assertion from the IdP may be encrypted, so that HTTPS is not the only protection against attackers accessing users' data. To add further security, signing and encryption keys may be rotated regularly.

#### 2.1.2.2. Authentication Protocols

Authentication protocols do not necessarily carry a personal identifier.

Who I am

##### 2.1.2.2.1. Tacacs
##### 2.1.2.2.2. Radius
##### 2.1.2.2.3. Diameter
##### 2.1.2.2.4. Kerberos

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.

#### 2.1.2.3. Authorization Protocols

provide a means to acquire access-protected resources without requiring the resource owner to share credentials. Interactive user consent is an important aspect of these protocols.

What I can do

##### 2.1.2.3.1. OAuth2 Open Authorization

OAuth2 is the industry-standard protocol for authorization.

The OAuth2 protocol is often used, casually, for identity and authentication using user data, such as an identifier, returned in the OAuth2 process.

an authorization standard that allows a user to grant limited access to their resources on one site to another site, without having to expose their credentials. You use this standard every time you log in to a site using your Google account and you are asked if you agree with sharing your email address and your contacts list with that site.

##### 2.1.2.3.2. UMA
#### 2.1.2.4. Audit

What have I done?

### 2.1.3. AAD Identity types
#### 2.1.3.1. User

A user identity is a representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

### 2.1.3.2. Service Principal

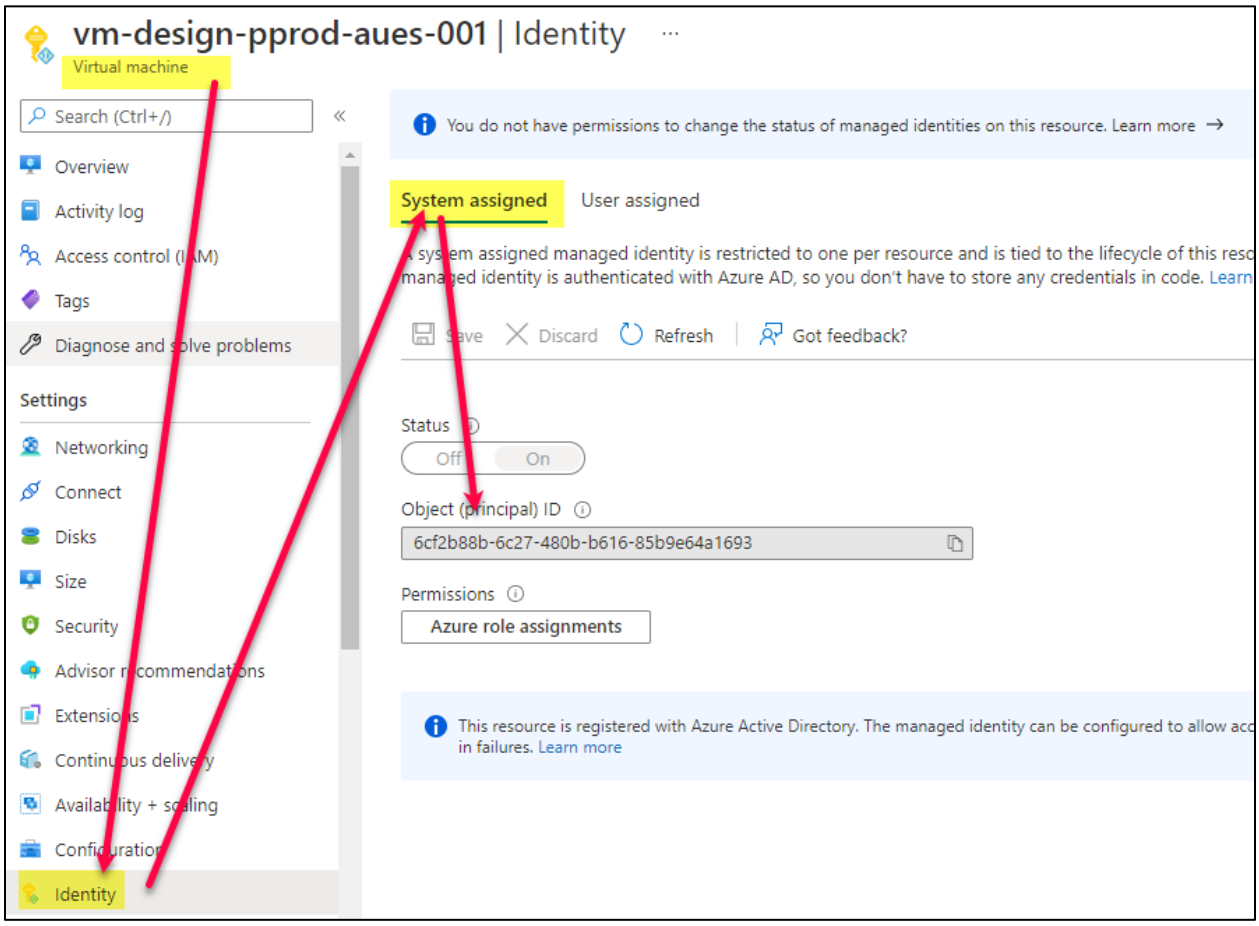
A service principal is a security identity used by applications or services to access specific Azure resources. You can think of it as an identity for an application.

### 2.1.3.3. Manage Identity

A managed identity is automatically managed in Azure AD. Managed identities are typically used to manage the credentials for authenticating a cloud application with an Azure service.

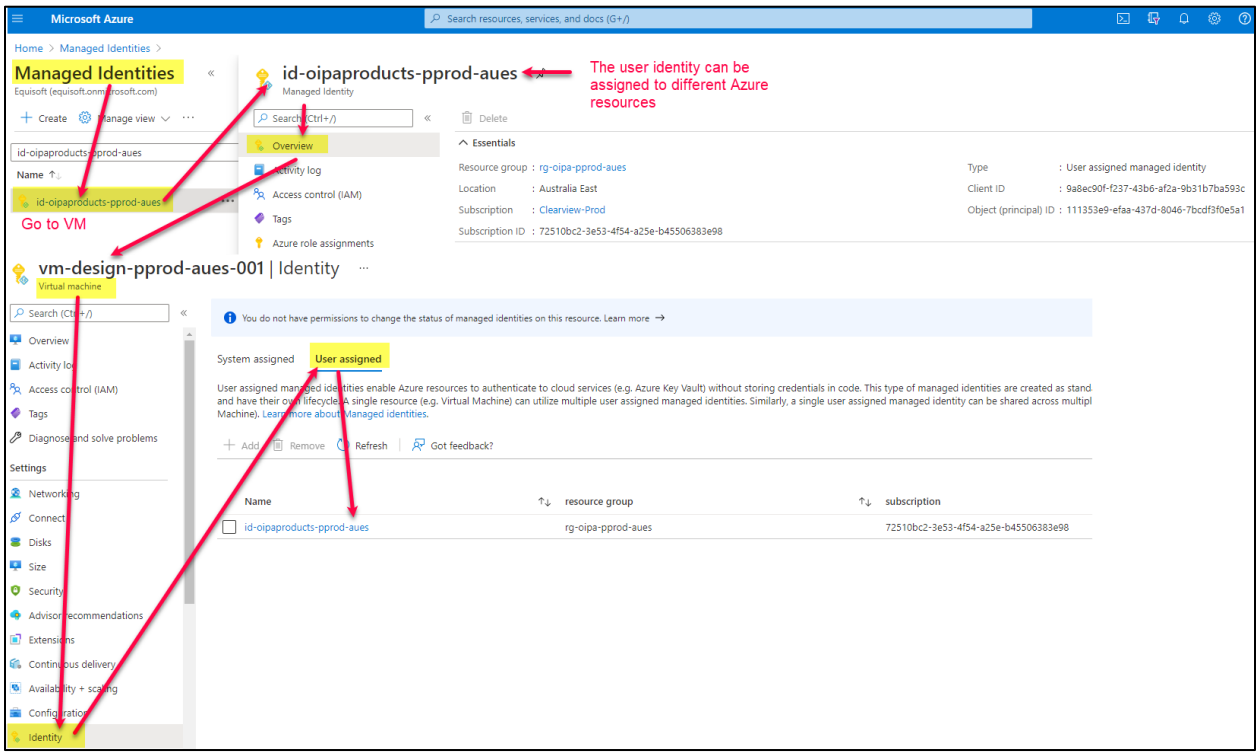
#### 2.1.3.3.1. MSI System Assigned

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



### 2.1.3.3.2. MSI User Assigned

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




### 2.1.3.4. Device

A device is a piece of hardware, such as mobile devices, laptops, servers, or printer. Device identities can be set up in different ways in Azure AD, to determine properties such as who owns the device. Managing devices in Azure AD allows an organization to protect its assets by using tools such as Microsoft Intune to ensure standards for security and compliance. Azure AD also enables single sign-on to devices, apps, and services from anywhere through these devices.

IT admins can use tools like **Microsoft Intune**, a mobile device management (MDM) solution, to manage devices.

There are multiple options for getting devices into Azure AD:

#### 2.1.3.4.1. Azure AD registered devices

Azure AD registered devices can be Windows 10, iOS, Android, or macOS devices. Devices that are Azure AD registered are typically **owned personally**, rather than by the organization.

They're signed in with a personal Microsoft account or another local account.

#### 2.1.3.4.2. Azure AD joined devices

Azure AD joined devices exist only in the cloud. Azure AD joined devices are **owned by an organization** and signed in with their account.

Users sign into their devices with their Azure AD or synced Active Directory work or school accounts.

You can configure Azure AD joined devices for all Windows 10 devices (except Windows 10 Home).

#### 2.1.3.4.3. Hybrid Azure AD joined devices

Hybrid Azure AD joined devices can be Windows 7, 8.1, or 10, or Windows Server 2008, or newer.

Devices that are hybrid Azure AD joined are owned by an organization and **signed in with an Active Directory Domain Services** account belonging to that organization. They exist in the cloud and on-premises.

### 2.1.4. AAD External Identities

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

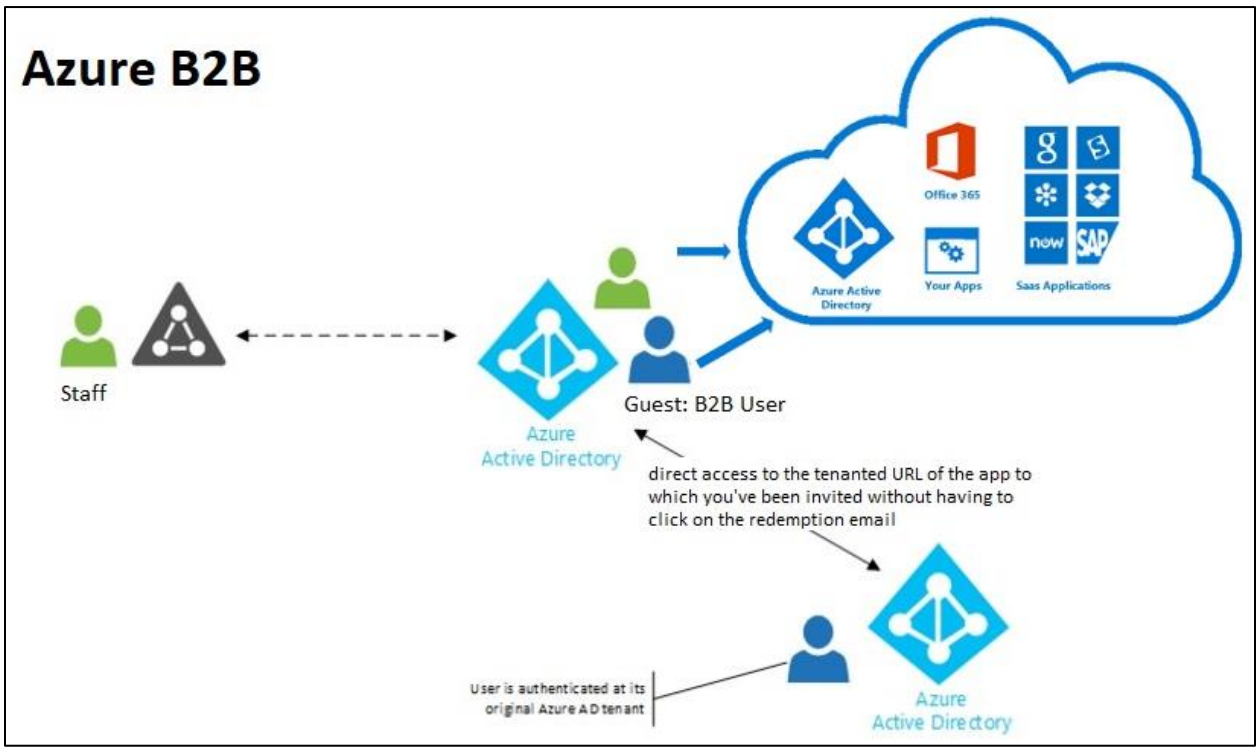
This ability for external users is enabled through Azure AD support of external identity providers like other Azure AD tenants, Facebook, Google, or enterprise identity providers. Admins can set up federation with identity providers so your external users can sign in with their existing social or enterprise accounts instead of creating a new account just for your application.

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

#### 2.1.4.1. B2B Collaboration (Remote AAD)

B2B collaboration allows you to share your organization's applications and services with guest users from other organizations, while maintaining control over your own data. B2B collaboration uses an invitation and redemption process, allowing external users to access your resources with their credentials. Developers can customize the invitation and redemption process using Azure AD business-to-business APIs.

With B2B collaboration, external users are managed in the same directory as employees but are typically annotated as guest users. Guest users can be managed in the same way as employees, added to the same groups, and so on. With B2B, SSO to all Azure AD-connected apps is supported.

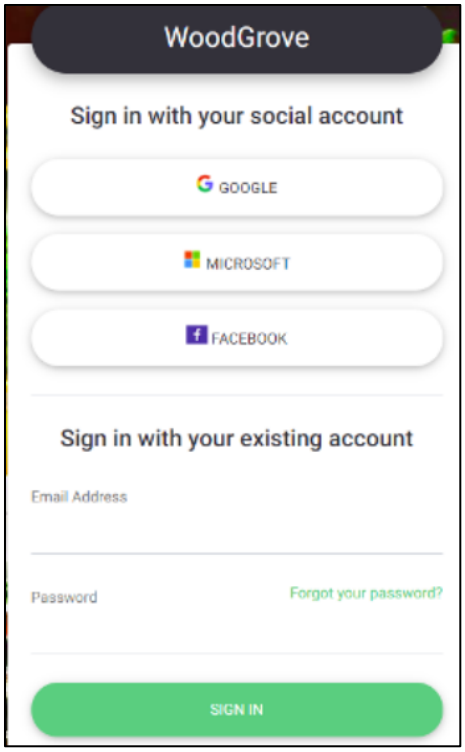


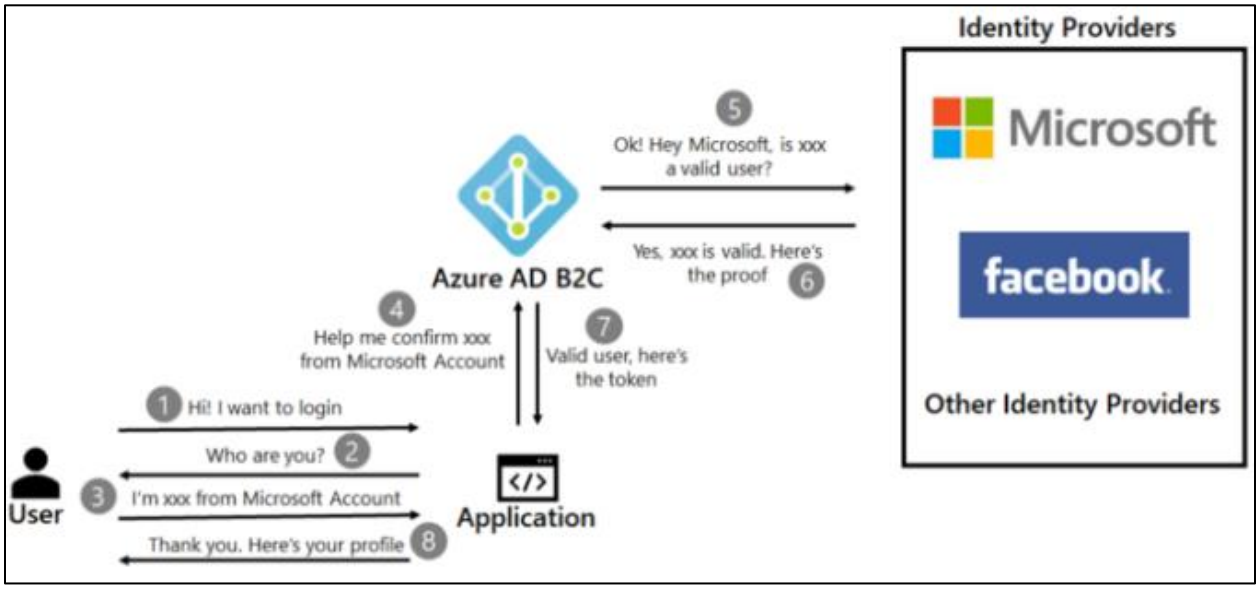

### 2.1.4.2. B2C access management (Use External Idp)

Azure AD B2C is a customer identity access management (CIAM) solution. Azure AD B2C allows external users to sign in with their preferred social, enterprise, or local account identities to get single sign-on to your applications. Azure AD B2C supports millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

With Azure AD B2C, external users are managed in the Azure AD B2C directory, separately from the organization's employee and partner directory. SSO to customer owned apps within the Azure AD B2C tenant is also supported.

Azure AD B2C is an authentication solution that you can customize with your brand so that it blends with your web and mobile applications.

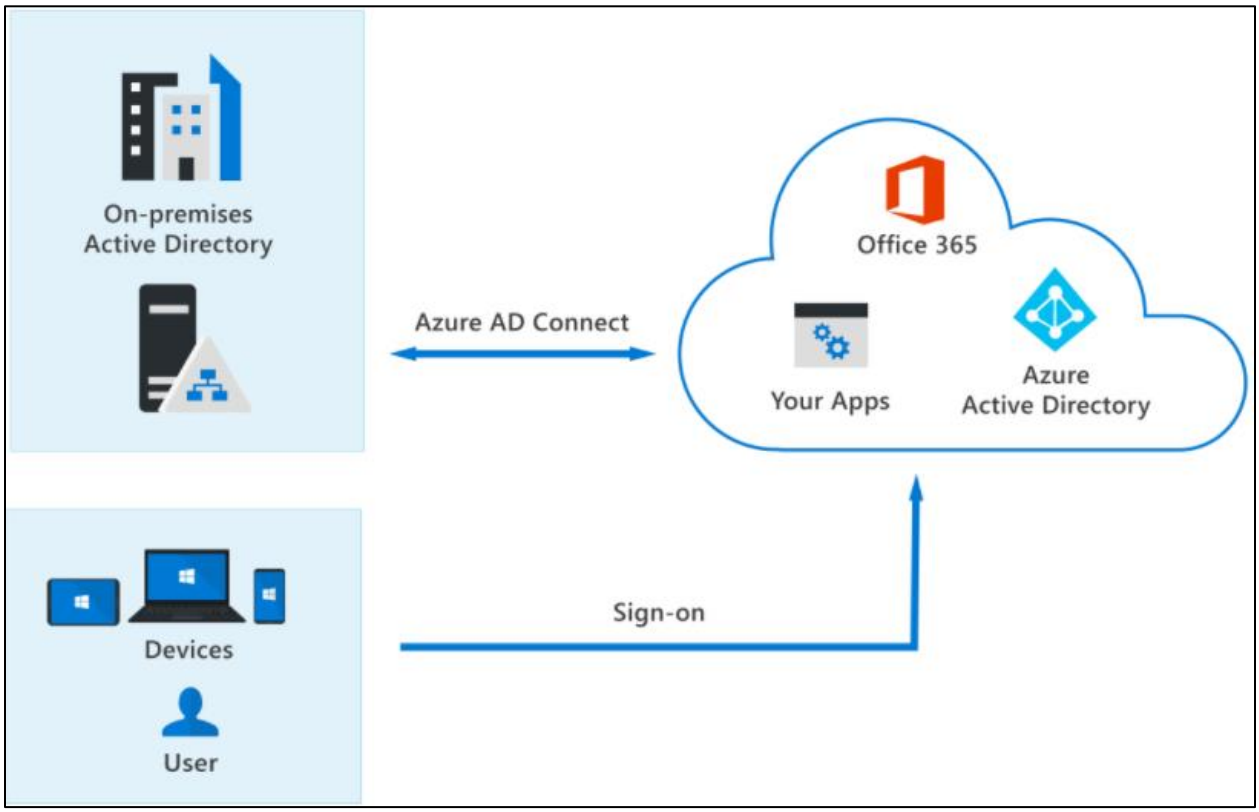



## 2.1.5. AAD Hybrid Identities

Organizations may use the hybrid identity model, or the cloud-only identity model. In the hybrid model, identities are created in Windows Active Directory or another identity provider, and then synchronized to Azure AD. In the cloud-only model, identities are created and wholly managed in Azure AD. Whether identities are created on-premises or in the cloud, users can access both cloud and on-premises resources.

With the hybrid model, users accessing both on-premises and cloud apps are hybrid users managed in the on-premises Active Directory. When you make an update in your on-premises AD DS, all updates to user accounts, groups, and contacts are synchronized to your Azure AD. The synchronization is managed with *Azure AD Connect*.




When using the hybrid model, authentication can either be done by Azure AD, which is known as managed authentication, or Azure AD redirects the client requesting authentication to another identity provider, which is known as federated authentication.

### 2.1.5.1. Three authentication methods for hybrid environment using Azure AD Connect

#### 2.1.5.1.1. Password hash synchronization

The simplest way to enable authentication for on-premises directory objects in Azure AD. Users have the same username and password that they use on-premises without any other infrastructure required.

#### 2.1.5.1.2. Pass-through authentication (PTA)

Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with an on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

#### 2.1.5.1.3. Federated authentication

Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

## 2.2.Azure AD Security Default (optional)

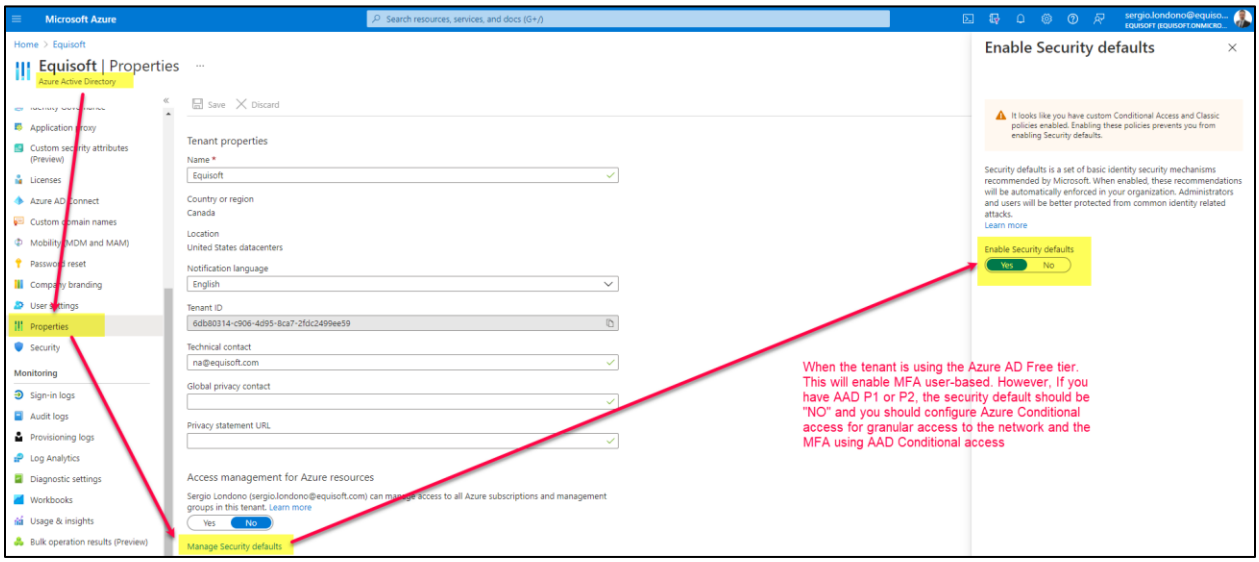
Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.

Managing security can be difficult with common identity-related attacks like password spray, replay, and phishing becoming more popular. Security defaults make it easier to help protect your organization from these attacks with preconfigured security settings:

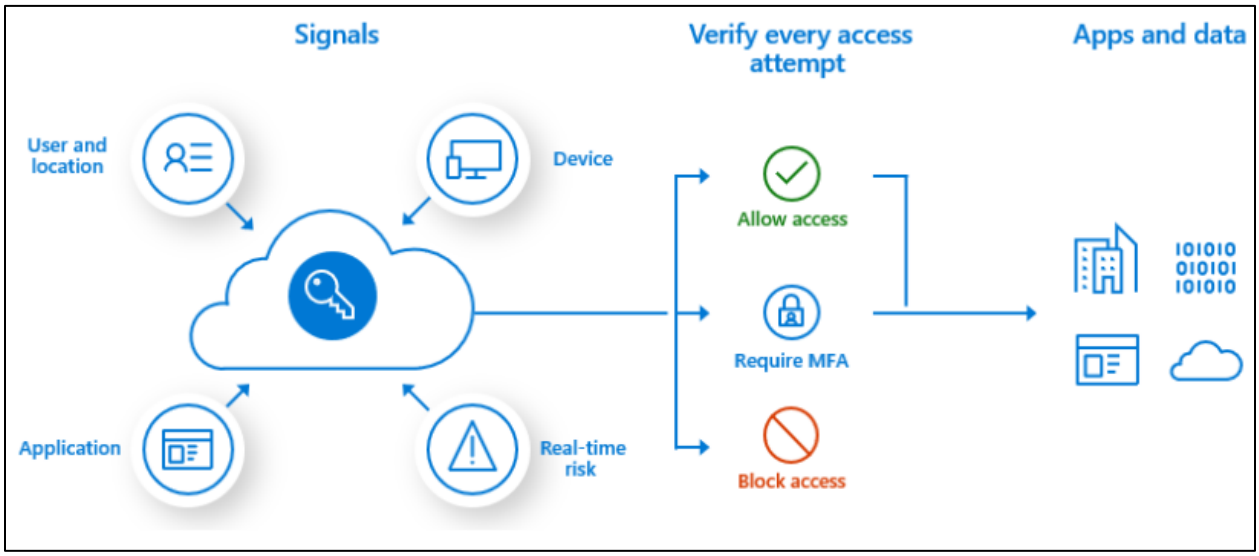
- Requiring all users to register for Azure AD Multi-Factor Authentication.
- Requiring administrators to do multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to do multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

When the tenant is using the Azure AD Free tier.

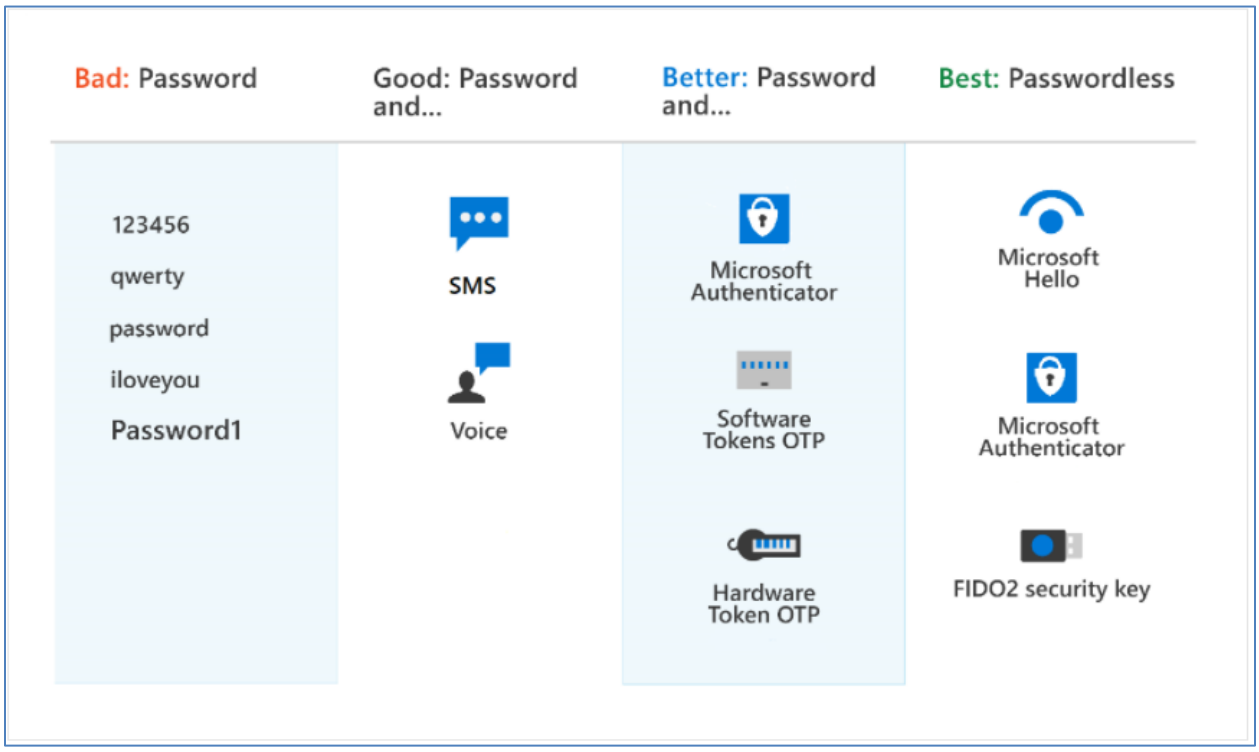
This will enable MFA user based. However, If you have AAD P1 or P2, the security default should be "NO" and you should configure Azure Conditional access for granular access to the network and the MFA using AAD Conditional access

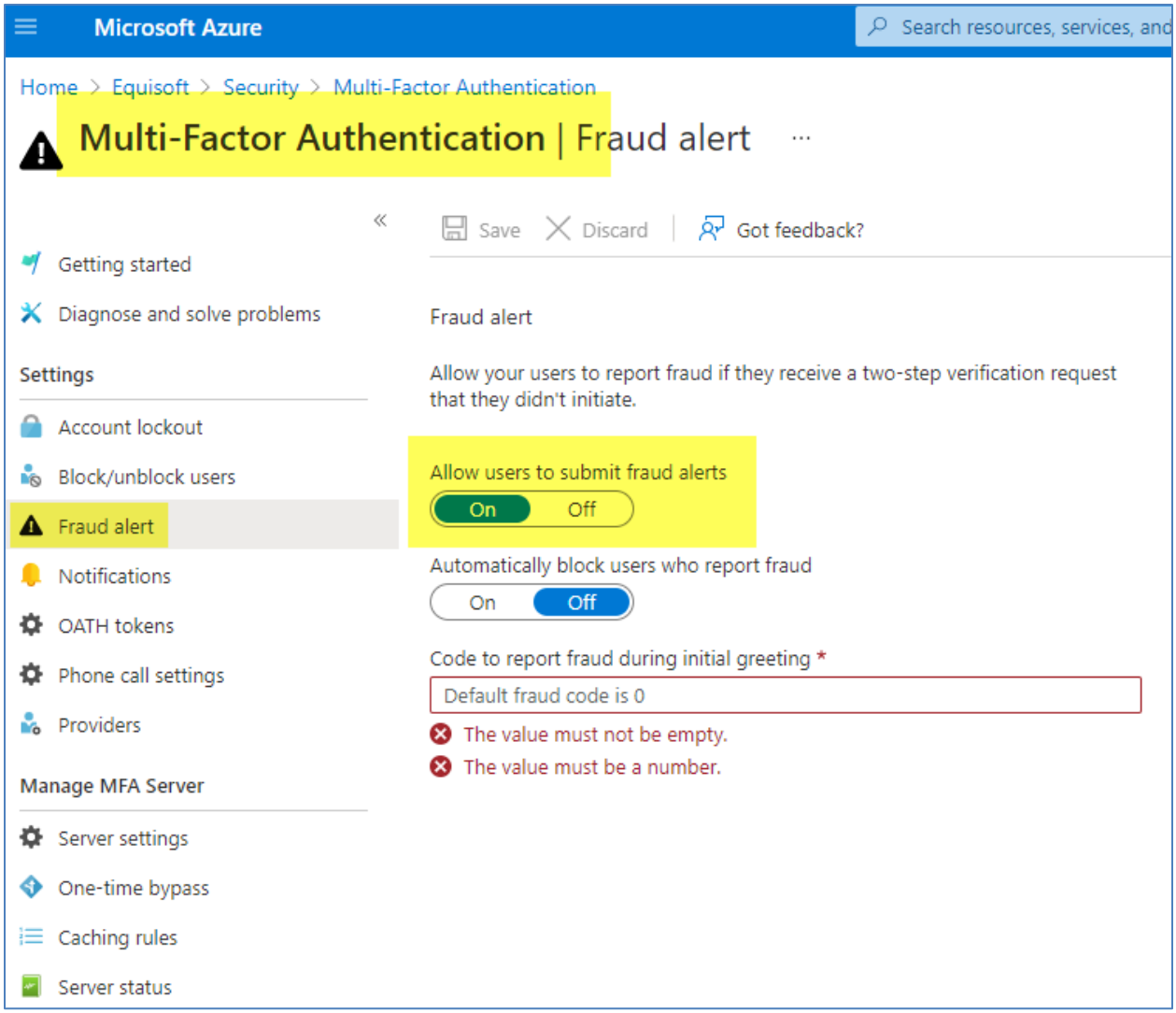


## 2.3.Multi-Factor Authentication




- **Something you know** – typically a password or PIN **and**
- **Something you have** – such as a trusted device that's not easily duplicated, like a phone or hardware key **or**
- **Something you are** – biometrics like a fingerprint or face scan.






### 2.3.1. Passwords

Passwords have many problems. If they're easy enough to remember, they're easy for a hacker to compromise. Strong passwords that aren't easily hacked are difficult to remember, and affect user productivity when forgotten.

### 2.3.2. Password and additional verification

With modern authentication and security features in Azure AD, passwords are supplemented or replaced with more secure authentication methods.

### 2.3.3. Phone

You can also use your phone, configured for either calls or text messages, as an extra means of authentication.

If you set up your extra security verification to receive a phone call, you'll get a call from Microsoft asking you to press a key on your mobile device to verify your identity.

If you set up your additional security verification to receive a text message, you'll be sent a code by text. You then enter the code to verify your identity.

### 2.3.4. Microsoft Authenticator app

The Microsoft Authenticator phone app allows you to securely verify your identity. The Authenticator app is used to provide the additional information required for two-step or multifactor authentication.

## 2.3.5. OATH

OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP is implemented using either software or hardware to generate the codes.

Software OATH tokens are typically applications such as the Microsoft Authenticator app and other authenticator apps.

OATH TOTP hardware tokens typically come with a secret key, preprogrammed in the token, which must be input into Azure AD. Users are associated with a specific hardware token. The hardware token does a refresh of the code every 30 or 60 seconds.

## 2.3.6. Passwordless authentication

Passwordless authentication is based on “something you are” rather than “something you know”.

A biometric facial scan used in Windows Hello for Business is an example of “something you are”.

A fingerprint scan used by the Microsoft Authenticator app or a FIDO2 security device, is also “something you are”.

Passwordless authentication with Azure AD, such as with the Microsoft Authenticator app or FIDO keys, is particularly applicable for shared PCs and where a mobile phone isn't a viable option, such as for help desk personnel, a public kiosk, or a hospital team.

### 2.3.7. Biometrics

Biometric sign-in uses human characteristics, such as a hand, iris, face, or fingerprint. Windows Hello uses facial or fingerprint biometric data to authenticate a user. You'll learn more about Windows Hello in the next unit. The Microsoft Authenticator app can also be used in passwordless mode, using biometric data such as a fingerprint scan, or a facial scan.

### 2.3.8. FIDO2

FIDO is an abbreviation for Fast Identity Online, an alliance that promotes open authentication standards and aims to reduce the reliance on passwords as a form of authentication.

Azure AD supports FIDO2, a passwordless authentication method that can come in different forms. FIDO2 allows users to sign in with an external security key. The external key may be a USB device, lightning connector, Bluetooth, or NFC. In whichever form FIDO2 is implemented, the user never has to enter a password.

Users can also register and select a FIDO2 security key as their main means of authentication.

## 2.4.Windows Hello for Business

Windows Hello, an authentication feature built into Windows 10, replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that's tied to a device and uses a biometric or PIN.

Windows Hello lets users authenticate to:

- A Microsoft account.
- An Active Directory account.
- An Azure Active Directory (Azure AD) account.
- Identity Provider Services or Relying Party Services that support Fast ID Online (FIDO) v2.0 authentication (in preview)

After initial verification of the user during enrollment, Windows Hello is set up on their device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate them.

Windows stores PIN and biometric data securely on the local device; it's never sent to external devices or servers. That means there's no single collection point that an attacker might compromise.

There are two configurations for Windows Hello: Windows Hello convenience PIN and Windows Hello for Business.

- Windows Hello convenience PIN is configured by a user on their personal device. Windows Hello convenience PIN is not backed by asymmetric (public or private key) or certificate-based authentication.
- Windows Hello for Business is configured by Group Policy or mobile device management (MDM) policy, such as Microsoft Intune. In addition, the PIN or biometric used with Windows Hello for Business is backed by key-based or certificate-based authentication, making it more secure than Windows Hello convenience PIN.

### 2.4.1. Why is Windows Hello safer than a password?

Windows Hello in Windows 10 enables users to sign in to their device using a PIN. Although a PIN looks much like a password, a Windows Hello PIN is more secure because it's tied to the specific device on which it was set up. Without the hardware, the PIN is useless.

A regular password is transmitted to a server where it can be intercepted in transmission or stolen from a server. A PIN is local to the device; it isn't transmitted anywhere, and it isn't stored on a server.

The Windows Hello PIN is backed by a Trusted Platform Module (TPM) chip, which is a secure crypto processor that's designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant, and malicious software can't tamper with the security functions of the TPM. Many mobiles phones and modern laptops have TPM.

## 2.5.Self-service password reset (SSPR)

Self-service password reset (SSPR) is a feature of Azure AD that allows users to change or reset their password, without administrator or help desk involvement.

If a user's account is locked or they forget the password, they can follow a prompt to reset it and get back to work. Self-service password reset has several benefits:

- It increases security, as help desks add an extra security layer.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

Self-service password reset works in the following 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.

To use self-service password reset, users must be:

- Assigned an Azure AD license. See Licensing requirements for Azure Active Directory self-service password reset in the Learn More section below.
- Enabled for SSPR by an administrator.
- Registered, with the authentication methods they want to use. Two or more authentication methods are recommended in case one is unavailable.

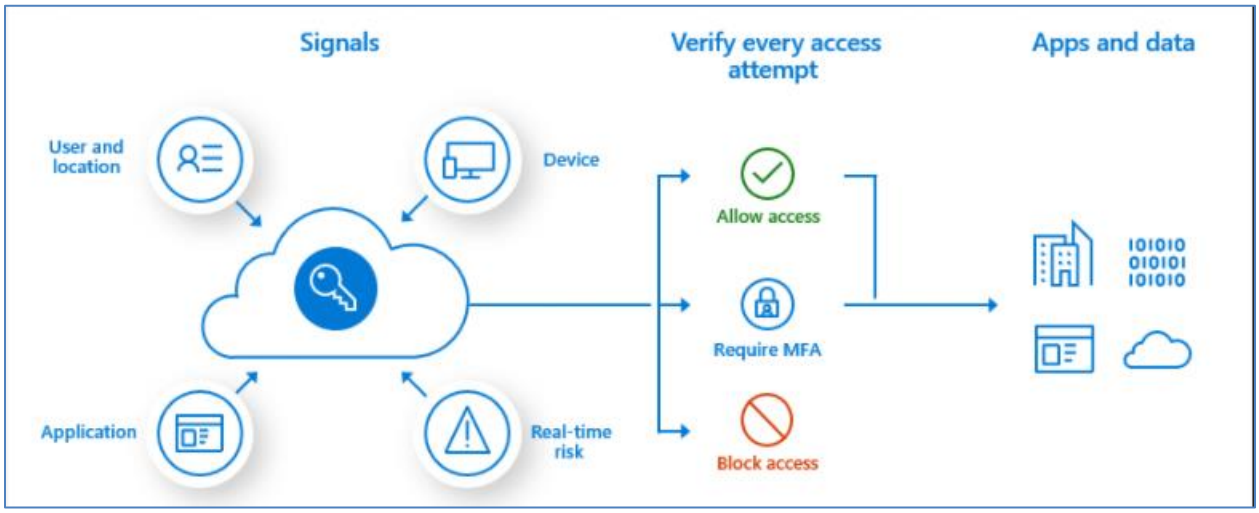
The following authentication methods are available for SSPR:

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

To keep users informed about account activity, admins can configure email notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an extra layer of awareness when a privileged administrator account password is reset using SSPR. All global admins would be notified when SSPR is used on an admin account.

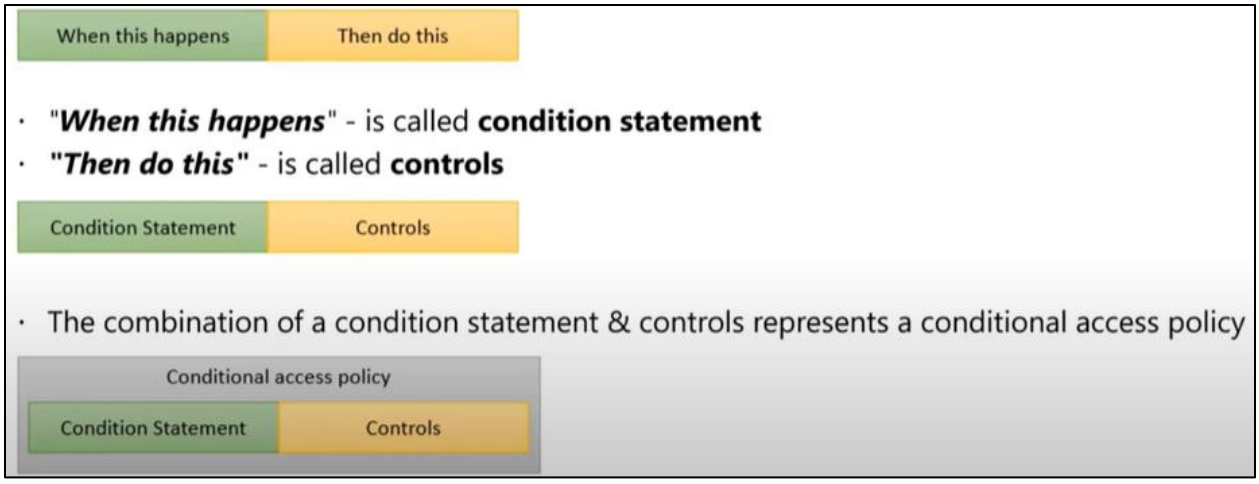
## 2.6.Azure Conditional Access

It is an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).




A Conditional Access policy might state that *if* a user belongs to a certain group, then they're required to provide multifactor authentication to sign into an application.

Conditional access is a capability of Azure AD that enables you to enforce controls on the access to apps in your environment based on specific conditions




### 2.6.1. Conditional access signals

When creating a conditional access policy, admins can determine which signals to use through assignments. The assignments portion of the policy controls the who, what, and where of the Conditional Access policy. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

Conditional Access can use the following signals:

#### 2.6.1.1. User or group membership.

Policies can be targeted to all users, specific groups of users, directory roles, or external guest users, giving administrators fine-grained control over access.

Control a user's access based on membership in a group

#### 2.6.1.2. Named location information.

Named location information can be created using IP address ranges, and used when making policy decisions. Also, administrators can opt to block or allow traffic from an entire country's IP range.

Use The location of the user to trigger MFA or block when not on a trusted network.

#### 2.6.1.3. Device.

Users with devices of specific platforms or marked with a specific state can be used.

Use the device platform, such as iOS, Android, Windows Mobile, or Windows, as a condition for applying policy.

#### 2.6.1.3.1. Device-enabled

Device state, whether enabled or disabled, is validated during device policy evaluation. If you disable a lost or stolen device in the directory, it can no longer satisfy policy requirements.

### 2.6.1.4. Application.

Users attempting to access specific applications can trigger different Conditional Access policies.

### 2.6.1.5. Real-time sign-in risk detection.

Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior - the probability that a given sign-in, or authentication request, isn't authorized by the identity owner. 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.

You can use Azure AD Identity Protection for conditional access risk policies, Conditional access risk policies help give your organization advance protection based on risk events and unusual sign-in activities.

### 2.6.1.6. Cloud apps or actions.

Cloud apps or actions can include or exclude cloud applications or user actions that will be subject to the policy.

### 2.6.1.7. 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.

### 2.6.1.8. Access Control

When the Conditional Access policy has been applied, an informed decision is reached on whether to grant access, block access, or require extra verification. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced. Common decisions are:

### 2.6.1.9. Block access
### 2.6.1.10. Grant access
### 2.6.1.11. Require one or more conditions to be met

- Require multifactor authentication.
- Require device to be marked as compliant.

- Require hybrid Azure AD joined device.
- Compliant device: you can set a policy to only allow Intune compliant devices.
- Require approved client app.
- Require app protection policy.
- Require password change.

#### 2.6.1.12. Session Controls

Limit what the user can do in their session once granted access to the app (Download, Sync, print). It is currently only supported for SharePoint and OneDrive.

to enable limited experiences within specific cloud applications.

As an example, Conditional Access App Control uses signals from **Microsoft Cloud App Security (MCAS) to block, download, cut, copy** and print sensitive documents, or to require labeling of sensitive files.

Other session controls include sign-in frequency and application enforced restrictions that, for selected applications, use the device information to provide users with a limited or full experience, depending on the device state.

Conditional Access policies can be targeted to members of specific groups or guests. For example, you can create a policy to exclude all guest accounts from accessing sensitive resources. Conditional Access is a feature of paid Azure AD editions.

## 2.7.Azure Roles and Microsoft 365 Roles

Azure AD roles control permissions to manage Azure AD resources. For example, allowing user accounts to be created, or billing information to be viewed. Azure AD supports built-in and custom roles.

### 2.7.1. Built-in Roles

There are many built-in roles for different areas of responsibility. All built-in roles are preconfigured bundles of permissions designed for specific tasks.

A few of the most common built-in roles are:

#### 2.7.1.1. Global administrator:

users with this role have access to all administrative features in Azure Active Directory. The person who signs up for the Azure Active Directory tenant automatically becomes a global administrator.

#### 2.7.1.2. User administrator:

users with this role can create and manage all aspects of users and groups. This role also includes the ability to manage support tickets and monitor service health.

#### 2.7.1.3. Billing administrator:

users with this role make purchases, manage subscriptions and support tickets, and monitor service health.

### 2.7.2. Custom Roles

Although there are many built-in admin roles in Azure AD, custom roles give flexibility when granting access.

Granting permission using custom Azure AD roles is a two-step process that involves creating a custom role definition, consisting of a collection of permissions that you add from a preset list. These permissions are the same ones used in the built-in roles. When you've created your role definition, you can assign it to a user by creating a role assignment.

### 2.7.3. Azure AD Role-Based Access Control RBAC

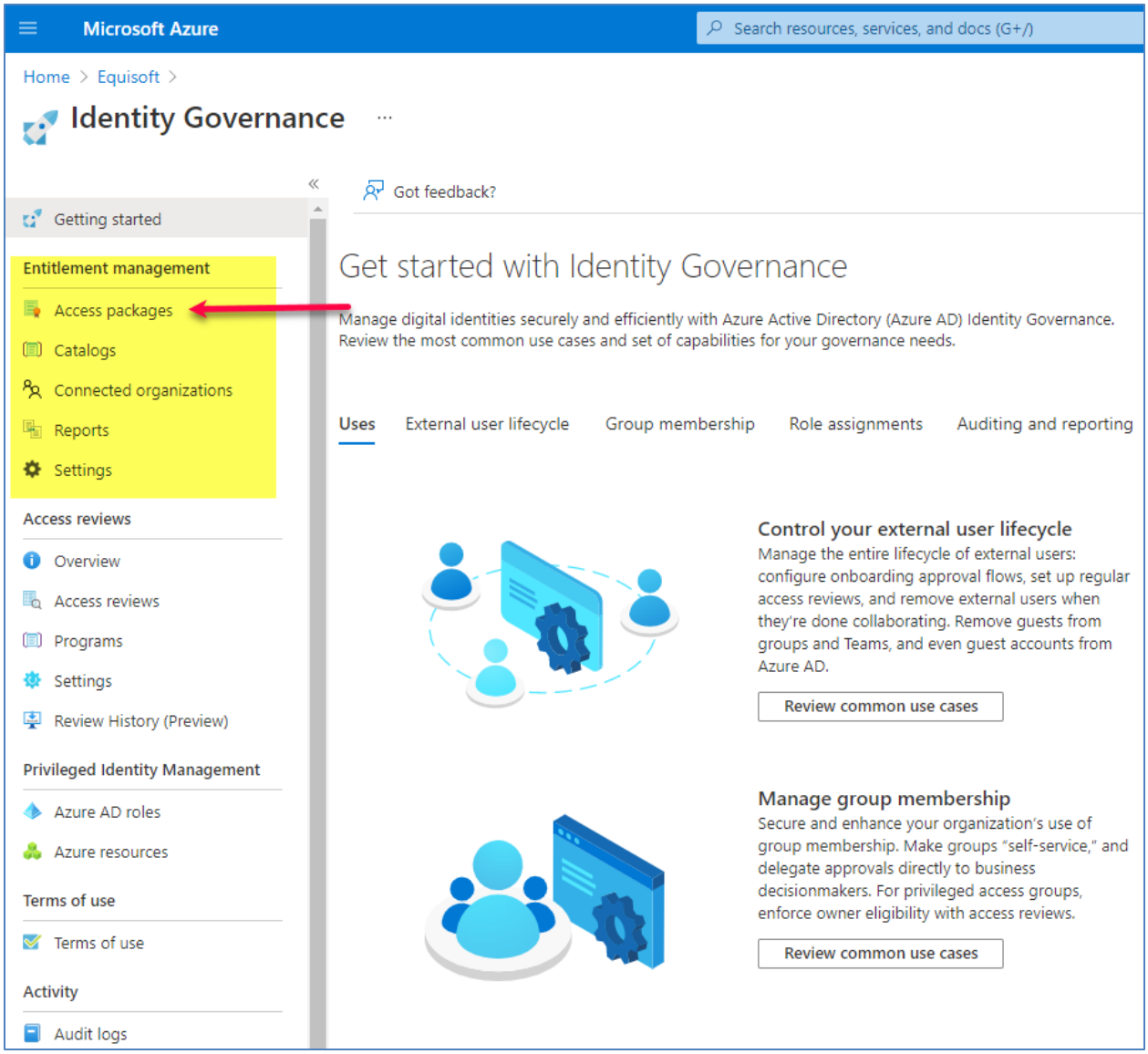
Managing access using roles is known as role-based access control (RBAC). Azure AD built-in and custom roles are a form of RBAC in that Azure AD roles control access to Azure AD resources.

## 2.8.Identity Governance in Azure AD

- 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?

### 2.8.1. Entitlement Management

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




Enterprise organizations often face challenges when managing employee access to resources such as:

- Users may not know what access they should have, and even if they do, they might have difficulty locating the right individuals to approve it.
- When users find and receive access to a resource, they may hold on to access longer than is required for business purposes.
- Managing access for external users.

Entitlement management includes the following capabilities to address these challenges:

- Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then

define policies that include rules such as which users can request access, who must approve their access, and when access expires.

- Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

Entitlement management is a feature of Azure AD Premium P2.

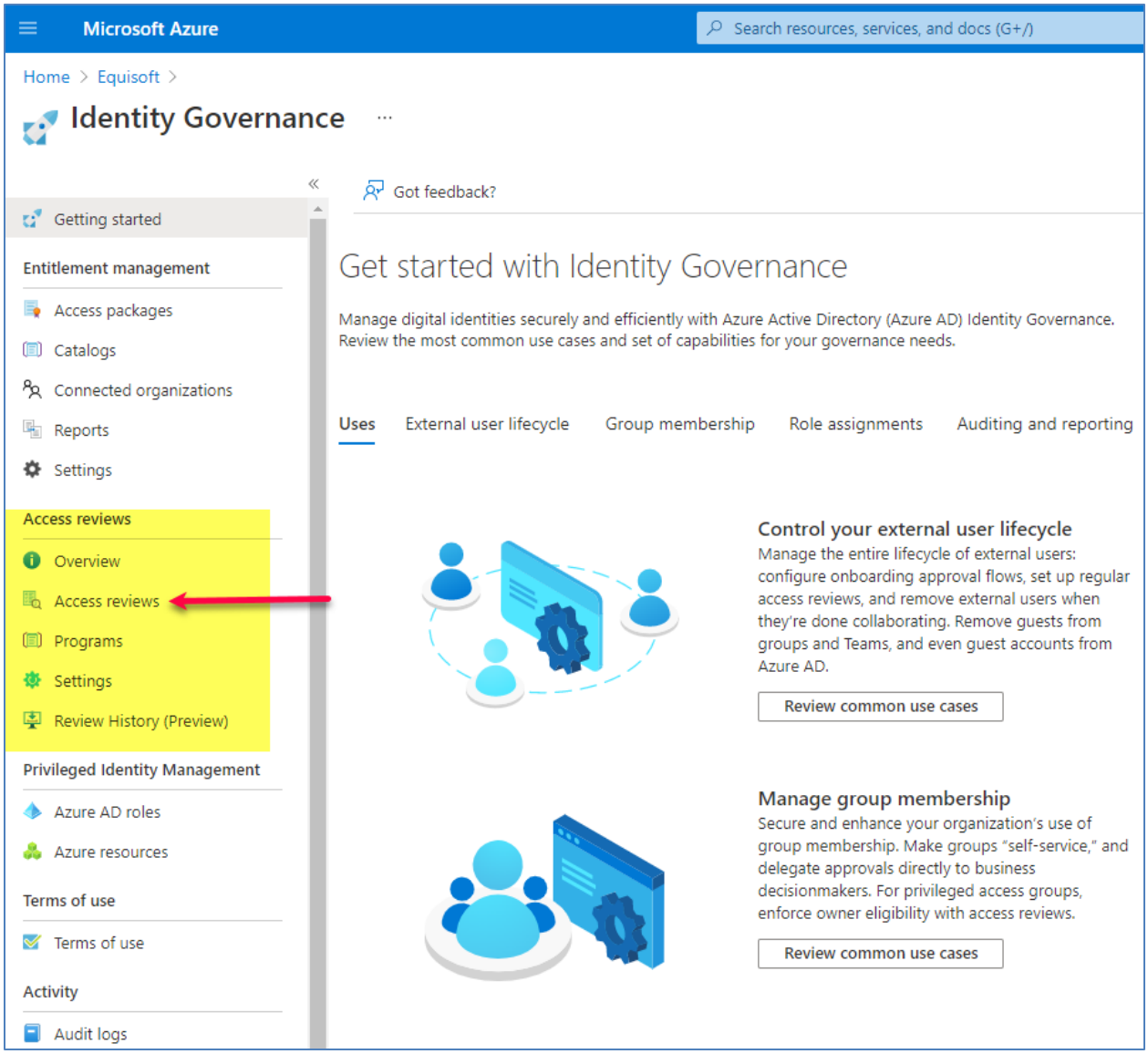
Entitlement management uses access packages to manage access to resources.

### 2.8.2. Azure AD Access Review

Azure Active Directory (AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access to resources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control.

Access reviews are helpful when:

- You have too many users in privileged roles, such as global administrator.
- When automation isn't possible, such as when HR data isn't in Azure AD.
- You want to control business critical data access.
- Your governance policies require periodic reviews of access permissions.




Access reviews can be created through Azure AD access reviews, or Azure AD Privileged Identity Management (PIM). Access reviews can be used to review and manage access for both users and guests. When an access review is created, it can be set up so that each user reviews their own access, or to have one or more users review everyone's access. Similarly, all guests can be asked to review their own access, or have it looked at by one or more users.

Admins who create access reviews can track progress as the reviewers complete their process. No access rights are changed until the review is finished. You can, however, stop a review before it reaches its scheduled end.

When the review is complete, it can be set to manually or auto-apply changes to remove access from a group membership or application assignment, except for a dynamic group or a group that originates on-premises. In those cases, the changes must be applied directly to the group.

Access reviews are a feature of Azure AD Premium P2.

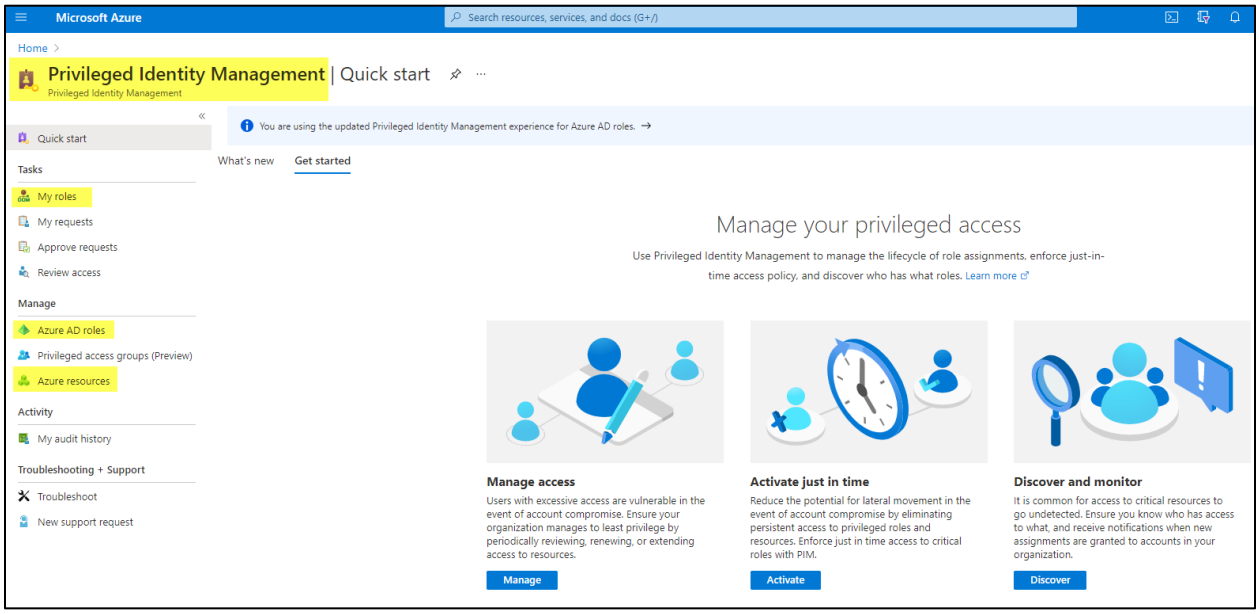
### 2.8.3. Privileged Identity Management PIM

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

PIM is:

- **Just in time**, providing privileged access only when needed, and not before.
- **Time-bound**, by assigning start and end dates that indicate when a user can access resources.
- **Approval-based**, requiring specific approval to activate privileges.
- **Visible**, sending notifications when privileged roles are activated.
- **Auditable**, allowing a full access history to be downloaded.

Privileged Identity Management is a feature of Azure AD Premium P2.




#### 2.8.3.1. Why to use PIM

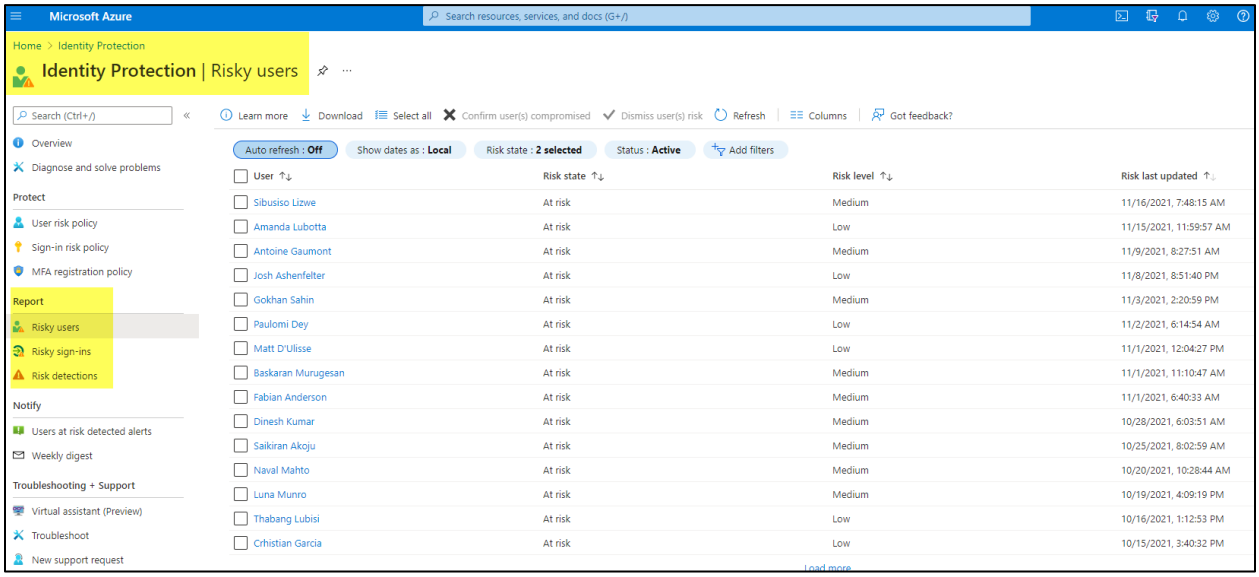
PIM reduces the chance of a malicious actor getting access by minimizing the number of people who have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges.

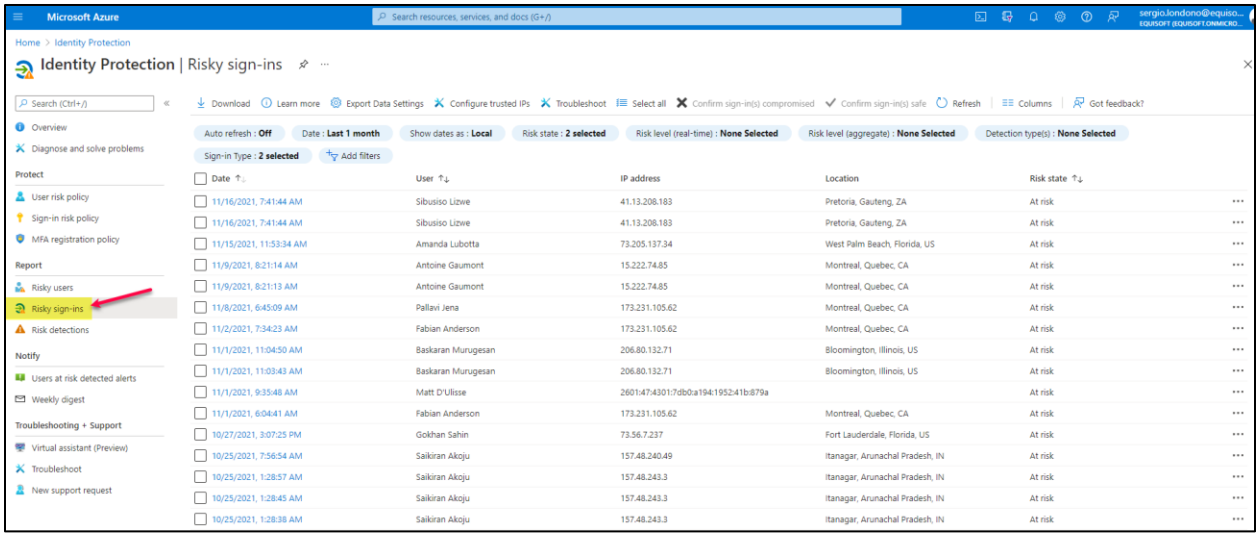
## 2.8.4. Azure Identity Protection

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

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.
- The signals generated by these services are fed to Identity Protection. These signals can then be used by tools such as Conditional Access, which uses them to make access decisions. Signals are also fed to security information and event management (SIEM) tools, such as Sentinel, for further investigation.
- Identity Protection categorizes risk into three tiers:
    - Low
    - Medium
    - high.

It can also calculate the sign-in risk, and user identity risk.






### 2.8.4.1. Sign-in risk

Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

Sign-in risk can be calculated in real-time or calculated offline using Microsoft's internal and external threat intelligence sources.

These risk detections can trigger actions such as requiring users to provide multifactor authentication, reset their password, or block access until an administrator takes action.

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

After completing an investigation, admins will want to take action to remediate the risk or unblock users. Organizations can also enable automated remediation using their risk policies. Microsoft recommends closing events quickly because time matters when working with risk.

Identity Protection is a feature of Azure AD Premium P2.

Listed below are some of the sign-in risks that Identity Protection in Azure AD is able to identify:

#### 2.8.4.2. Anonymous IP address.

This risk detection type indicates sign-ins from an anonymous IP address; for example, a Tor browser or anonymized VPNs.

#### 2.8.4.3. Atypical travel.

This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.

#### 2.8.4.4. Malware linked IP address.

This risk detection type indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server.

#### 2.8.4.5. Unfamiliar sign-in properties.

This risk detection type considers past sign-in history to look for anomalous sign-ins. The system stores information about previous locations used by a user, and considers these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations.

#### 2.8.4.6. Password spray.

This risk detection is triggered when a password spray attack has been performed.

Password Spraying Attack is a type of brute force attack where a malicious actor attempts the same password on many accounts before moving on to another one and repeating the process. This is effective because many users use simple, predictable passwords, such as “password123.”

#### 2.8.4.7. Azure AD threat intelligence.

This risk detection type indicates sign-in activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

### 2.8.5. User risk

User risk represents the probability that a given identity or account is compromised. These risks are calculated offline using Microsoft's internal and external threat intelligence sources. Listed below are some of the user risks that Identity Protection in Azure AD is able to identify:

#### 2.8.5.1. Leaked credentials.

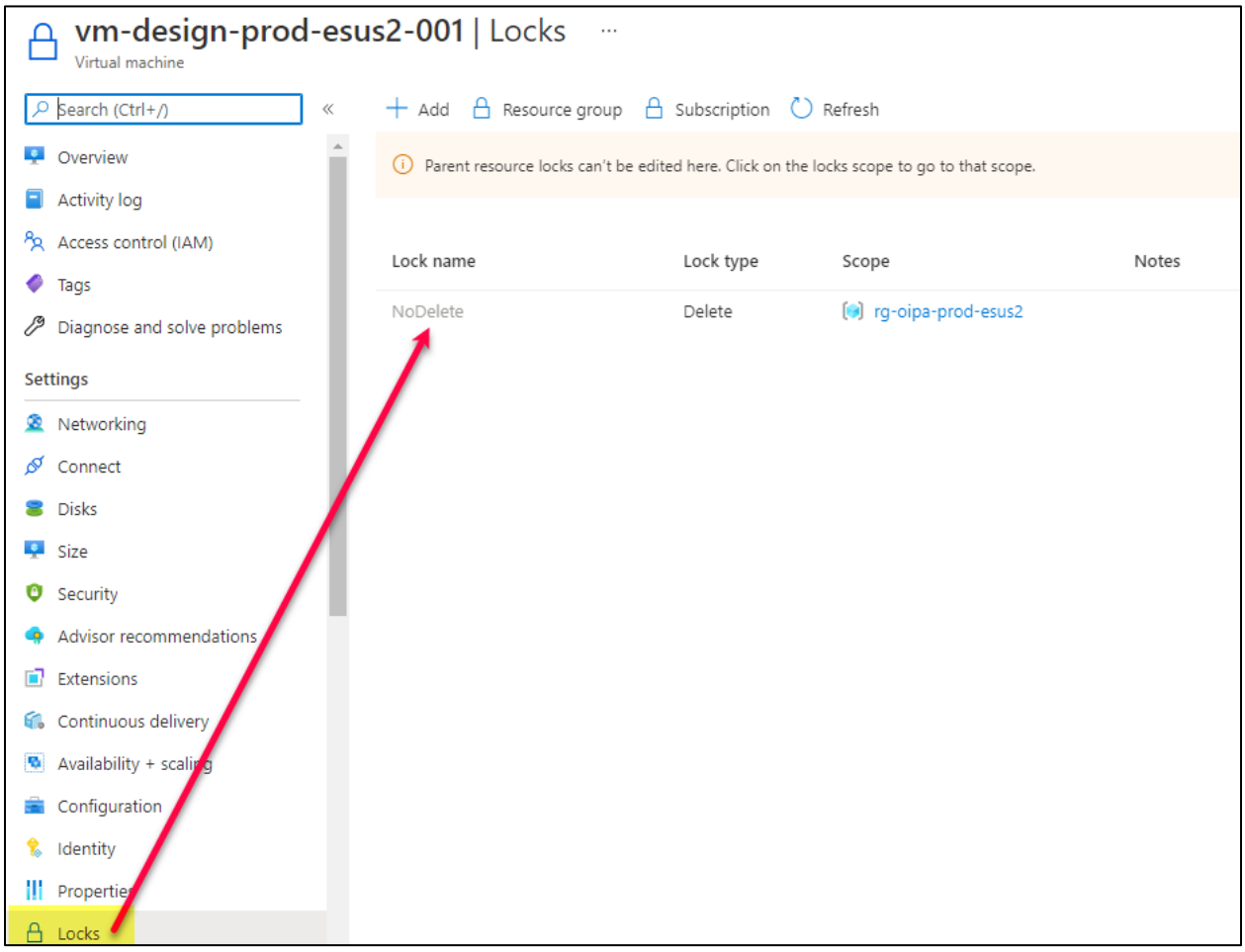
This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.

This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they are checked against Azure AD users' current valid credentials to find valid matches.

#### 2.8.5.2. Azure AD threat intelligence.

This risk detection type indicates user activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

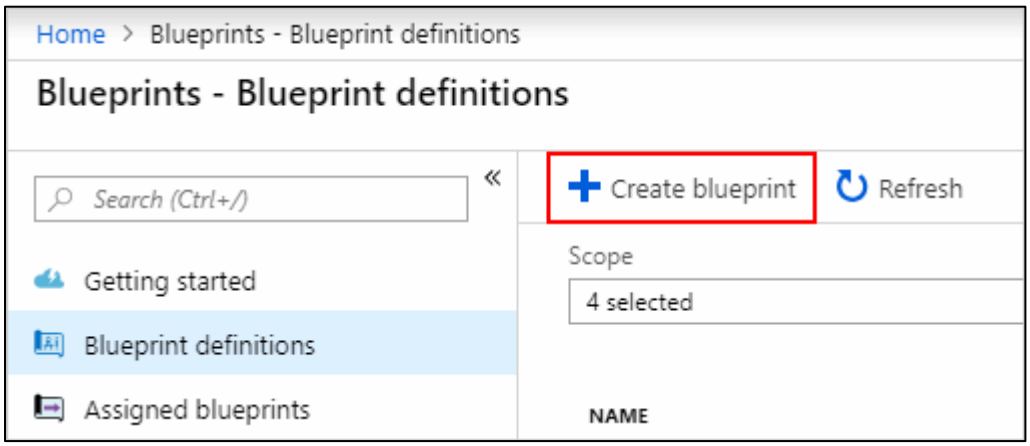
## 2.9.Azure Lock




### 2.9.1. Cannot Delete
### 2.9.2. ReadOnly

## 2.10. Azure Blueprints

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




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

2.10.1. Resource Groups
2.10.2. RBAC
2.10.3. Policy
2.10.4. ARM Templates

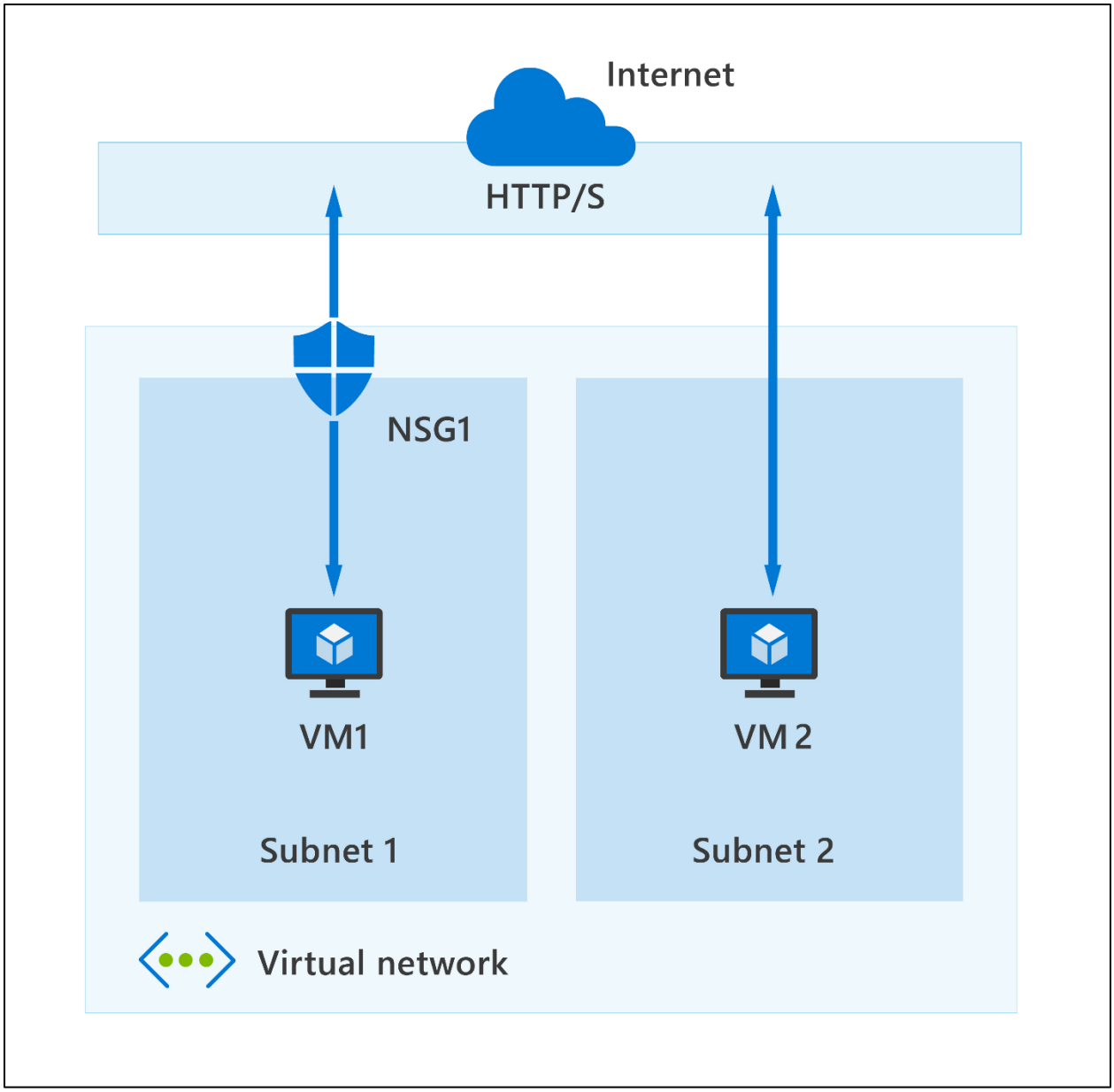
# 3. Describe the Capabilities of Microsoft Security Solutions

## 3.1. Basic Security Capabilities in Azure

### 3.1.1. Network Security Group

An NSG consists of rules that define how the traffic is filtered. You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. As a guideline, you shouldn't create two security rules with the same priority and direction.




### 3.1.2. DDoS

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

The three most frequent types of DDoS attack are:

### 3.1.2.1. Type of DDoS Attack

#### 3.1.2.1.1. Volumetric attacks

These are volume-based attacks that flood the network with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through. These types of attacks are measured in bits per second.

#### 3.1.2.1.2. Protocol attacks

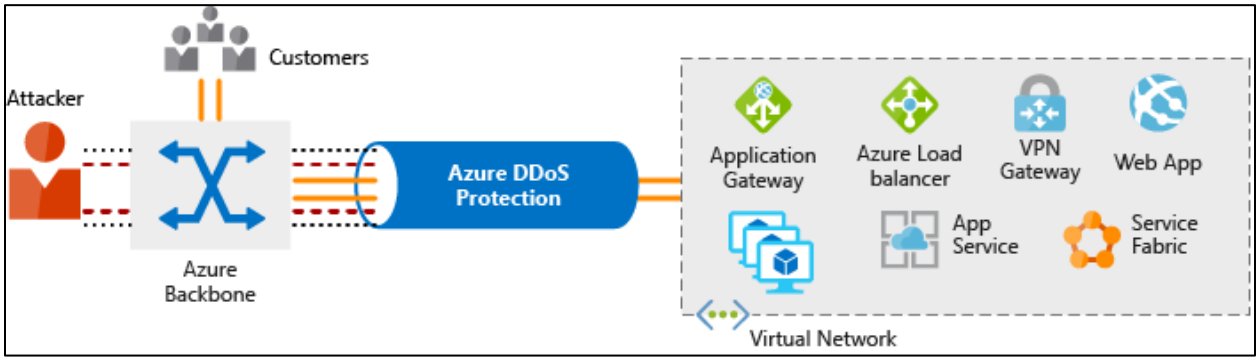
Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. These types of attacks are typically measured in packets per second.

#### 3.1.2.1.3. Resource (application) layer attacks

These attacks target web application packets, to disrupt the transmission of data between hosts.

### 3.1.2.2. Azure DDoS Protection

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




In the diagram above, Azure DDoS Protection identifies an attacker's attempt to overwhelm the network. It blocks traffic from the attacker, ensuring that it doesn't reach Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.

Azure DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. During a DDoS attack, Azure can scale your computing needs to meet demand. DDoS Protection manages cloud consumption by ensuring that your network load only reflects actual customer usage.

Azure DDoS Protection comes in two tiers:

#### 3.1.2.2.1. Azure DDoS Protection Basic tier

The Basic service tier is automatically enabled for every property in Azure, at no extra cost, as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.

#### 3.1.2.2.2. Azure DDoS Protection Standard tier

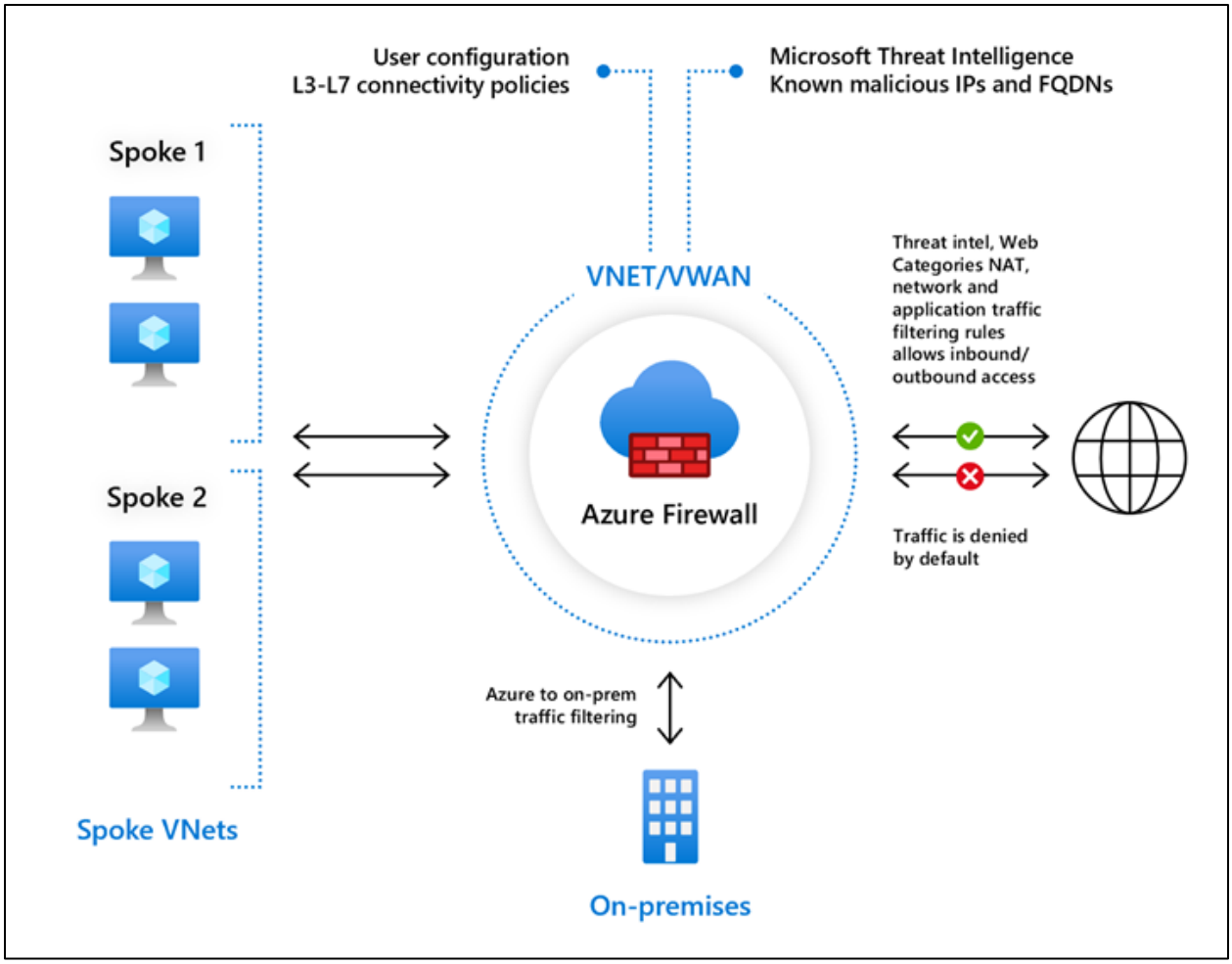
The Standard service tier provides extra mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway.

### 3.1.3. Azure Firewall

#### 3.1.3.1. Standard

Azure Firewall is a managed, cloud-based network security service that protects your Azure virtual network (VNet) resources from attackers. You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions.

Azure Firewall Standard provides L3-L7 filtering and threat intelligence feeds directly from Microsoft Cyber Security. Threat intelligence-based filtering can alert and deny traffic from/to known malicious IP addresses and domains which are updated in real time to protect against new and emerging attacks.




With Azure Firewall, you can scale up the usage to accommodate changing network traffic flows, so you don't need to budget for peak traffic. Network traffic is subjected to the configured firewall rules when you route it to the firewall as the subnet default gateway.

Use Azure Firewall to help protect the Azure resources you've connected to Azure Virtual Networks.

#### 3.1.3.1.1. Key Features of Azure Firewall

##### 3.1.3.1.1.1. Built-in high availability and availability zones

High availability is built in so there's nothing to configure. Also, Azure Firewall can be configured to span multiple availability zones for increased availability.

##### 3.1.3.1.1.2. Network and application level filtering

Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls.

#### 3.1.3.1.1.3. Outbound SNAT and inbound DNAT to communicate with internet resources

Translates the private IP address of network resources to an Azure public IP address (source network address translation) to identify and allow traffic originating from the virtual network to internet destinations. Similarly, inbound internet traffic to the firewall public IP address is translated (Destination Network Address Translation) and filtered to the private IP addresses of resources on the virtual network.

#### 3.1.3.1.1.4. Multiple public IP addresses

These addresses can be associated with Azure Firewall.

#### 3.1.3.1.1.5. Threat intelligence

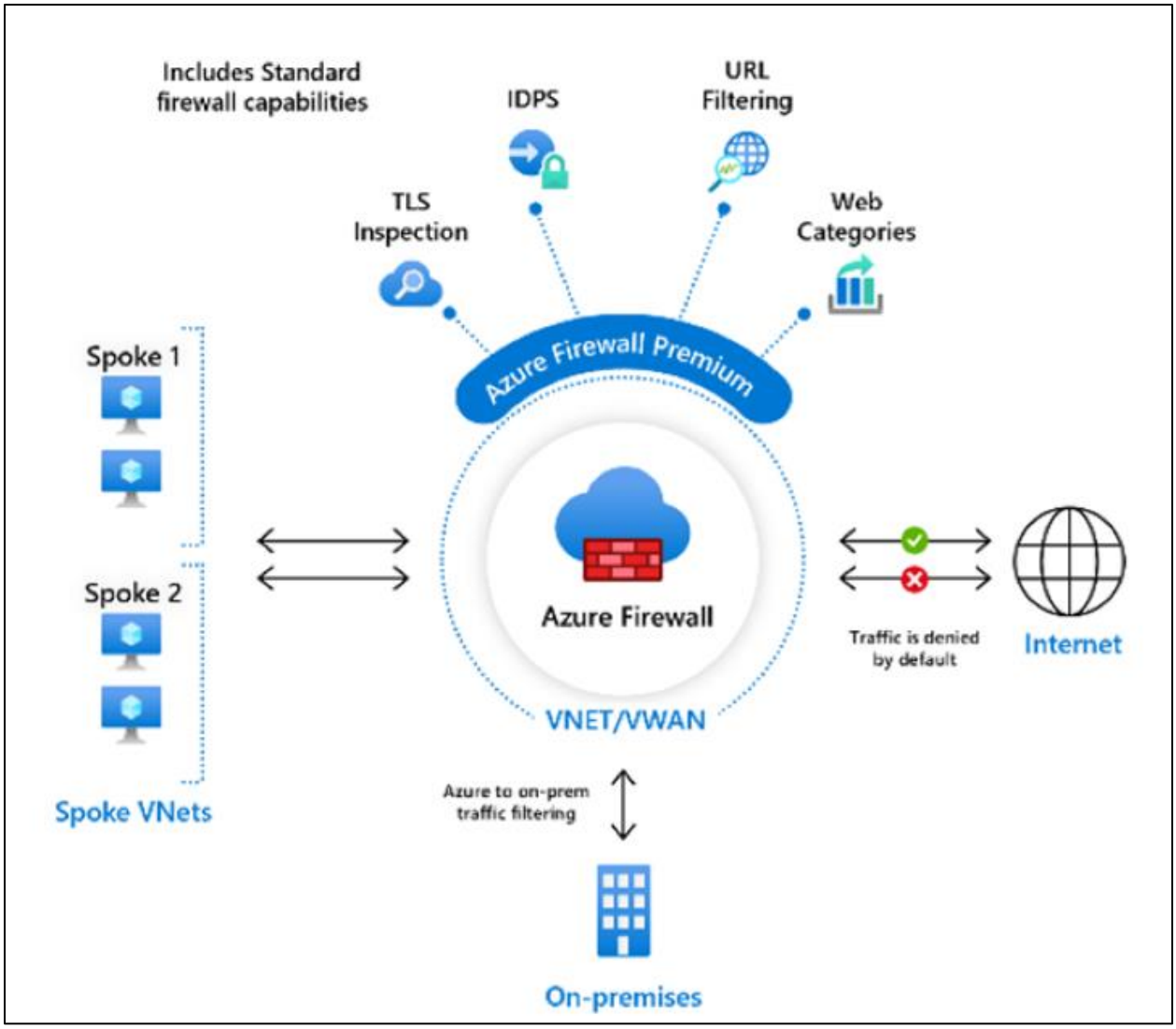
Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.

#### 3.1.3.1.1.6. Integration with Azure Monitor

Integrated with Azure Monitor to enable collecting, analyzing, and acting on telemetry from Azure Firewall logs.

### 3.1.3.2. Premium

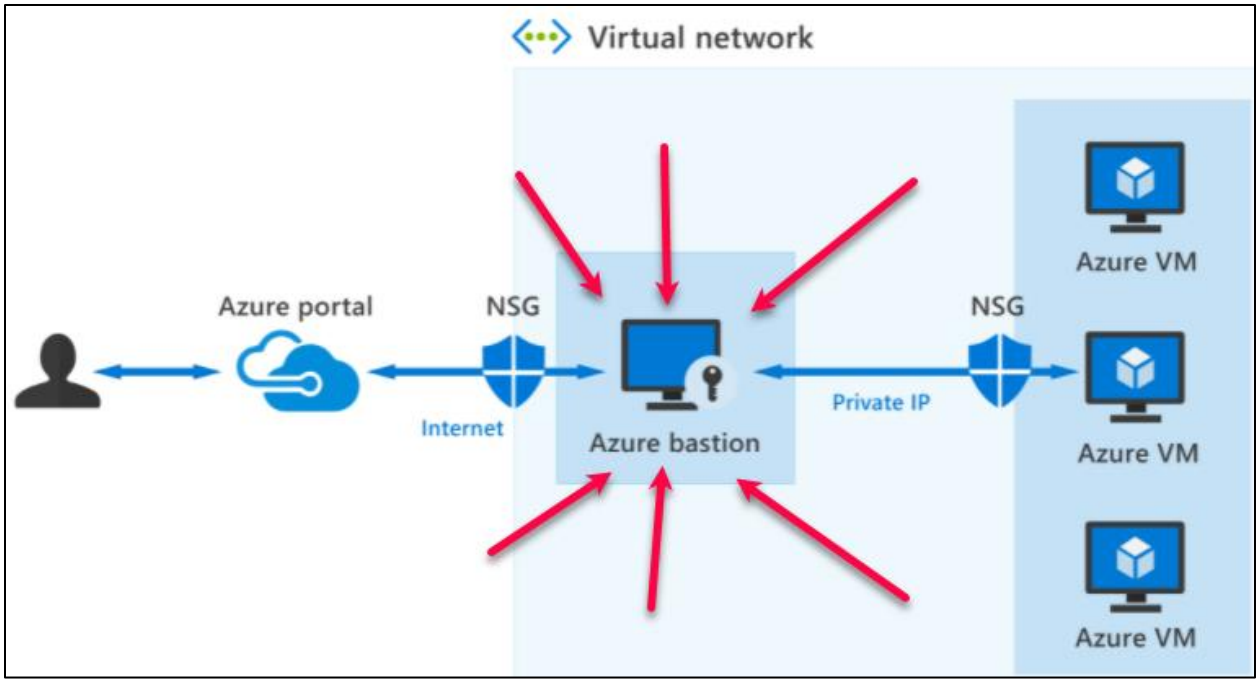
Azure Firewall Premium provides advanced capabilities include signature-based IDPS to allow rapid detection of attacks by looking for specific patterns. These patterns can includes byte sequences in network traffic, or known malicious instruction sequences used by malware. There are more than 58,000 signatures in over 50 categories which are updated in real time to protect against new and emerging exploits. The exploit categories include malware, phishing, coin mining, and Trojan attacks.




### 3.1.4. Azure Bastion

Let's assume you've set up multiple virtual networks that use a combination of NSGs and Azure Firewalls to protect and filter access to the assets and resources, including virtual machines (VMs). You're now protected from external threats, but need to allow your developers and data scientist, who are working remotely, direct access to those VMs.

In a traditional model, you'd need to expose the Remote Desktop Protocol (RDP) and Secure Shell (SSH) ports to the internet. These protocols can be used to gain remote access to your VMs. This process creates a significant surface threat that can be exploited by attackers.




Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network, and peered virtual networks, in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine. Once you provision the Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same VNet, as well as peered VNets.

#### 3.1.4.1. Key features of Azure Bastion

Use Azure Bastion to establish secure RDP and SSH connectivity to your virtual machines in Azure.

##### 3.1.4.1.1. RDP and SSH directly in Azure portal

You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.

##### 3.1.4.1.2. Remote session over TLS and firewall traversal for RDP/SSH

Use an HTML5-based web client that's automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely.

#### 3.1.4.1.3. No Public IP required on the Azure VM

Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.

#### 3.1.4.1.4. No hassle of managing NSGs

A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.

#### 3.1.4.1.5. Protection against port scanning

Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.

#### 3.1.4.1.6. Protect against zero-day exploits

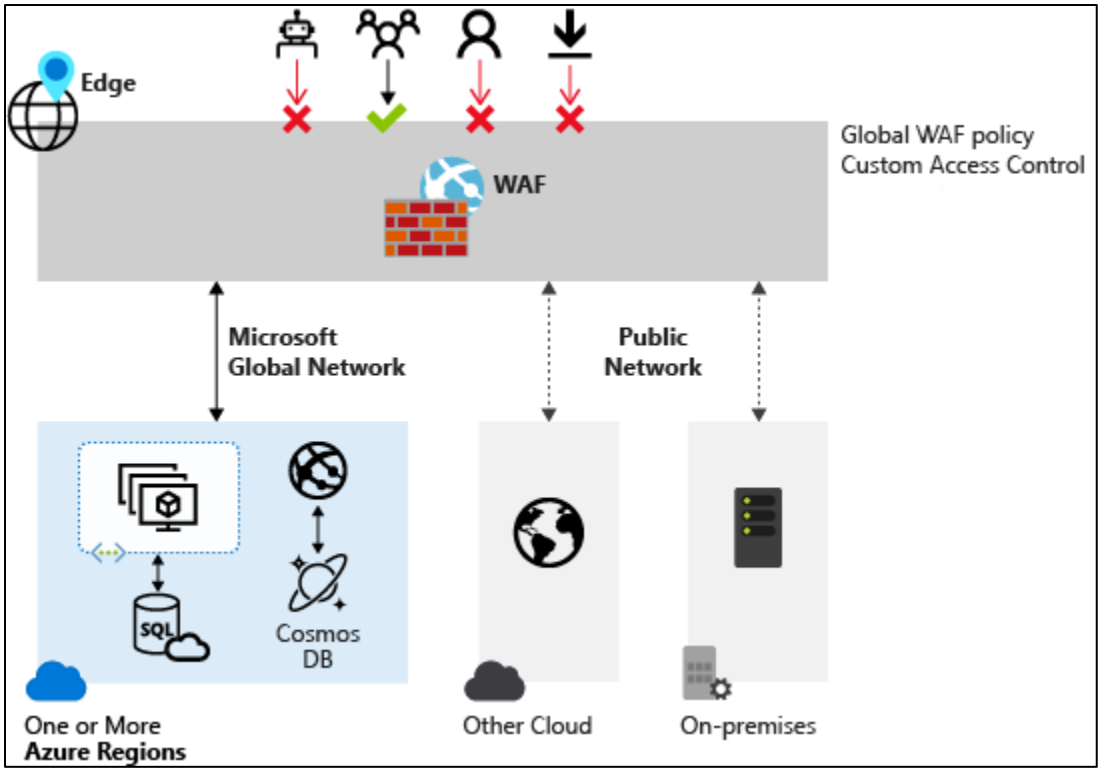
A fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don’t need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

### 3.1.5. Azure Web Application Firewall

We’ve looked at the traditional security concerns for the protection of your assets, resources, and data from external attack by using firewalls and network security groups. But there's another threat surface now being exploited by hackers: web applications.

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities, like SQL injection and cross-site scripting. Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring.

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




#### 3.1.5.1. WAF Azure Service Integration

WAF has features that are customized for each specific service.

WAF can be deployed with

##### 3.1.5.1.1. Azure Application Gateway
##### 3.1.5.1.2. Azure Front Door
##### 3.1.5.1.3. Azure Content Delivery Network (CDN) services from Microsoft.

Use Azure WAF to achieve centralized protection for your web applications from common exploits and vulnerabilities.

### 3.1.6. Encrypt Data in Azure

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

The loss of sensitive data can be crippling and have legal implications.

For most organizations, data is their most valuable asset.

In a layered security strategy, the use of encryption serves as the last and strongest line of defense.

### 3.1.6.1. Encryption on Azure

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

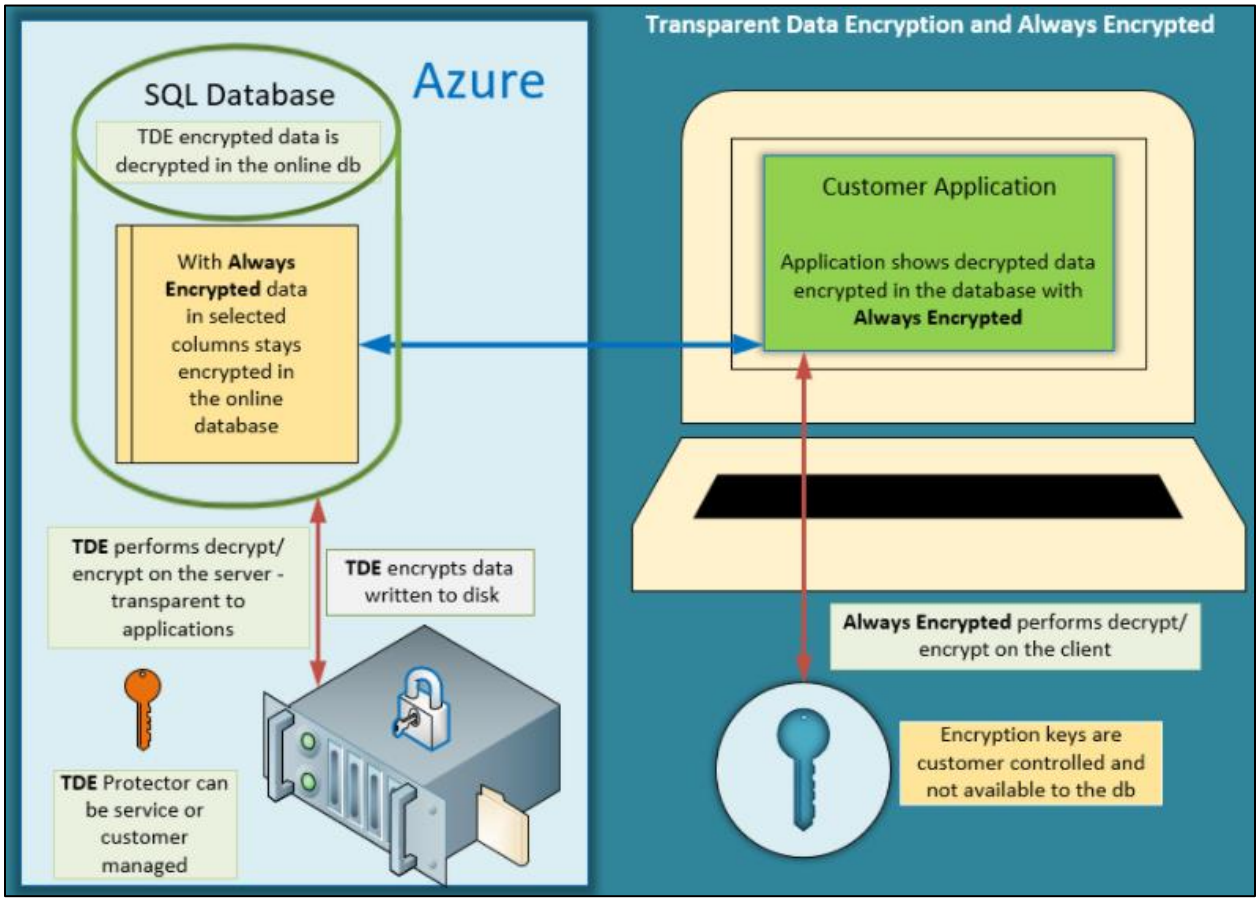
#### 3.1.6.1.1. Azure Storage Service Encryption

Helps to protect data at rest by automatically encrypting before persisting it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and decrypts the data before retrieval.

#### 3.1.6.1.2. Azure Disk Encryption

Helps you encrypt Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and data disks.

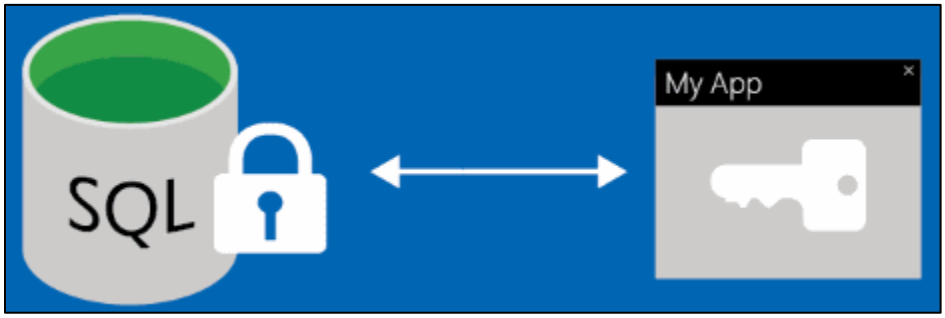
#### 3.1.6.1.3. Database encryption



#### 3.1.6.1.3.1.1. Transparent data encryption (TDE)

Helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

### 3.1.6.1.3.2. Always Encrypted




Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). As a result, Always Encrypted provides a separation between those who own the data and can view it, and those who manage the data but should have no access. By ensuring on-premises database administrators, cloud database operators, or other high-privileged unauthorized users, can't access the encrypted data, Always Encrypted enables customers to confidently store sensitive data outside of their direct control. This allows organizations to store their data in Azure and enable delegation of on-premises database administration to third parties, or to reduce security clearance requirements for their own DBA staff.

Always Encrypted provides confidential computing capabilities by enabling the Database Engine to process some queries on encrypted data, while preserving the confidentiality of the data and providing the above security benefits.

#### 3.1.6.1.3.2.1. Typical Scenarios

##### 3.1.6.1.3.2.1.1. Client and data on-premises

A customer has a client application and SQL Server both running on-premises, at their business location. The customer wants to hire an external vendor to administer SQL Server. In order to protect sensitive data stored in SQL Server, the customer uses Always Encrypted to ensure the separation of duties between database administrators and application administrators. The customer stores plaintext values of Always Encrypted keys in a trusted key store, which the client application can access. SQL Server administrators have no access to the keys and, therefore, are unable to decrypt sensitive data stored in SQL Server.

#### 3.1.6.1.3.2.1.2. Client on-premises with data in Azure

A customer has an on-premises client application at their business location. The application operates on sensitive data stored in a database hosted in Azure (SQL Database or SQL Server running in a virtual machine on Microsoft Azure). The customer uses Always Encrypted and stores Always Encrypted keys in a trusted key store hosted on-premises, to ensure Microsoft cloud administrators have no access to sensitive data.

#### 3.1.6.1.3.2.1.3. Client and Data in Azure

A customer has a client application, hosted in Microsoft Azure (for example, in a worker role or a web role), which operates on sensitive data stored in a database hosted in Azure (SQL Database or SQL Server running in a virtual machine on Microsoft Azure). Although Always Encrypted doesn't provide complete isolation of data from cloud administrators, as both the data and keys are exposed to cloud administrators of the platform hosting the client tier, the customer still benefits from reducing the security attack surface area (the data is always encrypted in the database).

### 3.1.7. Azure Key Vault

Use the various ways in which Azure can encrypt your data to help you secure it whatever the location or state.

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

#### 3.1.7.1. Secrets management

Secrets management you can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.

#### 3.1.7.2. Key management

Key Management you can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.

#### 3.1.7.3. Certificate management

Certificate management Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for Azure, and internally connected, resources more easily.

#### 3.1.7.4. Store secrets

Store secrets backed by hardware security modules (HSMs). The secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

## 3.2. Cloud Security Posture Management (CSPM)

Use CSPM to improve your cloud security management by assessing the environment, and automatically alerting security staff for vulnerabilities.

Cloud-based systems are continually evolving and changing as companies move away from on-premises to the cloud. This move makes it difficult for any IT department to know if your data, assets, and resources are as fully protected as they used to be. Even a small misconfiguration of a new feature can increase the attack surface available for cybercriminals to exploit.

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

The main goal for a cloud security team working on posture management is to continuously report on and improve the organization's security posture by focusing on disrupting a potential attacker's return on investment (ROI).

The function of CSPM in your organization might be spread across multiple teams, or there may be a dedicated team. CSPM can be useful to many teams in your organization:

### 3.2.1. CSPM tools and services:

#### 3.2.1.1. Zero Trust-based Access Control

Zero Trust-based access control considers the active threat level during access control decisions.

#### 3.2.1.2. Real-time risk scoring

Real-time risk scoring to provide visibility into top risks.

#### 3.2.1.3. Threat and vulnerability management (TVM)

Threat and vulnerability management (TVM) establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.

#### 3.2.1.4. Discover sharing risks

Discover sharing risks to understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.

#### 3.2.1.5. Technical policy

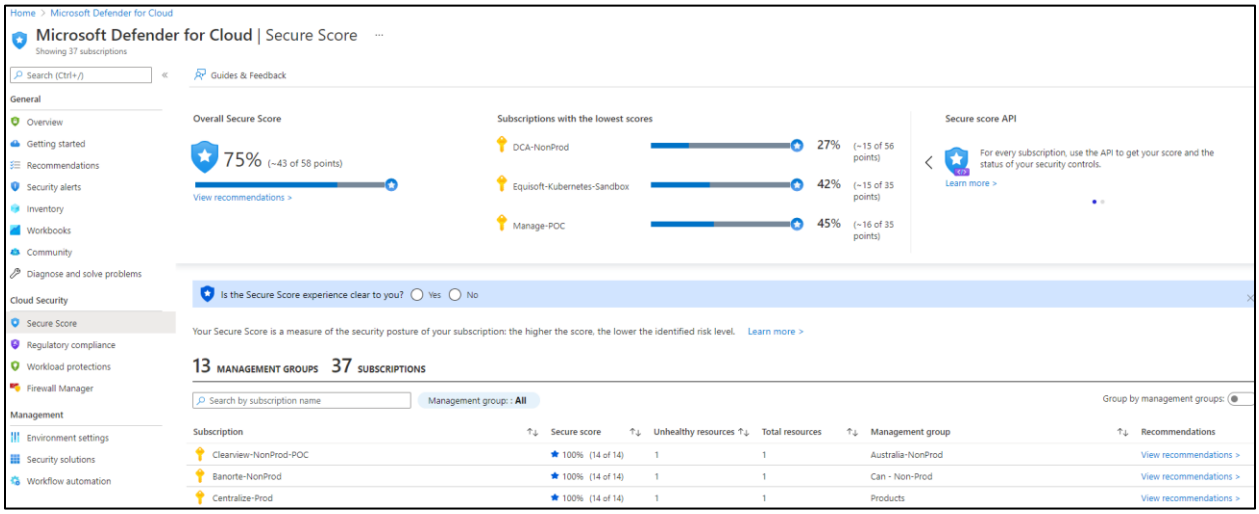
Technical applies guardrails to audit and enforce the organization's standards and policies to technical systems.

#### 3.2.1.6. Threat modeling systems and architectures

Threat modeling system and architectures used alongside other specific applications.

### 3.2.2. Microsoft Defender for Cloud (Legacy:Azure Security Center (ASC))

Network security is an ever-changing and shifting battleground where a moment's hesitation can allow cybercriminals to compromise your security perimeter, and steal valuable assets and resources. Using Azure Security Center gives you infrastructure level security management to protect your data. It also provides advanced threat protection for on-premises, cloud, and hybrid workloads in the cloud, whether they're in Azure or not, as well as on-premises. Azure Security Center provides the tools you need to harden your network, secure services, and ensure you're on top of your security posture.




Azure Security Center addresses the three most urgent security challenges:

- **Rapidly changing workloads**: As organizations empower users to do more, the challenge is to ensure that the ever-changing services people use and create meet your security standards and follow best practices.
- **Increasingly sophisticated attacks**: Wherever your work is situated, the attacks keep getting more sophisticated. Securing your public internet-facing services is essential; otherwise, you'll be even more vulnerable.
- **Security skills are in short supply**: The number of security alerts and alerting systems far outnumbers the total of administrators who have the necessary background and experience to ensure your environments are protected.

To help protect against these challenges, Azure Security Center provides tools to:

- **Strengthen security posture**: Security Center assesses your environment and enables you to understand the status of your resources and whether they're secure.
- **Protect against threats**: Security Center assesses your workloads and raises threat prevention recommendations and security alerts.
- **Get secure faster**: In Security Center, everything is done in cloud speed. Because it's natively integrated, Security Center deployment is easy, giving you autoprovisioning and protection with Azure services.

Also, Security Center protects non-Azure servers and virtual machines in the cloud or on-premises, for both Windows and Linux servers, by installing the Log Analytics agent. Azure virtual machines are auto-provisioned in Security Center.

#### 3.2.2.1. Strengthen your security posture

You can improve your security posture using Azure Security Center to identify and perform hardening tasks across your machines, data services, and applications. With Azure Security Center, you can manage and enforce security policies to ensure compliance across your virtual machines, non-Azure servers, and Azure PaaS services.

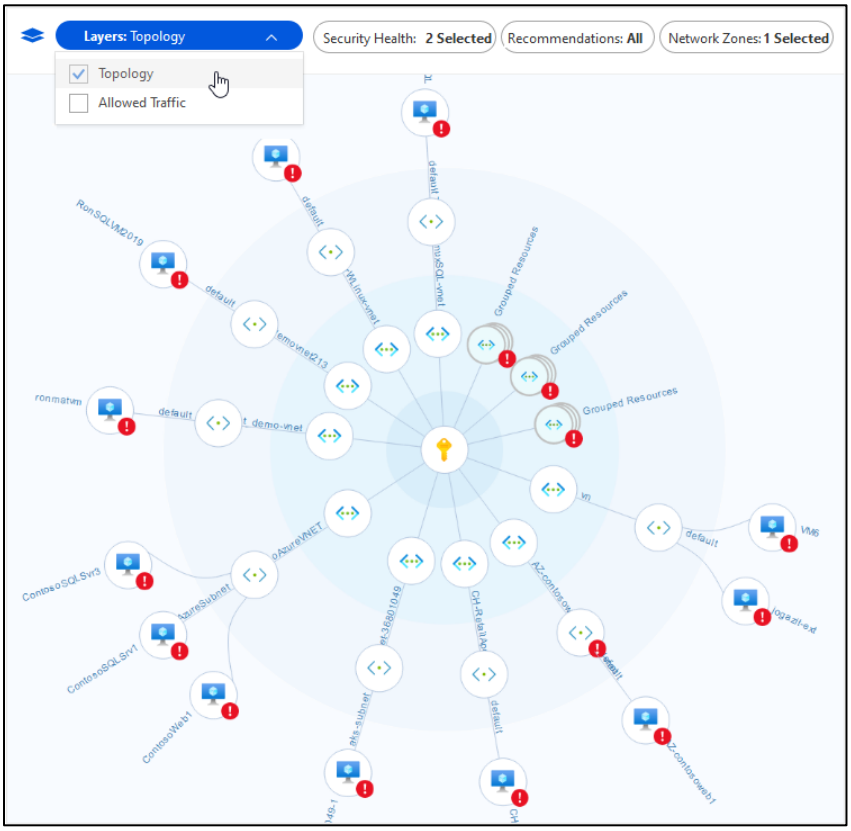
#### 3.2.2.2. Continuous Assessment

Security Center brings continuous assessment of your entire estate, discovering and reporting whether new and existing resources and assets are configured according to security compliance requirements. You'll get an ordered list of recommendations of what needs to be fixed to maintain maximum protection. Security Center groups the recommendations into security controls and adds a secure score value to each control. This process is crucial in enabling you to prioritize security work.

It is used to identify new and existing resources and assets.

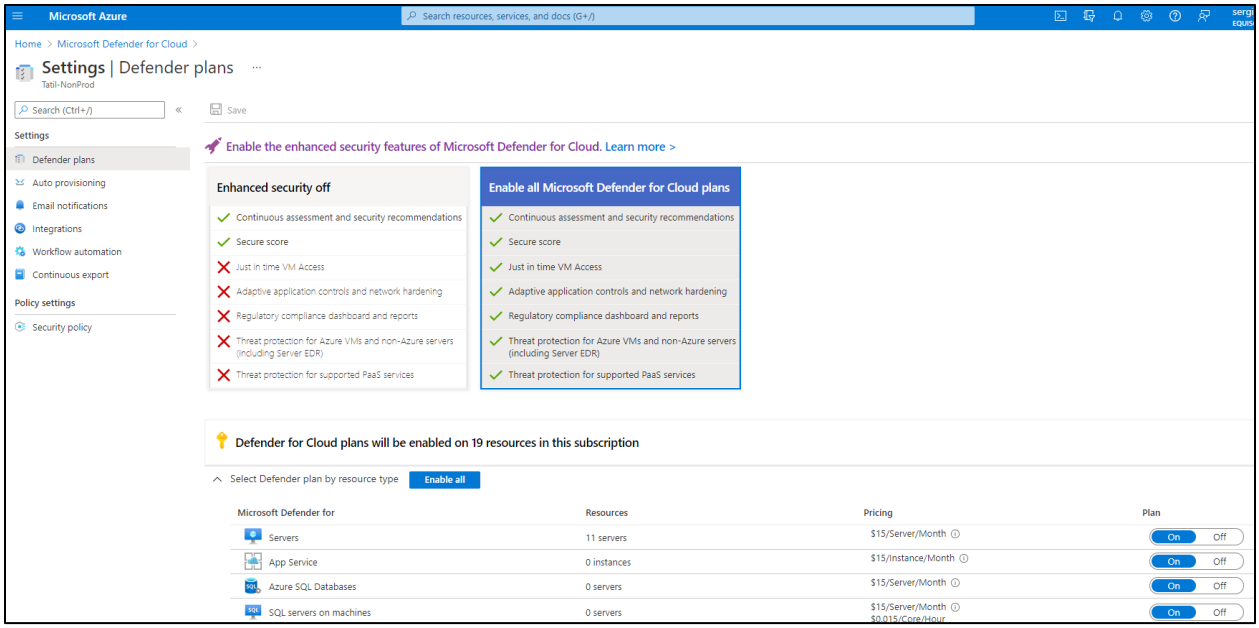
#### 3.2.2.3. Network map

One of the most powerful Security Center tools for continuously monitoring the security status of your network is the network map. Use the map to look at the topology of your workloads, so you can see if each node is properly configured. You'll see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.


## 3.2.2.4. Protect against Threats

Security Center's threat protection automatically correlates alerts in your environment based on cyber kill-chain analysis. It helps you to better understand the full story of an attack campaign, where it started and the impact it had on your resources.




With Azure Security Center's threat protection, you can detect and prevent threats on infrastructure as a service (IaaS), non-Azure servers, and platform as a service (PaaS). It comes with these features:

#### 3.2.2.4.1. Integration with Microsoft Defender

Security Center natively integrates with Microsoft Defender for Endpoint.

#### 3.2.2.4.2. Protect PaaS

Security Center helps you detect threats across Azure PaaS services. You can detect threats targeting Azure services, including Azure App Service, Azure SQL, Azure Storage Account, and more data services.

#### 3.2.2.4.3. Block brute force attacks

By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access.

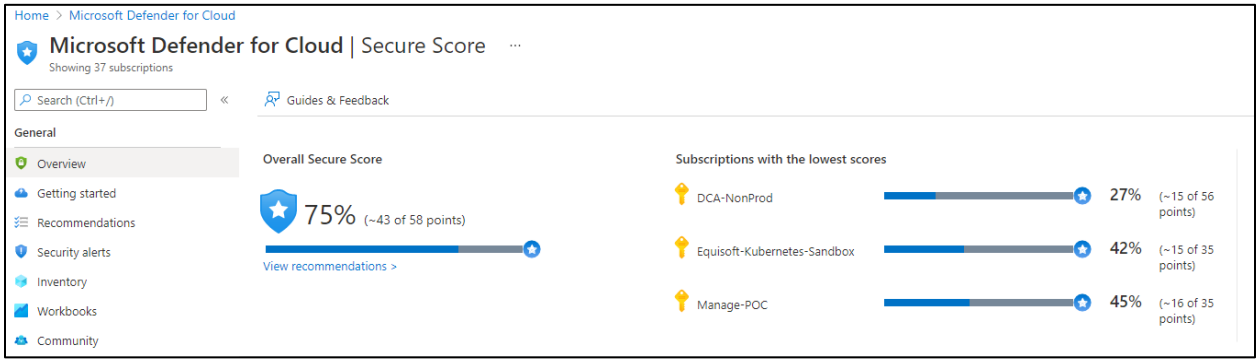
#### 3.2.2.4.4. Protect data services

Get assessments for potential vulnerabilities across Azure SQL and Storage services and recommendations for mitigating them.

### 3.2.3. 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 you can quickly see your current security situation: the higher the score, the lower the identified risk level.

The secure score is shown in the Azure portal pages as a percentage value. The underlying values are also clearly presented:

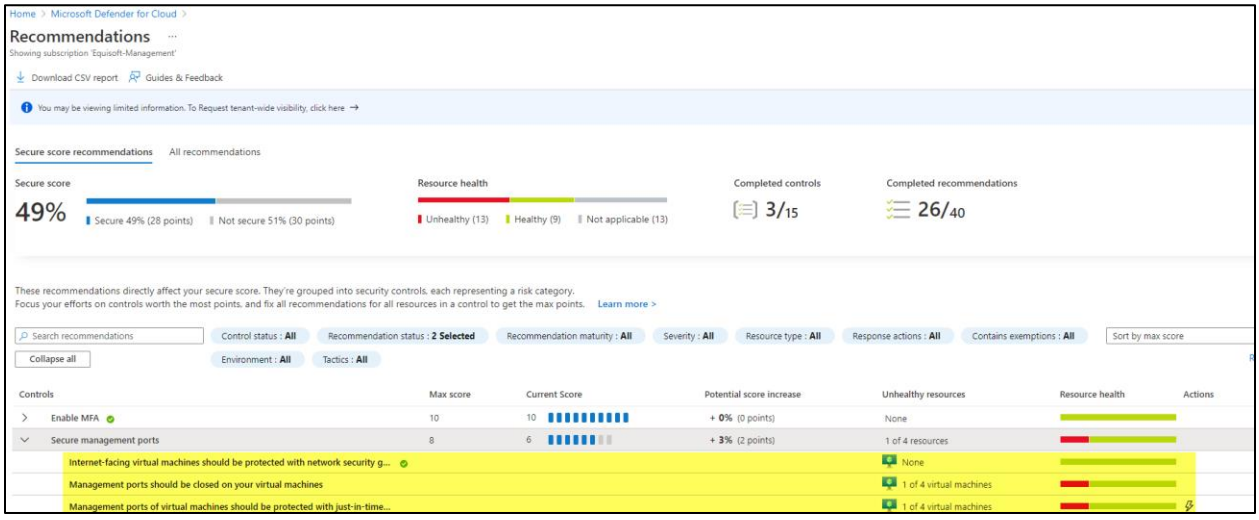



To increase your security and raise your score, review Security Center's recommendations page for the outstanding actions necessary. Each recommendation includes instructions to help you remediate the specific issue.

### 3.2.3.1. How to improve Security Score

To improve your secure score, remediate security recommendations from your recommendations list. You can manually remediate each recommendation for every resource or, by using the Quick Fix! option when available, apply remediation for a recommendation to a group of resources.

Use secure score to monitor your security posture, and easily implement actions to improve it.




### 3.2.3.2. Use cases Azure Defender

Azure Defender is a built-in tool that provides threat protection for workloads running in Azure, on-premises, and other clouds. Azure Defender is the leading Microsoft extended detection and response (XDR) solution for threat protection. Integrated with Azure Security Center, Azure Defender

protects your hybrid data, cloud-native services and servers, and integrates with your existing security workflows.

Built-in policies come with each Azure Defender plan, and you can add custom policies and initiatives. Also, you can add regulatory standards, such as NIST and Azure CIS, and the Azure Security Benchmark for a truly customized view of your compliance.

You'll find the Azure Defender dashboard in Azure Security Center. It provides visibility and control of your organization's cloud workload protection (CWP) features across the network.


#### 3.2.3.2.1. Scope of Azure Defender

Azure Defender comes with several different plans that can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment. The Azure Defender plans you can select from are:

##### 3.2.3.2.1.1. Azure Defender for servers

Azure Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.

##### 3.2.3.2.1.2. Azure Defender for App Service

Azure Defender for App Service uses the cloud scale to identify attacks targeting applications running over App Service.

##### 3.2.3.2.1.3. Azure Defender for Storage

Azure Defender for Storage detects potentially harmful activity on your Azure Storage accounts. Data can be protected, whether stored as blob containers, file shares, or data lakes.

#### 3.2.3.2.1.4. Azure Defender for SQL

Azure Defender for SQL extends Azure Security Center's data security package to secure your databases and their data wherever they're located.

#### 3.2.3.2.1.5. Azure Defender for Kubernetes

Azure Defender for Kubernetes provides the best cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.

#### 3.2.3.2.1.6. Azure Defender for container registries

Azure Defender for container registries protects all the Azure Resource Manager based registries in your subscription. Azure Defender scans all images pushed to the registry, or imported into the registry, or any images pulled within the last 30 days.

#### 3.2.3.2.1.7. Azure Defender for Key Vault

Azure Defender for Key Vault is Azure-native, advanced threat protection for Azure Key Vault, providing an extra layer of security intelligence.

### 3.2.3.3. Hybrid Cloud Protection

You can defend your Azure environment, and add Azure Defender capabilities to the hybrid cloud environment:

- Protect your non-Azure servers.
- Protect your virtual machines in other clouds (such as AWS and GCP).

To focus on what matters most, you can customize threat intelligence and prioritize alerts according to your specific environment.

### 3.2.3.4. Azure Defender Alerts

When Azure Defender detects a threat in any area of your environment, it generates an alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases, an option to trigger a logic app in response. The alerts can also be exported into Azure Sentinel.

### 3.2.3.5. Advanced protection

Azure Defender uses advanced analytics for tailored recommendations as they relate to your resources. These analytics might include securing the management ports of your VMs with just-in-time access and adaptive application controls to create allow lists for what apps should and shouldn't run on your machines.

#### 3.2.3.6. Advanced Protection

Azure Defender uses advanced analytics for tailored recommendations as they relate to your resources. These analytics might include securing the management ports of your VMs with just-in-time access and adaptive application controls to create allow lists for what apps should and shouldn't run on your machines.

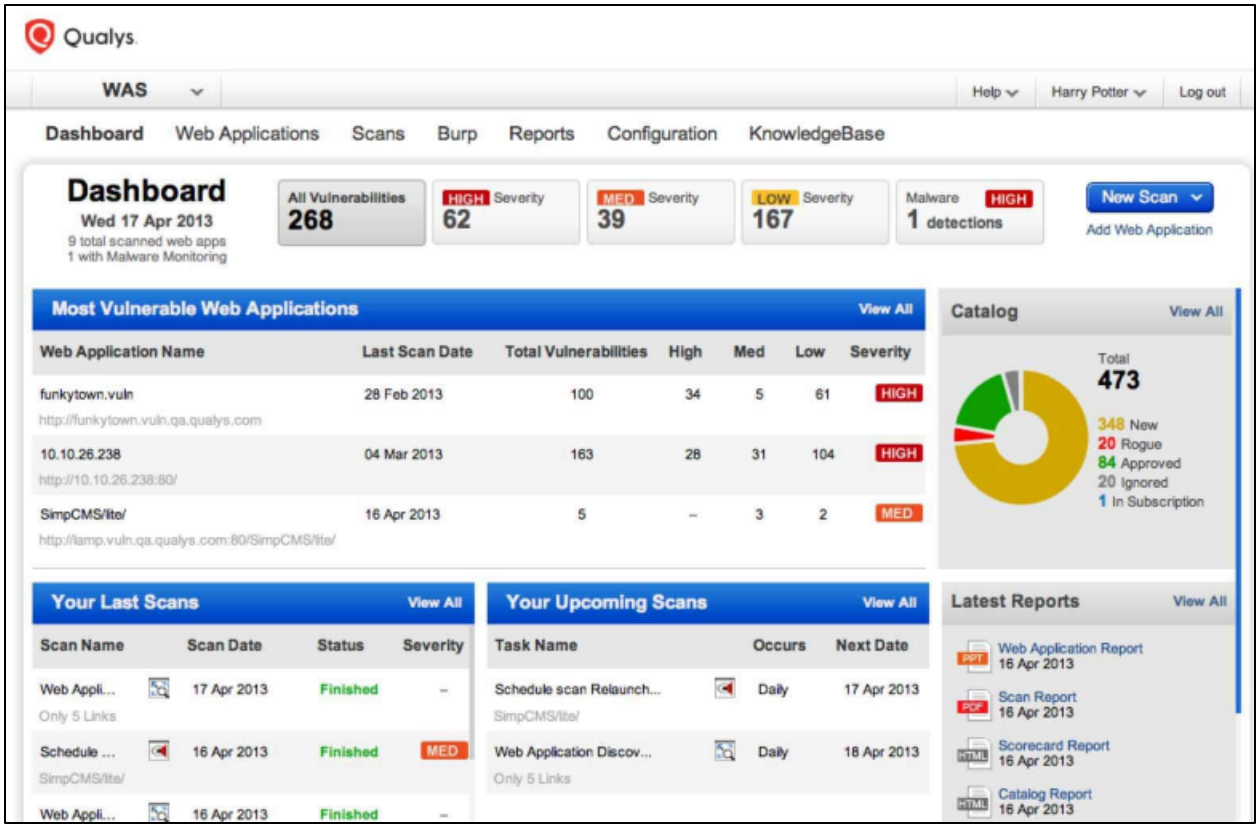
#### 3.2.3.7. Vulnerability assessment

Azure Defender includes vulnerability scanning for your virtual machines and container registries. Review the findings from these vulnerability scanners and respond to them all from within Security Center.

##### 3.2.3.7.1. Qualys Vulnerability assessment with Azure Security Center

include Qualys vulnerability assessment for no additional fee in Azure Security Center standard edition so that you have a richer set of security recommendations.  We are further extending Azure Security Center to include partner recommendations with Check Point, Tenable and CyberArk shipping integrations today.  We continue to focus on making sure you can maximize your valuable time addressing important security issues with new quick fix capabilities so that you can secure multiple items at once far faster than before, custom policy support, simplifications in secure score including making it a percentage.

Defender for Cloud includes vulnerability scanning for your machines at no extra cost. You don't need a Qualys license or even a Qualys account - everything's handled seamlessly inside Defender for Cloud. This page provides details of this scanner and instructions for how to deploy it.




### 3.2.4. Security Baselines for Azure

Microsoft's cybersecurity group and the Center for Internet Security (CIS), have developed best practices to help establish security baselines for the Azure platform. A baseline is the implementation of the benchmark on the individual Azure service.

CIS benchmarks have been used with Azure security services and tools to make security and compliance easier for customer applications running on Azure services. Every service comes with a baseline that's already designed to help provide security for most common-use cases. These baselines also provide a consistent experience when securing your environment.

#### 3.2.4.1. Azure Security Benchmark

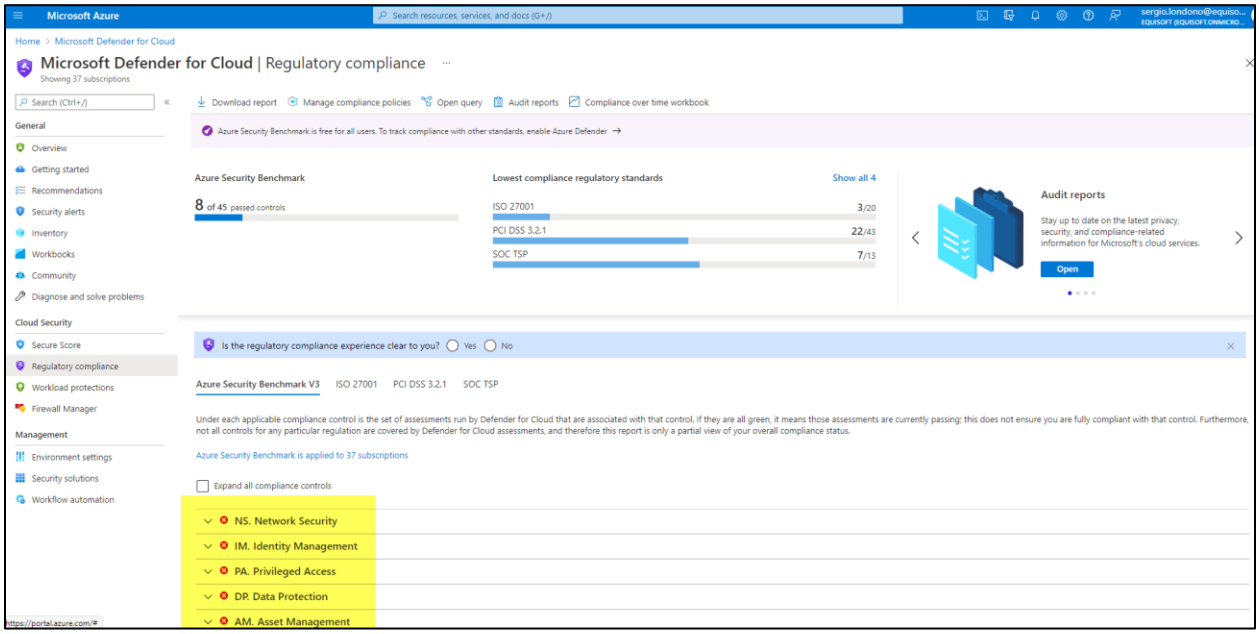
A benchmark contains security recommendations for a specific technology, such as Azure. The recommendations are categorized by the control to which they belong. The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. Some of the controls used in the ASB include network security, identity and access control, data protection, data recovery, incident response, and more.

Security baselines for Azure focus on cloud-centric control areas and apply guidance fro the Azure Security Benchmark.

Each Azure security baseline includes the following information:

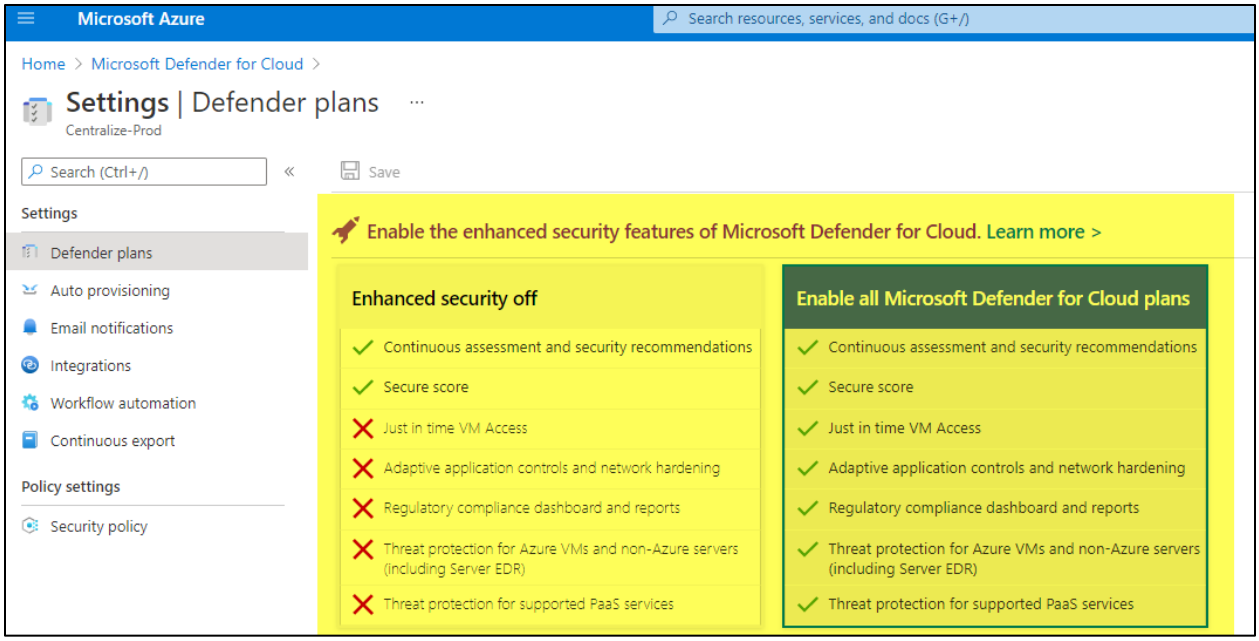
- **Azure ID**: The Azure Security Benchmark ID that corresponds to the recommendation.
- **Recommendation**: The recommendation provides a high-level description of the control.
- **Guidance**: The rationale for the recommendation and links to guidance on how to implement it.
- **Responsibility**: Who is responsible for implementing the control? Possible scenarios are customer responsibility, Microsoft responsibility, or shared responsibility.
- **Azure Security Center monitoring**: Does Azure Security Center monitor the control?

Security baselines are included for many Azure services.




## 3.2.5. Security Baselines for Azure

Cloud security posture management is essential for every organization. Microsoft Azure lets you decide how much you need to meet your regulatory, compliance, and corporate security needs.




#### 3.2.5.1. Azure Defender off

Security Center without Azure Defender is enabled free of charge on all your Azure subscriptions when you visit the Azure Security Center dashboard in the Azure portal for the first time, or if enabled programmatically via API.

#### 3.2.5.2. Azure Defender on

Enabling Azure Defender extends the free mode capabilities to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads.

## 3.3. Microsoft Sentinel (Legacy Azure Sentinel)

Build next-generation security operations with cloud and AI.

The foundation of Microsoft Sentinel is the data store; it combines high-performance querying, dynamic schema, and scales to massive data volumes. The Azure portal and all Microsoft Sentinel tools use a common API to access this data store.

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI). Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs – while reducing costs by as much as 48 per cent compared to traditional SIEMs.


## 3.3.1. Define the concepts of SIEM, SOAR, XDR

Protecting an organization's estate, resources, assets, and data from security breaches and attacks is an ongoing and escalating challenge. Recently, the business world changed almost overnight as large numbers of staff switched to remote working, creating an exploitable window for cybercriminals. IT departments rushed to patch and strengthen their staff's devices and their access to company assets and resources.

Cybercriminals will often escalate their activity in times of national or global crisis, looking to exploit the situation and find ways into your organization. Having a resilient and robust, industry-standard set of tools can help mitigate and prevent these exploits. Security information event management (SIEM), security orchestration automated response (SOAR), and extended detection and response (XDR) provide excellent security insights and security automation that can enhance an organization's network security perimeter.

Here, you'll gain a general understanding of the Azure tools that support SIEM, SOAR, and XDR in protecting your network's security perimeter.

To provide a comprehensive security perimeter, an organization needs to use a solution that embraces or combines all of the above systems.

### 3.3.1.1. Security information and event management (SIEM)

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

#### 3.3.1.2. Security orchestration automated response (SOAR)

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

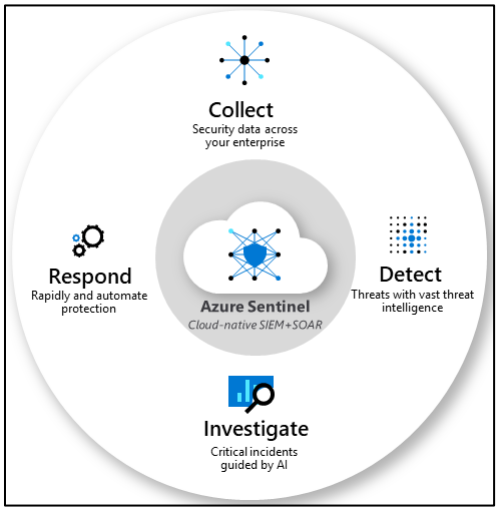
#### 3.3.1.3. Extended detection and response (XDR)

An XDR system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

### 3.3.2. How Sentinel provides integrated threat protection (SIEM/SOAR)

A SIEM/SOAR solution uses collect, detect, investigate and respond to identify and protect your organization's network perimeter

Effective management of an organization's network security perimeter requires the right combination of tools and systems. Microsoft Azure Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.




This diagram shows the end-to-end functionality of Azure Sentinel.

#### 3.3.2.1. Functionalities Azure Sentinel

Azure Sentinel helps enable end-to-end security operations. It starts with log ingestion and continues through to automated response to security alerts.

#### 3.3.2.1.1. Collect

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

#### 3.3.2.1.2. Detect

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

#### 3.3.2.1.3. Investigate

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

#### 3.3.2.1.4. Respond

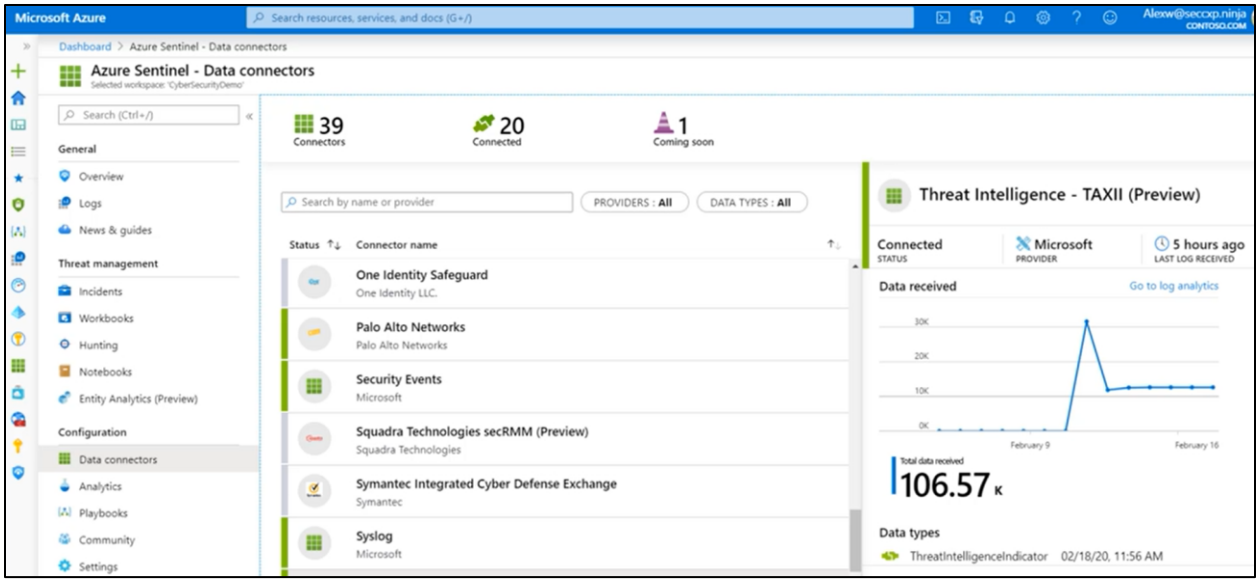
Respond to incidents rapidly with built-in orchestration and automation of common security tasks.

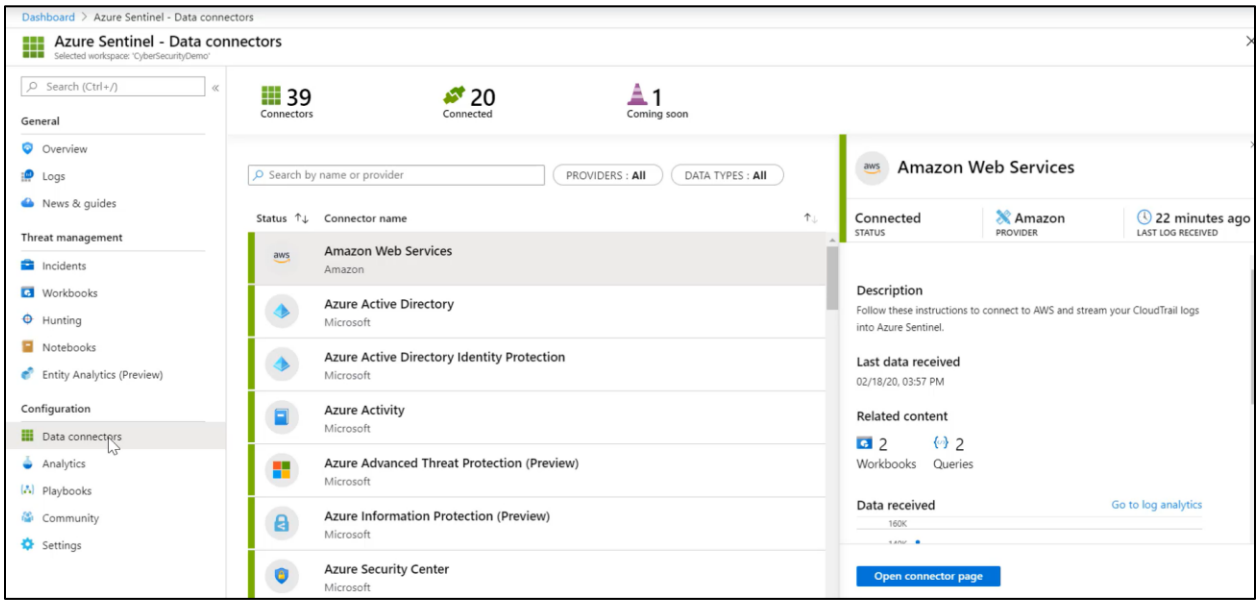
### 3.3.2.2. Connectors  Azure Sentinel to your data

Azure Sentinel comes with many connectors for Microsoft solutions, available out of the box and providing real-time integration. Included are Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Cloud App Security, and more.

First, you must have your data ingested into Azure Sentinel, for which you need data connectors. There are data connectors that cover a wide range of scenarios and sources, including but not limited to:

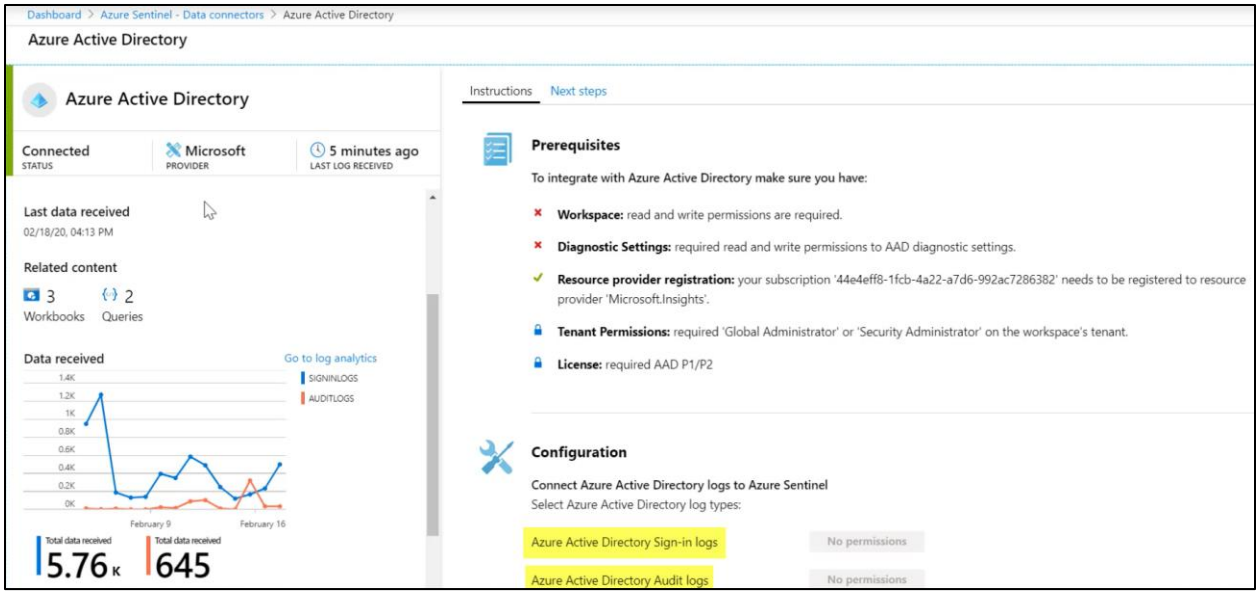
- syslog
- Windows Event Logs
- Common Event Format (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII), for threat intelligence
- Azure
- AWS services
    - CloudTrail
- Azure AD
- Microsoft 365
- Office 365




### 3.3.2.2.1. Azure Active Directory to Azure Sentinel

You can use Microsoft Sentinel's built-in connector to collect data from Azure Active Directory and stream it into Microsoft Sentinel. The connector allows you to stream the following log types:




#### 3.3.2.2.1.1. Sign-in logs

which contain information about interactive user sign-ins where a user provides an authentication factor.

The Azure AD connector now includes the following three additional categories of sign-in logs, all currently in PREVIEW:

#### 3.3.2.2.1.2. Non-interactive user sign-in logs

which contain information about sign-ins performed by a client on behalf of a user without any interaction or authentication factor from the user.

#### 3.3.2.2.1.3. Service principal sign-in logs

Service principal sign-in logs which contain information about sign-ins by apps and service principals that do not involve any user. In these sign-ins, the app or service provides a credential on its own behalf to authenticate or access resources.

#### 3.3.2.2.1.4. Managed Identity sign-in logs

Managed Identity sign-in logs which contain information about sign-ins by Azure resources that have secrets managed by Azure. For more information, see What are managed identities for Azure resources?

#### 3.3.2.2.1.5. Audit logs

Audit logs which contain information about system activity relating to user and group management, managed applications, and directory activities.

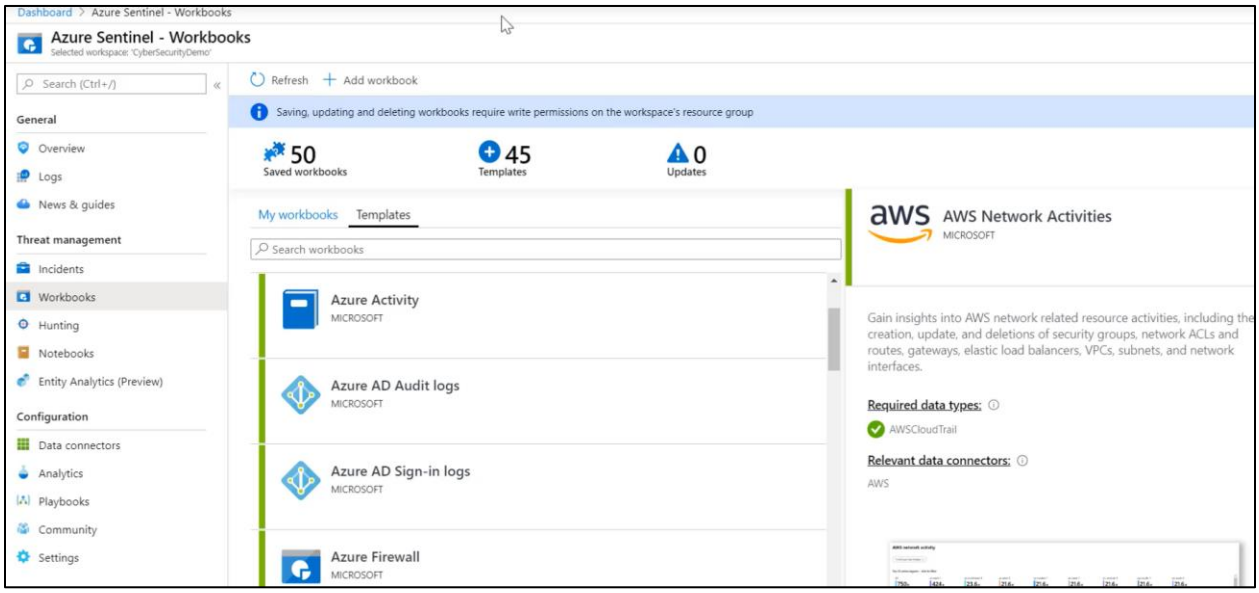
#### 3.3.2.2.1.6. Provisioning logs (also in PREVIEW)

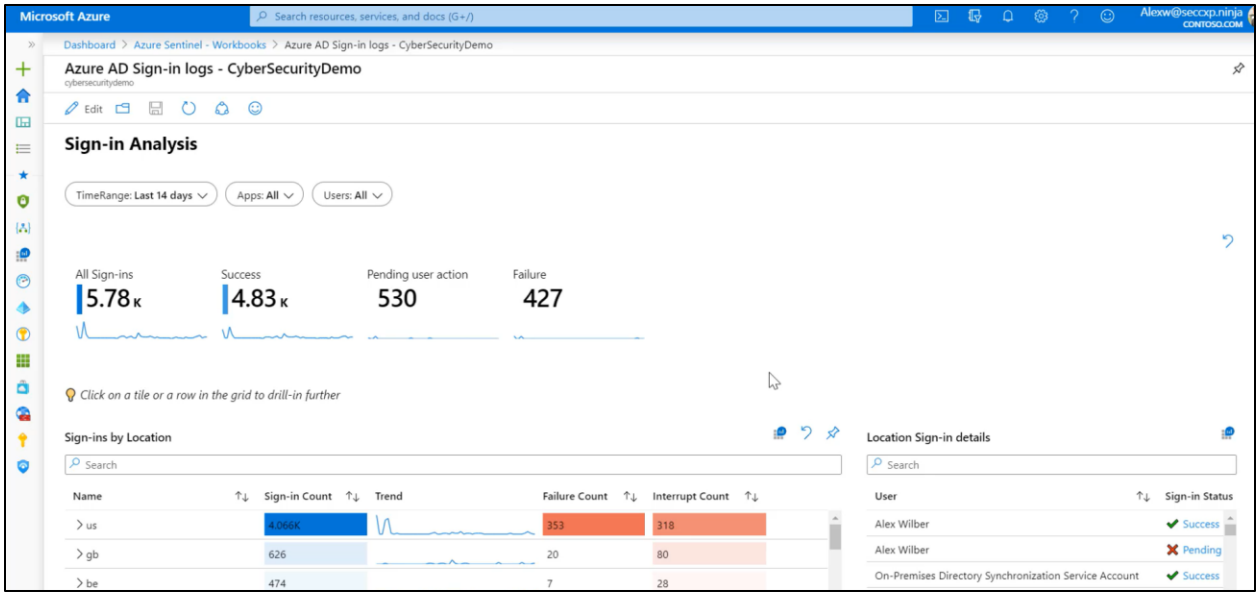
Provisioning logs which contain system activity information about users, groups, and roles provisioned by the Azure AD provisioning service.

### 3.3.2.3. Workbooks

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

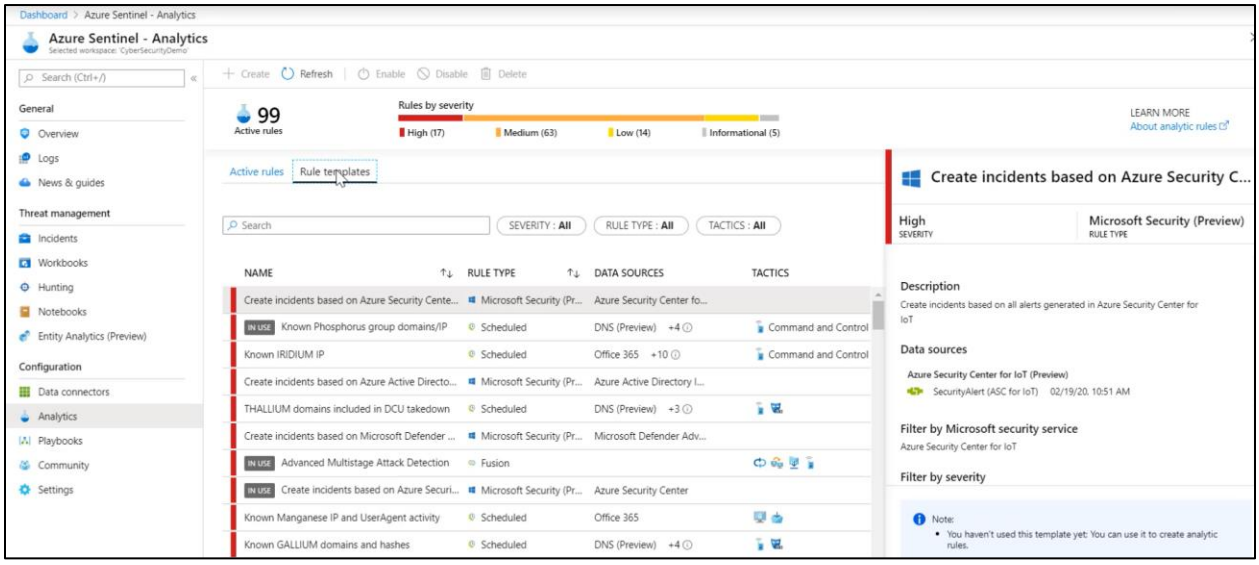
Using Azure Sentinel Integration with Azure Monitor Workbooks allos you to monitor data and provides versatility in creating custom workloads.






### 3.3.2.4. Analytics

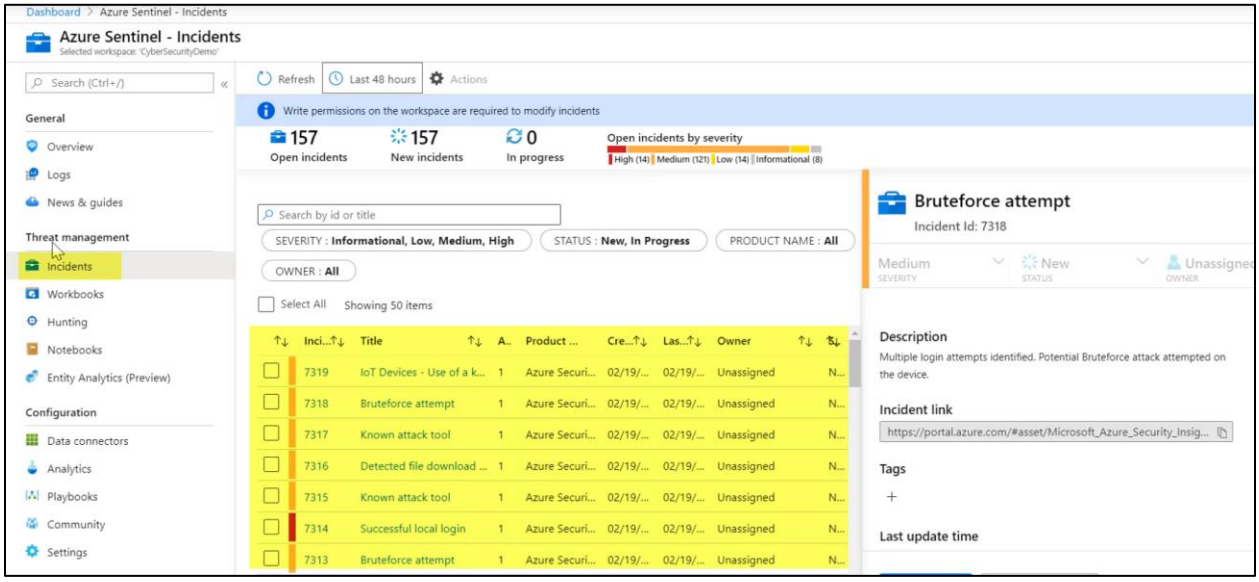
The power of Azure Sentinel comes into play here. Using built-in analytics alerts within the Azure Sentinel workspace, you'll get notified when anything suspicious occurs. There are various types of alerts, some of which you can edit to your own needs. Other alerts are built on machine learning models that are proprietary to Microsoft.

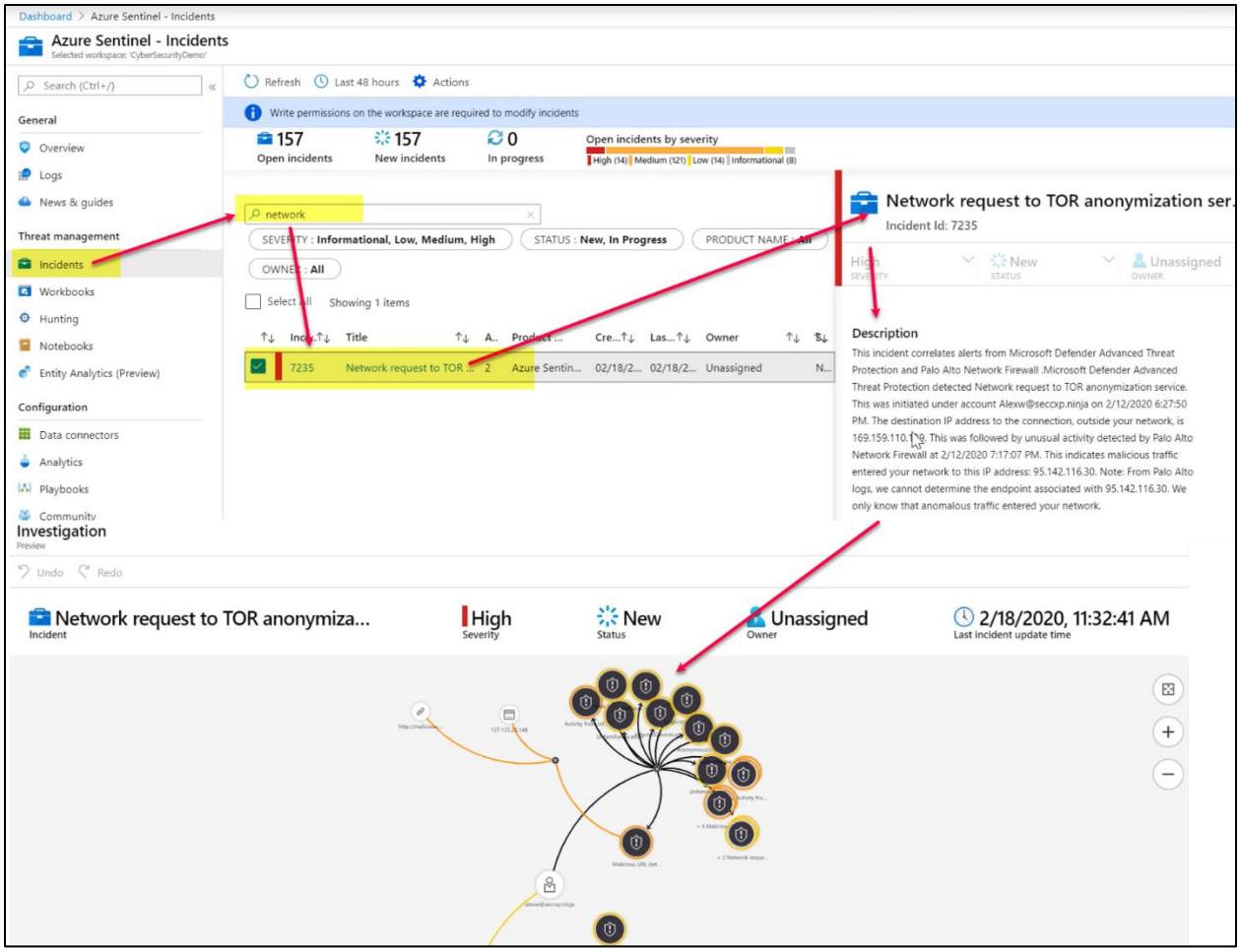



### 3.3.2.5. Incidents: Manage incident in Azure Sentinel

An incident is created when an alert that you've enabled is triggered. You can do standard incident management tasks like changing status or assigning incidents to individuals for investigation in Azure Sentinel. It also has investigation functionality, so you can visually investigate incidents by mapping entities across log data along a timeline.

Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve. Azure Sentinel uses analytics to correlate alerts into incidents. Use the built-in correlation rules as-is, or use them as a starting point to build your own.
Azure Sentinel also provides machine learning rules to map your network behavior and then look for anomalies across your resources. These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.





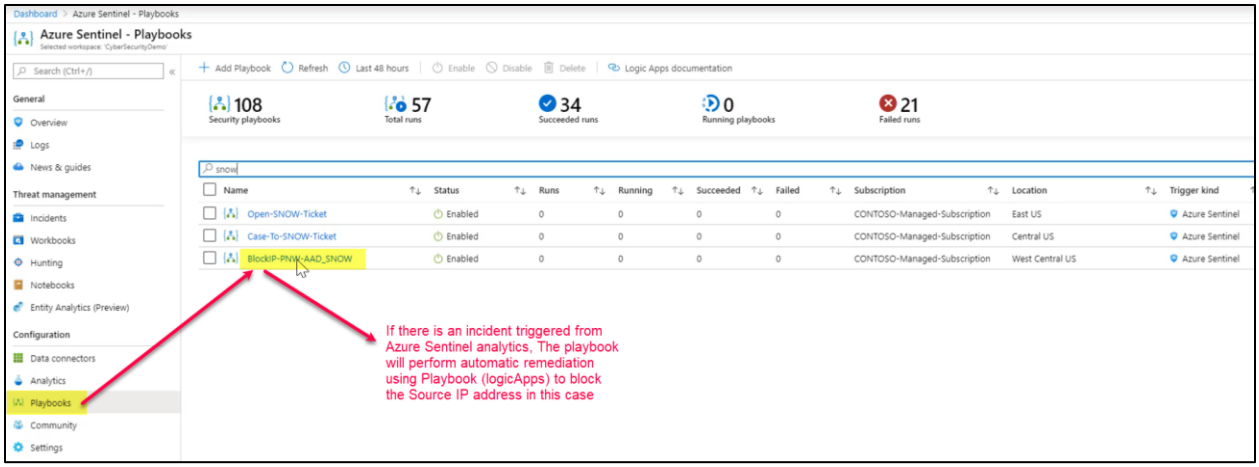

### 3.3.2.6. Security Automation and orchestration (SOAR)

You can use Azure Sentinel to automate some of your security operations and make your security operations center (SOC) more productive. Azure Sentinel integrates with Azure Logic Apps, so you can create automated workflows, or playbooks, in response to events. This functionality could be used for incident management, enrichment, investigation, or remediation.

### 3.3.2.7. Playbooks

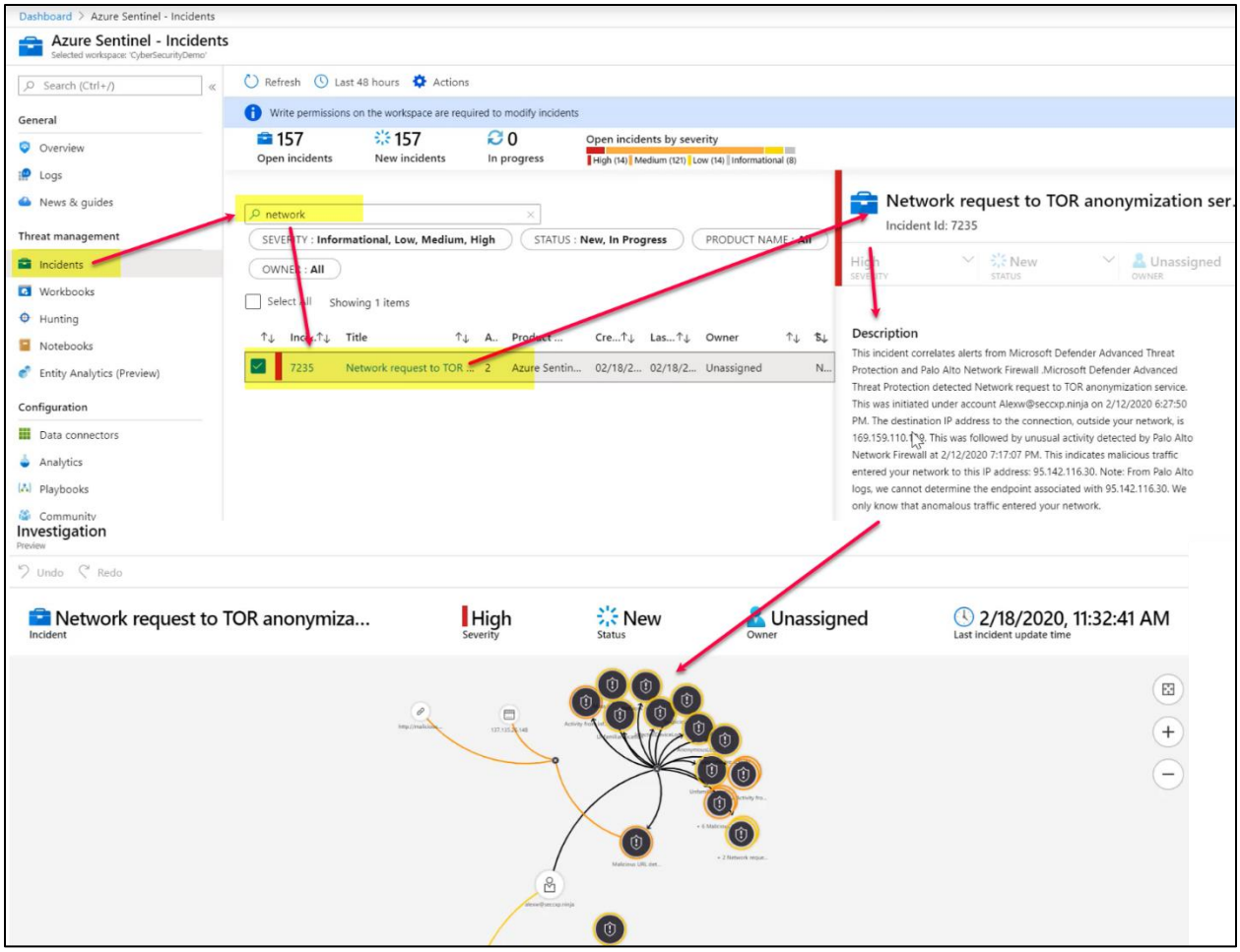
A security playbook is a collection of procedures that can help automate and orchestrate your response. It can be run manually or set to run automatically when specific alerts are triggered. Security playbooks in Azure Sentinel are based on Azure Logic Apps. You get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription you choose.

Playbooks allow you to automate your common task and simplify security orchestration.




### 3.3.2.8. Investigation

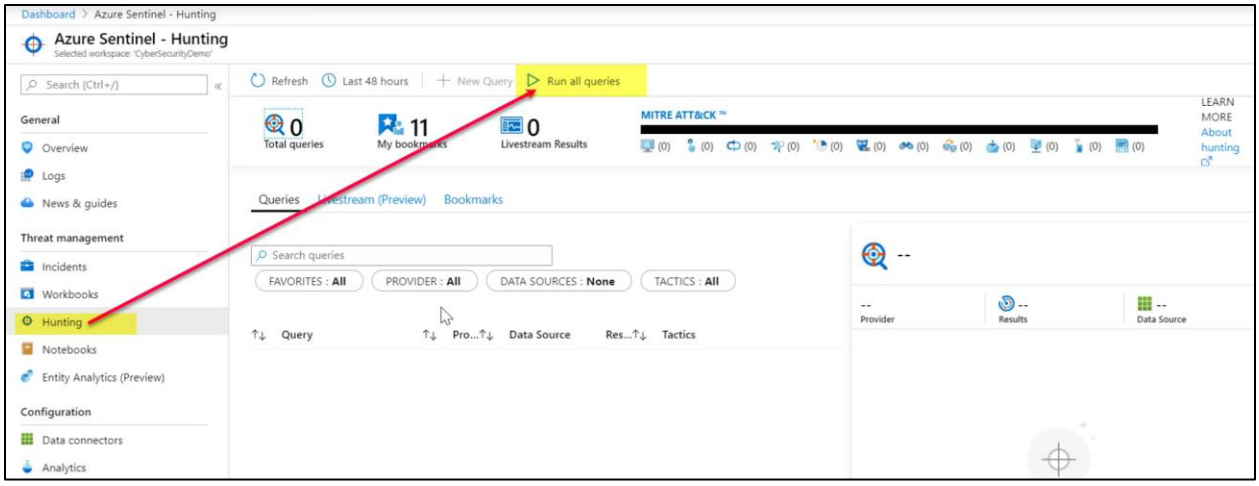
Currently in preview, Azure Sentinel's deep investigation tools help you to understand the scope of a potential security threat and find the root cause. You choose an entity on the interactive graph to ask specific questions, then drill down into that entity and its connections to get to the root cause of the threat.

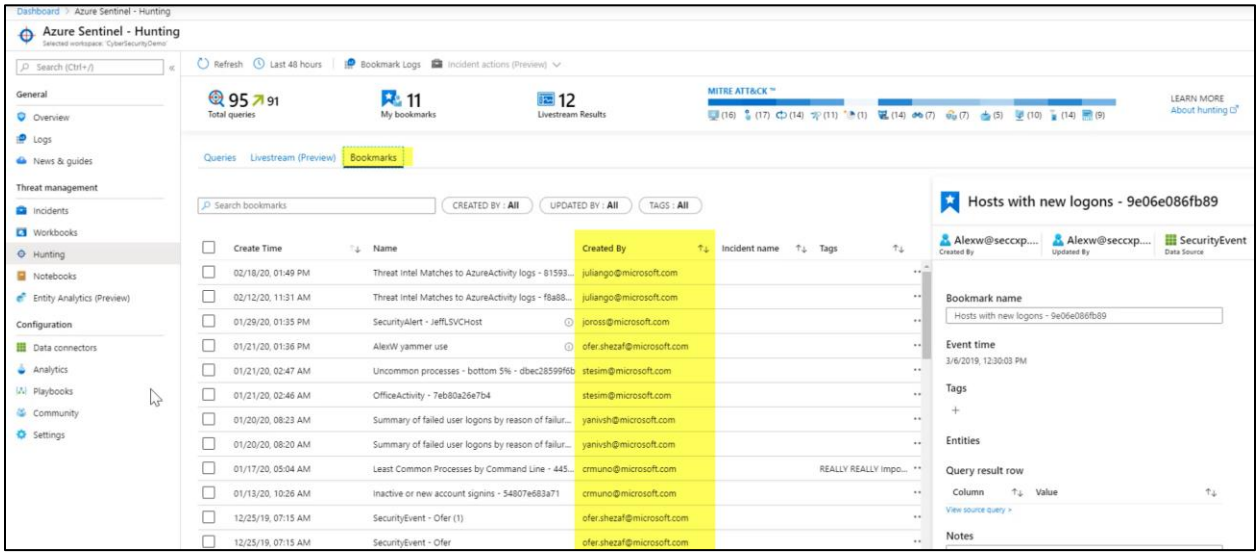



### 3.3.2.9. Hunting

Use Azure Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, to hunt proactively for security threats across your organization's data sources, before an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.

While hunting, you can bookmark interesting events, 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.

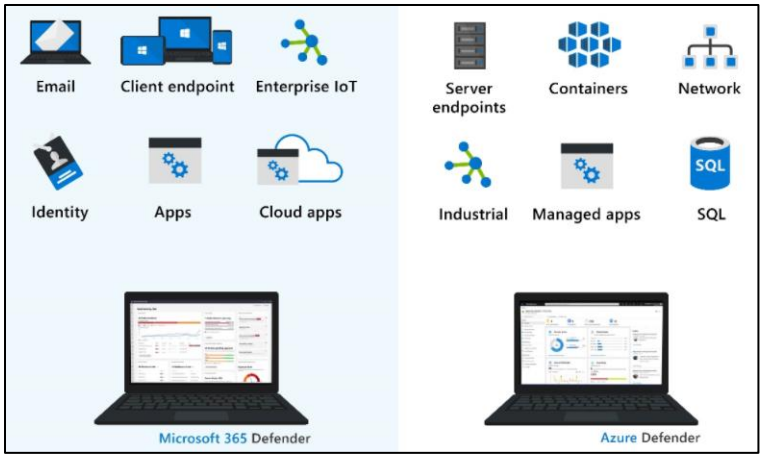



## 3.3.2.10. Integrated Threat Protection

Threat protection is a continuously evolving battle front. Cybercriminals look for any vulnerability they can exploit to steal, damage, or extort company data, assets, and resources. Microsoft provides a suite of tools that give extended detection and response (XDR) through Microsoft 365 Defender and Azure Defender.

Microsoft 365 Defender provides protection for email, client endpoints, enterprise IoT, Identity, Apps, and Cloud apps.




Both tools integrate smoothly with Azure Sentinel to provide a complete and thorough threat protection capability for your organization.


### 3.3.2.11. Azure Sentinel Cost

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

#### Capacity Reservations

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

#### Pay-As-You-Go

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

## 3.4.Threat protection With Microsoft 365 Defender

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

### 3.4.1. Microsoft Defender for Identities

Microsoft Defender for Identity, formerly Azure Advanced Threat Protection (Azure ATP), is a cloud-based security solution. It uses your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity covers these key areas:

- Monitor and profile user behavior and activities.
- Protect user identities and reduce the attack surface.
- Identify suspicious activities and advanced attacks across the cyberattack kill-chain.

#### 3.4.1.1. Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence. It gives insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.

#### 3.4.1.2. Monitor and profile user behavior and activities

Defender for Identity gives invaluable insights on identity configurations and suggested security best practices. Through security reports and user profile analytics, Defender for Identity helps reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack.

Defender for Identity security reports, help identify users and devices that authenticate using clear-text passwords. It also provides extra insights into how to improve security posture and policies.

#### 3.4.1.3. Identify suspicious activities and advanced attacks across the cyberattack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user. Attacks then quickly move laterally until the attacker accesses valuable assets. These assets might include sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill chain:

#### 3.4.1.4. Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Use the Defender for Identity attack timeline view and the intelligence of smart analytics to stay focused on what matters. Also, you can use Defender for Identity to quickly investigate threats, and gain insights across the organization for users, devices, and network resources.

Microsoft Defender for Identity protects your organization from compromised identities, advanced threats, and malicious insider actions.

### 3.4.2. Microsoft Defender for Office365 (Legacy: Office365 Advanced Threat Protection ATP)

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

Microsoft Defender for Office 365 covers these key areas:

Microsoft Defender for Office 365 is available in two plans. The plan you choose influences the tools you'll see and use. It's important to make sure you select the best plan to meet your organization's needs.

#### 3.4.2.1. Threat protection policies

Threat protection policies define threat protection policies to set the appropriate level of protection for your organization.

#### 3.4.2.2. Reports

Reports view real-time reports to monitor Microsoft Defender for Office 365 performance in your organization.

#### 3.4.2.3. Threat investigation and response capabilities

Use leading-edge tools to investigate, understand, simulate, and prevent threats.

#### 3.4.2.4. Automated investigation and response capabilities

Save time and effort investigating and mitigating threats.

Microsoft Defender for Office 365 is available in two plans. The plan you choose influences the tools you'll see and use. It's important to make sure you select the best plan to meet your organization's needs.

#### 3.4.2.5. Microsoft Defender For Office 365 Pricing options

##### 3.4.2.5.1. Microsoft Defender for Office 365 Plan 1

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

###### 3.4.2.5.1.1. Safe Attachments

Checks email attachments for malicious content.

###### 3.4.2.5.1.2. Safe Links

Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.

###### 3.4.2.5.1.3. Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.

###### 3.4.2.5.1.4. Anti-phishing protection

Detects attempts to impersonate your users and internal or custom domains.

###### 3.4.2.5.1.5. Real-time detections

A real-time report that allows you to identify and analyze recent threats.

##### 3.4.2.5.2. Microsoft Defender for Office 365 Plan 2

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

#### 3.4.2.5.2.1. Threat Trackers

Provide the latest intelligence on prevailing cybersecurity issues and allow an organization to take countermeasures before there's an actual threat.

#### 3.4.2.5.2.2. Threat Explorer

A real-time report that allows you to identify and analyze recent threats.

#### 3.4.2.5.2.3. Automated investigation and response (AIR)

Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.

#### 3.4.2.5.2.4. Attack Simulator

Allows you to run realistic attack scenarios in your organization to identify vulnerabilities.

### 3.4.2.5.3. Microsoft Defender for Office 365 availability

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

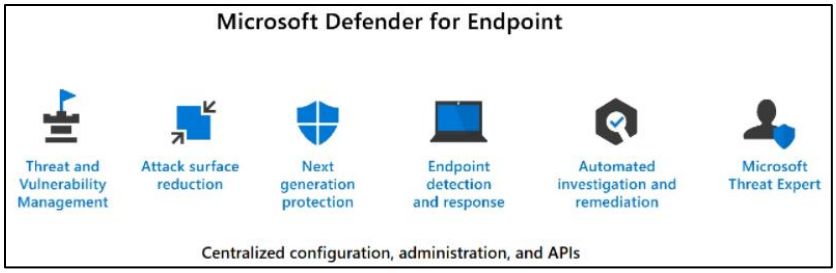
If your subscription doesn’t include Defender for Office 365, you can purchase it as an add-on.

Use Microsoft 365 Defender for Office 365 to protect your organization's collaboration tools and messages.

## 3.4.3. Microsoft Defender for Endpoint

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

This technology includes endpoint behavioral sensors that collect and process signals from the operating system, cloud security analytics that turn signals into insights, detections and recommendations, and threat intelligence to identify attacker tools, techniques, generate alerts.




Microsoft Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve overall security. Microsoft Defender for Endpoint integrates with various components in the Microsoft Defender suite, and with other Microsoft solutions including Intune and Azure Security Center.

Use Microsoft Defender for Endpoint to protect your organization's endpoints and respond to advanced threats.

Microsoft Defender for Endpoint includes:

#### 3.4.3.1. Threat and vulnerability management

A risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. It uses sensors on devices to avoid the need for agents or scans, and prioritizes vulnerabilities.

#### 3.4.3.2. Attack surface reduction

The attack surface reduction set of capabilities provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs; helping prevent apps from accessing dangerous locations

#### 3.4.3.3. Next generation protection

Brings together machine learning, big data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices in your enterprise organization.

#### 3.4.3.4. Endpoint detection and response

Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.

#### 3.4.3.5. Automated investigation and remediation

The automated investigation feature uses inspection algorithms and processes used by analysts (such as playbooks) to examine alerts and take quick remediation action to resolve breaches. This process significantly reduces the volume of alerts that must be investigated individually.

#### 3.4.3.6. Microsoft Threat Experts

A managed threat hunting service that provides Security Operation Centers (SOCs) with monitoring and analysis tools to ensure critical threats don't get missed.

#### 3.4.3.7. Management and APIs

Provides APIs to integrate with other solutions.

### 3.4.4. Microsoft Cloud App Security (MCAS)

Moving to the cloud increases flexibility for employees and IT teams. However, it also introduces new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance for supporting access while protecting critical data.

Microsoft Cloud App Security (MCAS) is a Cloud Access Security Broker (CASB). It's a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the cloud provider. Microsoft Cloud App Security provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Use this service to gain visibility into Shadow IT by discovering the cloud apps being used. You can control and protect data in the apps after you sanction them to the service.

#### 3.4.4.1. What is a Cloud Access Security Broker

A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use, wherever they're located, and whatever device they're using.

CASBs address security gaps in an organization's use of cloud services. Protection is provided by many capabilities across these areas: visibility to detect all cloud services, data security, threat protection, and compliance. These capability areas represent the basis of the Cloud App Security framework described below.

#### 3.4.4.2. The Cloud App Security framework

MCAS is built on a framework that provides the following capabilities:

#### 3.4.4.2.1. Discover and control the use of Shadow IT

Identify the cloud apps, and IaaS and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks.

#### 3.4.4.2.2. Protect your sensitive information anywhere in the cloud

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

#### 3.4.4.2.3. Protect against cyberthreats and anomalies

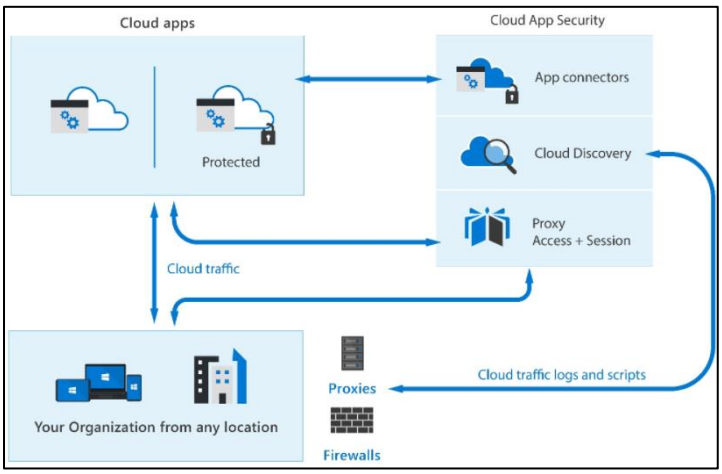
Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage, and remediate automatically to limit risks.

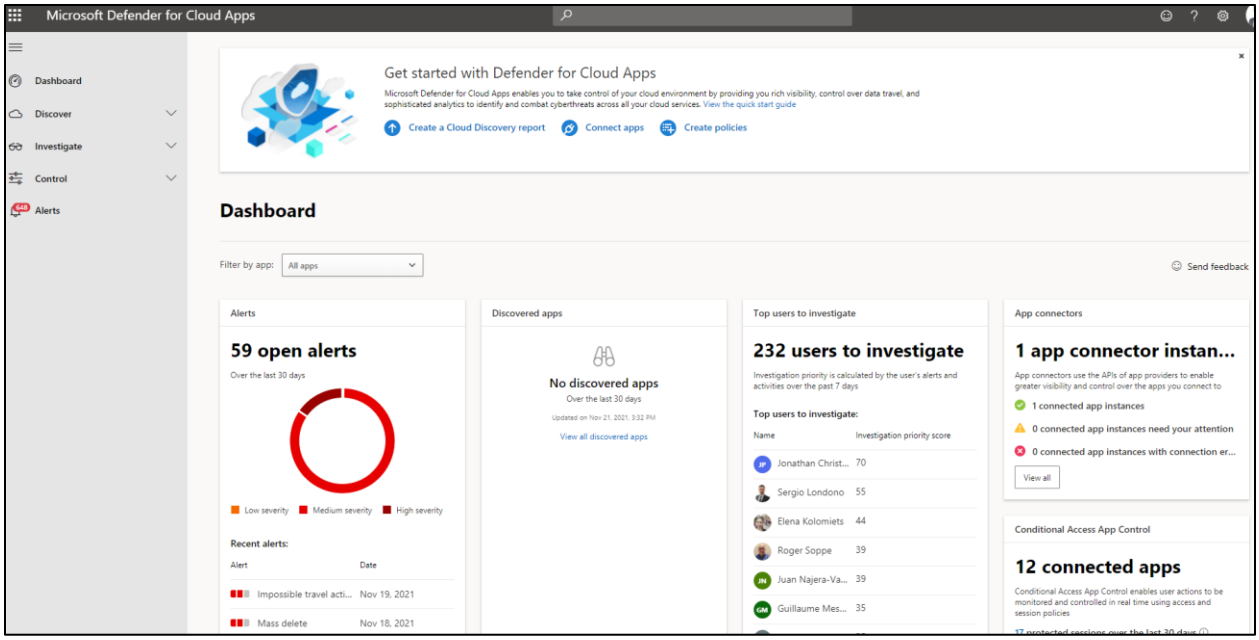
#### 3.4.4.2.4. Assess your cloud apps' compliance

Assess if your cloud apps meet relevant compliance requirements, including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.

### 3.4.4.3. Microsoft Cloud App Security architecture

Cloud App Security isn't only about how you strengthen or harden your servers to detect and prevent cyberattacks. It requires consideration on the architecture of your entire estate. How each server connects to its neighbor, and the routes that network traffic takes can make a significant difference your security model.

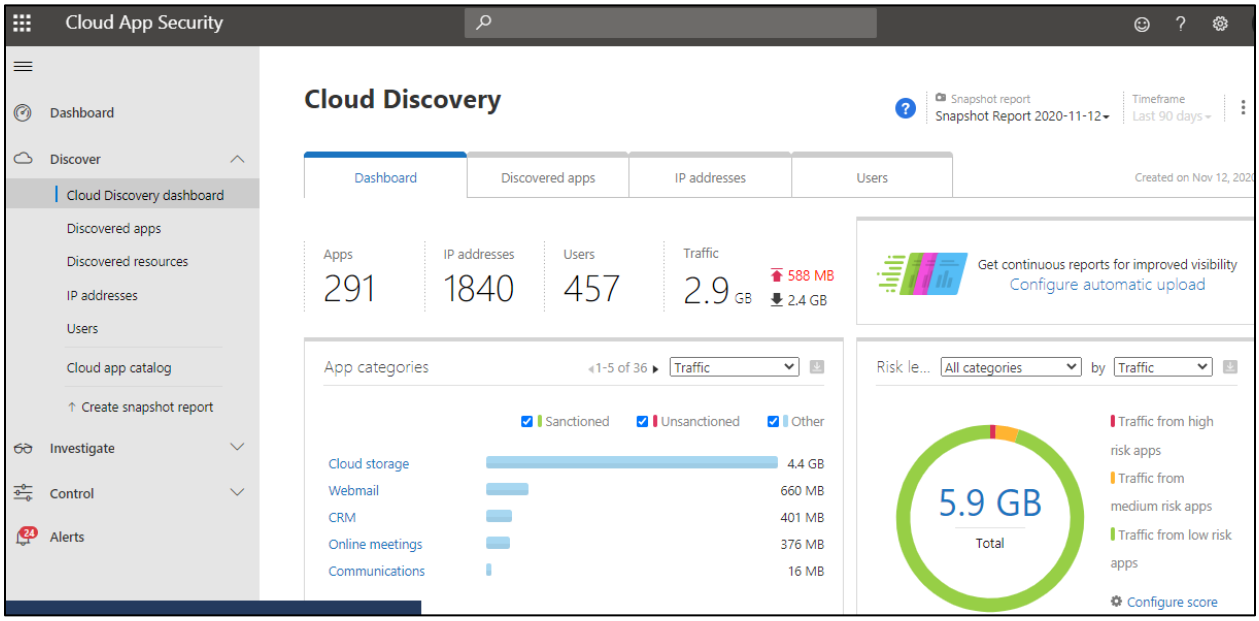





Cloud App Security integrates visibility with your cloud by:

### 3.4.4.3.1. Using Cloud Discovery

Using Cloud Discovery to map and identify your cloud environment and the cloud apps your organization uses. Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps being used.

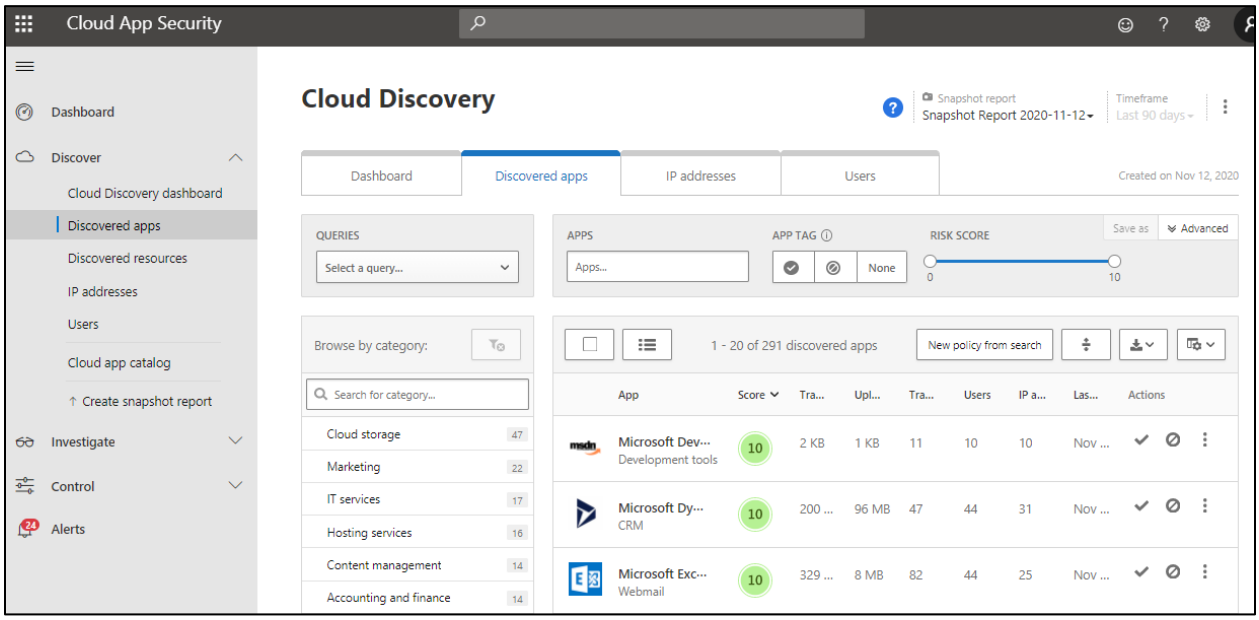


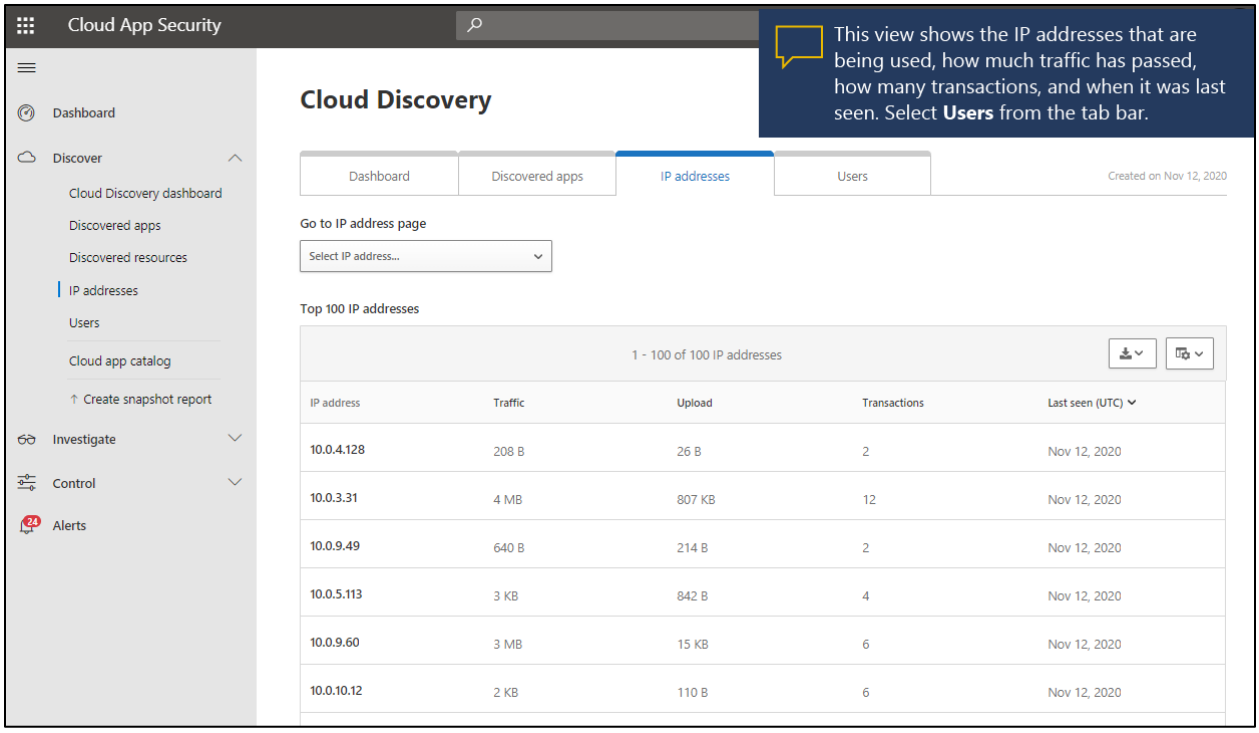
### 3.4.4.3.2. Sanctioning and unsanctioning apps in your cloud

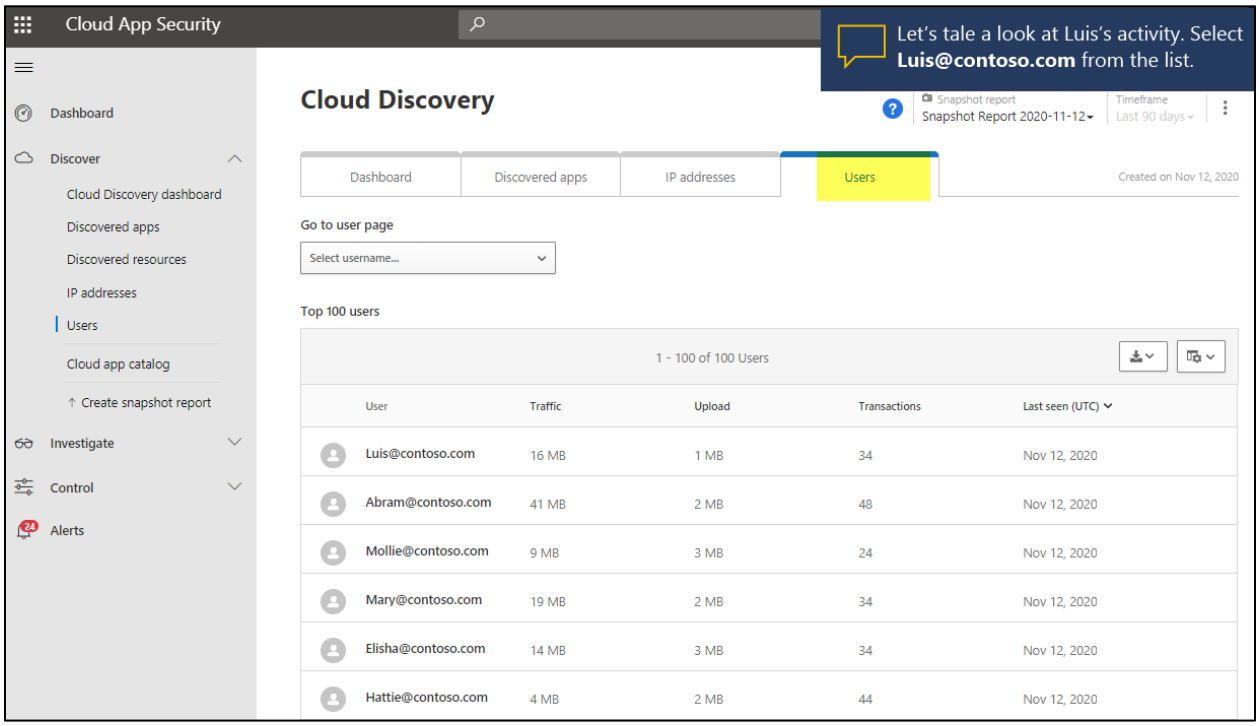
You can use Cloud App Security to sanction or unsanction apps in your organization by using the Cloud app catalog. It includes more than 16,000 cloud apps that are ranked and scored based on industry standards.

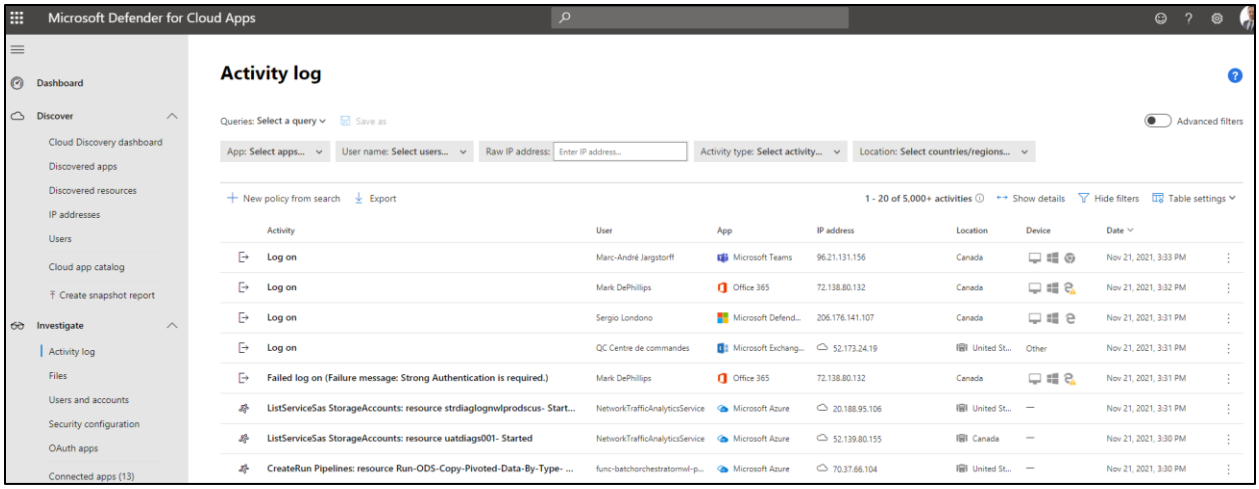
### 3.4.4.3.3. App Connectors

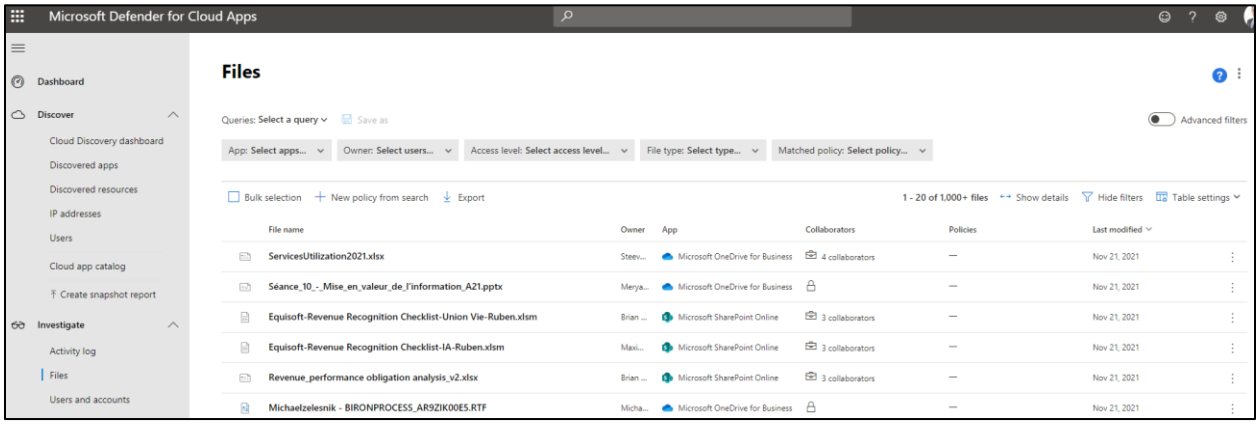
Using straightforward app connectors that use provider APIs for visibility and governance of apps you connect to. App connectors use APIs from cloud app providers to integrate their cloud apps with MCAS, extending control and protection. These connectors also give you access to information directly from cloud apps, for Cloud App Security analysis.

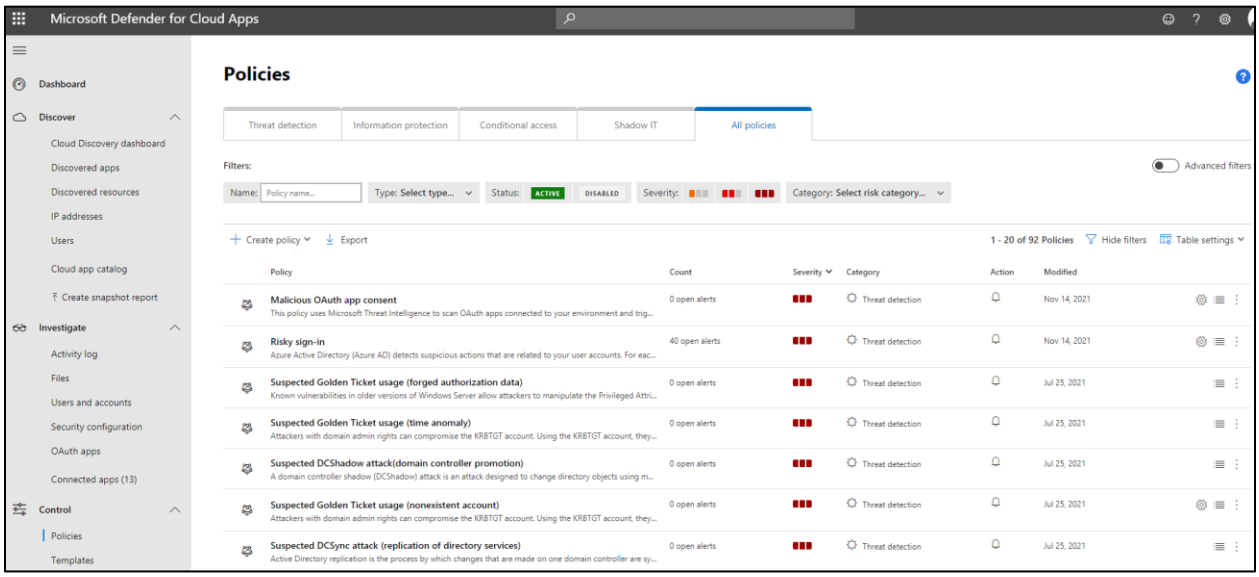



Cloud App Security
This view shows the IP addresses that are being used, how much traffic has passed, how many transactions, and when it was last seen. Select **Users** from the tab bar.
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Control
Alerts
Cloud Discovery
Dashboard
Discovered apps
IP addresses
Users
Created on Nov 12, 2020
Go to IP address page
Select IP address...
Top 100 IP addresses
1 - 100 of 100 IP addresses
IP address
Traffic
Upload
Transactions
Last seen (UTC)
10.0.4.128 208 B 26 B 2 Nov 12, 2020
10.0.3.31 4 MB 807 KB 12 Nov 12, 2020
10.0.9.49 640 B 214 B 2 Nov 12, 2020
10.0.5.113 3 KB 842 B 4 Nov 12, 2020
10.0.9.60 3 MB 15 KB 6 Nov 12, 2020
10.0.10.12 2 KB 110 B 6 Nov 12, 2020


Cloud App Security
Let's tale a look at Luis's activity. Select **Luis@contoso.com** from the list.
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Control
Alerts
Cloud Discovery
Snapshot report
Snapshot Report 2020-11-12
Timeframe
Last 90 days
Dashboard
Discovered apps
IP addresses
Users
Created on Nov 12, 2020
Go to user page
Select username...
Top 100 users
1 - 100 of 100 Users
User
Traffic
Upload
Transactions
Last seen (UTC)
Luis@contoso.com 16 MB 1 MB 34 Nov 12, 2020
Abram@contoso.com 41 MB 2 MB 48 Nov 12, 2020
Mollie@contoso.com 9 MB 3 MB 24 Nov 12, 2020
Mary@contoso.com 19 MB 2 MB 34 Nov 12, 2020
Elisha@contoso.com 14 MB 3 MB 34 Nov 12, 2020
Hattie@contoso.com 4 MB 2 MB 44 Nov 12, 2020


Microsoft Defender for Cloud Apps
Activity log
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Activity log
Files
Users and accounts
Security configuration
OAuth apps
Connected apps (13)
Queries: Select a query
Save as
Advanced filters
App: Select apps...
User name: Select users...
Raw IP address:
Enter IP address...
Activity type: Select activity...
Location: Select countries/regions...
New policy from search
Export
1 - 20 of 5,000+ activities
Show details
Hide filters
Table settings
Activity
User
App
IP address
Location
Device
Date
Log on
Marc-André Jargstorff
Microsoft Teams
96.21.131.156
Canada
Nov 21, 2021, 3:33 PM
Log on
Mark DePhillips
Office 365
72.138.80.132
Canada
Nov 21, 2021, 3:32 PM
Log on
Sergio Londono
Microsoft Defend...
206.176.141.107
Canada
Nov 21, 2021, 3:31 PM
Log on
QC Centre de commandes
Microsoft Exchang...
52.173.24.19
United St...
Other
Nov 21, 2021, 3:31 PM
Failed log on (Failure message: Strong Authentication is required.)
Mark DePhillips
Office 365
72.138.80.132
Canada
Nov 21, 2021, 3:31 PM
ListServiceSas StorageAccounts: resource strdiaglognwlprodscus- Start...
NetworkTrafficAnalyticsService
Microsoft Azure
20.188.95.106
United St...
Nov 21, 2021, 3:31 PM
ListServiceSas StorageAccounts: resource uatdiags001- Started
NetworkTrafficAnalyticsService
Microsoft Azure
52.139.80.155
Canada
Nov 21, 2021, 3:30 PM
CreateRun Pipelines: resource Run-ODS-Copy-Pivoted-Data-By-Type- ...
func-batchorchestratornwl-p...
Microsoft Azure
70.37.66.104
United St...
Nov 21, 2021, 3:30 PM


Microsoft Defender for Cloud Apps
Files
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Activity log
Files
Users and accounts
Queries: Select a query
Save as
Advanced filters
App: Select apps...
Owner: Select users...
Access level: Select access level...
File type: Select type...
Matched policy: Select policy...
Bulk selection
New policy from search
Export
1 - 20 of 1,000+ files
Show details
Hide filters
Table settings
File name
Owner
App
Collaborators
Policies
Last modified
ServicesUtilization2021.xlsx
Microsoft OneDrive for Business
4 collaborators
Nov 21, 2021
Séance_10_-_Mise_en_valeur_de_l'information_A21.pptx
Microsoft OneDrive for Business
Nov 21, 2021
Equisoft-Revenue Recognition Checklist-Union Vie-Ruben.xlsm
Microsoft SharePoint Online
3 collaborators
Nov 21, 2021
Equisoft-Revenue Recognition Checklist-IA-Ruben.xlsm
Microsoft SharePoint Online
3 collaborators
Nov 21, 2021
Revenue_performance obligation analysis_v2.xlsx
Microsoft SharePoint Online
3 collaborators
Nov 21, 2021
Michaelzelesnik - BIRONPROCESS_AR9ZIK00E5.RTF
Microsoft OneDrive for Business
Nov 21, 2021


Microsoft Defender for Cloud Apps
Policies
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Activity log
Files
Users and accounts
Security configuration
OAuth apps
Connected apps (13)
Control
Policies
Templates
Threat detection
Information protection
Conditional access
Shadow IT
All policies
Filters:
Advanced filters
Name:
Policy name...
Type: Select type...
Status:
ACTIVE
DISABLED
Severity:
Category: Select risk category...
Create policy
Export
1 - 20 of 92 Policies
Hide filters
Table settings
Policy
Count
Severity
Category
Action
Modified
Malicious OAuth app consent
This policy uses Microsoft Threat Intelligence to scan OAuth apps connected to your environment and trig...
0 open alerts
Threat detection
Nov 14, 2021
Risky sign-in
Azure Active Directory (Azure AD) detects suspicious actions that are related to your user accounts. For eac...
40 open alerts
Threat detection
Nov 14, 2021
Suspected Golden Ticket usage (forged authorization data)
Known vulnerabilities in older versions of Windows Server allow attackers to manipulate the Privileged Attri...
0 open alerts
Threat detection
Jul 25, 2021
Suspected Golden Ticket usage (time anomaly)
Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they...
0 open alerts
Threat detection
Jul 25, 2021
Suspected DCShadow attack(domain controller promotion)
A domain controller shadow (DCShadow) attack is an attack designed to change directory objects using m...
0 open alerts
Threat detection
Jul 25, 2021
Suspected Golden Ticket usage (nonexistent account)
Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they...
0 open alerts
Threat detection
Jul 25, 2021
Suspected DCSync attack (replication of directory services)
Active Directory replication is the process by which changes that are made on one domain controller are sy...
0 open alerts
Threat detection
Jul 25, 2021

#### 3.4.4.3.4. Conditional Access App Control protection

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. You can use policies to define users' behavior in the cloud. Use policies to detect risky behavior, violations, or suspicious data points and activities in your cloud environment.

### 3.4.4.4. Office 365 Cloud App Security

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

It offers a subset of the core MCAS features.

### 3.4.4.5. Enhanced Cloud App Discovery in Azure Active Directory

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

It provides a reduced subset of the MCAS discovery capabilities.

Use Microsoft Cloud App Security to intelligently and proactively identify and respond to threats across your organization's Microsoft and non-Microsoft cloud services.

## 3.5.Security Management Capabilities of Microsoft 365

The Microsoft 365 Defender portal, provides a centralized site where you can manage security across Microsoft identities, data, devices, and apps. Throughout this module, you will explore the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, dashboards, reports, and incident management.

In this module, you will:

- Describe and explore Microsoft 365 Defender portal.
- Describe how to use Microsoft Secure score.
- Explore security reports and dashboards.
- Describe incidents and incident management capabilities.

### 3.5.1. Microsoft 365 Defender Portal

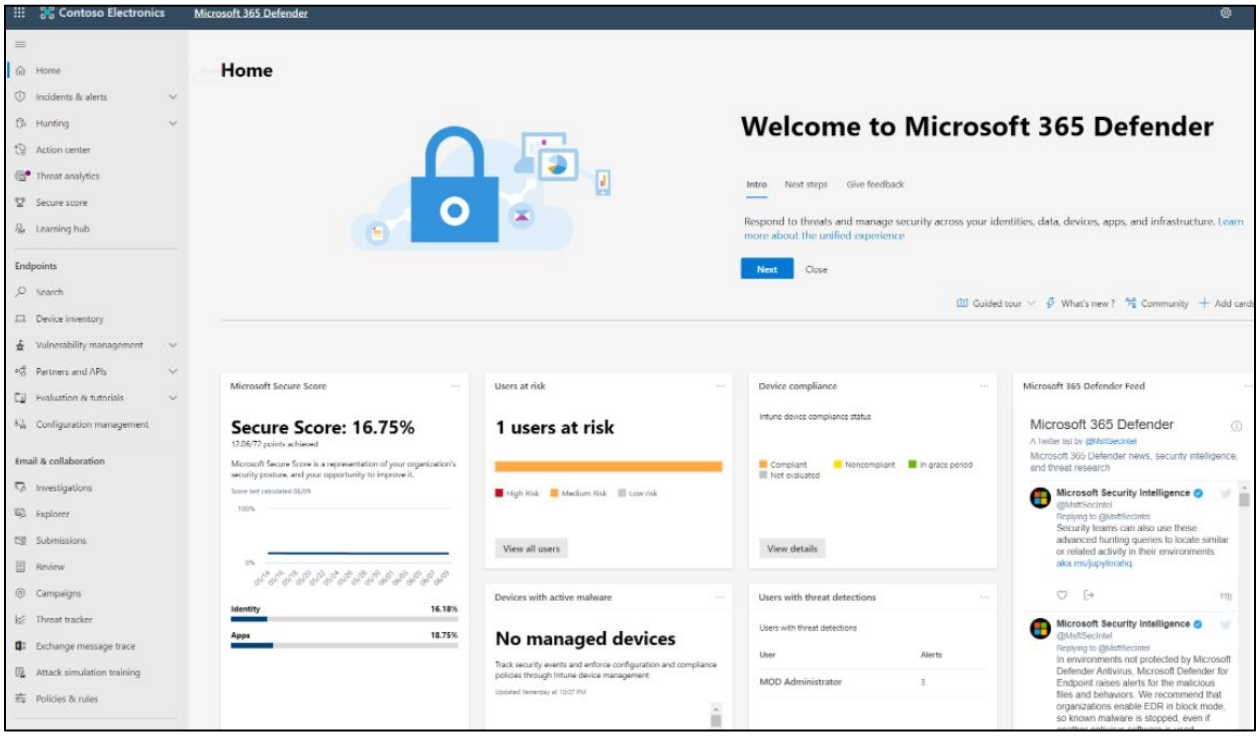
The Microsoft 365 Defender portal (previously Microsoft 365 security center) combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.

The Microsoft 365 Defender portal is a specialized workspace designed to meet the needs of security teams and provides actionable insights to help reduce risks and safeguard your digital estate.

Here you can view the security health of your organization, act to configure devices, users, and apps, and get alerts for suspicious activity. The Microsoft 365 Defender portal helps security admins and security operations teams manage and protect their organization.

The Microsoft 365 Defender portal home page shows many of the common cards that security teams need. The composition of cards and data depends on the user role. Because the Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day-to-day jobs.

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




The Microsoft 365 Defender portal allows admins to tailor the navigation pane to meet daily operational needs. Admins can customize the navigation pane to show or hide functions and services

based on their specific preferences. Customization is specific to the individual admin, so other admins won't see these changes.

The navigation pane in the Microsoft 365 Defender portal includes these options and many more:

#### 3.5.1.1. Home

Get an at-a-glance view of the overall security health of your organization.

#### 3.5.1.2. Incidents

See the broader story of an attack by connecting the dots seen on individual alerts on entities. You'll know exactly where an attack started, what devices are impacted, who was affected, and where the threat has gone.

#### 3.5.1.3. Alerts

Have greater visibility into all the alerts across your Microsoft 365 environment. Includes alerts from Microsoft Cloud App Security, Microsoft Defender for Office 365, Azure Active Directory, Microsoft Defender for Identity, and Microsoft Defender for Endpoint.

#### 3.5.1.4. Hunting

Proactively search for malware, suspicious files, and activities in your Microsoft 365 organization.

#### 3.5.1.5. Action center

Reduce the volume of alerts your security team must address manually, allowing them to focus on more sophisticated threats and other high-value initiatives.

#### 3.5.1.6. Threat analytics

Track and respond to emerging threats with an integrated Microsoft 365 Defender threat analytics experience

#### 3.5.1.7. Secure Score

Improve your overall security posture with Microsoft Secure Score. This page provides an all up summary of the different security features and capabilities you've enabled and includes recommendations for areas to improve.

#### 3.5.1.8. Learning hub

The Microsoft 365 Defender portal includes a learning hub that bubbles up official guidance from resources such as the Microsoft security blog, the Microsoft security community on YouTube, and the official documentation at docs.microsoft.com.

#### 3.5.1.9. Endpoints

Microsoft Defender for Endpoints delivers preventative protection, post-breach detection, automated investigation, and response for devices in your organization.

#### 3.5.1.10. Email & collaboration

Microsoft Defender for Office 365 helps organizations secure their enterprise with a set of prevention, detection, investigation and hunting features to protect email, and Office 365 resources.

#### 3.5.1.11. Reports

Get the detail and information you need to better protect your users, devices, apps, and more.

#### 3.5.1.12. Permissions & roles

Access to Microsoft 365 Defender is configured with Azure Active Directory global roles or by using custom roles.

### 3.5.2. Microsoft Secure Score

Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture. The higher the score, the better your protection.

Secure Score helps organizations:

- Report on the current state of their security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Compare benchmarks and establish key performance indicators (KPIs).

Points are given for the following actions:

- Configuring recommended security features.
- Doing security-related tasks.
- Addressing the improvement action with a third-party application or software, or an alternate mitigation.

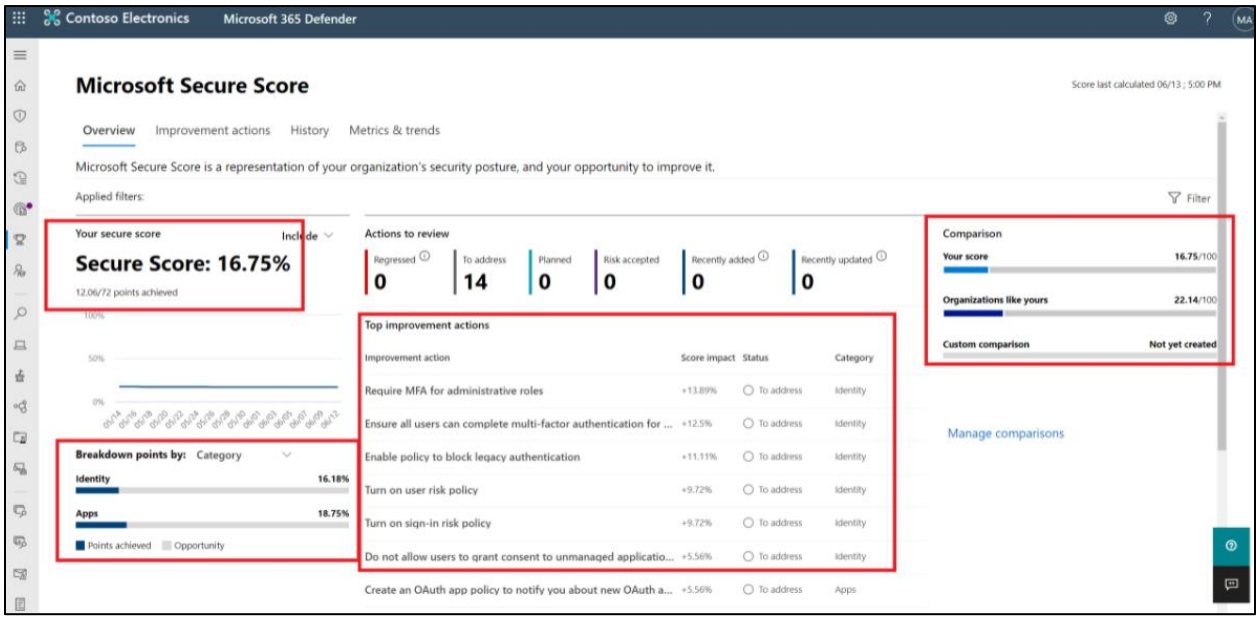
Some improvement actions only give points when fully completed. Others give partial points if they're completed for some devices or users. If you can't, or don't want to, enact one of the improvement actions, you can choose to accept the risk or remaining risk.

If you have a license for one of the supported Microsoft products, you'll see related recommendations. Secure Score will show all possible improvements for the product, whatever the license edition, subscription, or plan. You'll then see all the security best practices and improvements that can be made to your score.

Your absolute security posture, represented by Secure Score, stays the same whatever licenses your organization owns for a specific product. Keep in mind that security should be balanced with usability, and not every recommendation can work for your environment.

Currently Microsoft Secure Score supports recommendations for Microsoft 365 (including Exchange Online), Azure Active Directory, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Cloud App Security. New recommendations are being added to Secure Score all the time.

The image below shows an organization's Secure Score, a breakdown of the score by points, and the improvement actions that can boost the organization's score. Finally, it provides an indication of how well the organization's Secure Score compares to other similar organizations.




### 3.5.2.1. Differences between the Azure and Microsoft Secure Score

There's a Secure Score for both Microsoft 365 Defender and Azure Defender, but they're subtly different.

Both the Azure and Microsoft Secure Score provide a list of steps you can take to improve your score.

The steps you can take to improve your score are called security recommendations and they're grouped into security controls.

Use Microsoft Secure Score to understand and rapidly improve your organization's security posture.

#### 3.5.2.1.1. Secure Score in the Azure Security Center

Secure Score in the Azure Security Center is a measure of the security posture of your Azure subscriptions.

In the Azure Secure Score, scores are assessed for each subscription.

#### 3.5.2.1.2. Secure Score in the Microsoft 365 Defender portal

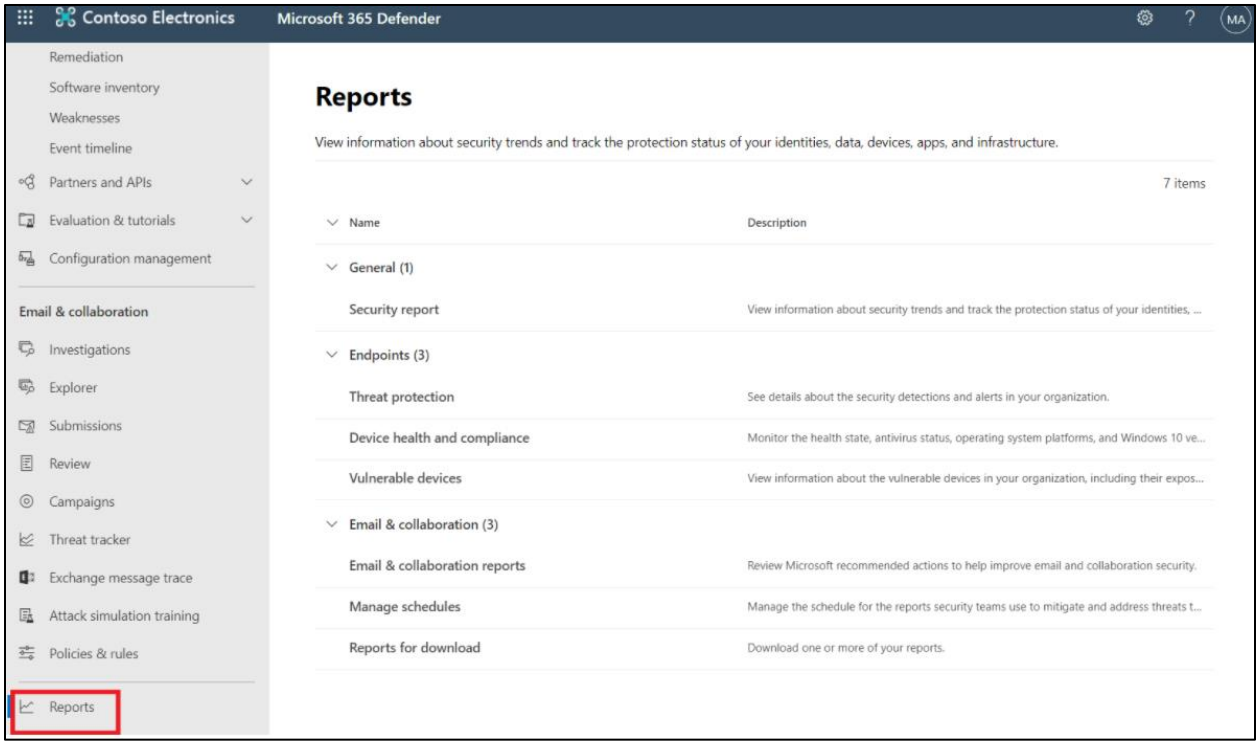
Secure Score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

In Microsoft 365 Secure Score, these steps are called improvement actions.

### 3.5.3. Security Reports and Dashboards

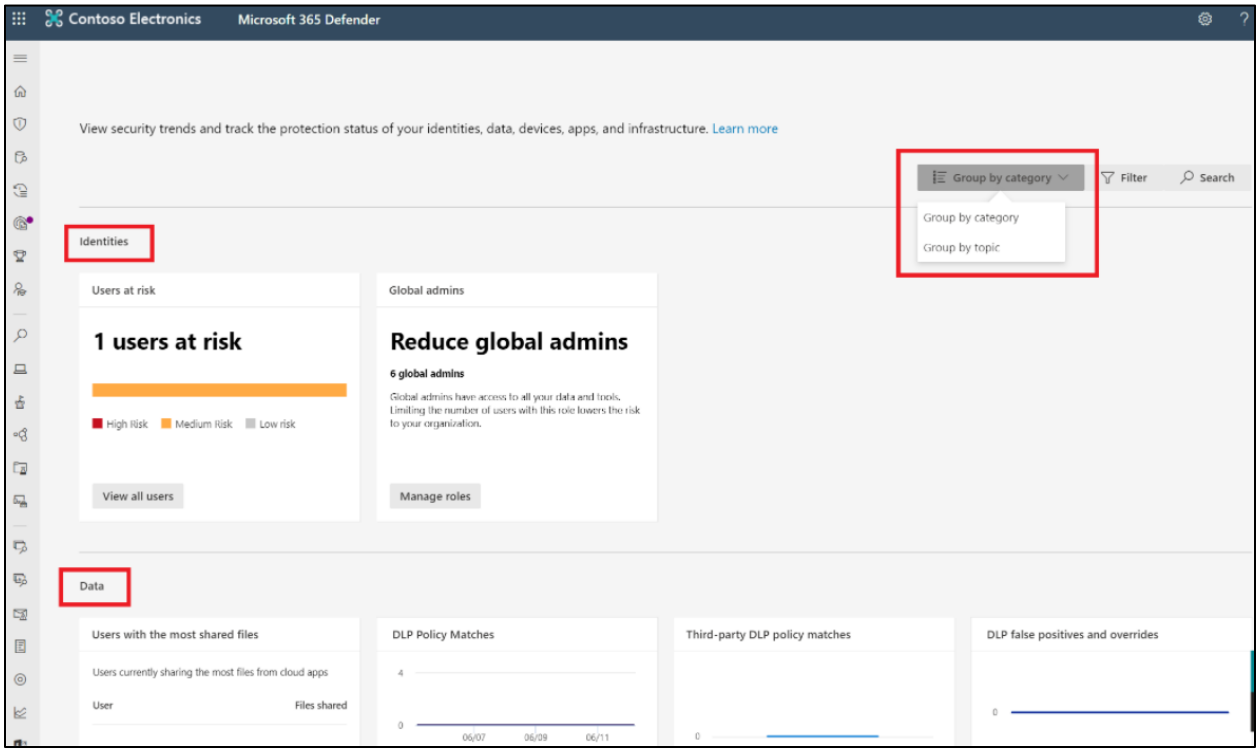
The Microsoft 365 Defender portal includes a Reports section that includes a general security report, reports related to endpoints, and reports related to email and collaboration.

Reports provide status of trends for the compliance of your Microsoft 365 devices, data, identities, apps, and infrastructure.




### 3.5.3.1. Security Report

The general security report enables admins to view information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.



By default, cards are grouped by the following categories:

#### 3.5.3.1.1. Identities

user accounts and credentials.

#### 3.5.3.1.2. Data

Email and document contents.

#### 3.5.3.1.3. Devices

Computers, mobile phones, and other devices.

#### 3.5.3.1.4. Apps

Programs and attached online services

### 3.5.3.2. Endpoint Reports

The endpoints section on the reports page includes a threat protection report, a device health and compliance report, and a vulnerable devices report.

#### 3.5.3.2.1. Threat Protection Report

The threat protection report provides high-level information about alerts generated in your organization. The report includes trending information showing the detection sources, categories, severities, statuses, classifications, and determinations of alerts across time.

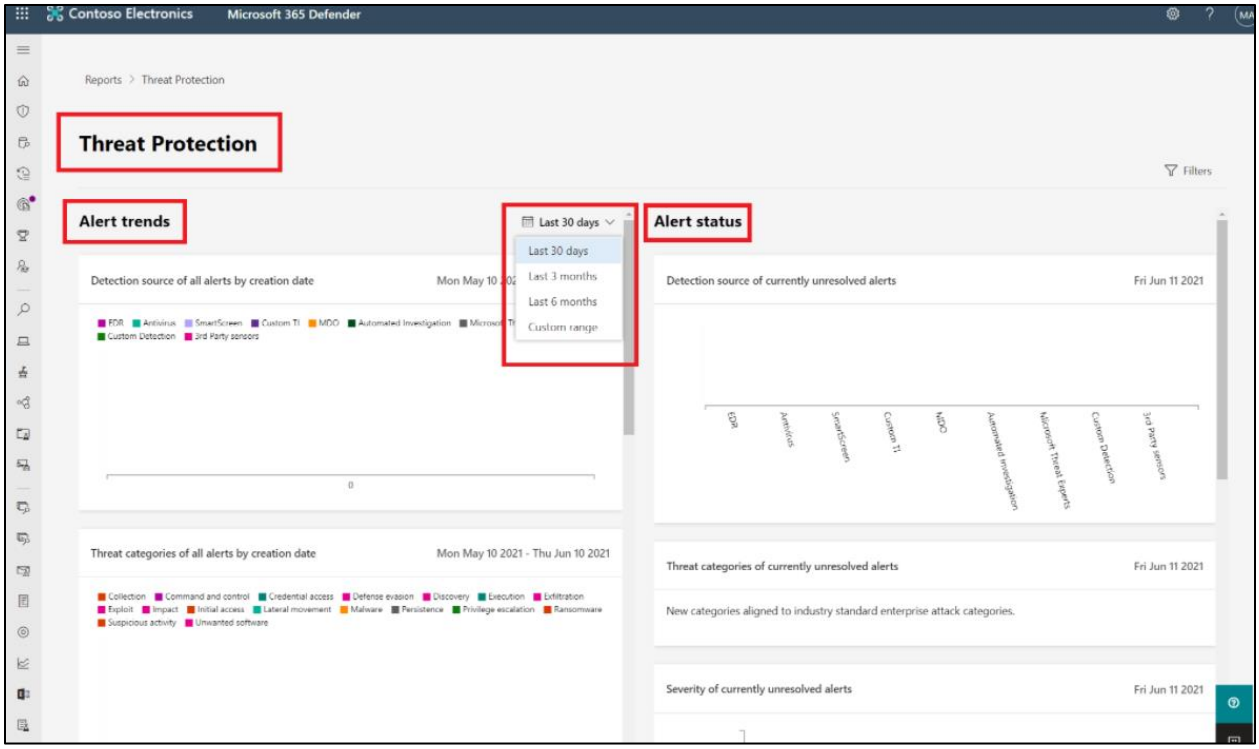
The report's dashboard is structured into two sections:

##### 3.5.3.2.1.1. Alert trends

By default, the alert trends display alert information from the 30-day period ending in the latest full day. To gain better perspective on trends occurring in your organization, you can fine-tune the reporting period by selecting a time range (30 days, 3 months, 6 months, or custom)

##### 3.5.3.2.1.2. Alert summary

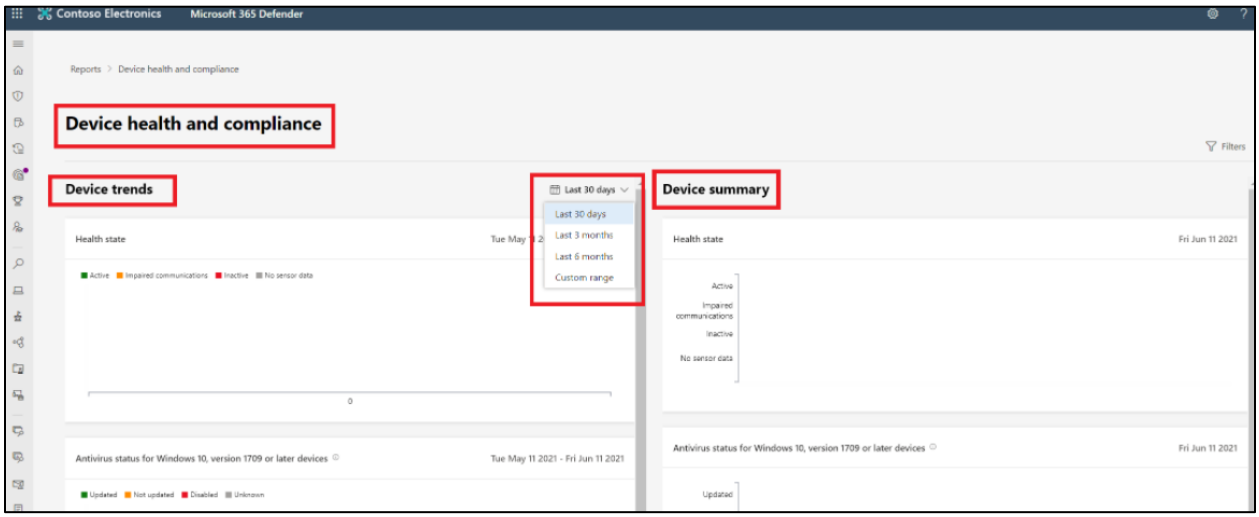
The alert summary shows alert information scoped to the current day.




### 3.5.3.2.2. Device Health and Compliance Report

The device health and compliance report enables admins to monitor the health state, antivirus status, operating system platforms, and Windows 10 versions for devices in your organization.

This report's dashboard is also structured into two sections:



#### 3.5.3.2.2.1. Device trends

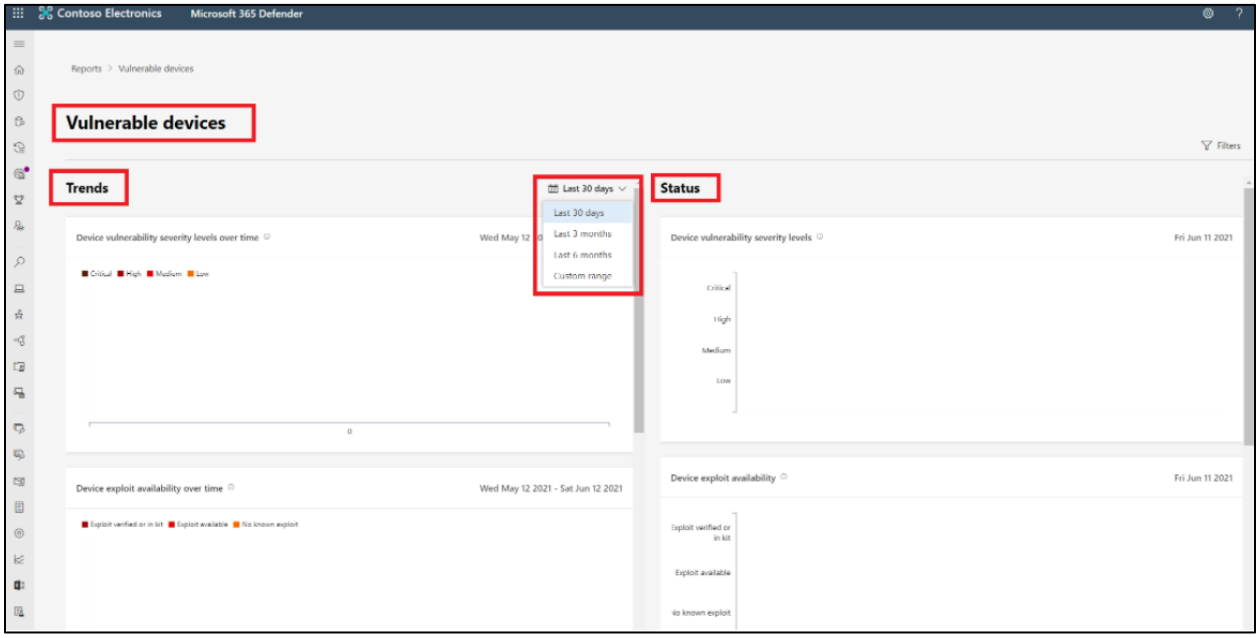
By default, the device trends displays device information from the 30-day period ending in the latest full day. To gain better perspective on trends occurring in your organization, you can fine-tune the reporting period by adjusting the time period.

#### 3.5.3.2.2.2. Device summary

The device summary shows device information scoped to the current day.

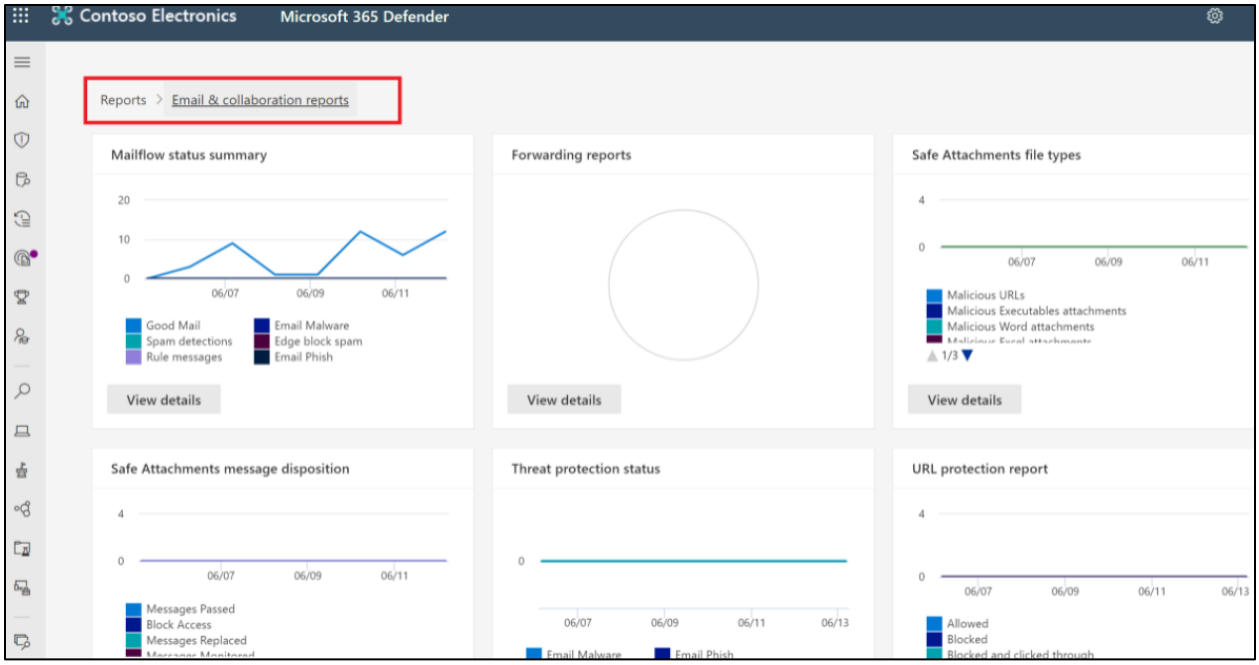
### 3.5.3.2.3. Vulnerable Devices Report

The vulnerable devices report enables admins to view information about the vulnerable devices in your organization, including their exposure to vulnerabilities by severity level, exploitability, age, and more.




### 3.5.3.3. Email and Collaboration Reports

The email and collaboration reports enable admins to review Microsoft recommended actions to help improve email and collaboration security.




## 3.5.4. Incidents Capabilities

Incidents are a collection of correlated alerts created when a suspicious event is found. Alerts are generated from a different device, user, and mailbox entities, and can come from many different domains. These alerts are automatically aggregated by Microsoft 365 Defender. It's the grouping of these related alerts that form an incident. The incident provides a comprehensive view and context of an attack.

Security personnel can use an incident to determine where an attack started, what methods were used, and to what extent the attack has progressed within the network. They can also determine the scope of the attack, and how many users, devices, and mailboxes were affected. The severity of the attack can also be determined.

### 3.5.4.1. Incident Management

Managing incidents is critical in ensuring that threats are contained and addressed. In Microsoft 365 Defender, you can manage incidents on devices, users accounts, and mailboxes.

You can manage incidents by selecting one from the Incidents queue.

Incidents are automatically assigned a name based on an alert. You can edit the name of an incident, resolve it, then set its classification and determination. You can also assign the incident to yourself and add incident tags and comments.

When you investigate cases where you want to move alerts from one incident to another, you can also do so from the Alerts tab. You'll create a larger or smaller incident that includes all relevant alerts.

Use incidents to effectively and appropriately respond to alerts across your organization's environment.

## 3.6. Endpoint Security with Microsoft Intune

Refer to File:

1. Compliance Scenario Based Demo SDB
   1.1. Unit 2.10. SBD10&SBD11- Microsoft Endpoint Management (Intune) with MIP

### 2.10. SBD10&SBD11- Microsoft Endpoint Management (Intune) with MIP

- Scenario and environment configuration
- What is Conditional access?
- Introduction to Microsoft Endpoint Manager
- What is a Device compliance?
- Preparing your tenant and enrolling devices into Microsoft endpoint manager
  - Windows
  - iOS
- Compliance Policies in Microsoft Endpoint Manager

#### 2.10.1. Scenario Description for Requirement from Organization to Manage Devices

"COVID Research Users" accessing Office365 must be using a device that is compliant with the organizational standards.

Organizational standards.

| Name | Platform | Organizational Standards |
|---|---|---|
| iOS compliance requirements | iOS | 1. Device is protected by a 6-digit passcode<br>2. Passcode must be alphanumeric |
| Windows Compliance requirements | Windows | 1. Device must be encrypted using Bitlocker. |
| Android compliance requirements | Android | 1. Android devices are not allowed to access corporate resources. |

# 4. Describe the Capabilities of Microsoft Compliance Solutions

1. DLP
2. IRM
3. Audit Logs

4. Advanced Audit
5. Communication compliance
6. Trainable Classifiers
7. Exact Data Match (EDM)
8. Sensitive Information Type (SIT)
9. Record Management
10. MIP
11. MIG
12. eDiscovery
13. Advanced eDiscovery
14. Content search
15. Compliance manager
16. Data Classification

## 4.1.Describe the Compliance Management Capabilities in Microsoft

### 4.1.1. Common Compliance Needs

Data has become more important than ever. Organizations, institutions, and entire societies generate and rely on data to function on a day-to-day basis. Any manipulation or loss of data can damage organizations, institutions, and societies alike. The sheer scale of data generated and the increasing reliance on it, means data management has become pivotal.

Governments are working hard to protect people by creating regulations (laws) that are designed to protect data through several measures including:

- Granting individuals, the right to access their data at any time.
- Granting individuals, the right to correct or delete data about them if needed.
- Introducing retention periods that dictate a minimum or maximum amount of 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.

Some regulations also require that data remains protected even if it's moved between geographic locations. For example, regulations in some countries require that any personal data transferred outside of their borders meets several conditions including:

- The destination country where personal data is to be transferred must be considered to have adequate protections for the data.
- Organizations must create appropriate safeguards, such as specific clauses that must be included in contracts with organizations or bodies that handle any personal data.

#### 4.1.1.1. Common Compliance Regulations

Some of the regulations that organizations and institutions commonly work with include:

- Health Insurance Portability and Accountability Act (HIPAA) – introduces rules on how health-related information should be protected.
- The Family Educational Rights and Privacy Act (FERPA) – introduces rules to protect student information.
- ISO 27701 – specifies rules and guidance to manage personal information, and demonstrate compliance.

Microsoft supports organizations' compliance needs with built-in tools and capabilities to help them protect information, manage data governance, and respond to regulatory requests.

## 4.1.2. The Offerings of the Service Trust Portal

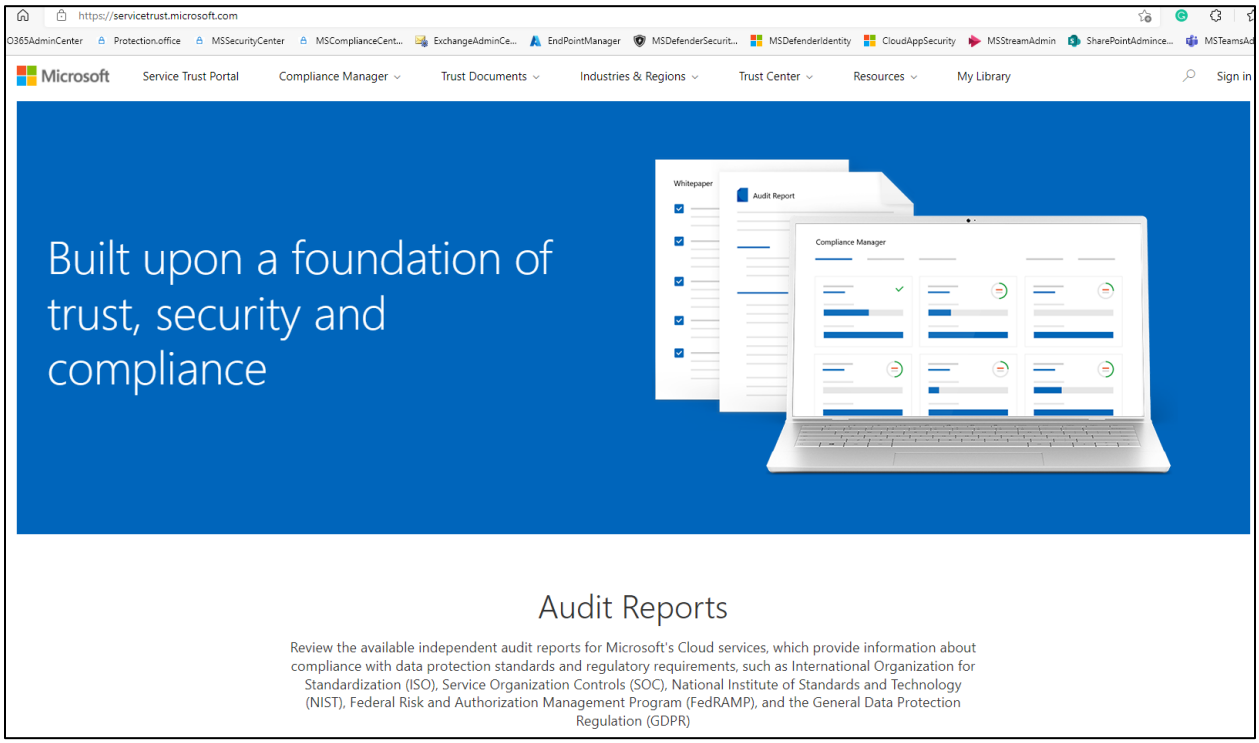
The Service Trust Portal provides information, tools, and other resources about Microsoft security, privacy, and compliance practices. Sign in with your Microsoft cloud services account to access all the available documentation.

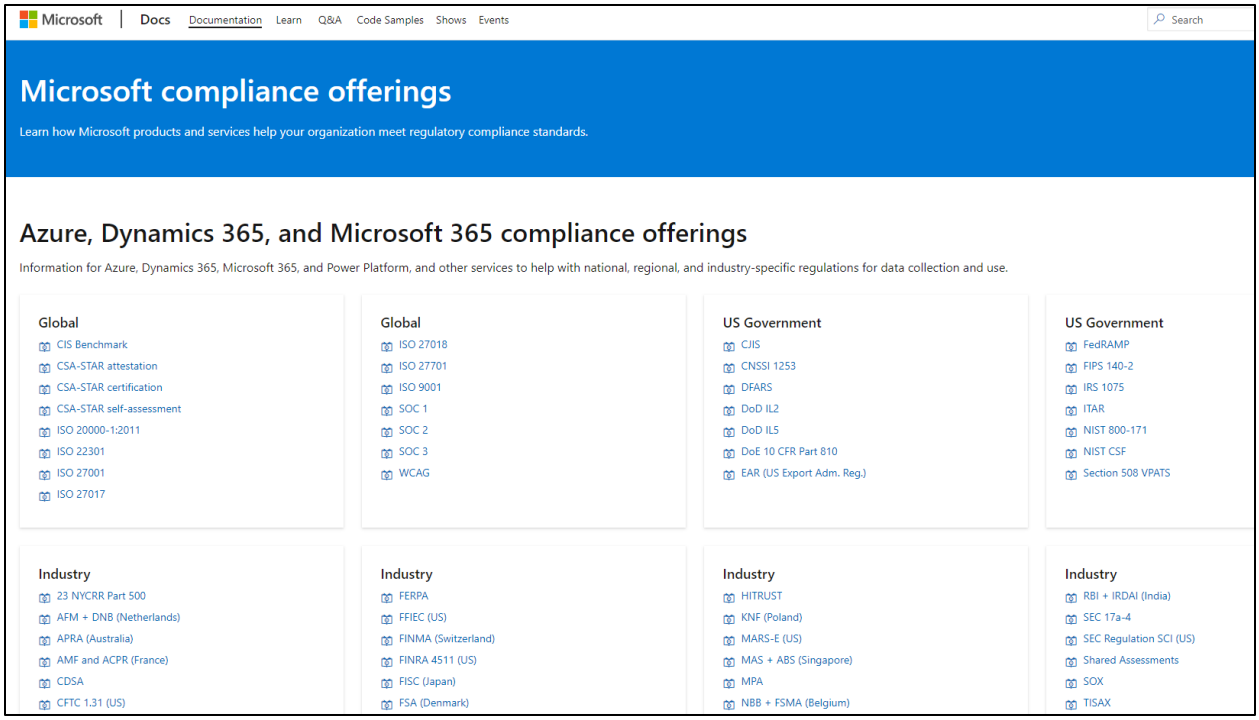
From the main menu, you access:

### 4.1.2.1. Service Trust Portal

Service Trust Portal (microsoft.com)

Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Docs



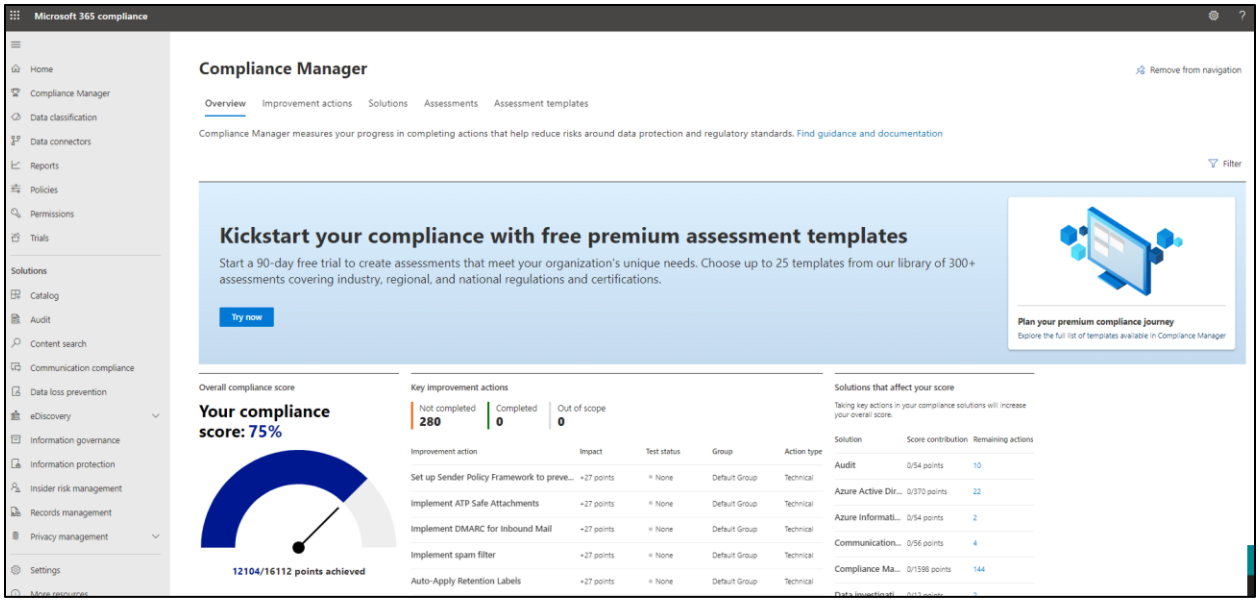



Review the available independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements, such as:

#### 4.1.2.1.1. ISO: International Organization for Standardization (ISO)
#### 4.1.2.1.2. SOC: Service Organization Controls (SOC)
#### 4.1.2.1.3. NIST: National Institute of Standards and Technology (NIST)
#### 4.1.2.1.4. FedRAMP: Federal Risk and Authorization Management Program (FedRAMP)
#### 4.1.2.1.5. GDPR: General Data Protection Regulation (GDPR)

### 4.1.2.2. Compliance Manager

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. To find out more, see the Microsoft Compliance Manager documentation in the Learn More section below.




### 4.1.2.3. Trust Documents

Trust Documents links to a security implementation and design information.

### 4.1.2.4. Industries & Regions

Industries & Regions contains compliance information about Microsoft Cloud services organized by industry and region. The Industry Solutions link currently displays the home page for Financial Services. The Regional Solutions links currently have information for: Australia, Canada, Czech Republic, Denmark, Germany, Poland, Romania, Spain, and the United Kingdom.

### 4.1.2.5. Trust Center

Trust Center links to the Microsoft Trust Center, which provides more information about security, compliance, and privacy in the Microsoft Cloud.

### 4.1.2.6. Resources

Resources links to resources including information about the features and tools available for data governance and protection in Office 365, the Microsoft Global Datacenters, and Frequently Asked Questions.

### 4.1.2.7. My Library

My Library allows you to add documents and resources that are relevant to your organization. Everything is in one place. You can also opt to have email notifications sent when a document is updated and set the frequency you receive notifications.

### 4.1.3. Microsoft's privacy principles

Microsoft’s products and services run on trust. Microsoft focuses on six key privacy principles when making decisions about data. Privacy is about making meaningful choices for how and why data is collected and used. It's about ensuring that you have the information you need to make the choices that are right for you, across all Microsoft products and services.

These principles form Microsoft’s privacy foundation, and they shape the way that products and services are designed. Find out more at the Microsoft Trust Center in the Learn More section below.

The six privacy principles are:

#### 4.1.3.1. Control

Control Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.

#### 4.1.3.2. Transparency

Transparency being transparent about data collection and use so that everyone can make informed decisions.

#### 4.1.3.3. Security

Security protecting the data that's entrusted to Microsoft by using strong security and encryption.

#### 4.1.3.4. Strong legal protections

Strong Legal Protections respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

#### 4.1.3.5. No content-based targeting

No content-Based targeting not using email, chat, files, or other personal content to target advertising.

#### 4.1.3.6. Benefits to you

Benefits to you when Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

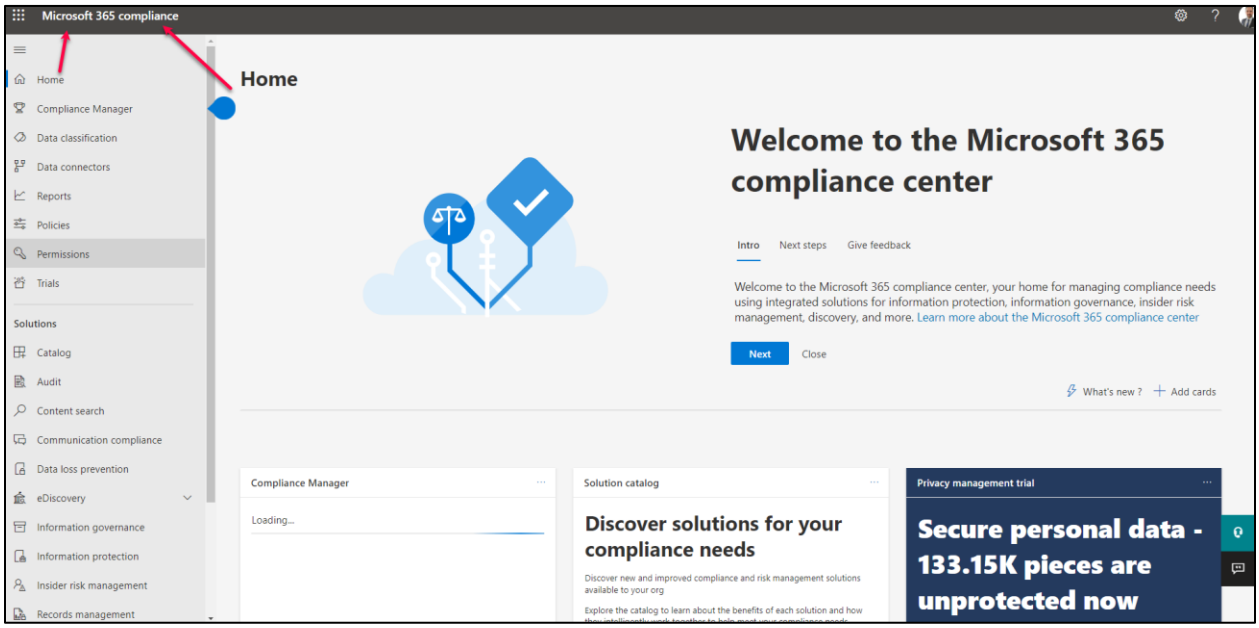
### 4.1.4. The Compliance Center

The Microsoft 365 compliance center brings together all of the tools and data that are needed to help understand and manage an organization’s compliance needs.

Compliance center is available to customers with a Microsoft 365 SKU with one of the following roles:

- Global administrator
- Compliance administrator
- Compliance data administrator

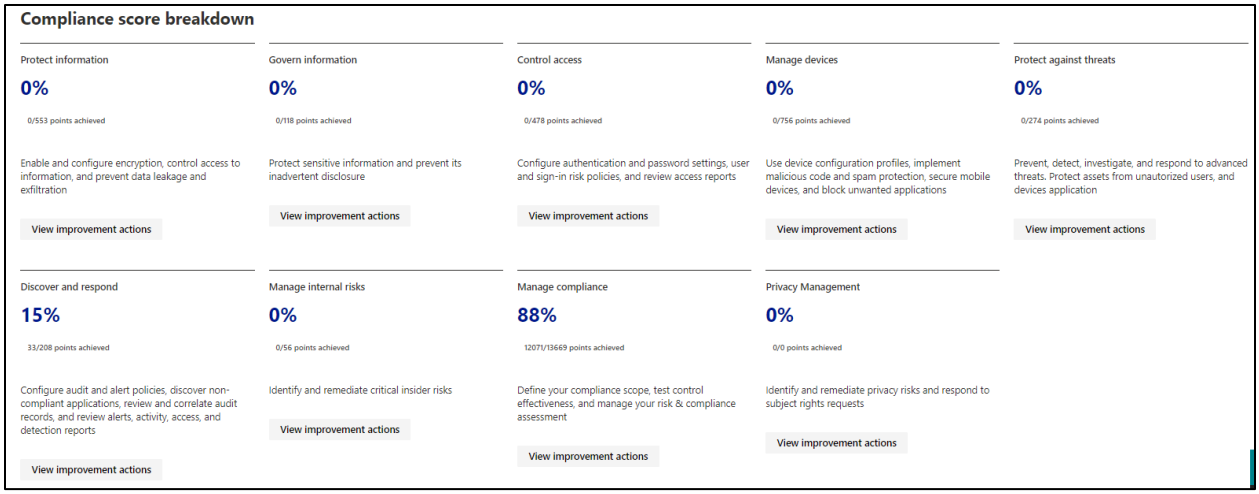
When an admin signs into the Microsoft 365 compliance center portal, they'll get a bird's-eye view of how the organization is meeting its compliance requirements, along with which solutions can be used to help with compliance, information about any active alerts, and more.




The default compliance center home page contains several cards including:

### 4.1.4.1. The Compliance Score Card.

This card shows the compliance score and will forward admins to the Compliance Manager where they can see a breakdown of the compliance score. Compliance score measures the progress in completing recommended improvement actions within controls. The score helps an organization to understand its current compliance posture. It also helps an organization to prioritize actions based on their potential to reduce risk.



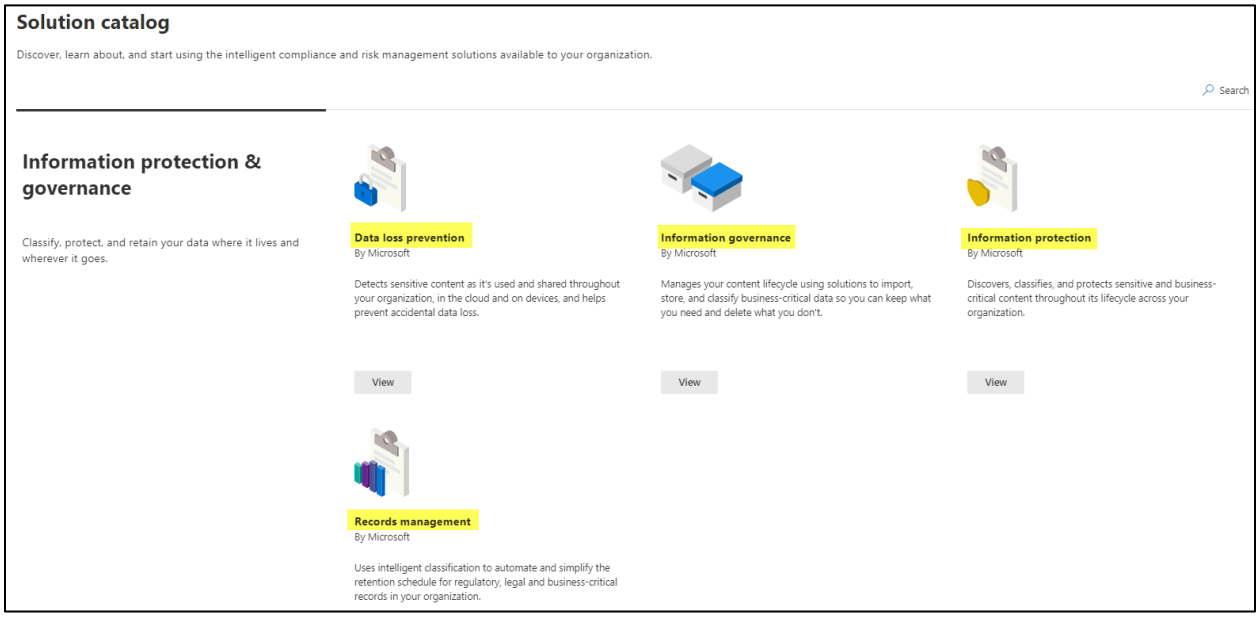

## 4.1.4.2. Data Connectors

Connect to your data sources: Connectors help you connect your important data sources to your compliance solutions.

Microsoft 365 lets administrators use data connectors to import and archive third-party data from social media platforms, instant messaging platforms, and document collaboration platforms, to mailboxes in your Microsoft 365 organization.

The Microsoft 365 compliance center provides native third-party data connectors from Microsoft to import data from various data sources, such as LinkedIn, Instant Bloomberg, and Twitter and data connectors that support the Insider risk management solution. In addition to these data connectors, Microsoft works with the following partners to provide many more third part data connectors in the Microsoft 365 compliance center. Your organization works with these partners to set up their archiving service before creating a corresponding data connector in the Microsoft 365 compliance center.

### 4.1.4.3. Solution Catalog




The new Solution catalog card, links to collections of integrated solutions that are used to manage end-to-end compliance scenarios across three compliance solutions areas:

#### 4.1.4.3.1. The information Protection & Governance

The Information protection & governance section quickly shows you how to use Microsoft 365 compliance solutions to protect and govern data in your organization.

#### 4.1.4.3.2. The Insider Risk Management

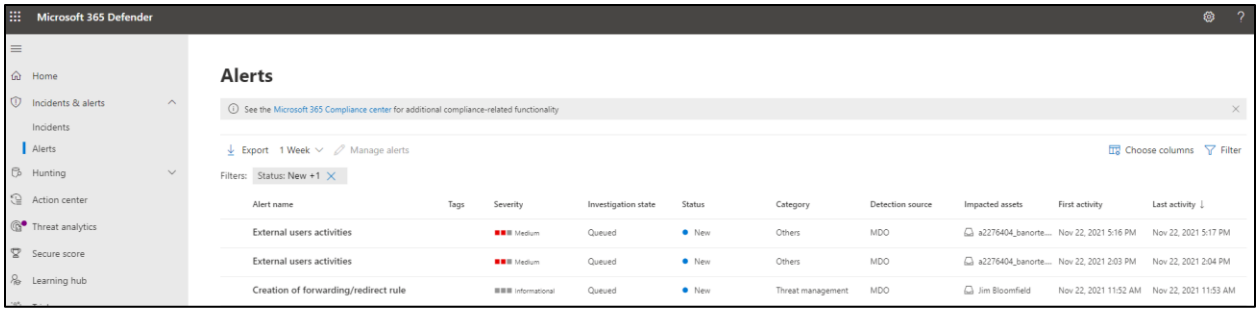
The Insider risk management section on the home page shows how your organization can identify, analyze, and act on internal risks before they cause harm.

#### 4.1.4.3.3. The Discovery & Respond

The Discovery & respond section on the home page shows how your organization can quickly find, investigate, and respond to compliance issues with relevant data.

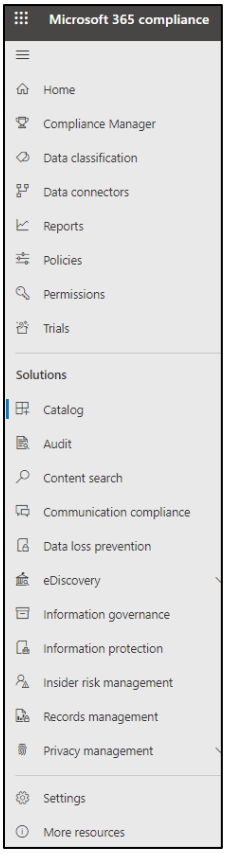
### 4.1.4.4. Active Alerts

The Active alerts card includes a summary of the most active alerts and a link where admins can view more detailed information, such as alert severity, status, category, and more.




### 4.1.4.5. Navigation

In addition to the cards on the home page, there's a navigation pane on the left of the screen that gives easy access to alerts, reports, policies, compliance solutions, and more. To add or remove options for a customized navigation pane, the Customize navigation control on the navigation pane can be used to configure which items appear there.




## 4.1.5. Compliance Manager

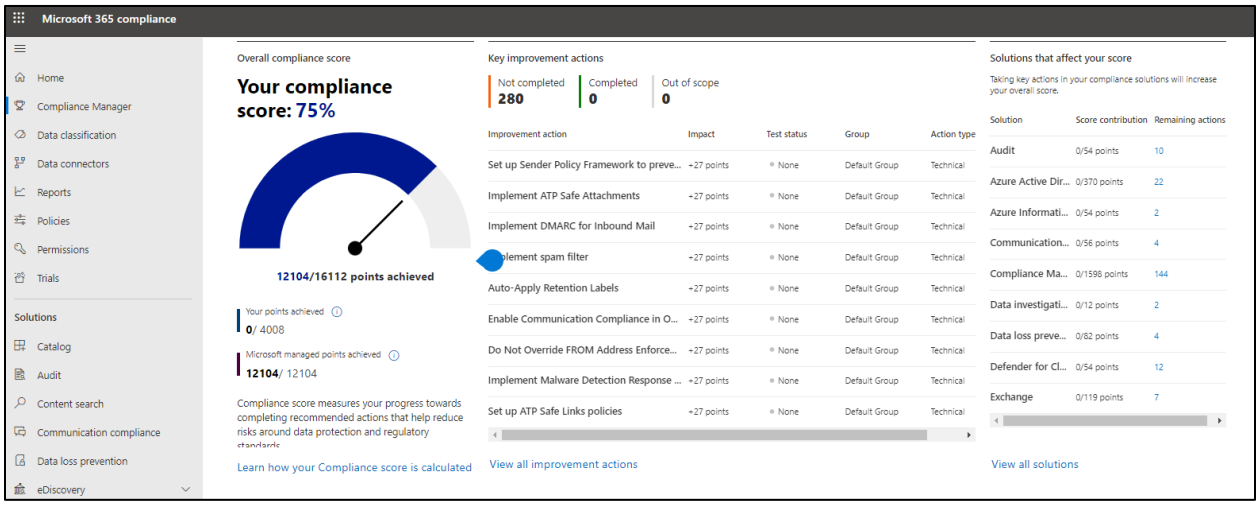
Microsoft Compliance Manager is a feature in the Microsoft 365 compliance center that helps admins to manage an organization's compliance requirements with greater ease and convenience. Compliance Manager can help organizations throughout their compliance journey, from taking

inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Compliance Manager helps simplify compliance and reduce risk by providing:

- **Prebuilt assessments** based on common regional and industry regulations and standards. Admins can also use custom assessment to help with compliance needs unique to the organization.
- **Workflow** capabilities that enable admins to efficiently complete risk assessments for the organization.
- **Step-by-step improvement actions** that admins can take to help meet regulations and standards relevant to the organization. Some actions will also be managed for the organization by Microsoft. Admins will get implementation details and audit results for those actions.
- **Compliance score**, which is a calculation that helps an organization understand its overall compliance posture by measuring how it's progressing with improvement actions.

The Compliance Manager dashboard shows the current compliance score, helps admins to see what needs attention, and guides them to key improvement actions.




Compliance Manager uses several data elements to help manage compliance activities. As admins use Compliance Manager to assign, test, and monitor compliance activities, it's helpful to have a basic understanding of the key elements: controls, assessments, templates, and improvement actions.

### 4.1.5.1. Controls

A control is a requirement of a regulation, standard, or policy. It defines how to assess and manage system configuration, organizational process, and people responsible for meeting a specific requirement of a regulation, standard, or policy.

Compliance Manager continuously assesses controls by scanning through your Microsoft 365 environment and detecting your system settings, continuously and automatically updating your technical action status.

Compliance Manager tracks the following types of controls:

#### 4.1.5.1.1. Microsoft-managed controls:

Controls for Microsoft cloud services, which Microsoft is responsible for implementing.

#### 4.1.5.1.2. Your controls

sometimes referred to as customer-managed controls, these are implemented and managed by the organization.

#### 4.1.5.1.3. Shared controls

Responsibility for implementing these controls is shared by the organization and Microsoft.

### 4.1.5.2. Assessment

An assessment is a grouping of controls from a specific regulation, standard, or policy. Completing the actions within an assessment helps to meet the requirements of a standard, regulation, or law. For example, an organization may have an assessment that, when the admin completes all actions within it, it helps to bring the organization's Microsoft 365 settings in line with ISO 27001 requirements.

Assessments have several components:

- **In-scope services**: the specific set of Microsoft services applicable to the assessment.
- **Microsoft-managed controls**: controls for Microsoft cloud services, which Microsoft implements for the organization.
- **Your controls**: these controls, sometimes referred to as customer-managed controls, are implemented and managed by the organization.
- **Shared controls**: responsibility for implementing these controls is shared by the organization and Microsoft.
- **Assessment score**: shows the progress in achieving total possible points from actions within the assessment that are managed by the organization and by Microsoft.

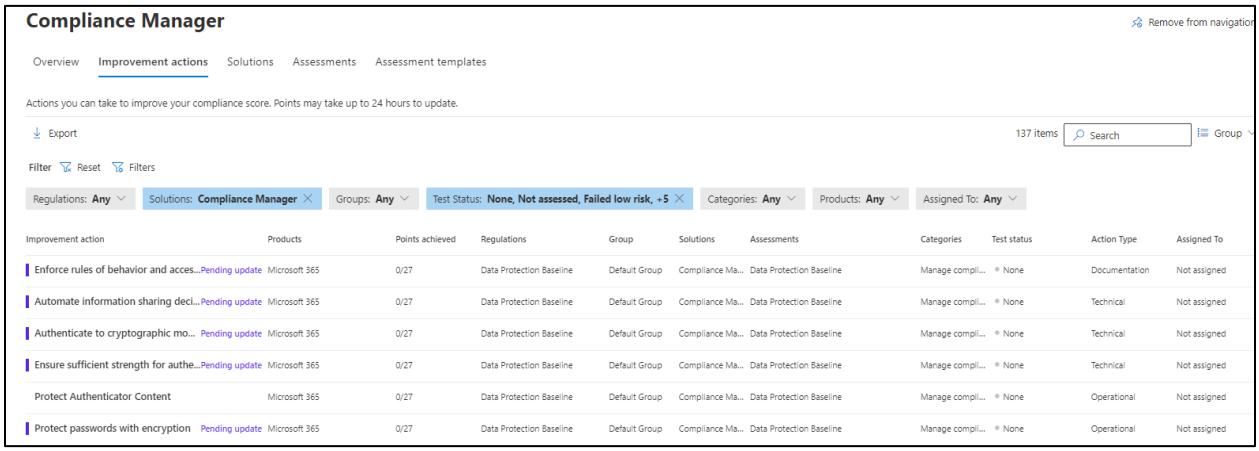
When creating assessments, an admin will assign them to a group. The admin can configure groups in whatever way is most logical for the organization. For example, they might group assessments by audit year, region, solution, teams within the organization, or some other way. Once the admin has created groups, the admin can filter the Compliance Manager dashboard to view the score by one or more groups.

### 4.1.5.3. Templates

Compliance Manager provides templates to help admins to quickly create assessments. They can modify these templates to create an assessment optimized for their needs. Admins can also build a custom assessment by creating a template with their own controls and actions. For example, the admin may want a template to cover an internal business process control, or a regional data protection standard that isn't covered by one of Microsoft's 150-plus prebuilt assessment templates.

### 4.1.5.4. Improvement Actions

Improvement actions help centralize compliance activities. Each improvement action provides recommended guidance that's intended to help organizations to align with data protection regulations and standards. Improvement actions can be assigned to users in the organization to do implementation and testing work. Admins can also store documentation, notes, and record status updates within the improvement action.




### 4.1.5.5. Benefits of compliance Manager

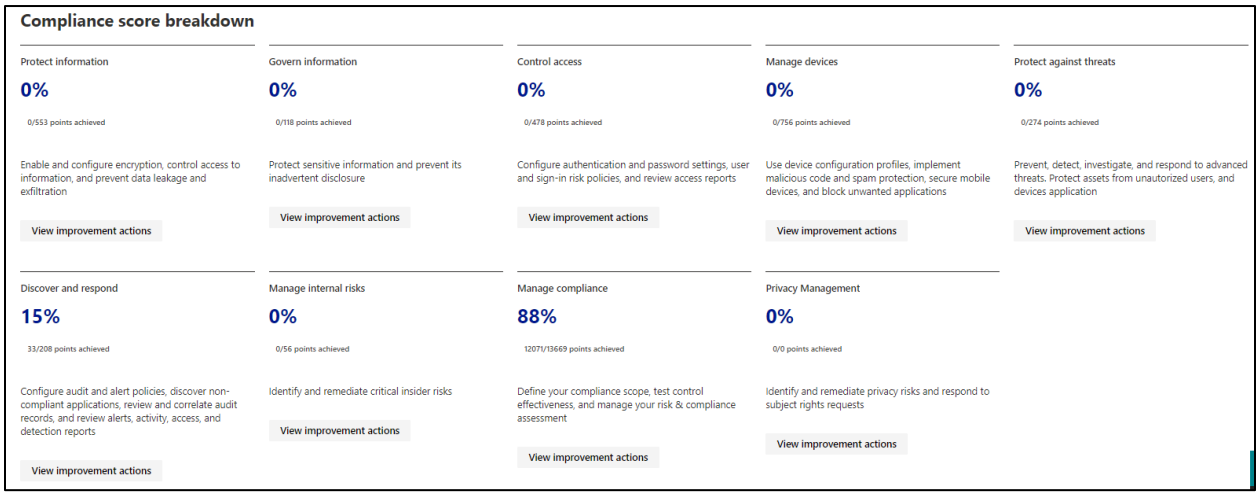
Compliance Manager provides many benefits, including:

- Translating complicated regulations, standards, company policies, or other control frameworks into a simple language.
- Providing access to a large variety of out-of-the-box assessments and custom assessments to help organizations with their unique compliance needs.
- Mapping regulatory controls against recommended improvement actions.
- Providing step-by-step guidance on how to implement the solutions to meet regulatory requirements.
- Helping admins and users to prioritize actions that will have the highest impact on their organizational compliance by associating a score with each action.

## 4.1.6. Use and Benefits of Compliance Score

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

Admins can get a breakdown of the compliance score in the Compliance Manager overview pane:




### 4.1.6.1. Difference between Compliance Manager and compliance score

Compliance Manager is an end-to-end solution in Microsoft 365 compliance center to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization. The compliance score is available through Compliance Manager.

Compliance Manager gives admins the capabilities to understand and increase their compliance score, so they can ultimately improve the organization's compliance posture and help it to stay in line with compliance requirements.

### 4.1.6.2. Understanding the Compliance Score

The overall compliance score is calculated using scores that are assigned to actions. Actions come in two types:

#### 4.1.6.2.1. Type of Actions

##### 4.1.6.2.1.1. Your Improved Actions

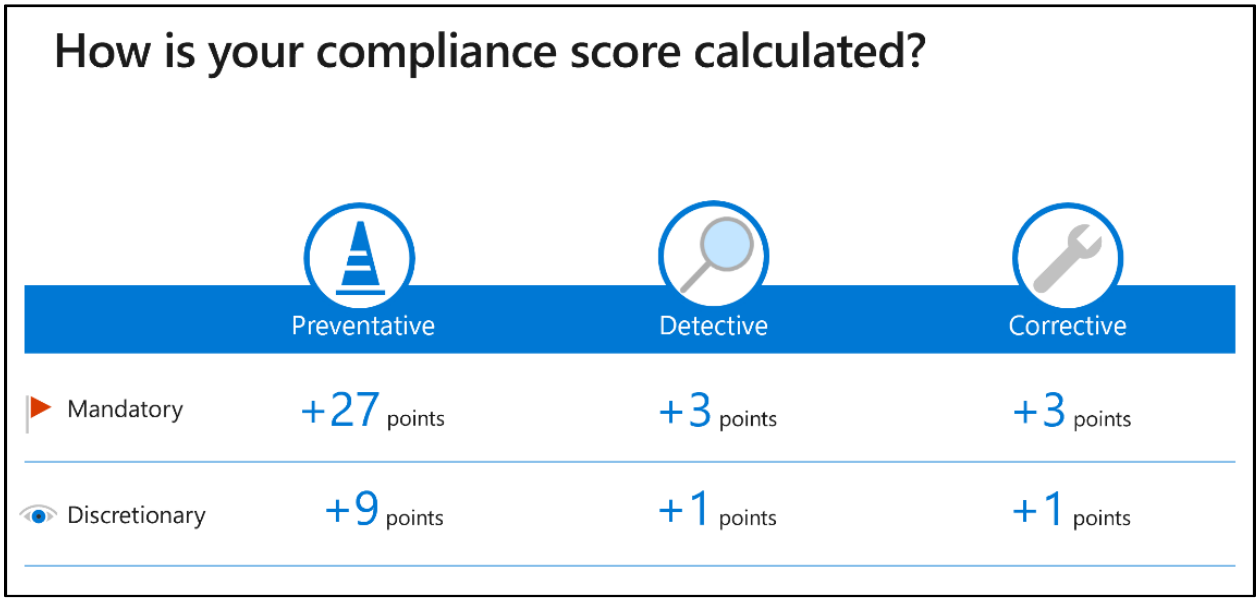
actions that the organization is expected to manage.

#### 4.1.6.2.1.2. Microsoft Actions

actions that Microsoft manages for the organization.

### 4.1.6.2.2. Category of Actions

These action types have points assigned to them that count towards the compliance score. Actions can also be considered technical or nontechnical, which also affects how they impact the overall compliance score.




Actions are also assigned a score value based on whether they're categorized as mandatory, discretionary, preventative, detective, or corrective:

#### 4.1.6.2.2.1. Action Mandatory

Mandatory – these actions shouldn't be bypassed. For example, creating a policy to set requirements for password length or expiration.

#### 4.1.6.2.2.2. Action Discretionary

Discretionary – these actions depend on the users understanding and adhering to a policy. For example, a policy where users are required to ensure their devices are locked before they leave them.

### 4.1.6.2.3. Subcategories of Actions

The following are subcategories of actions that can be classified as mandatory or discretionary:

#### 4.1.6.2.3.1. Preventative Actions

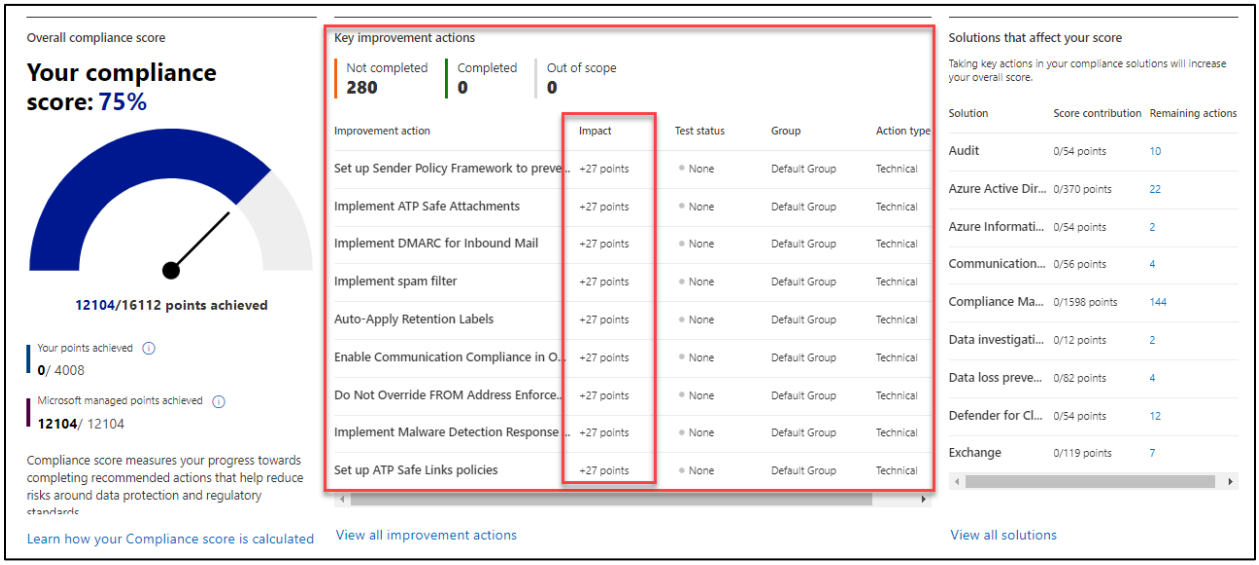
Preventative actions are designed to handle specific risks, like using encryption to protect data at rest if there were breaches or attacks.

#### 4.1.6.2.3.2. Detective Actions

Detective actions actively monitor systems to identify irregularities that could represent risks, or that can be used to detect breaches or intrusions. Examples of these types of actions are system access audits, or regulatory compliance audits.

#### 4.1.6.2.3.3. Corrective Actions

Corrective actions help admins to minimize the adverse effects of security incidents, by undertaking corrective measures to reduce their immediate effect or possibly even reverse damage.




## 4.2. Describe Information Protection and Governance Capabilities of Microsoft 365

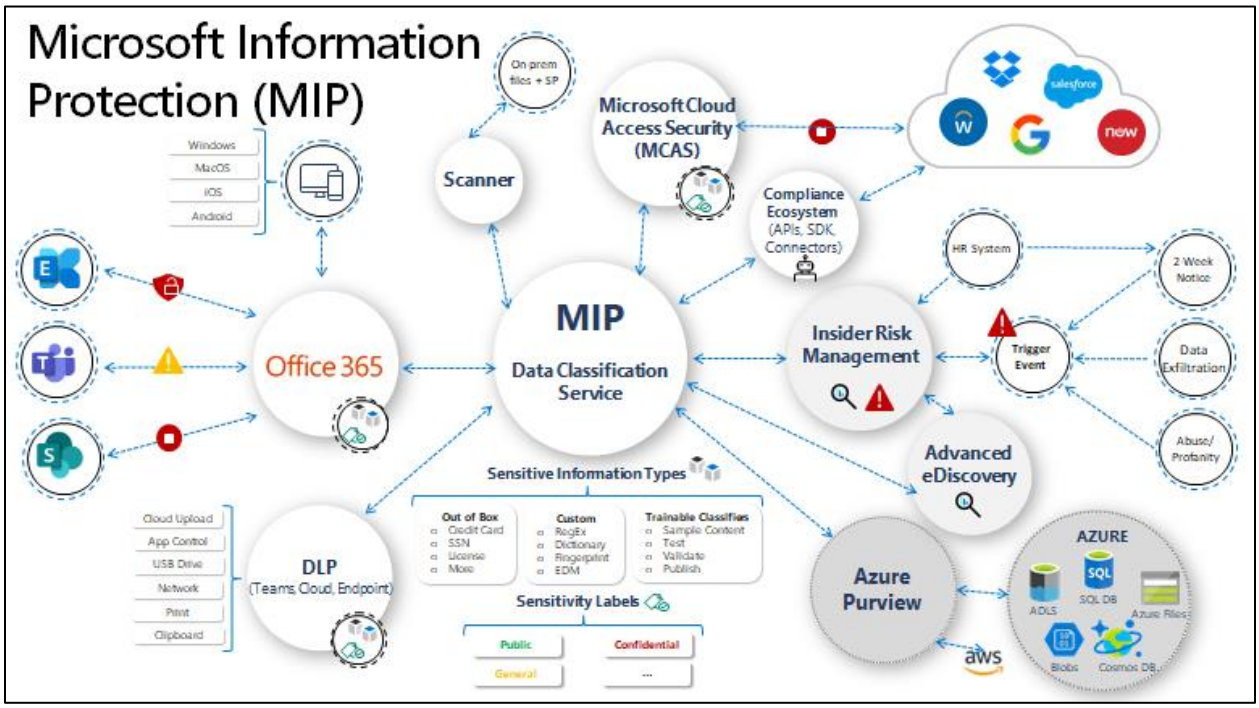
Organizations need to protect all sorts of information, including financial and personal information. This must be done to ensure customers, employees, and the organization are protected from risks. The organization needs to stay in line with compliance standards wherever it operates.

Microsoft provides solutions that can help organizations to implement information protection and governance.

In this module, you'll learn about how Microsoft solutions and capabilities like data classification, records management, and data loss prevention, can help you implement information protection and governance.

After completing this module, you should be able to:

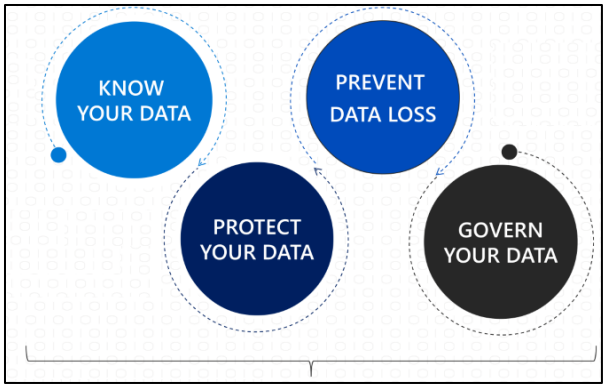
- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.




## 4.2.1. Know your data, protect your data, and govern your data

Microsoft Information Protection (MIP) discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.

Microsoft Information Governance (MIG) manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. It gives organizations the capabilities to govern their data, for compliance or regulatory requirements. Microsoft Information Protection and Microsoft Information Governance work together to classify, protect, and keep your data where it lives, and wherever it goes.




#### 4.2.1.1. Know Your Data

Organizations can understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Capabilities and tools such as trainable classifiers, activity explorer, and content explorer allow organizations to know their data.

#### 4.2.1.2. Protect Your Data

Organizations can apply flexible protection actions including encryption, access restrictions, and visual markings.

#### 4.2.1.3. Prevent Data Loss

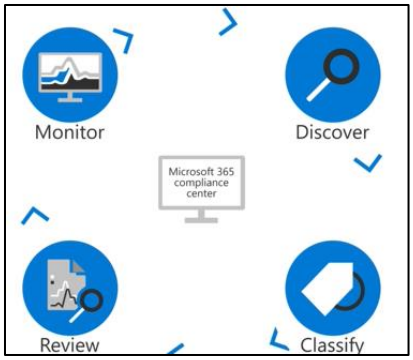
Organizations can detect risky behavior and prevent accidental oversharing of sensitive information. Capabilities such as data loss prevention policies and endpoint data loss prevention enable organizations to avoid data loss.

#### 4.2.1.4. Govern Your Data

Organizations can automatically keep, delete, and store data and records in a compliant manner. Capabilities like retention policies, retention labels, and records management enable organizations to govern their data.

### 4.2.2. Describe data classification capabilities in the Microsoft 365 Compliance Center

Organizations need to know their data to identify important information across the estate and ensure that data is handled in line with compliance requirements. Admins can enable their organization to know its data through data classification capabilities and tools in the Microsoft 365 compliance center, such as sensitive information types, trainable classifiers, content explorer, and activity explorer.




#### 4.2.2.1. Sensitive Information Types

With Microsoft 365 compliance center, admins can identify and protect sensitive information types. Sensitive information types have set patterns that can be used to identify them. For example, an identification number in a region/country may be based on a specific pattern, like this:

123-456-789-ABC

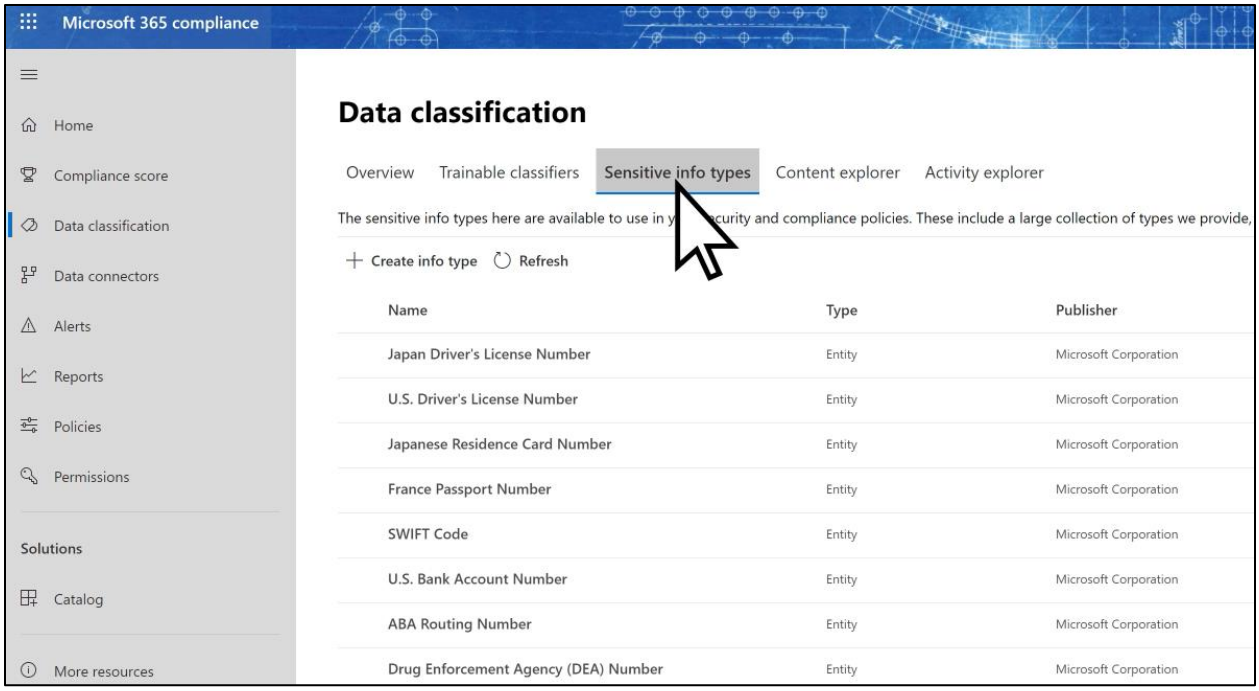
Microsoft 365 includes many built-in sensitive information types based on patterns that are defined by a regular expression (regex) or a function.

Examples include:

- Credit card numbers
- Passport or identification numbers
- Bank account numbers
- Health service numbers

Refer to Sensitive information type entity definitions for a listing of available built-in sensitive information types.

Data classification in Microsoft 365 also supports the ability to create custom sensitive information types to address organization-specific requirements. For example, an organization may need to create sensitive information types to represent employee IDs or project numbers.



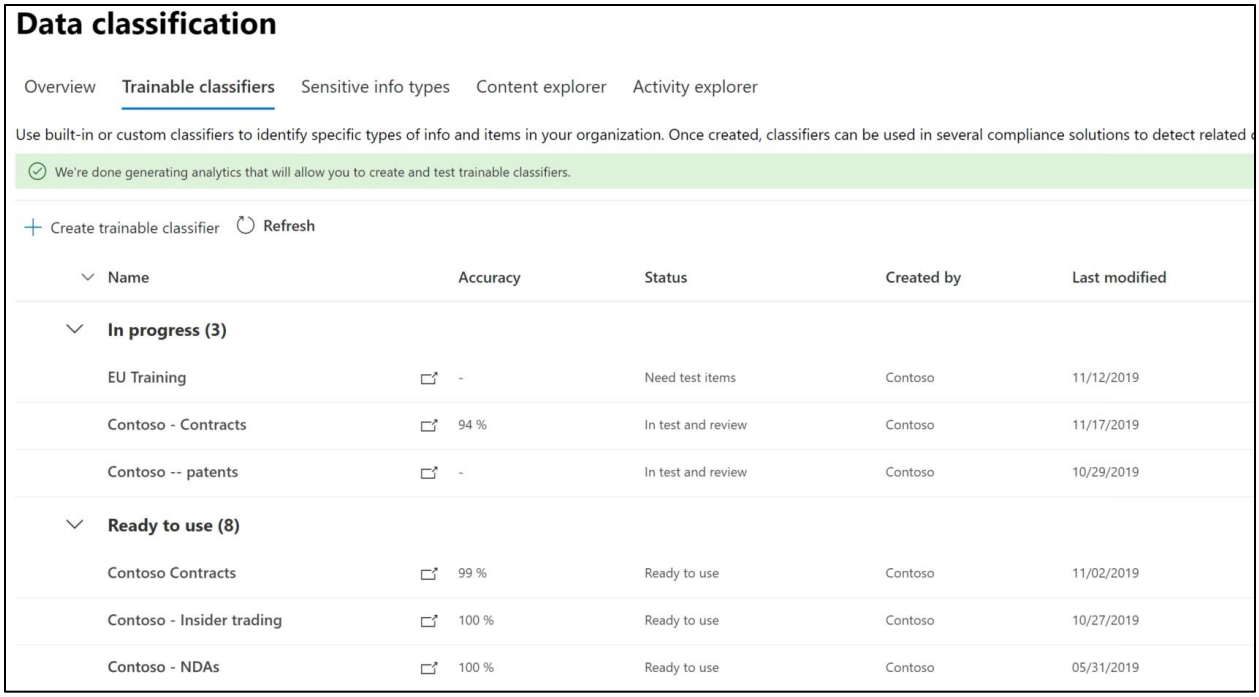

### 4.2.2.2. Trainable Classifiers

Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They're most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records.

The model gets tested to determine if the classifier can correctly distinguish between items that match the category and items that don't. The result of each prediction is manually verified, which serves as input to improve the accuracy of the prediction model.

After the accuracy score of the model has stabilized, the classifier can be published. Trainable classifiers can then sort through items in locations like SharePoint Online, Exchange, and OneDrive, and classify the content.

NOTE: At this time, classifiers only work with items that are in English and aren't encrypted.




This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). Two types of classifier are available:

#### 4.2.2.2.1. Pre-trained classifiers

Microsoft has created and pretrained many classifiers that you can start using without training them. These classifiers will appear with the status of Ready to use. Microsoft 365 comes with five pretrained classifiers that detect and classify things like resumes, source code, harassment, profanity, and threat (relates to committing violence or doing physical harm).

#### 4.2.2.2.2. Custom trainable classifiers

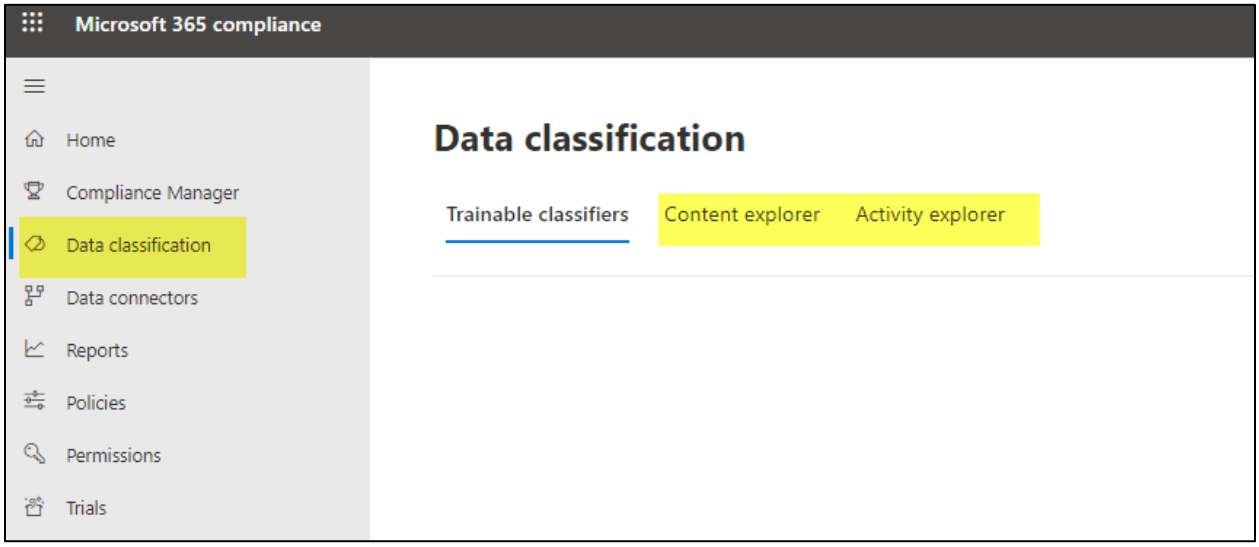
Microsoft supports the ability to create and train custom classifiers. They're most useful when classifying data unique to an organization, like specific kinds of contracts, invoices, or customer records.

### 4.2.2.3. Understand And Explore The Data

Data classification can involve large numbers of documents and emails. To help administrators to easily derive insights and understanding, the overview section of the data classification pane in compliance center provides many details at a glance, including:

- The number of items classified as sensitive information and which classifications they are.
- Details on the locations of data based on sensitivity.
- Summary of actions that users are taking on sensitive content across the organization.

Administrators can also use the content and activity explorers to gain a deeper understanding and guide their actions.



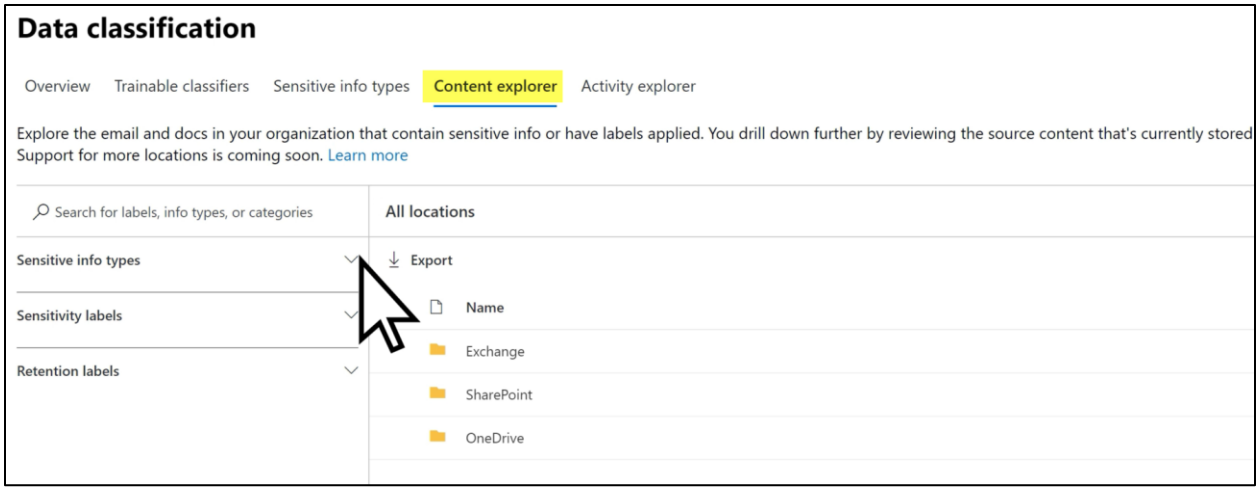

#### 4.2.2.3.1. Content Explorer

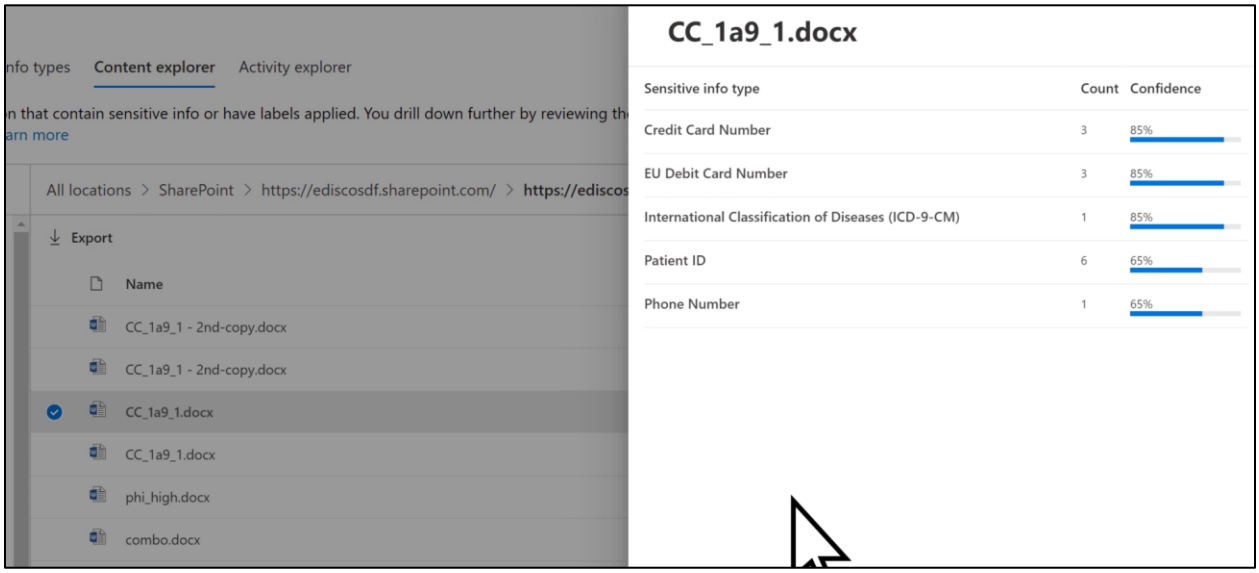
The content explorer is available as a tab in the data classification pane of compliance center. It enables administrators to gain visibility into the content that has been summarized in the overview pane. Access to content explorer is highly restricted because it makes it possible to read the contents of scanned files. There are two roles that grant access to content explorer:

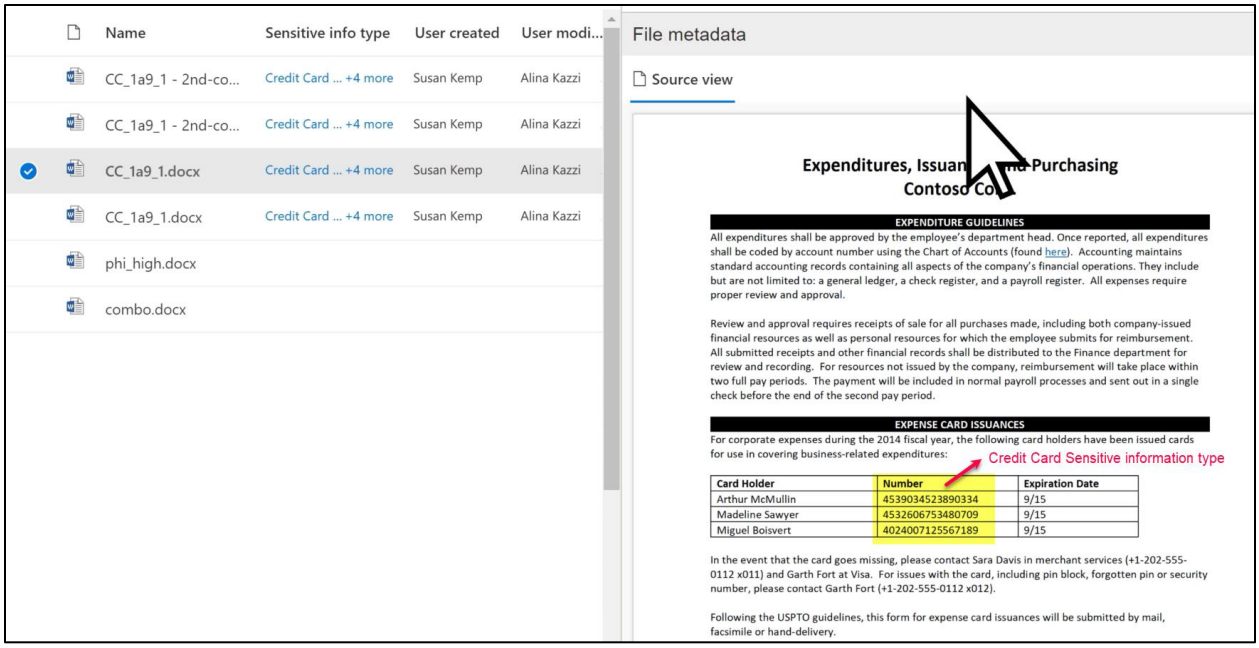
- Content explorer list viewer.
- Content explorer content viewer.

Anyone who wants to access content explorer must have an account in one or both of the role groups.

With content explorer, administrators get a current snapshot of individual items that have been classified across the organization. It enables administrators to further drill down into items by allowing them to access and review the scanned source content that's stored in different kinds of locations, such as Exchange, SharePoint, and OneDrive.


Data classification
Overview
Trainable classifiers
Sensitive info types
Content explorer
Activity explorer
Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored
Support for more locations is coming soon. Learn more
Search for labels, info types, or categories
All locations
Sensitive info types
Sensitivity labels
Retention labels
Export
Name
Exchange
SharePoint
OneDrive


nfo types
Content explorer
Activity explorer
n that contain sensitive info or have labels applied. You drill down further by reviewing th
arn more
All locations > SharePoint > https://ediscosdf.sharepoint.com/ > https://ediscos
Export
Name
CC_1a9_1 - 2nd-copy.docx
CC_1a9_1 - 2nd-copy.docx
CC_1a9_1.docx
CC_1a9_1.docx
phi_high.docx
combo.docx
CC_1a9_1.docx
Sensitive info type
Count
Confidence
Credit Card Number
3
85%
EU Debit Card Number
3
85%
International Classification of Diseases (ICD-9-CM)
1
85%
Patient ID
6
65%
Phone Number
1
65%




### 4.2.2.3.2. Activity Explorer

Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. It makes it possible to monitor what's being done with labeled content across the organization. Admins gain visibility into document-level activities like label changes and label downgrades (such as when someone changes a label from confidential to public).

Admins use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer helps you understand what's being done with labeled content over time. Admins use activity explorer to evaluate if controls already in place are effective.

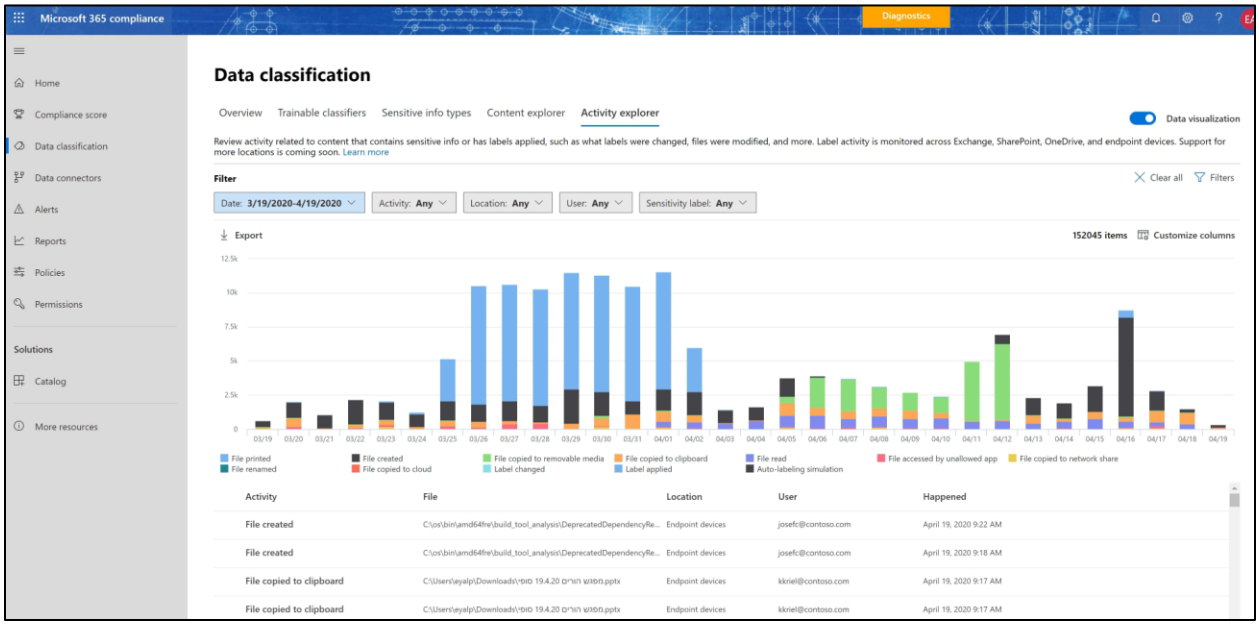
Here are a few of the activity types that can be analyzed:

- File copied to removable media
- File copied to network share
- Label applied
- Label changed

Admins can use more than 30 filters for data including:

- Date range
- Activity type
- Location
- User
- Sensitivity label
- Retention label

The value of understanding what actions are being taken with sensitive content is that admins can see if the controls that they've already put in place, such as data loss prevention policies, are effective or not. For example, if it's discovered that a large number of items labeled Highly Confidential have suddenly been downgraded to Public, admins can update policies and act to restrict undesired behavior as a response.




## 4.2.3. Describe Sensitivity Labels And Policies

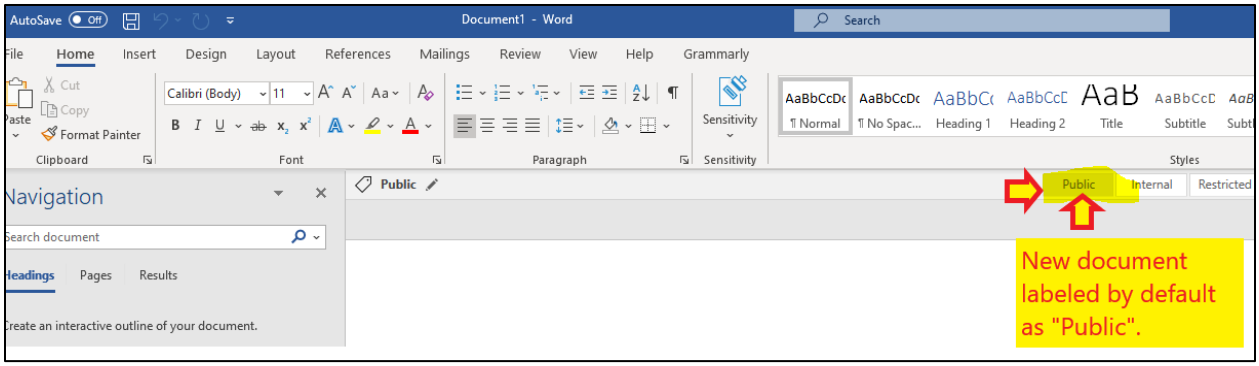
Organizations must protect their data, to safeguard customers and business operations, and to meet compliance standards. Admins can enable their organization to protect its data, through capabilities and tools such as sensitivity labels and policies in Microsoft 365 compliance center.

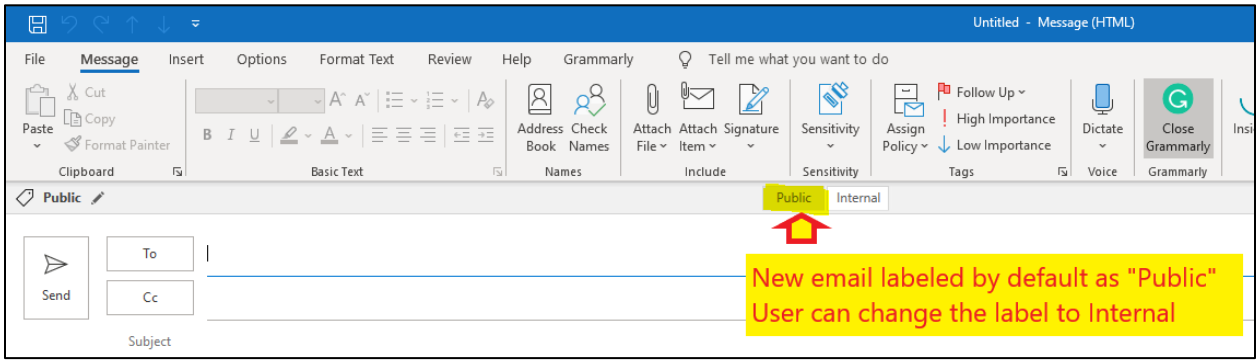
### 4.2.3.1. Sensitivity Labels

Sensitivity labels, available as part of information protection in the Microsoft 365 compliance center, enable the labeling and protection of content, without affecting productivity and collaboration. With sensitivity labels, organizations can decide on labels to apply to content such as emails and documents, much like different stamps are applied to physical documents:

Note:

Each item that supports sensitivity labels can only have one label applied to it, at any given time.




#### 4.2.3.1.1. Labels are
#### 4.2.3.1.1.1. Customizable

Admins can create different categories specific to the organization, such as Personal, Public, Confidential, and Highly Confidential.

#### 4.2.3.1.1.2. Clear text

Because each label is stored in clear text in the content's metadata, third-party apps and services can read it and then apply their own protective actions, if necessary.

#### 4.2.3.1.1.3. Persistent

After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. The label then moves with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.

### 4.2.3.2. Use Case Sensitivity Labels
#### 4.2.3.2.1. Encrypt email only or both email and documents

When a document or email is encrypted, access to the content is restricted, so that:

- It can be decrypted only by users authorized by the label's encryption settings.
- Remains encrypted no matter where it stays, inside or outside your organization, even if the file is renamed.
- It's encrypted both at rest (for example, in a OneDrive account) and in transit (for example, an email message as it traverses the internet).

#### 4.2.3.2.2. Mark the content when Office apps are used

Marking the content includes adding watermarks, headers, or footers. Headers or footers can be added to emails or documents that have the label applied. Watermarks can be applied to documents but not to email.

#### 4.2.3.2.3. Apply the label automatically in Office apps or recommend a label

Admins choose the types of sensitive information to be labeled. The label can be applied automatically or configured to prompt users to apply the recommended label.

#### 4.2.3.2.4. Protect content in containers such as sites and groups when this capability is enabled

This label configuration doesn't result in documents being automatically labeled. Instead, the label settings protect content by controlling access to the container where documents are stored.

#### 4.2.3.2.5. Extend sensitivity labels to third-party apps and services

Using the Microsoft Information Protection SDK, third-party apps can read sensitivity labels and apply protection settings.

#### 4.2.3.2.6. Classify content without using any protection settings

A classification can be assigned to content (just like a sticker) that persists and roams with the content as it's used and shared. The classification can be used to generate usage reports and view activity data for sensitive content.

### 4.2.3.3. Label Policies

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups. The sensitivity labels can be applied to documents and emails. Label policies enable admins to:

#### 4.2.3.3.1. 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.

#### 4.2.3.3.2. 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.

#### 4.2.3.3.3. 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.

#### 4.2.3.3.4. 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.

#### 4.2.3.3.5. Link users to custom help pages

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

#### 4.2.3.3.6. Sensitive Label after applied

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content. For example, by choosing encryption settings for a sensitivity label, admins can protect content so that:

- Only users within the organization can open a confidential document or email.
- Only users in a specific department can edit and print a document or email, while all other users in the organization can only read it.
- Users can't forward or copy information from an email.
- Users can't open a document after a specified date.

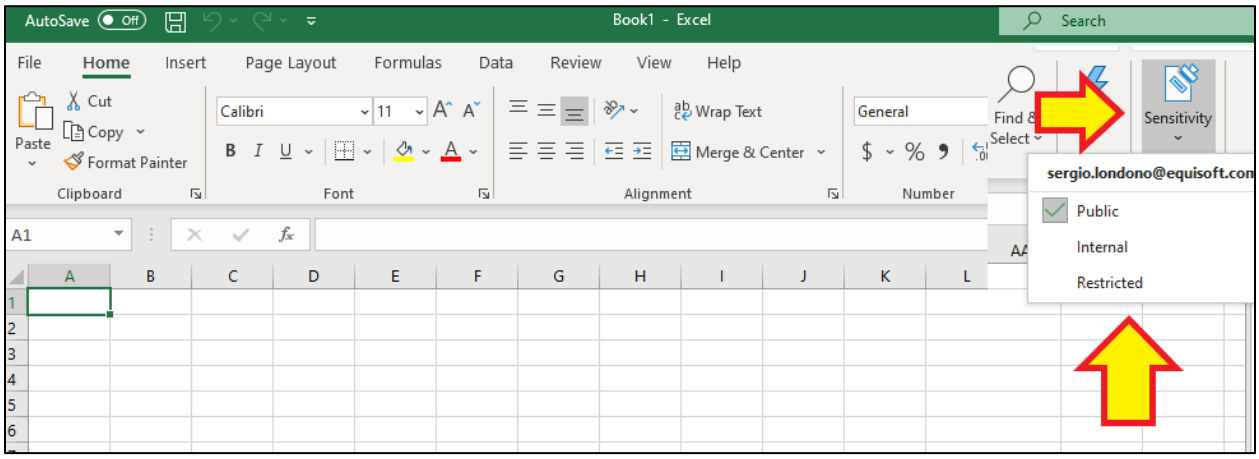
### 4.2.3.4. Azure Information Protection

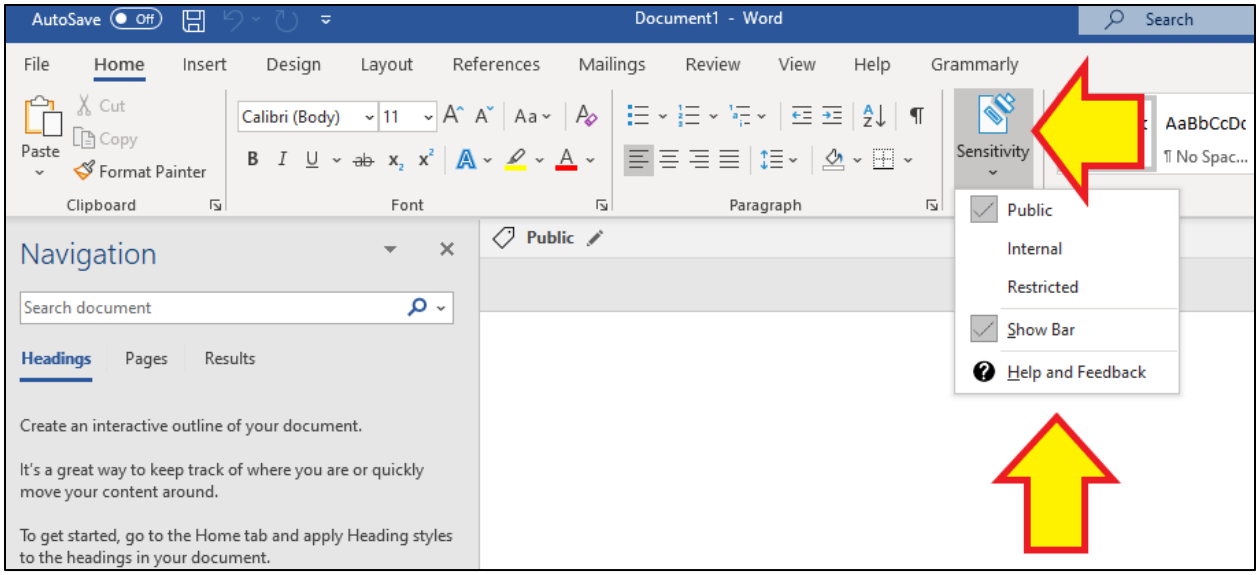
Admins can also enable users to label and protect their files using the Windows File Explorer (to label extra file types, and more files simultaneously), by installing the Azure Information Protection unified labeling client on Windows devices.

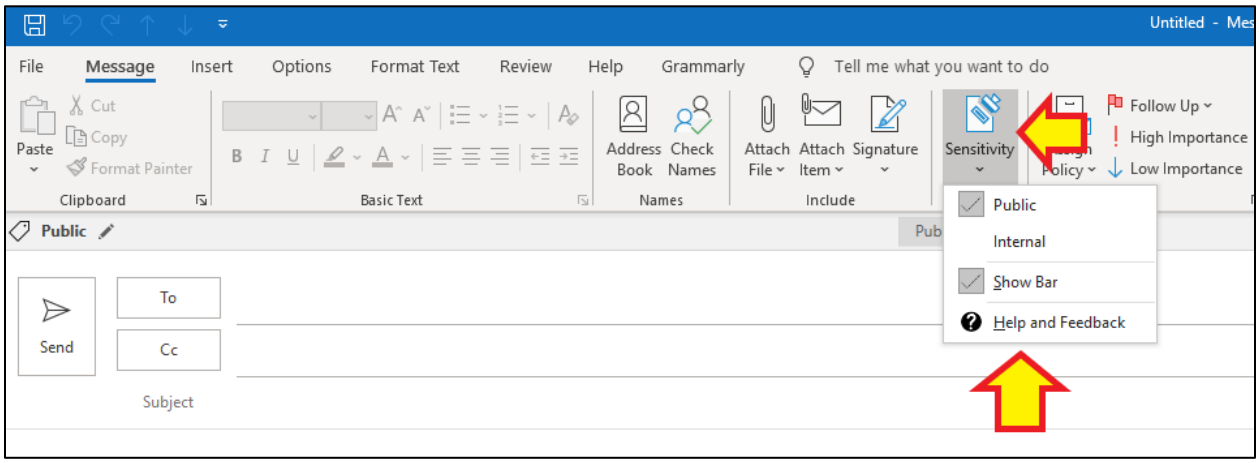
Install the Azure Information Protection unified labeling client (AzInfoProtection_UL) for labels that can be used by:

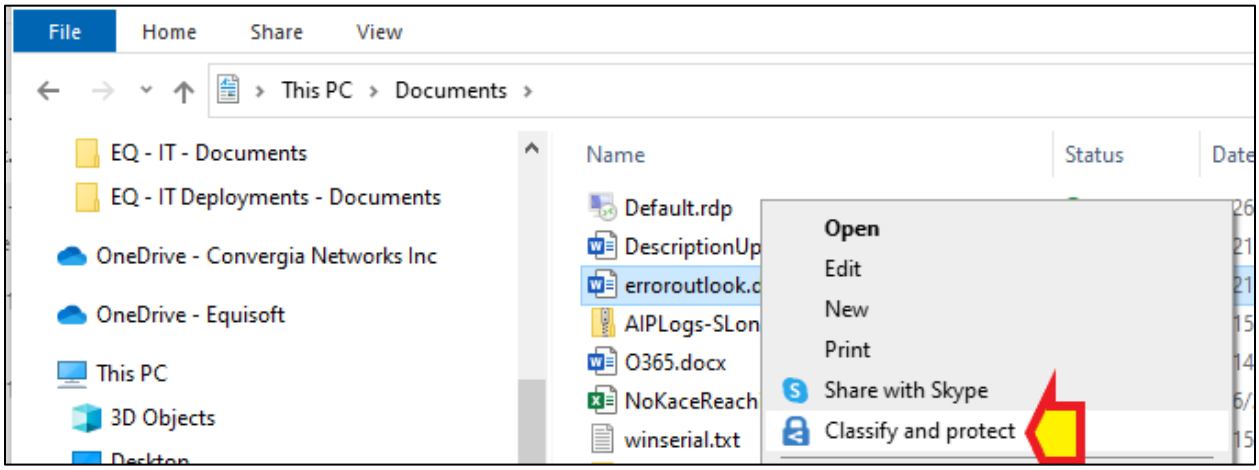
- Office365 Apps
- MacOS
- iOS
- Android

Microsoft Azure Information Protection helps you classify and label data in your organization at the time of creation, as well as apply protection, based on encryption and usage rights for sensitive data. Labels and protection are persistent, traveling with the data throughout its lifecycle so that it's detectable and controlled at all times – regardless of where it's stored or with whom it's shared – internally or externally.


AutoSave
Document1 - Word
Search
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Grammarly
Paste
Cut
Copy
Format Painter
Clipboard
Calibri (Body)
11
Font
Paragraph
Sensitivity
AaBbCcDc
¶ No Spac...
Public
Internal
Restricted
Show Bar
Help and Feedback
Navigation
Search document
Headings
Pages
Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.


Untitled - Mes
File
Message
Insert
Options
Format Text
Review
Help
Grammarly
Tell me what you want to do
Paste
Cut
Copy
Format Painter
Clipboard
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Sensitivity
Follow Up
High Importance
Low Importance
Public
Internal
Show Bar
Help and Feedback
Send
To
Cc
Subject


File
Home
Share
View
This PC
Documents
EQ - IT - Documents
EQ - IT Deployments - Documents
OneDrive - Convergia Networks Inc
OneDrive - Equisoft
This PC
3D Objects
Name
Status
Default.rdp
DescriptionUp
erroroutlook.c
AIPLogs-SLon
O365.docx
NoKaceReach
winserial.txt
Open
Edit
New
Print
Share with Skype
Classify and protect

### 4.2.4. Describe Data Loss Prevention

Data loss can harm an organization's customers, business processes, and the organization itself. Organizations need to prevent data loss by detecting risky behavior and preventing sensitive information from being shared inappropriately. Admins can use data loss prevention policies, available in Microsoft 365 compliance center, to help their organization.

Data loss prevention (DLP) is a way to protect sensitive information and prevent its inadvertent disclosure. With DLP policies, admins can:

#### 4.2.4.1. Identify, monitor, and automatically protect

sensitive information across Microsoft 365, including:

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

#### 4.2.4.2. Help users learn how compliance works

Without interrupting their workflow. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip.

#### 4.2.4.3. View DLP reports

Showing content that matches the organization's DLP policies. To assess how the organization is following a DLP policy, admins can see how many matches each policy has over time.

#### 4.2.4.4. DLP policies protect content through the enforcement of rules

For example, an admin can configure a DLP policy that helps detect information that's subject to a compliance regulation like the Health Insurance Portability and Accountability Act (HIPAA) across all SharePoint sites and OneDrive for Business. The admin can block the relevant documents from being shared inappropriately.

DLP policies protect information by identifying and automatically protecting sensitive data. Here's some scenarios where DLP policies can help:

- Identify any document containing a credit card number stored in users' OneDrive for Business accounts.
- Automatically block an email containing employee personal information from being sent outside the organization.

#### 4.2.4.4.1. Conditions

Conditions that the content must match before the rule is enforced.

#### 4.2.4.4.2. Actions

Actions that the admin wants the rule to take automatically when content that matches the conditions has been found.

#### 4.2.4.4.3. Locations

Locations where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.

### 4.2.4.5. DLP Rules

A policy can contain one or more rules, and each rule consists of conditions and actions at a minimum. For each rule, when the conditions are met, the actions are taken automatically. Rules can be grouped into one policy, to help simplify management and reporting. The diagram below shows how multiple rules, each with their own conditions and actions, are grouped into a single policy:


The rules inside the policy are prioritized in how they're implemented. For example, in the above diagram, rule one will be prioritized before rule two, and so on.

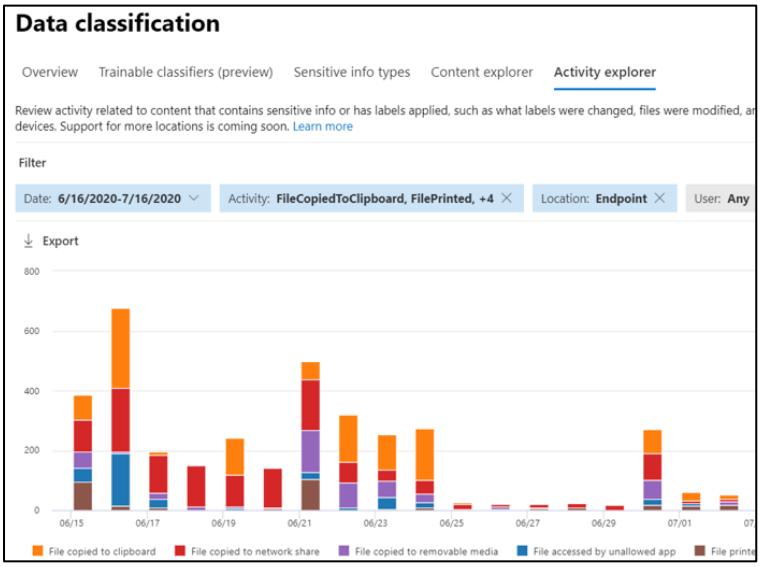
### 4.2.4.6. What is endpoint data loss prevention?

Endpoint data loss prevention is how the protection and activity monitoring capabilities of DLP for sensitive content can be extended to Windows 10 devices. Admins can choose to target Windows 10 when creating a DLP policy (after onboarding the devices to Microsoft 365 compliance solutions). Endpoint DLP enables admins to audit and manage activities that users complete on sensitive content, including:

- Creating an item
- Renaming an item
- Copying items to removable media

- Copying items to network shares
- Printing documents
- Accessing items using unallowed apps and browsers

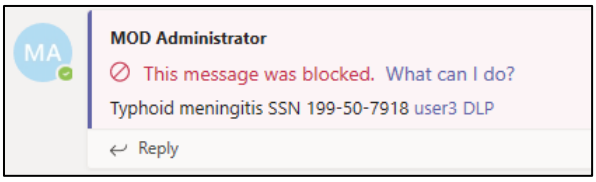
In the activity explorer, you can view information about what users are doing with sensitive content:



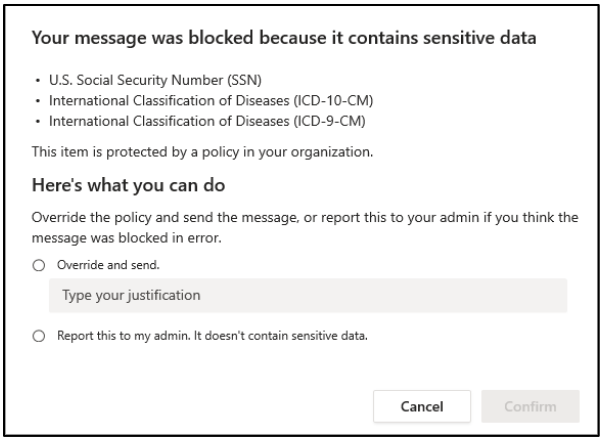

Admins use this information to enforce protective actions for content through controls and policies.

### 4.2.4.7. Data Loss Prevention in Microsoft Teams

Data loss prevention capabilities have been extended to Microsoft Teams chat and channel messages, including messages in private channels. With DLP, administrators can now define policies that prevent users from sharing sensitive information in a Teams chat session or channel, whether it's in a message, or a file. Just like with Exchange, Outlook, SharePoint, and OneDrive for Business, administrators can use DLP policy tips that will be displayed to the user to show them why a policy has been triggered. For example, the screenshot below shows a policy tip on a chat message that was blocked because the user attempted to share a U.S. Social Security Number:




The user can then find out more information about why their message was blocked by selecting the "What can I do?" link, and take appropriate action:




With DLP policies, Microsoft Teams can help users across organizations to collaborate securely and in a way that's in line with compliance requirements.

## 4.2.5. Describe Retention Policies And Retention Labels

Retention labels and policies help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

- Comply proactively with industry regulations and internal policies that require content to be kept for a minimum time.
- Reduce risk when there's litigation or a security breach by permanently deleting old content that the organization is no longer required to keep.
- Ensure users work only with content that's current and relevant to them.
    - When content has retention settings assigned to it, that content remains in its original location. People can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy of the content is automatically kept in a secure location. The secure locations and the content are not visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.

When using retention policies and retention labels to assign retention settings to content, there are some points to understand about each. Listed below are just a few of the key points.

### 4.2.5.1. Retention Setting Locations

Retention settings work with the following different workloads:

### 4.2.5.2. Retention policies

- Retention policies are used to assign the same retention settings to content at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container specified in the retention policy. If a policy is configured to keep content, and an item is then moved outside that container, a copy of the item is kept in the workload's secured location. However, the retention settings don't travel with the content in its new location.

### 4.2.5.3. Retention labels

- Retention labels are used to assign retention settings at an item level, such as a folder, document, or email.
- An email or document can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content if it’s moved to a different location within your Microsoft 365 tenant.
- Admins can enable users in the organization to apply a retention label manually.
- A retention label can be applied automatically if it matches defined conditions.
- A default label can be applied for SharePoint documents.
- Retention labels support disposition review to review the content before it's permanently deleted.

Consider the following scenarios. If all documents in a SharePoint site should be kept for five years, it's more efficient to do with a retention policy than apply the same retention label to all documents in that site.

However, if some documents in that site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual item with a retention setting of 10 years.

## 4.2.6. Describe Records Management

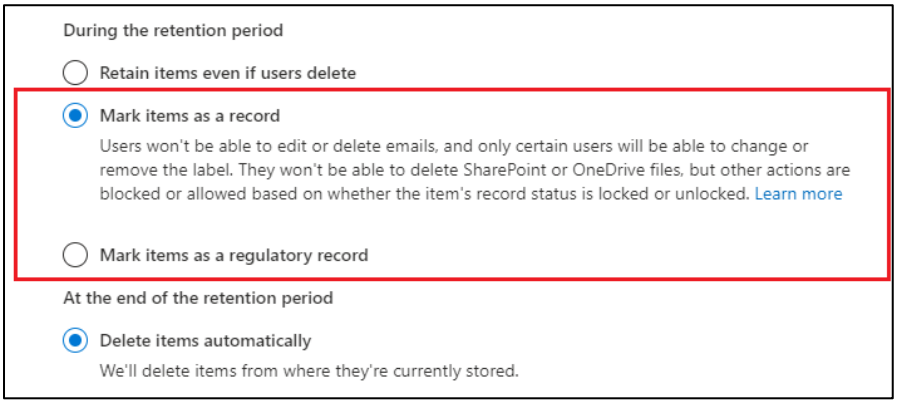
Organizations of all types require a management solution to manage regulatory, legal, and business-critical records across their corporate data. Records management in Microsoft 365 helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or no longer required for business purposes. It provides the following capabilities:

- 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.

When content is labeled as a record, the following happens:

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

To enable items to be marked as records, an administrator sets up retention labels.




Items such as documents and emails can then be marked as records based on those retention labels. Items might be marked as records, but they can also be shown as regulatory records. Regulatory records provide other controls and restrictions such as:

- A regulatory label can't be removed when an item has been marked as a regulatory record.
- The retention periods can't be made shorter after the label has been applied.

For more information on comparing, use the Compare restrictions for what actions are allowed or blocked section of the documentation.

The most important difference is that if content has been marked as a regulatory record, nobody, not even a global administrator, can remove the label. Marking an item as a regulatory record can have irreversible consequences, and should only be used when necessary. As a result, this option isn't available by default, and has to be enabled by the administrator using PowerShell.

#### 4.2.6.1. Common Use Cases For Records Management

Microsoft 365's records management capabilities are flexible. There are different ways in which records management can be used across an organization, including:

- Enabling administrators and users to manually apply retention and deletion actions for documents and emails.
- Automatically applying retention and deletion actions to documents and emails.
- Enabling site admins to set default retain and delete actions for all content in a SharePoint library, folder, or document set.
- Enabling users to automatically apply retain and delete actions to emails by using Outlook rules.

To ensure records management is used correctly across the organization, administrators can work with content creators to put together training materials. Documentation should explain how to apply labels to drive usage, and ensure a consistent understanding.

#### 4.2.6.2. Compare restrictions for what actions are allowed or blocked

| Action | Retention label | Record - locked | Record - unlocked | Regulatory record |
|---|---|---|---|---|
| Edit contents | Allowed | **Blocked** | Allowed | **Blocked** |
| Edit properties, including rename | Allowed | Allowed | Allowed | **Blocked** |
| Delete | Allowed [1] | **Blocked** | **Blocked** | **Blocked** |
| Copy | Allowed | Allowed | Allowed | Allowed |
| Move within container [2] | Allowed | Allowed | Allowed | Allowed |
| Move across containers [2] | Allowed | Allowed if never unlocked | **Blocked** | **Blocked** |
| Open/Read | Allowed | Allowed | Allowed | Allowed |
| Change label | Allowed | Allowed - container admin only | Allowed - container admin only | **Blocked** |
| Remove label | Allowed | Allowed - container admin only | Allowed - container admin only | **Blocked** |

## 4.3. Describe Insider Risk Capabilities in Microsoft 365

Learn how Microsoft 365 enables organizations to identify critical insider risks and take the appropriate action.

Organizations understand that risks can come from insiders, like contractors, or even employees. There's always a risk that people might share information with competitors after leaving the company. Organizations need to ensure that they're protected from these kinds of risks.

In this module, you'll learn how Microsoft 365 capabilities like insider risk management, communication compliance, information barriers, privileged access management, and Customer Lockbox can help you protect your organization.

After completing this module, you should be able to:

- Describe how Microsoft 365 can help organizations identify insider risks and take appropriate action.
- Describe how Microsoft 365 helps organizations identify, investigate, and remediate malicious and inadvertent activities in your organization.

# Initial tailored risk playbook categories

**Departing Employee Data Theft**

Theft of intellectual property by a departing employee

**Data Leaks**

Intentional or unintentional leak or sensitive or confidential information

Disgruntled Employee
High Priority Employee

**Security Policy Violations**

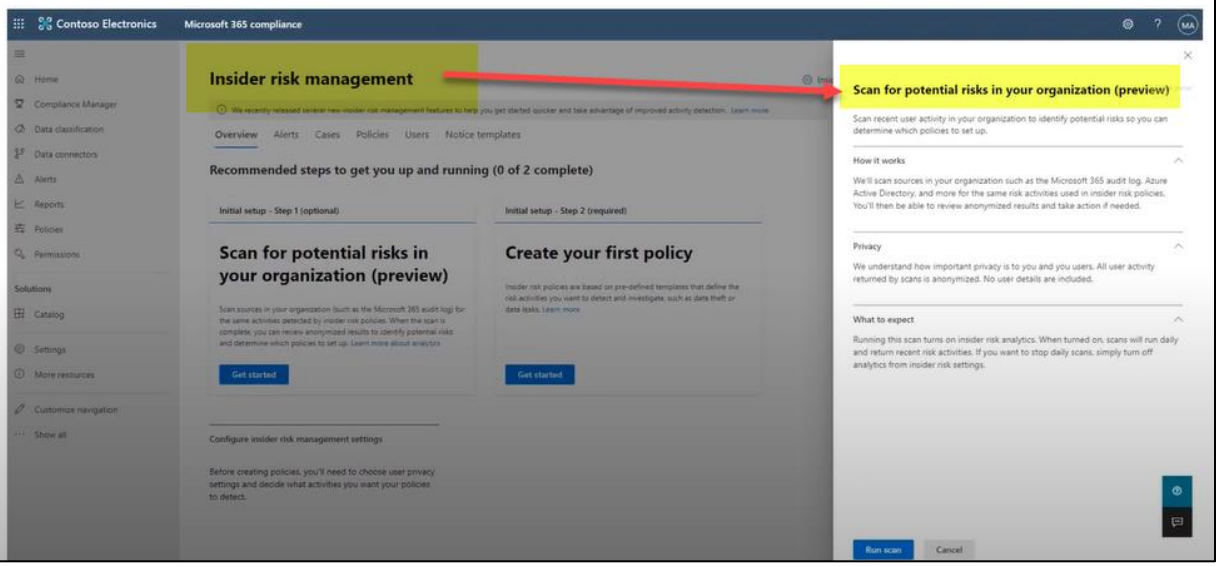
Malicious or unintentional violation of company security policies on endpoints

General Violations
Violations by departing, disgruntled, or high priority users

*59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data*[1]

# Insider Risk Analytics

- **Easy to configure –** single click at the start of set up



### 4.3.1. Describe the Insider Risk Management Solution

Insider risk management is a solution in Microsoft 365 that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in Microsoft 365 compliance center.

There are various capabilities available from Microsoft 365 to help protect organizations from insider risks. Without these capabilities, organizations wouldn't be protected from insider risk, which could have serious negative financial and reputational consequences. Instead, organizations can prevent this from happening by protecting themselves from insider risk.

Managing and minimizing risk in an organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors, and are outside an organization's direct control. Other risks are driven by internal events and employee activities that can be eliminated and avoided. Some examples are risks from illegal, inappropriate, unauthorized, or unethical behavior and actions by employees and managers. These behaviors can lead to a broad range of internal risks from employees:

#### 4.3.1.1. Internal Risk

##### 4.3.1.1.1. Leaks of sensitive data and data spillage

##### 4.3.1.1.2. Confidentiality violations

##### 4.3.1.1.3. Intellectual property (IP) theft

##### 4.3.1.1.4. Fraud

##### 4.3.1.1.5. Insider trading

##### 4.3.1.1.6. Regulatory compliance violations

#### 4.3.1.2. Insider Risk Management Principles

Insider risk management is centered around the following principles:

##### 4.3.1.2.1. Transparency

Transparency: Balance user privacy versus organization risk with privacy-by-design architecture.

##### 4.3.1.2.2. Configurable

Configurable: Configurable policies based on industry, geographical, and business groups.

##### 4.3.1.2.3. Integrated

Integrated: Integrated workflow across Microsoft 365 compliance solutions.

##### 4.3.1.2.4. Actionable

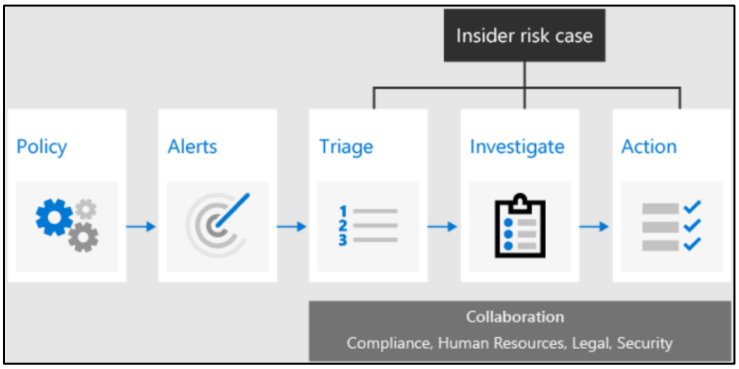
Actionable: Provides insights to enable user notifications, data investigations, and user investigations.

### 4.3.1.3. Insider risk management workflow

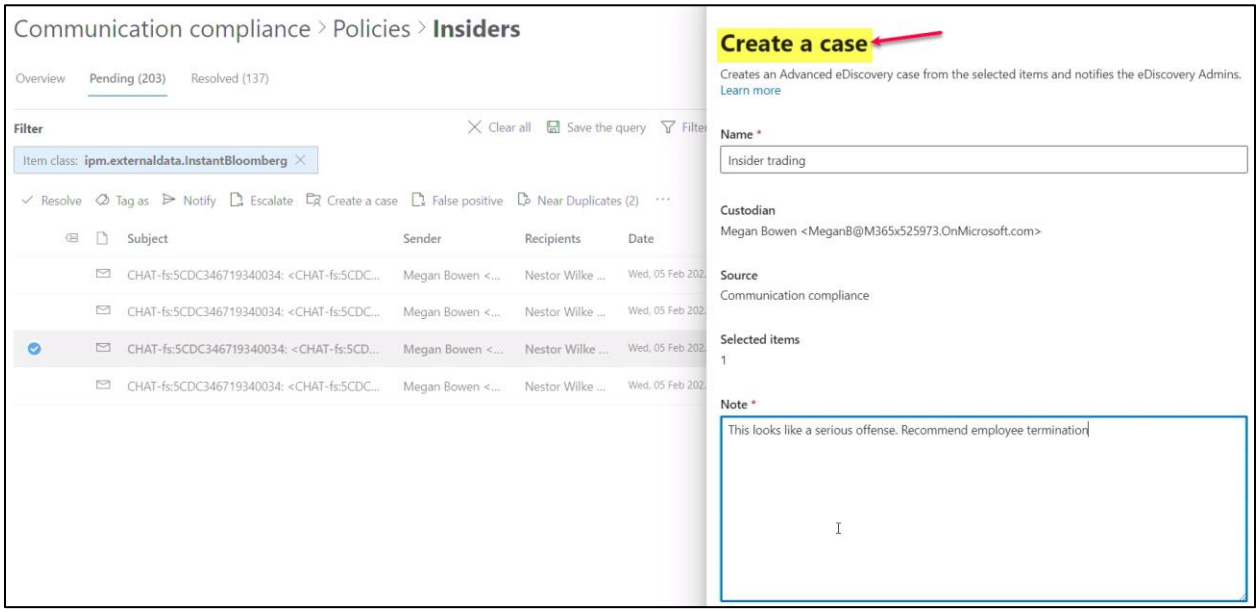
Insider risk management helps organizations to identify, investigate, and address internal risks. With focused policy templates, comprehensive activity signaling across Microsoft 365, and a flexible workflow, organizations can take advantage of actionable insights to help identify and resolve risky behavior quickly.

Insider risk management can help you detect, investigate, and take action to mitigate **internal risks in your organization** in several common scenarios. These scenarios include data theft by employees, the intentional, or unintentional leak of confidential information, offensive behavior, and more.

Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft 365 is achieved using the following workflow:



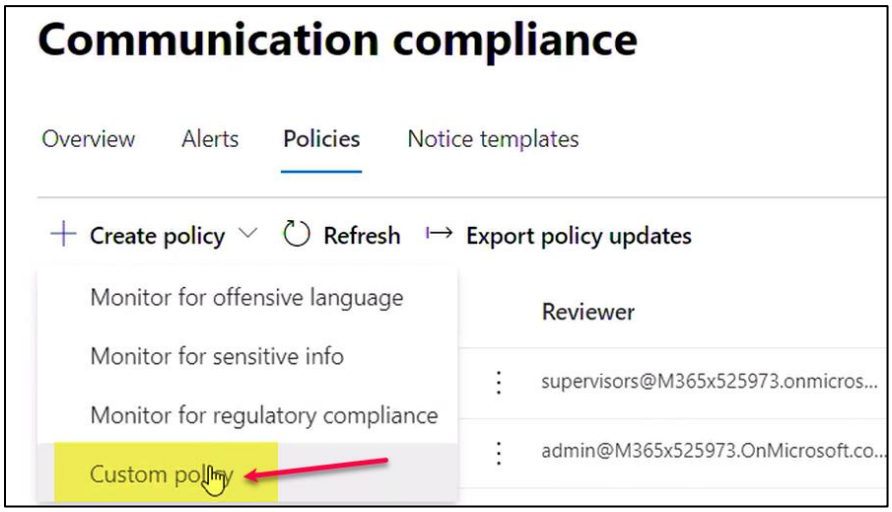

### 4.3.1.4. Insider Risk Case

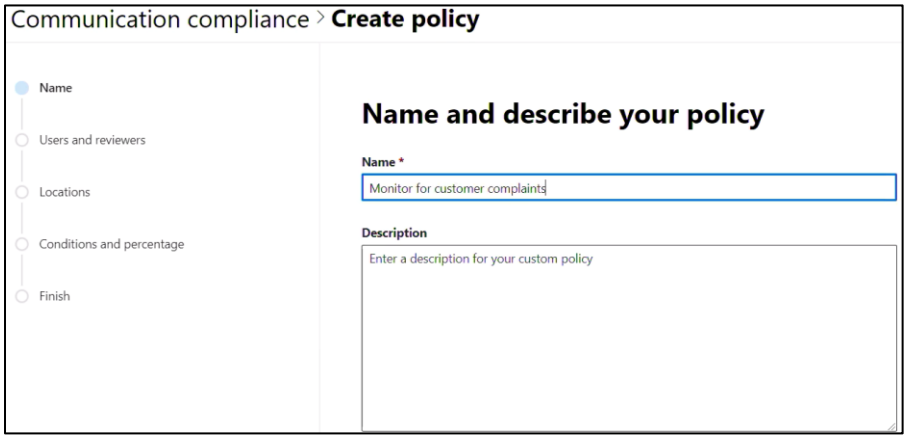


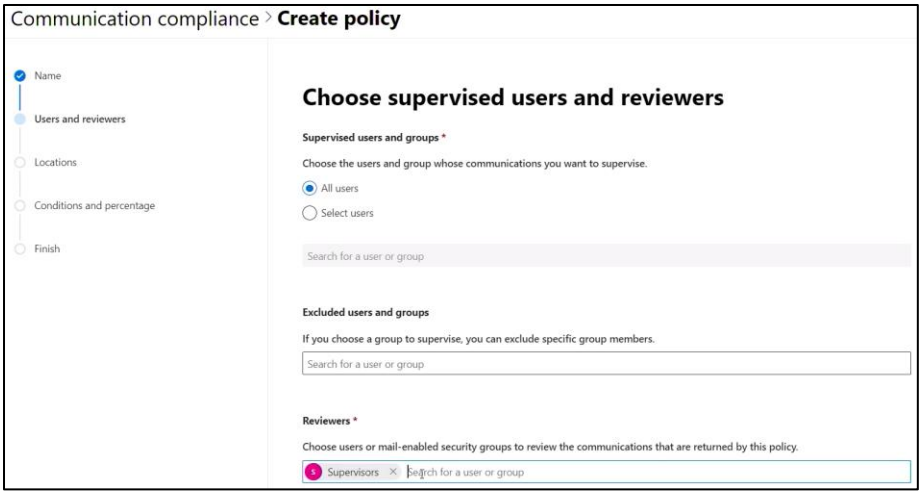
#### 4.3.1.4.1. Policies

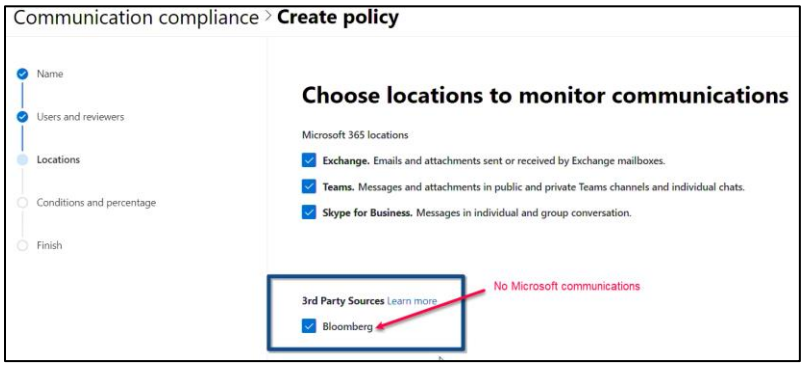
Policies - Insider risk management policies are created using predefined templates and policy conditions that define what risk indicators are examined in Microsoft 365 feature areas. These conditions include how indicators are used for alerts, what users are included in the policy, which services are prioritized, and the monitoring time period.

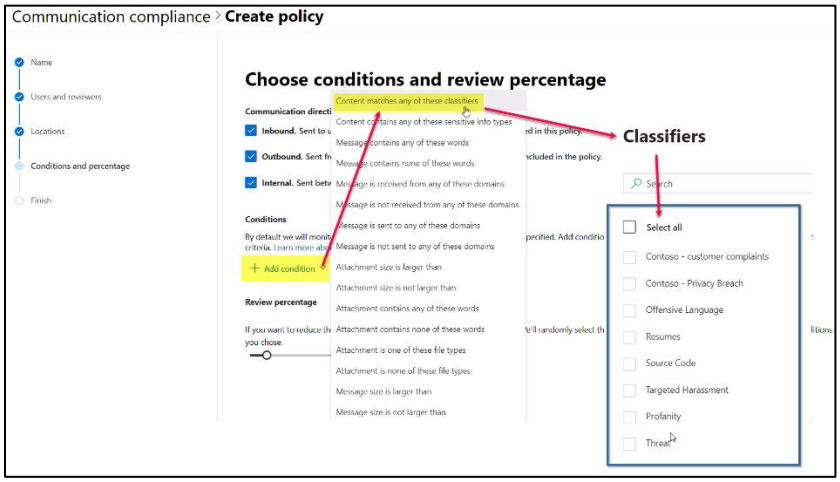
##### 4.3.1.4.1.1. How to create a Policy

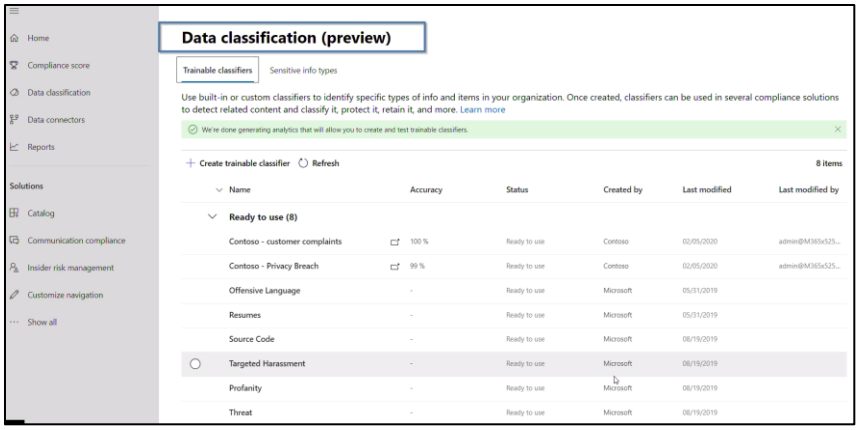


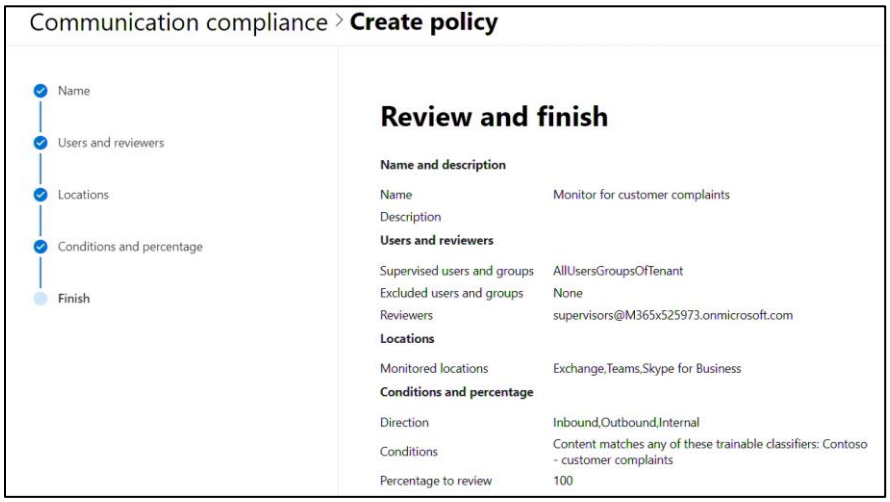




Communication compliance > Create policy
Name
Users and reviewers
Locations
Conditions and percentage
Finish
Choose supervised users and reviewers
Supervised users and groups *
Choose the users and group whose communications you want to supervise.
All users
Select users
Search for a user or group
Excluded users and groups
If you choose a group to supervise, you can exclude specific group members.
Search for a user or group
Reviewers *
Choose users or mail-enabled security groups to review the communications that are returned by this policy.
Supervisors
Search for a user or group


Communication compliance > Create policy
Name
Users and reviewers
Locations
Conditions and percentage
Finish
Choose locations to monitor communications
Microsoft 365 locations
Exchange. Emails and attachments sent or received by Exchange mailboxes.
Teams. Messages and attachments in public and private Teams channels and individual chats.
Skype for Business. Messages in individual and group conversation.
3rd Party Sources Learn more
Bloomberg
No Microsoft communications


Communication compliance > Create policy
Name
Users and reviewers
Locations
Conditions and percentage
Finish
Choose conditions and review percentage
Content matches any of these classifiers
Content contains any of these sensitive info types
Message contains any of these words
Message contains none of these words
Message is received from any of these domains
Message is not received from any of these domains
Message is sent to any of these domains
Message is not sent to any of these domains
Attachment size is larger than
Attachment size is not larger than
Attachment contains any of these words
Attachment contains none of these words
Attachment is one of these file types
Attachment is none of these file types
Message size is larger than
Message size is not larger than
Add condition
Classifiers
Search
Select all
Contoso - customer complaints
Contoso - Privacy Breach
Offensive Language
Resumes
Source Code
Targeted Harassment
Profanity
Threat




#### 4.3.1.4.2. Alerts

Alerts - Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the Alerts dashboard. This dashboard enables a quick view of all alerts needing review, open alerts over time, and alert statistics for the organization.

#### 4.3.1.4.3. Triage

Triage - New activities that need investigation automatically generate alerts that are assigned a Needs review status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.

#### 4.3.1.4.4. Investigate

Investigate - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The Case dashboard provides an all-up view of all active

cases, open cases over time, and case statistics for the organization. Selecting a case on the dashboard opens it for investigation and review. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers.

#### 4.3.1.4.5. Action

Action - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.

##### 4.3.1.4.5.1. Actions

Actions can be as simple as sending a notification when employees accidentally or inadvertently violate policy conditions.

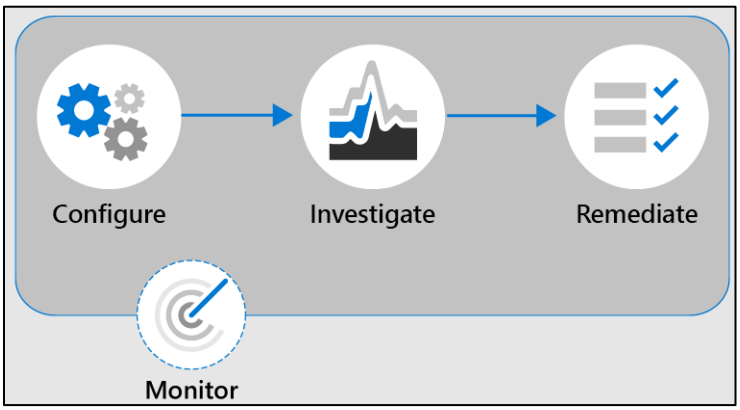
In more serious cases, reviewers may need to share the insider risk management case information with other reviewers in the organization. Escalating a case for investigation makes it possible to transfer data and management of the case to Advanced eDiscovery in Microsoft 365.

### 4.3.2. Describe communication compliance

Communication compliance in Microsoft 365 compliance center helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages. Predefined and custom policies in communication compliance make it possible to scan internal and external communications for policy matches so they can be examined by chosen reviewers.

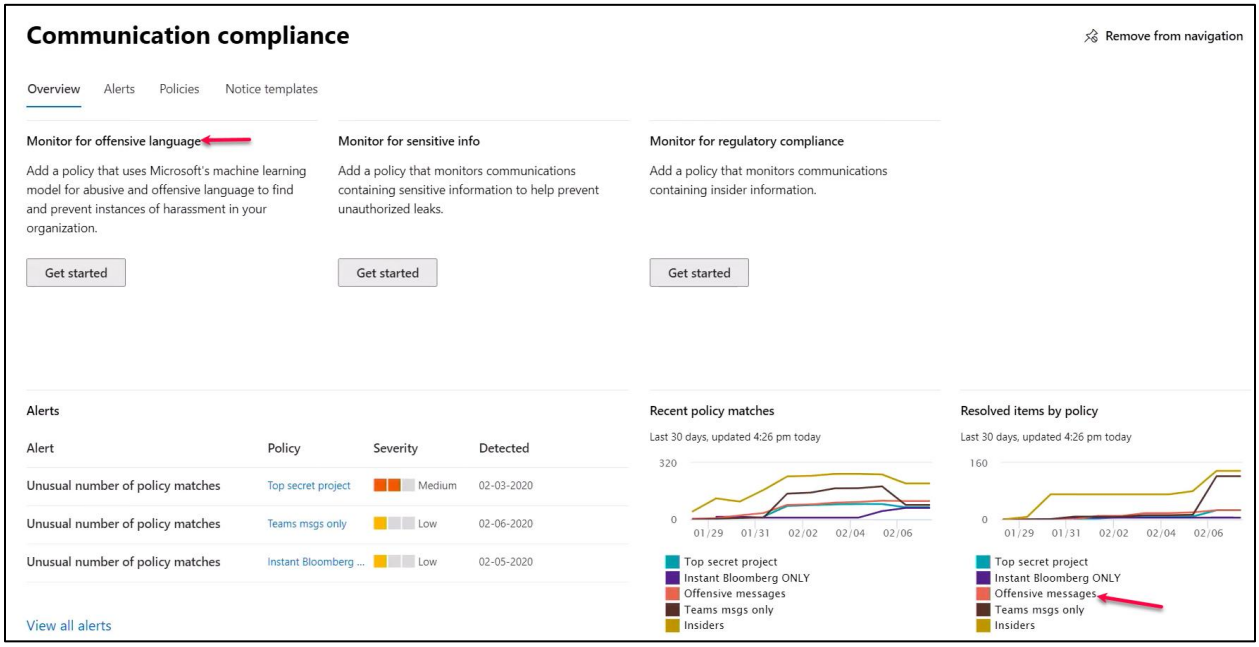
#### 4.3.2.1. Communication Compliance Workflow

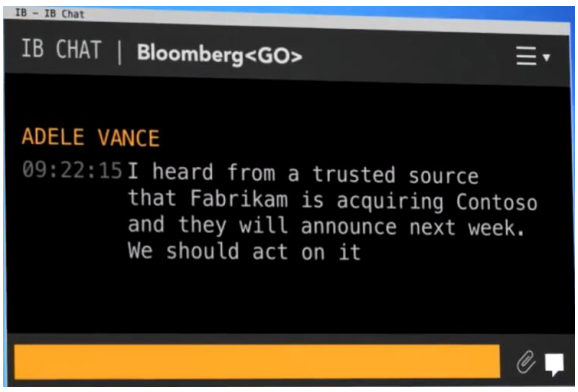
Identifying and resolving compliance issues with communication compliance in Microsoft 365 uses the following workflow:

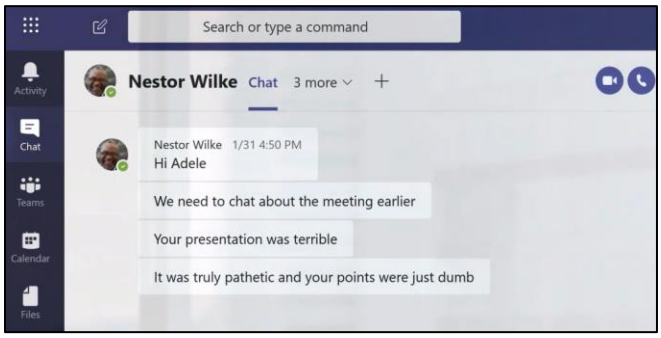


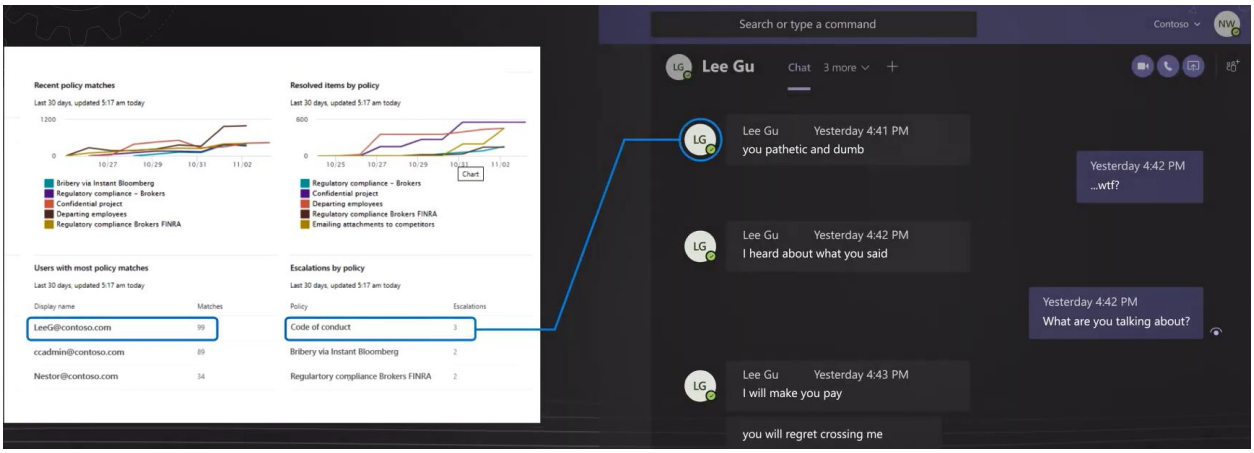

Communication compliance enables reviewers to investigate scanned emails, and messages across Microsoft Teams, Exchange Online, Yammer, or third-party communications in an organization,

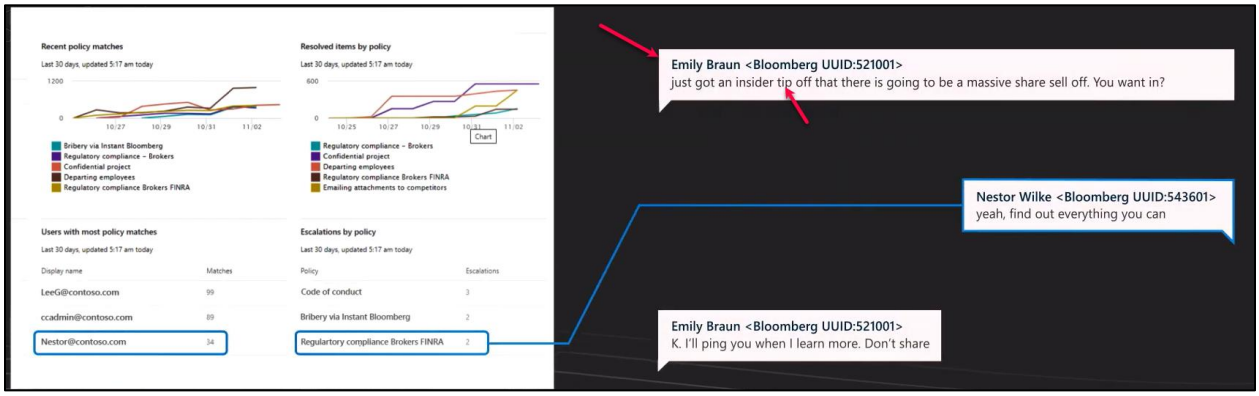
taking appropriate remediation actions to make sure they're compliant with the organization's message standards.

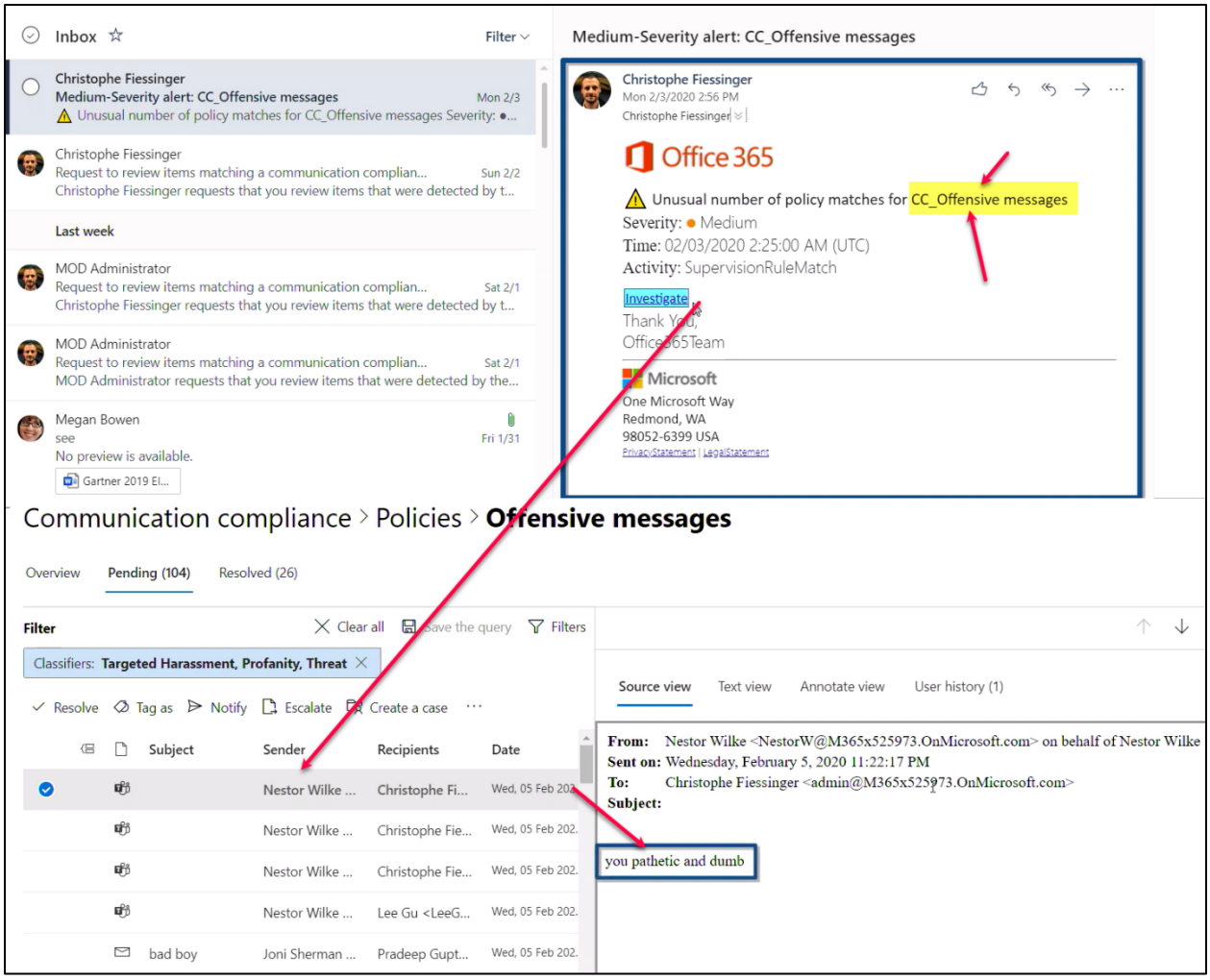


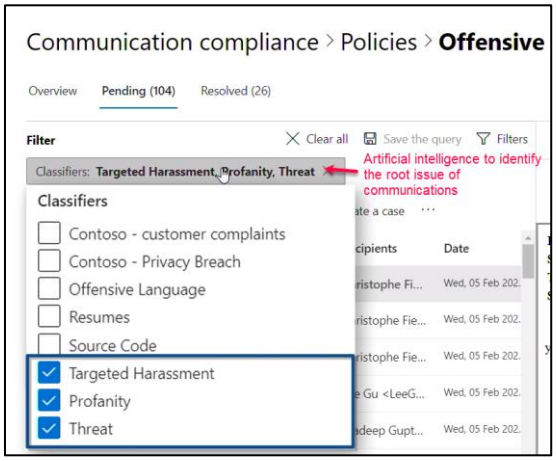




Recent policy matches
Last 30 days, updated 5:17 am today
Bribery via Instant Bloomberg
Regulatory compliance – Brokers
Confidential project
Departing employees
Regulatory compliance Brokers FINRA
Resolved items by policy
Last 30 days, updated 5:17 am today
Regulatory compliance – Brokers
Confidential project
Departing employees
Regulatory compliance Brokers FINRA
Emailing attachments to competitors
Chart
Users with most policy matches
Last 30 days, updated 5:17 am today
Display name
Matches
LeeG@contoso.com 99
ccadmin@contoso.com 89
Nestor@contoso.com 34
Escalations by policy
Last 30 days, updated 5:17 am today
Policy
Escalations
Code of conduct 3
Bribery via Instant Bloomberg 2
Regulartory compliance Brokers FINRA 2
Search or type a command
Contoso
Lee Gu
Chat
3 more
Lee Gu Yesterday 4:41 PM
you pathetic and dumb
Yesterday 4:42 PM
...wtf?
Lee Gu Yesterday 4:42 PM
I heard about what you said
Yesterday 4:42 PM
What are you talking about?
Lee Gu Yesterday 4:43 PM
I will make you pay
you will regret crossing me


Recent policy matches
Last 30 days, updated 5:17 am today
Bribery via Instant Bloomberg
Regulatory compliance – Brokers
Confidential project
Departing employees
Regulatory compliance Brokers FINRA
Resolved items by policy
Last 30 days, updated 5:17 am today
Regulatory compliance – Brokers
Confidential project
Departing employees
Regulatory compliance Brokers FINRA
Emailing attachments to competitors
Chart
Users with most policy matches
Last 30 days, updated 5:17 am today
Display name
Matches
LeeG@contoso.com 99
ccadmin@contoso.com 89
Nestor@contoso.com 34
Escalations by policy
Last 30 days, updated 5:17 am today
Policy
Escalations
Code of conduct 3
Bribery via Instant Bloomberg 2
Regulartory compliance Brokers FINRA 2
Emily Braun <Bloomberg UUID:521001>
just got an insider tip off that there is going to be a massive share sell off. You want in?
Nestor Wilke <Bloomberg UUID:543601>
yeah, find out everything you can
Emily Braun <Bloomberg UUID:521001>
K. I'll ping you when I learn more. Don't share


Inbox
Filter
Christophe Fiessinger
Medium-Severity alert: CC_Offensive messages
Mon 2/3
Unusual number of policy matches for CC_Offensive messages Severity: ●...
Christophe Fiessinger
Request to review items matching a communication complian...
Sun 2/2
Christophe Fiessinger requests that you review items that were detected by t...
Last week
MOD Administrator
Request to review items matching a communication complian...
Sat 2/1
Christophe Fiessinger requests that you review items that were detected by t...
MOD Administrator
Request to review items matching a communication complian...
Sat 2/1
MOD Administrator requests that you review items that were detected by the...
Megan Bowen
see
Fri 1/31
No preview is available.
Gartner 2019 El...
Medium-Severity alert: CC_Offensive messages
Christophe Fiessinger
Mon 2/3/2020 2:56 PM
Christophe Fiessinger
Office 365
Unusual number of policy matches for CC_Offensive messages
Severity: Medium
Time: 02/03/2020 2:25:00 AM (UTC)
Activity: SupervisionRuleMatch
Investigate
Thank You,
Office365Team
Microsoft
One Microsoft Way
Redmond, WA
98052-6399 USA
PrivacyStatement | LegalStatement
Communication compliance > Policies > Offensive messages
Overview
Pending (104)
Resolved (26)
Filter
Clear all
Save the query
Filters
Classifiers: Targeted Harassment, Profanity, Threat
Resolve
Tag as
Notify
Escalate
Create a case
Subject
Sender
Recipients
Date
Nestor Wilke ...
Christophe Fi...
Wed, 05 Feb 202.
Nestor Wilke ...
Christophe Fie...
Wed, 05 Feb 202.
Nestor Wilke ...
Christophe Fie...
Wed, 05 Feb 202.
Nestor Wilke ...
Lee Gu <LeeG...
Wed, 05 Feb 202.
bad boy
Joni Sherman ...
Pradeep Gupt...
Wed, 05 Feb 202.
Source view
Text view
Annotate view
User history (1)
From: Nestor Wilke <NestorW@M365x525973.OnMicrosoft.com> on behalf of Nestor Wilke
Sent on: Wednesday, February 5, 2020 11:22:17 PM
To: Christophe Fiessinger <admin@M365x525973.OnMicrosoft.com>
Subject:
you pathetic and dumb


Communication compliance > Policies > Offensive
Overview
Pending (104)
Resolved (26)
Filter
Clear all
Save the query
Filters
Classifiers: Targeted Harassment, Profanity, Threat
Artificial intelligence to identify the root issue of communications
Classifiers
Contoso - customer complaints
Contoso - Privacy Breach
Offensive Language
Resumes
Source Code
Targeted Harassment
Profanity
Threat
Date

#### 4.3.2.1.1. Configure

in this step, admins identify compliance requirements and configure applicable communication compliance policies.

#### 4.3.2.1.2. Investigate

admins look deeper into the issues detected when matching your communication compliance policies. Tools and steps that help include alerts, issue management to help remediation, document reviews, reviewing user history, and filters.

#### 4.3.2.1.3. Remediate

remediate communications compliance issues. Options include resolving an alert, tagging a message, notifying the user, escalating to another reviewer, marking an alert as a false positive, removing a message in Teams, and escalating for investigation.

#### 4.3.2.1.4. Monitor

Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. Communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs can be used to continually evaluate and improve your compliance posture.

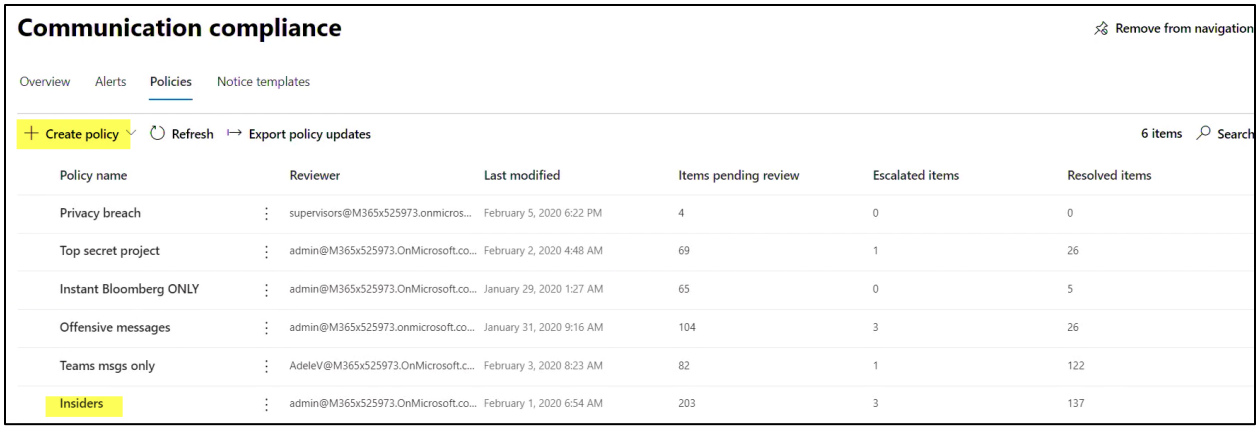
### 4.3.2.2. Review messages

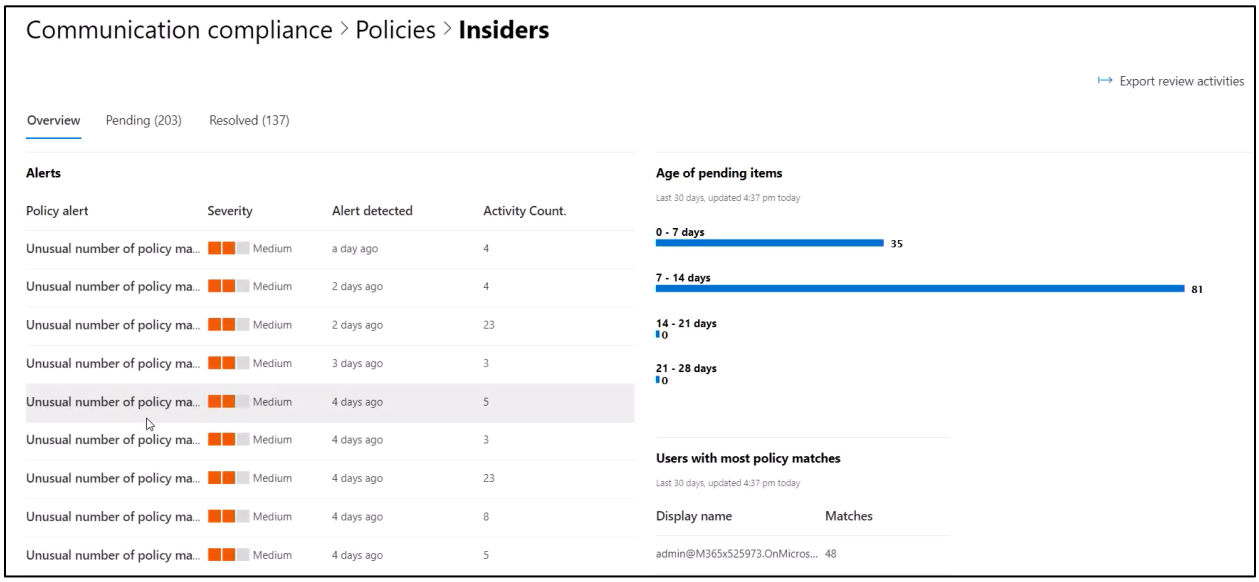
Communication compliance is a powerful tool, that can help maintain and safeguard your staff, your data and your organization.

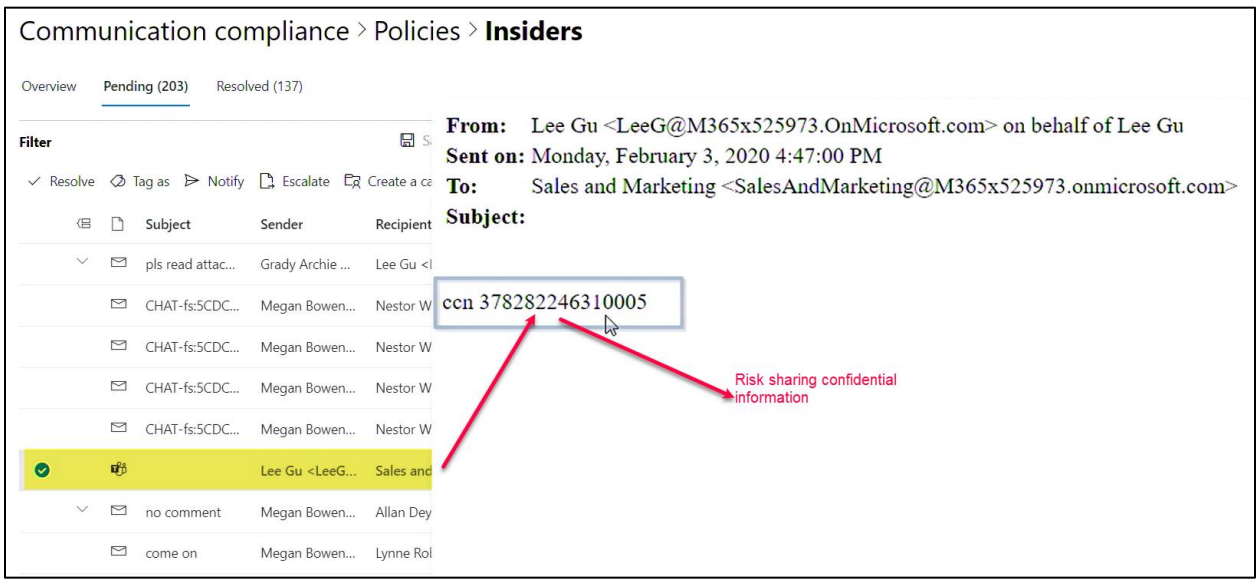
Some important compliance areas where communication compliance policies can assist with reviewing messages include:

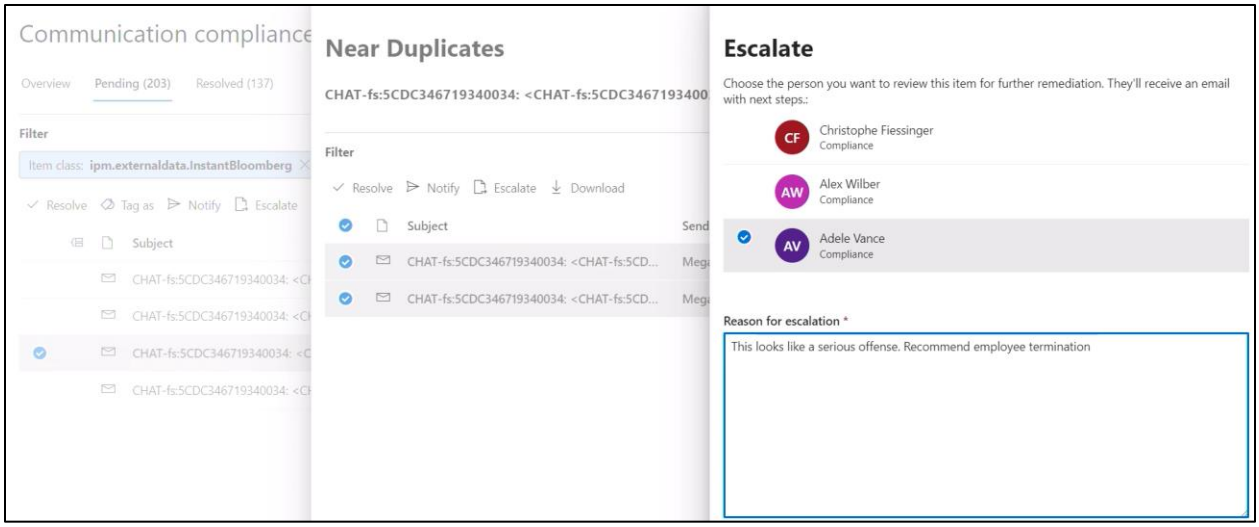
#### 4.3.2.2.1. Corporate policies

Corporate policies - Users have to follow corporate policies like usage and ethical standards in their day-to-day business communications. With communication compliance, admins can scan user communications across the organization for potential concerns of offensive language or harassment.


Communication compliance
Remove from navigation
Overview
Alerts
Policies
Notice templates
Create policy
Refresh
Export policy updates
6 items
Search
Policy name
Reviewer
Last modified
Items pending review
Escalated items
Resolved items
Privacy breach
supervisors@M365x525973.onmicros...
February 5, 2020 6:22 PM
4
0
0
Top secret project
admin@M365x525973.OnMicrosoft.co...
February 2, 2020 4:48 AM
69
1
26
Instant Bloomberg ONLY
admin@M365x525973.OnMicrosoft.co...
January 29, 2020 1:27 AM
65
0
5
Offensive messages
admin@M365x525973.onmicrosoft.co...
January 31, 2020 9:16 AM
104
3
26
Teams msgs only
AdeleV@M365x525973.OnMicrosoft.c...
February 3, 2020 8:23 AM
82
1
122
Insiders
admin@M365x525973.OnMicrosoft.co...
February 1, 2020 6:54 AM
203
3
137


Communication compliance > Policies > Insiders
Export review activities
Overview
Pending (203)
Resolved (137)
Alerts
Policy alert
Severity
Alert detected
Activity Count.
Unusual number of policy ma... Medium a day ago 4
Unusual number of policy ma... Medium 2 days ago 4
Unusual number of policy ma... Medium 2 days ago 23
Unusual number of policy ma... Medium 3 days ago 3
Unusual number of policy ma... Medium 4 days ago 5
Unusual number of policy ma... Medium 4 days ago 3
Unusual number of policy ma... Medium 4 days ago 23
Unusual number of policy ma... Medium 4 days ago 8
Unusual number of policy ma... Medium 4 days ago 5
Age of pending items
Last 30 days, updated 4:37 pm today
0 - 7 days
35
7 - 14 days
81
14 - 21 days
0
21 - 28 days
0
Users with most policy matches
Last 30 days, updated 4:37 pm today
Display name
Matches
admin@M365x525973.OnMicros... 48


Communication compliance > Policies > Insiders
Overview
Pending (203)
Resolved (137)
Filter
Resolve
Tag as
Notify
Escalate
Create a ca
Subject
Sender
Recipient
pls read attac... Grady Archie ... Lee Gu <l
CHAT-fs:5CDC... Megan Bowen... Nestor W
CHAT-fs:5CDC... Megan Bowen... Nestor W
CHAT-fs:5CDC... Megan Bowen... Nestor W
CHAT-fs:5CDC... Megan Bowen... Nestor W
Lee Gu <LeeG... Sales and
no comment Megan Bowen... Allan Dey
come on Megan Bowen... Lynne Rol
From: Lee Gu <LeeG@M365x525973.OnMicrosoft.com> on behalf of Lee Gu
Sent on: Monday, February 3, 2020 4:47:00 PM
To: Sales and Marketing <SalesAndMarketing@M365x525973.onmicrosoft.com>
Subject:
ccn 378282246310005
Risk sharing confidential information




#### 4.3.2.2.2. Risk management

Risk management - Communication compliance can help admins scan for unauthorized communication about projects that are considered to be confidential, such as acquisitions, earnings disclosures, and more.

#### 4.3.2.2.3. Regulatory compliance

Regulatory compliance - Most organizations are expected to follow some regulatory compliance standards during their day-to-day operations. For example, a regulation might require organizations to review communications of its brokers to safeguard against potential insider trading, money laundering, or bribery. Communication compliance enables the organization to scan and report on these types of communications in a way that meets their requirements.

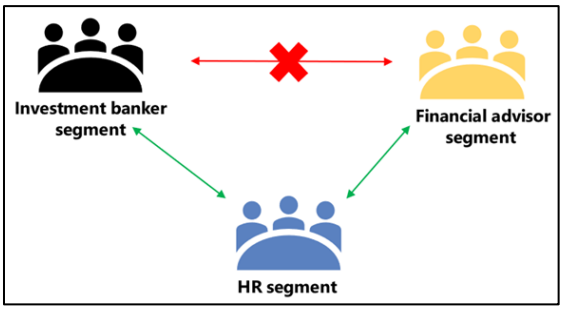
### 4.3.3. Describe information barriers

Microsoft 365 provides organizations with powerful communication and collaboration capabilities. However, an organization might want to restrict communications between some groups to avoid a conflict of interest from occurring in the organization, or to restrict communications between certain people to safeguard internal information. With information barriers, the organization can restrict communications among specific groups of users.

It's important to note that information barriers only support two-way restrictions. One-way restrictions, such as marketing, can communicate with day traders but day traders who can't communicate with marketing are not supported.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other. When information barrier policies are in place, people who shouldn't communicate with other specific users can't find, select, chat, or call those users. With information barriers, checks are in place to prevent unauthorized communication.

Information barriers are supported in solutions like Microsoft Teams, OneDrive for Business, SharePoint Online, and more.




#### 4.3.3.1. Information Barriers Examples

Here are some examples of how information barriers can be applied:

##### 4.3.3.1.1. Education

Education: Students in one school can't look up contact details for students of other schools.

##### 4.3.3.1.2. Legal

Legal: Maintaining confidentiality of data obtained by the lawyer of one client from being accessed by a lawyer for the same firm representing a different client.

##### 4.3.3.1.3. Professional services

Professional services: A group of people in a company is only able to chat with a client or specific customer via federation or guest access during a customer engagement.

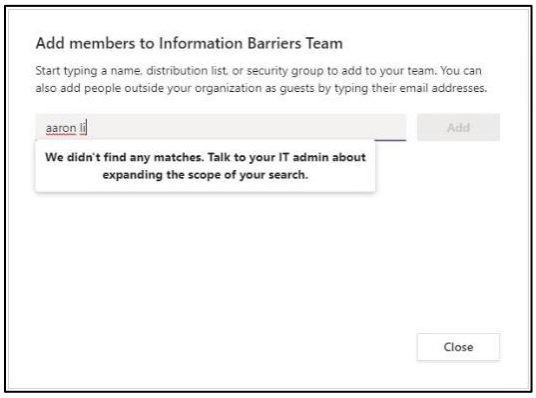
#### 4.3.3.2. Information Barrier in Microsoft Teams

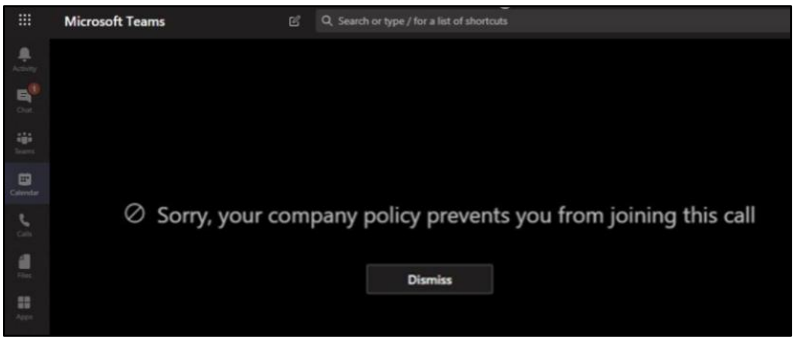
In Microsoft Teams, information barrier policies determine and prevent the following kinds of unauthorized communications:

- 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

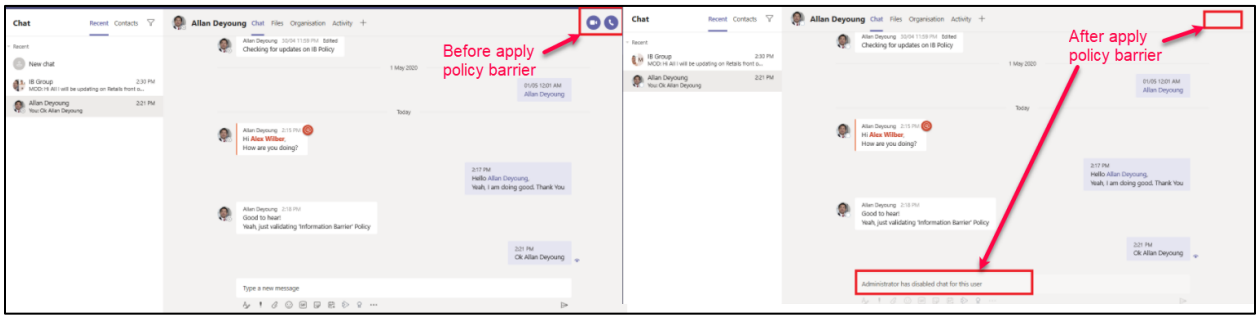
- Sharing a screen
- Placing a call
- Sharing a file with another user
- Access to file through sharing link

If the people involved are included in an information barrier policy to prevent the activity, they cannot continue. Potentially, everyone included in an information barrier policy can be blocked from communicating with others in Microsoft Teams. When people affected by information barrier policies are part of the same team or group chat, they might be removed from those chat sessions and further communication with the group might not be allowed.



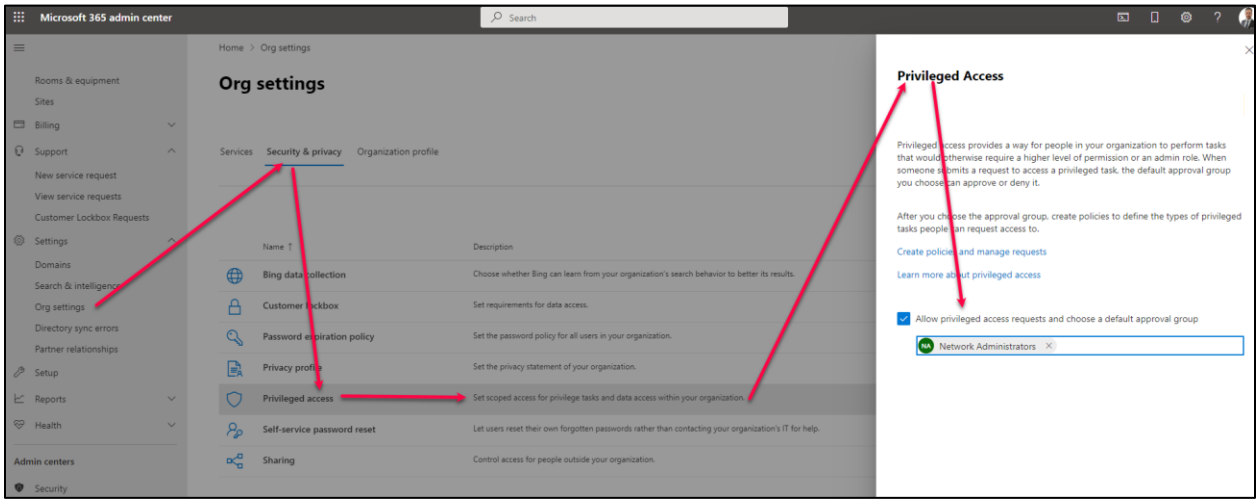

#### 4.3.3.2.1. Communication barrier example in MS teams

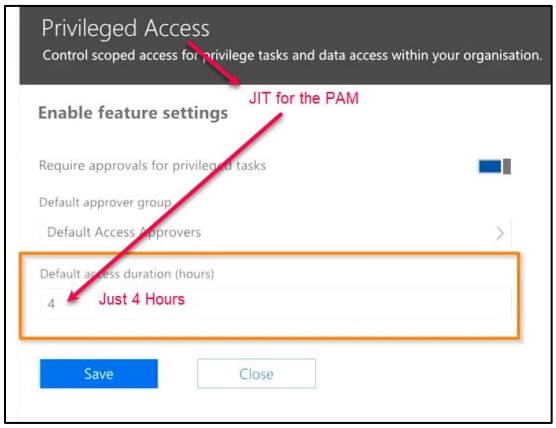


## 4.3.4. Describe privileged access management

Privileged access management allows granular access control over privileged admin tasks in Microsoft 365. It can help protect organizations from breaches that use existing privileged admin accounts with standing access to sensitive data, or access to critical configuration settings.

Enabling privileged access management in Microsoft 365 allows organizations to operate with zero standing access. This means that any user who needs privileged access must request permissions for access and will receive only the level of access they need just when they need it, and with just-enough access to do the job at hand. Zero standing access provides a layer of protection against standing administrative access vulnerabilities.

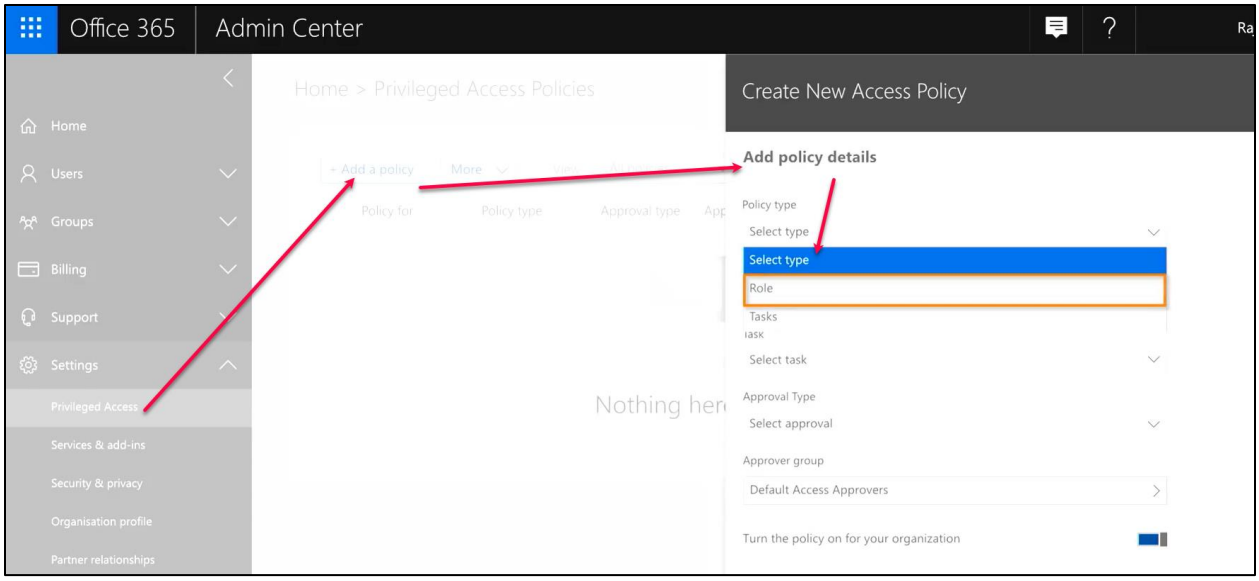


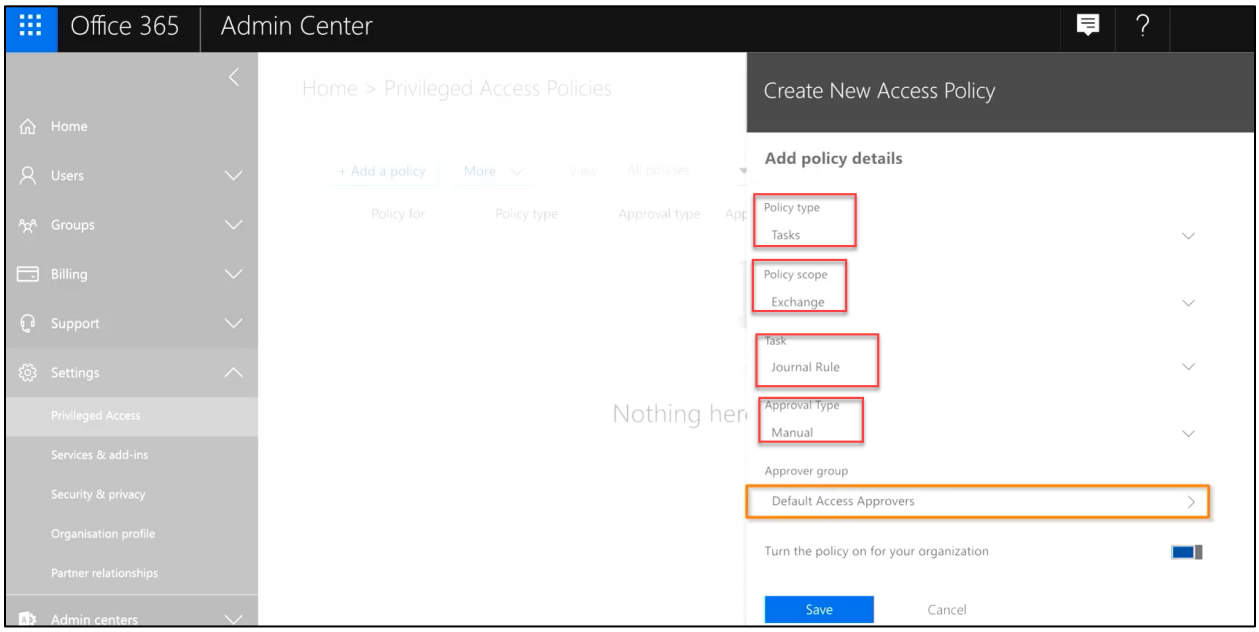



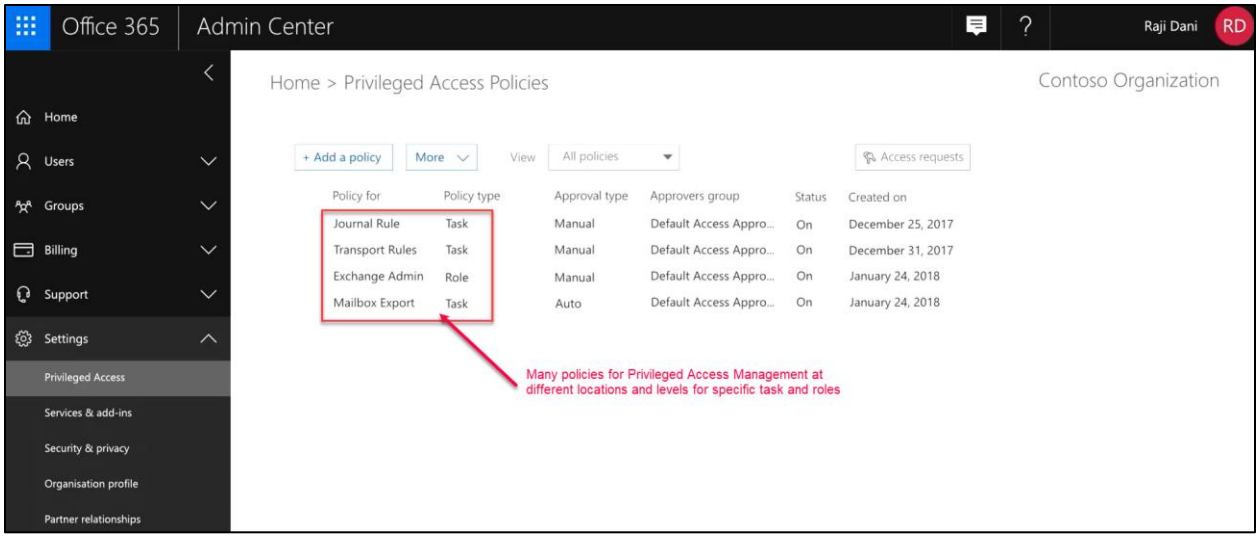

### 4.3.4.1. Time-bound approval workflow

#### 4.3.4.1.1. Configure a privileged access policy

Configure a privileged access policy - Configuring an approval policy allows the admin to define the specific approval requirements scoped at individual tasks.


Office 365
Admin Center
Home
Users
Groups
Billing
Support
Settings
Privileged Access
Services & add-ins
Security & privacy
Organisation profile
Partner relationships
Home > Privileged Access Policies
+ Add a policy
More
Create New Access Policy
Add policy details
Policy type
Select type
Select type
Role
Tasks
Select task
Approval Type
Select approval
Approver group
Default Access Approvers
Turn the policy on for your organization


Office 365
Admin Center
Home
Users
Groups
Billing
Support
Settings
Privileged Access
Services & add-ins
Security & privacy
Organisation profile
Partner relationships
Admin centers
Home > Privileged Access Policies
+ Add a policy
More
Create New Access Policy
Add policy details
Policy type
Tasks
Policy scope
Exchange
Task
Journal Rule
Approval Type
Manual
Approver group
Default Access Approvers
Turn the policy on for your organization
Save
Cancel



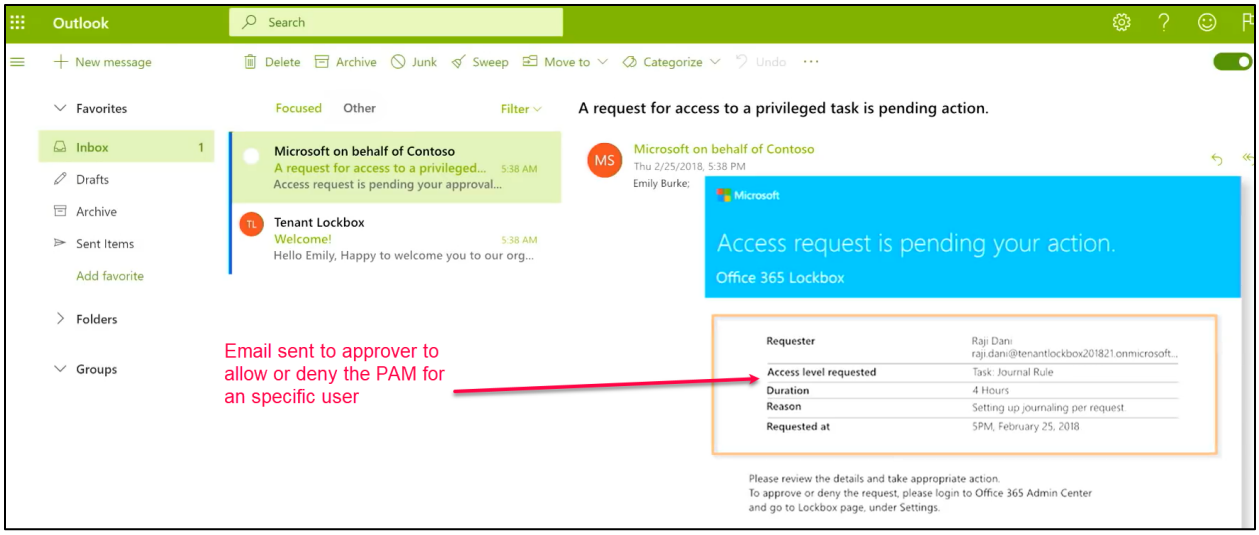

#### 4.3.4.1.2. Access request

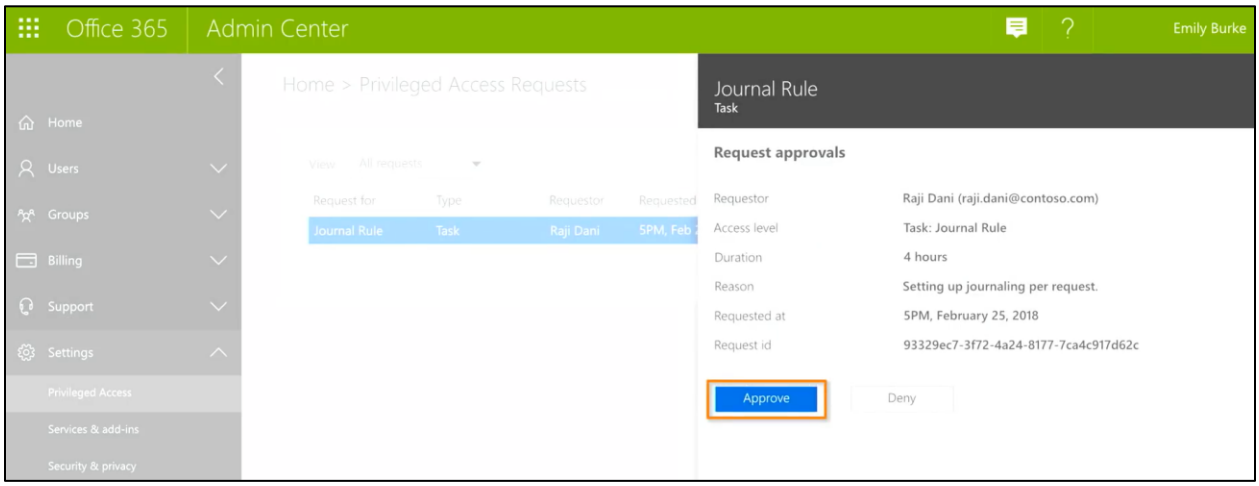
Access request - Users can request access to elevated or privileged tasks. The privileged access feature sends the request to Microsoft 365 for processing against the configured privilege access policy and records the activity in the Security and Compliance Center logs.

```
PS C:\Users\raji.dani> New-ElevatedAccessRequest -Task 'Exchange\New-JournalRule' -Reason 'Setting journaling
per request.' -DurationHours 4
```

#### 4.3.4.1.3. Access approval

Access approval - An approval request is generated, and the pending request notification is emailed to approvers. If approved, the privileged access request is processed as an approval and the task is ready to be completed. If denied, the task is blocked and no access is granted to the requestor. The requestor is notified of the request approval or denial via email message.

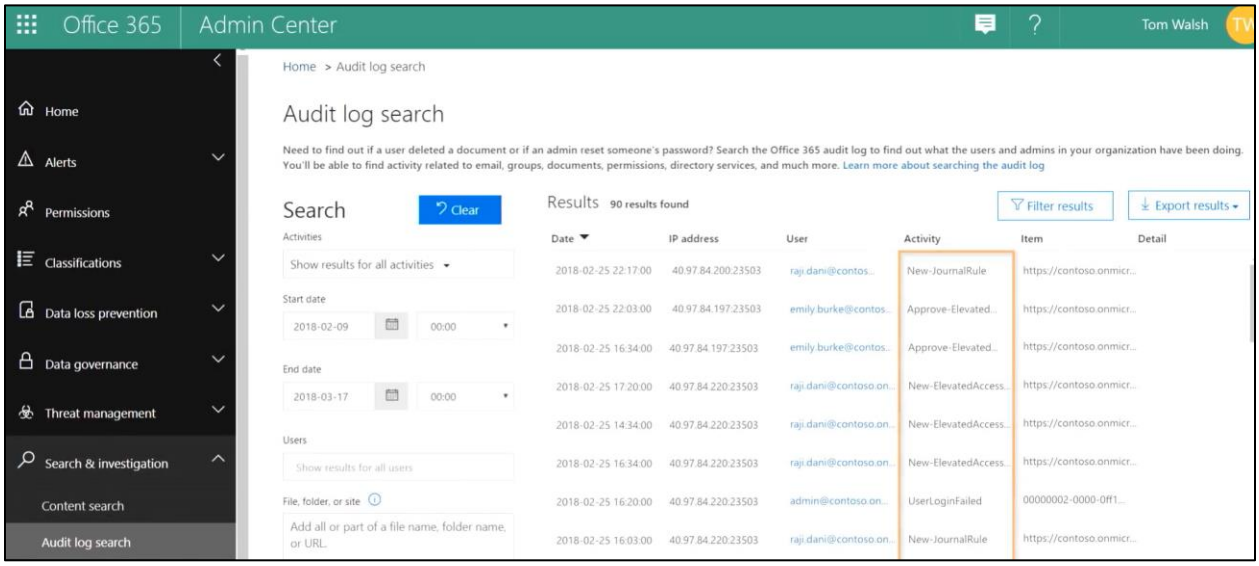



### 4.3.4.1.4. Access processing

Access processing - For an approved request, the task is processed. The approval is checked against the privileged access policy and processed by Microsoft. All activity for the task is logged in the Security and Compliance Center.

#### 4.3.4.1.5. Privileged Access Management Audit



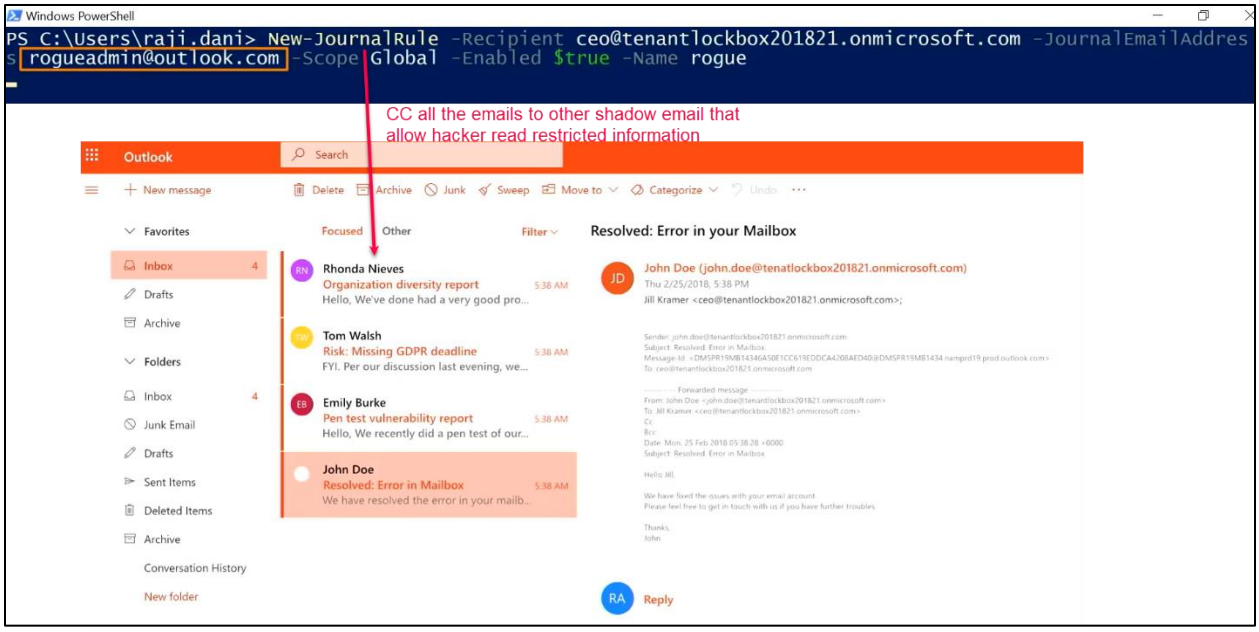

### 4.3.4.2. Privileged Access Management PAM Vs. Privileged Identity Management PIM

Privileged access management is defined and scoped at the task level, while Azure AD Privileged Identity Management applies protection at the role level with the ability to execute multiple tasks. Azure AD Privileged Identity Management primarily allows managing accesses for AD roles and role groups, while privileged access management in Microsoft 365 applies only at the task level.

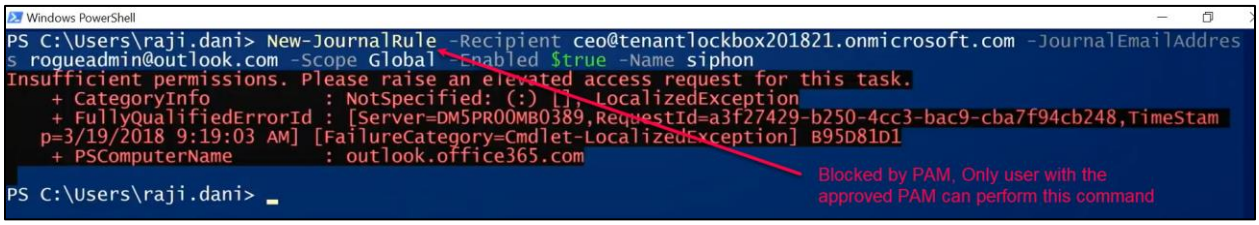
Control the use privileged admin accounts with standing access to sensitive data, so that admins receive only the level of access they need, when they need it.

### 4.3.4.3. Example of usage of Privileged Access Management (PAM)

Using the PS command New-JournalRule will copy all the email to a shadow email, It is possible to execute this command by a hacker and copy all the emails from CEO, CFO, Legal and HR to a shadow email to be monitored and access restricted information




With PAM:



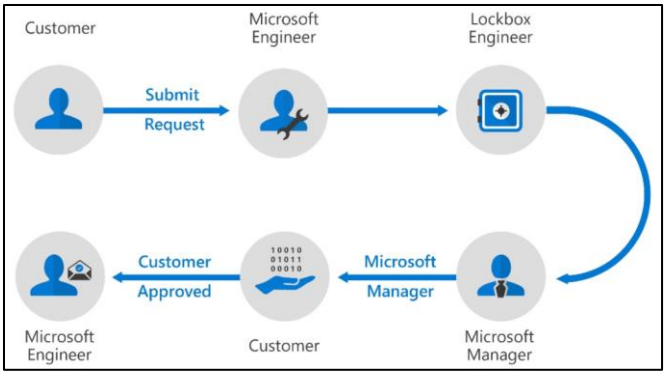

## 4.3.5. Describe Customer Lockbox

Occasionally, an organization might need Microsoft engineers help to help troubleshoot and fix reported issues. Usually, issues are fixed through extensive telemetry and debugging tools Microsoft has in place for its services. However, some cases require a Microsoft engineer to access the organization's content to determine the root cause and fix the issue.

Customer Lockbox ensures that Microsoft can't access the content to perform a service operation without explicit approval. Customer Lockbox brings the organization into the approval workflow for requests to access their content.

Customer Lockbox is used if a Microsoft engineer requires access the organization's content to determine the root cause and fix the issue. To protect the organization, the engineer shouldn't be able to access content and perform service operations without explicit approval.

Customer Lockbox supports requests to access data in Exchange Online, OneDrive for Business, and SharePoint Online. Here's what the process looks like:




1. Someone at an organization experiences an issue with their Microsoft 365 mailbox, for example. After the user troubleshoots the issue, but can't fix it, they open a support request with Microsoft Support.
2. A Microsoft support engineer reviews the service request and determines a need to access the organization's tenant to repair the issue in Exchange Online.
3. The Microsoft support engineer logs into the Customer Lockbox request tool and makes a data access request that includes the organization's tenant name, service request number, and the estimated time the engineer needs access to the data.
4. After a Microsoft Support manager approves the request, Customer Lockbox sends the designated approver at the organization an email notification about the pending access request from Microsoft.
5. The approver signs into the Microsoft 365 admin center and approves the request. This step also triggers the creation of an audit record available by searching the audit log. If the customer rejects the request or doesn't approve the request within 12 hours, the request expires, and no access is granted to the Microsoft engineer.
6. After the approver from the organization approves the request, the Microsoft engineer receives the approval message, logs into the tenant in Exchange Online, and fixes the customer's issue. Microsoft engineers have the requested duration to fix the issue after which the access is automatically revoked.

Because Customer Lockbox follows a formal approval for access control, a common question is how this capability relates to Privileged Access Management, described in the previous unit, that also requires approval for access control. Customer Lockbox allows a level of access control for organizations when Microsoft accesses data. Privileged access management allows granular access control within an organization for all Microsoft 365 privileged tasks.

## 4.3.6. Knowledge Check Insider Risk Capabilities

### 4.3.6.1. Question 1.

The compliance admin for the organization wants to explain the importance of insider risk management, to the business leaders? What use case would apply?

- To identify and protect against risks like an employee sharing confidential information.

- To identify and protect against malicious software across your network, such as ransomware.
- To identify and protect against devices shutting down at critical moments.

#### 4.3.6.2. Question 2.

To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need?

- Use Policy Compliance in Microsoft 365.
- Use Communication Compliance.
- Use information barriers.

#### 4.3.6.3. Question 3.

Your organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need?

- Use Communication Compliance.
- Use Customer Lockbox.
- Use information barriers.

#### 4.3.6.4. Question 4.

The compliance team wants to control the use privileged admin accounts with standing access to sensitive data, so that admins receive only the level of access they need, when they need it. How can this requirement be implemented?

- Use Communication Compliance.
- Use privileged access management.
- Use the Audit log.

#### 4.3.6.5. Question 5.

A customer has identified an issue that requires a Microsoft engineer to access the organization's content to determine the root cause and fix the issue. To protect the organization, the engineer shouldn't be able to access content and perform service operations without explicit approval. What capability can address this requirement?

- Use privileged access management
- Use information barriers
- Use Customer Lockbox

## 4.4. Describe the eDiscovery and Audit Capabilities of Microsoft 365

Organizations may need to identify, collect, and/or audit information for legal, regulatory, or business reasons. With today's volume and variety of data, it's vital that an organization can do this in an efficient and timely manner. Microsoft 365's eDiscovery and audit capabilities can help organizations to achieve this goal.

eDiscovery and audit can help organizations to identify, collect, and/or audit information in a rapid and effective manner to meet legal requirements.

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft 365 to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Advanced eDiscovery solution in Microsoft 365.

### 4.4.1. Purpose of eDiscovery

Sometimes a company may become involved in litigation and need to find electronic information to be used as evidence.

Temporally hold that exist during the course of investigation. It is used for specific cases.

It is reactive case to be used as evidence in a legal case.

Electronic discovery or eDiscovery tools can be used to search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams. You can search across mailboxes and sites in a single eDiscovery search by using the Content Search tool. And you can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the Advanced eDiscovery solution in Microsoft 365. Microsoft 365 provides the following eDiscovery tools:

- Content Search
- Core eDiscovery
- Advanced eDiscovery

## 4.4.2. eDiscovery Solutions

Microsoft 365 provides three eDiscovery solutions: Content search, Core eDiscovery, and Advanced eDiscovery.


### 4.4.2.1. Content search.

Use the Content search tool to search for content across Microsoft 365 data sources and then export the search results to a local computer.

The Content Search eDiscovery tool, accessible from the compliance center in Office 365 or Microsoft 365, enables search for in-place items such as email, documents, and instant messaging conversations in your organization. Search for items is supported in the following services:

- Exchange Online mailboxes and public folders
- SharePoint Online sites and OneDrive for Business accounts
- Skype for Business conversations
- Microsoft Teams
- Microsoft 365 Groups
- Yammer Groups

#### 4.4.2.1.1. Role required for Content Search

To have access to the content search page to run searches and preview and export results, an administrator, compliance officer, or eDiscovery manager must be a member of the eDiscovery Manager role group in the Security and Compliance Center.

#### 4.4.2.1.2. Run a Search

To start using the Content Search tool, you must choose content locations to search and configure a keyword query to find specific items. Or the user can just leave the query blank and return all items in the target locations. Examples of some of the capabilities for running a search include:

- **Build search queries and use conditions** to narrow your search.
- **Configure search permissions filtering** so that an eDiscovery manager can only search for a subset of mailboxes or sites in your organization.

- **Run an ID list search** to search for specific mailbox email messages and other mailbox items using a list of Exchange IDs.
- **Search for Teams chat data** across on-premises users.
- **View keyword statistics** for the results of a search and then refine the query if necessary.
- **Search for third-party data** that your organization has imported to Microsoft 365.
- **Preserve Bcc recipients** to follow regulatory compliance and eDiscovery requirements that may require organizations to preserve mailbox content, including the ability to search for and reproduce details about all recipients of a message, not just those on the "to" and "cc" list.

#### 4.4.2.1.3. Complete Actions on Content

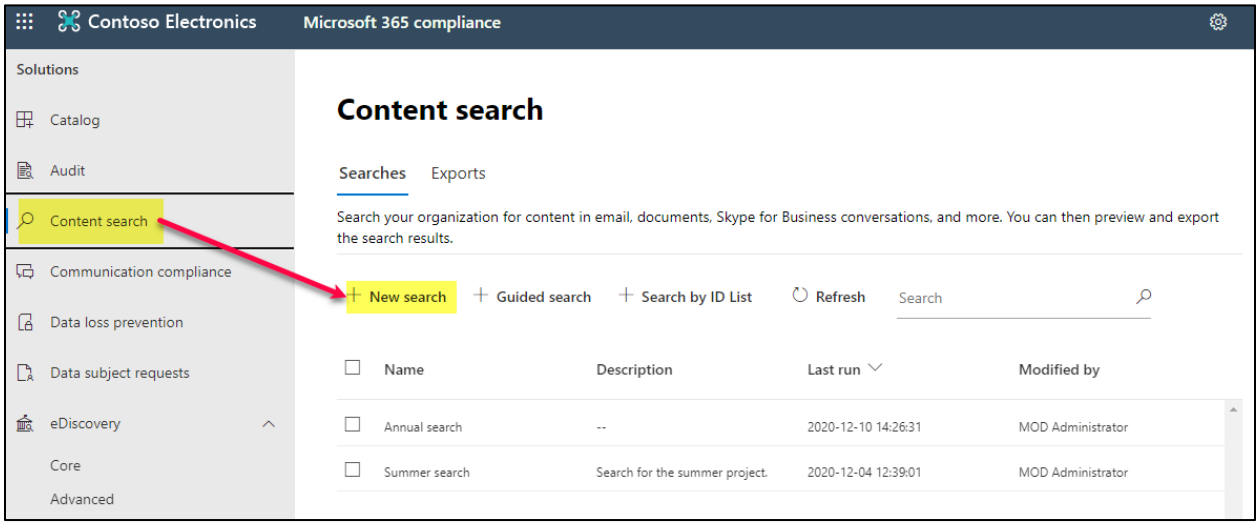
After you run a search and refine it as necessary, the next step is to do something with the results returned by the search. You can export and download the results to your local computer or, if there is an email-based attack, you can delete the results of a search from user mailboxes. You can also use scripts for advanced scenarios. Sometimes you have to do more advanced, complex, and repetitive content search tasks. To help make this easier, Microsoft has created a number of Security and Compliance Center PowerShell scripts to help complete complex content search-related tasks.

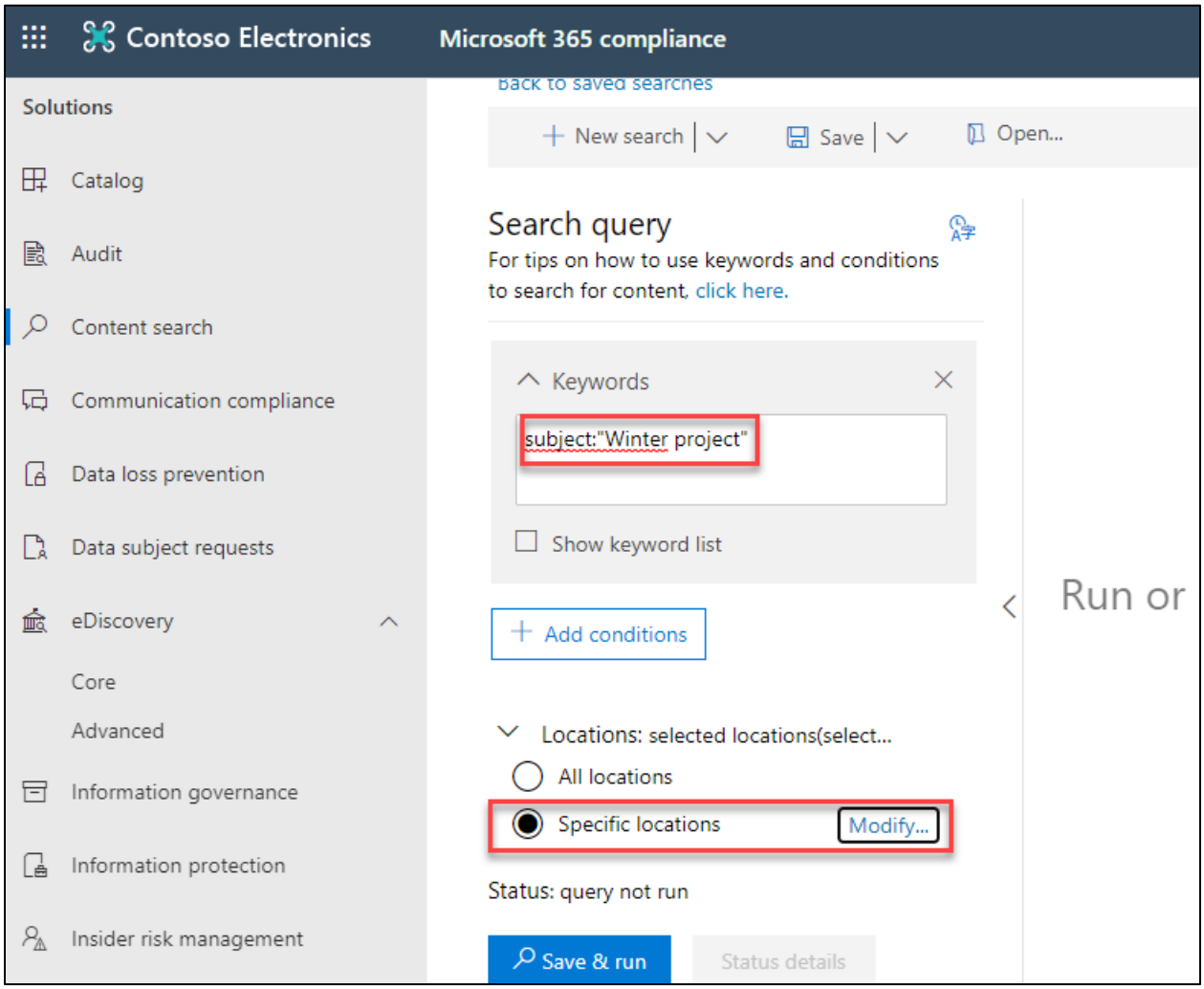
Content Search is easy to use, but it's also a powerful tool.

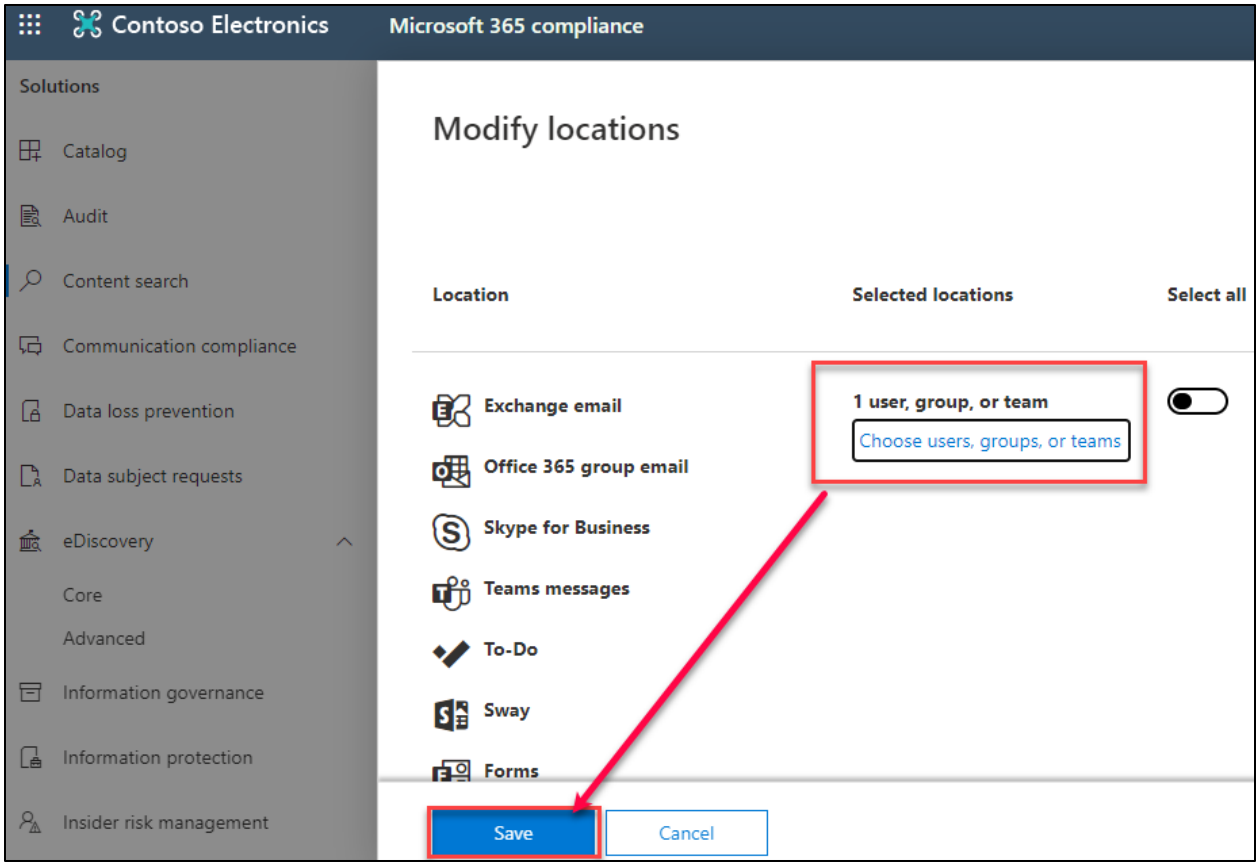
Some of these scripts include:

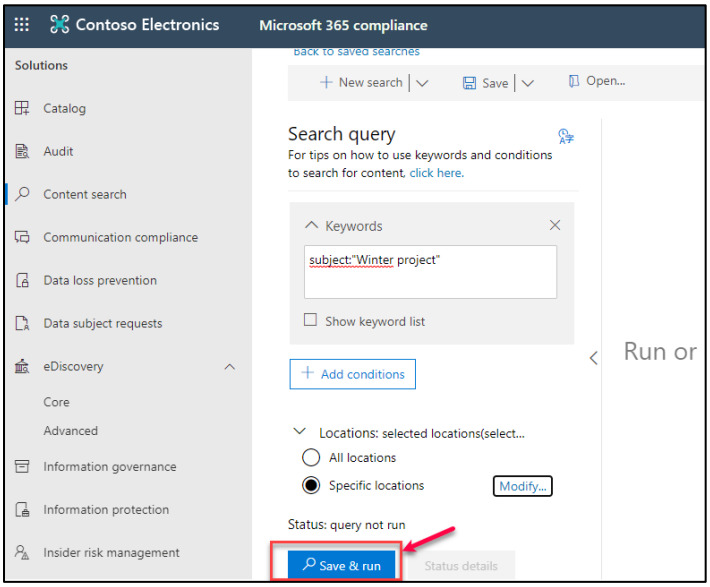
- Search-specific mailbox and site folders (called a targeted collection) when you're confident that items responsive to a case are located in that folder.
- Search the mailbox and OneDrive location for a list of users.
- Create, report on, and delete multiple searches to quickly and efficiently identify, and cull search data.
- Clone a content search and quickly compare the results of different keyword search queries run on the same content locations; or use the script to save time by not having to reenter a large number of content locations when you create a new search.

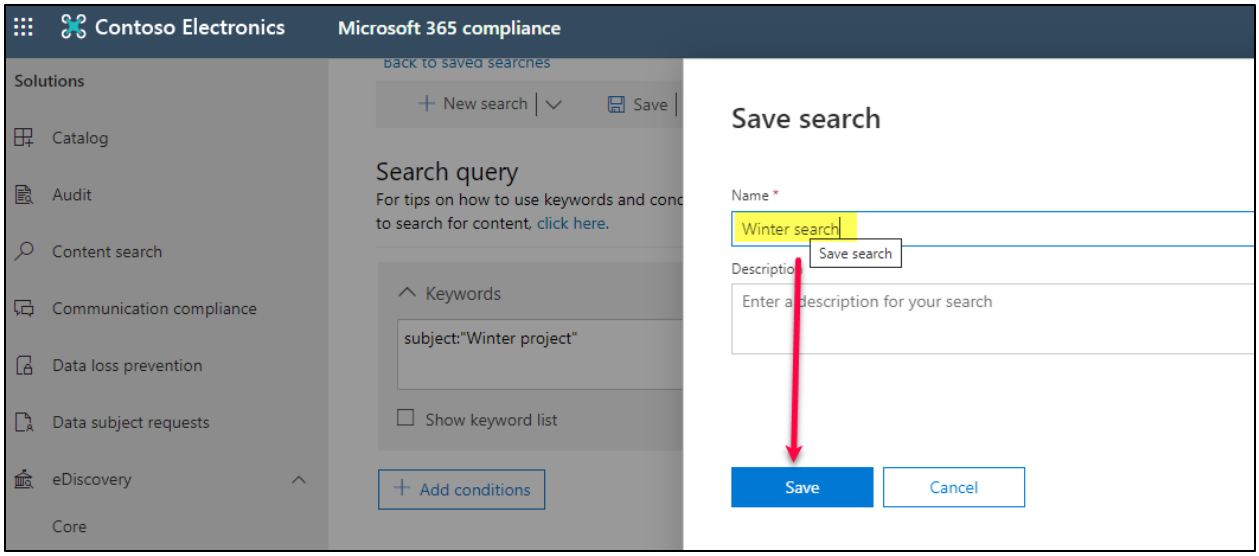
### 4.4.2.1.4. How to Search Content from an eDiscovery Hold

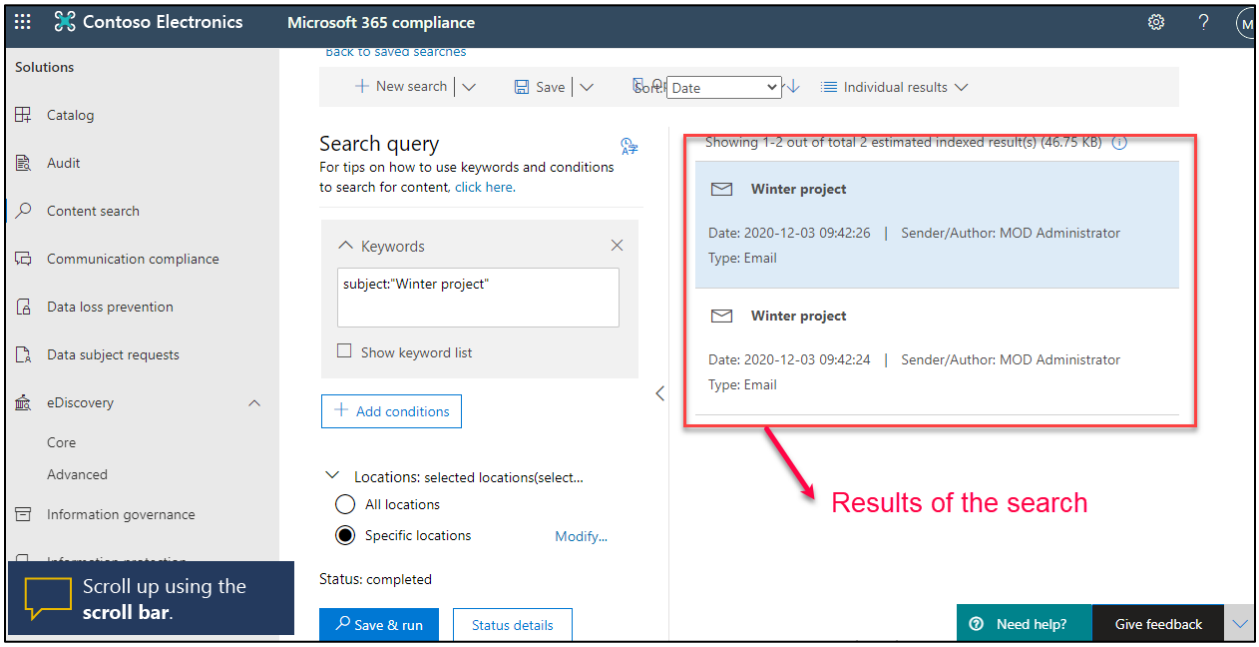


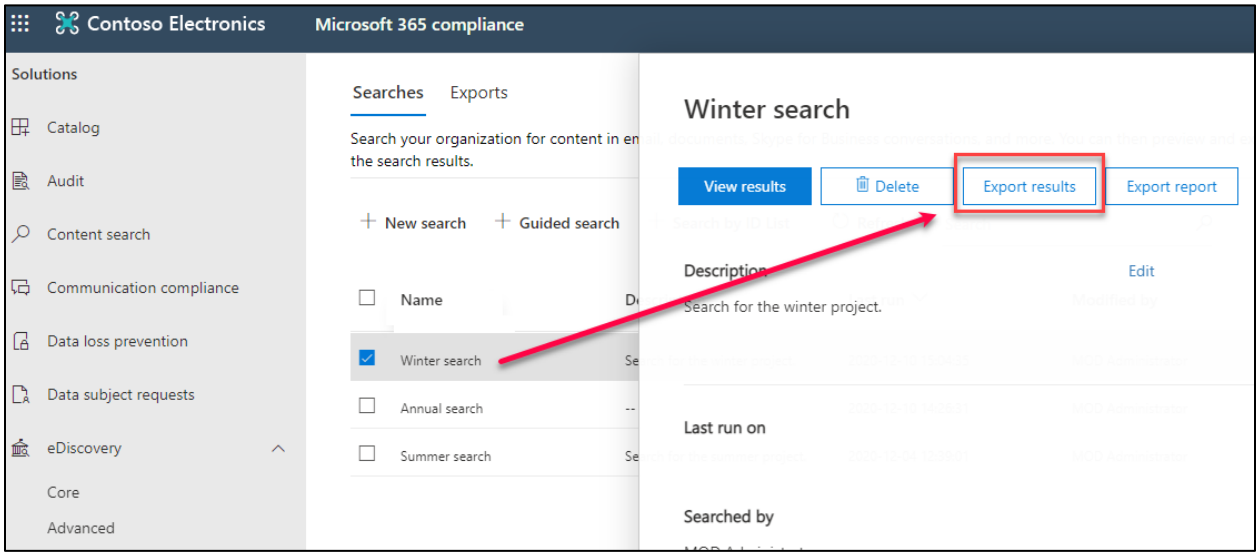

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
Information protection
Insider risk management
Modify locations
Location
Selected locations
Select all
Exchange email
Office 365 group email
Skype for Business
Teams messages
To-Do
Sway
Forms
1 user, group, or team
Choose users, groups, or teams
Save
Cancel

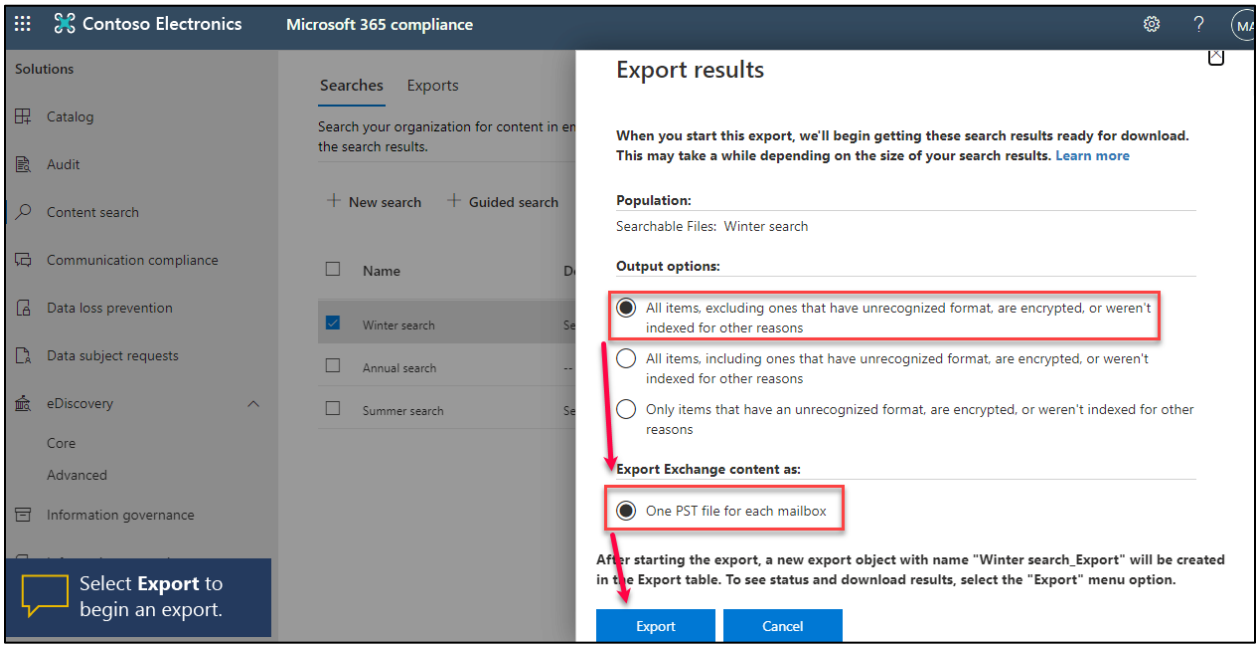

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
Information protection
Insider risk management
New search
Save
Open...
Search query
For tips on how to use keywords and conditions to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Locations: selected locations(select...
All locations
Specific locations
Modify...
Status: query not run
Save & run
Status details
Run or

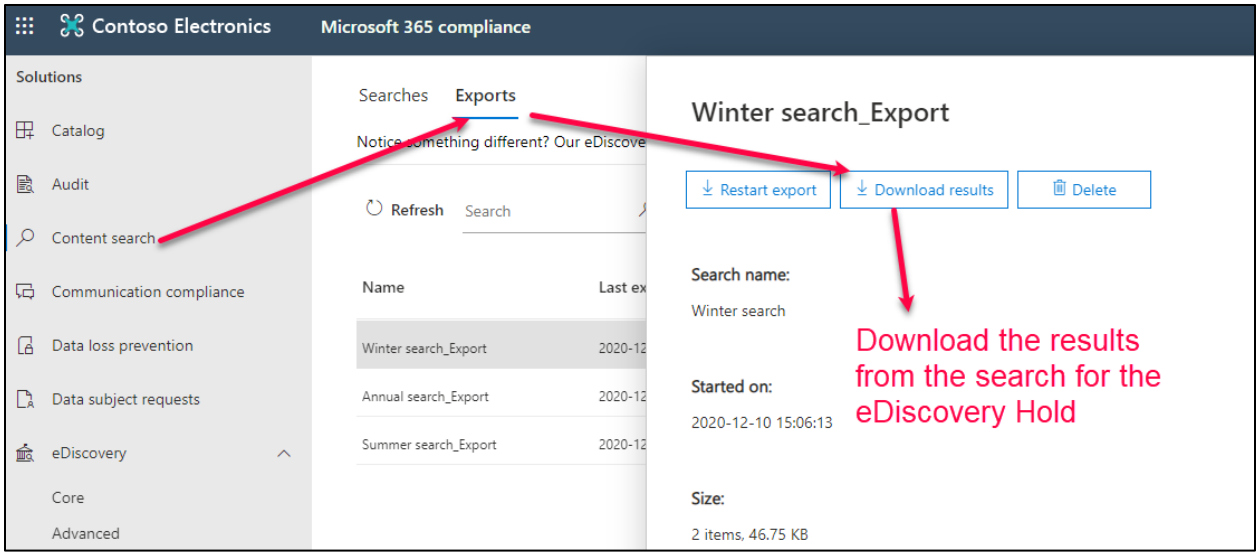

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
New search
Save
Search query
For tips on how to use keywords and conc
to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Save search
Name *
Winter search
Save search
Description
Enter a description for your search
Save
Cancel


Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
New search
Save
Sort: Date
Individual results
Search query
For tips on how to use keywords and conditions
to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Locations: selected locations(select...
All locations
Specific locations
Modify...
Status: completed
Save & run
Status details
Showing 1-2 out of total 2 estimated indexed result(s) (46.75 KB)
Winter project
Date: 2020-12-03 09:42:26 | Sender/Author: MOD Administrator
Type: Email
Winter project
Date: 2020-12-03 09:42:24 | Sender/Author: MOD Administrator
Type: Email
Results of the search
Scroll up using the scroll bar.
Need help?
Give feedback

## 4.4.2.1.5. How to Export the Search Results






### 4.4.2.2. Core eDiscovery.

Core eDiscovery builds on the basic search and export functionality of Content search by enabling you to create eDiscovery cases and assign eDiscovery managers to specific cases. eDiscovery managers can only access the cases of which they are members. Core eDiscovery also lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.

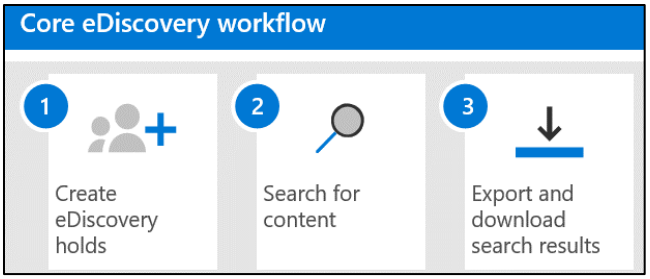
Core eDiscovery in Microsoft 365 provides a basic tool that organizations can use to search and export content in Microsoft 365.

You start by creating an eDiscovery case, which starts from within Microsoft 365 compliance center. When you create a case, you must specify a name for it and optionally define a case number. You can assign members to the case. From that point, the case will be displayed in the eDiscovery page and the user can step through the workflow.

The workflow consists of creating holds, searching for content, and exporting and downloading search results.

#### 4.4.2.2.1. Role required for Core eDiscovery

To access Core eDiscovery or be added as a member of a Core eDiscovery case, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the eDiscovery Manager role group in the Office 365 Security and Compliance Center.




#### 4.4.2.2.2. Create an eDiscovery Hold

You can use an eDiscovery case to create a hold to preserve content that might be relevant to the case. You can place a hold on the Exchange mailboxes and OneDrive for Business accounts of people you're investigating in the case. You can also place a hold on the mailboxes and sites that are associated with Microsoft Teams, Office 365 Groups, and Yammer Groups. When you place content locations on hold, it's preserved until you remove the hold from the content location, or until you delete the hold.

It may take up to 24 hours after you create the hold for it to take effect.

You have two options to scope the content that's preserved:

- You create an infinite hold where all content in the specified locations is placed on hold. Or you can create a query-based hold where only the content in the specified locations that matches a search query is placed on hold.
- You can specify a date range to preserve only the content that was sent, received, or created within that date range. Or you can hold all content in specified locations regardless of when it was sent, received, or created.

#### 4.4.2.2.3. Search for content in the case

When you've placed a hold, you can create and run searches for content that relates to the case. You start the search from within the home page for that specific case. Searches associated with a case can only be accessed by members assigned to it.

You can specify keywords, message properties such as sent and received dates, or document properties such as file names, or the date a document was last changed. You can use Boolean operators such as AND, OR, NOT, or NEAR. You can also search for sensitive information (for example, social security numbers) in documents, or search for documents that have been shared externally. If you don't specify keywords, all content located in the specified content locations will be included in the search results.

#### 4.4.2.2.4. Export content from a case

You can export search results. Mailbox items are downloaded in a PST file or as individual messages. Content from SharePoint, OneDrive for Business sites, copies of native Office documents, and other documents are exported. A Results.csv file that contains information about every item that's exported and a manifest file (in XML format) that contains information about every search result is also exported.

You can export the results of both a single search or results from multiple searches associated with a case.

#### 4.4.2.2.5. Close, reopen, and delete a core eDiscovery case

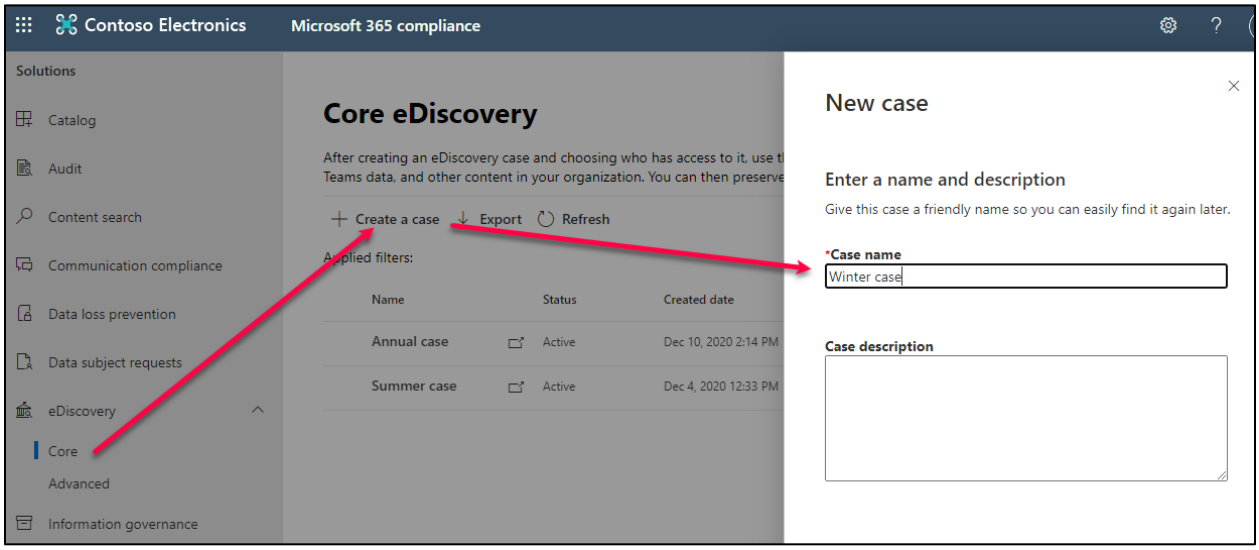
Core eDiscovery cases can be closed when the investigations or legal cases they were supporting have been completed. When a case is closed, any holds associated with it will be turned off. Once turned off, there's a 30-day grace period (referred to as a delay hold) on the content locations that were on hold. This helps ensure that content isn't deleted immediately and gives admins the chance to look for and restore any content before it's deleted permanently.

The main difference between an active and closed case is that eDiscovery holds are turned off for a closed case. When you reopen a closed case, any holds that were in place when it was closed, won't be reinstated automatically. After reopening the case, you'll need to turn on previous holds. A reopened case will have its status changed from closed to active.

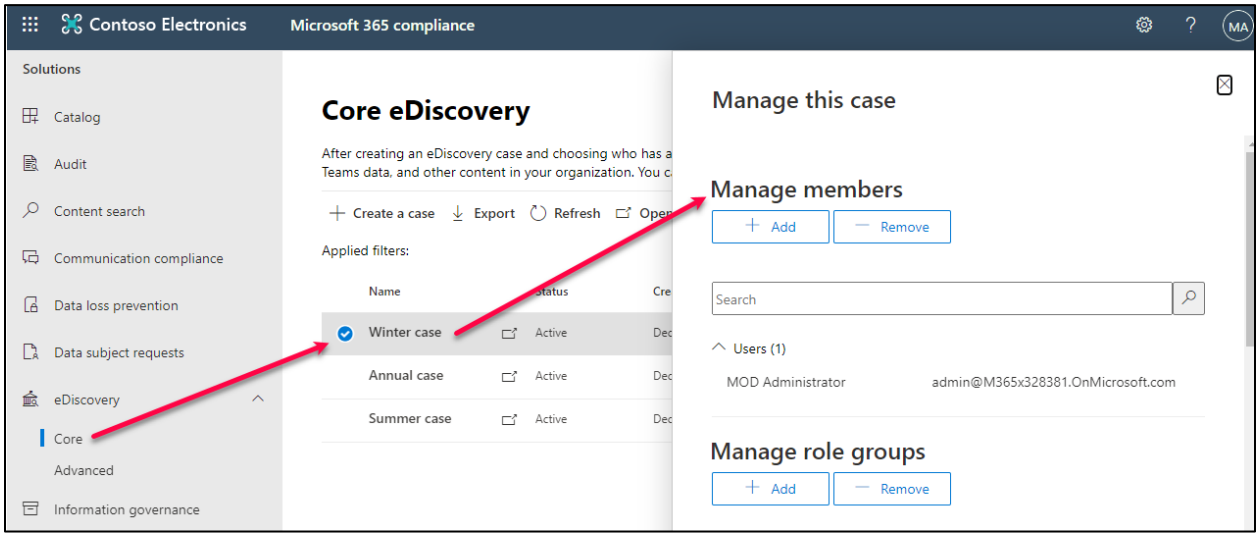
You can delete both active and closed cases. If you delete a case, all searches and exports in that case are also deleted, the case is removed from the list in the Microsoft 365 compliance center. The deleted case can't be reopened.

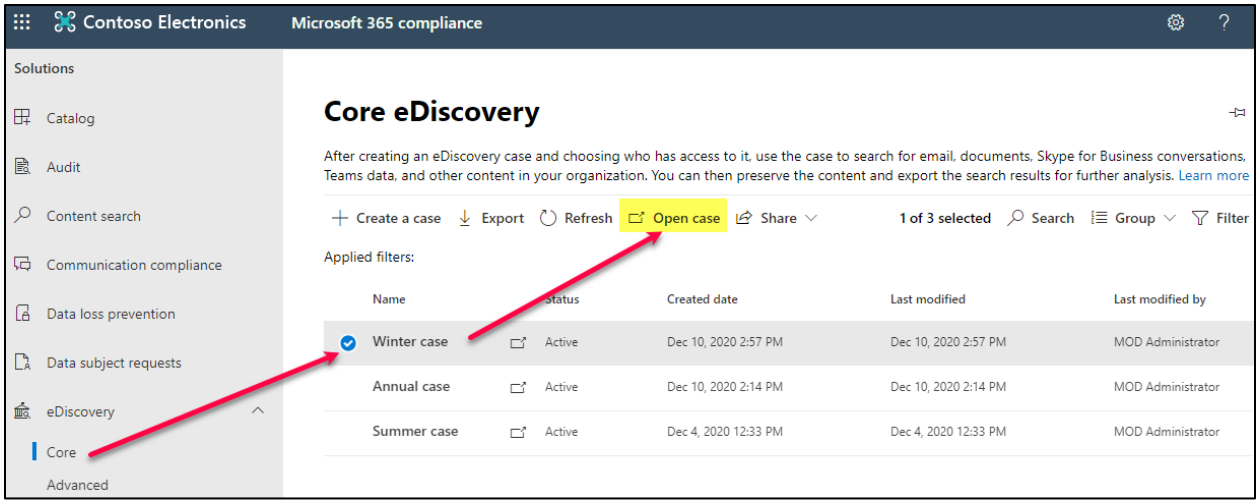
If the case you want to delete contains eDiscovery holds, you can't delete it. You'll need to delete all the holds linked to the case then try to delete it again.

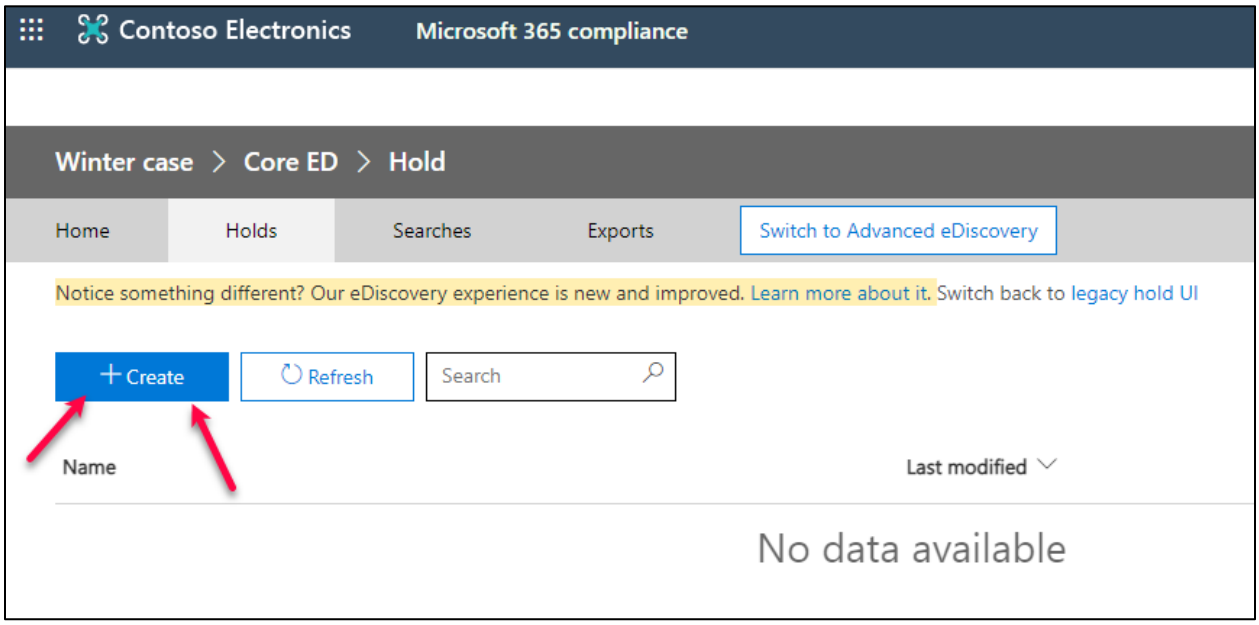
### 4.4.2.2.6. How to Create a Case

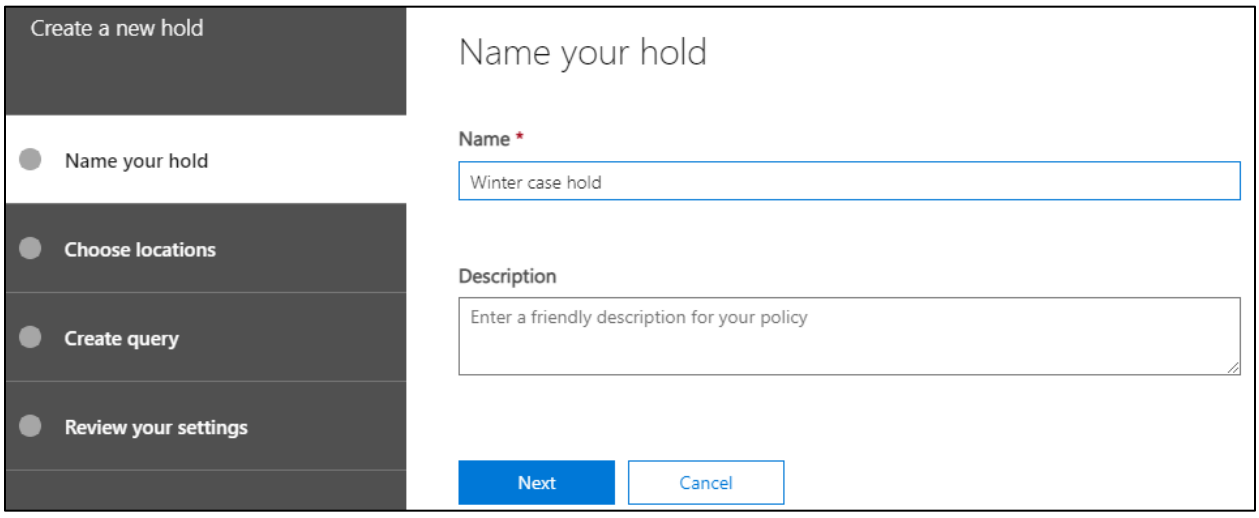


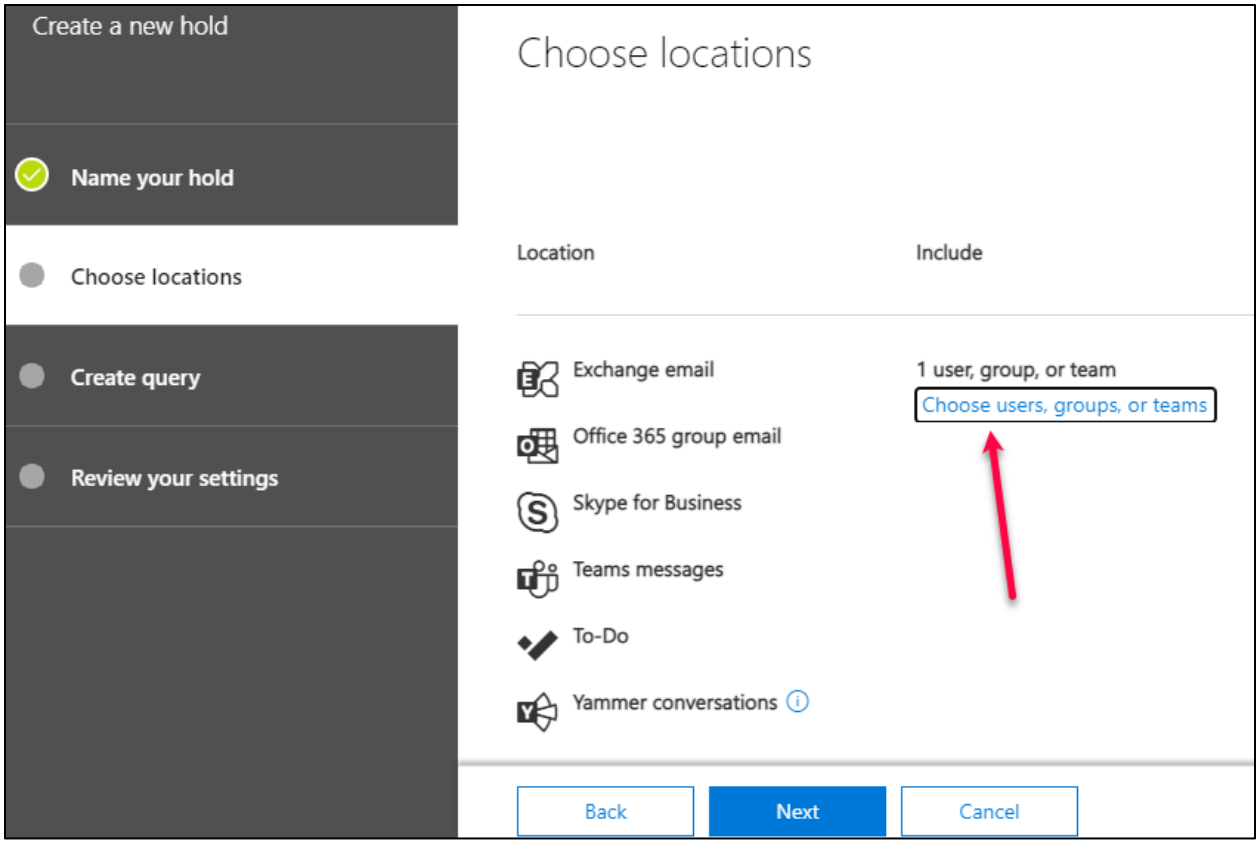

### 4.4.2.2.7. How to Create an eDiscovery Hold

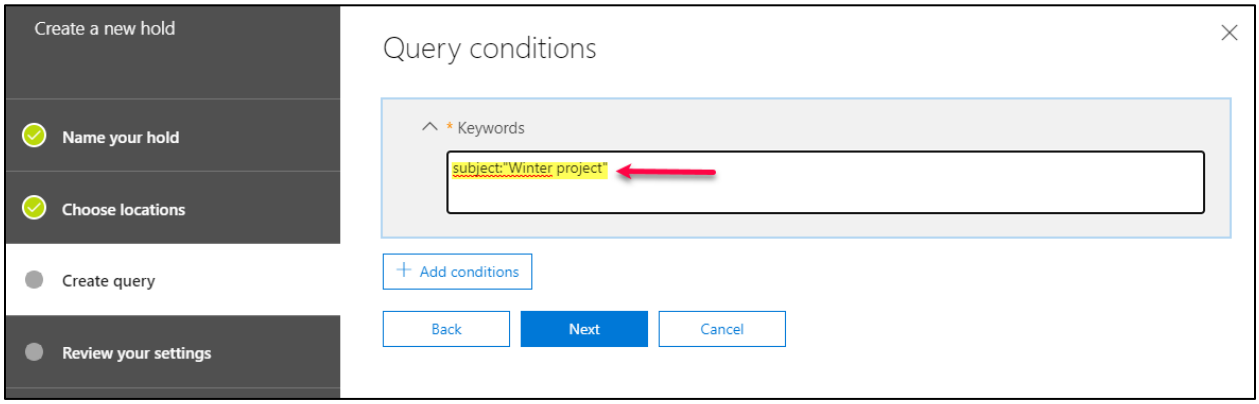


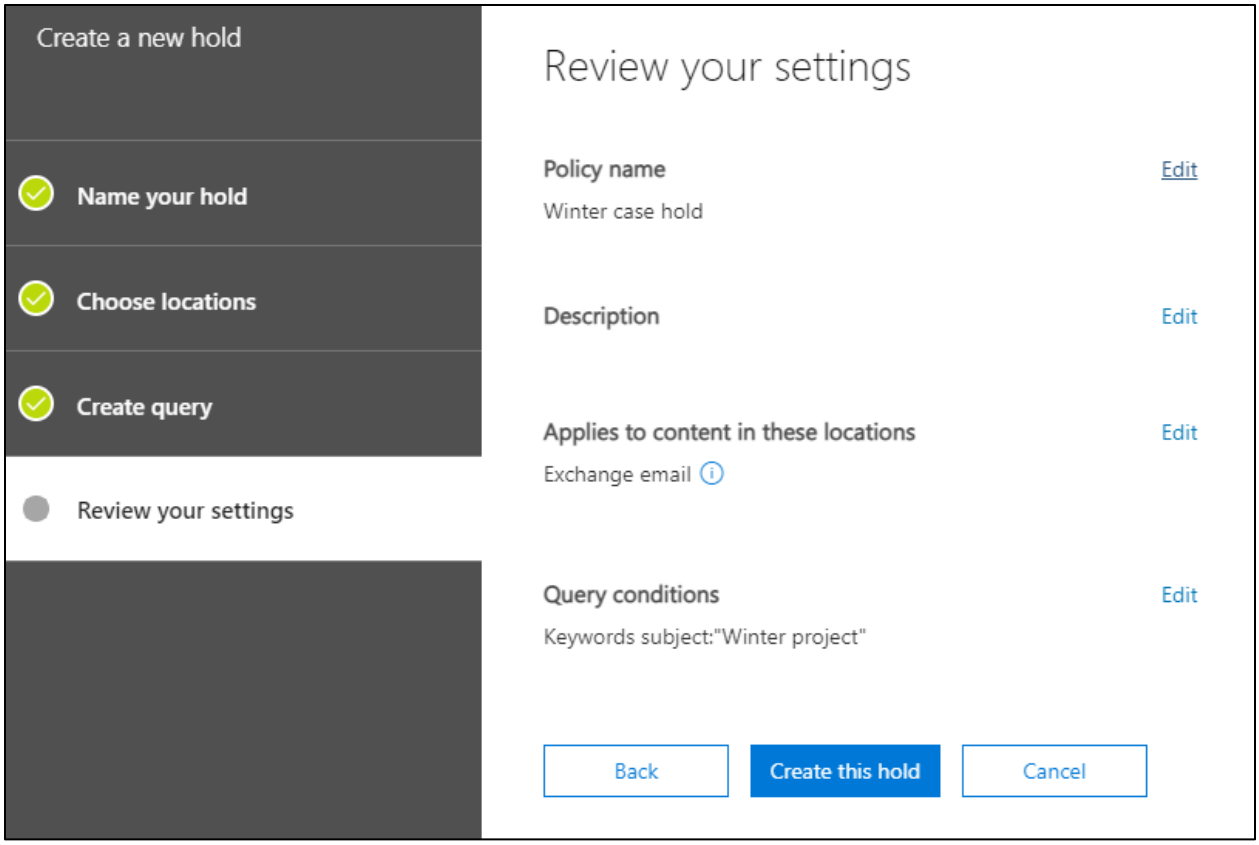

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Core eDiscovery
After creating an eDiscovery case and choosing who has access to it, use the case to search for email, documents, Skype for Business conversations, Teams data, and other content in your organization. You can then preserve the content and export the search results for further analysis. Learn more
Create a case
Export
Refresh
Open case
Share
1 of 3 selected
Search
Group
Filter
Applied filters:
Name
Status
Created date
Last modified
Last modified by
Winter case
Active
Dec 10, 2020 2:57 PM
Dec 10, 2020 2:57 PM
MOD Administrator
Annual case
Active
Dec 10, 2020 2:14 PM
Dec 10, 2020 2:14 PM
MOD Administrator
Summer case
Active
Dec 4, 2020 12:33 PM
Dec 4, 2020 12:33 PM
MOD Administrator


Contoso Electronics
Microsoft 365 compliance
Winter case > Core ED > Hold
Home
Holds
Searches
Exports
Switch to Advanced eDiscovery
Notice something different? Our eDiscovery experience is new and improved. Learn more about it. Switch back to legacy hold UI
Create
Refresh
Search
Name
Last modified
No data available

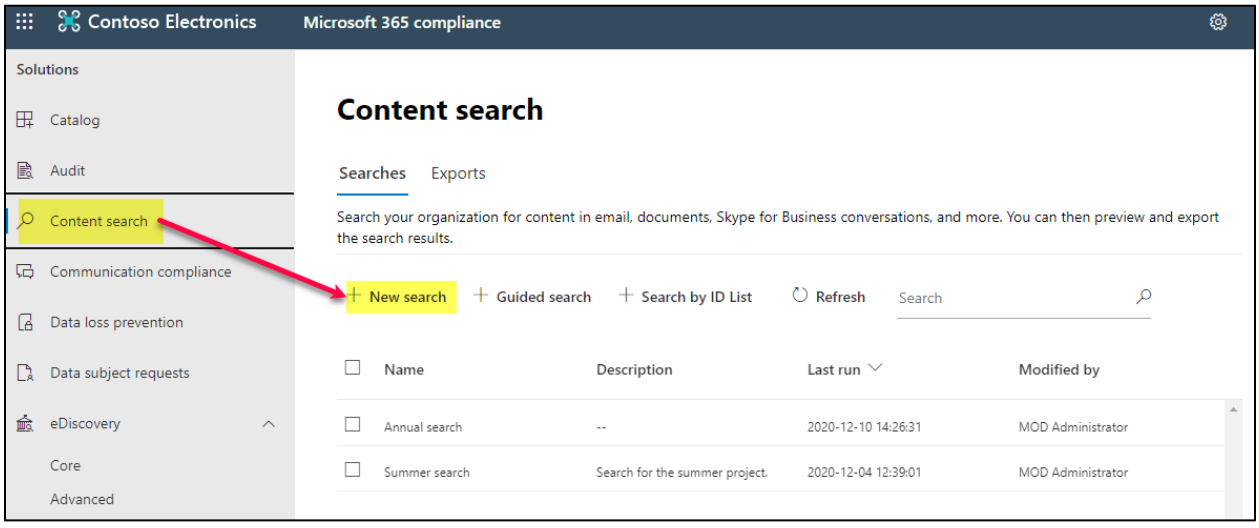

Create a new hold
Name your hold
Choose locations
Create query
Review your settings
Name your hold
Name *
Winter case hold
Description
Enter a friendly description for your policy
Next
Cancel

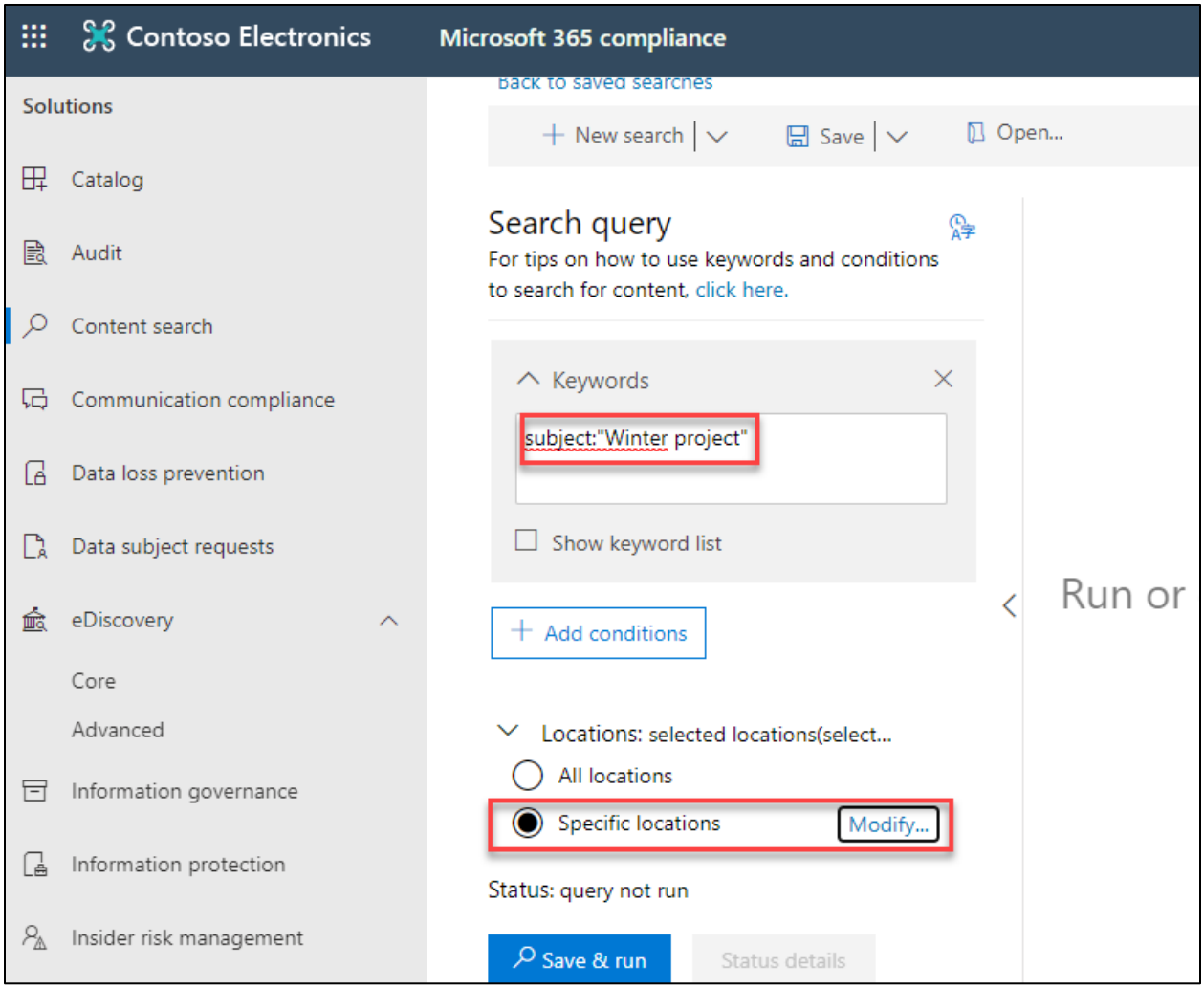

Create a new hold
Name your hold
Choose locations
Create query
Review your settings
Choose locations
Location
Include
Exchange email
1 user, group, or team
Choose users, groups, or teams
Office 365 group email
Skype for Business
Teams messages
To-Do
Yammer conversations
Back
Next
Cancel

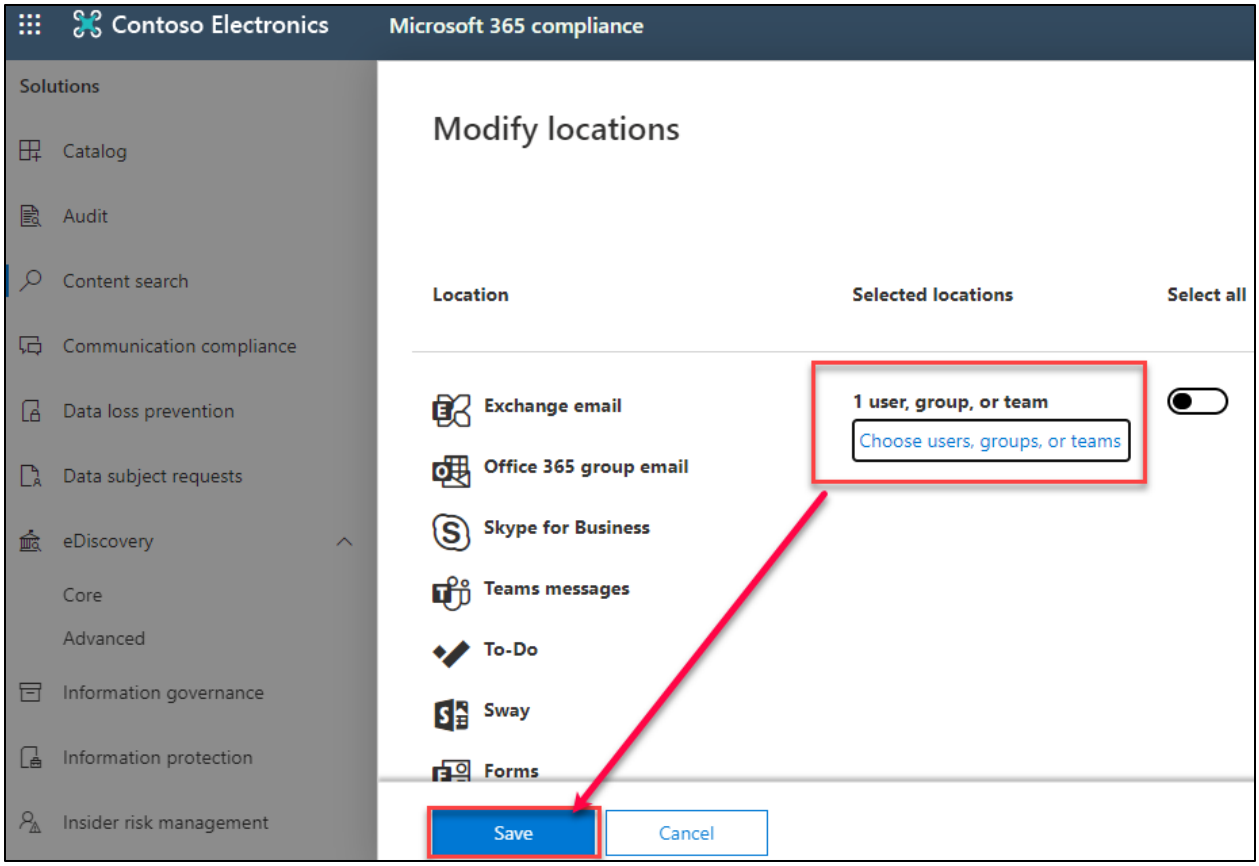

Create a new hold
Name your hold
Choose locations
Create query
Review your settings
Query conditions
* Keywords
subject:"Winter project"
Add conditions
Back
Next
Cancel

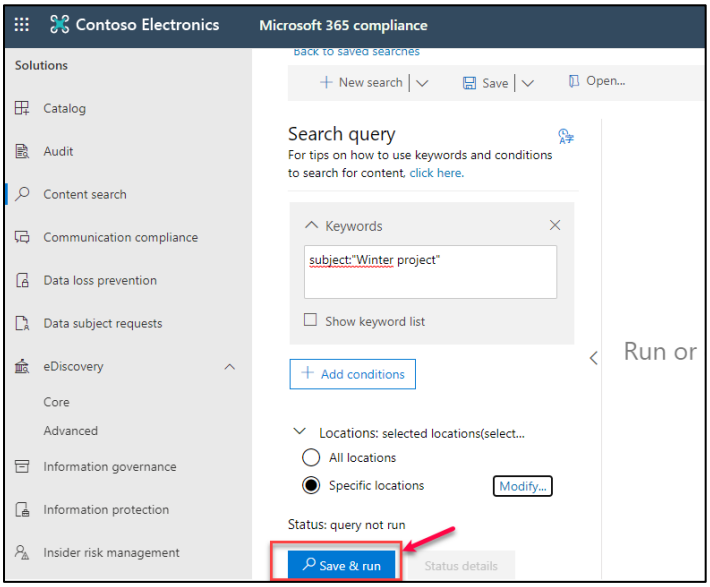


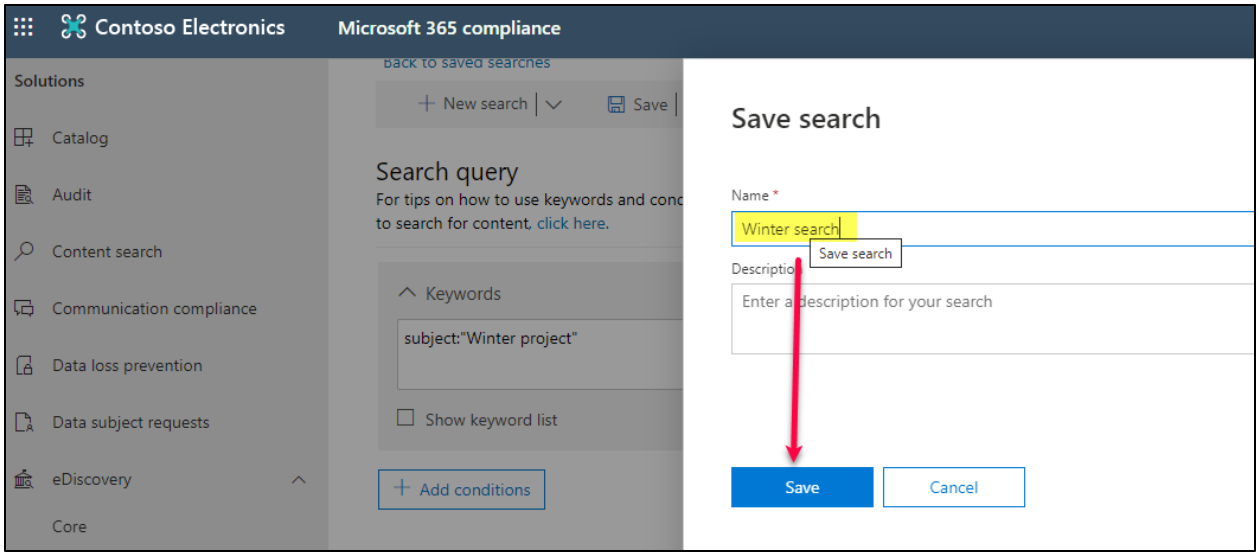

## 4.4.2.2.8. How to Search Content from an eDiscovery Hold

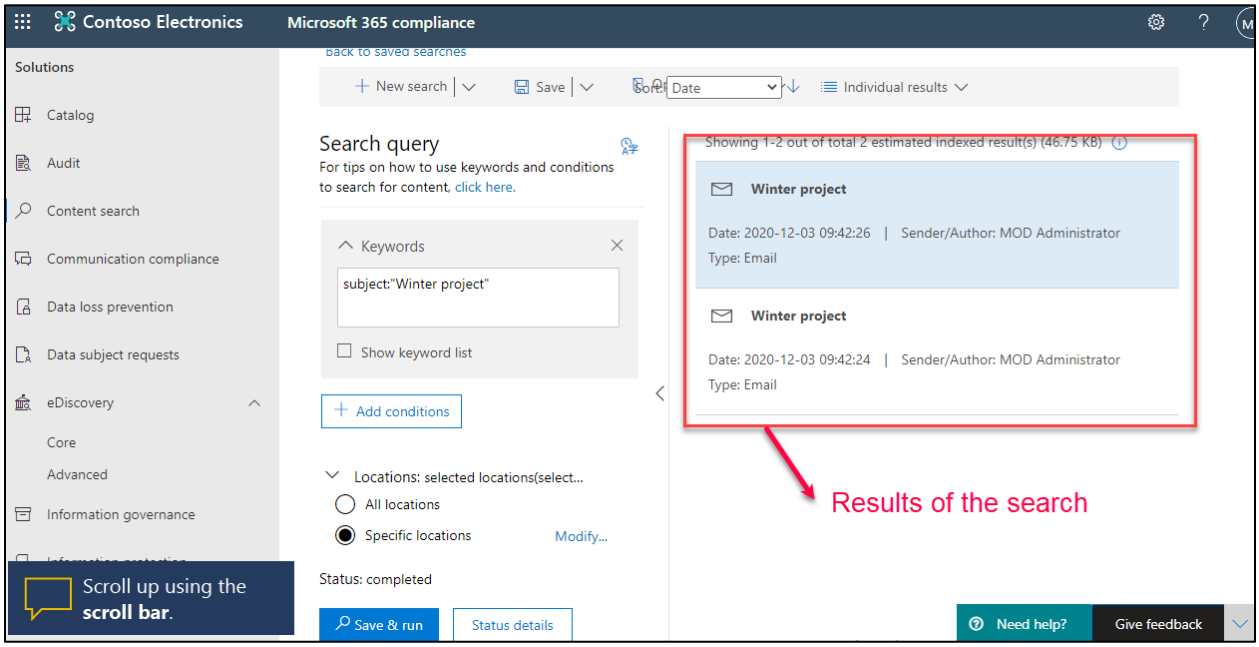



Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
Information protection
Insider risk management
Back to saved searches
New search
Save
Open...
Search query
For tips on how to use keywords and conditions to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Locations: selected locations(select...
All locations
Specific locations
Modify...
Status: query not run
Save & run
Status details
Run or

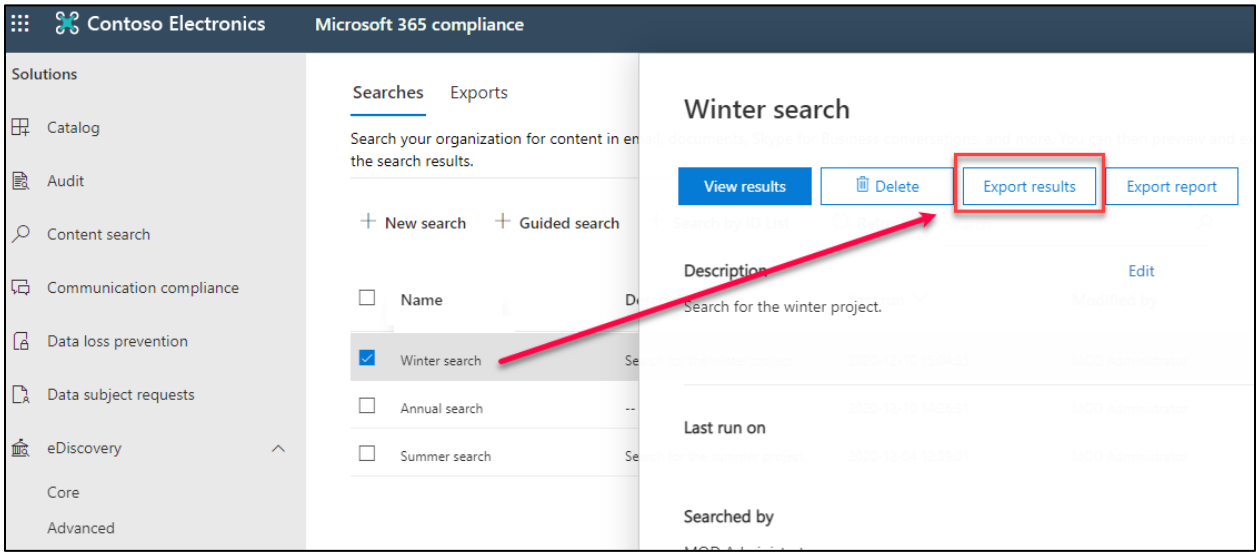

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
Information protection
Insider risk management
Modify locations
Location
Selected locations
Select all
Exchange email
Office 365 group email
Skype for Business
Teams messages
To-Do
Sway
Forms
1 user, group, or team
Choose users, groups, or teams
Save
Cancel

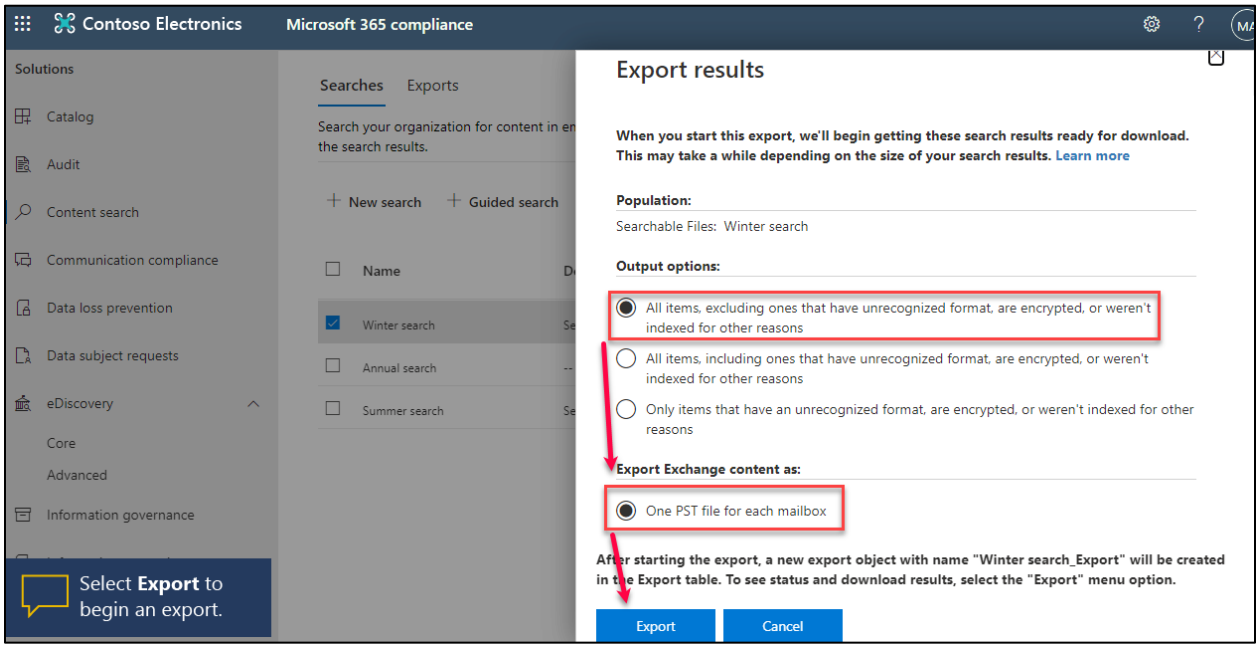

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
Information protection
Insider risk management
New search
Save
Open...
Search query
For tips on how to use keywords and conditions to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Locations: selected locations(select...
All locations
Specific locations
Modify...
Status: query not run
Save & run
Status details
Run or

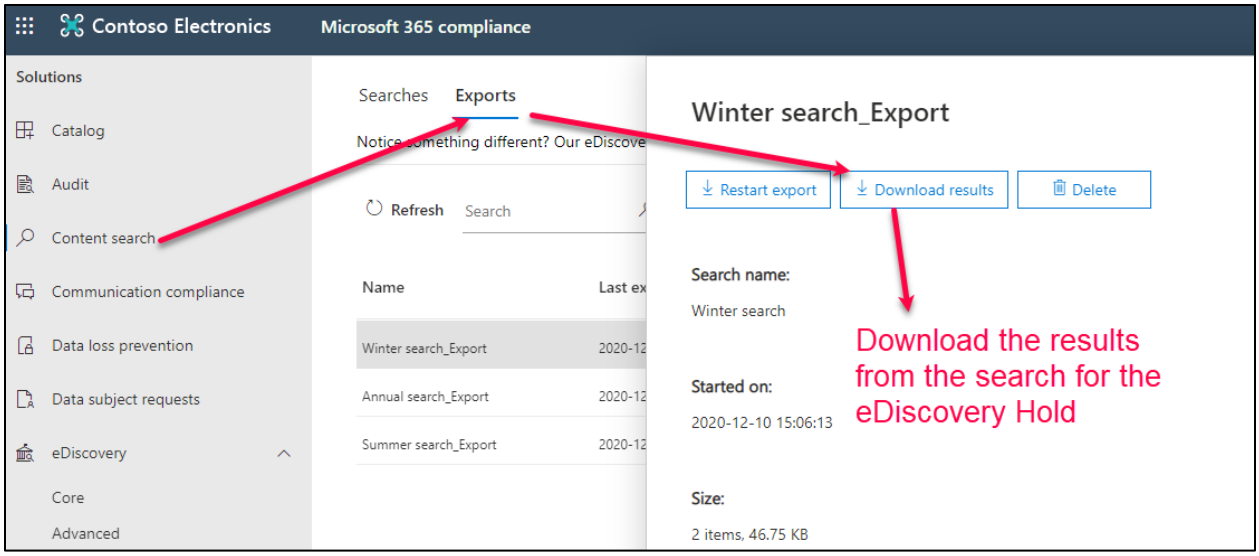

Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
New search
Save
Search query
For tips on how to use keywords and conc
to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Save search
Name *
Winter search
Save search
Description
Enter a description for your search
Save
Cancel


Contoso Electronics
Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Core
Advanced
Information governance
New search
Save
Sort: Date
Individual results
Search query
For tips on how to use keywords and conditions
to search for content, click here.
Keywords
subject:"Winter project"
Show keyword list
Add conditions
Locations: selected locations(select...
All locations
Specific locations
Modify...
Status: completed
Save & run
Status details
Showing 1-2 out of total 2 estimated indexed result(s) (46.75 KB)
Winter project
Date: 2020-12-03 09:42:26 | Sender/Author: MOD Administrator
Type: Email
Winter project
Date: 2020-12-03 09:42:24 | Sender/Author: MOD Administrator
Type: Email
Results of the search
Scroll up using the scroll bar.
Need help?
Give feedback

## 4.4.2.2.9. How to Export the Search Results






### 4.4.2.3. Advanced eDiscovery.

Use Advanced eDiscovery in Microsoft 365 to preserve, collect, review, analyze, and export data that's relevant to your organization's internal and external investigations.

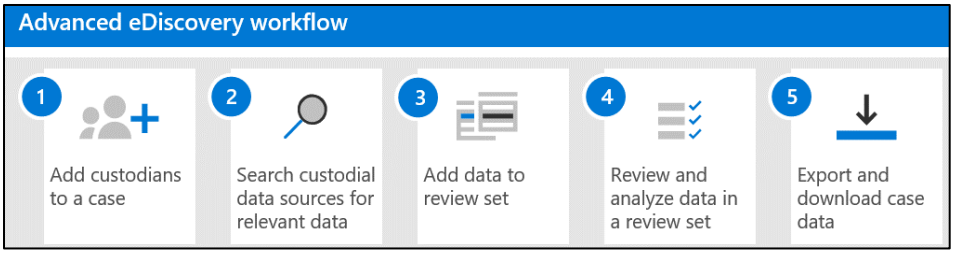
The Advanced eDiscovery tool builds on the existing case management, preservation, search, and export capabilities in Core eDiscovery. Advanced eDiscovery provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations.

It lets legal teams manage custodians and the legal hold notification workflow to communicate with custodians involved in a case.

It allows you to collect and copy data from the live service into review sets, when you can filter, search, and tag content to cull non-relevant content from further review so your workflow can identify and focus on content that's most relevant. Advanced eDiscovery provides analytics and machine learning-based predictive coding models to further narrow to scope of your investigation to the most relevant content.

The Advanced eDiscovery solution in Microsoft 365 builds on the existing core eDiscovery. This new solution provides an 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 described below aligns with the Electronic Discovery Reference Model (EDRM), a framework that outlines standards for recovery and discovery of digital data.




#### 4.4.2.3.1. Add custodians to a case

Add custodians to a case. This is the first step after creating a case. Custodians are people who have administrative control of a document or electronic file that could be relevant to the case.

#### 4.4.2.3.2. Search custodial data sources for data relevant to the case.

Search custodial data sources for data relevant to the case. After custodians have been added to a case, you can use the built-in search tool to find the custodian locations for data that might be relevant. You do this by using keywords, properties, and conditions to build your search queries, which will return search results that contain data that's likely to be relevant to the case. You can preview search results to quickly verify whether the data is relevant and revise your queries and rerun searches to improve results.

#### 4.4.2.3.3. Add data to a review set

Add data to a review set. After configuring and verifying that a search result has provided you with the right data, you'll need to prepare your results for review and analysis. You can do this by adding the search results to a review set. Doing this means that items are copied from their location of origin to a secure location in Azure Storage. The data is also reindexed to optimize it for review and analysis. You can also add data to conversation review sets, which will provide you with the capabilities to reconstruct conversations, and enable you to review and export conversations like those in Microsoft Teams.

#### 4.4.2.3.4. Review and analyze data in a review set

Review and analyze data in a review set. When your data is in a review set, you're ready to view and analyze the case data through a wide variety of capabilities and tools such as filters, queries, and tags. The goal of review and analysis is to reduce the data set to what is the most relevant to the case that's being investigated.

#### 4.4.2.3.5. Export and download case data

Export and download case data. Finally, you can export the data out of Advanced eDiscovery for external review. For example, for an external team of investigators. You export the data out of the review set, and then copy it to a different Azure Storage location. You can then use Azure Storage Explorer to download that data as an export package, to a local device. This export package will contain other components like a summary report, and an error report.

### 4.4.3. Compare eDiscovery Solutions

The following table compares the key capabilities available in Content search, Core eDiscovery, and Advanced eDiscovery.

| Capability | Content search | Core eDiscovery | Advanced eDiscovery |
|---|---|---|---|
| Search for content | ✔ | ✔ | ✔ |
| Keyword queries and search conditions | ✔ | ✔ | ✔ |
| Search statistics | ✔ | ✔ | ✔ |
| Export search results | ✔ | ✔ | ✔ |
| Role-based permissions | ✔ | ✔ | ✔ |
| Case management | | ✔ | ✔ |
| Place content locations on legal hold | | ✔ | ✔ |
| Custodian management | | | ✔ |
| Legal hold notifications | | | ✔ |
| Advanced indexing | | | ✔ |
| Error remediation | | | ✔ |
| Review sets | | | ✔ |
| Support for cloud attachments and SharePoint versions | | | ✔ |

| | |
|---|---|
| Optical character recognition | ✔ |
| Conversation threading | ✔ |
| Collection statistics and reports | ✔ |
| Review set filtering | ✔ |
| Tagging | ✔ |
| Analytics | ✔ |
| Predictive coding models | ✔ |
| Computed document metadata | ✔ |
| Transparency of long-running jobs | ✔ |
| Export to customer-owned Azure Storage location | ✔ |

Here's a description of each eDiscovery capability.

#### 4.4.3.1. Search for content

Search for content. Search for content that's stored in Exchange mailboxes, OneDrive for Business accounts, SharePoint sites, Microsoft Teams, Microsoft 365 Groups, and Yammer Teams. This includes content generated by other Microsoft 365 apps that store data in mailboxes and sites.

#### 4.4.3.2. Keyword queries and search conditions

Keyword queries and search conditions. Create KQL keyword search queries to search for content that match query criteria. You can also include conditions to narrow the scope of your search.

#### 4.4.3.3. Search statistics

Search statistics. After you run a search, you can view statistics of the estimated search results, such as the number and total size of items matching your search criteria. Other statistics include the top content locations that contain search results and the number of items that match different parts of the search query.

#### 4.4.3.4. Export search results

Export search results. Export search results to a local computer in your organization in a two-step process. When you export search results, items are copied from their original content location in Microsoft 365 to a Microsoft-provided Azure Storage location. Then you can download those items to a local computer.

#### 4.4.3.5. Role-based permissions

Role-based permissions. Use role-based access (RBAC) permissions to control what eDiscovery-related tasks that different users can perform. You can users to built-in eDiscovery-related role group or create custom role groups that assign specific eDiscovery permissions.

#### 4.4.3.6. Case management

Case management. eDiscovery cases in Core eDiscovery and Advanced eDiscovery let you associate specific searches and exports with a specific investigation. You can also assign members to a case to control who can access the case and view the contents of the case.

#### 4.4.3.7. Place content locations on legal hold

Place content locations on legal hold. Preserve content relevant to your investigation by placing a legal hold on the content locations in a case. This lets you secure electronically stored information from inadvertent (or intentional) deletion during your investigation.

#### 4.4.3.8. Custodian management

Custodian management. Manage the people that you've identified as people of interest in the case (called custodians) and other data sources that may not be associated with a custodian. When you add custodians and non-custodial data sources to a case, you can place a legal hold on these data sources, communicate with custodians by using the legal hold notification process, and search custodian and non-custodial data sources to collect content relevant to the case.

#### 4.4.3.9. Legal hold notifications

Legal hold notifications. Manage the process of communicating with case custodians. A legal hold notification instructs custodians to preserve content that's relevant to the case. You can track the notices that were received, read, and acknowledged by custodians. The communications workflow in Advanced eDiscovery allows you to create and send initial notifications, reminders, and escalations if custodians fail to acknowledge a hold notification.

#### 4.4.3.10. Advanced indexing

Advanced indexing. When you add custodial and non-custodian data sources to a case, the associated content locations are reindexed (in a process called Advanced indexing) so that any content deemed as partially indexed is reprocessed to make it fully searchable when you collect data for an investigation.

#### 4.4.3.11. Error remediation

Error remediation. Fix processing errors using a process called error remediation. Error remediation allows you to rectify data issues that prevent Advanced eDiscovery from properly processing the content during Advanced indexing. For example, files that are password protected can't be processed since the files are locked or encrypted. Using error remediation, you can download files with errors, remove the password protection, and then upload the remediated files.

#### 4.4.3.12. Review sets

Review sets. Add relevant data to a review set. A review set is a secure, Microsoft-provided Azure Storage location in the Microsoft cloud. When you add data to a review set, the collected items are copied from their original content location to the review set. Review sets provide a static, known set of content that you can search, filter, tag, analyze, and predict relevancy using predictive coding models. You can also track and report on what content gets added to the review set.

#### 4.4.3.13. Support for cloud attachments and SharePoint versions

Support for cloud attachments and SharePoint versions. When you add content to a review set, you have the option to include cloud attachments or linked files. This means that the target file of a cloud attachment or linked file is added to the review set. You also have the option to add all versions of a SharePoint document to a review set.

#### 4.4.3.14. Optical character recognition (OCR)

Optical character recognition (OCR). When content is added to a review set, OCR functionality extracts text from images, and includes the image text with the content that's added to a review set. This lets you search for image text when you query the content in the review set.

#### 4.4.3.15. Conversation threading

Conversation threading. When chat messages from Teams and Yammer conversations are added to a review set, you can collect the entire conversation thread. This means that the entire chat conversation that contains items that match the collection criteria is added to the review set. This lets you review chat items in the context of the back-and-forth conversation.

#### 4.4.3.16. Collection statistics and reports

Collection statistics and reports. After you create a draft collection or commit a commit a collection to a review set, you can view a rich set of statistics on the retrieved items, such as the content locations that contain the most items that matched the search criteria and the number of items returned by the search query. You can also preview a subset of the results. Additionally, this includes the number of child items extracted from their parent items and added as separate items to the review set.

#### 4.4.3.17. Review set filtering

Review set filtering. After content is added to a review set, you can apply filters to display only the set of items that match your filtering criteria. Then you can save the filter sets as a query, which lets you quickly reapply the saved filters. Review set filtering and saved queries help you quickly cull content to the items that are most relevant to your investigation.

#### 4.4.3.18. Tagging

Tagging. Tags also help you cull non-relevant content and identify the most relevant content. When experts, attorneys, or other users review content in a review set, their opinions related to the content can be captured by using tags. For example, if the intent is to cull unnecessary content, a user can tag documents with a tag such as "non-responsive". After content has been reviewed and tagged, a review set query can be created to exclude any content tagged as "non-responsive". This process eliminates the non-responsive content from subsequent steps in the eDiscovery workflow.

#### 4.4.3.19. Analytics

Analytics. Advanced eDiscovery provides tools to analyze review set documents to help you organize the documents in a coherent manner and reduce the volume of documents to be reviewed. Near duplicate detection groups textually similar documents together to help you make your review process more efficient. Email threading identifies specific email messages that give a complete context of the conversation in an email thread. Themes functionality attempts to analyze themes in review set documents and assign a theme to documents so that you can review documents with related theme. These analytics capabilities help make your review process more efficient so that reviewers can review a fraction of collected documents.

#### 4.4.3.20. Predictive coding models

Predictive coding models. Use predictive coding models to reduce and cull large volumes of case content to a relevant set of items that you can prioritize for review. This is accomplished by creating and training your own predictive coding models that help you prioritize the review of the most relevant items in a review set. The system uses the training to apply prediction scores to every item in the review set. This lets you filter items based on the prediction score, which allows you to review the most relevant (or non-relevant) items first.

#### 4.4.3.21. Computed document metadata

Computed document metadata. Many of the Advanced eDiscovery features, such as Advanced indexing, conversation threading, analytics, and predictive coding add metadata properties to review set documents. This metadata contains information related to the function performed by a specific feature. When reviewing documents, you can filter on metadata properties to display documents that match your filter criteria. This metadata can be imported into third-party review applications after review set documents are exported.

#### 4.4.3.22. Transparency of long-running jobs

Transparency of long-running jobs. Jobs in Advanced eDiscovery are typically long-running processes that are triggered by user actions, such as the adding custodians to a case, adding content to a review set, running analytics, and training predictive coding models. You can track the status of these jobs and get support information if you need to escalate issues to MS Support.

#### 4.4.3.23. Export to customer-owned Azure Storage location

Export to customer-owned Azure Storage location. When you export documents from a review set, you have the option to export them to an Azure Storage account managed by your organization. Additionally, Advanced eDiscovery lets you customize what data is exported. This includes exporting file metadata, native files, text files, tags, and redacted documents saved to a PDF file.

### 4.4.4. eDiscovery Subscription Comparison

The following sections show the minimum subscription requirements for Content search, Core eDiscovery, and Advanced eDiscovery. Subscriptions that support Core eDiscovery also support Content search. Subscriptions that support Advanced eDiscovery also support Content search and Core eDiscovery.

#### 4.4.4.1. Content search

- Microsoft 365 E1 subscription
- Microsoft 365 G1 subscription
- Microsoft 365 F1 or F3 subscription, or F5 Security add-on
- Microsoft 365 Business Premium subscription
- Office 365 Education A1 subscription
- Office 365 E1 subscription

#### 4.4.4.2. Core eDiscovery

- Microsoft 365 E3 subscription
- Microsoft 365 G3 subscription
- Microsoft 365 Business Premium subscription
- Microsoft 365 F5 Compliance add-on or F5 Security & Compliance add-on
- Microsoft 365 Education A3 or Office 365 Education A3 subscription

- Office 365 E3 subscription

#### 4.4.4.3. Advanced eDiscovery

- Microsoft 365 E5 or Office 365 E5 subscription
- Microsoft 365 E3 subscription with E5 Compliance add-on
- Microsoft 365 E3 subscription with E5 eDiscovery and Audit add-on
- Microsoft 365 G5 subscription
- Microsoft 365 G5 subscription with G5 Compliance add-on
- Microsoft 365 G5 subscription with G5 eDiscovery and Audit add-on
- Microsoft 365 F5 Compliance add-on or F5 Security & Compliance add-on
- Microsoft 365 Education A5 or Office 365 Education A5 subscription

### 4.4.5. The Core Audit Capabilities of Microsoft 365

Your organization is working with an audit team to find information about activities, such as whether a user sent an email, viewed a document, or whether an admin has had their password reset. To help the audit team, you've been asked to verify whether a specific user has sent emails about a particular confidential project. Audit log searches will help you find this kind of information.

The audit functionality in the Microsoft 365 compliance center allows organizations to view user and administrator activity through a unified audit log. For example, did an administrator reset a password? Did a user change a setting for a team in Microsoft Teams? A unified audit log supports the search of many users and/or admin activities across Microsoft 365 services, Dynamics 365, Microsoft Power Apps, Microsoft Power Automate, Power BI, Azure Active Directory, and more.

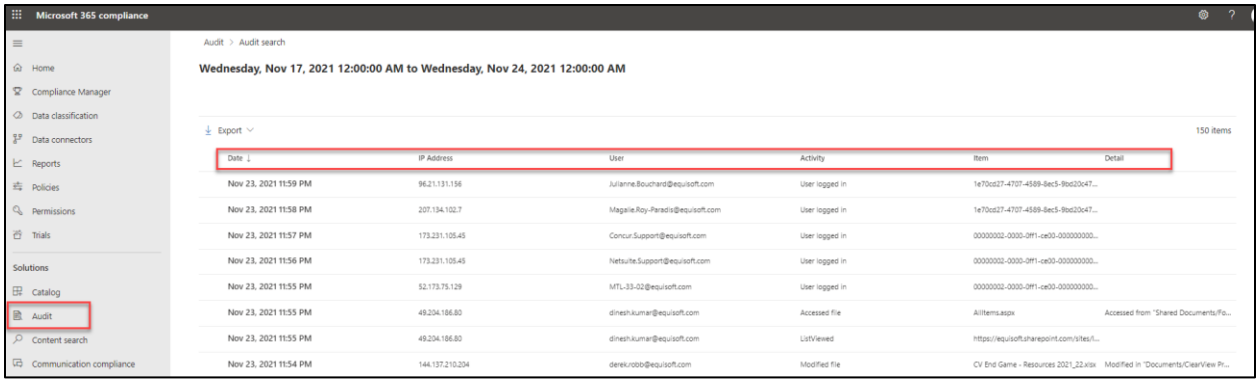
When an audited activity is performed by a user or admin, an audit record is generated and stored in the audit log for the organization. The length of time that an audit record is kept (and searchable in the audit log) depends on the Office 365 or Microsoft 365 Enterprise subscription, and specifically the type of the license that's assigned to specific users. For core audit capability, **the audit record is kept and searchable for 90 days**.

Searching the audit log requires the search capability to be turned on, and for the user doing the search to be assigned the appropriate role. The search criteria can be configured based on:

- Activities
- Start date and end date
- Users
- File, folder, or site

#### 4.4.5.1. Result from audit search

The results of the audit log search, which can be filtered and exported to a CSV file, contain the following information about each event returned by the search




It can take up to 30 minutes or up to 24 hours after an event occurs for the corresponding audit log record to be returned in the results of an audit log search.

#### 4.4.5.1.1. Date

Date: The date and time (in UTC format) when the event occurred.

#### 4.4.5.1.2. IP address

IP address: The IP address of the device that was used when the activity was logged. The IP address is displayed in either an IPv4 or IPv6 address.

#### 4.4.5.1.3. User

User: The user (or service account) who completed the action that triggered the event.

#### 4.4.5.1.4. Activity

Activity: The activity completed by the user. This is based on activities configured.

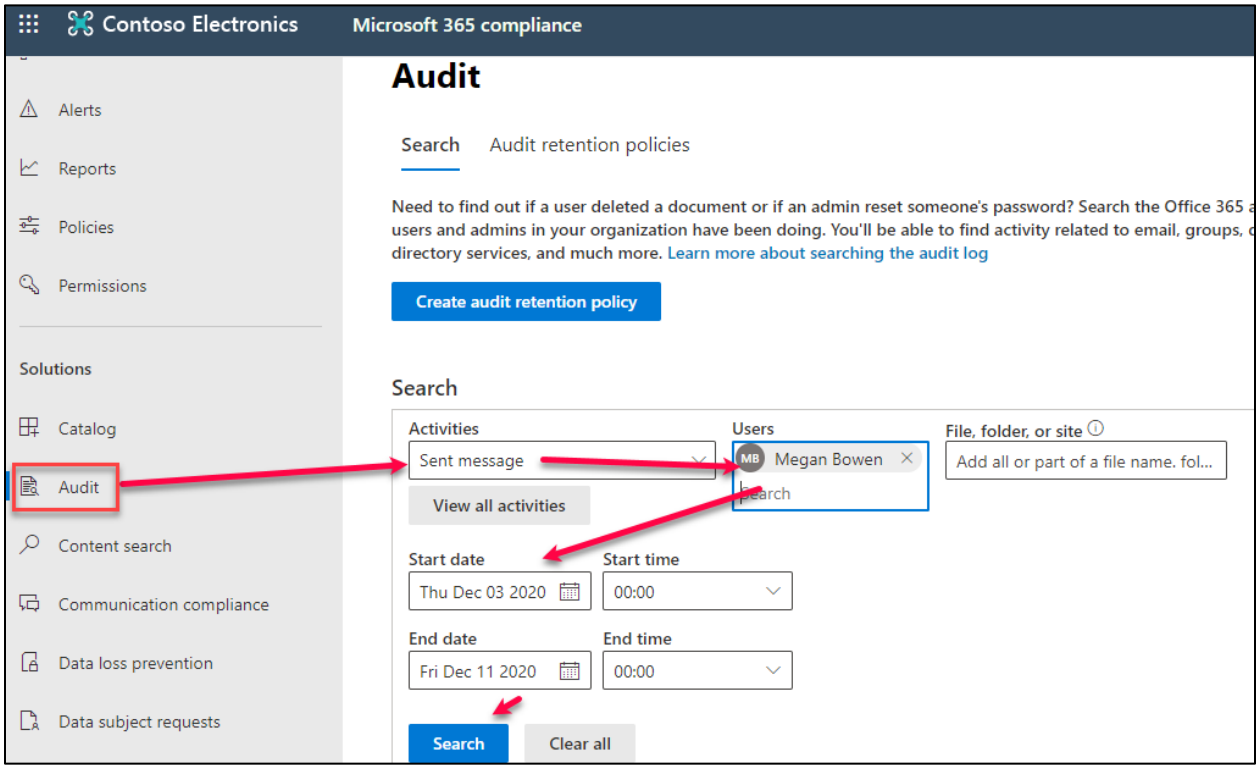
#### 4.4.5.1.5. Item

Item: The object that was created or modified because of the corresponding activity. For example, the file that was viewed or modified, or the user account that was updated. Not all activities have a value in this column.

#### 4.4.5.1.6. Detail

Detail: Additional information about an activity. Again, not all activities have a value.

#### 4.4.5.2. How to perform an Audit Search Log




### 4.4.6. The Purpose and Value of Advanced Auditing

Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention that's required to conduct an investigation. Audit log retention provides access to crucial events that help determine the scope of compromise, and faster access to Office 365 Management Activity API.

These capabilities differentiate Advanced Audit from the core audit functionality described in the previous unit and require a Microsoft 365 E5 license, or a Microsoft 365 E3 or Office 365 E3 license with a Microsoft 365 E5 Compliance, or Microsoft 365 E5 eDiscovery and Audit add-on license.

#### 4.4.6.1. Long-Term Retention of Audit Logs

Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or Azure Active Directory for the Workload property for one year. Retaining audit records for longer periods can help with on-going forensic or compliance investigations.

Microsoft now has the capability to keep audit logs for 10 years. The 10-year retention of audit logs helps support long-running investigations and respond to regulatory, legal, and internal obligations.

Retaining audit logs for 10 years requires an additional add-on license.

#### 4.4.6.1.1. Audit log retention policies

With Advanced Audit, admins can create customized audit log retention policies to retain audit records for durations less than the default of 1 year or up to 10 years (add-on license). Any custom audit log retention policy will take precedence over the default audit retention policy.


### 4.4.6.2. Access to Crucial Events for Investigation

Advanced Auditing helps organizations to conduct forensic and compliance investigations by providing access to crucial events, such as when mail items were accessed, when mail items were replied to and forwarded, and when and what a user searched for in Exchange Online and SharePoint Online. These crucial events can help admins and users investigate possible breaches and determine the scope of compromise.

#### 4.4.6.2.1. Crucial Events

Advanced Auditing provides the following crucial events:

##### 4.4.6.2.1.1. MailItemsAccessed

MailItemsAccessed - The MailItemsAccessed event is a mailbox auditing action that's triggered when mail data is accessed by mail protocols and mail clients. The MailItemsAccessed action can help investigators identify data breaches and determine the scope of messages that may have been compromised.

#### 4.4.6.2.1.2. Send

Send - The Send event is also a mailbox auditing action and is triggered when a user does one of the following actions:

- Sends an email message
- Replies to an email message
- Forwards an email message

Investigators can use the Send event to identify emails sent from a compromised account. The audit record for a Send event contains information about the message. The actual content of the message is not displayed. However, information such as when the message was sent, the InternetMessage ID, the subject line, and if the message contained attachments, are accessible. This auditing information can help investigators identify information about email messages sent from a compromised account or sent by an attacker.

#### 4.4.6.2.1.3. SearchQueryInitiatedExchange

SearchQueryInitiatedExchange - The SearchQueryInitiatedExchange event is triggered when a person uses the Search bar in Outlook on the web (OWA) to search for items in a mailbox. Investigators can use the SearchQueryInitiatedExchange event to determine if an attacker may have compromised an account, or tried to access sensitive information in the mailbox. The audit record for a SearchQueryInitiatedExchange event contains information such as the actual text of the search query. By looking at the search queries that an attacker may have made, an investigator can better understand the intent of the email data that was searched for.

#### 4.4.6.2.1.4. SearchQueryInitiatedSharePoint

SearchQueryInitiatedSharePoint - Similar to searching for mailbox items, the SearchQueryInitiatedSharePoint event is triggered when a person searches for items in the SharePoint home site for your organization. Investigators can use the SearchQueryInitiatedSharePoint event to determine if an attacker tried to find (and possibly accessed) sensitive information in SharePoint. The audit record for a SearchQueryInitiatedSharePoint event also contains the actual text of the search query. By looking at the search queries that an attacker may have performed, an investigator can better understand the intent and scope of the file data being searched for.

### 4.4.6.3. High-bandwidth access to Office 365 Management Activity API

Organizations that access auditing logs through the Office 365 Management Activity API were previously restricted by throttling limits at the publisher level. This means that for a publisher pulling data on behalf of multiple customers, the limit was shared by all those customers.

With the release of Advanced Audit, Microsoft is moving from a publisher-level limit to a tenant-level limit. The result is that each organization will get their own fully allocated bandwidth quota to access their auditing data. The bandwidth isn't a static, predefined limit but is modeled on a combination of factors, including the number of seats in the organization and the type of Microsoft 365 license (organizations with an E5 license will get more bandwidth than non-E5 organizations).

### 4.4.7. Ediscovery Advance with Microsoft Teams

https://aka.ms/edisco

https://aka.ms/ediscoveryninja

https://aka.ms/ediscovery

https://aka.ms/ediscoveryblog

https://aka.ms/learnediscovery

https://aka.ms/ediscoveryandteams

Team message

1. 1:1
2. Group private channel message
3. Direct files 1:1 or group chats
4. Teams channel messages

#### 4.4.7.1. With an eDiscovery Hold:

1. If a chat or channel message is edited by a user, the original message is copied to the SubstrateHolds folder. The message is stored there for the duration of the eDiscovery hold policy. When the policy is lifted it is permanently deleted the next time MFA runs (typically between 1-7 days).

2. If a chat or channel message is deleted by a user, the original message remains in the TeamsMessagesData folder for 30 days. It is no longer accessible to the end-user after a maximum of duration of 48 hours. It then moves to the SubstrateHolds folder when MFA runs typically between (1-7 days) The message is stored there for the duration of the eDiscovery hold policy. When the policy is lifted it is permanently deleted the next time the timer job runs (typically between 1-7 days).

3. If a chat or channel message is deleted by a retention policy (deletion policy) the message is moved to the SubstrateHolds folder in accordance with the timing associated with the retention policy deletion action. This action typically takes between 1-7 days from the expiry date. The

message is stored there for the duration eDiscovery hold policy. When the policy is lifted it is permanently deleted the next time MFA runs (typically between 1-7 days).

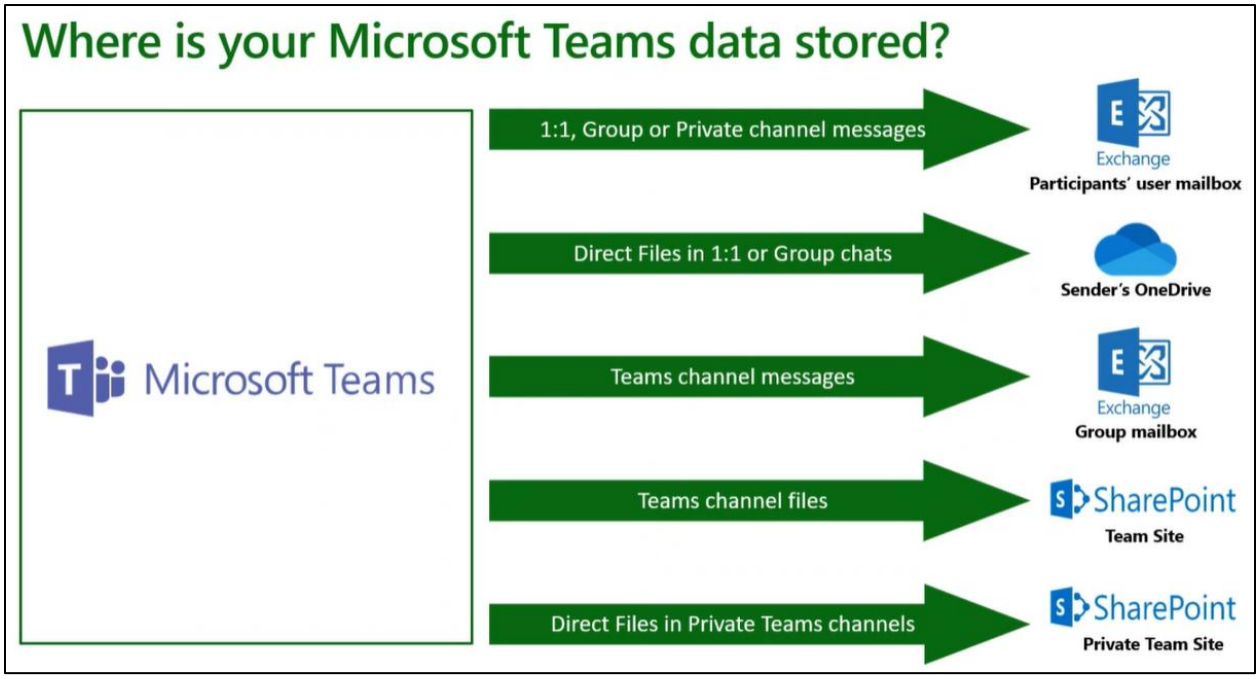
#### 4.4.7.2. Without an eDiscovery Hold:

1. If a chat or channel message is edited by a user, the original message is copied to the SubstrateHolds. The message is stored there for at least 1 day. The message is permanently deleted the next time MFA runs (typically between 1-7 days).

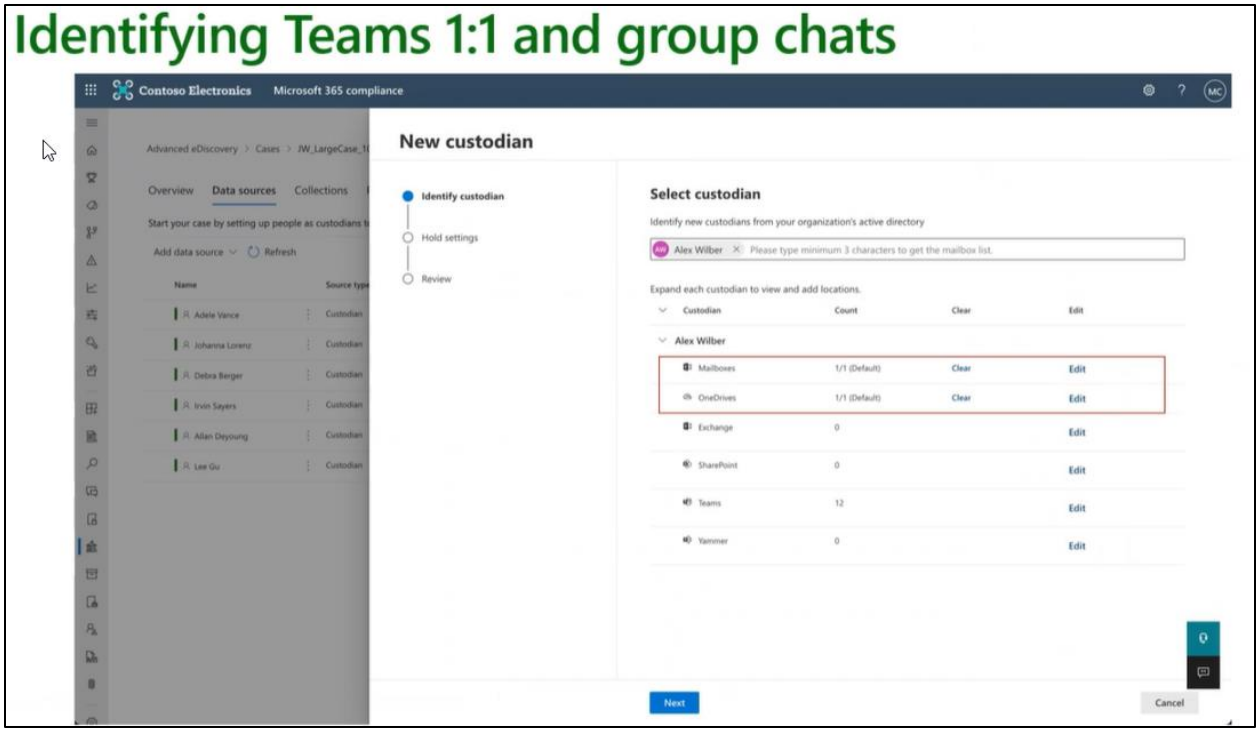
2. If a chat or channel message is deleted by a user, the original message remains in the TeamsMessagesData folder for 30 days. It is no longer accessible to the end-user after a maximum of duration of 48 hours. It then moves to the SubstrateHolds folder where the message is stored for at least 1 day. The message is permanently deleted the next time MFA runs (typically between 1-7 days).

3. If a chat or channel message is not deleted by a user or retention policy, it will be retained indefinitely.

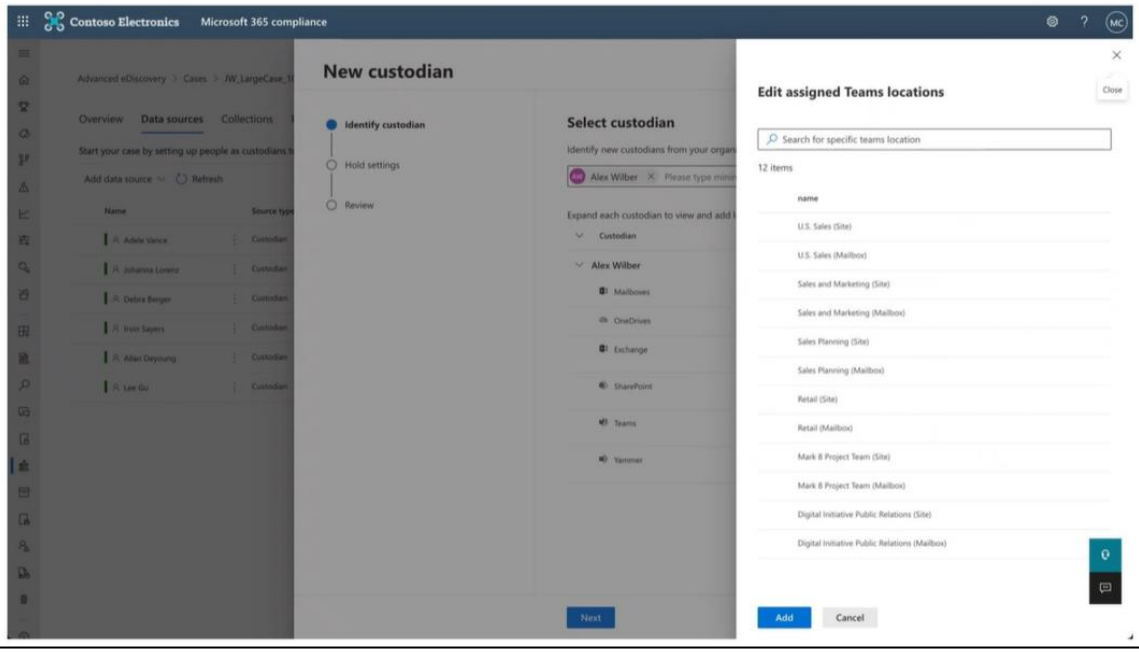
#### 4.4.7.3. MS Teams Data location for eDiscovery Hold

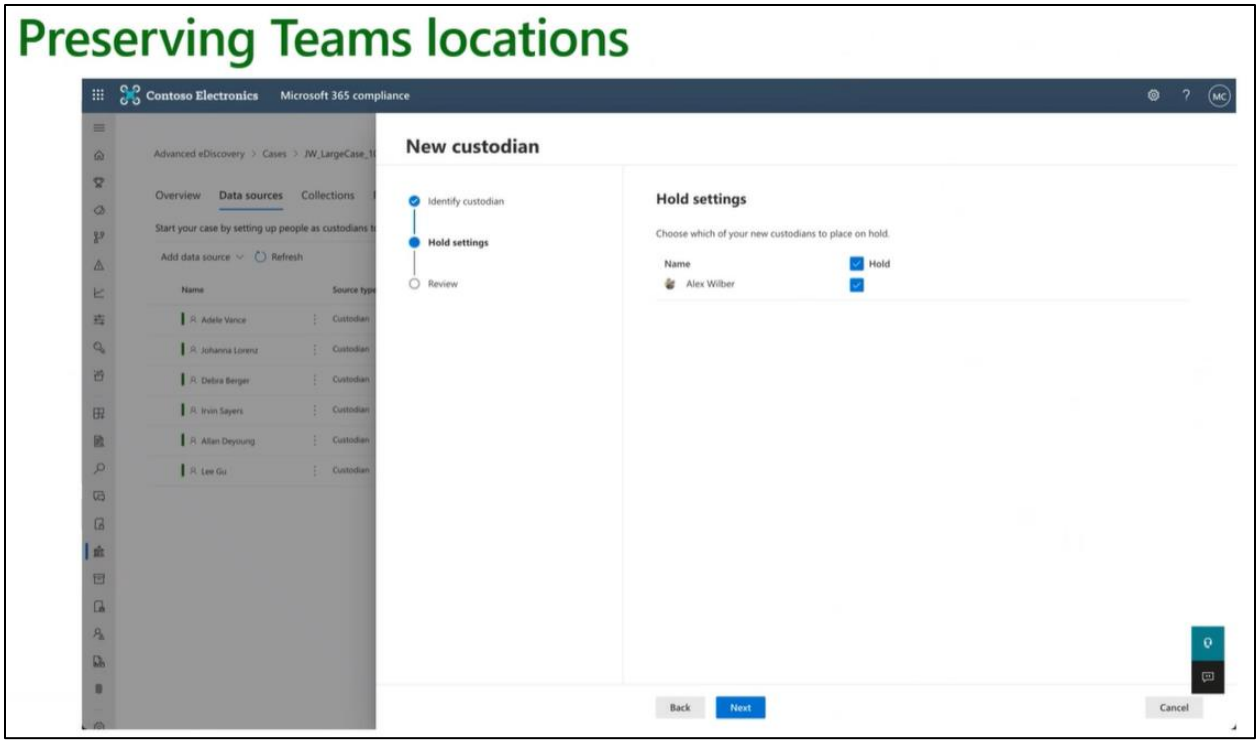


# Identifying Teams 1:1 and group chats




# Identifying Teams based on custodial membership




Preserving Teams locations
Contoso Electronics
Microsoft 365 compliance
New custodian
Identify custodian
Hold settings
Review
Hold settings
Choose which of your new custodians to place on hold.
Name
Hold
Alex Wilber
Back
Next
Cancel

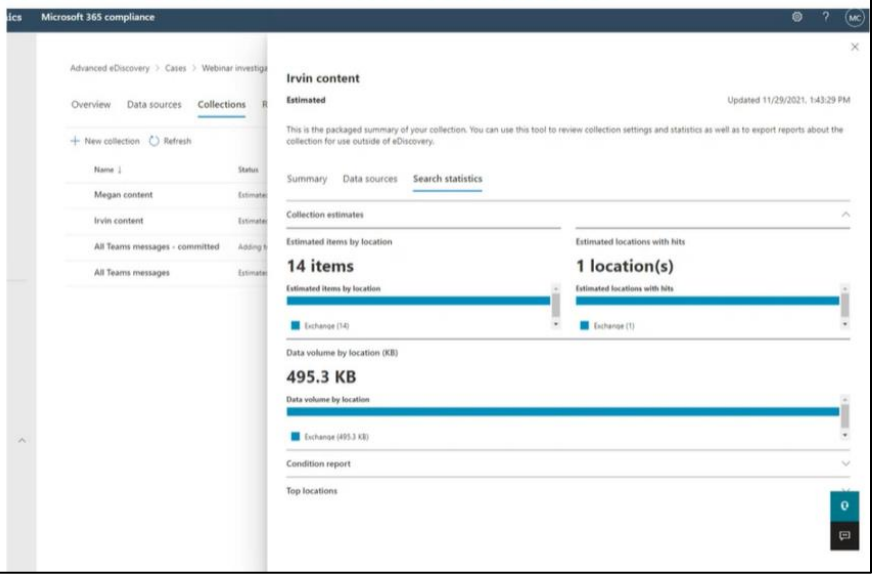

eDiscovery ask:
How do I collect Teams content ?
with Advanced eDiscovery:
Conduct targeted collections of Teams content

# Quickly search for and collect Teams content

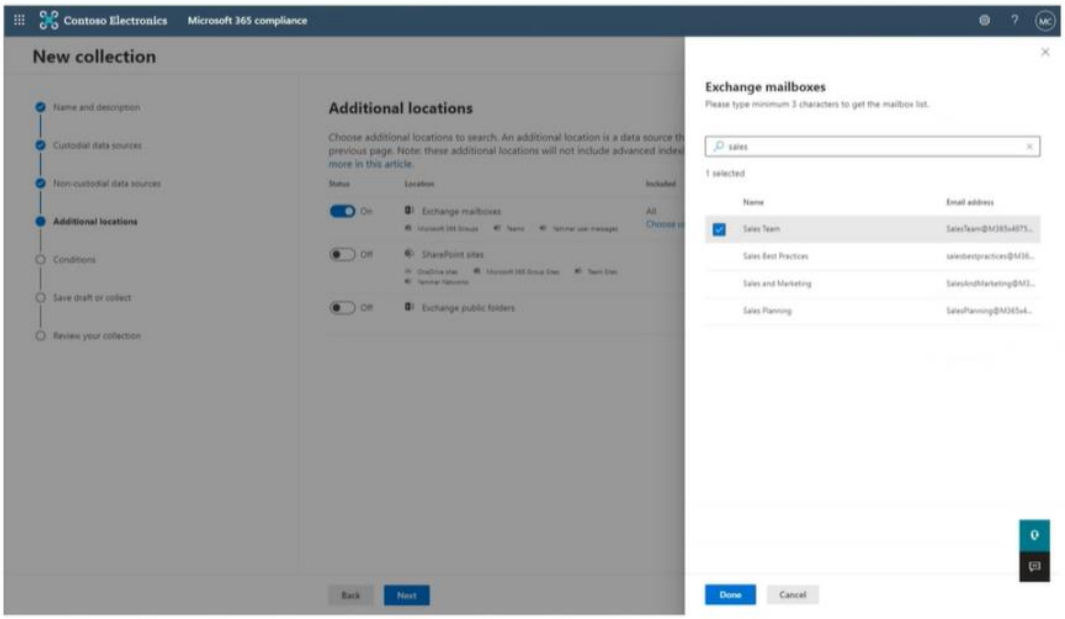
By custodian or location

Using queries and conditions

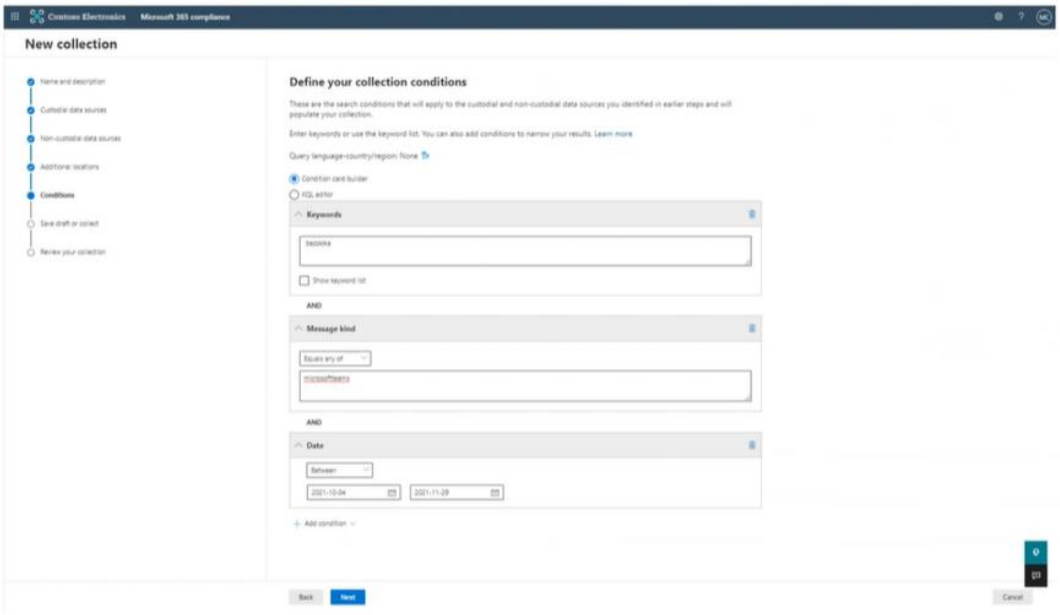
Including cloud attachments shared



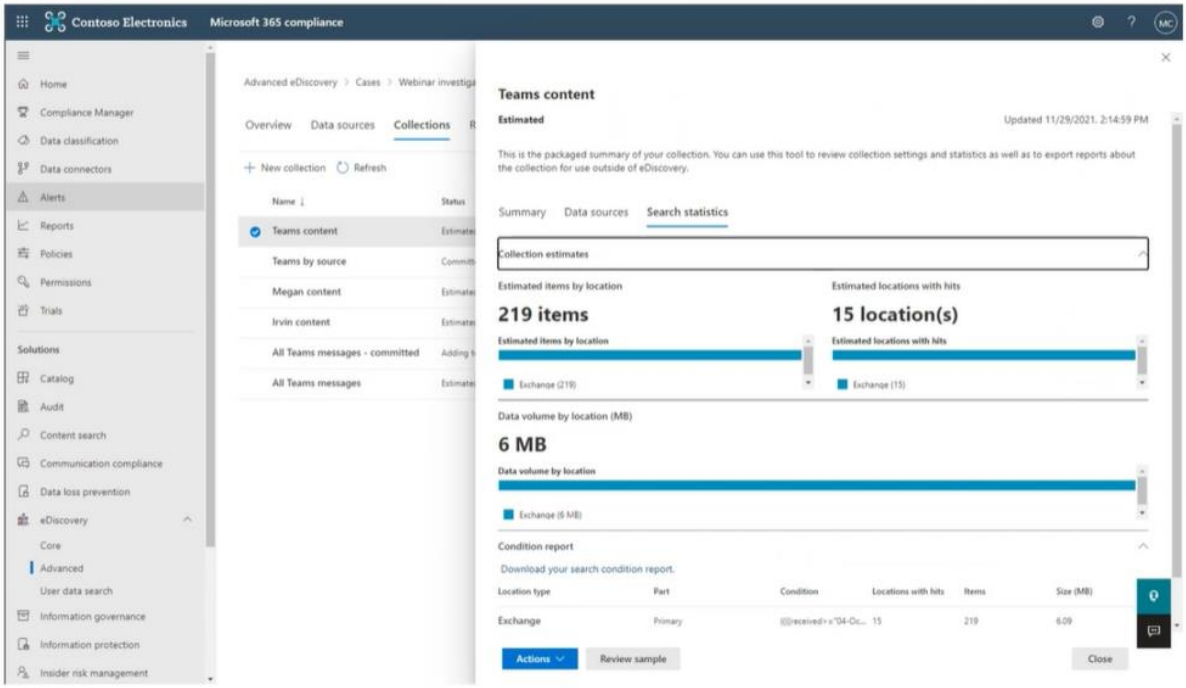

# Collect by Custodian (employee) or Team



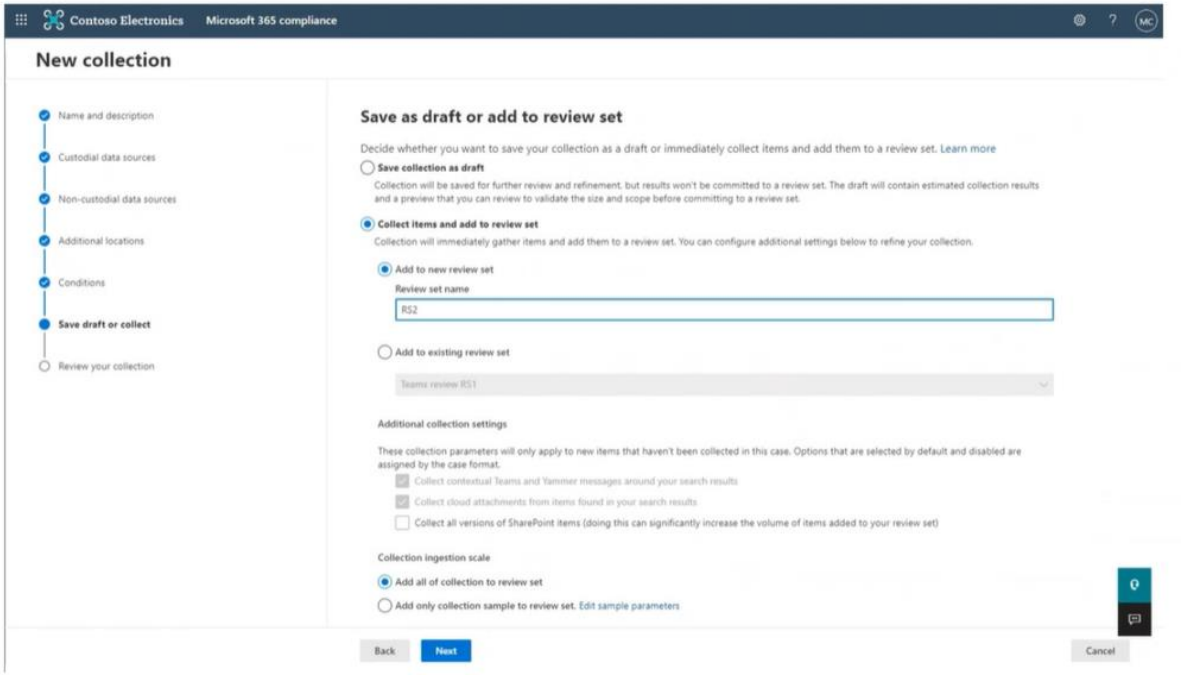
# Target Teams content with conditions & queries




# Get estimates before committing collection

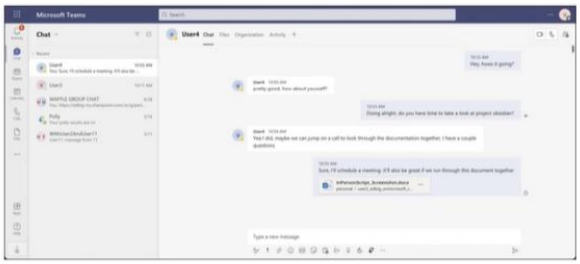


# Include Cloud attachments relevant to your search

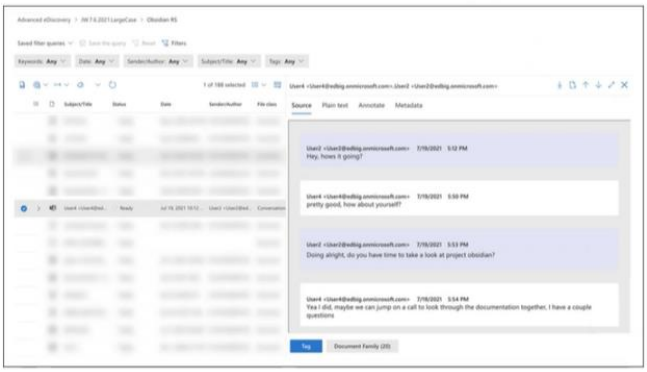



# Threaded messages for Teams 1:1 or group chats

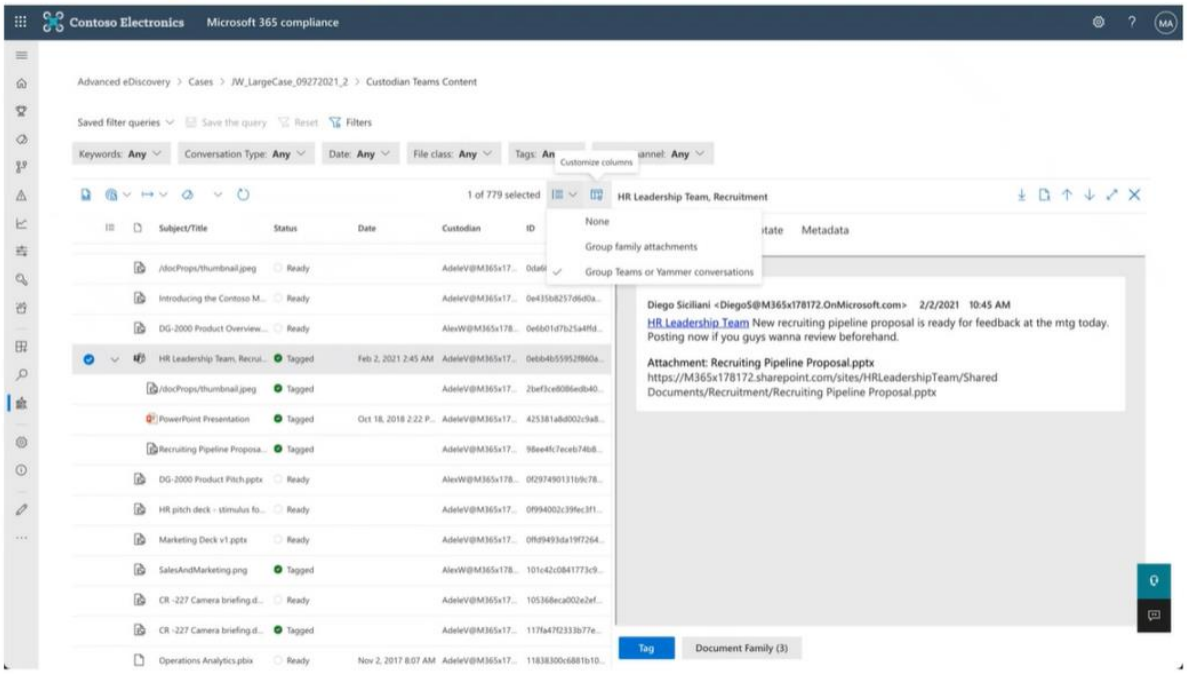
What a Teams user sees:



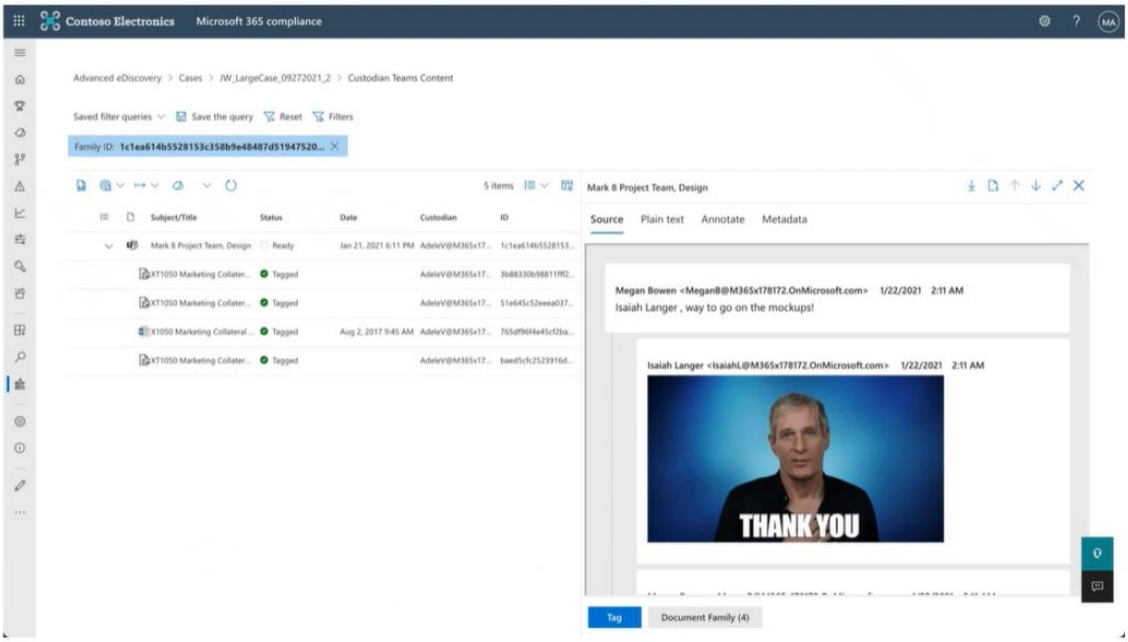
What an eDiscovery manager sees with threaded transcript view in Advanced eDiscovery:



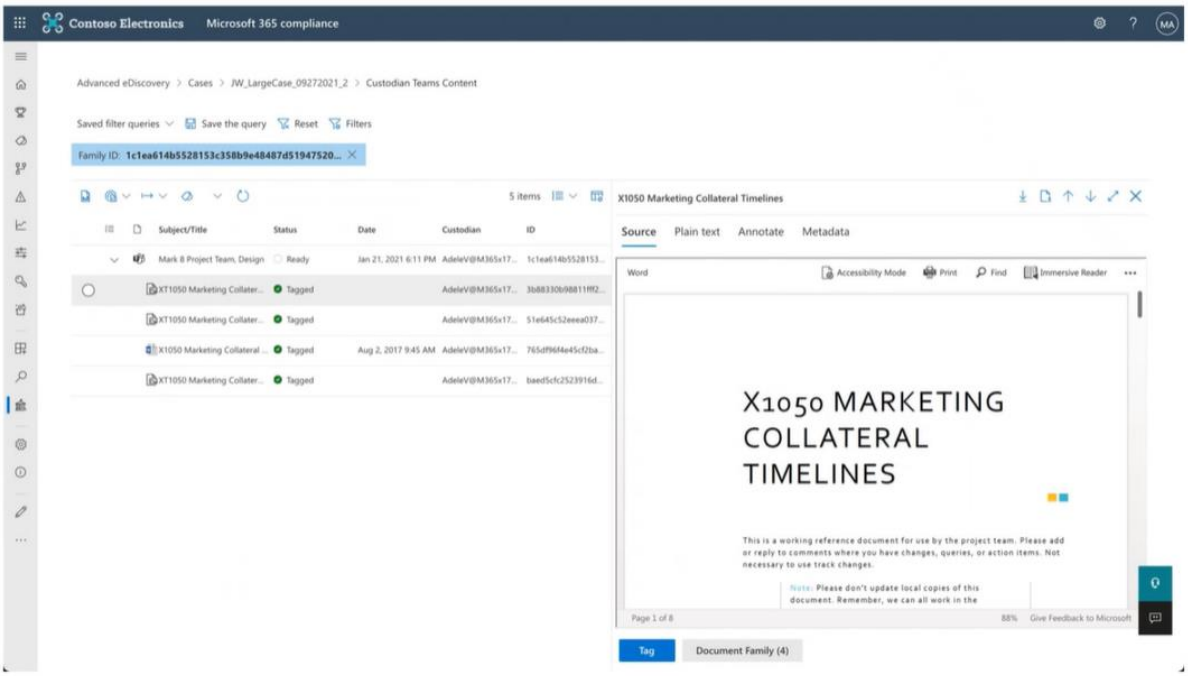
# Reviewing 1:1 or group chats



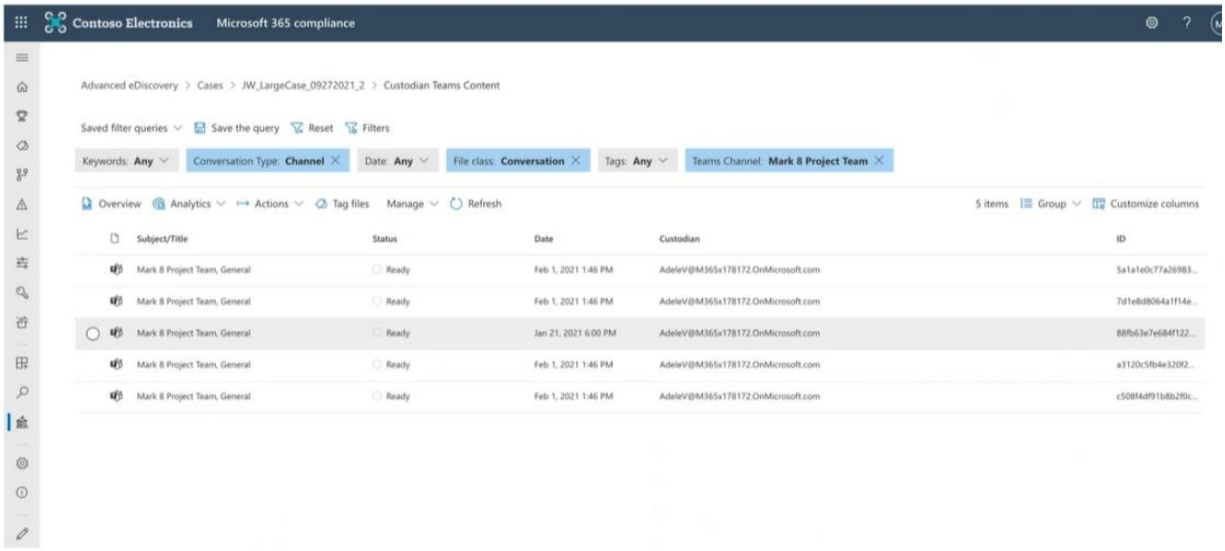
# Reviewing Teams Channel posts

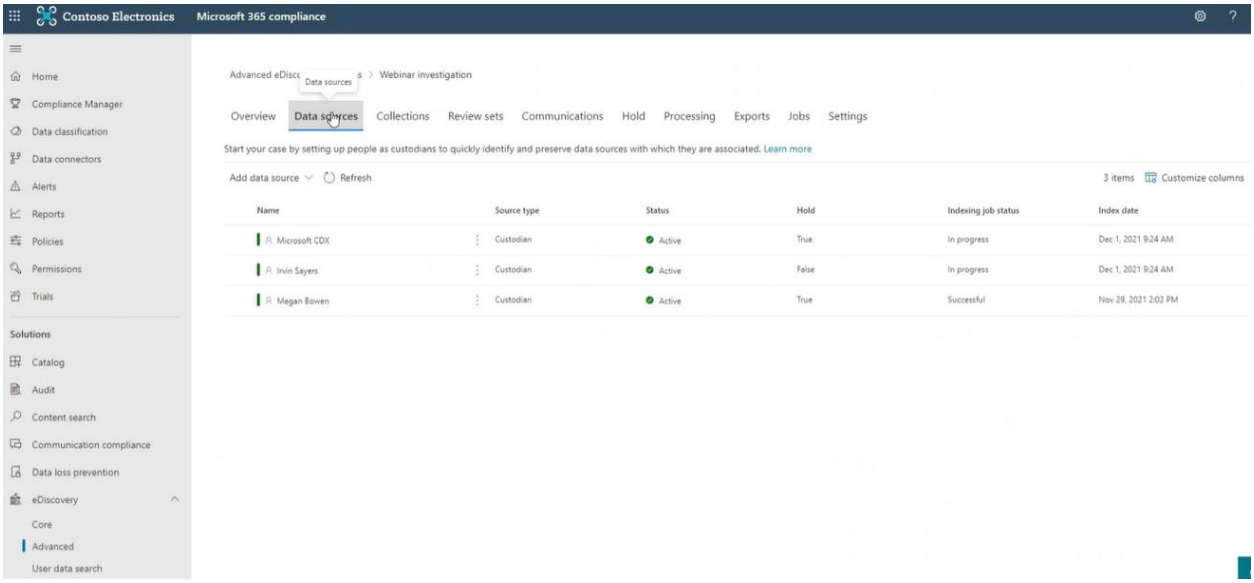


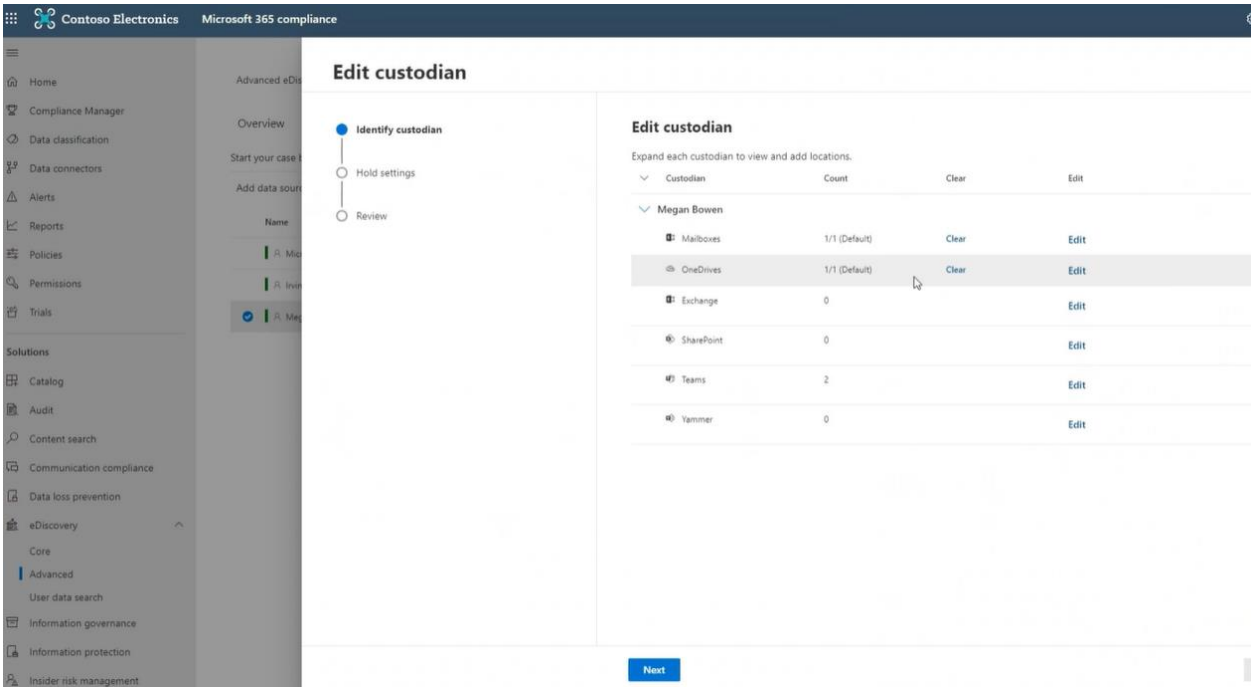

# Reviewing Cloud Attachments

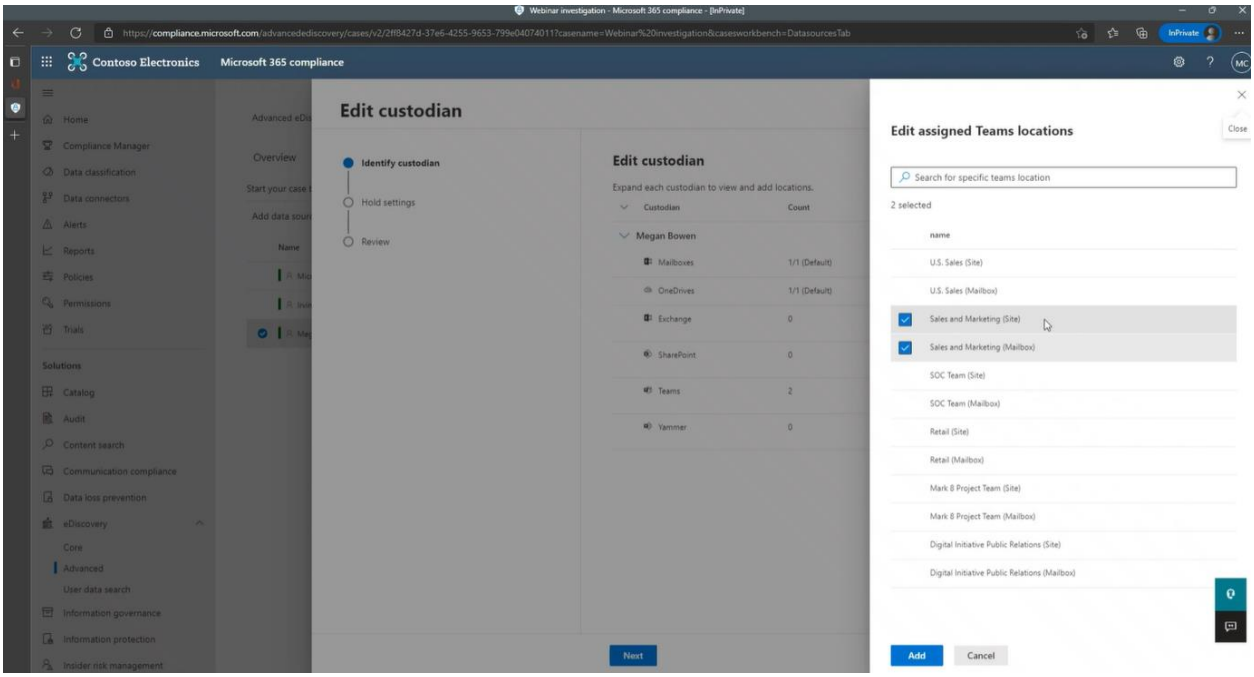


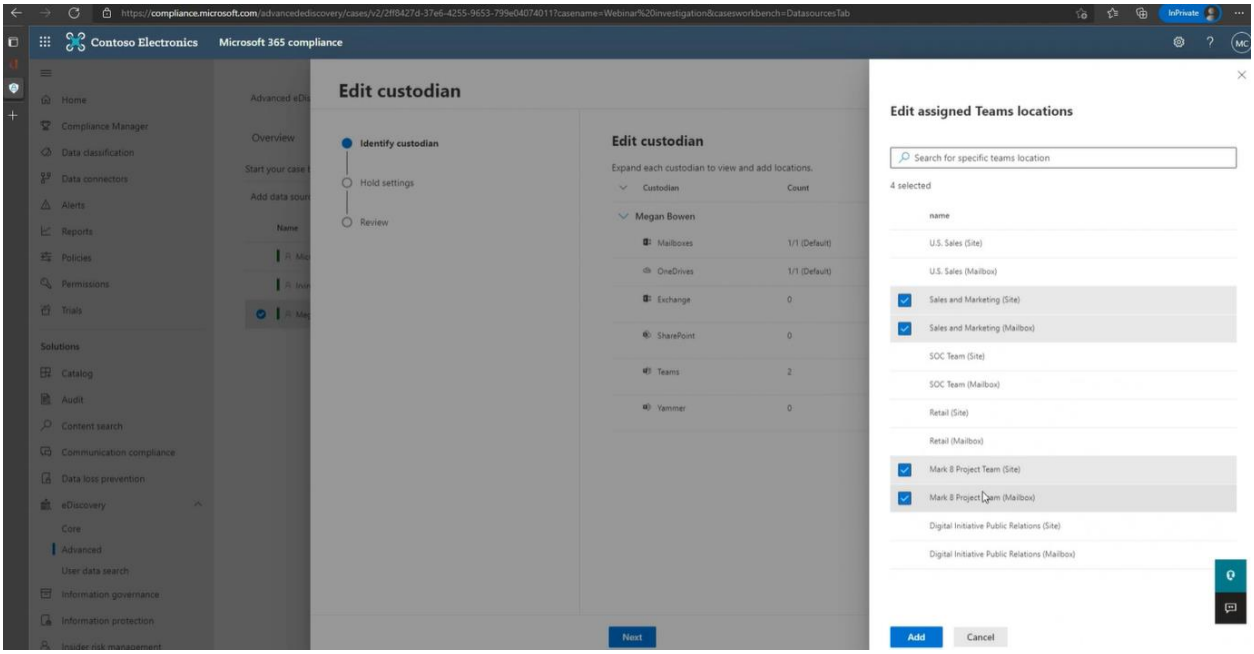
# Filters for Teams conversations

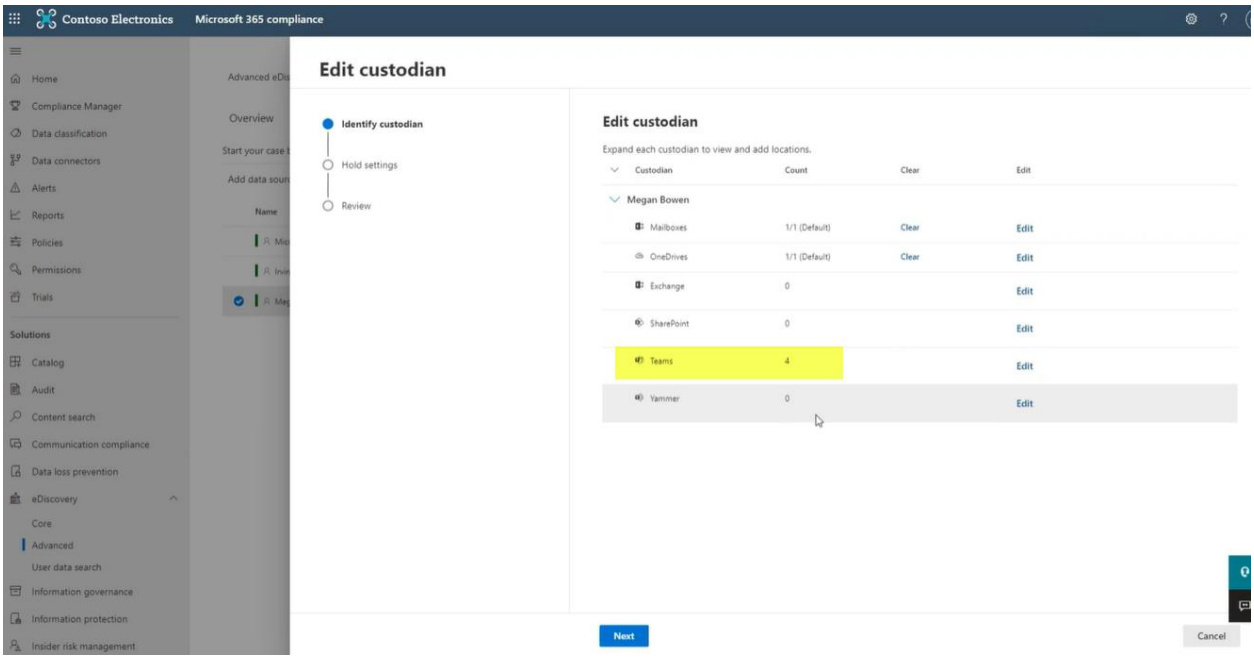


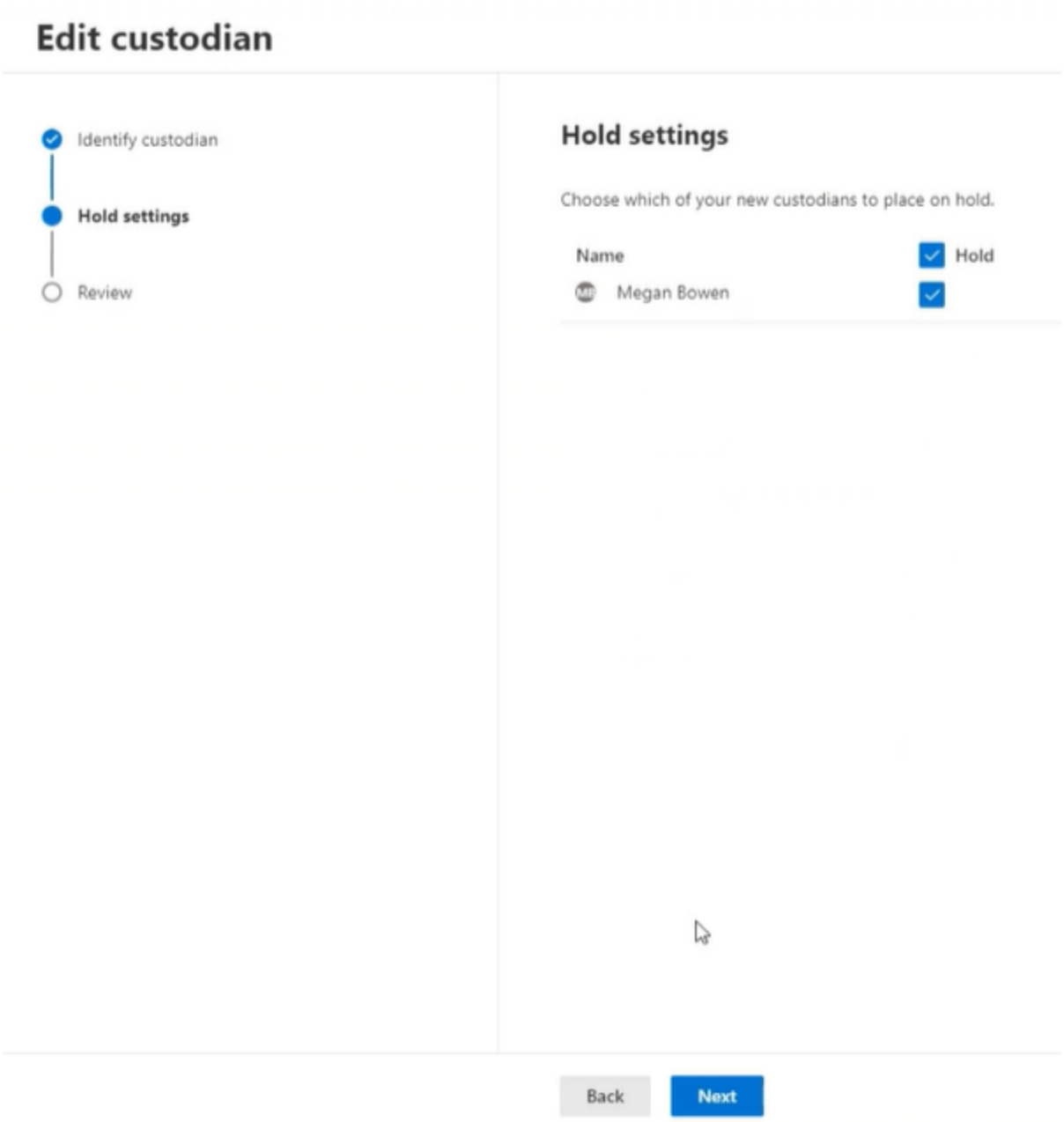



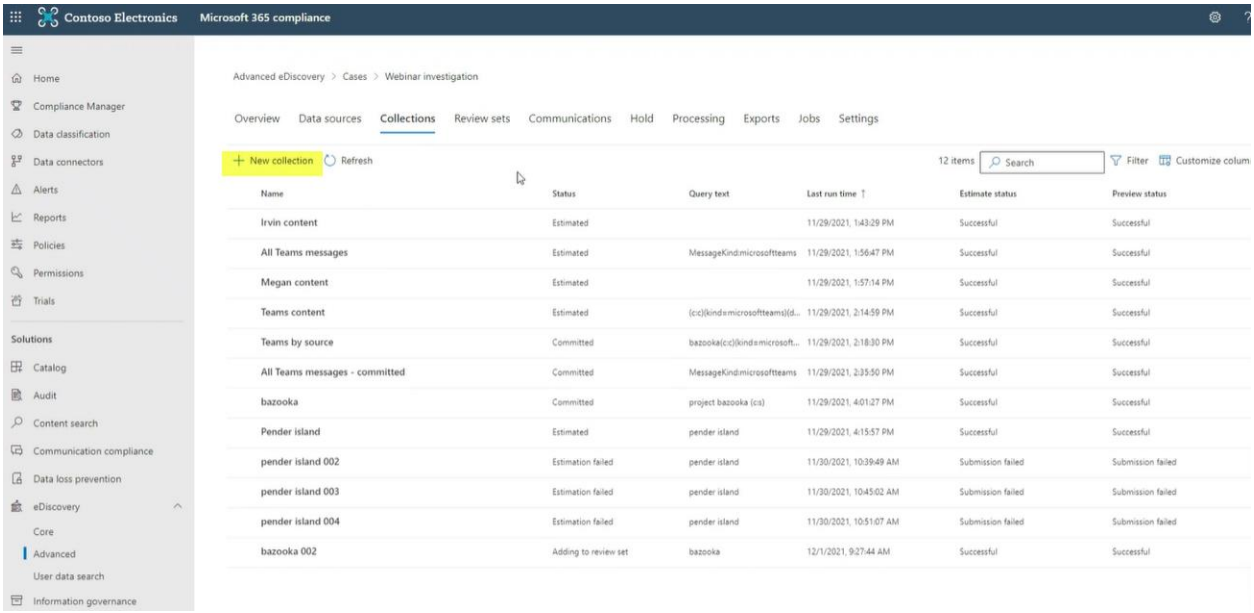

Contoso Electronics
Microsoft 365 compliance
Edit custodian
Identify custodian
Hold settings
Review
Edit custodian
Expand each custodian to view and add locations.
Custodian
Count
Clear
Edit
Megan Bowen
Mailboxes
1/1 (Default)
OneDrives
1/1 (Default)
Exchange
0
SharePoint
0
Teams
2
Yammer
0
Next

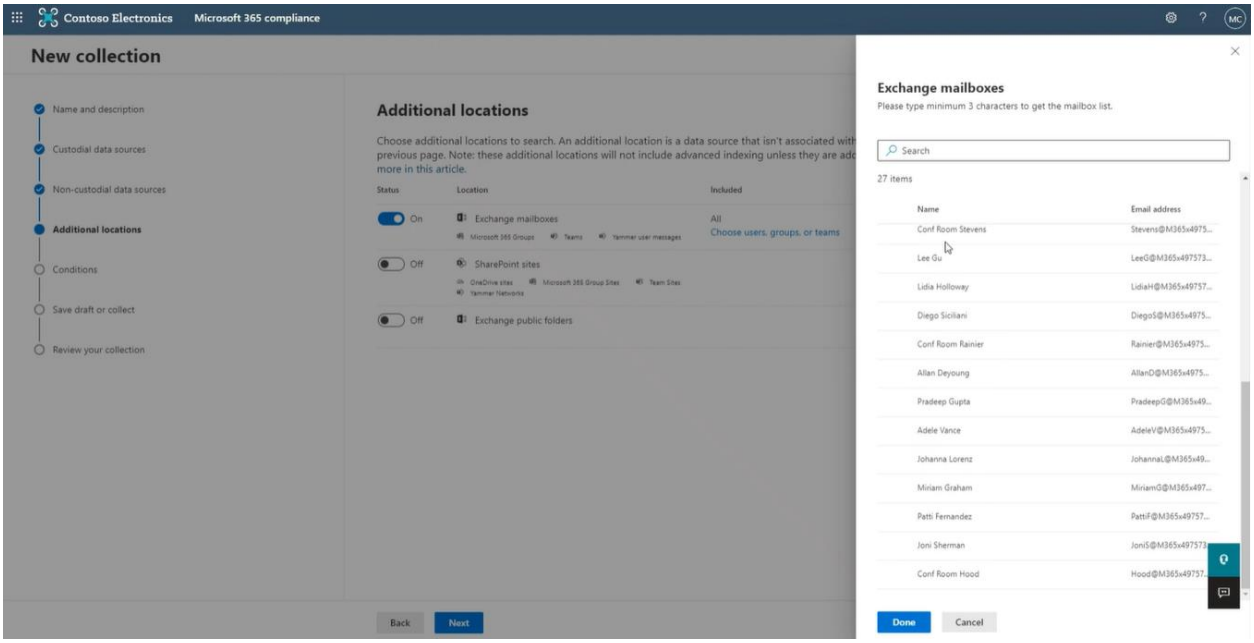

Contoso Electronics
Microsoft 365 compliance
Edit custodian
Identify custodian
Hold settings
Review
Edit custodian
Megan Bowen
Next
Edit assigned Teams locations
Search for specific teams location
2 selected
name
U.S. Sales (Site)
U.S. Sales (Mailbox)
Sales and Marketing (Site)
Sales and Marketing (Mailbox)
SOC Team (Site)
SOC Team (Mailbox)
Retail (Site)
Retail (Mailbox)
Mark 8 Project Team (Site)
Mark 8 Project Team (Mailbox)
Digital Initiative Public Relations (Site)
Digital Initiative Public Relations (Mailbox)
Add
Cancel

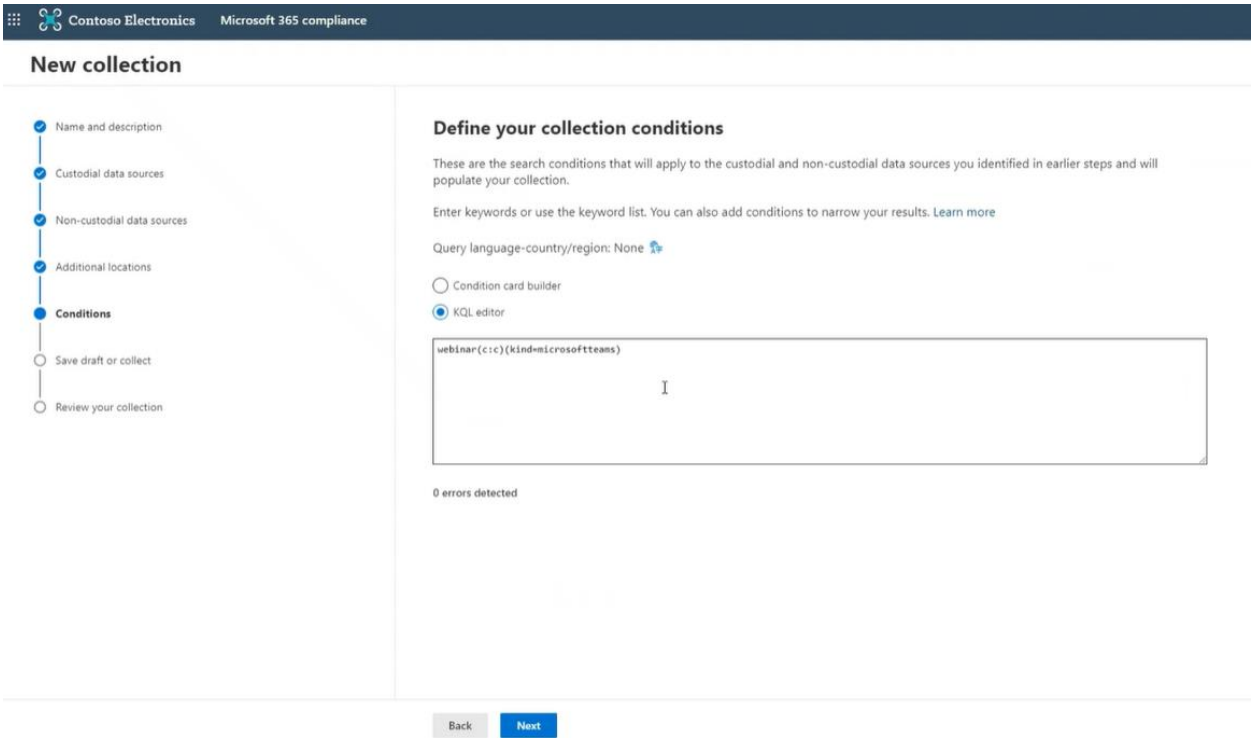

Contoso Electronics
Microsoft 365 compliance
Edit custodian
Identify custodian
Hold settings
Review
Edit custodian
Expand each custodian to view and add locations.
Custodian
Count
Megan Bowen
Mailboxes 1/1 (Default)
OneDrives 1/1 (Default)
Exchange 0
SharePoint 0
Teams 2
Yammer 0
Next
Edit assigned Teams locations
Search for specific teams location
4 selected
name
U.S. Sales (Site)
U.S. Sales (Mailbox)
Sales and Marketing (Site)
Sales and Marketing (Mailbox)
SOC Team (Site)
SOC Team (Mailbox)
Retail (Site)
Retail (Mailbox)
Mark 8 Project Team (Site)
Mark 8 Project Team (Mailbox)
Digital Initiative Public Relations (Site)
Digital Initiative Public Relations (Mailbox)
Add
Cancel

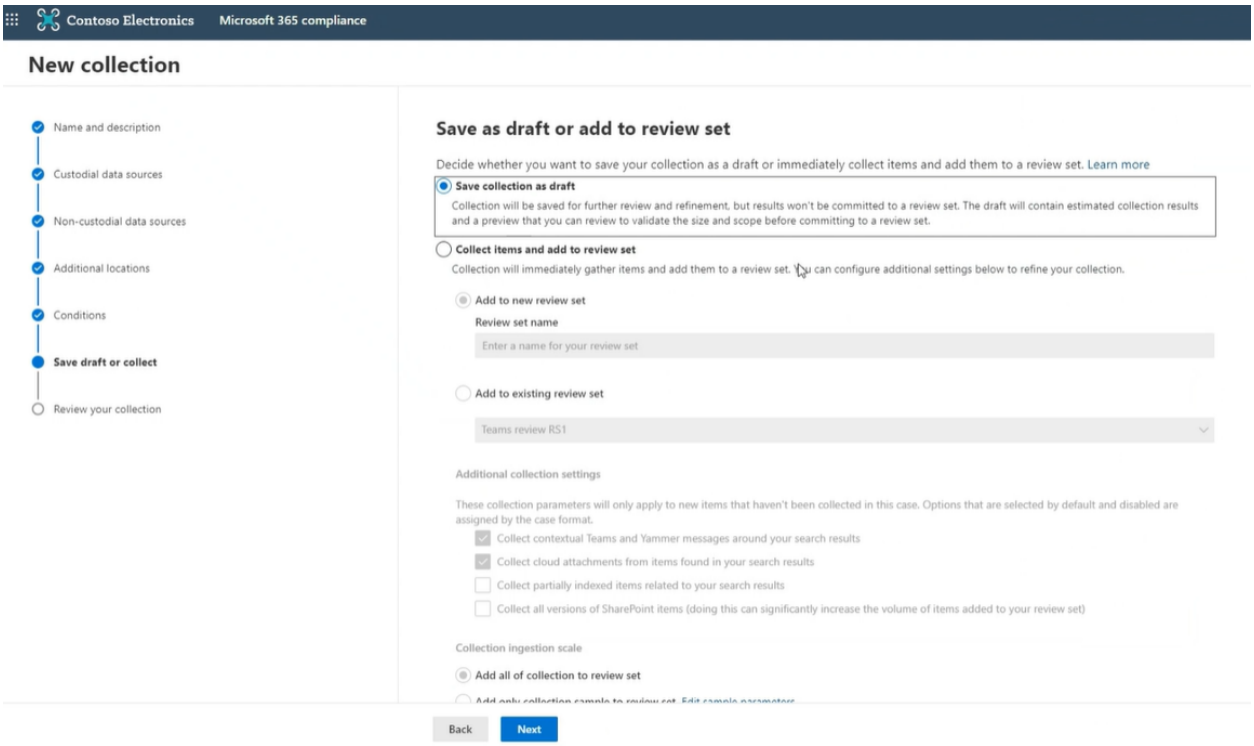

Contoso Electronics
Microsoft 365 compliance
Edit custodian
Identify custodian
Hold settings
Review
Edit custodian
Expand each custodian to view and add locations.
Custodian
Count
Clear
Edit
Megan Bowen
Mailboxes 1/1 (Default) Clear Edit
OneDrives 1/1 (Default) Clear Edit
Exchange 0 Edit
SharePoint 0 Edit
Teams 4 Edit
Yammer 0 Edit
Next
Cancel

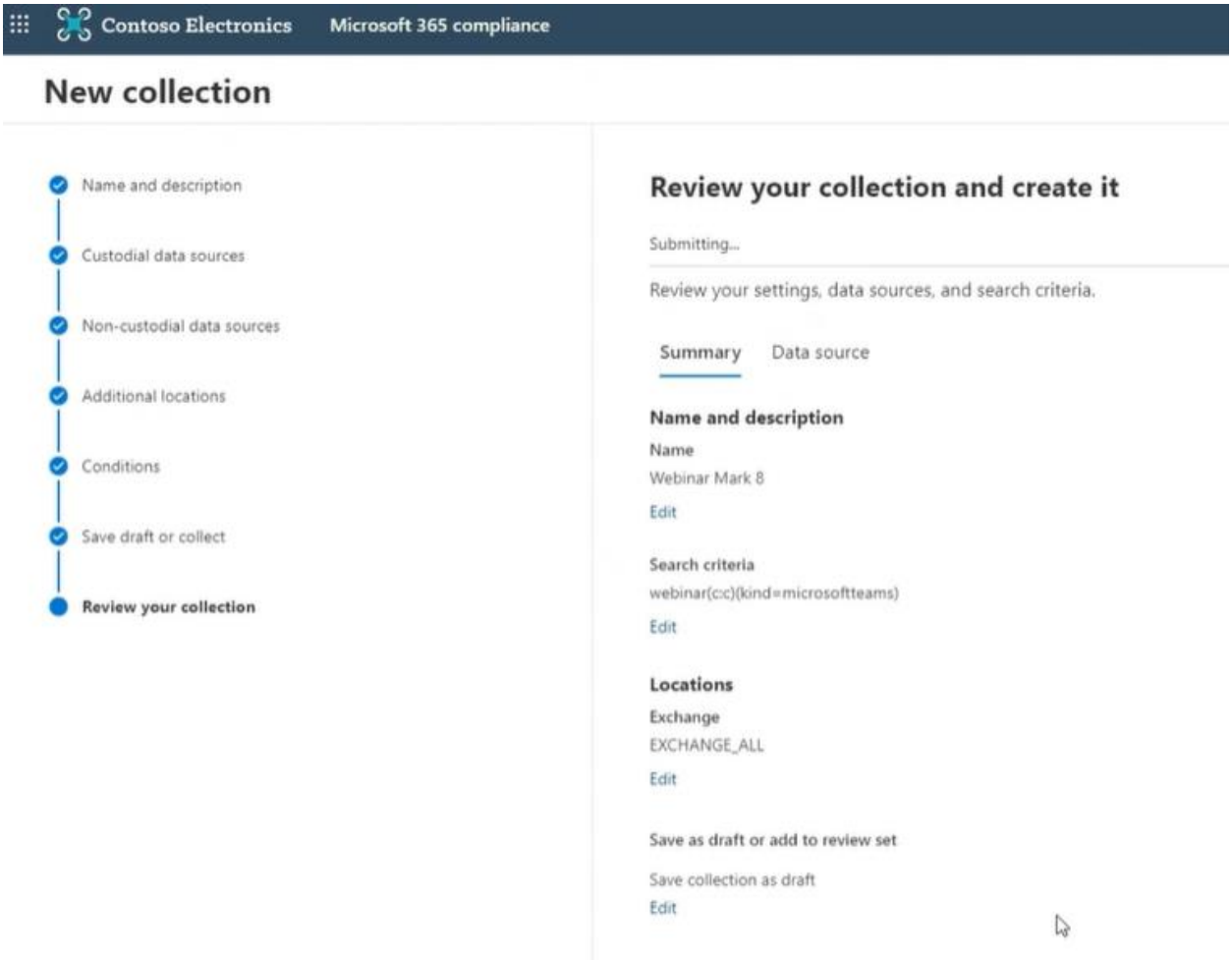

Edit custodian
Identify custodian
Hold settings
Review
Hold settings
Choose which of your new custodians to place on hold.
Name
Hold
Megan Bowen
Back
Next


Contoso Electronics
Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Trials
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Core
Advanced
User data search
Information governance
Advanced eDiscovery > Cases > Webinar investigation
Overview
Data sources
Collections
Review sets
Communications
Hold
Processing
Exports
Jobs
Settings
New collection
Refresh
12 items
Search
Filter
Customize colum
Name
Status
Query text
Last run time
Estimate status
Preview status
Irvin content
Estimated
11/29/2021, 1:43:29 PM
Successful
All Teams messages
Estimated
MessageKind:microsoftteams
11/29/2021, 1:56:47 PM
Megan content
Estimated
11/29/2021, 1:57:14 PM
Teams content
Estimated
11/29/2021, 2:14:59 PM
Teams by source
Committed
11/29/2021, 2:18:30 PM
All Teams messages - committed
Committed
11/29/2021, 2:35:50 PM
bazooka
Committed
project bazooka (cs)
11/29/2021, 4:01:27 PM
Pender island
Estimated
pender island
11/29/2021, 4:15:57 PM
pender island 002
Estimation failed
11/30/2021, 10:39:49 AM
Submission failed
pender island 003
11/30/2021, 10:45:02 AM
pender island 004
11/30/2021, 10:51:07 AM
bazooka 002
Adding to review set
12/1/2021, 9:27:44 AM

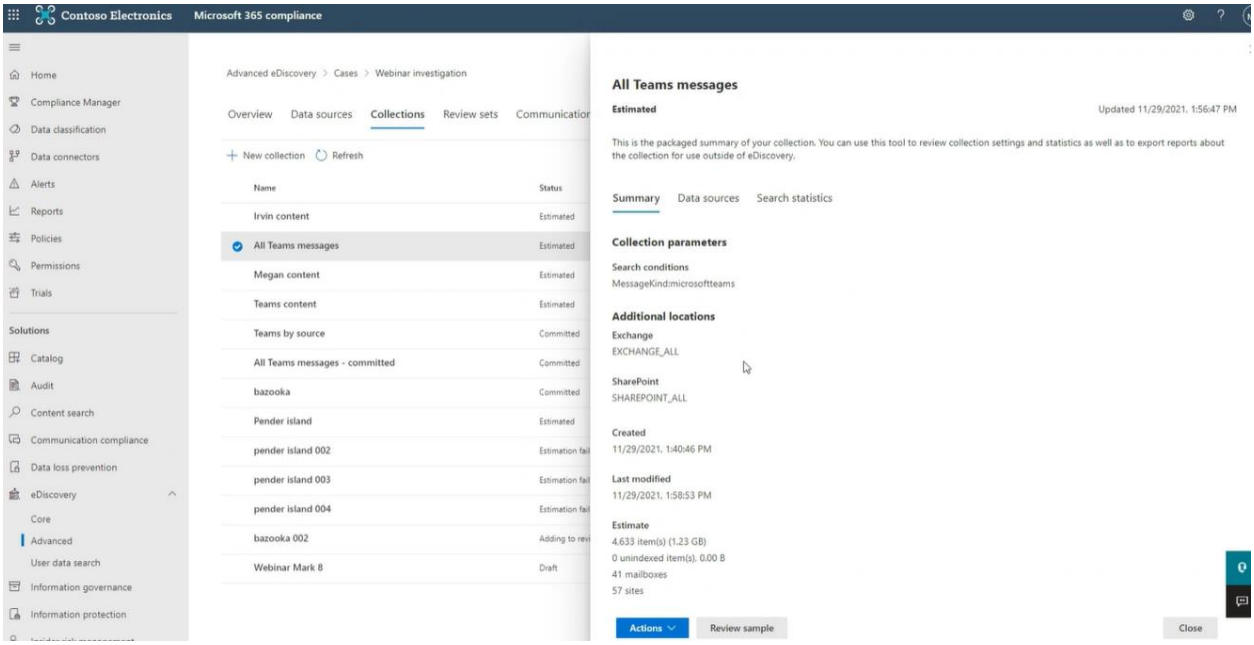

Contoso Electronics
Microsoft 365 compliance
New collection
Name and description
Custodial data sources
Non-custodial data sources
Additional locations
Conditions
Save draft or collect
Review your collection
Additional locations
Status
Location
Included
On
Exchange mailboxes
All
Choose users, groups, or teams
Off
SharePoint sites
Off
Exchange public folders
Back
Next
Exchange mailboxes
Please type minimum 3 characters to get the mailbox list.
Search
27 items
Name
Email address
Conf Room Stevens
Lee Gu
Lidia Holloway
Diego Siciliani
Conf Room Rainier
Allan Deyoung
Pradeep Gupta
Adele Vance
Johanna Lorenz
Miriam Graham
Patti Fernandez
Joni Sherman
Conf Room Hood
Done
Cancel

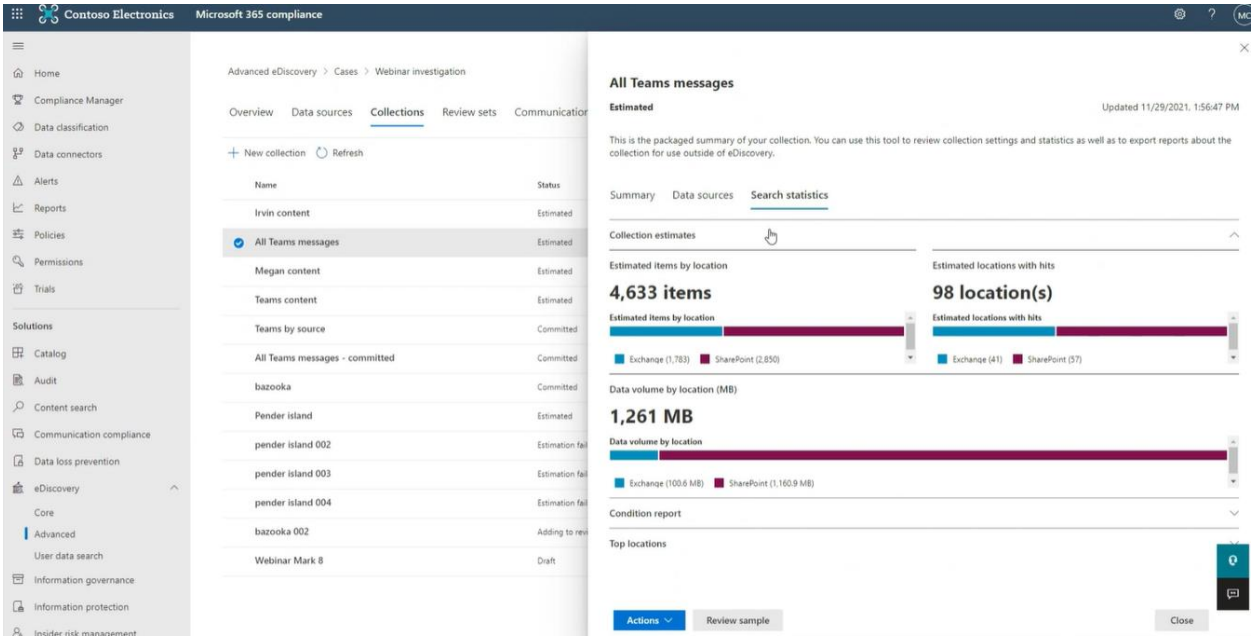

Contoso Electronics
Microsoft 365 compliance
New collection
Name and description
Custodial data sources
Non-custodial data sources
Additional locations
Conditions
Save draft or collect
Review your collection
Define your collection conditions
These are the search conditions that will apply to the custodial and non-custodial data sources you identified in earlier steps and will populate your collection.
Enter keywords or use the keyword list. You can also add conditions to narrow your results. Learn more
Query language-country/region: None
Condition card builder
KQL editor
webinar(c:c)(kind=microsoftteams)
0 errors detected
Back
Next

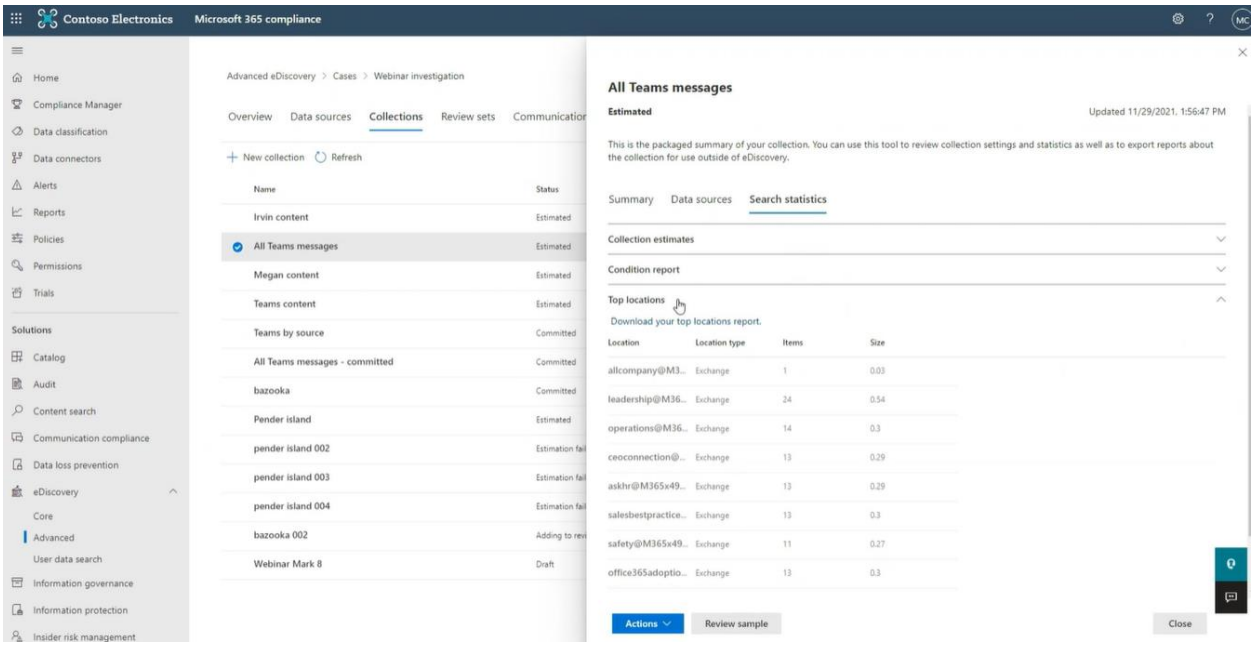

Contoso Electronics
Microsoft 365 compliance
New collection
Name and description
Custodial data sources
Non-custodial data sources
Additional locations
Conditions
Save draft or collect
Review your collection
Save as draft or add to review set
Decide whether you want to save your collection as a draft or immediately collect items and add them to a review set. Learn more
Save collection as draft
Collection will be saved for further review and refinement, but results won't be committed to a review set. The draft will contain estimated collection results and a preview that you can review to validate the size and scope before committing to a review set.
Collect items and add to review set
Collection will immediately gather items and add them to a review set. You can configure additional settings below to refine your collection.
Add to new review set
Review set name
Enter a name for your review set
Add to existing review set
Teams review RS1
Additional collection settings
These collection parameters will only apply to new items that haven't been collected in this case. Options that are selected by default and disabled are assigned by the case format.
Collect contextual Teams and Yammer messages around your search results
Collect cloud attachments from items found in your search results
Collect partially indexed items related to your search results
Collect all versions of SharePoint items (doing this can significantly increase the volume of items added to your review set)
Collection ingestion scale
Add all of collection to review set
Back
Next


Contoso Electronics
Microsoft 365 compliance
New collection
Name and description
Custodial data sources
Non-custodial data sources
Additional locations
Conditions
Save draft or collect
Review your collection
Review your collection and create it
Submitting...
Review your settings, data sources, and search criteria.
Summary
Data source
Name and description
Name
Webinar Mark 8
Edit
Search criteria
webinar(c:c)(kind=microsoftteams)
Edit
Locations
Exchange
EXCHANGE_ALL
Edit
Save as draft or add to review set
Save collection as draft
Edit

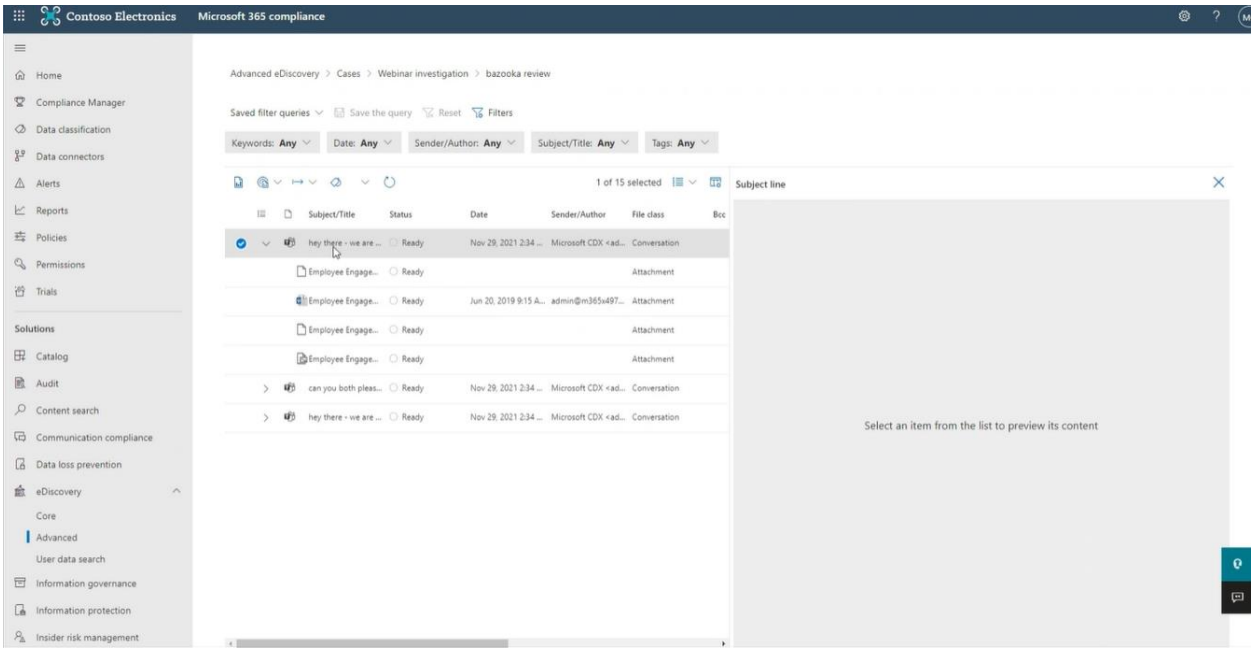
## 4.4.7.4. Review experience

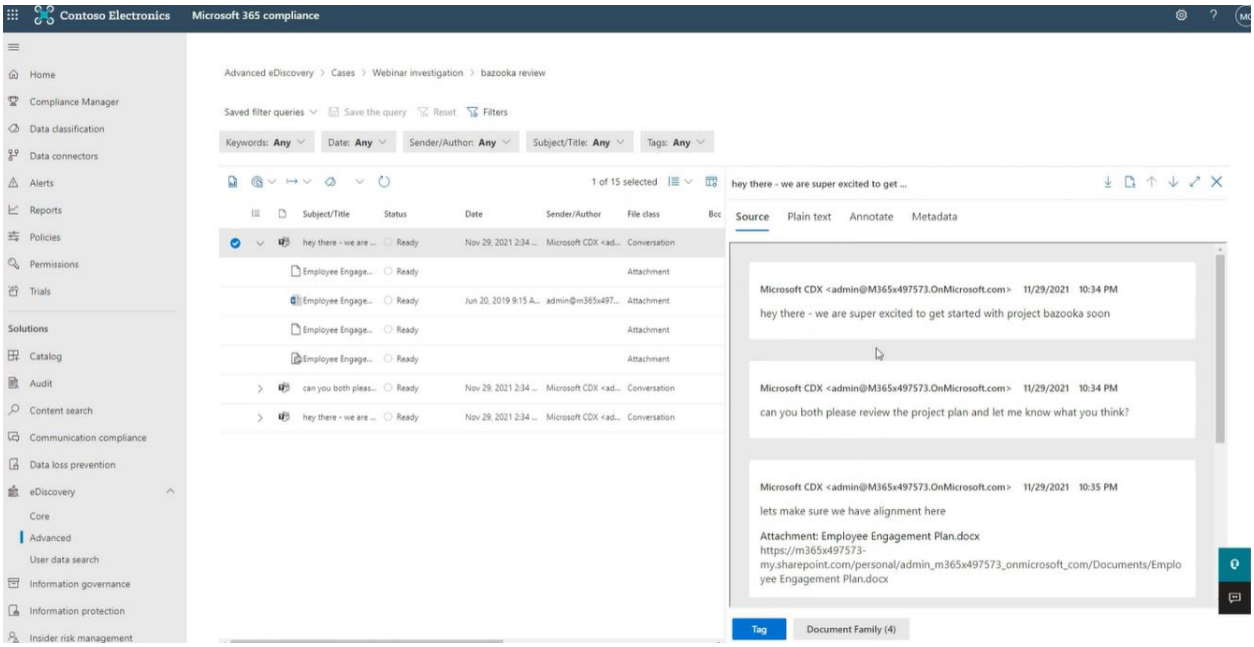


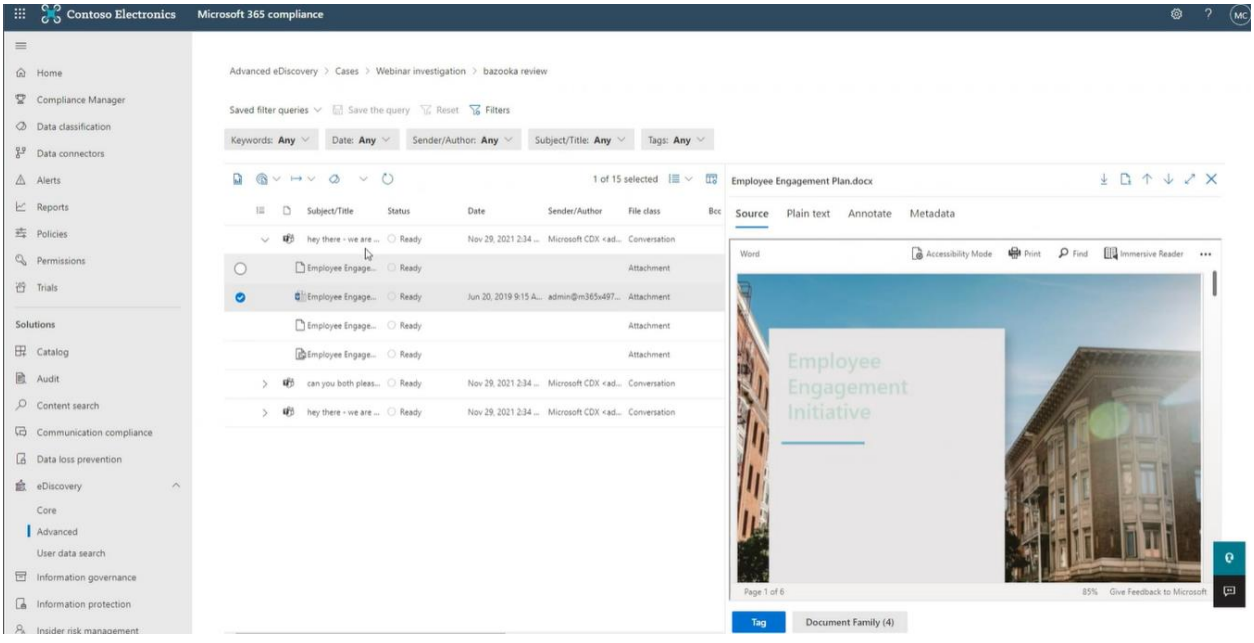



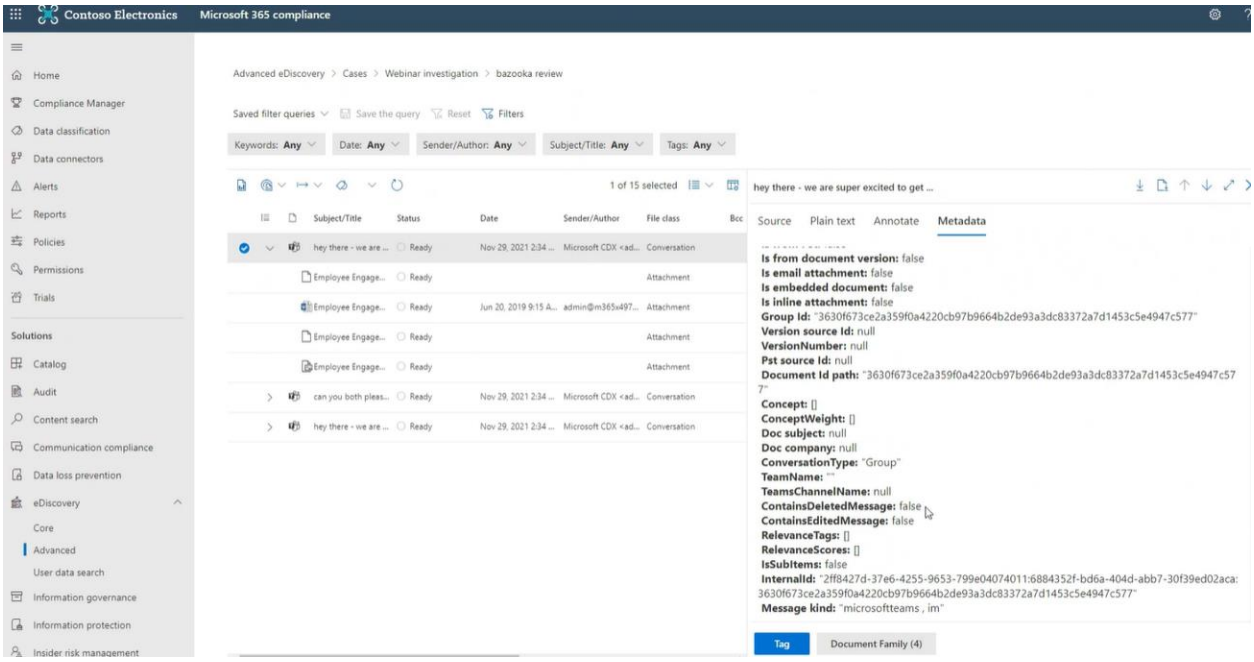


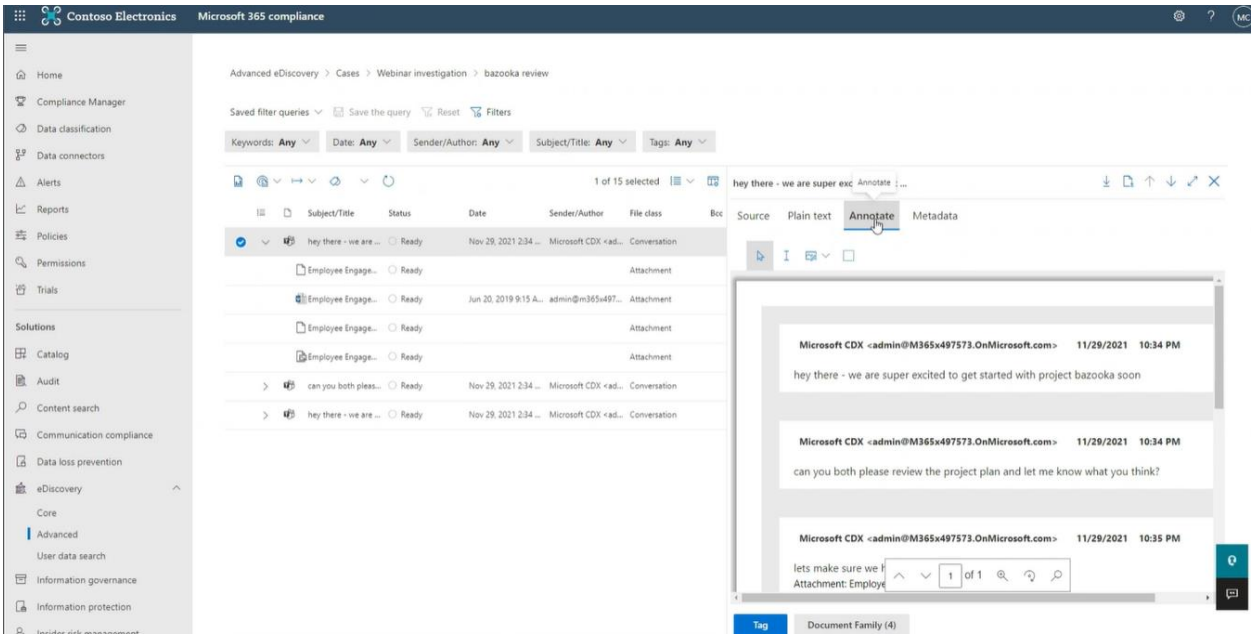

## 4.4.7.4.1. Review Set

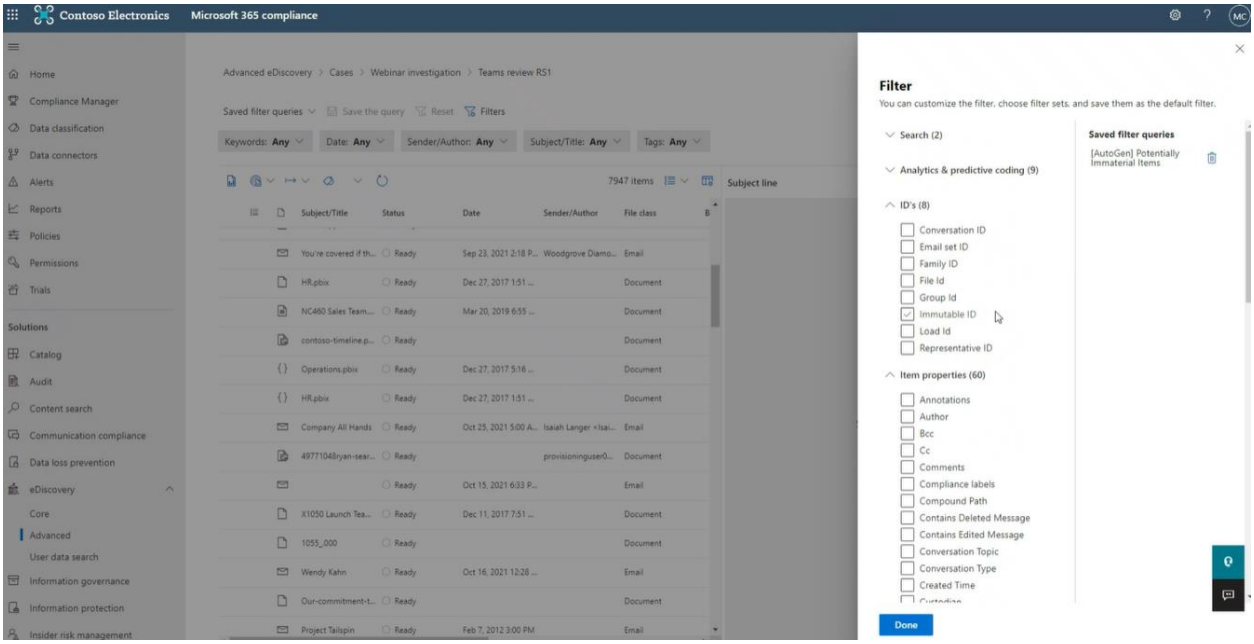


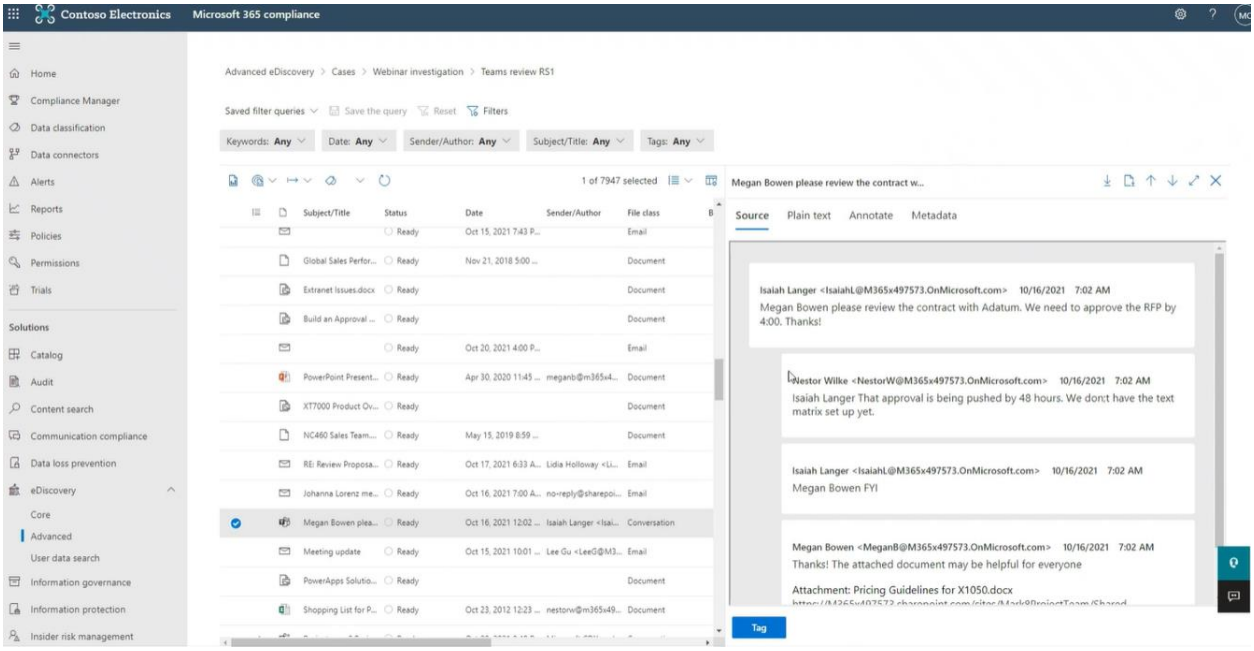

Contoso Electronics
Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Trials
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Core
Advanced
User data search
Information governance
Information protection
Insider risk management
Advanced eDiscovery > Cases > Webinar investigation > bazooka review
Saved filter queries
Save the query
Reset
Filters
Keywords: Any
Date: Any
Sender/Author: Any
Subject/Title: Any
Tags: Any
1 of 15 selected
Subject/Title
Status
Date
Sender/Author
File class
hey there - we are super excited to get ...
Source
Plain text
Annotate
Metadata
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:34 PM
hey there - we are super excited to get started with project bazooka soon
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:34 PM
can you both please review the project plan and let me know what you think?
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:35 PM
lets make sure we have alignment here
Attachment: Employee Engagement Plan.docx
https://m365x497573-my.sharepoint.com/personal/admin_m365x497573_onmicrosoft_com/Documents/Employee Engagement Plan.docx
Tag
Document Family (4)

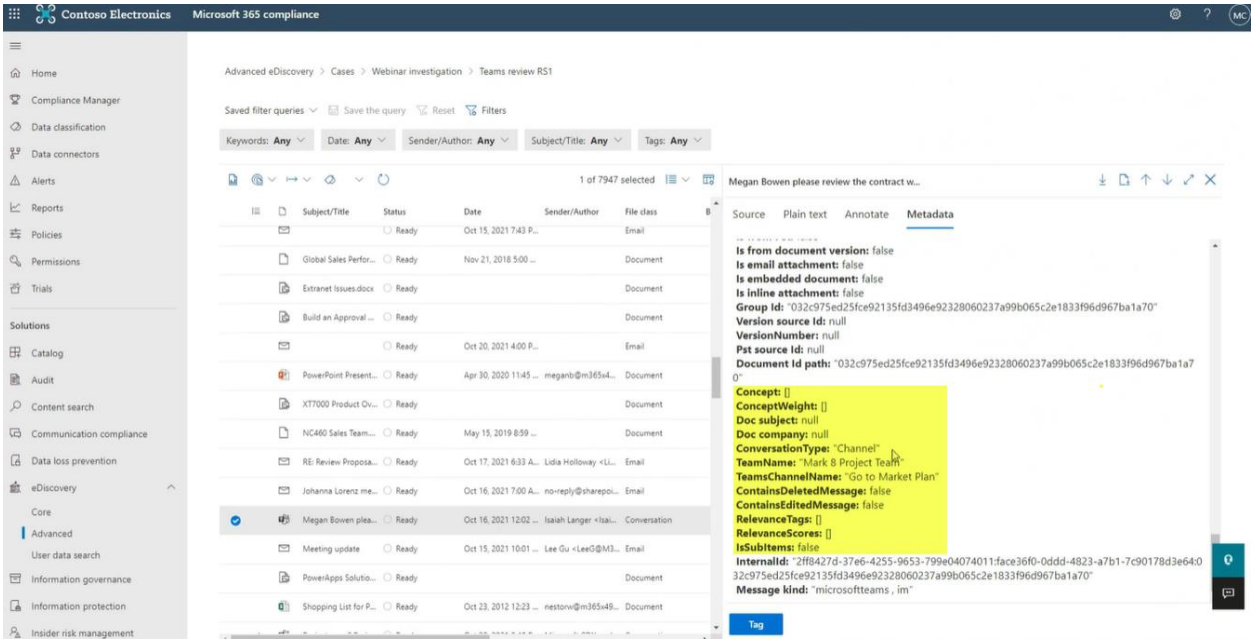

Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > bazooka review
Saved filter queries
Save the query
Reset
Filters
Keywords: Any
Date: Any
Sender/Author: Any
Subject/Title: Any
Tags: Any
1 of 15 selected
Employee Engagement Plan.docx
Source
Plain text
Annotate
Metadata
Word
Accessibility Mode
Print
Find
Immersive Reader
Employee Engagement Initiative
Page 1 of 6
85%
Give Feedback to Microsoft
Tag
Document Family (4)

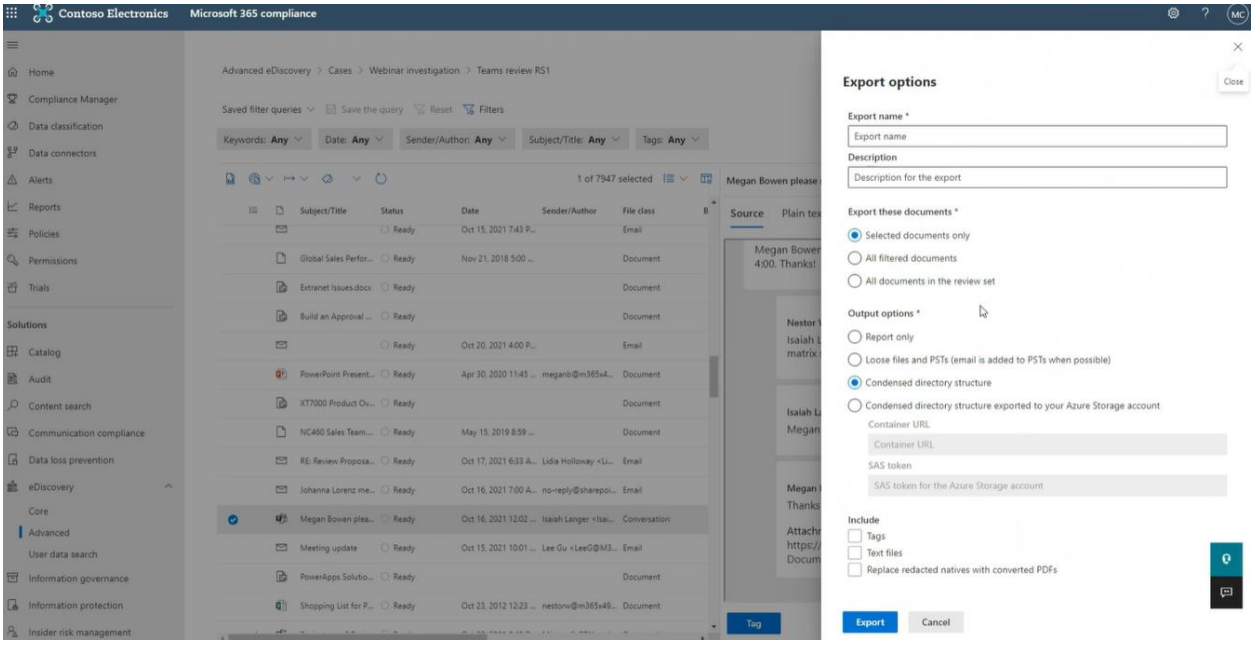

Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > bazooka review
Saved filter queries
Save the query
Reset
Filters
Keywords: Any
Date: Any
Sender/Author: Any
Subject/Title: Any
Tags: Any
1 of 15 selected
Subject/Title
Status
Date
Sender/Author
File class
hey there - we are super excited to get ...
Source
Plain text
Annotate
Metadata
Is from document version: false
Is email attachment: false
Is embedded document: false
Is inline attachment: false
Group Id: "3630f673ce2a359f0a4220cb97b9664b2de93a3dc83372a7d1453c5e4947c577"
Version source Id: null
VersionNumber: null
Pst source Id: null
Document Id path: "3630f673ce2a359f0a4220cb97b9664b2de93a3dc83372a7d1453c5e4947c577"
Concept: []
ConceptWeight: []
Doc subject: null
Doc company: null
ConversationType: "Group"
TeamName: ""
TeamsChannelName: null
ContainsDeletedMessage: false
ContainsEditedMessage: false
RelevanceTags: []
RelevanceScores: []
IsSubItems: false
InternalId: "2ff8427d-37e6-4255-9653-799e04074011:6884352f-bd6a-404d-abb7-30f39ed02aca:3630f673ce2a359f0a4220cb97b9664b2de93a3dc83372a7d1453c5e4947c577"
Message kind: "microsoftteams , im"
Tag
Document Family (4)
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Trials
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Core
Advanced
User data search
Information governance
Information protection


Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > bazooka review
Source
Plain text
Annotate
Metadata
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:34 PM
hey there - we are super excited to get started with project bazooka soon
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:34 PM
can you both please review the project plan and let me know what you think?
Microsoft CDX <admin@M365x497573.OnMicrosoft.com> 11/29/2021 10:35 PM
1 of 1
Tag
Document Family (4)


Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > Teams review RS1
Filter
You can customize the filter, choose filter sets, and save them as the default filter.
Search (2)
Analytics & predictive coding (9)
ID's (8)
Conversation ID
Email set ID
Family ID
File Id
Group Id
Immutable ID
Load Id
Representative ID
Item properties (60)
Annotations
Author
Bcc
Cc
Comments
Compliance labels
Compound Path
Contains Deleted Message
Contains Edited Message
Conversation Topic
Conversation Type
Created Time
Saved filter queries
[AutoGen] Potentially Immaterial Items
Done

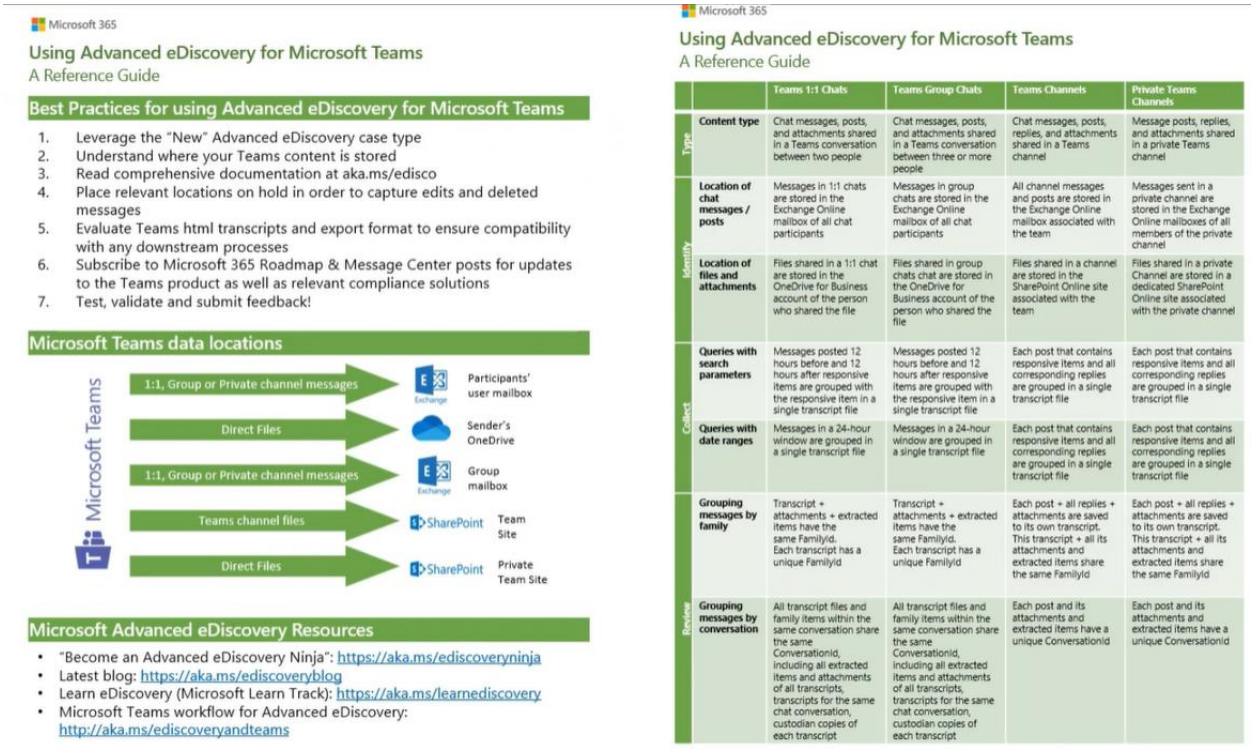

Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > Teams review RS1
Megan Bowen please review the contract w...
Source
Plain text
Annotate
Metadata
Isaiah Langer <IsaiahL@M365x497573.OnMicrosoft.com> 10/16/2021 7:02 AM
Megan Bowen please review the contract with Adatum. We need to approve the RFP by 4:00. Thanks!
Nestor Wilke <NestorW@M365x497573.OnMicrosoft.com> 10/16/2021 7:02 AM
Isaiah Langer That approval is being pushed by 48 hours. We don;t have the text matrix set up yet.
Isaiah Langer <IsaiahL@M365x497573.OnMicrosoft.com> 10/16/2021 7:02 AM
Megan Bowen FYI
Megan Bowen <MeganB@M365x497573.OnMicrosoft.com> 10/16/2021 7:02 AM
Thanks! The attached document may be helpful for everyone
Attachment: Pricing Guidelines for X1050.docx
Tag


Contoso Electronics
Microsoft 365 compliance
Advanced eDiscovery > Cases > Webinar investigation > Teams review RS1
Megan Bowen please review the contract w...
Source
Plain text
Annotate
Metadata
Is from document version: false
Is email attachment: false
Is embedded document: false
Is inline attachment: false
Group Id: "032c975ed25fce92135fd3496e92328060237a99b065c2e1833f96d967ba1a70"
Version source Id: null
VersionNumber: null
Pst source Id: null
Document Id path: "032c975ed25fce92135fd3496e92328060237a99b065c2e1833f96d967ba1a70"
Concept: []
ConceptWeight: []
Doc subject: null
Doc company: null
ConversationType: "Channel"
TeamName: "Mark 8 Project Team"
TeamsChannelName: "Go to Market Plan"
ContainsDeletedMessage: false
ContainsEditedMessage: false
RelevanceTags: []
RelevanceScores: []
IsSubItems: false
InternalId: "2ff8427d-37e6-4255-9653-799e04074011:face36f0-0ddd-4823-a7b1-7c90178d3e64:032c975ed25fce92135fd3496e92328060237a99b065c2e1833f96d967ba1a70"
Message kind: "microsoftteams , im"
Tag


Contoso Electronics
Microsoft 365 compliance
Export options
Export name *
Export name
Description
Description for the export
Export these documents *
Selected documents only
All filtered documents
All documents in the review set
Output options *
Report only
Loose files and PSTs (email is added to PSTs when possible)
Condensed directory structure
Condensed directory structure exported to your Azure Storage account
Container URL
SAS token
SAS token for the Azure Storage account
Include
Tags
Text files
Replace redacted natives with converted PDFs
Export
Cancel

# 7 Best Practices for using Adv eDiscovery with MS Teams

1. Leverage the "New" Advanced eDiscovery case type
2. Understand where your Teams content is stored
3. Read comprehensive documentation at aka.ms/edisco
4. Place relevant locations on hold in order to capture edits and deleted messages
5. Evaluate Teams html transcripts and export format to ensure compatibility with any downstream processes
6. Subscribe to Microsoft 365 Roadmap & Message Center posts for updates to Teams and our M365 compliance solutions
7. Test, validate and submit feedback!



Microsoft 365

Using Advanced eDiscovery for Microsoft Teams

A Reference Guide

**Best Practices for using Advanced eDiscovery for Microsoft Teams**

1. Leverage the "New" Advanced eDiscovery case type
2. Understand where your Teams content is stored
3. Read comprehensive documentation at aka.ms/edisco
4. Place relevant locations on hold in order to capture edits and deleted messages
5. Evaluate Teams html transcripts and export format to ensure compatibility with any downstream processes
6. Subscribe to Microsoft 365 Roadmap & Message Center posts for updates to the Teams product as well as relevant compliance solutions
7. Test, validate and submit feedback!

**Microsoft Teams data locations**



**Microsoft Advanced eDiscovery Resources**

- "Become an Advanced eDiscovery Ninja": https://aka.ms/ediscoveryninja
- Latest blog: https://aka.ms/ediscoveryblog
- Learn eDiscovery (Microsoft Learn Track): https://aka.ms/learnediscovery
- Microsoft Teams workflow for Advanced eDiscovery: http://aka.ms/ediscoveryandteams

Microsoft 365

Using Advanced eDiscovery for Microsoft Teams

A Reference Guide

| | | Teams 1:1 Chats | Teams Group Chats | Teams Channels | Private Teams Channels |
|---|---|---|---|---|---|
| Type | Content type | Chat messages, posts, and attachments shared in a Teams conversation between two people | Chat messages, posts, and attachments shared in a Teams conversation between three or more people | Chat messages, posts, replies, and attachments shared in a Teams channel | Message posts, replies, and attachments shared in a private Teams channel |
| Identify | Location of chat messages / posts | Messages in 1:1 chats are stored in the Exchange Online mailbox of all chat participants | Messages in group chats are stored in the Exchange Online mailbox of all chat participants | All channel messages and posts are stored in the Exchange Online mailbox associated with the team | Messages sent in a private channel are stored in the Exchange Online mailboxes of all members of the private channel |
| | Location of files and attachments | Files shared in a 1:1 chat are stored in the OneDrive for Business account of the person who shared the file | Files shared in group chats chat are stored in the OneDrive for Business account of the person who shared the file | Files shared in a channel are stored in the SharePoint Online site associated with the team | Files shared in a private Channel are stored in a dedicated SharePoint Online site associated with the private channel |
| Collect | Queries with search parameters | Messages posted 12 hours before and 12 hours after responsive items are grouped with the responsive item in a single transcript file | Messages posted 12 hours before and 12 hours after responsive items are grouped with the responsive item in a single transcript file | Each post that contains responsive items and all corresponding replies are grouped in a single transcript file | Each post that contains responsive items and all corresponding replies are grouped in a single transcript file |
| | Queries with date ranges | Messages in a 24-hour window are grouped in a single transcript file | Messages in a 24-hour window are grouped in a single transcript file | Each post that contains responsive items and all corresponding replies are grouped in a single transcript file | Each post that contains responsive items and all corresponding replies are grouped in a single transcript file |
| Review | Grouping messages by family | Transcript + attachments + extracted items have the same FamilyId. Each transcript has a unique FamilyId | Transcript + attachments + extracted items have the same FamilyId. Each transcript has a unique FamilyId | Each post + all replies + attachments are saved to its own transcript. This transcript + all its attachments and extracted items share the same FamilyId | Each post + all replies + attachments are saved to its own transcript. This transcript + all its attachments and extracted items share the same FamilyId |
| | Grouping messages by conversation | All transcript files and family items within the same conversation share the same ConversationId, including all extracted items and attachments of all transcripts, transcripts for the same chat conversation, custodian copies of each transcript | All transcript files and family items within the same conversation share the same ConversationId, including all extracted items and attachments of all transcripts, transcripts for the same chat conversation, custodian copies of each transcript | Each post and its attachments and extracted items have a unique ConversationId | Each post and its attachments and extracted items have a unique ConversationId |

## 4.4.8. Knowledge Check eDiscovery and Audit

### 4.4.8.1. Question 1.

A new admin has joined the compliance team and needs access to Core eDiscovery to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned?

- Add them as a member of the eDiscovery Manager role group.

- Add them as a member of the eDiscovery review role.
- Add them as a member of the eDiscovery custodian role.

#### 4.4.8.2. Question 2.

The compliance team needs to perform more advanced, complex, and repetitive content search tasks. What can enable the team to do more complex search tasks?

- Use the Microsoft 365 autocontent search client.
- Use the continuous eDiscovery autosearch client.
- Use the PowerShell scripts provided by Microsoft.

#### 4.4.8.3. Question 3.

The compliance admin has been asked to use Advanced eDiscovery to help a legal team that is working on a case. What is the workflow the admin will use?

- Search custodial data, add custodians to a case, add data to a review set, review and analyze data, then finally export and download case data.
- Add custodians to a case, search custodial sources for relevant data, add data to a review set, review and analyze data, then finally export and download the case data.
- Add data to a review set, review and analyze data, add custodians to a case, search custodial sources for relevant data, then finally export and download the case data.

#### 4.4.8.4. Question 4.

The audit team needs to conduct compliance investigations across emails. They need access to crucial events, such as when mail items were accessed, when mail items were replied to and forwarded. What capability can the team use?

- Use Advanced Auditing so that you access and investigate those events.
- Use Core Auditing so that you can access and investigate those events.
- Use alert policies to generate and view alerts on when users perform certain actions on emails.

## 4.5. Describe Resource Governance Capabilities in Azure

Azure has the capabilities that admins need to ensure that resources are governed properly, that they're secure, and in line with the organization's compliance requirements.

In this module, you'll learn about the resource governance capabilities available for Azure.

After completing this module, you should be able to:

- Describe the capabilities of Azure resource locks.
- Describe the function of Azure Blueprints.
- Describe how Azure policy helps organizations assess compliance.

## 4.5.1. Describe The Use Of Azure Resource Manager Locks

Before we can describe the use of Azure resource locks, it's important to understand what Azure Resource Manager is. Azure Resource Manager is the deployment and management service for Azure. Azure Resources Manager provides a management layer that enables administrators to create, update, and delete resources in an Azure account. Admins can use management features such as resource locks to secure resources after deployment.

Resource locks are used to prevent resources from being accidentally deleted or changed. Even with role-based access control policies in place, there's still a risk that people with the correct level of access could delete a critical resource. Azure resource locks prevent users from accidentally deleting or modifying a critical resource, and can be applied to a subscription, a resource group, or a resource.

For example, there may be times when an administrator needs to lock a subscription, a resources group, or a resource. In these situations, a lock would be applied to prevent users from accidentally deleting or modifying a critical resource.

### 4.5.1.1. Lock types

A lock level can be set to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

#### 4.5.1.1.1. CanNotDelete

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

#### 4.5.1.1.2. ReadOnly

ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

### 4.5.1.2. One Lock Per Resource

A resource can have more than one lock. For example, a resource may have a ReadOnly lock and a CanNotDelete lock. When you apply a lock at a parent scope, all resources within that scope inherit that lock. Even resources you add later inherit the lock from the parent. The most restrictive lock in the inheritance takes precedence.

Resource Manager locks apply only to operations that happen in the management plane. The locks don't restrict how resources complete their functions. If a lock is applied, changes to the actual resource are restricted, but resource operations aren't restricted. For example, a ReadOnly lock on an Azure SQL Database logical server prevents deletion or modification of the server. However, it doesn't prevent you from creating, updating, or deleting data in the databases on that server.

### 4.5.2. Describe The Use Of Azure Blueprints

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

Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, whatever region Azure Blueprints deploys your resources to.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments.

Azure Blueprints helps ensure Azure resources are deployed in a way that's in line with compliance requirements. However, a service like Azure Policy should be used to continuously monitor resources and ensure a continuation with compliance requirements.

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

#### 4.5.2.1. Role Assignments
#### 4.5.2.2. Policy Assignments
#### 4.5.2.3. Azure Resource Manager templates (ARM templates)
#### 4.5.2.4. Resource Groups

### 4.5.3. Describe Azure Policy

Azure Policy is designed to help enforce standards and assess compliance across your organization. Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment. You can drill down to a per-resource, or per-policy level granularity. You can also use capabilities like bulk remediation for existing resources and automatic remediation for new resources, to resolve issues rapidly and effectively. Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.

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

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

#### 4.5.3.1. Evaluation outcomes

Azure Policy evaluates resources at specific times during the resource lifecycle and the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following events or times will trigger an evaluation:

1. A resource has been created, deleted, or updated in scope with a policy assignment.
2. A policy or an initiative is newly assigned to a scope.
3. A policy or an initiative that's been assigned to a scope is updated.
4. The standard compliance evaluation cycle (happens once every 24 hours).

Organizations will vary in how they respond to non-compliant resources. Here's some examples:

1. Deny a change to a resource.
2. Log changes to a resource.
3. Alter a resource before or after a change.
4. Deploy related compliant resources.

With Azure Policy, responses like these are made possible by using effects, which are specified in policy definitions.

#### 4.5.3.2. Azure Policy Vs. Azure role-based access control (RBAC)

It’s important not to confuse Azure Policy and Azure RBAC.

##### 4.5.3.2.1. Azure Policy

You use Azure Policy to ensure that the resource state is compliant to your organization’s business rules, no matter who made the change or who has permission to make changes. Azure Policy will evaluate the state of a resource, and act to ensure the resource stays compliant.

##### 4.5.3.2.2. Azure RBAC

Azure RBAC focuses instead on managing user actions at different scopes. Azure RBAC manages who has access to Azure resources, what they can do with those resources, and what areas they can

access. If actions need to be controlled, then you would use Azure RBAC. If an individual has access to complete an action, but the result is a non-compliant resource, Azure Policy still blocks the action.

Azure RBAC and Azure Policy should be used together to achieve full scope control in Azure.

### 4.5.4. Knowledge Check For Resource Governance In Azure

#### 4.5.4.1. Question 1.

The compliance admin for the organization wants to ensure that users can access the resources they need, but not accidentally delete resources. Which Azure resource lock level can the admin set to ensure that users can read and modify a resource, but can't delete the resource?

- ReadOnly
- CanNotDelete
- UpdateAndDelete

#### 4.5.4.2. Question 2.

Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization’s compliance requirements?

- Azure Policy
- Azure Rapid Build
- Azure Blueprints

#### 4.5.4.3. Question 3.

As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use?

- Use Azure role-based access control (RBAC).
- Use Azure Policy.
- Use Azure resource locks.