

Mastering Microsoft Defender XDR Deployment

Defender for Identity
Defender for Office 365
Defender for Endpoint
Defender for Cloud Apps
Sentinel
Exposure Management
Security Copilot

Author – Ray Reyes

Defender & Purview, Subject Matter Expert @ Microsoft

Reviewer – Shadab Rasheed

Microsoft Security, Subject Matter Expert @ Microsoft

Disclaimer: This is not an official Microsoft document.

About the author



Ray Reyes is a Senior Microsoft Security Subject Matter Expert at Microsoft. Has over 26+ years in the Tech Industry, have spent the last 15 years dedicated to cybersecurity and data security. After working for 13 years running an International Charity for street-children he co-founded, he joined Microsoft as Subject Matter Expert in Security and Compliance and have been with Microsoft for the last four years. Ray has consistently contributed to the Cyber and Data Security community from being a speaker, presenter and developing comprehensive Microsoft Security and Purview best practice guides. He is currently working on his first Purview book.

Content - High Level Deployment Guide for

- Microsoft Defender for Office 365 (MDO)
- Microsoft Defender for Identity + Microsoft Entra ID Protection = (ITDR)
- Microsoft Defender for Endpoint (MDE)
- Microsoft Defender for Cloud Apps (MDA)
- Microsoft Sentinel
- Exposure Management

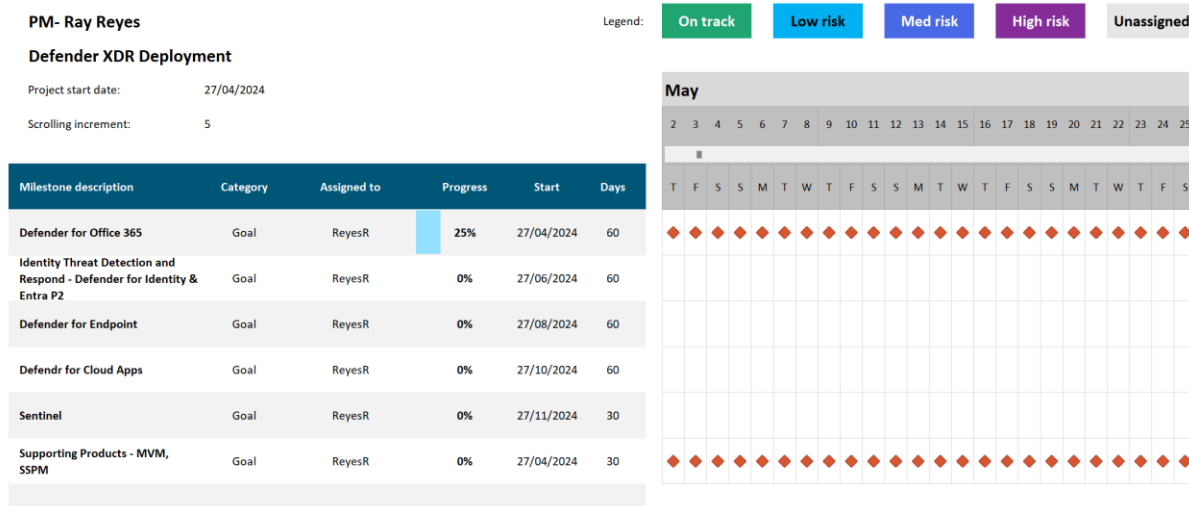
Key mentions

- Security Copilot
- Advanced Hunting

Background

A story goes a long way to support technical deployments. My role at Microsoft is to help customers deploy our Defender and Purview products. One of the feedback items I had a while back from a customer is not knowing 'why they should' turn things on, and this guide answers the WHY. The WHY is what allows customers to re-think and visual what the product is capable of. I work with customers daily across our Security Solutions, this guide is to help customers find the easiest path to enabling our overall Microsoft Defender XDR and to answer two common questions we get in my role.

'Where do I start? What should I turn on first?



An example of a realistic deployment but not a blanket for all as each customer is different from small to large to using internal to external resources to deploy the products.

This document is based on my experience helping customers deploy our Microsoft E5 Security Products across our core Defender stack and Sentinel

This is a blog style guide, which is NOT intended to replace our Microsoft public doc guides or our Advanced Deployment Guide in M365 Admin Portal rather giving customers a different perspective based on my daily customer engagements.

Emphasise that this is a high-level guide to give you direction.

Just like any project plan, our security products should be tested against your environment and applications before you deploy it in bulk. A reminder that some products require a **learning period** from MDI to MDO and MDE, which about a minimum 30 days for Machine Learning to collect any data. MDA anomaly detection has an initial learning period of 7 days during which the Machine Learning learns new user's activity pattern. During the learning period, it's important to have active participation from your users to feedback and help you fine tune policies or at least based your testing during this timeline. As most of our deployment guide, we apply around **Crawl, Jog and Run** approach

Definition of the 3 phases:

Crawl

This phase is to test the technology, usually only involving IT. To test the start to end finish of the deployment process, resolve technical issues before bringing in people from the business and resolve any outstanding issues. Just like with most of our policies, we can scope the users or devices we want to test policies on. From a security perspective, it's important we can produce alerts based on various scenarios, from alerts from a phishing link, from email or Teams to the ability of disabling an account directly from Defender XDR. The Crawl stage of deploying Defender is important because it's the point to also ensure that when the product becomes operational, we can support it. So, one of the key objectives of this stage is to educate the SOC

team on how to support the products. The risk of simply deploying this is, yes you can safeguard the environment but unlikely be able to triage alerts or incidents if the SOC team 1. Misconfigured the setup. 2. Unsure how to action incidents.

Walk

This stage of the project is when you extend the number of users and devices to test. Bring the power users from the business, champions of business-critical apps and add them to this phase to ensure testing of the apps are done appropriately. The Pilot users should feedback on your Change Management (comms, training, adoption plan). In my former years of being a Project Manager, this phase takes the longest cause you're in that grey area of polishing all your test, ticking off all the issue list, potentially educating your IT on how to support the product. From Defender perspective, you can continue just adding users and devices within the scope of the policies. You can start adding VIP devices from an ASR device group as an example. From your SOC perspective, they should see more and more various alerts during this phase. Various products such as MDO, they will start fine tuning configuration, highlighting which are false positives. This is important because once you get to the Run Phase, you want to really minimise the number of false positives at that point.

Run

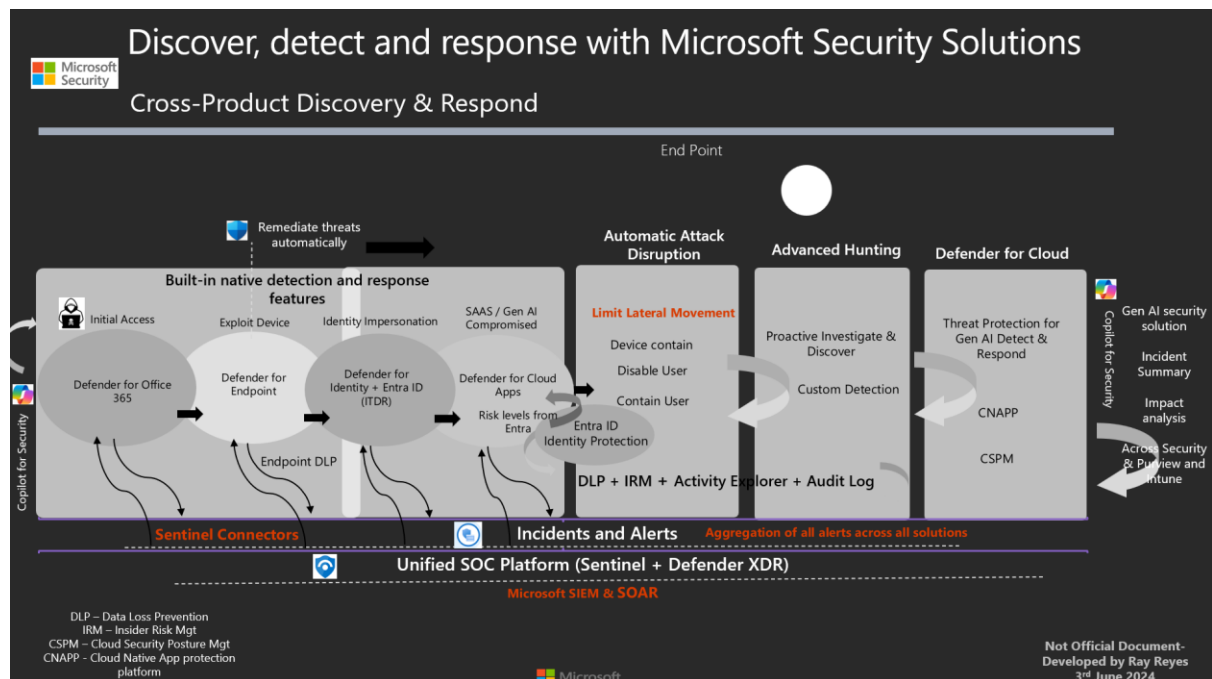
Now, depending on the size of your company. You may just want to add everyone at this stage. But some larger companies, will simply do a bulk deploy. Whether is a 100 users and devices a week, so the impact is mitigated if there was an issue.

What is Microsoft Defender XDR?

Microsoft Defender XDR is a unified pre- and post-breach enterprise defence suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. What will go through on this document is how to deploy all the products that make up enriching our Defender XDR

Benefits of Defender XDR

- Making triaging easier for SOC team
- Key sections of Zero Trust framework
- Enablement of Automatic Attack Disruption
- XDR + Sentinel better together story

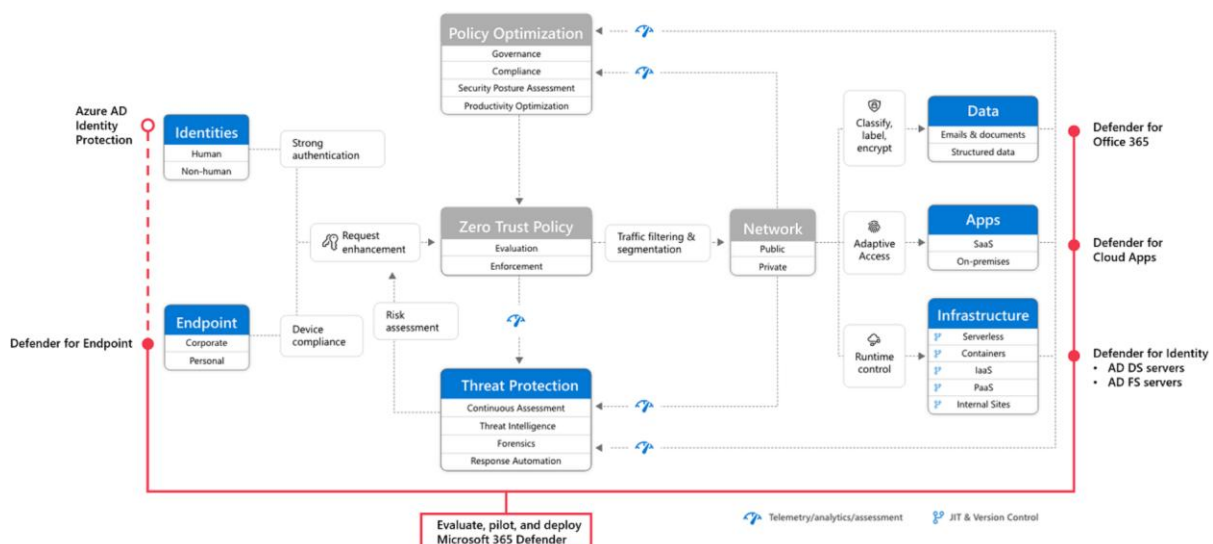


Synergy between each security product helps enable a more powerful detection and respond

Microsoft Defender XDR helps you apply the principles of Zero Trust.

In the illustration: Microsoft Defender XDR provides XDR capabilities for protecting:

- Endpoints, including laptops and mobile devices
- Data in Office 365, including email
- Cloud apps, including other SaaS apps that your organization uses
- On-premises Active Directory Domain Services (AD DS) and Active Directory Federated Services (AD FS) servers



Microsoft Defender XDR services protect:

Endpoints with Defender for Endpoint - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.

Security Recommendations with Microsoft Defender Vulnerability Management - Microsoft Defender Vulnerability Management delivers continuous asset visibility, intelligent risk-based assessments, and built-in remediation tools to help your security and IT teams prioritize and address critical vulnerabilities and misconfigurations across your organization.

Email and collaboration with Defender for Office 365 - Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools such as Microsoft Teams, SharePoint & OneDrive.

Identities with Defender for Identity and Microsoft Entra ID Protection (ITDR) – ITDR gives you a holistic protection of your on-prem identities and cloud identities. With an approach, it leverages native detection and responds to threats and alerts.

Applications with Defender for Cloud Apps - Microsoft Defender for Cloud Apps is a comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.

Cross-product threat hunting - Security teams can leverage their unique organizational knowledge to hunt for signs of compromise by creating their own custom queries over the raw data collected by the various protection products. Microsoft Defender XDR provides query-based access to 30 days of historic raw signals and alert data across endpoint and Defender for Office 365 data, MDI and MDA

Scenario Story

The story we will follow for this guide is a **customer that is migrating from our Defender stack** (of course you can also use this guide if you're completely evergreen). The customer is currently using some 3rd party protection in all pillars like endpoint, email protection, let's assume they also have identity on-prem but don't have any on-prem identity protection, let's also assume they have a tonne of internal and 3rd party application but no governance and ways to confirm that configuration is done probably. Lastly, they have MFA and some Conditional Access enabled but haven't leveraged P2 capabilities in Entra even though they're licensed for it.

Customer 'We've just upgraded to E5, but which one do we deploy first'?

In many of my customer scenarios, they may have various vendors that protect different pillars like email protection, endpoint protection, identity, SaaS and all have a different license expiration. Therefore, in many cases, they will use the license expiration to decide which pillar needs to migrate first which makes sense from a cost perspective. That approach doesn't mess

the whole XDR component, if we eventually enable all the products to get that full enrich XDR experience.

Important note: Keep a reset mindset. What customers often try to do is feature match their **current protection against the Microsoft Defender XDR. Remember, it's a totally different** product, different platform, a lot more natively built-in integration, and we just do things slightly differently, we detect differently, we process logs differently, we can engineer our detection faster or enable them in the OS (*we own windows so things do get engineered fast*) and features might be different.

Another key takeaway and one I often come across with customers, it's how the migration is 'urgent' so the deployment timeline is 'aggressive' migration. The downside is, there is no time for change management, no time for machine learning to kick in, no time for a 'phase' deployment, no time for pilot users to feedback issues or report false positives or assess reports. So, if you're a customer who's reading this, plan this like a normal business project, have a project manager involved, resource it properly, give some time for testing and fine tuning. Don't make this an urgent migration and blame the product. Just like any project you rush; you're putting it at risk. So, keep that in mind.

IF we look at a common Attack Kill Chain. The most common initial access to an environment is through Phishing emails, and every year, from the moment emails matured enough to be the number source of communication, it's still the most common attacks. There is a tonne of various techniques from your credential harvesting technique to more sophisticated ones like QR Code

Microsoft Defender XDR Unified role-based access control (RBAC)

Full details for the Unified RBAC [Details of custom permissions in Microsoft Defender XDR Unified role-based access control \(RBAC\) - Microsoft Defender XDR | Microsoft Learn](#)

There are three key roles in the XDR Portal, Security Operations, Security Posture and Authorization and Settings. However, when creating the roles and groups, you can create multiple groups if you have different levels of SOC and their responsibilities

Security Operations permissions

Choose permissions

Select permissions from each permission group

Permission group

- ☒ **Security operations**
None selected
- ☐ **Security posture**
None selected
- ☐ **Authorization and settings**
None selected

Security operations

Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories.

☐ All read-only permissions

☐ All read and manage permissions

☐ Select custom permissions

Security data

☐ Read-only

☐ Select all permissions

☐ Select custom permissions

- ☐ Security data basics (read)
- ☐ Alerts (manage)
- ☐ Response (manage)
- ☐ Basic live response (manage)
- ☐ Advanced live response (manage)
- ☐ File collection (manage)
- ☐ Email & collaboration quarantine (manage)
- ☐ Email & collaboration advanced actions (manage)
- ☐ Security Copilot (read)

Raw data (Email & collaboration)

☐ Read-only

☐ Select custom permissions

- ☐ Email & collaboration metadata (read)
- ☐ Email & collaboration content (read)

Security Posture Permissions

Choose permissions

Select permissions from each permission group

Permission group

- ☐ **Security operations**
None selected
- ☒ **Security posture**
None selected
- ☐ **Authorization and settings**
None selected

Security posture

Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.

☐ All read-only permissions

☐ All read and manage permissions

☐ Select custom permissions

Posture management

☐ Read-only

☐ Select all permissions

☐ Select custom permissions

- ☐ Vulnerability management (read)
- ☐ Exception handling (manage)
- ☐ Remediation handling (manage)
- ☐ Exposure Management (read)
- ☐ Exposure Management (manage)

Authorization and Settings permissions

The screenshot shows the 'Choose permissions' and 'Authorization and settings' panels in the Microsoft Defender XDR console. The 'Choose permissions' panel on the left lists three permission groups: 'Security operations' (None selected), 'Security posture' (None selected), and 'Authorization and settings' (None selected). The 'Authorization and settings' panel on the right contains a warning message, a 'Clear all permissions' button, and three radio button options: 'All read-only permissions', 'All read and manage permissions', and 'Select custom permissions'. Below these are sections for 'Authorization', 'Security settings', and 'System settings', each with radio button options for 'Read-only' and 'Read and manage'. A red box highlights the 'Authorization and settings' permission group in the 'Choose permissions' panel and the 'Authorization and settings' panel on the right.

Choose permissions

Select permissions from each permission group.

Permission group

- Security operations
None selected
- Security posture
None selected
- Authorization and settings
None selected

Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

ⓘ If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

✕ Clear all permissions

☐ All read-only permissions

☐ All read and manage permissions

☐ Select custom permissions

Authorization

☐ Read-only

☐ Read and manage

Security settings

☐ Read-only

☐ Select all permissions

☐ Select custom permissions

☐ Detection tuning (manage)

☐ Core security settings (read)

☐ Core security settings (manage)

System settings

☐ Read-only

☐ Read and manage

Back Next Apply Cancel

Unified – Security - Permissions

The screenshot shows the 'Permissions' page in the Microsoft Defender console. The page title is 'Permissions' and it includes a subtitle: 'Admins are users added to the admin role, and can view any data and complete any task in the Microsoft Defender portal. You should have few admins, and grant users only the permissions needed to perform their duties when you assign access.' The page lists 7 items, which are roles and their descriptions. The roles are: Microsoft Defender XDR (1), Microsoft Entra ID (1), Endpoints roles & groups (2), Email & collaboration roles (1), and Cloud Apps (2). The descriptions for each role are provided in the 'Description' column.

Name	Description
Microsoft Defender XDR (1)	
Roles	Manage who has access to view tasks and take actions in Microsoft Defender XDR. Assign only the minimum permissions that admins need to get the job done.
Microsoft Entra ID (1)	
Roles	Manage who has access to view tasks and take actions in the Microsoft Defender portal. Assign them only the permissions needed to perform their duties.
Endpoints roles & groups (2)	
Roles	Manage endpoint access to view content and perform tasks. Grant only the permissions needed for users to perform their tasks.
Device groups	Organize devices into groups, set automated remediation levels, and assign administrators as needed.
Email & collaboration roles (1)	
Roles	Manage who in your organization has access to view email and collaboration content and take actions. Grant only the permissions needed for users to perform their tasks.
Cloud Apps (2)	
Roles	Manage who has access to view cloud apps content and take actions. Assign them only the permissions needed to perform their duties.
Activity Privacy Permissions	Control which admins can reveal private activities.

A mind map to Defender XDR Roles and Permissions

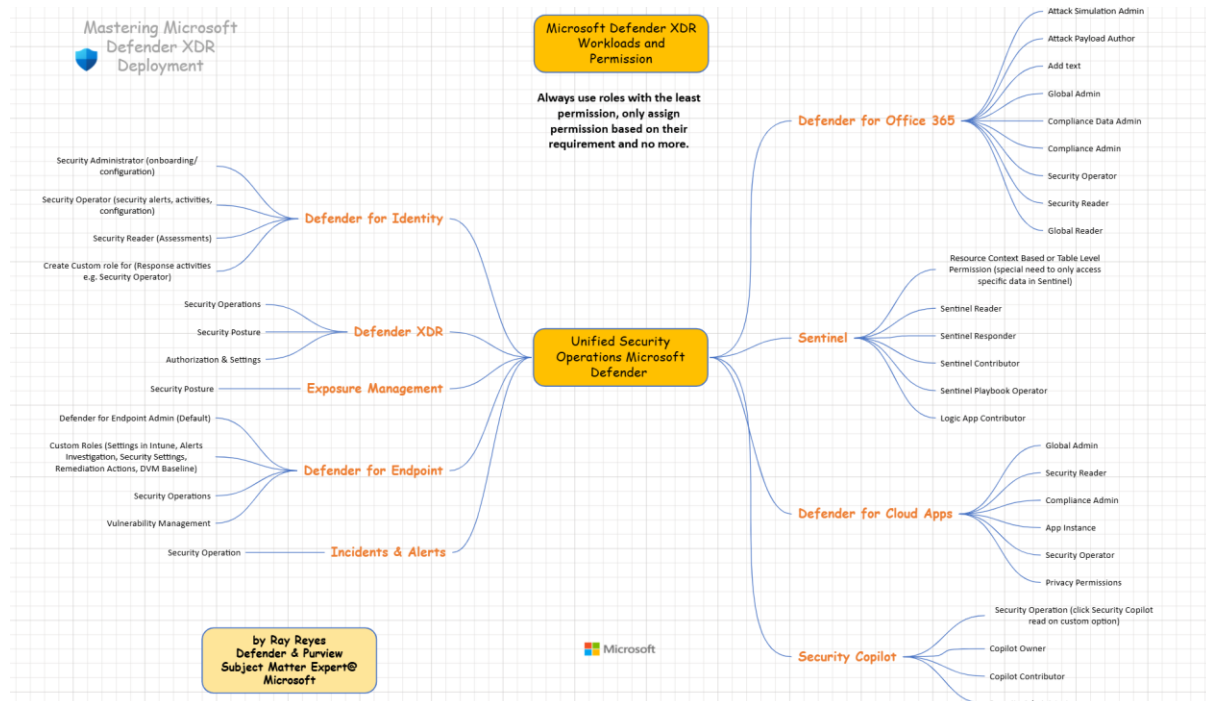
Resources

[RBAC XDR](#)

[Sentinel](#)

[MDO Permissions](#)

[MDI](#)



Phase 1 - Microsoft Defender for Office 365

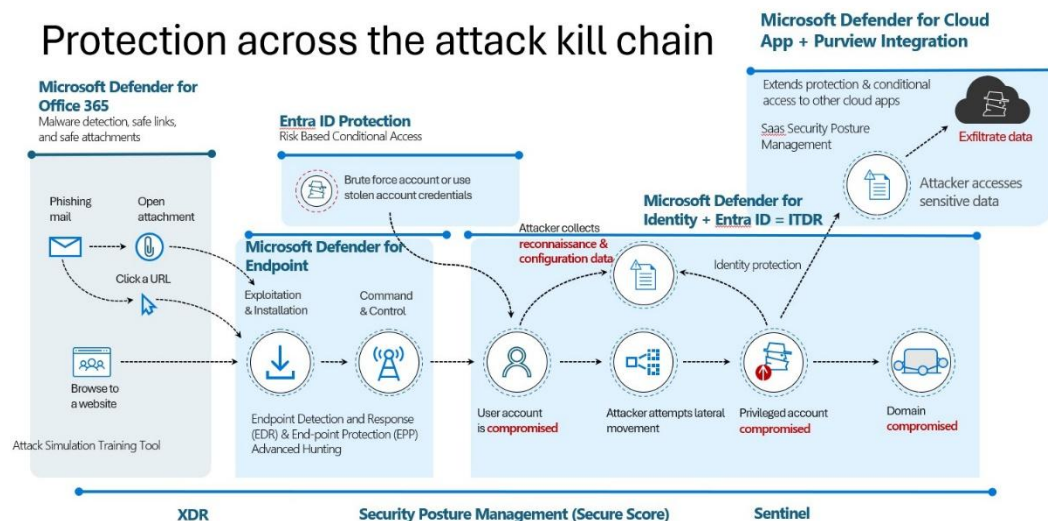
Key new features since the last version of this guide, August 2024

- AI-powered Submissions Response introduces generative AI explanations for admin email submissions to Microsoft
- You can now run QR Simulation
- The built-in Report button in Outlook for Microsoft 365 now supports the user reported settings experience to report messages as Phishing, Junk, and Not Junk
- Introducing LLM-based BEC detection and classification: Microsoft Defender for Office 365 now detects BEC attacks using large language model (LLM)-based filters to analyse an email's language and infer intent
- Defender for Office 365 is now able to detect and classify mail bombing attacks.

Key Watch outs

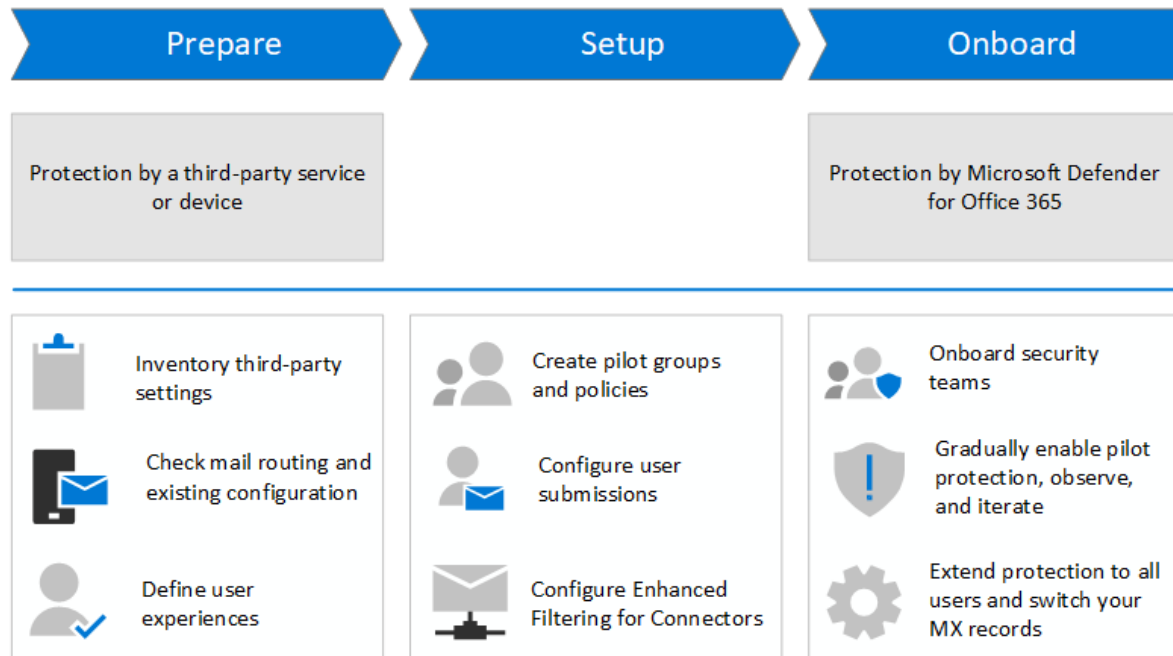
- Get your users involved early, provide some instructions on how they can assist with change management, feedback on false positives, how to submit FP.
- As part of the project, ensure there is an additional program for Attack Simulation Training. Using email protection is one thing but your best protection are your users

- Have confidence using Config Analyzer to enable the recommended settings



In the scenario, * we will assume you already have mailboxes in M365 * you need to retire your current 3rd party email protection service, which means we need to point the MX records for your email domains to M365. When you're done, mail from the internet flows directly into Microsoft 365 and is protected exclusively by Exchange Online Protection (EOP) and Defender for Office 365.

If you're coming from a 3rd party protection, we have a comprehensive guide in migration in our public docs [Migrate from a third-party protection service to Microsoft Defender for Office 365](#) | [Microsoft Learn](#)

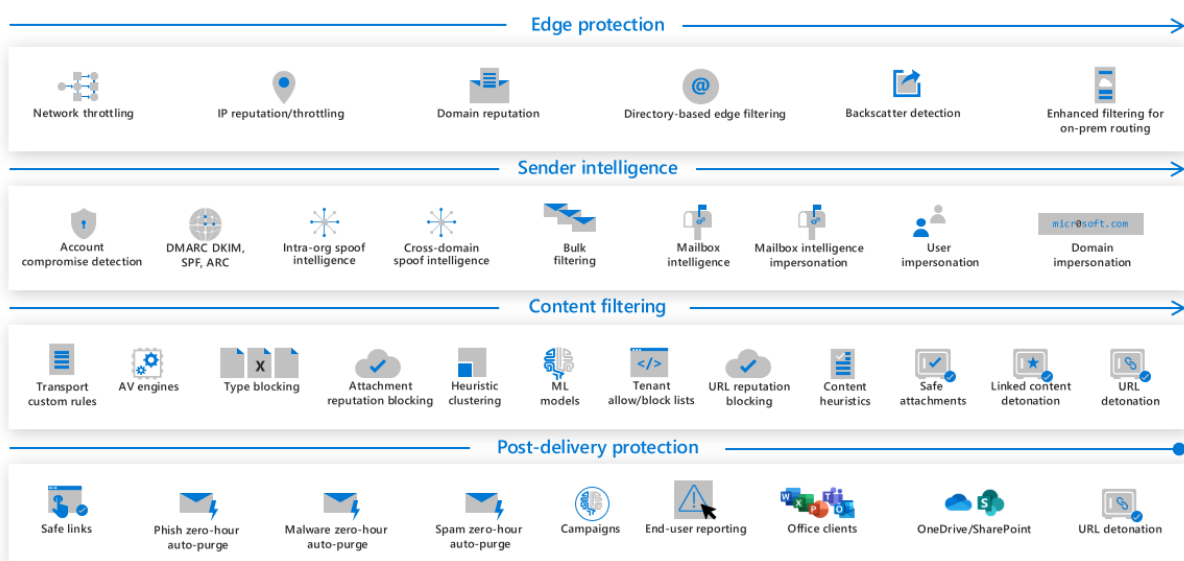


But before we get into the nitty gritty of configuration, there are few key things you need to know and understand

The protect stack is layered in 4 phases. Highlighting that these are a mixture of EOP, P1 and P2 subscription features, **but if you're an E5 customer, nee bother.**

Essentially, the incoming mail passes through all of these phases before delivery, but the actual path email takes depend on how you configure MDO.

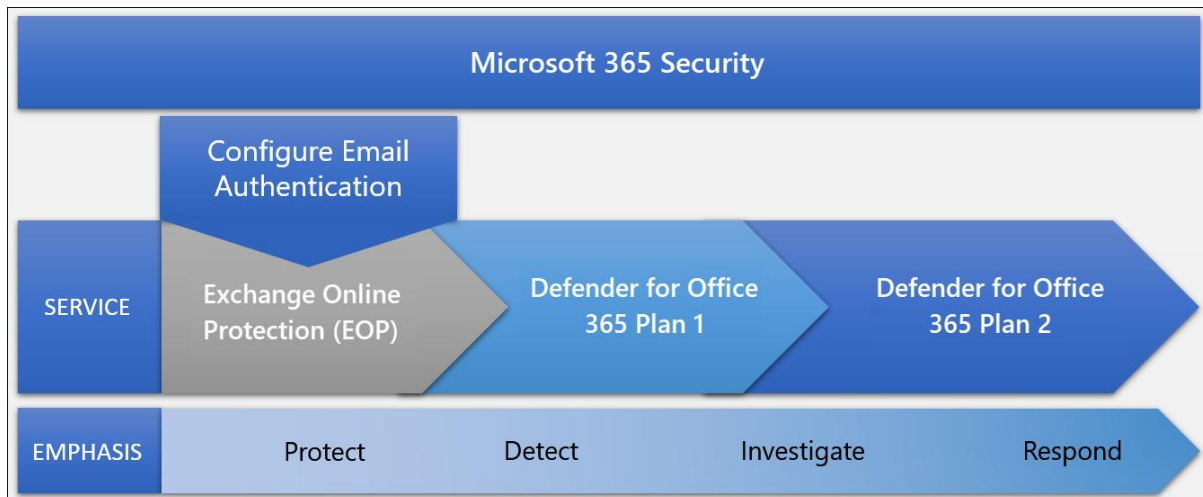
Microsoft Defender for Office 365 protection stack



- Edge Protection – still a crucial part of the stack, this phase is designed to block automatically though bad actors are now overcoming this layer much easier

- Features in sender intelligence are critical for catching spam, bulk, impersonation, and unauthorized spoof messages, and also factor into phish detection. Most of these features are individually configurable.
- In this phase the filtering stack begins to handle the specific contents of the mail, including its hyperlinks and attachments.
- The last stage takes place after mail or file delivery, acting on mail that is in various mailboxes and files and links that appear in clients like Microsoft Teams.

Another way to look at the MDO structure is through the phases from EOP to MDO P2



Order and Precedence on email protection

There are two major factors that determine which policy is applied to a message:

- **The order of processing for the email protection type:** This order isn't configurable
- **The priority order of policies:**

For more information - [Order and precedence of email protection | Microsoft Learn](#)

It's important to understand how user allows and blocks, tenant allows and blocks, and filtering stack verdicts in EOP and Defender for Office 365 complement or contradict each other.

- Filtering stack which we covered above.
- After the filtering stack determines a verdict, only then are tenant policies and their configured actions evaluated.
- If the same email address or domain exists in a user's Safe Senders list and Blocked Senders list, the Safe Senders list takes precedence.
- If the same entity (email address, domain, spoofed sending infrastructure, file, or URL) exists in an allow entry and a block entry in the Tenant Allow/Block List, the block entry takes precedence.

EOP – Email Office 365 Protection or we sometimes call it, Secure by default.

In EOP, we have by default policies already in place to keep your email secured. This is our high recommendation from the moment you create email accounts in Office 365 so you can be confident that you're secured straight away, this includes

- Email with suspected malware will automatically be quarantined. Whether recipients are notified about quarantined malware messages is controlled by the quarantine policy and the settings in the anti-malware policy. For more information, see [Configure anti-malware policies in EOP](#).
- Email identified as high confidence phishing will be handled according to the anti-spam policy action. See [Configure anti-spam policies in EOP](#).

Ok let's Migrate

Preparation - You have Steps 1-6 to follow

All sections are important., from removing old customisation, email subject and body tags to deciding on what to do with spam emails whether to put them in junk folder or quarantine, in this section, its important you take a snapshot of your existing protection settings but don't try to re-create it in MDO. Think of this as a fresh reset, in most of my customers, they find this a good reset of removing legacy settings that they inherited from previous engineer.

Some customers with 3rd party email also have phishing simulation tools. You need to configure the [advanced delivery policy](#) so MDO doesn't pick this up. Don't worry, we got you with our Attack Simulation tool, definitely the best out there today with live authored playbooks.

You can use Attack simulation training in the Microsoft Defender portal to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line. This helps and trains your users to identify what is a phish email may look like in various forms or scenarios. This keeps them on their feet and a reminder how close some phish email looks like from real ones.

AST read more <https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-get-started>

Set up MDO - You have Steps 1-5

This section emphasises on pilot users, will suggest to create some DL groups so we can use them to for exemption and include them in the [SCL=-1 mail flow rule](#) which the instruction is actually on the onboard section. Also, to configure on reported settings, on how you want your users to report on false positives and false negatives

We need to also check that our buttons are working so users can report on these.

- [The built-in Report button in Outlook on the web](#)
- [The Report Message and Report Phishing add-ins](#)
- Supported third party reporting tools as described [here](#).

This section also instructs on creating your pilot policies for anti-spam, anti-phish, safe links and safe attachments [Configure spam filter policies - Microsoft Defender for Office 365](#) |

[Microsoft Learn](#). For each one, we recommend creating a group for each policy. For example **(you can create your own)**

- **A Safe Attachments pilot group:** For example, **MDOPilot_SafeAttachments**
- **A Safe Links pilot group:** For example, **MDOPilot_SafeLinks**
- **A pilot group for Standard anti-spam and anti-phishing policy settings:** For example, **MDOPilot_SpamPhish_Standard**
- **A pilot group for Strict anti-spam and anti-phishing policy settings:** For example, **MDOPilot_SpamPhish_Strict**

So, the focus is to ensure that we configure settings that will exempt your pilot users from your existing protection so that MDO can fully be tested by your pilot.

When building your pilot policies for the above you can use our config-analyser which is our best practice configuration recommendation which will be your best friend going forward

The goal of config analyser is to find and fix security policies where the settings are less secure than the Standard protection and Strict protection

You can filter the recommendation.

Microsoft Defender

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Reports
Learning hub
Trials
More resources
System
Customize navigation

Search

Policies & rules > Threat policies > Configuration analyzer

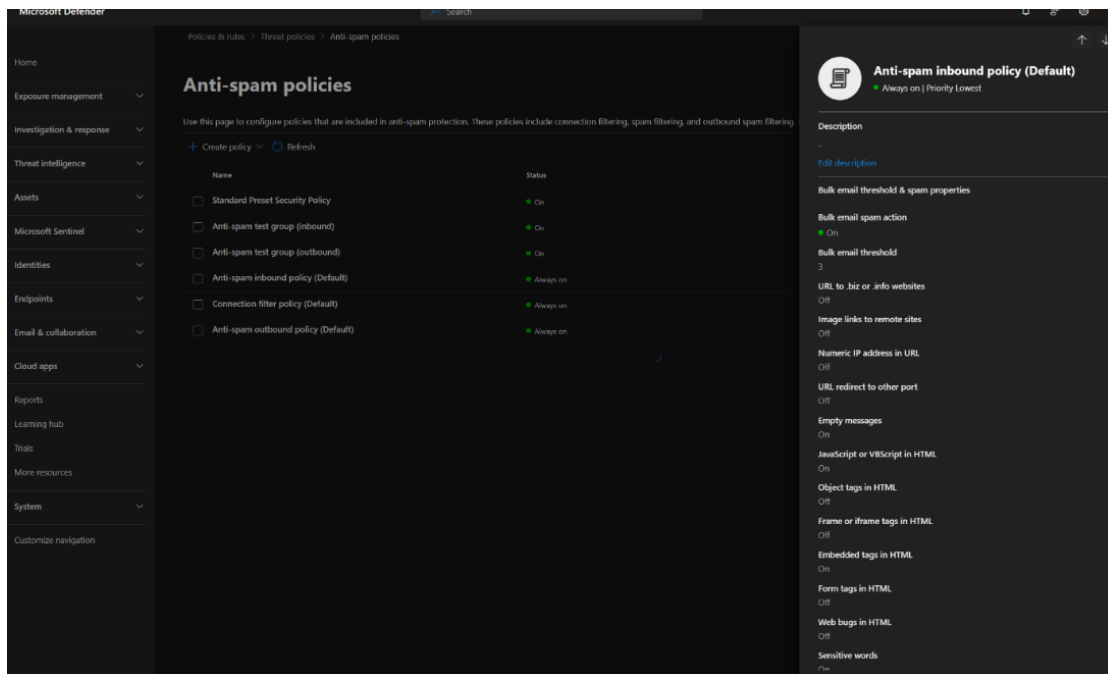
Configuration analyzer

The Configuration analyzer can help identify issues in your current configuration and help improve your policies for better security. Want to automatically stay updated with recommendation configuration? Switch on [alerts](#). [Learn more.](#)

Standard recommendations
Strict recommendations
Configuration drift analysis and history

Anti-spam 20	Anti-phishing 16	DKIM 2	Outlook 1				
Refresh 39 items Search Filter							
☐	Recommendations	Policy	Policy group/setting name	Policy type	Current configuration	Last modified	Status
☐	Quarantine message	Default	High confidence spam detection action	Anti-spam	Move to Junk Email folder	Invalid date	Not started
☐	Quarantine message	Default	Phishing email detection action	Anti-spam	Move to Junk Email folder	Invalid date	Not started
☐	Change 15 to 30	Default	Quarantine retention period	Anti-spam	15	Invalid date	Not started
☐	Change On to Off	Default	Empty messages	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Default	Javascript or VBScript in HTML	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Default	Embedded tags in HTML	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Default	Apply sensitive word list	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Anti-spam test group (inbound)	Image links to remote sites	Anti-spam	On	Invalid date	Not started
☐	Change Test to Off	Anti-spam test group (inbound)	Numeric IP address in URL	Anti-spam	Test	Invalid date	Not started
☐	Change On to Off	Anti-spam test group (inbound)	Empty messages	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Anti-spam test group (inbound)	Javascript or VBScript in HTML	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Anti-spam test group (inbound)	Frame or iframe tags in HTML	Anti-spam	On	Invalid date	Not started
☐	Change On to Off	Anti-spam test group (inbound)	Object tags in HTML	Anti-spam	On	Invalid date	Not started

When you go into a recommendation, you can open it up, click on recommendation and it will take you to the setting itself to make the change



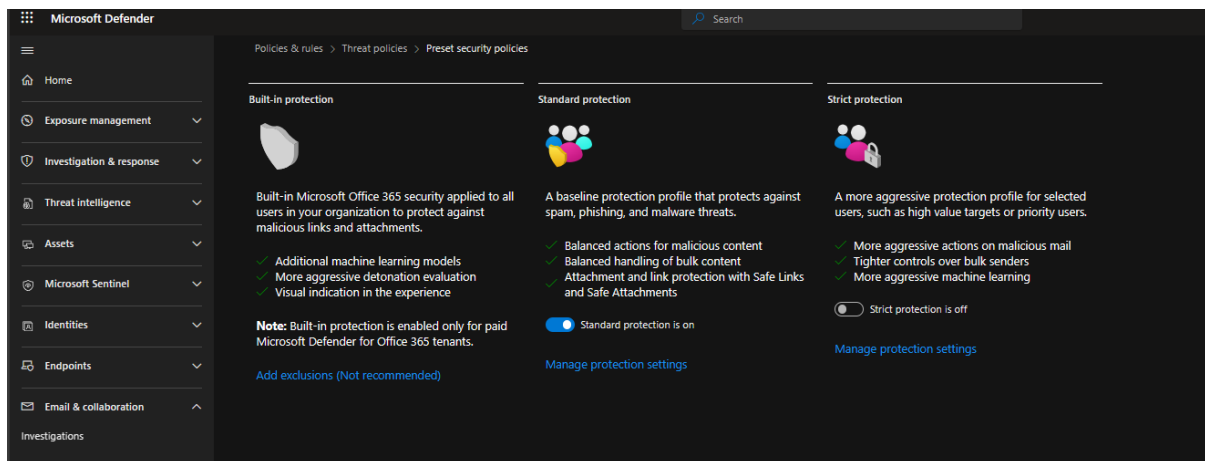
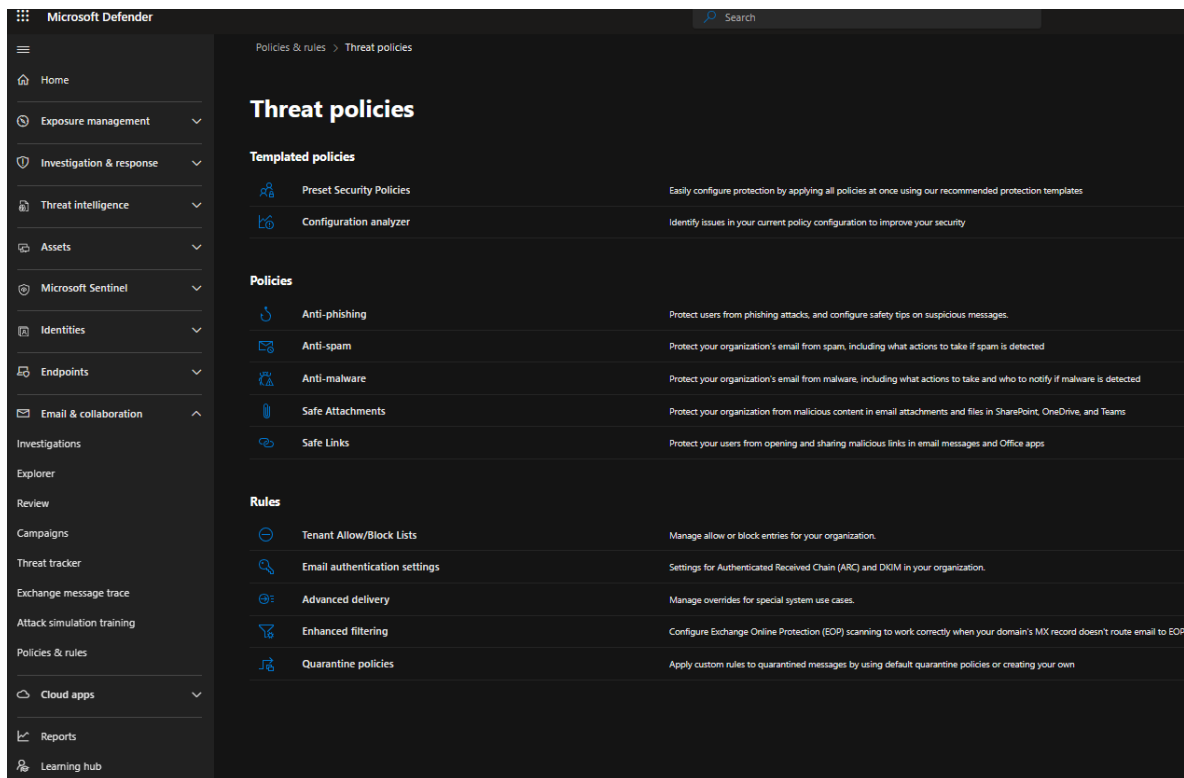
Important note: when deploying policies, our recommendation is to use **users or groups** for your pilot phase and domains when you're ready for general deployment. We don't recommend mixing all 3.

Exchange Online Protection (EOP) and Microsoft Defender for Office 365 (MDO) Policies

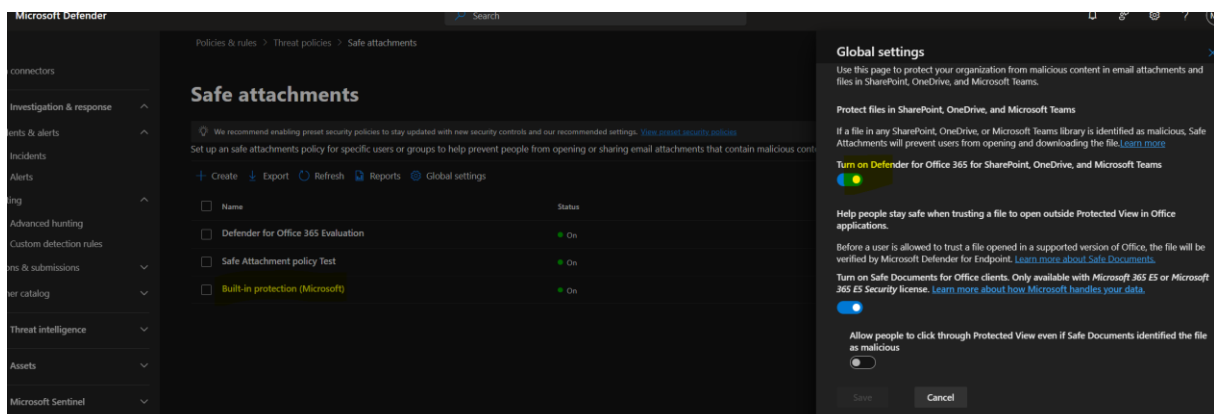
There are two ways to approach policies in EOP and MDO, you can either manually do this or chose using our Preset Security Policies. There are 3 different preset policies, there is the built-in which is done automatically. Then you have the standard and strict preset policies.

[Preset security policies - Microsoft Defender for Office 365 | Microsoft Learn](#)

Under Email & Collaboration in the Defender XDR Portal. Under Policies, you will find all the settings you need under Threat Policies.



By default, both Safe attachments and Safe links are enabled. However, you can still customised users or groups for granular or more specific use case policy



[Set up Safe Attachments policies in Microsoft Defender for Office 365 - Microsoft Defender for Office 365 | Microsoft Learn](#)

[Complete Safe Links overview for Microsoft Defender for Office 365 - Microsoft Defender for Office 365 | Microsoft Learn](#)

Apply strict protection

- Exchange online protection
- Defender for Office 365 protection
- Impersonation protection
- Policy mode
- Review

Apply Exchange Online Protection

Add the users, groups, and domains to protect using Exchange Online Protection capabilities, including inbound anti-spam, anti-malware, and anti-phishing. [Learn more about preset security policies](#)

Apply protection to:

☐ All recipients

☒ Specific recipients

Users

And

Groups

And

Domains

☐ None

☐ Exclude these recipients

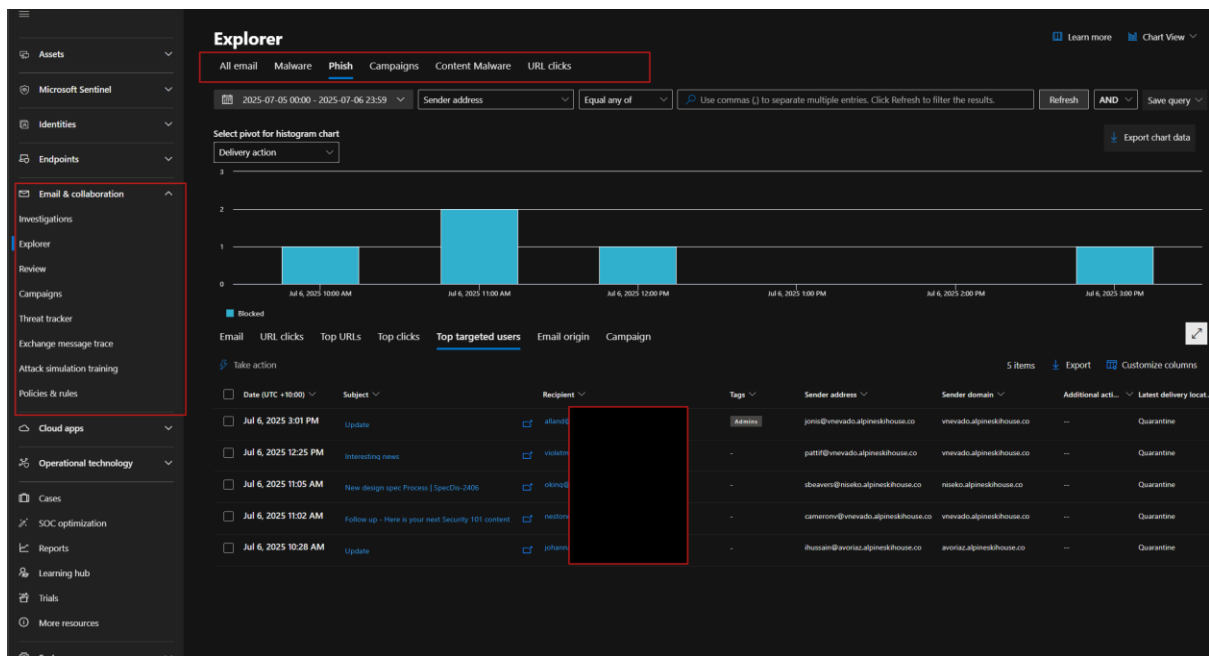
Onboard MDO – Steps 1-8

In this section, we will do a lot of fine tuning, make a decision to add more users to your pilot group but first things first, ensure that the right folks have the right permission. Just like with all of our Defender stack, each one has certain roles you can assign, for the simple reason that you may have various people looking after each product.

Leverage the Role Based Permission [Microsoft Defender for Office 365 permissions in the Microsoft Defender portal - Microsoft Defender for Office 365 | Microsoft Learn](#)

The goal of this section is to be basically complete your migration. So, the first few steps are fine tuning the last pieces of settings, continue going through the list of recommendation via Config Analyzer. As you continue to feel comfortable, continue adding more and more users to the Pilot group. The more users you have reporting any potential false positives, the more that machine learning will pick this up and fine tune your alerts.

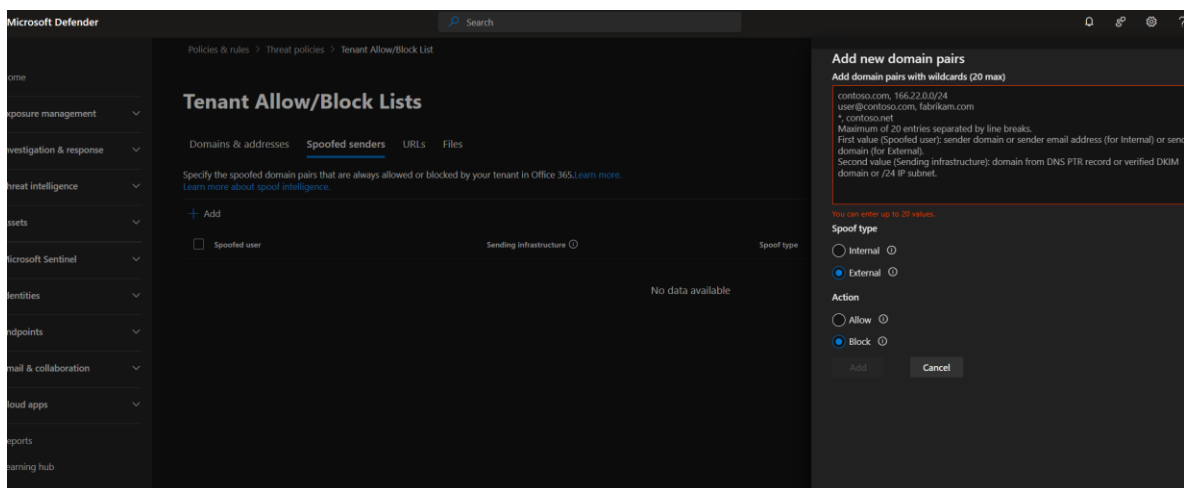
As your users report false positives, there's a few features you can leverage to confirm the validity of their concern, these are a mixture of P1 and P2 features so look carefully. As an example. Threat explorer is a great feature to dive deeper on emails that could be malicious and the validity of it.



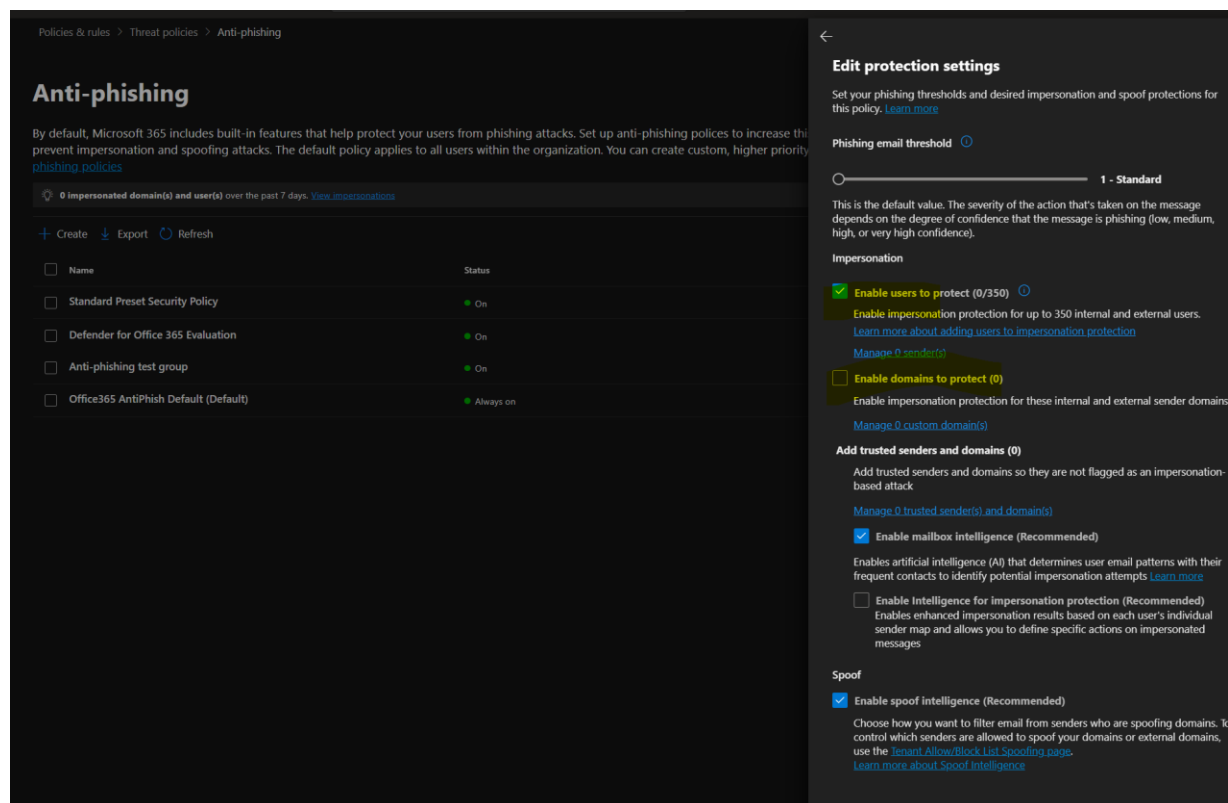
- [Quarantine](#)
- [Threat Explorer \(Explorer\)](#)
- [Email security reports](#)
- [Defender for Office 365 reports](#)
- [Mail flow insights](#)
- [Mail flow reports](#)

Let's fine tune some features before we start adding more pilot users

Tune Spoof in Tenant Allow/Block List



Impersonation users and domains



Some sources of your business-critical email might have misconfigured email authentication records in DNS (SPF, DKIM, and DMARC)

The spoof intelligence insight and the impersonation insight are most helpful, but consider making the following activities a regular occurrence:

- Review user reported messages, especially user-reported phishing messages
- Review overrides in the Threat protection status report.
- Use Advanced Hunting queries to look for tuning opportunities and risky messages.

The next two steps are crucial, we're close to completing the migration.

Once you're happy with your testing, got the green light from your pilot users. Then you are ready to remove that Pilot policy and apply it to all org.

Essentially you have two steps in this section, apply the policy to all and **then Turn off the mail flow so it can now point to M365....** [Turn off the SCL = 1 mailflow rule](#)

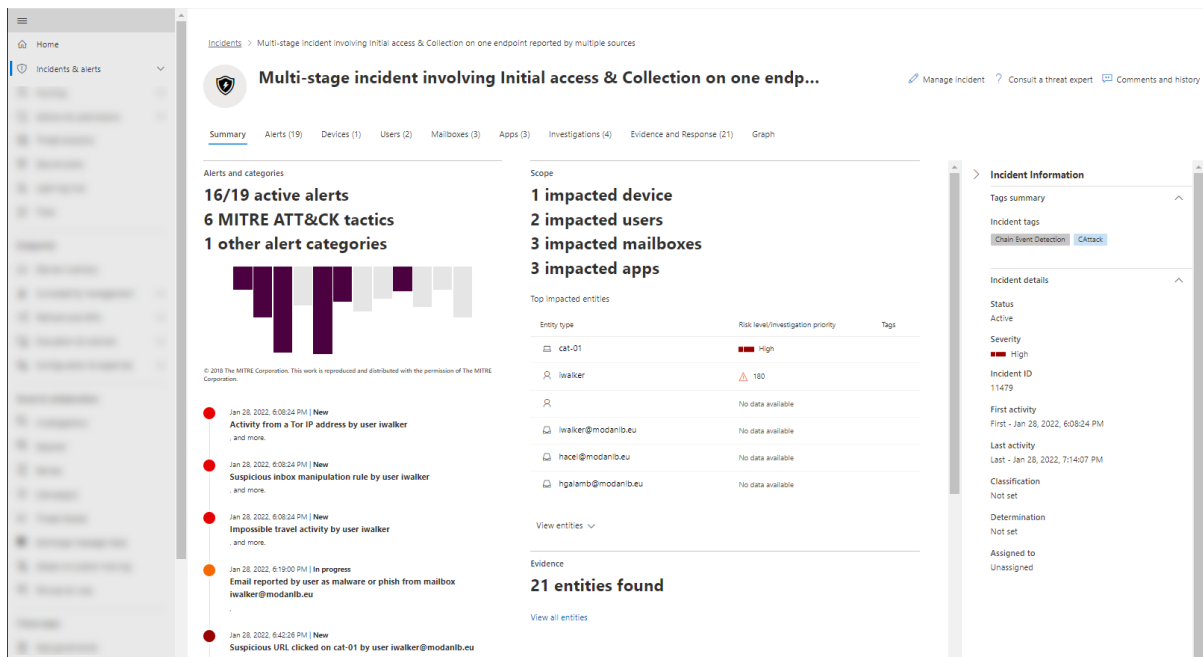
The last step is switching your MX Record; I've copied the link here as this is quite a detail steps to follow. Once you've done this, then you are completely Migrated. Well done!

[Switch your MX Records](#)

Managing Alerts and Incidents

We highly recommend for SOC team to triage alerts in the Incidents page. Incidents are a correlation of alerts which our ML will build a story from the alerts that is calculated to be part

of a specific attack. You can view summary of the attack, see all the alerts it correlated, view devices that are impacted, more important the recommendation on how to resolve this incident. All of alerts from MDO, MDE, MDI, MDA, Entra (if diverted) will come into this incidents page, so its def worth getting to know this quite well



Be Proactive

Security is a team sport, and we all need to be proactive. I've divided each player for MDO

SOC Team. If you don't have a playbook, use this to reference and create your own.

[Security Operations Guide for Defender for Office 365 - Microsoft Defender for Office 365 | Microsoft Learn](#)

USERS

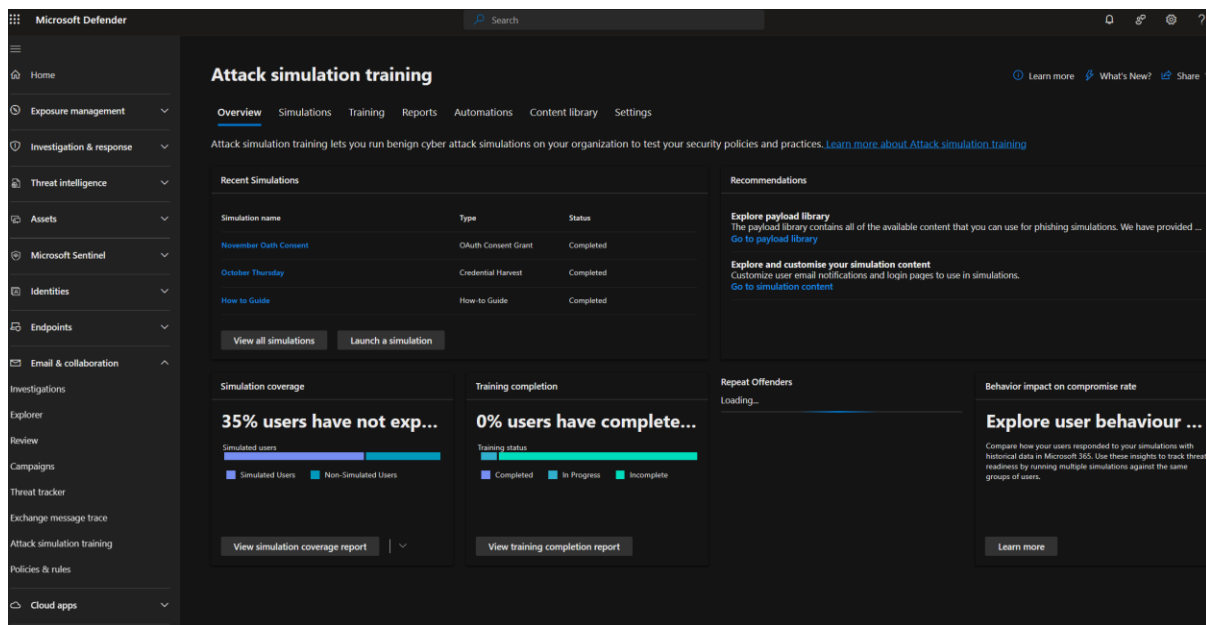
[Manage submissions - Microsoft Defender for Office 365 | Microsoft Learn](#)

Microsoft Ninja Training [Defender for Office 365 Ninja Training \(microsoft.com\)](#)

SOC Team + Change Management

[Get started using Attack simulation training - Microsoft Defender for Office 365 | Microsoft Learn](#)

Once the dust settles from your MDO migration. Attack Sim needs to be part of your MDO adoption or Phase 2 of your MDO migration. One of the coolest and critical features of MDO. User Education. You can have the best security tools out but if you don't have a change - program to adopt security, then you still have a huge gap in your security posture. Attack Simulation is an amazing way to educate your users. We use real life phishing emails (payloads) that users submit to Microsoft, so we use real life phishing emails to educate users. We use the most common phishing technique to newly trending technique. The tool is integrated with your M365, so we can leverage pulling information from M365 to simulate phishing emails.



Phase 2 - Microsoft Defender for Identity + Microsoft Entra ID Protection (Identity, Threat, Detection and Responds (ITDR))

What's new since last version of this guide, August 2024

- Scoped access by Active Directory domain now supported (Preview)
- Okta integration is now available in Microsoft Defender for Identity
- Lots of new detection
- PowerShell module update
- New Entra Connect Sensor update
- New Entra Connect Sensor Detections
- Lots of new MDI Posture recommendations
- New and updated events in the Advanced hunting IdentityDirectoryEvents table

'A security discipline that encompasses threat intelligence, best practices, knowledge base, tools, and processes to protect identity systems. It works by implementing detection mechanisms like login and access, investigating suspect posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure - Gartner'

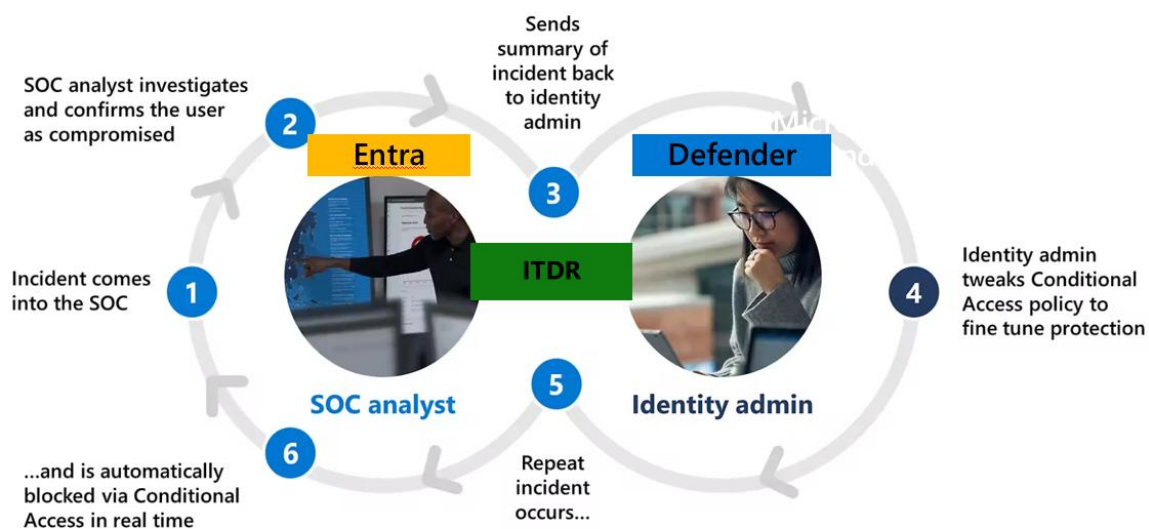
Key Watch outs

- Capacity planning! Crucial on the early stages on this deployment, importance on ensuring opening those pre-reqs, network ports 443 and sizing tool for all your servers you want to install the sensors on.
- Don't run the sensors on those servers that need more specs, upgrade them before you install the sensors

- [Watch this video!](#) Running PS Module to do most of the configuration of event logs and creating Group Policy objects has been a time saver for new deployment in recent months.
- So, this is crucial especially if you have multiple DCS - [New Defender for Identity PowerShell module - YouTube](#)

In this Phase 2, we will cover Identity holistically and not just from Defender for Identity deployment but also reviewing Entra ID's Risk Based Conditional Access. ITDR isn't **new** from a solution perspective, as we have always had solutions to cover on-prem, our cloud and third-party identities. You can safely say, it is new from a Gartner perspective in terms of categorization. Identity has been at the forefront of initial access to a company's environment for decades, hackers intelligently scripting new malicious actors from mimikats to solorigates to printanightmare to the new modern attacks of human operated ransomware.

From the Microsoft Perspective, we have two key products that protects On-prem identities and Cloud identities, so on this article we will take a look at deploying MDI from a high-level approach and Entra P2 Risk Based Policies which is the most important security feature I believe in Entra that you can deploy



Microsoft Defender for Identity (MDI) Deployment

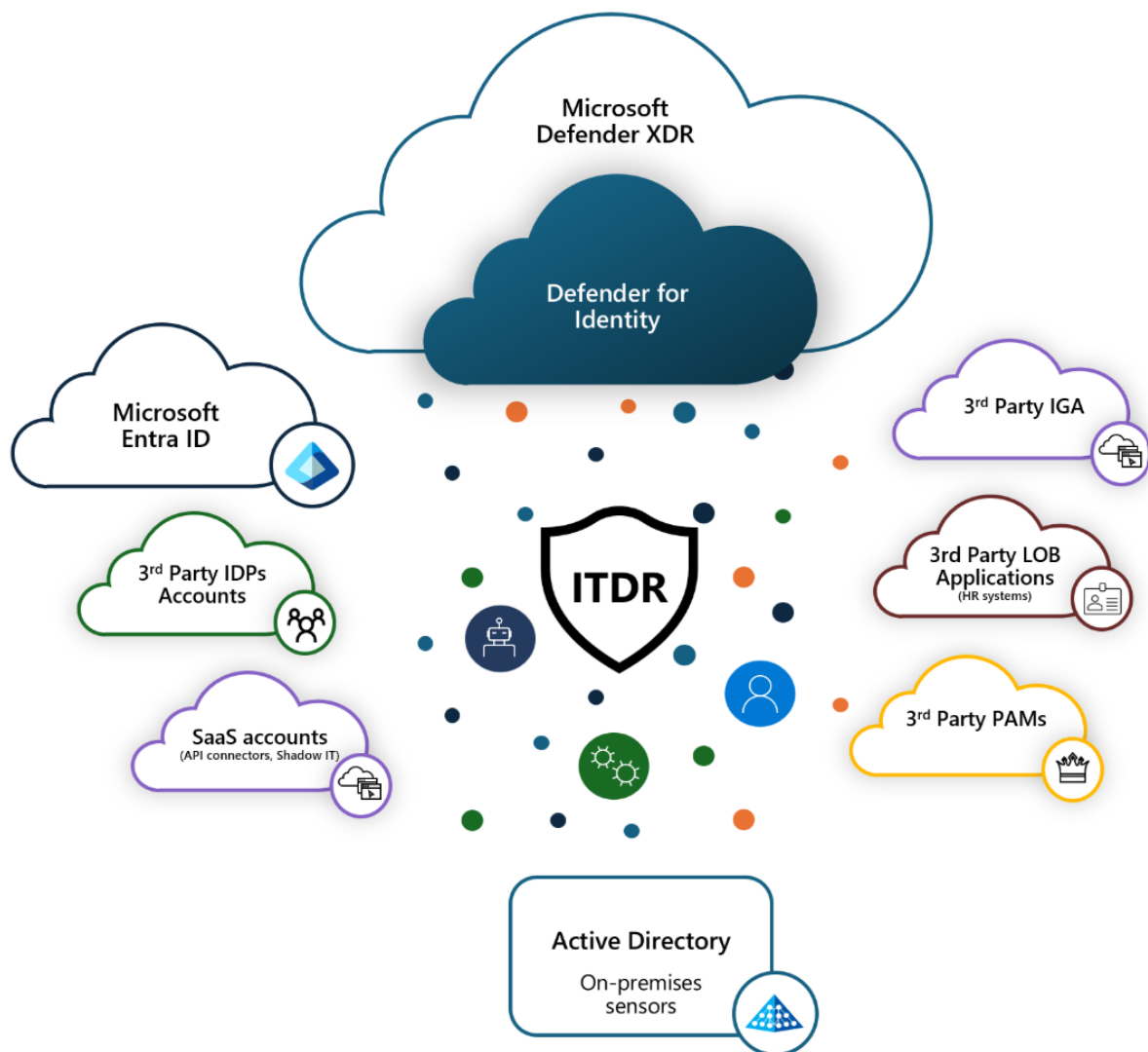
The time deploying this product depends on how large your organisation is based on the number of DCs, ADFS, ADCS and where I often see customers hit some delays are upgrading some of the servers that require more specs, and the back and forth change request can slow things down in the beginning. One of key pre-reqs we suggest is to run the sizing tool against all your servers that you will be planning to install the sensor.

So, you don't get lost, let's look at how MDI architecture looks like.

We have a sensor install that you install on your DC or ADFS or ADCS. The `Sensor is a lightweight bit of code.

In the domain controller, we collect and parse network data from the Domain Controller and sending that telemetry to the cloud services.... In the Domain Controller, what we are looking at, we have a network capture driver, which is parsing the network traffic to and from the domain controller, looking for various authentication protocols like the Kerberos packets, NTLM packets

Additionally, we will also parse from Event Tracing and events - Event Tracing for Windows (ETW) provides a mechanism to trace and log events that are raised by user-mode applications and kernel-mode drivers. ETW is implemented in the Windows operating system and provides developers a fast, reliable, and versatile set of event tracing features.



Step 1... We need to ensure we have the appropriate ports opened so that cross over signals will work from signals from DC to cloud service and resolution of any IP to name will be easier to resolve. We only need one of these ports, more info here [Prerequisites - Microsoft Defender for Identity | Microsoft Learn](#)

Protocol	Transport	Port	Source	Destination
NTLM over RPC*	TCP	135	Domain Controller	All devices on the network
NetBIOS*	UDP	137	Domain Controller	All devices on the network
RDP*	TCP	3389	Domain Controller	All devices on the network
DNS	UDP	53	Domain Controller	DNS Server
HTTPS**	TCP	443	Domain Controller	Defender for Identity Cloud Service
SAM-R	TCP/UDP	445	Domain Controller	All devices on the network

* One of these is required, but recommendation is to use them all

** Outbound connection to MDI instance hosted at *.atp.azure.com

Step 2. Run that sizing tool, grab the sizing tool on this doc and also follow the instructions on how to run it [Plan capacity for deployment - Microsoft Defender for Identity | Microsoft Learn](#)

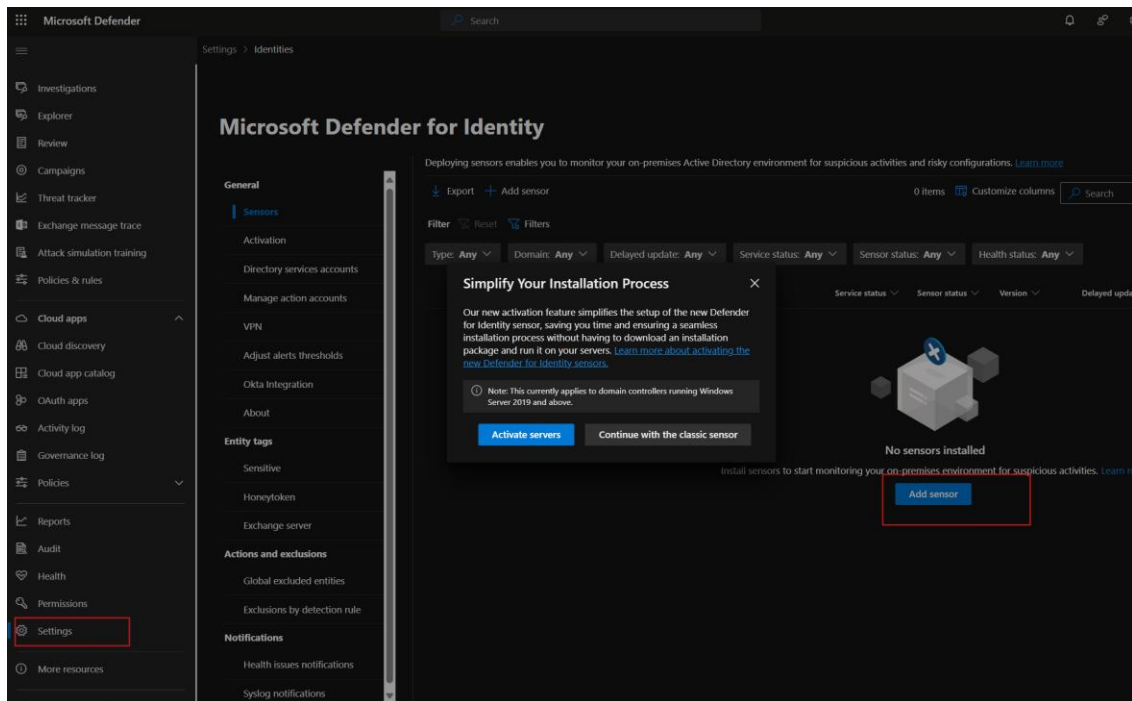
The sizing tool determines whether your server is supported based on the **Busy Packets/Second** value, which is calculated based on the 15 busiest minutes over a 24-hour period

Step 3. Install and configure the sensor in DC

[Install the sensor - Microsoft Defender for Identity | Microsoft Learn](#)

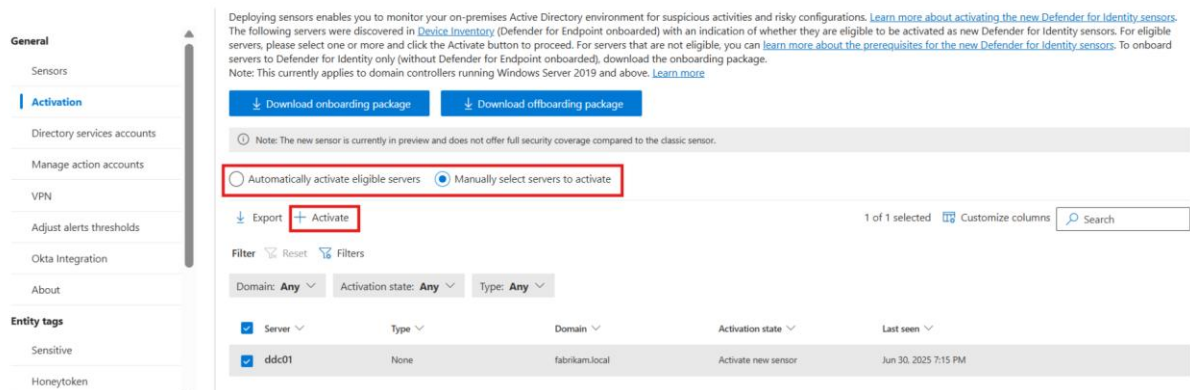
Microsoft Defender for Identity										
Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. Learn more										
Filter										
Type: Any Domain: Any Delayed update: Any Service status: Any Sensor status: Any Health status: Any										
7 items Customize columns Search										
Sensor	Type	Domain	Service status	Sensor status	Version	Delayed update	Health status	Health issues	Created	
☐ DC2	Domain controller Sensor	domain1.test.local	Running	Up to date	2.185.15524.950	Disabled	Healthy	0	Jul 21, 2022 6:08 PM	
☐ STANDALONE	Standalone Sensor	domain1.test.local	Running	Up to date	2.184.15485.42267	Enabled	Healthy	0	Mar 6, 2022 3:22 PM	
☐ DC4	Domain controller Sensor	domain1.test.local	Running	Up to date	2.185.15524.950	Disabled	Healthy	0	Jul 21, 2022 6:07 PM	

Install sensor on ADFS and ADCS if this is still applicable to you, we won't dive too deep on this but touch base on the detection you can enable [Activate the Defender for Identity sensor v3.x on a domain controller - Microsoft Defender for Identity | Microsoft Learn](#)



Activating Servers is the easiest approach and recommended if you're onboarding MDI

Microsoft Defender for Identity



IMPORTANT NOTE - This doesn't support side-by-side installation with an existing Defender for Identity sensor and isn't recommended as a replacement for the Defender for Identity sensor.

Make sure that the domain controller where you're planning to activate Defender for Identity capabilities doesn't have a [Defender for Identity sensor](#) deployed

Step 4. Once if you've confirmed that the sensor is installed and is healthy, it's time to enable the windows event collection so we can start collecting this log to Defender. The good news is that in the past we had to do this manually and a few months ago we've recently released the NEW PowerShell MDI Module, which is a god send!

Overview of the Microsoft Defender for Identity PowerShell module | Microsoft Learn

Watch this video for a full demo

[New Defender for Identity PowerShell module \(youtube.com\)](#)

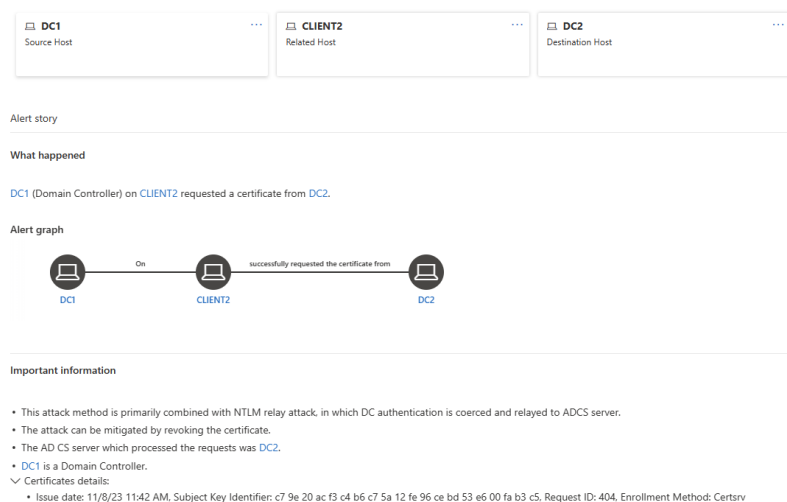
The way we've designed and think about collecting events is we follow an Attack Kill chain flow, which is also aligned to the MITRE Att&ck framework.

MDI detects identity attacks throughout different phases:

Initial Access	Credential Access	Lateral Movement	Defense Evasion
Suspicious VPN Connection	Suspected NTLM authentication tampering	Suspected use of Metasploit hacking framework	Suspected DCS ~~hadow~~ attack (domain controller promotion)
Discovery	Suspected brute-force attack (SMB)	Suspected WannaCry ransomware attack	Suspected DCS ~~hadow~~ attack (domain controller replication request)
Account enumeration reconnaissance	Suspected AD FS DKM key read	Remote code execution attempt over DNS	Suspected SID-History injection
Network mapping reconnaissance (DNS)	Suspected AS-REP Roasting attack	~~Abnormal~~ Exchange attribute change	
User and IP address reconnaissance (SMB)	Suspicious Kerberos delegation attempt using ~~BronzeBit~~ method	Suspected ~~Netlogon~~ privilege elevation attempt	Execution
Security principal reconnaissance (LDAP)	Suspected brute-force attack (Kerberos, NTLM)	Suspected over-pass-the-hash attack	Suspicious service creation
User and group membership reconnaissance (SAMR)	Suspected ~~DFSCoerce~~ attack using Distributed File System Protocol	Suspected identity theft (pass-the-certificate)	Remote code execution attempt
Active Directory attributes Reconnaissance using LDAP	Suspected ~~DCSync~~ attack	Suspected identity theft (pass-the-hash)	Persistence
Honeytoken activity	Suspected Golden Ticket usage	Suspected identity theft (pass-the-ticket)	Suspicious additions to sensitive groups
Privilege Escalation	Suspected Kerberos SPN exposure	Suspicious network connection over Encrypting File System Remote Protocol	Exfiltration
Suspicious modification of ~~dnshostname~~ attribute	Suspected brute-force attack (LDAP)	File System Remote Protocol	Suspicious communication over DNS
Suspicious Kerberos delegation attempt	Suspected NTLM relay attack (Exchange Server account)	Suspected Print Spooler service exploitation attempt	Data exfiltration over SMB
Suspicious modification of the RBCD attribute	Suspected skeleton key attack	Suspected SMB packet manipulation	
Suspicious modification of a ~~samNameAccount~~	Malicious request of Data Protection API (DPAP I) master key		
Suspicious modification of the trust relationship of AD FS server	Suspected rogue Kerberos certificate usage		
	Suspicious Kerberos ticket request		

Last year, we added new detection for AD CS, if AD CS is prominent in your environment, I highly recommend you turn this on. AD CS can generate password-equivalent digital certificates, AD CS servers are classified as tier-0 assets whose compromise can be as catastrophic as a compromise to a Domain Controller itself. Despite being a prime target, AD CS security has been largely overlooked by security products and professionals over the years allowing cyber-criminals to continue exploiting gaps in protection to escalate privileges, steal credentials and gain domain persistence.

Suspicious Domain-Controller certificate request (ESC8)



To give you what the Event Collection means

[Event collection overview - Microsoft Defender for Identity | Microsoft Learn](#)

To configure the MDI Windows Collection using the new PowerShell Module, watch this clip

[New Defender for Identity PowerShell module - YouTube](#)

For instructions on how to run the MDI PowerShell Module

[Introducing the new PowerShell Module for Microsoft Defender for Identity](#)

Latest module to install [PowerShell Gallery | DefenderForIdentity 1.0.0.4](#)

For more information, see:

- [DefenderForIdentity Module](#)
- [Defender for Identity in the PowerShell Gallery](#)

For example, the following command defines all settings for the domain, creates group policy objects, and links them.

Set-MDIConfiguration -Mode Domain -Configuration All

Once we've configured and run PS modules, there are few key features to go through

First, are the learning periods. It's important to know that with MDI, there is a learning period where some Defender for Identity alerts rely on *learning periods* to build a profile of patterns and then distinguish between legitimate and suspicious activities. Each alert also has specific conditions within the detection logic to help distinguish between legitimate and suspicious activities, such as alert thresholds and filtering for popular activities. You can also switch alert into Test Mode if this is something you really want to consider switching thresholds

[Adjust alert thresholds \(Preview\) - Microsoft Defender for Identity | Microsoft Learn](#)

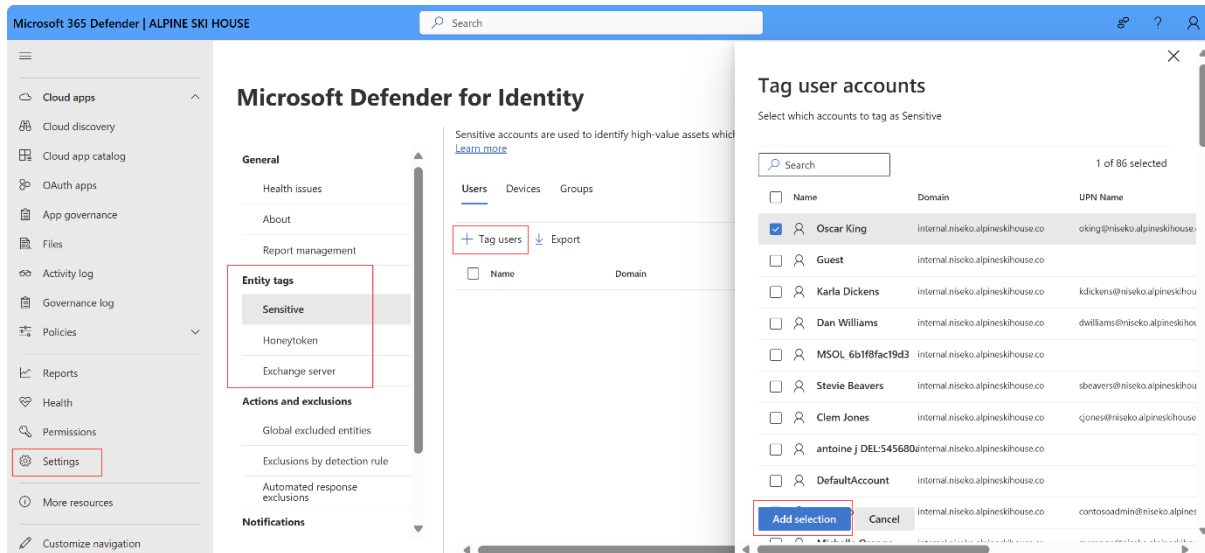
Microsoft Defender for Identity

Some of the Microsoft Defender for Identity alerts rely on learning periods to build a profile of patterns and then distinguish between legitimate and suspicious activities. Each alert incorporates specific conditions within the detection logic such as thresholds and filtering of popular activities. On this page, you can customize the threshold level (High/Medium/Low) for individual alerts, influencing their alert volume. The 'High' level reflects the default and standard behavior as per the product configuration. Changing the threshold level from High to Medium or Low will increase the number of alerts generated by Microsoft Defender for Identity. Enabling the 'Recommended Test Mode' button sets all alert threshold levels to 'Low'. This adjustment results in an increased number of alerts, including some related to legitimate traffic and activities. [Learn more.](#)

☒ Recommended test mode ☐ Revert to default

Alert name	Threshold level	Information
Security principal reconnaissance (LDAP)	Low	On Medium mode, this detection triggers immediately and disables the filtering of popular queries in the environ... On Low mode, this detection triggers immediately.
Suspected AD FS DKM key read	Low	On Low mode, this detection triggers immediately.
Suspected Brute Force attack (Kerberos, NTLM)	Low	On Medium mode, this detection ignores any learning done and has a lower threshold for failed passwords. On Low mode, this detection ignores any learning done and has the lowest possible threshold for failed pa...
Suspected DCSync attack (replication of directory services)	Low	On Medium mode, this detection triggers immediately. On Low mode, this detection triggers immediately and avoids IP filtering like NAT or VPN.
Suspected Golden Ticket usage (encryption downgrade)	Low	On Low mode, this detection triggers an alert based on lower confidence resolution of a device.
Suspected Golden Ticket usage (forged authorization data)	Low	On Low mode, this detection triggers immediately.
Suspected identity theft (pass-the-ticket)	Low	On Low mode, this detection triggers immediately and avoids IP filtering like NAT or VPN.
Suspicious additions to sensitive groups	Low	On Low mode, this detection avoids the sliding window and ignores any previous learnings.
User and Group membership reconnaissance (SAMR)	Low	On Medium mode, this detection triggers immediately. On Low mode, this detection triggers immediately and includes a lower alert threshold.

To get a sense that your sensitive accounts are truly set as a priority for alerts, you can tag them here to get priority on alerts. There is already a list of accounts that are automatically tag such as Domain Admins, Admins, Power Users.



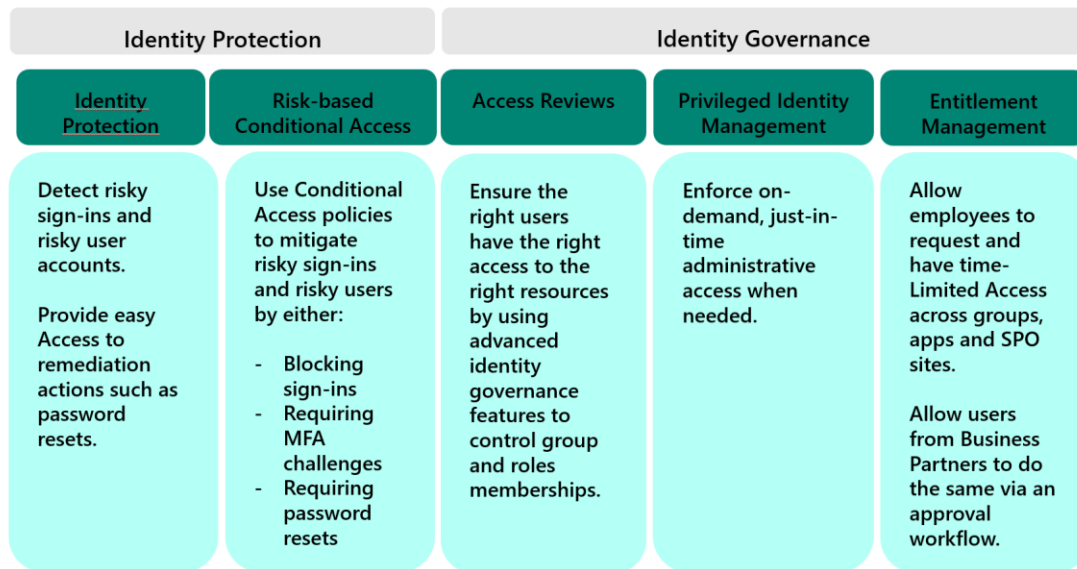
So, once we've done our On-Prem side of protection and detection. Let's assume you have Entra P1-P2 Subscription and if you don't, what are you doing!

As an FYI, let's look at both P1 and P2 Features. But today we will focus on the Risk Based Conditional Access that is featured in P2 capabilities

Entra P1 features at a glance

Condicional Access (CA)	Azure AD Self Service Password Reset (SSPR)	Azure AD Application Proxy	Azure AD Password Protection	Azure AD Connect Health
Manage access to your cloud apps using MFA and SSO. Apply the right access controls when needed to keep an organization secure.	Give users the ability to change or reset their password, with no administrator or help desk involvement.	Support single sign-on (SSO) across devices, resources, and apps in the cloud and on-premises. Support multi-factor authentication for apps in the cloud and on-premises	Ban weak passwords and define parameters to lock out an account after repeated bad password attempts.	Provide robust monitoring of on-premises identity infrastructure. Enable a single lens of health for key identity components in one place.

Entra P2 features at a glance



Identity Protection is simple to implement you just need to understand what Risk is.... We have Risky sign-ins and Risky User. Both has mostly P2 capabilities that you need to implement

[What are risks in Microsoft Entra ID Protection - Microsoft Entra ID Protection | Microsoft Learn](#)

User Risk

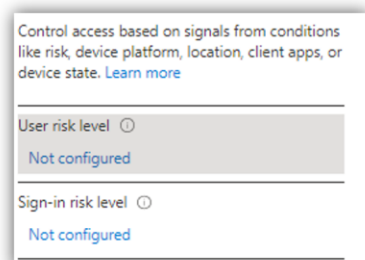
User risk represents the probability that a given identity or account is compromised

- Administrators can decide based on this risk score signal to enforce organizational requirements and block access, allow access, or allow access but require a password change using Azure AD self-service password reset (SSPR).
- Microsoft recommends password reset (with MFA) as a Conditional Access control if a user risk is triggered.**

Sign-in Risk

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

- Identity Protection analyzes signals from each sign-in, both real-time and offline, and calculates a risk score based on the probability that the sign-in wasn't performed by the user.
- Administrators can decide based on this risk score signal to enforce organizational requirements and block access, allow access, or allow access but require multi-factor authentication (MFA).
- Microsoft recommends to require MFA as a Conditional Access control if sign-in risk is triggered.**



One of the key benefits

Auto-remediate risky users and sign-ins to reduce the burden on IT admins.

Premium (P2) tenants who use RBCA remediate user risk **140X faster** than P2 tenants who don't use RBCA. And the time to remediation is **2.5 minutes** for tenants using RBCA vs. **5.9 hours** for tenants that don't.

🔍

Sign-in risk detections

🔍 Expand table

Risk detection	Detection type	Type
Atypical travel	Offline	Premium
Anomalous Token	Real-time or Offline	Premium
Suspicious browser	Offline	Premium
Unfamiliar sign-in properties	Real-time	Premium
Malicious IP address	Offline	Premium
Suspicious inbox manipulation rules	Offline	Premium
Password spray	Offline	Premium
Impossible travel	Offline	Premium
New country	Offline	Premium
Activity from anonymous IP address	Offline	Premium
Suspicious inbox forwarding	Offline	Premium
Mass Access to Sensitive Files	Offline	Premium
Verified threat actor IP	Real-time	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Anonymous IP address	Real-time	Nonpremium
Admin confirmed user compromised	Offline	Nonpremium
Microsoft Entra threat intelligence	Real-time or Offline	Nonpremium

User risk detections

🔍 Expand table

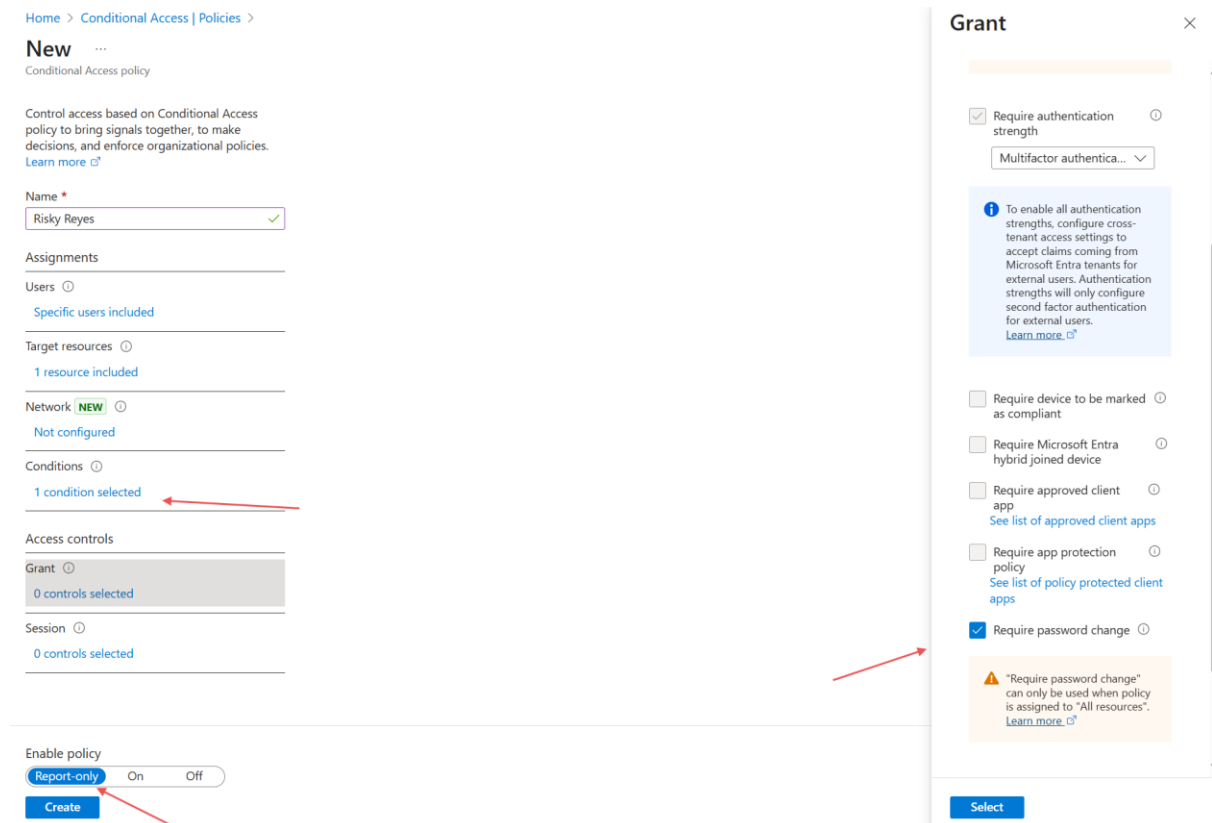
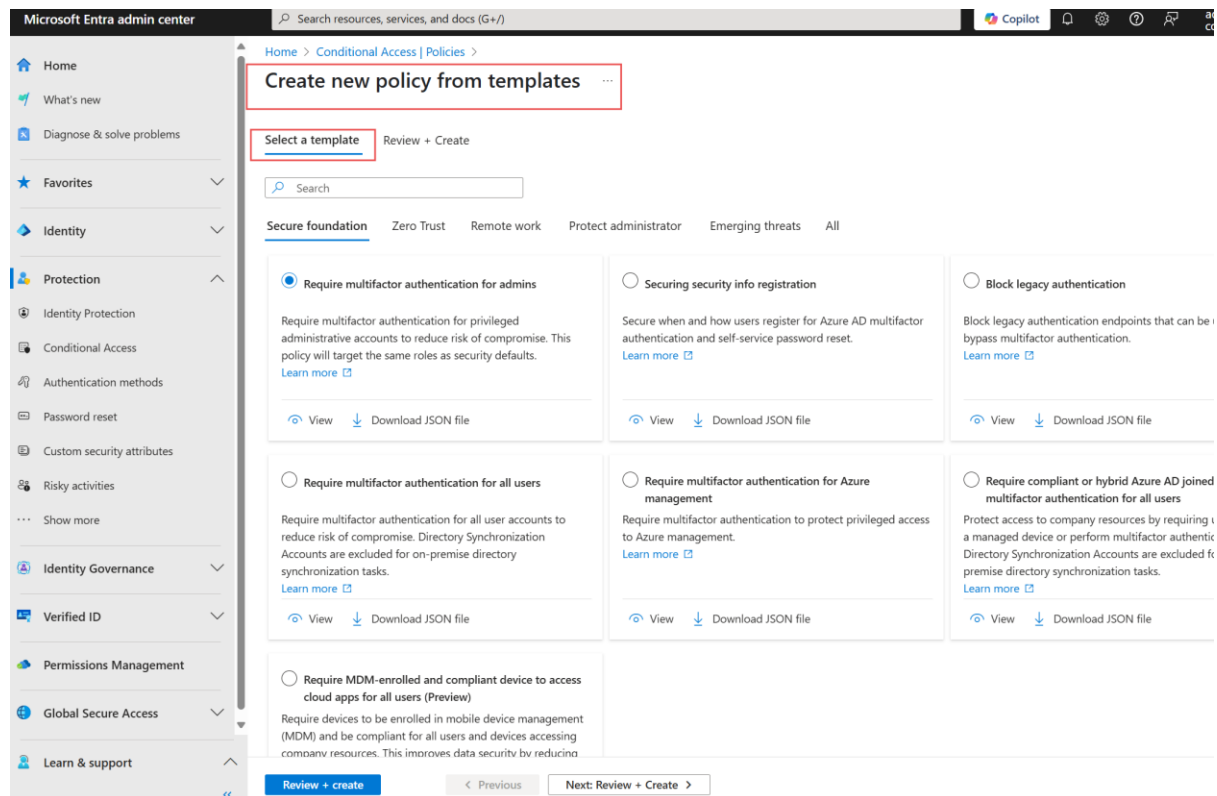
Risk detection	Detection type	Type
Possible attempt to access Primary Refresh Token (PRT)	Offline	Premium
Anomalous user activity	Offline	Premium
User reported suspicious activity	Offline	Premium
Suspicious API Traffic	Offline	Premium
Suspicious sending patterns	Offline	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Leaked credentials	Offline	Nonpremium
Microsoft Entra threat intelligence	Offline	Nonpremium

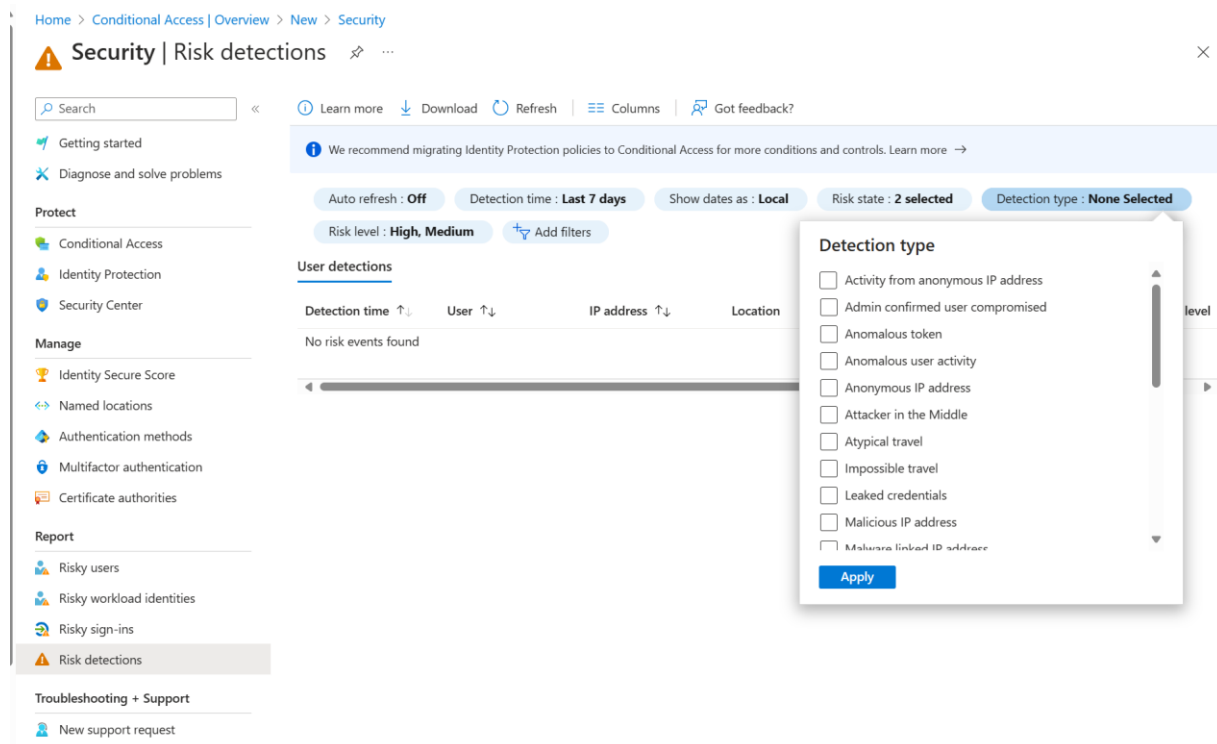
Enabling Risk Based Conditional Access can be found in entra.microsoft.com

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation pane has a red box around 'Conditional Access' with an arrow pointing to the 'Overview' tab in the main content area. The 'Overview' tab displays a 'Policy Summary' with sections for 'Policy Snapshot' (4 Enabled, 3 Report-only, 0 Off), 'Users' (1 user signed in), 'Devices' (100% of sign-ins from managed devices), and 'Applications'. Below this, there are 'What's new' notifications, including a warning about the retirement of the approved client app grant in March 2026 and a note about the Conditional Access Insider Risk policy.

The screenshot shows the 'New' Conditional Access policy configuration page. The 'Name' field is set to 'Reyes RBCA'. The 'Assignments' section shows 'All users' and '2 included' target resources. The 'Conditions' section shows '2 conditions selected'. The 'Access controls' section shows '1 control selected' and '0 controls selected'. On the right, the 'Sign-in risk' section is visible, with a 'Configure' dropdown set to 'Yes' and a 'Sign-in risk level' dropdown set to 'Medium'.

With all Conditional Access, you can enable the policy on Report Mode first





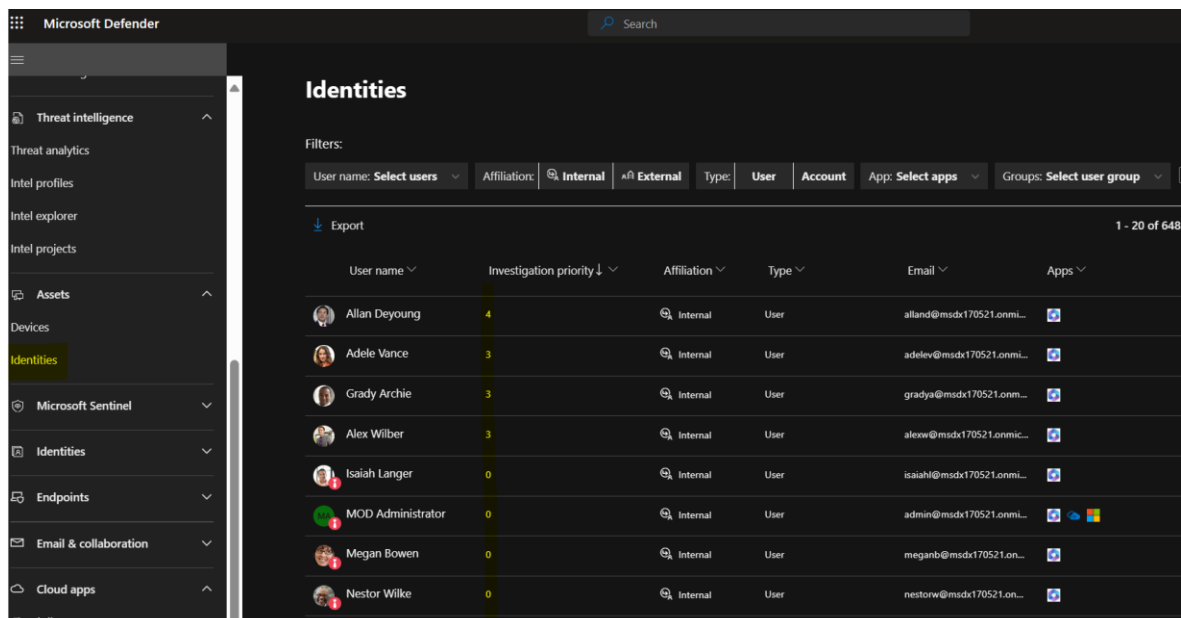
Understanding Alerts and using Incidents to Triage

[Security alerts - Microsoft Defender for Identity | Microsoft Learn](#)

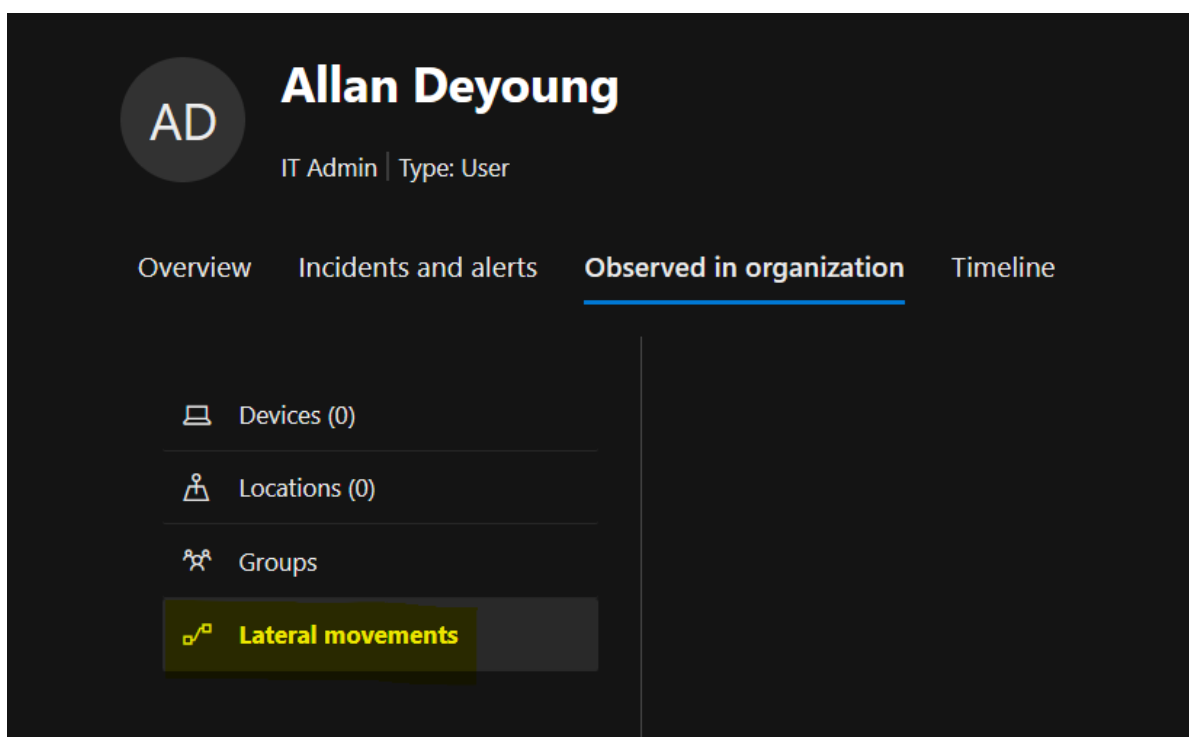
In Microsoft Defender XDR:

1. Check the **Users at risk** widget on the **Home** page or the **Entra ID users at risk** on the **Identities > Dashboard** page.
2. If you have users listed at *High risk*:
 - Select **View all users** to review high risk identities in Microsoft Entra.
 - Go to the **Identities** page and sort the grid to view users with high **Investigation priority** scores at the top. Select an identity to view the identity details page, including more details in the **Investigation priority** widget.

The investigation priority widget includes the calculated investigation priority score breakdown and a two-week trend for an identity, including whether the identity score is on the high percentile for that tenant.

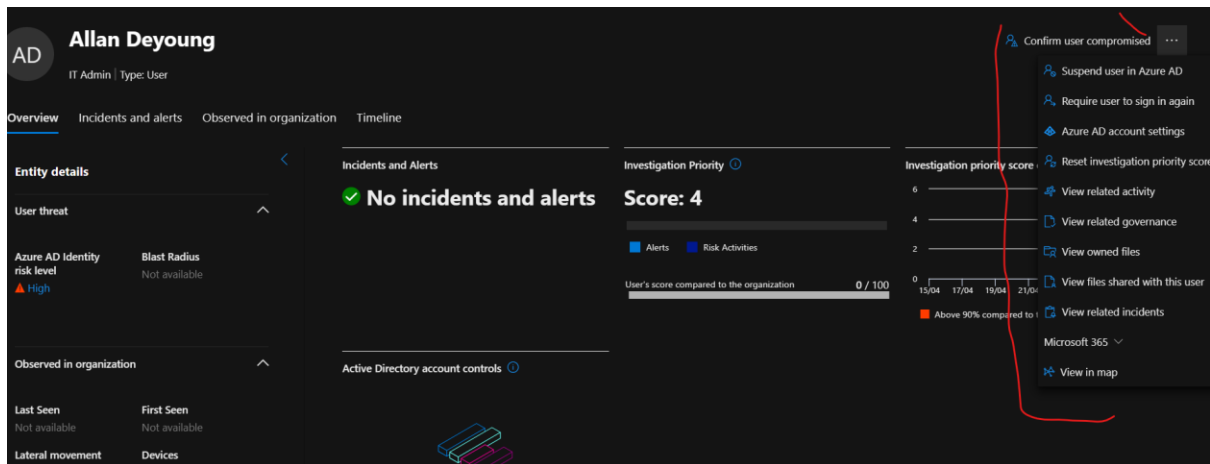


As an example, if Allan's investigation priority score is high and you get an alert, you can dive deeper in Allan's User's Page in Assets / Identities and look at a possible LMP

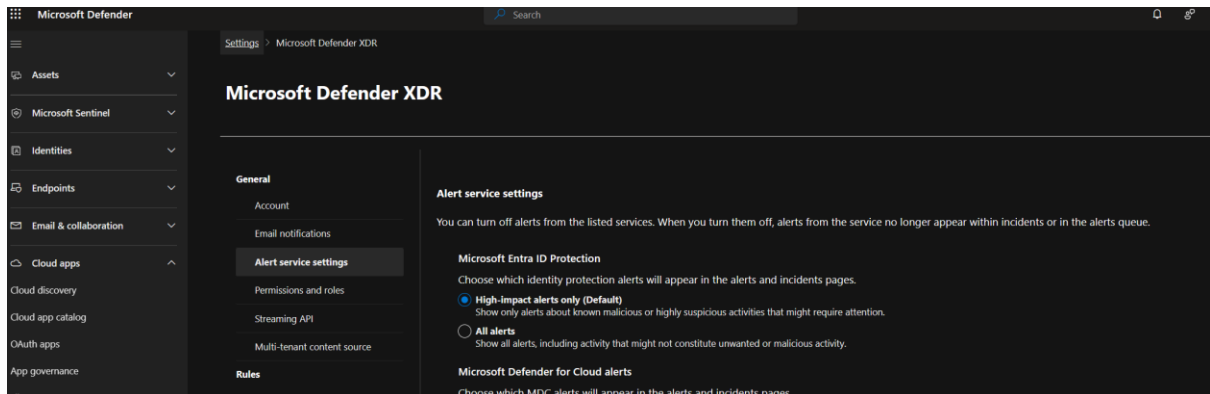


We've created a possible Lateral Movement story that could be a high confidence chance that an identity has been compromised

If you have identified Allan has been compromised, we have a bunch of native response actions we can take. This is when on-prem and cloud has that integration where if you click on compromised this can increase Allan's score in Entra and in turn puts his account at high risk which will force him to reset his password if the RBCA policies have been enabled.



To see alerts in Defender XDR Portal from Entra activities. Ensure you have the right settings



ITDR DASHBOARD



Important to note and consider

Microsoft Entra Suite

Important Update. 06.08.2024

What is Microsoft Entra Suite?

The Microsoft Entra Suite delivers a complete cloud-based solution for workforce access. It brings together identity and network access that secures employee access to any cloud or on-premises application and resource from any location, consistently enforces least privilege access, and improves the employee experience.

[Microsoft Entra Suite now generally available - Microsoft Community Hub](#)

The Microsoft Entra Suite includes the following products:



- [Microsoft Entra Private Access](#) – an identity-centric Zero Trust Network Access that secures access to private apps and resources and reduces operational complexity and cost by replacing legacy VPNs.
- [Microsoft Entra Internet Access](#) – an identity-centric Secure Web Gateway (SWG) for SaaS apps and internet traffic that protects against malicious internet traffic, unsafe or non-compliant content, and other threats from the open internet.
- [Microsoft Entra ID Governance](#) – a complete identity governance and administration solution that automates identity and access lifecycle to ensure that the right people have the right access to the right apps and services at the right time.
- [Microsoft Entra ID Protection](#) – an advanced identity solution that blocks identity compromise in real time using high-assurance authentication methods, automated risk and threat assessment, and adaptive access policies powered by advanced machine learning (also included in Microsoft Entra ID P2).
- [Microsoft Entra Verified ID](#) - a managed verifiable credentials service based on open standards that enables real-time identity verification in a secure and privacy respecting

way. Included in the Microsoft Entra Suite are premium Verified ID capabilities, starting with Face Check.

Phase 3 - Microsoft Defender for Endpoint (MDE)

Key new features since the last version of this guide, August 2024

- Two new ASR rules
 - Block rebooting machine in Safe Mode
 - Block use of copied or impersonated system tools
- [Aggregated Reporting](#)
- Fantastic 5 new demo scenarios - [Demo](#)
- BitLocker support for Device control

In this phase of Defender deployment, we will focus on MDE P2 features to deploy

Key Watch outs

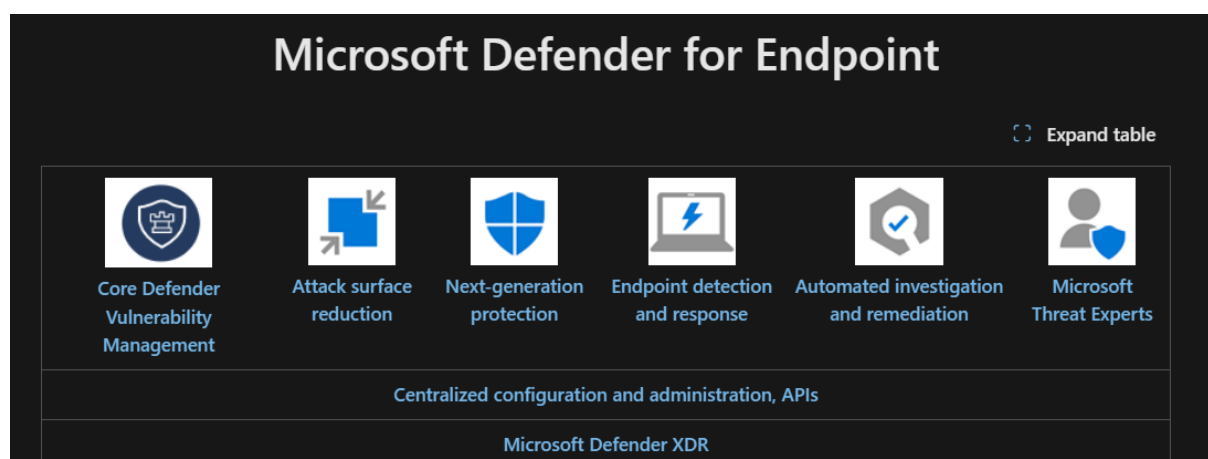
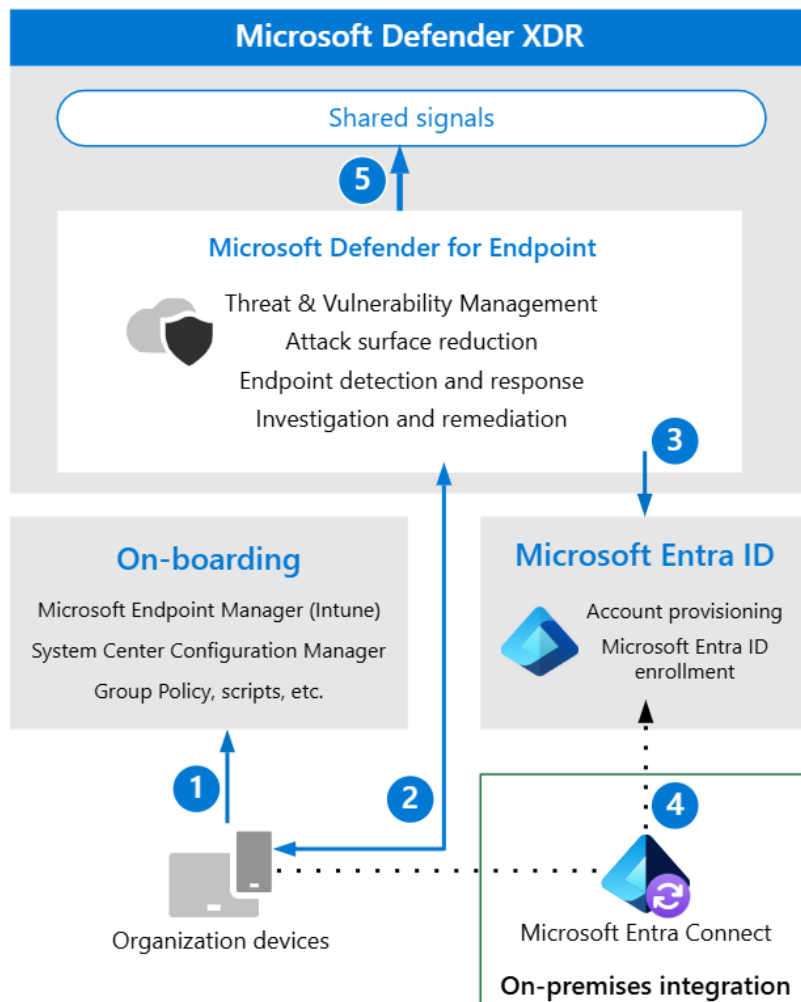
- Intune is our recommended device management tool, SCCM is not going anywhere but managing policies through SCCM does take a little bit more work. Not all policies are in SCCM, in fact most advanced policies still need to be deployed via GPO
- We recommend at least 30 days to put your ASR in audit mode to help you fine tune your policies and create exclusion where you need to.
- Passive Mode in Servers doesn't work the same as your standard Windows 10/11. You need to edit a registry key to manually set it in passive
- Plan your Server migration carefully, ensure capacity planning is one of your key focus to ensure that you don't run into issues like CPU spiking up because you haven't done your capacity planning and excluding certain files or folders

Emphasis that this doesn't need to be 3rd option to deploy but what we're doing here is following the Attack Kill Chain approach of Left to Right to protect

If you have other requirements for your devices to be onboarded to MDE, such as onboarding for Endpoint Data Loss Prevention workload or Insider Risk Management or even starting Defender for Cloud Apps to ingest data. Certainly, go ahead and onboard devices and you may choose to do that on passive mode until you're 100% ready to migrate.

When we talk about MDE P2 features, we talk about these pillars below. Our bread and butter, they're the finest features known to any endpoint protection and I've managed and deployed plenty of endpoint protection over the course of my career Security roles and I'm not even in sales or marketing, just calling it out. Maybe because when it comes to endpoint, Microsoft knows how to protect their own Operating System, our Security Engineers and our Windows engineers sit next to each other to create magic. That just make sense right?

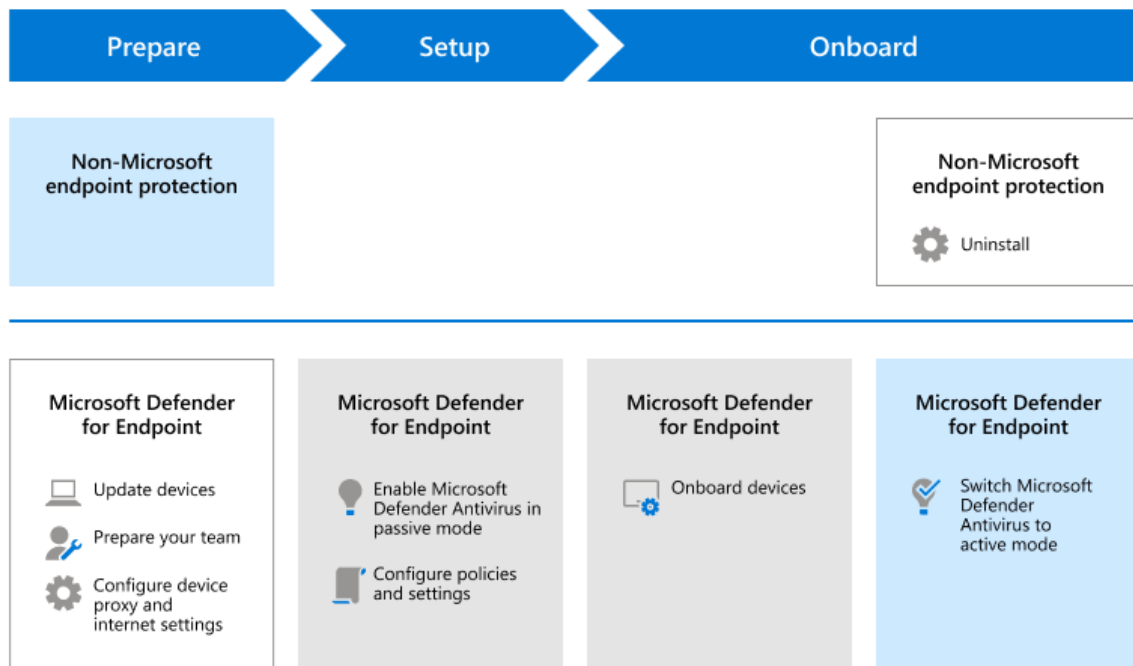
But before we jump talking about what these P2 features mean we need to onboard the devices first to MDE and architecture



Keeping with our scenario, we are assuming that we have a customer that is migrating from a 3rd party protection. Focusing on Windows 10/11 devices only on this document. You have a current 3rd party, onboarding the devices to MDE doesn't mean it will switch automatically as your primary protection. This will run in passive mode. Only when you uninstall your 3rd party protection that this will automatically switch to your primary.

The Migration Process

Migration process



Preparing Phase

In this phase, we simply call out it's important that you have all your devices up to date with windows updates/ patches and including your current 3rd party protection. Setup your custom permissions who will get access for MDE. Depending on where you're deploying your policies, folks in the end user space may need to get involved.

Setup Phase

Depending on how you plan your migration, whether you do your server migration in parallel to the end user. This is the phase you may want to consider changing the reg key so you can set AV in passive mode.

Onboarding Phase

This Phase and the next (building new policies) are commonly where most of my customers spend a lot of time, in some cases is due to the fact they have a mixture of Intune and SCCM device management or they're in a transitioning to moving everything to Intune. So, onboarding and deploying policies will need to be done in two areas. It's important to know the various infrastructure, what we recommend and what's to expect. In our scenario we will only focus on Windows Client devices but as you can see in the screenshot below, these are the OS / mobile OS we support

Architecture	Description
Cloud-native	We recommend using Microsoft Intune to onboard, configure, and remediate endpoints from the cloud for enterprises who don't have an on-premises configuration management solution or are looking to reduce their on-premises infrastructure.
Co-management	For organizations who host both on-premises and cloud-based workloads we recommend using Microsoft's ConfigMgr and Intune for their management needs. These tools provide a comprehensive suite of cloud-powered management features, and unique co-management options to provision, deploy, manage, and secure endpoints and applications across an organization.
On-premises	For enterprises who want to take advantage of the cloud-based capabilities of Microsoft Defender for Endpoint while also maximizing their investments in Configuration Manager or Active Directory Domain Services, we recommend this architecture.
Evaluation and local onboarding	We recommend this architecture for SOCs (Security Operations Centers) who are looking to evaluate or run a Microsoft Defender for Endpoint pilot, but don't have existing management or deployment tools. This architecture can also be used to onboard devices in small environments without management infrastructure, such as a DMZ (Demilitarized Zone).

Endpoint	Deployment tool
Windows	Local script (up to 10 devices) Group Policy Microsoft Intune/ Mobile Device Manager Microsoft Configuration Manager VDI scripts
Windows servers Linux servers	Integration with Microsoft Defender for Cloud
macOS	Local script Microsoft Intune JAMF Pro Mobile Device Management
Linux servers	Local script Puppet Ansible Chef Saltstack
Android	Microsoft Intune
iOS	Microsoft Intune Mobile Application Manager

Methods of Onboarding user devices - [Migrate to Microsoft Defender for Endpoint - Onboard - Microsoft Defender for Endpoint | Microsoft Learn](#)

Onboarding Servers [Onboard Windows servers to the Microsoft Defender for Endpoint service - Microsoft Defender for Endpoint | Microsoft Learn](#)

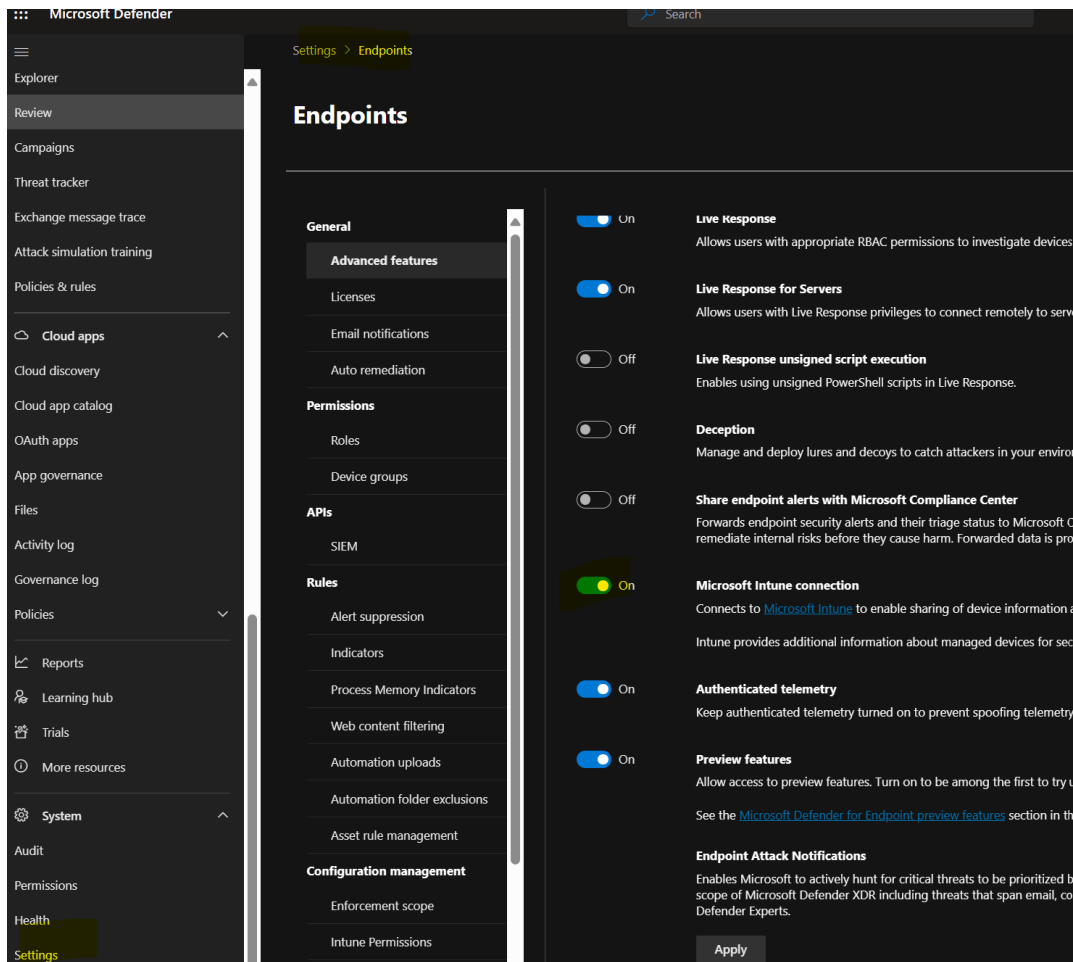
Onboarding Mac OS [Microsoft Defender for Endpoint on Mac - Microsoft Defender for Endpoint | Microsoft Learn](#)

Onboarding Linux Servers [Microsoft Defender for Endpoint plug-in for Windows Subsystem for Linux \(WSL\) - Microsoft Defender for Endpoint | Microsoft Learn](#)

Let's dive deeper on the onboarding and configuring MDE with Intune, as this is our recommendation approach and also the most common approach most of my customers are taking. Some even using this to progress their device management migration ahead of schedule from SCCM to Intune

[Configure Microsoft Defender for Endpoint in Microsoft Intune | Microsoft Learn](#)

Step 1. Enable to cross over service between MDE to Intune.



Confirm the connection has been established in Intune. The sync happens once everyday

[Home](#) > [Endpoint security](#)

 **Endpoint security | Microsoft Defender for Endpoint** ...

<<  Refresh  Save  Discard  Delete

Overview

-  Overview
-  All devices
-  Security baselines

Connection status
 Available

Last synchronized
29/04/2024, 6:52:53 pm



Now go back to Intune, Endpoint Security – and create a policy under Endpoint detection and response.

The image shows two screenshots from the Microsoft Intune admin center. The top screenshot is the 'Edit Policy' page for 'Microsoft Defender for Endpoint'. The bottom screenshot is the 'Endpoint security | Endpoint detection and response' overview page.

Top Screenshot: Edit Policy

Navigation: Home > Endpoint security | Endpoint detection and response > AllAboard >

Section: Edit Policy (Endpoint detection and response)

Tabs: Basics (selected), Configuration settings, Scope tags, Assignments, Review

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type: Auto from connector

Onboarding blob from Connector: [Redacted]

Sample Sharing: Not configured

[Deprecated] Telemetry Reporting Frequency: Not configured

Bottom Screenshot: Endpoint security | Endpoint detection and response

Navigation: Home > Endpoint security

Section: Endpoint security | Endpoint detection and response

Summary: EDR Onboarding Status

Instructions: Create an Endpoint detection and response policy to onboard devices to Microsoft Defender for Endpoint. Other options can be found in the Defender Portal. For devices that are on premises, learn more about deploying Defender for Endpoint.

Actions: Refresh, Export, Columns, Deploy preconfigured policy

Report generated 04/29/2024, 09:26 PM | 3 items

Search: [Search bar] Add filters

3 / 3

Onboarded: 3, Not Onboarded: 0, Total: 3

Device name	Managed by	Defender sensor state	Onboarding status	Last check-in
CLIENT1	Co-managed	Yes	Onboarded	29/04/2024, 2:11:50 a
CLIENT2	Co-managed	Yes	Onboarded	29/04/2024, 3:59:39 a
Ella1	Intune	Yes	Onboarded	29/04/2024, 12:54:02

Once you've established the pilot devices you're testing is done, we can now start creating our policies. Because you're coming from a 3rd party protection you may have some idea on what settings you want to re-create in MDE.

Our recommendation, and I personally like this approach is to reference our Microsoft Defender for Endpoint Baseline. This baseline has been created by our top Security Experts within Microsoft. Now, bear in mind every environment is different, so create your settings out of this baseline may have some conflicts against your environment. Or you can create a custom baseline and reference some of the recommended baseline. So, test, test and test. Use a test group to test this against

How to create a profile and using the MDE Baseline

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Endpoint security | Security baselines'. It includes a search bar, a 'Refresh' button, an 'Export' button, and a 'Columns' dropdown. A table lists various security baselines, with 'Microsoft Defender for Endpoint Security Baseline' highlighted by a red box. Below this, the 'Microsoft Defender for Endpoint baseline | Profiles' section is shown. It features a search bar, a '+ Create profile' button (indicated by a red arrow), a 'Refresh' button, an 'Export' button, and a 'Change Version' button. A table below shows the existing profile:

Profile Name	Current Baseline	Assigned
☐ MDE Baseline	Version 6	No

You will see all the settings that has been recommended, enabled. When you're testing, it's a good idea to **put the settings in audit mode**, this will give you a chance to see what will be affected or has been blocked. This is a stage where a lot of fine tuning happens from creating exclusions, talking to the business to see if irrelevant macros are still running etc.

This is also a great time to study what features and settings have been recommended to turn on, this will give you a good sense what is covered from ASR, AV, Firewall settings.

Important to note, that the baseline is not recommended for VM or VDI

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Edit profile' and shows the 'Configuration settings' tab. Under the 'Attack Surface Reduction Rules' section, the following rules are listed:

- Block Office communication apps from creating child processes (1) - Enable
- Block Adobe Reader from creating child processes (1) - Not configured
- Block Office applications from injecting code into other processes (1) - **Audit mode** (highlighted)
- Block Office applications from creating executable content (1) - Warn
- Block JavaScript or VBScript from launching downloaded executable content (1) - Block
- Enable network protection (1) - Enable
- Block untrusted and unsigned processes that run from USB (1) - Block
- Block credential stealing from the Windows local security authority subsystem (lsass.exe) (1) - Enable
- Block executable content download from email and webmail clients (1) - Block
- Block all Office applications from creating child processes (1) - Block

At first, it's a good idea to use a test group (preferably your IT), this is your walk phase, then add a little more to your pilot. Increase the numbers over time across your business. Choose your pilot users wisely so you get a good sense that everything is being tested and being feedback to

you

The screenshot shows the 'Create profile' page in the Microsoft Intune admin center. The breadcrumb trail is: Home > Endpoint security | Security baselines > Microsoft Defender for Endpoint baseline | Profiles >. The page title is 'Create profile' with a three-dot menu. Below the title is the subtitle 'Microsoft Defender for Endpoint baseline'. There are five steps in a progress bar: Basics (checked), Configuration settings (checked), Scope tags (checked), Assignments (active, highlighted with a blue bar and number 4), and Review + create (disabled, with a number 5). Under 'Included groups', there are links for 'Add groups', 'Add all users', and 'Add all devices'. A table lists the included groups:

Groups	Group Members ⓘ	Remove
MDE Test group	0 devices, 0 users	Remove

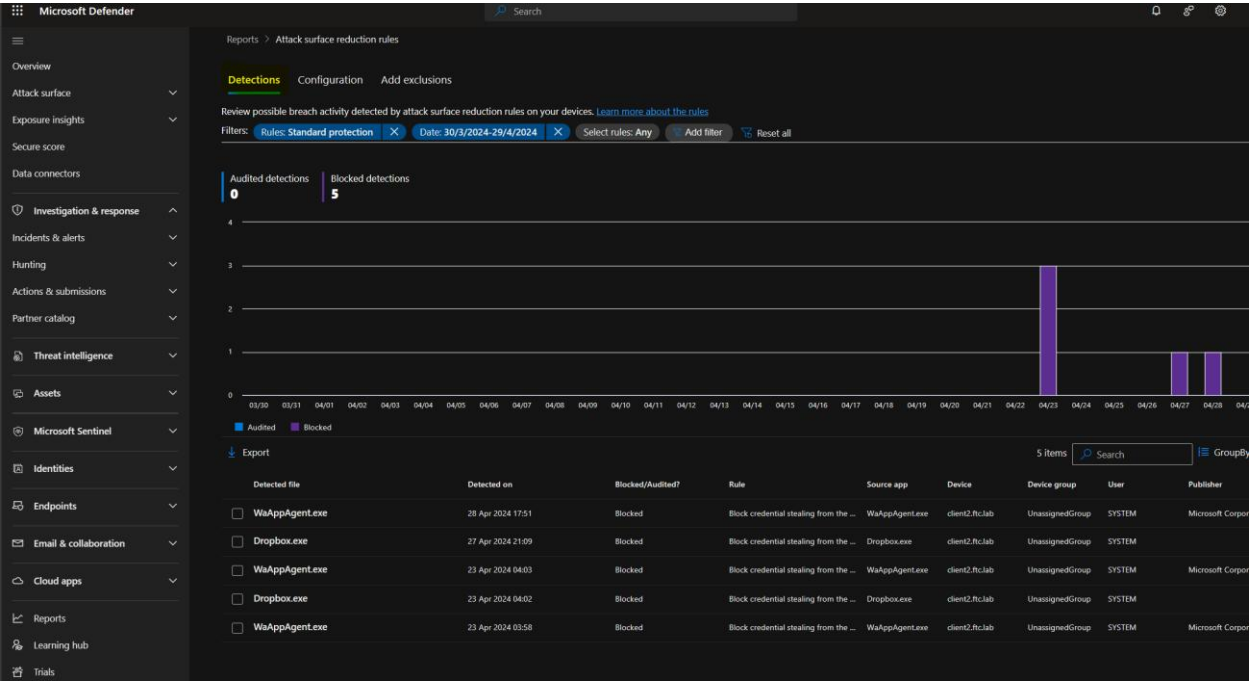
Below the table is a section for 'Excluded groups' with a link to 'Add groups'. A blue information box states: 'When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)' Below this is another table for excluded groups, which currently shows 'No groups selected'.

Reporting. When you're in the early stages you will be visiting the reports quite a bit. As an example, if we look at the ASR rules. This is to see what is being detected and being blocked. Some may be relevant to your business, and you will need to create exclusions.

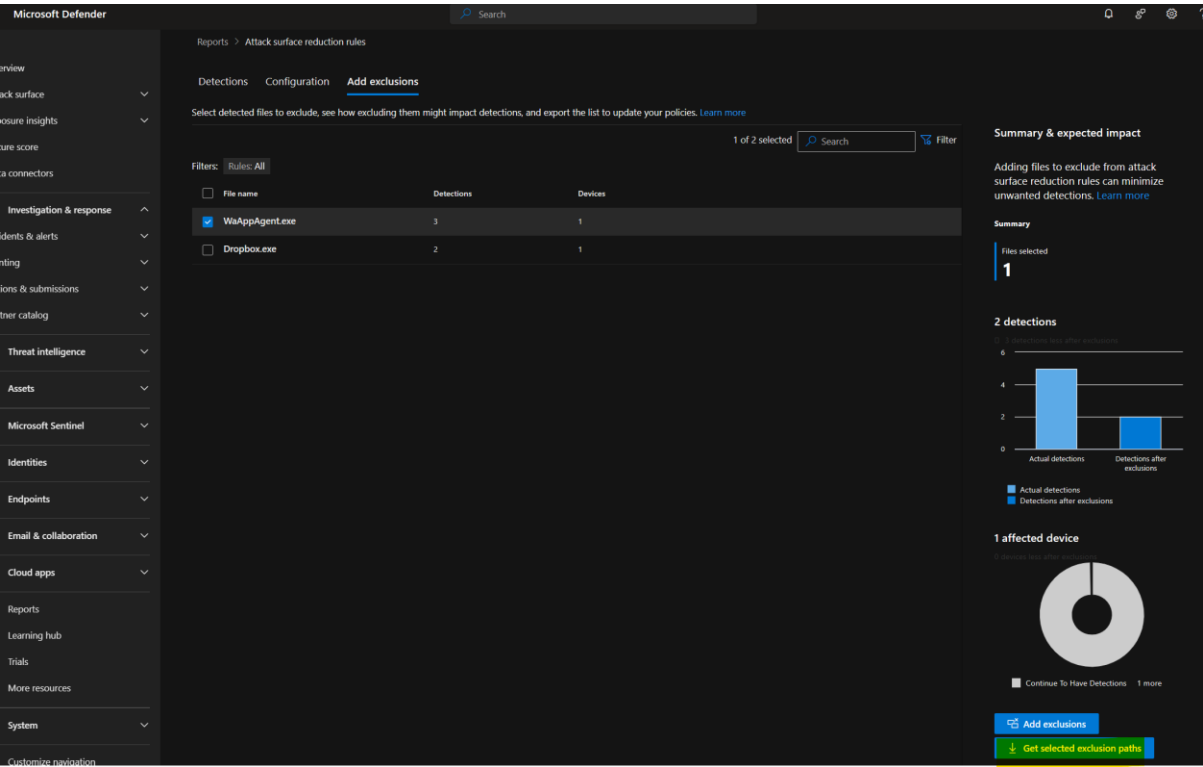
The screenshot shows the 'Reports' page in the Microsoft Defender console. The left sidebar contains a navigation menu with categories: Overview, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Reports, Learning hub, Trials, More resources, and System. The main content area is titled 'Reports' and has a subtitle: 'View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.' Below the subtitle is a list of reports, each with a 'Name' and a 'Description':

- General (2)**
 - Security report**: View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.
 - Query resources**: Review how your hunting queries consume resources and understand how to prevent throttling due to excessive use.
- Endpoints (7)**
 - Device health**: Monitor device health, antivirus software status, antivirus update versions, and operating system platforms.
 - Vulnerable devices**: View information about the vulnerable devices in your organization, including their exposure to vulnerabilities by severity level.
 - Monthly security summary**: View a monthly executive report that shows a snapshot of your organization's protection state and the work that was done to protect it.
 - Web protection**: Get information about the web activity and web threats detected within your organization.
 - Firewall**: View connections blocked by your firewall including related devices, why they were blocked, and which ports were used.
 - Device control**: This report shows your organization's media usage data.
 - Attack surface reduction rules**: View information about detections, misconfiguration, and suggested exclusions in your environment.
- Email & collaboration (4)**
 - Email & collaboration reports**: Review Microsoft recommended actions to help improve email and collaboration security.
 - Manage schedules**: Manage the schedule for the reports security teams use to mitigate and address threats to your organization.
 - Reports for download**: Download one or more of your reports.
 - Exchange mail flow reports**: Deep link to Exchange mail flow report in the Exchange admin center.
- Cloud Apps (1)**
 - Exported reports**: Exports you generated for Cloud App Discovery, Conditional Access App Control data, policies and files.
- Identities (1)**

Relevant apps are being blocked. To create an exclusion, ensure to get the path and add it to the exclusion list.



You can get the location you need on the bottom right.



Another powerful option is leveraging *Advanced Hunting* to iron out your Attack Surface rules

Using Advanced Hunting, you can produce a report on attack surface reduction rules and get in-depth information on the context of a given attack surface reduction rule audit or block event.

[Operationalize attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn](#)

Let's look at the 4 key features of MDE



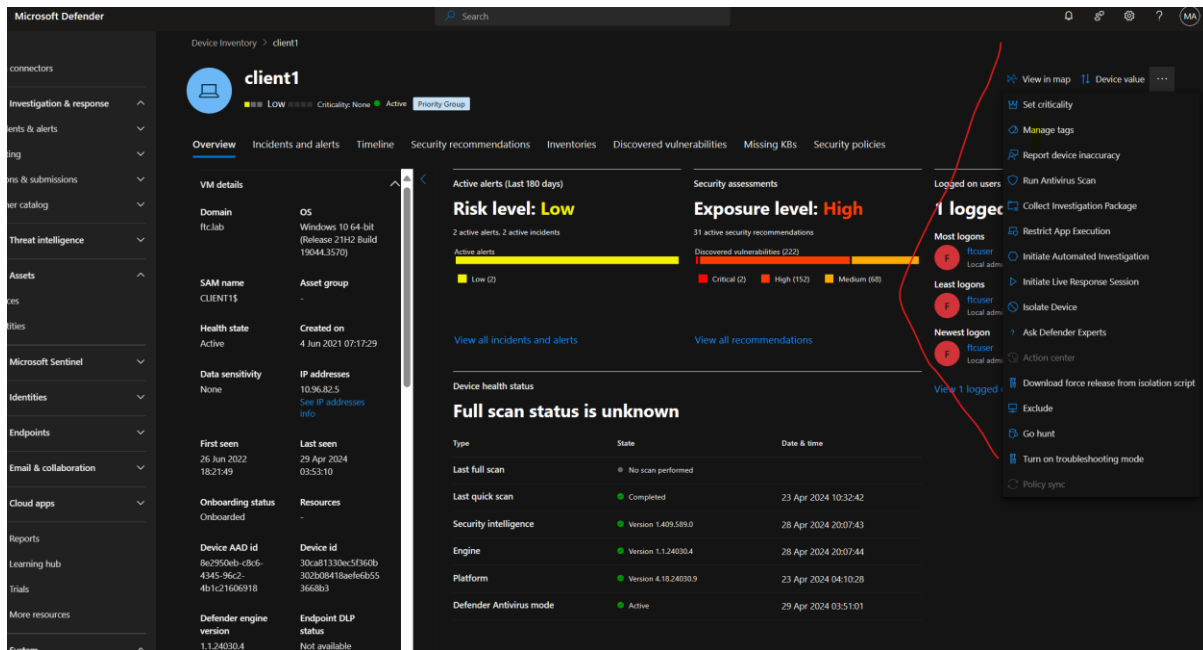
Attack Surface Reduction - [Understand and use attack surface reduction - Microsoft Defender for Endpoint | Microsoft Learn](#)

Endpoint Detection and Response (EDR) [Overview of endpoint detection and response capabilities - Microsoft Defender for Endpoint | Microsoft Learn](#)

With our EDR, we have a bunch of components that make up our EDR solution, from our alerts to incidents page where we can triage an attack, from learning about each alert that was correlated to this story. We can collect 6 months of data if we want to go that far

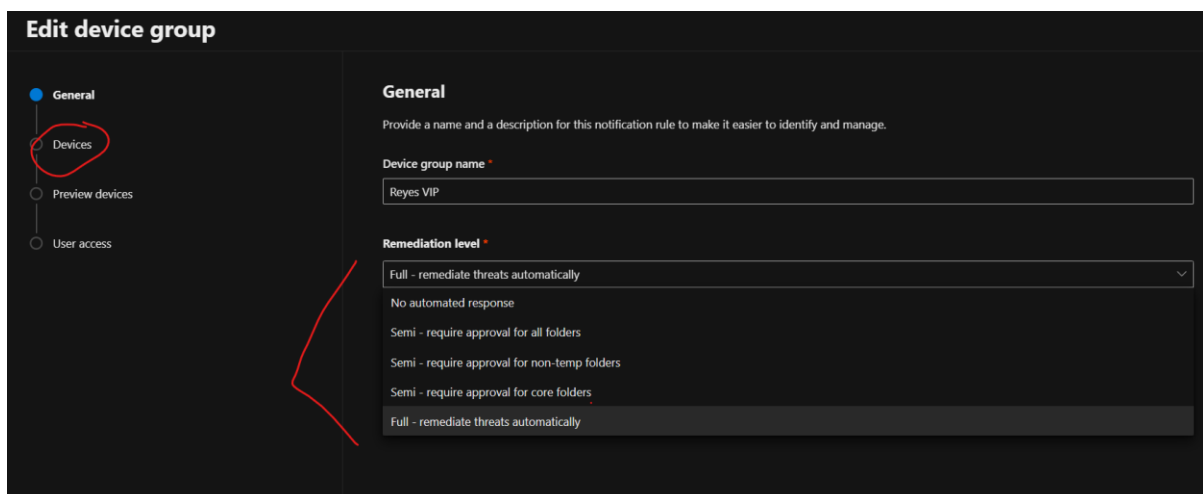
The screenshot shows the Microsoft Defender for Endpoint console. At the top, there's a header for 'Incidents' with a sub-header 'Multi-stage incident involving initial access & Collection on one endpoint reported by multiple sources'. Below this, there's a navigation bar with tabs for 'Attack story', 'Recommended actions (27)', 'Alerts (1)', 'Assets (5)', 'Investigations (4)', 'Evidence and Response (25)', and 'Summary'. The main area is divided into two sections. On the left, there's a list of alerts with details like 'Suspicious URL clicked', 'User accessed link in ZAP-queried email', and 'Suspicious email forwarding rule'. On the right, there's a detailed view of the incident, including a timeline of events, a list of affected assets, and a table of related alerts. The table has columns for 'Time', 'Alert', 'Title', 'Category', 'Severity', 'Service/Source', 'Detection/Source', 'Attack/Technique', and 'Detected'. The table shows several alerts related to the incident, including 'User compromised in AI...', 'Suspicious URL clicked', and 'Connection to a suspicious...'. The right sidebar contains a 'Multi-stage incident' summary, 'Incident details', 'Assigned to', 'Classification', 'Categories', 'First activity', 'Last activity', 'Impacted assets', and 'Users (5)'.

We also have a bunch of built-in native responses from scanning to isolating a device to running a [Live Response](#) which is a remote shell to a device and you can run a bunch of commands investigation



Auto Investigation and Remediation (AIR) Feature is one of the coolest features and it will be one of your SOC's best friend. You'll find this under Endpoint Settings.

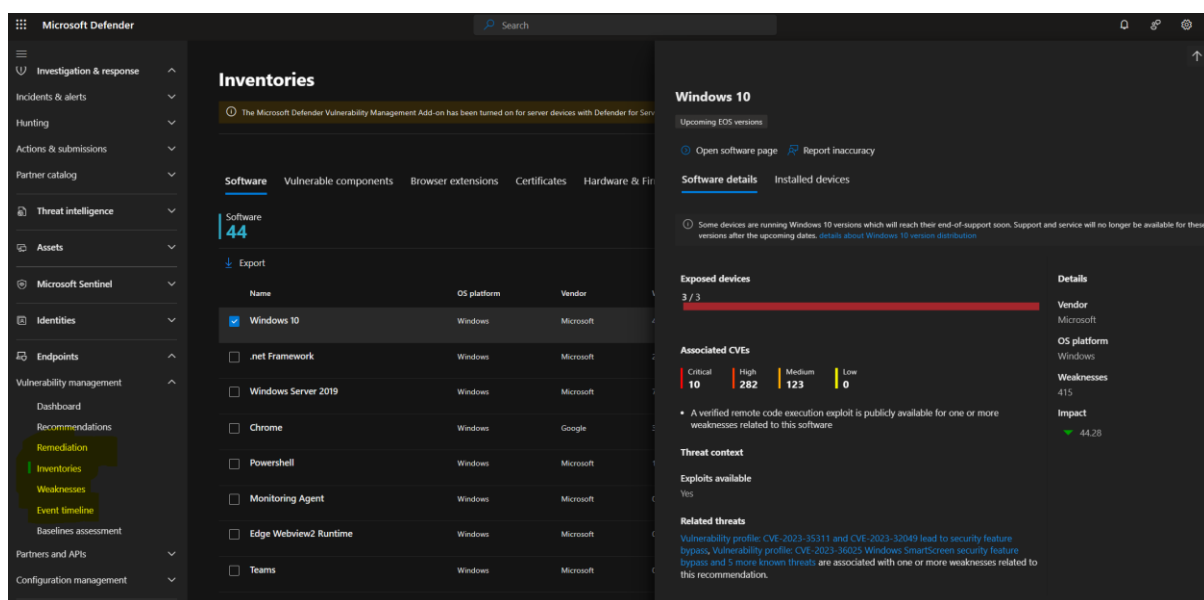
As you may have guessed, this feature essentially remediates alerts/Incidents automatically when an alert is triggered. You can also run AIR manually from the native respond buttons. Our recommendation is to use the **Full – remediation** which gives us a higher confidence to resolve malware and free up your SOC's time. You can see all that's been remediated in the Action Centre in the history tab



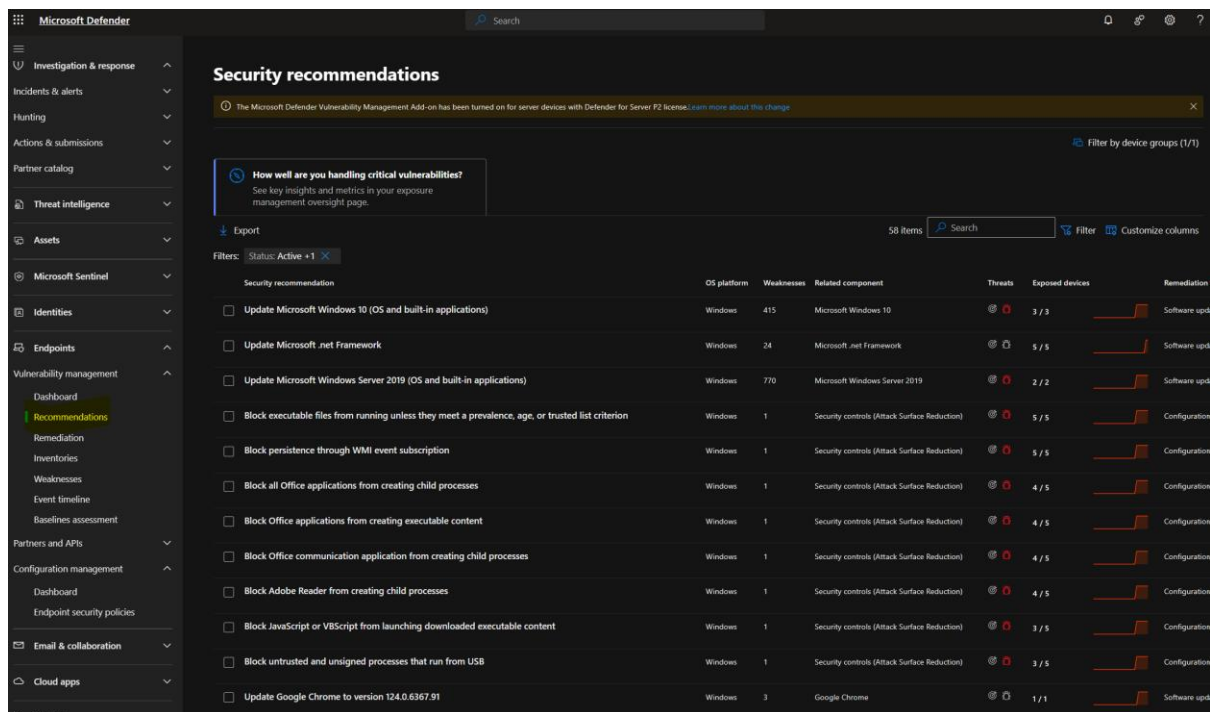
Microsoft Defender Vulnerability Management

At a high level, if we think about how Defender for Endpoint works, is that we send an onboarding package to the device, which is a small instruction set to a windows device or mac, Linux or IOS or android. server, and this onboards the device. This includes a set of instructions which highlights its tenant ID for MDE cloud service to send its singles to. We use Microsoft Sense to collect data from the device's OS from event viewer logs to Even Tracing Windows and this data is sent to the cloud service which is then correlated to data we can read in Vulnerability Management.

On the left pane under Vulnerability Management, we see a number of features. Each one highlights some sort of recommendation or update that a device or devices that are affected by vulnerability or patch is gathered together.



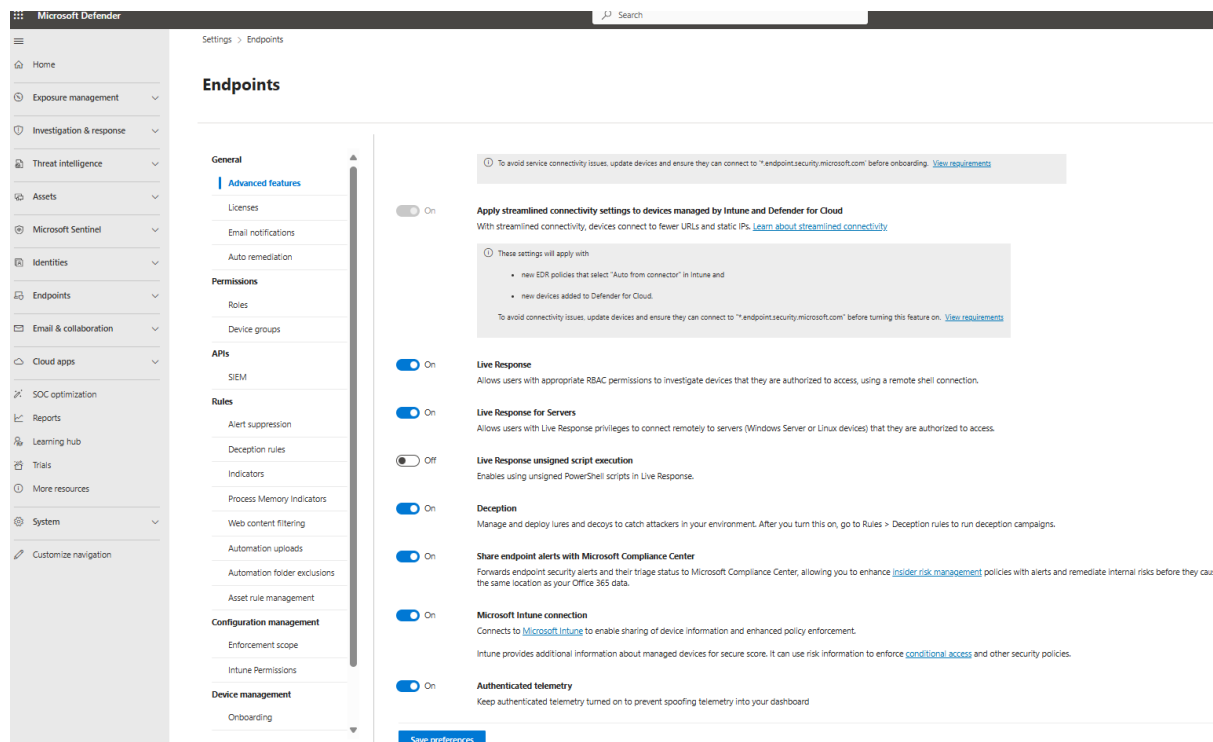
Once you've done your last group for your pilot phase, you can assess that all the recommendation has been actioned or at least be aware there's still items being recommended. You can go to Secure Score.



Once the onboarding is complete. It's important to assess all the Advanced Features under MDE – Settings. We have some default settings that are already enabled such as Tamper Protection but there are some great features to consider such as Deception or removing duplicate device records.

You can go through all the advanced features here such as Live Response, Deception feature are all great features to consider and enable.

<https://learn.microsoft.com/en-us/defender-endpoint/advanced-features>



Onboard Windows Servers to MDE

Key watch outs

- Change reg key prior to onboarding
- Capacity planning on servers

Just highlighting this as many customers do migrate their servers, as there's too many options to dive in to from Intune to configuration manager, I will just leave this link here.

[Defender for Endpoint onboarding Windows Server - Microsoft Defender for Endpoint | Microsoft Learn](#)

To onboard Windows servers to Microsoft Defender for Endpoint (MDE), you'll need to set specific registry keys. Here's a general overview of the process:

1. [Verify that the Windows Defender AV component is installed and running on the server, as it's required for MDE onboarding](#)
2. **Set the registry key** for passive mode if another antivirus solution is in place. [The key is ForceDefenderPassiveMode and you should set it to 1](#)
3. **Onboard the server** to MDE using the onboarding script from the MDE portal. [This script will modify the necessary registry entries, start the sensor service, and generate event logs](#)
4. [Check the registry entries and event logs to verify successful onboarding](#)

It's important to note that the registry key should be set **before** onboarding. [If you try to change it afterward, tamper protection may prevent the modification](#)

Here's an example of how you might set the registry key using PowerShell:

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" -Name "ForceDefenderPassiveMode" -Value 1
```

Remember to replace the path and key name with the actual ones required for your specific server version and scenario. Always ensure you have a backup of your registry before making changes, and if possible, test the changes in a non-production environment first

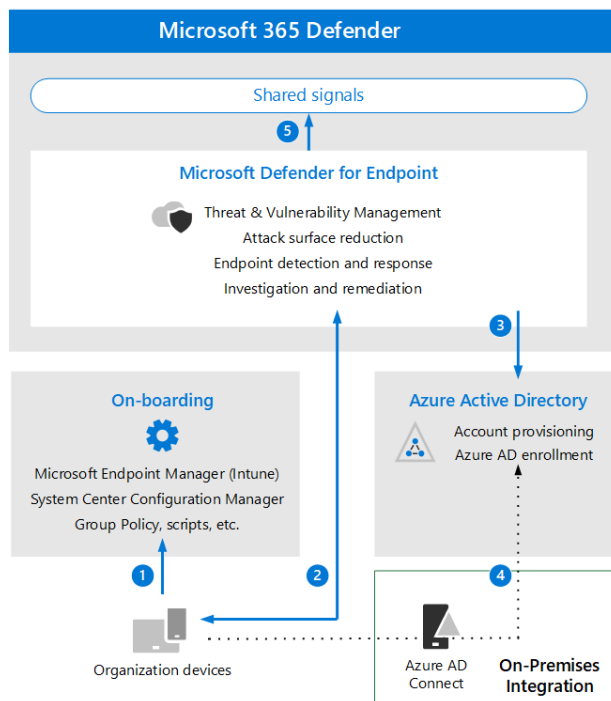
Attack Simulation Demos

We have moved our demos in public docs. None of these actual files or links are malicious, they're intended to showcase what it would look like in the real world. This is good training for SOC juniors who may not have seen what the reaction of the security tools does.

[Microsoft Defender for Endpoint demonstration scenarios - Microsoft Defender for Endpoint | Microsoft Learn](#)

Demonstrations			
The following table lists the available demonstrations alphabetically, with their associated protection area.			
 Expand table			
#	Demonstration name	Protection area	Description
1	Endpoint Detection and Response (EDR) detections	EDR	Confirm that EDR is detecting cyber threats such as malware.
2	Validate antimalware	NGP	Confirm that antivirus/antimalware is detecting and blocking malware.
3	Potentially unwanted applications (PUA) demonstration	NGP	Confirm that potentially unwanted applications (PUAs) are being blocked on your network by downloading a fake (safe) PUA file.
4	Cloud-delivered protection demonstration	NGP	Confirm that cloud-delivered protection is working properly on your computer.
5	App reputation demonstration	NGP	Navigate to the app reputation page to see the demonstration scenario using Microsoft Edge.
6	URL reputation demonstrations	NGP	Navigate to the URL Reputation page to see the demonstration scenarios using Microsoft Edge.
7	Network protection demonstrations	ASR	Navigate to a suspicious URL to trigger network protection.
8	Attack surface reduction rules (ASR rules) demonstrations	ASR	Download sample files to trigger each ASR rule.
9	Exploit protection (EP) demonstrations	ASR	Apply custom exploit protection settings.
10	Controlled folder access (CFA) demonstration (block script)	ASR	Download the CFA test tool.
11	Controlled folder access (CFA) demonstrations (block ransomware)	ASR	Download and execute a sample file to trigger CFA ransomware protection.

To get a deeper understanding of how MDE works is to look at the architecture



Phase 4. Microsoft Defender for Cloud Apps (MDA)

What's new since August 2024

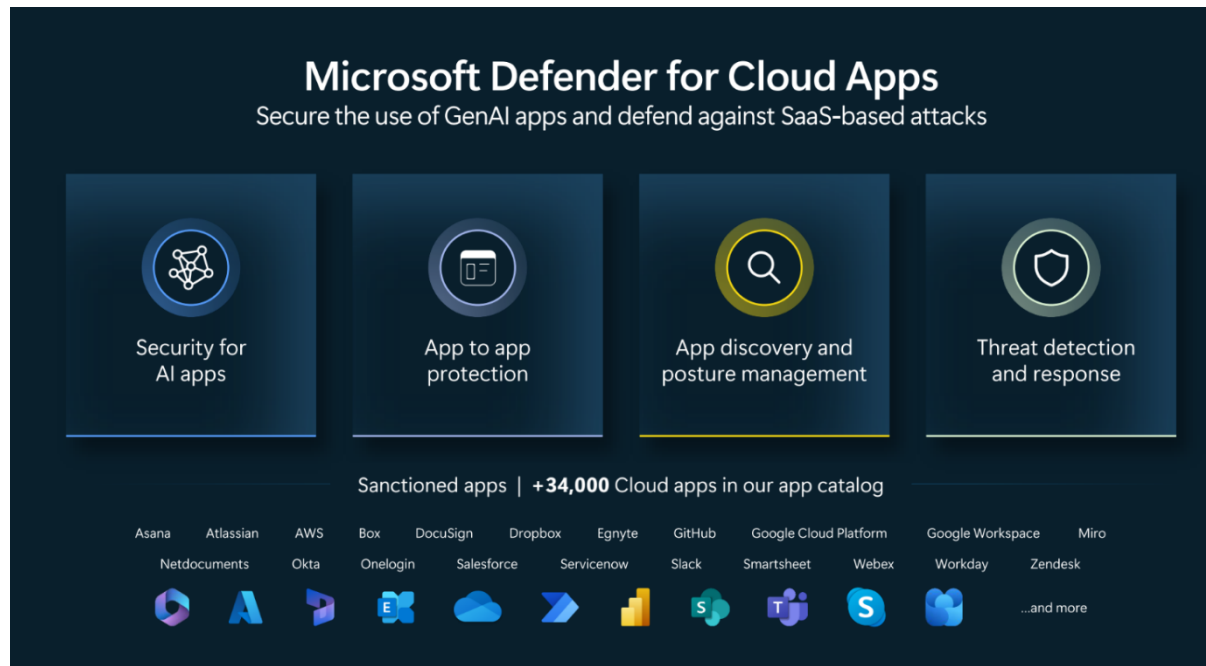
- “Behaviours” data type in Microsoft Defender for Cloud Apps
 - [Use Advanced Hunting to investigate behaviours](#)
- New Dynamic Threat Detection model
 - [Anomaly Detection Policy](#)
- New Applications inventory page now available in Defender XDR
- New and improved Cloud App Catalog page
- OAuth app information is now available in attack paths (Preview)
- SaaS Security initiative in Exposure Management

Key watch outs:

- Lots of teams involved, from Security, Compliance, to Applications Team, to Desktop Support. So really get to know this product well and what is capable of, then breakdown what your priorities are on what to deploy.
- Try to find out what Regulation your organisation follows, NIST, ISO. This will be clear when you go through the compliance section in discovery
- Ideally, you would want to have a customer's purview journey already quite mature at this stage so you can simply leverage your sensitivity labels. But this is not mandatory but would be nice

My personal favourite out of the core Defender products. I'd say it's the first XDR pillar out of the Defender stack, MDA integrates with MDE, Entra, Purview, Defender XDR, and whole lot of 3rd party SaaS apps

Our MDA isn't your ordinary CASB, as it does so many cool things, we'd like to call it a holistic SAAS security. We have four main components that make up MDA, which we will use to adopt and deploy MDA



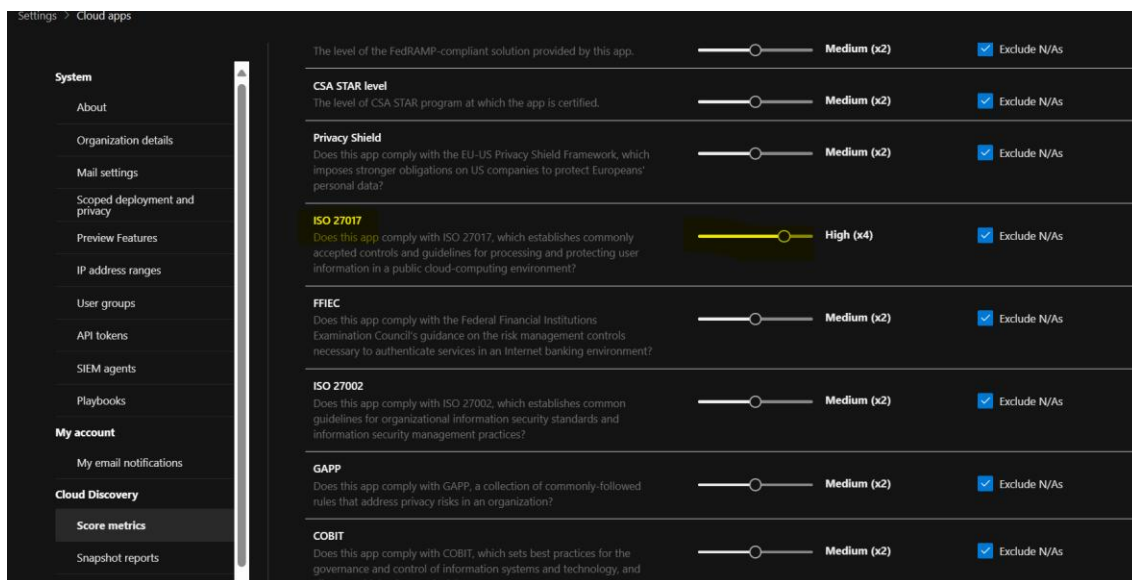
In our public docs, we have a tick list of best practice deployment but not necessarily in order. Which I will highlight some key ones to get you started

1. [Discover and assess cloud apps](#)
 - Integrating Defender for Cloud Apps with Microsoft Defender for Endpoint gives you the ability to use cloud discovery beyond your corporate network or secure web gateways
2. [Discover, monitor and protect the use of Generative AI apps](#)
 - Leveraging MDA's new and also integrating other tools such as Purview, this gives us insight on how Microsoft's security solution can come together
3. [Apply cloud governance policies](#)
 - You can secure your environment against unwanted app use
4. [Limit exposure of shared data and enforce collaboration policies](#)
 - Connecting Microsoft 365 to Defender for Cloud Apps gives you immediate visibility into your users' activities, files they are accessing, and provides governance actions for Microsoft 365, SharePoint, OneDrive, Teams, Power BI, Exchange, and Dynamics.
5. [Secure collaboration with external users by enforcing real-time session controls](#)
 - To secure collaboration in your environment, you can create a session policy to monitor sessions between your internal and external users
6. [Detect cloud threats, compromised accounts, malicious insiders, and ransomware](#)
 - Anomaly detection policies provide out-of-the-box user and entity behavioral analytics (UEBA) and machine learning (ML) so that you can immediately run advanced threat detection across your cloud environment
7. [Secure IaaS services and custom apps](#)

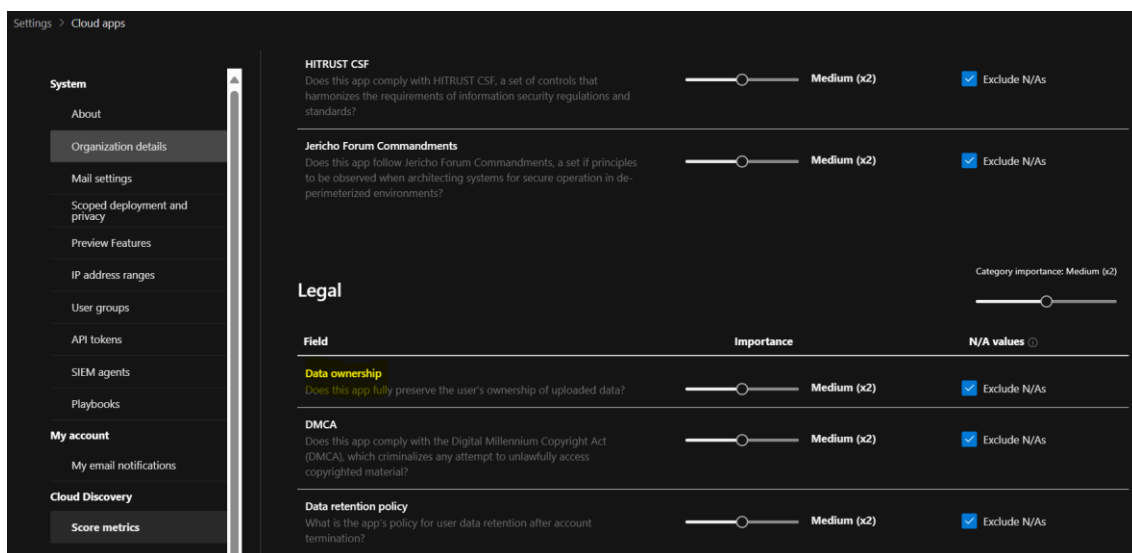
Let's dive in the Settings under Cloud Apps in Defender XDR. We will focus on a few keys must enable and consider.

Cloud Discovery features

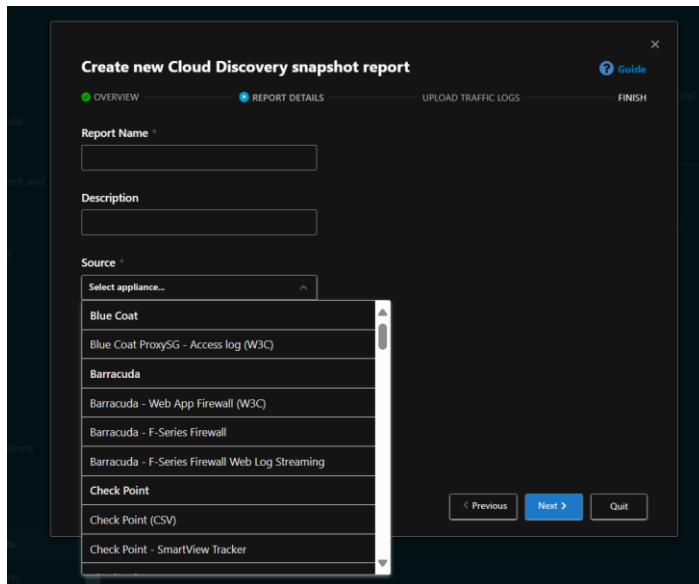
Score Metric is important to set your criteria of what is acceptable for your organisation regarding the overall Security, Compliance and Legal that applications adhere to. Say your organisation needs to be ISO compliant, you can set the criteria for ISO to High or Very High. With this change, you can typically sanction or unsanctioned any apps that's got lower than High (this is just an example). Just like Security + MFA. If an app isn't MFA enabled, this is something your company might feel very strongly in and increase that to a high. Just bear in mind that putting metrics into high may rule out a lot of apps.



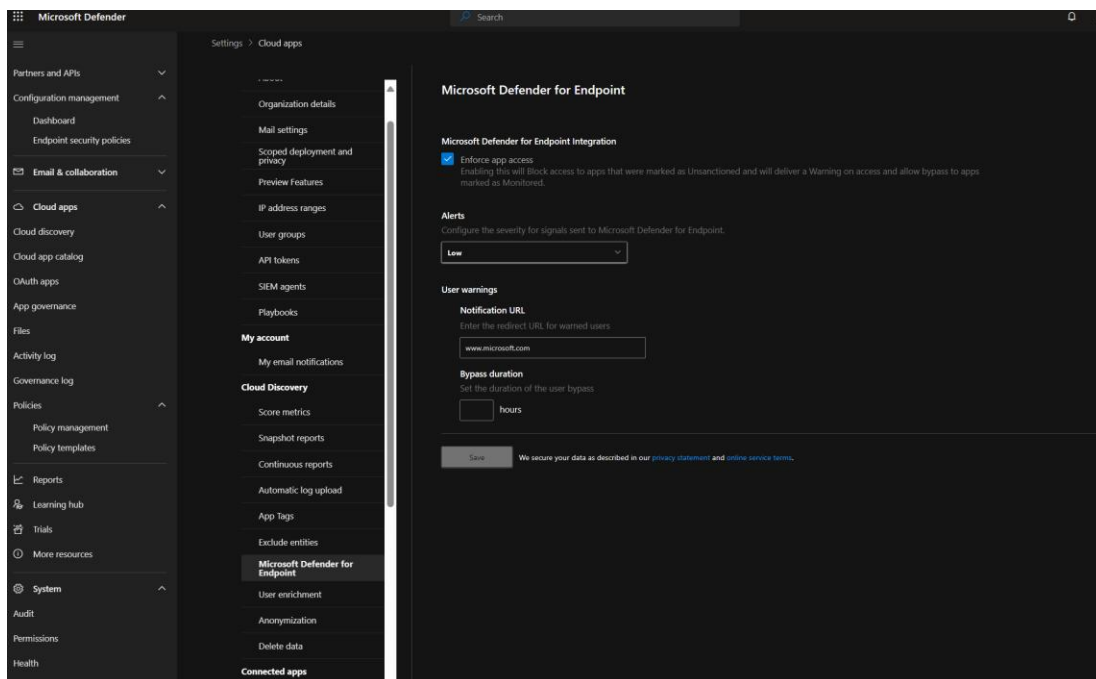
One very cool metric is Data Ownership which I don't see any other CASBs (at least me). This metric allows you to unsanctioned any apps that basically starts to own your data if you upload data into their cloud service. Which is very important to most, if not all organisation as they want to own their data no matter what.



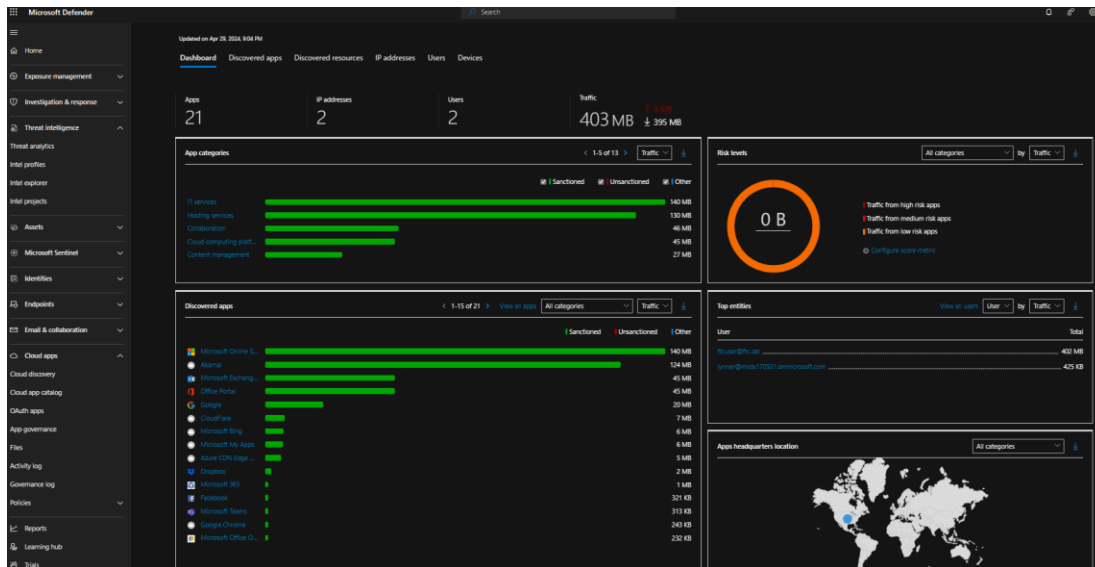
Snapshot reports is simply that, it's a sample report based on what source you may be thinking of using to digest the data from and the point of this is to give you what results it can digest. Again, our recommended log collector is MDE which is our native built-in agent which doesn't require much work to do especially if you have devices already onboarded to MDE (which at this point, I hope you do)



With your devices already onboarded to Defender for Endpoint, it's a simple toggle. [Integrate Microsoft Defender for Endpoint - Microsoft Defender for Cloud Apps | Microsoft Learn](#)



Once you've enabled MDE, the data being absorb will slowly start to be interpreted in MDA and Cloud Discovery will start to fill up. MDA absorbs the network traffic, so as soon as users starts to access websites, you'll absorb all that traffic. You'll be able to see all sorts of information from apps, traffic of uploads



One of the first key steps you can take when rolling out MDA is to view your SaaS landscape. This is sometimes a scary moment when discovering you have 1000s of apps that are unknown to anyone, but they're installed on user's devices.

You can filter your search based on acceptable score metric, what isn't compliant etc. You can go to the Discovered Apps and do an advanced filter to search for your criteria. You can build a Policy out of this search, and you can also create a custom action. So potentially anything below the score of 4, you can potential unsanctioned.

On the right side of the app, you have some native response, whether sanctioning the app or unsanctioning it or creating a Conditional Access for it.

Cloud Discovery

Updated on Apr 20, 2024, 5:04 PM

DashboardDiscovered appsDiscovered resourcesIP addressesUsersDevices

Queries: Select a query Save as

Compliance risk factorISO 27001equalsSelect value

Risk scoreequals6

Add a filter

Advanced

Browse by category

Search for category

Collaboration

Content management

Hosting services

Online meetings

Development tools

IT services

Social network

Cloud storage

Security

News and entertainment

Productivity

Business management

Cloud computing platform

Office Portal

Microsoft Exchange Online

Microsoft Teams

Microsoft 365

Microsoft Online Services

Microsoft SharePoint Online

Microsoft Live

Microsoft Skype

Microsoft Bing

Microsoft Office Online

Microsoft MSN

Microsoft Graph

Traffic

Upload

Transactions

Users

IP addresses

Devices

Last seen (UTC)

Actions

1 - 20 of 21 discovered apps

Show details

Table settings

10

20

30

40

50

60

70

80

90

100

110

120

130

140

150

160

170

180

190

200

210

220

230

240

250

260

270

280

290

300

310

320

330

340

350

360

370

380

390

400

410

420

430

440

450

460

470

480

490

500

510

520

530

540

550

560

570

580

590

600

610

620

630

640

650

660

670

680

690

700

710

720

730

740

750

760

770

780

790

800

810

820

830

840

850

860

870

880

890

900

910

920

930

940

950

960

970

980

990

1000

1010

1020

1030

1040

1050

1060

1070

1080

1090

1100

1110

1120

1130

1140

1150

1160

1170

1180

1190

1200

1210

1220

1230

1240

1250

1260

1270

1280

1290

1300

1310

1320

1330

1340

1350

1360

1370

1380

1390

1400

1410

1420

1430

1440

1450

1460

1470

1480

1490

1500

1510

1520

1530

1540

1550

1560

1570

1580

1590

1600

1610

1620

1630

1640

1650

1660

1670

1680

1690

1700

1710

1720

1730

1740

1750

1760

1770

1780

1790

1800

1810

1820

1830

1840

1850

1860

1870

1880

1890

1900

1910

1920

1930

1940

1950

1960

1970

1980

1990

2000

2010

2020

2030

2040

2050

2060

2070

2080

2090

2100

2110

2120

2130

2140

2150

2160

2170

2180

2190

2200

2210

2220

2230

2240

2250

2260

2270

2280

2290

2300

2310

2320

2330

2340

2350

2360

2370

2380

2390

2400

2410

2420

2430

2440

2450

2460

2470

2480

2490

2500

2510

2520

2530

2540

2550

2560

2570

2580

2590

2600

2610

2620

2630

2640

2650

2660

2670

2680

2690

2700

2710

2720

2730

2740

2750

2760

2770

2780

2790

2800

2810

2820

2830

2840

2850

2860

2870

2880

2890

2900

2910

2920

2930

2940

2950

2960

2970

2980

2990

3000

3010

3020

3030

3040

3050

3060

3070

3080

3090

3100

3110

3120

3130

3140

3150

3160

3170

3180

3190

3200

3210

3220

3230

3240

3250

3260

3270

3280

3290

3300

3310

3320

3330

3340

3350

3360

3370

3380

3390

3400

3410

3420

3430

3440

3450

3460

3470

3480

3490

3500

3510

3520

3530

3540

3550

3560

3570

3580

3590

3600

3610

3620

3630

3640

3650

3660

3670

3680

3690

3700

3710

3720

3730

3740

3750

3760

3770

3780

3790

3800

3810

3820

3830

3840

3850

3860

3870

3880

3890

3900

3910

3920

3930

3940

3950

3960

3970

3980

3990

4000

4010

4020

4030

4040

4050

4060

4070

4080

4090

4100

4110

4120

4130

4140

4150

4160

4170

4180

4190

4200

4210

4220

4230

4240

4250

4260

4270

4280

4290

4300

4310

4320

4330

4340

4350

4360

4370

4380

4390

4400

4410

4420

4430

4440

4450

4460

4470

4480

4490

4500

4510

4520

4530

4540

4550

4560

4570

4580

4590

4600

4610

4620

4630

4640

4650

4660

4670

4680

4690

4700

4710

4720

4730

4740

4750

4760

4770

4780

4790

4800

4810

4820

4830

4840

4850

4860

4870

4880

4890

4900

4910

4920

4930

4940

4950

4960

4970

4980

4990

5000

5010

5020

5030

5040

5050

5060

5070

5080

5090

5100

5110

5120

5130

5140

5150

5160

5170

5180

5190

5200

5210

5220

5230

5240

5250

5260

5270

5280

5290

5300

5310

5320

5330

5340

5350

5360

5370

5380

5390

5400

5410

5420

5430

5440

5450

5460

5470

5480

5490

5500

5510

5520

5530

5540

5550

5560

5570

5580

5590

5600

5610

5620

5630

5640

5650

5660

5670

5680

5690

5700

5710

5720

5730

5740

5750

5760

5770

5780

5790

5800

5810

5820

5830

5840

5850

5860

5870

5880

5890

5900

5910

5920

5930

5940

5950

5960

5970

5980

5990

6000

6010

6020

6030

6040

6050

6060

6070

6080

6090

6100

6110

6120

6130

6140

6150

6160

6170

6180

6190

6200

6210

6220

6230

6240

6250

6260

6270

6280

6290

6300

6310

6320

6330

6340

6350

6360

6370

6380

6390

6400

6410

6420

6430

6440

6450

6460

6470

6480

6490

6500

6510

6520

6530

6540

6550

6560

6570

6580

6590

6600

6610

6620

6630

6640

6650

6660

6670

6680

6690

6700

6710

6720

6730

6740

6750

6760

6770

6780

6790

6800

6810

6820

6830

6840

6850

6860

6870

6880

6890

6900

6910

6920

6930

6940

6950

6960

6970

6980

6990

7000

7010

7020

7030

7040

7050

7060

7070

7080

7090

7100

7110

7120

7130

7140

7150

7160

7170

7180

7190

7200

7210

7220

7230

7240

7250

7260

7270

7280

7290

7300

7310

7320

7330

7340

7350

7360

7370

7380

7390

7400

7410

7420

7430

7440

7450

7460

7470

7480

7490

7500

7510

7520

7530

7540

7550

7560

7570

7580

7590

7600

7610

7620

7630

7640

7650

7660

7670

7680

7690

7700

7710

7720

7730

7740

7750

7760

7770

7780

7790

7800

7810

7820

7830

7840

7850

7860

7870

7880

7890

7900

7910

7920

7930

7940

7950

7960

7970

7980

7990

8000

8010

8020

8030

8040

8050

8060

8070

8080

8090

8100

8110

8120

8130

8140

8150

8160

8170

8180

8190

8200

8210

8220

8230

8240

8250

8260

8270

8280

8290

8300

8310

8320

8330

8340

8350

8360

8370

8380

8390

8400

8410

8420

8430

8440

8450

8460

8470

8480

8490

8500

8510

8520

8530

8540

8550

8560

8570

8580

8590

8600

8610

8620

8630

8640

8650

8660

8670

8680

8690

8700

8710

8720

8730

8740

8750

8760

8770

8780

8790

8800

8810

8820

8830

8840

8850

8860

8870

8880

8890

8900

8910

8920

8930

8940

8950

8960

8970

8980

8990

9000

9010

9020

9030

9040

9050

9060

9070

9080

9090

9100

9110

9120

9130

9140

9150

9160

9170

9180

9190

9200

9210

9220

9230

9240

9250

9260

9270

9280

9290

9300

9310

9320

9330

9340

9350

9360

9370

9380

9390

9400

9410

9420

9430

9440

9450

9460

9470

9480

9490

9500

9510

9520

9530

9540

9550

9560

9570

9580

9590

9600

9610

9620

9630

9640

9650

9660

9670

9680

9690

9700

9710

9720

9730

9740

9750

9760

9770

9780

9790

9800

9810

9820

9830

9840

9850

9860

9870

9880

9890

9900

9910

9920

9930

9940

9950

9960

9970

9980

9990

10000

10010

10020

10030

10040

10050

10060

10070

10080

10090

10100

10110

10120

10130

10140

10150

10160

10170

10180

10190

10200

10210

10220

10230

10240

10250

10260

10270

10280

10290

10300

10310

10320

10330

10340

10350

10360

10370

10380

10390

10400

10410

10420

10430

10440

10450

10460

10470

10480

10490

10500

10510

10520

10530

10540

10550

10560

10570

10580

10590

10600

10610

10620

10630

10640

10650

10660

10670

10680

10690

10700

10710

10720

10730

10740

10750

10760

10770

10780

10790

10800

10810

10820

10830

10840

10850

10860

10870

10880

10890

10900

10910

10920

10930

10940

10950

10960

10970

10980

10990

11000

11010

11020

11030

11040

11050

11060

11070

11080

11090

11100

11110

11120

11130

11140

11150

11160

11170

11180

11190

11200

11210

11220

11230

11240

11250

11260

11270

11280

11290

11300

11310

11320

11330

11340

11350

11360

11370

11380

11390

11400

11410

11420

11430

11440

11450

11460

11470

11480

11490

11500

11510

11520

11530

11540

11550

11560

11570

11580

11590

11600

11610

11620

11630

11640

11650

11660

11670

11680

11690

11700

11710

11720

11730

11740

11750

11760

11770

11780

11790

11800

11810

11820

11830

11840

11850

11860

11870

11880

11890

11900

11910

11920

11930

11940

11950

11960

11970

11980

11990

12000

12010

12020

12030

12040

12050

12060

12070

12080

12090

12100

12110

12120

12130

12140

12150

12160

12170

12180

12190

12200

12210

12220

12230

12240

12250

12260

12270

12280

12290

12300

12310

12320

12330

12340

12350

12360

12370

12380

12390

12400

12410

12420

12430

12440

12450

12460

12470

12480

12490

12500

12510

12520

12530

12540

12550

12560

12570

12580

12590

12600

12610

12620

12630

12640

12650

12660

12670

12680

12690

12700

12710

12720

12730

12740

12750

12760

12770

12780

12790

12800

12810

12820

12830

12840

12850

12860

12870

12880

12890

12900

12910

12920

12930

12940

12950

12960

12970

12980

12990

13000

13010

13020

13030

13040

13050

13060

13070

13080

13090

13100

13110

This is a good segway to how we Discover, monitor and protect the use of Generative AI apps

We are in a global midst of the Generative AI apps sprawl and MDA can provide ways to enable organisations to safely interact with these apps and continue being productive and add value to the organisation. Defender for Cloud Apps discovery capabilities continue to extend every month as Gen AI apps to continue to grow.

Defender for Cloud App is just one part of a holistic approach. Natively, across our Defender / Purview stack, we can provide a more in-depth protection. Given the number of ways GenAI attack can happen, we need to leverage various pillars to protect our environment from endpoints to data security



You can proactively govern Generative AI on your environment by un-sanctioning ones that don't make compliance or simply allowing ones that you have allowed

The screenshot shows the 'Cloud app catalog' in Microsoft Defender. The left sidebar contains navigation options like Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog (highlighted), OAuth apps, and App governance. The main area is titled 'Cloud app catalog' and features filters for Apps, App tag (Sanctioned, Unsanctioned, None), Risk score (0 to 10), and Compliance risk factor (Select factors). Below the filters, there's a 'Browse by category' section with 'Generative AI' (413 items) and 'Business intelligence' (389 items) highlighted. The main table lists various apps with their risk scores and actions. The table has columns for App, Risk score, and Actions. The apps listed are Microsoft Bing Chat, Microsoft Designer, Amazon Polly, Dialogflow, Adobe Firefly, Google Bard, Google Assistant, and Google DeepMind.

App	Risk score	Actions
Microsoft Bing Chat Generative AI	10	ⓘ ⚙️ ⌵ ⌶
Microsoft Designer Generative AI	10	ⓘ ⚙️ ⌵ ⌶
Amazon Polly Generative AI	10	ⓘ ⚙️ ⌵ ⌶
Dialogflow Generative AI	10	ⓘ ⚙️ ⌵ ⌶
Adobe Firefly Generative AI	10	ⓘ ⚙️ ⌵ ⌶
Google Bard Generative AI	9	ⓘ ⚙️ ⌵ ⌶
Google Assistant Generative AI	9	ⓘ ⚙️ ⌵ ⌶
Google DeepMind	9	ⓘ ⚙️ ⌵ ⌶

The screenshot shows the 'Create app discovery policy' form in Microsoft Defender. The form includes fields for Policy template (No template), Policy name (New Generative AI apps), Policy severity (3 red squares), and Category (Cloud Discovery). The Description field contains the text: 'Trigger an alert when a new Generative AI app has been used in the environment.' Below the description, there's a section for 'Apps matching all of the following' with a filter set to 'Category equals Generative AI'. The 'Apply to' section is set to 'All continuous reports'. At the bottom, there's a checkbox labeled 'Trigger a policy match if all the following occur on the same day:' which is checked.

Create app discovery policy

Cloud Discovery policies enable you to create alerts for new apps that are discovered in your organization.

Policy template *
No template

Policy name *
New Generative AI apps

Policy severity *
[3 red squares]

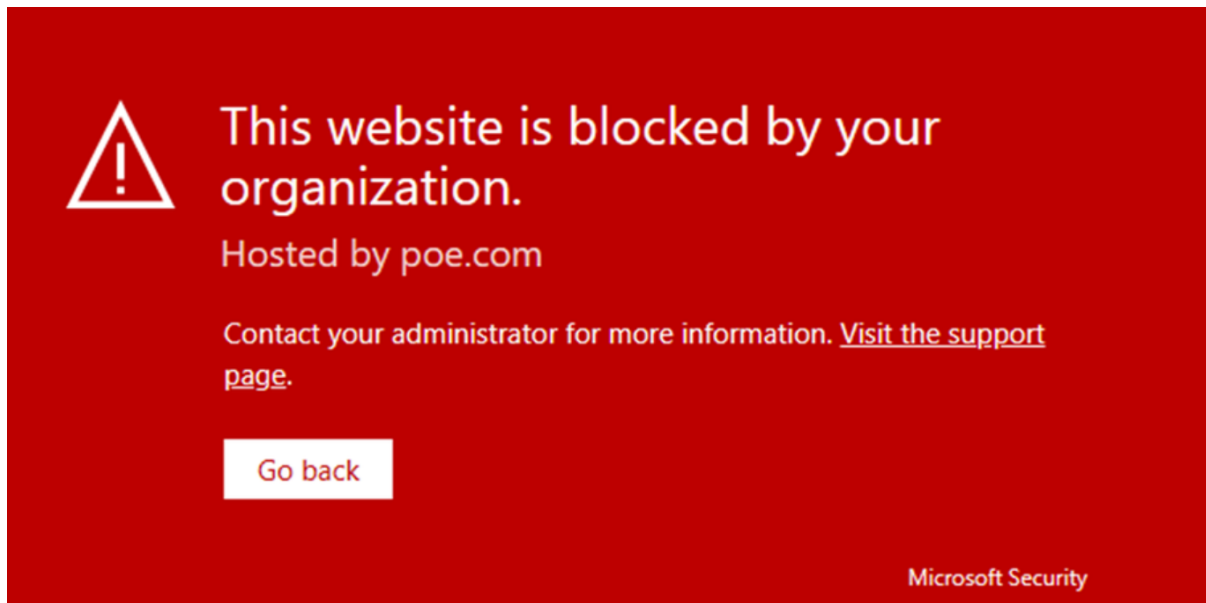
Category *
Cloud Discovery

Description
Trigger an alert when a new Generative AI app has been used in the environment.

Apps matching all of the following
Category equals Generative AI

Apply to:
All continuous reports

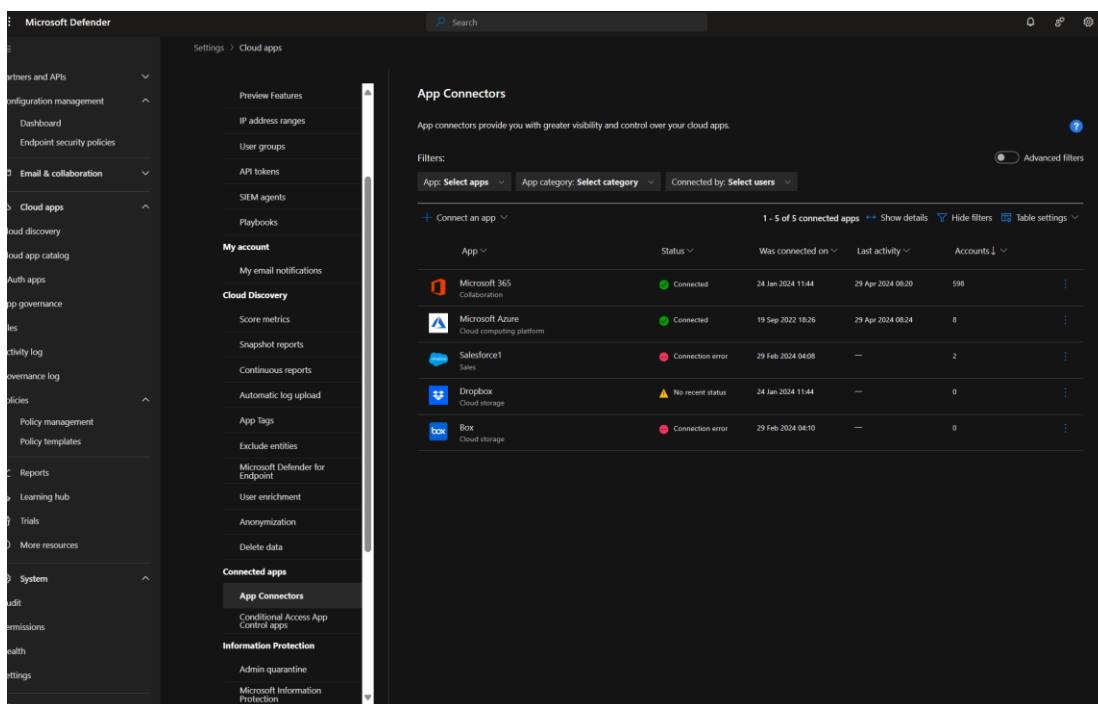
☒ Trigger a policy match if all the following occur on the same day:



Another the key feature in MDA is Connected Apps. We recommend connecting at minimum your M365 and Azure to get a deeper visibility on that platform and integrate products like Purview and Conditional Access from Entra ID

Using an app connector, we're able to get deeper visibility on apps, user list, data scan, governance, app permission etc. not all apps is able to give the same visibility. Here is the full doc on how this works

[Connect apps to get visibility and control - Microsoft Defender for Cloud Apps | Microsoft Learn](#)

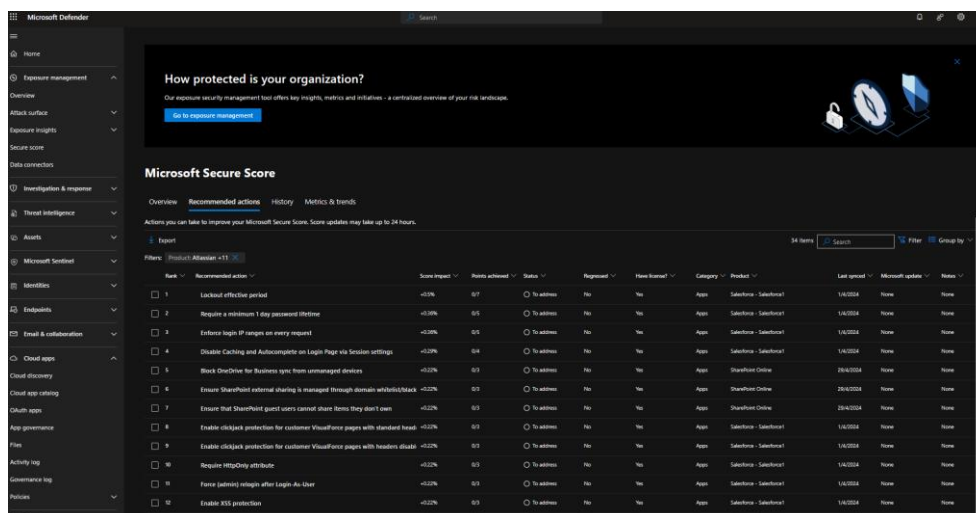


SaaS Security Posture Management

Using this feature as a proactive security investigation.

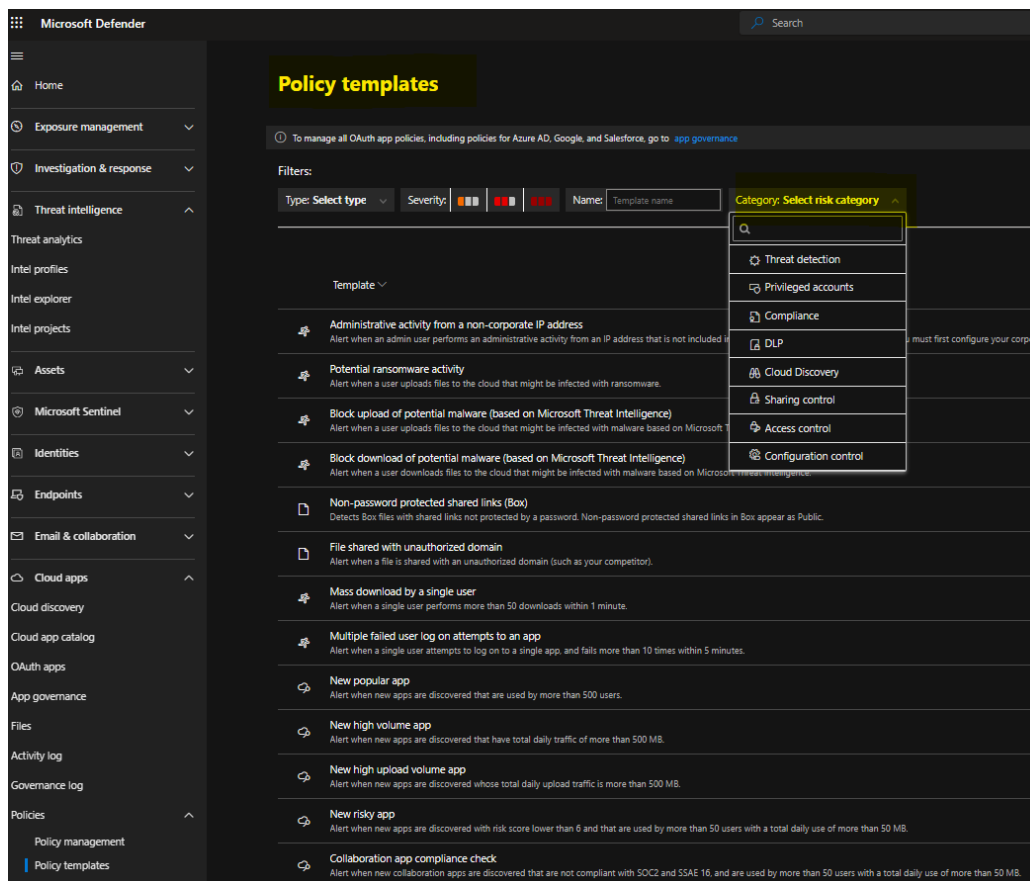
By working closely with 3rd party apps and building integration with our platform and theirs, we need to be able to detect and respond to misconfiguration. SSPM allows us to recommend at a deepest level when 3rd party apps are not configured correctly.

[Turn on and manage SaaS security posture management \(SSPM\) - Microsoft Defender for Cloud Apps | Microsoft Learn](#)

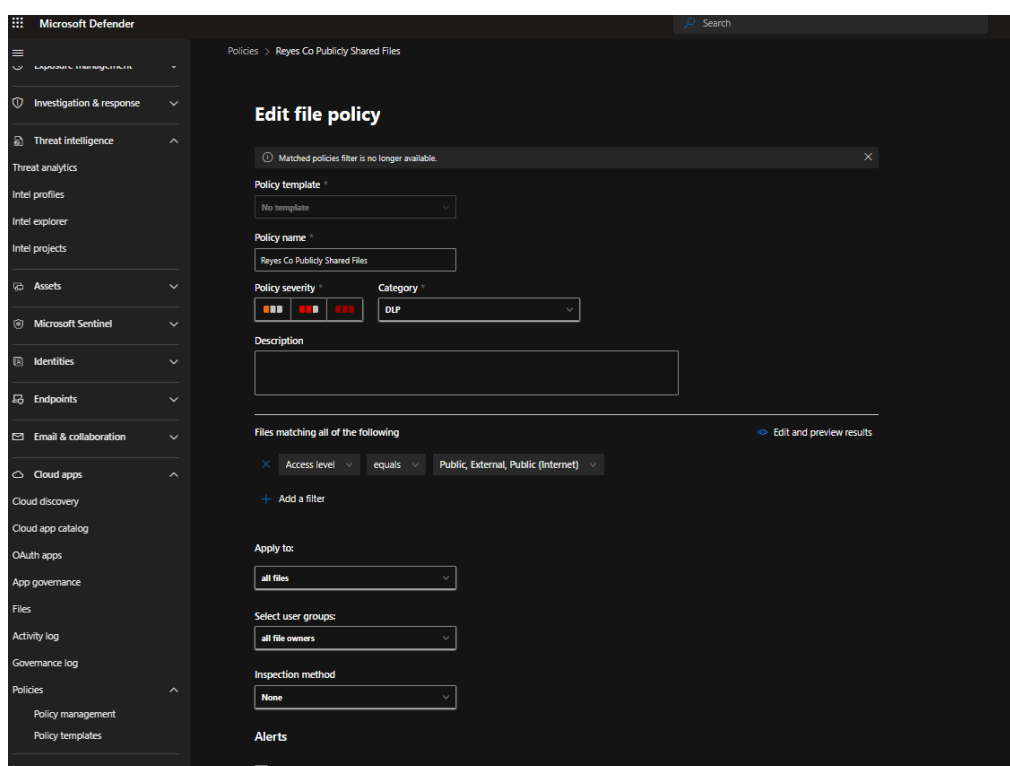


You can find all the policy templates under Cloud Apps – Policies – Policy Template

You can switch categories to see any templates that could be useful or you can also create your own – All the template policies [Control cloud apps with policies - Microsoft Defender for Cloud Apps | Microsoft Learn](#)

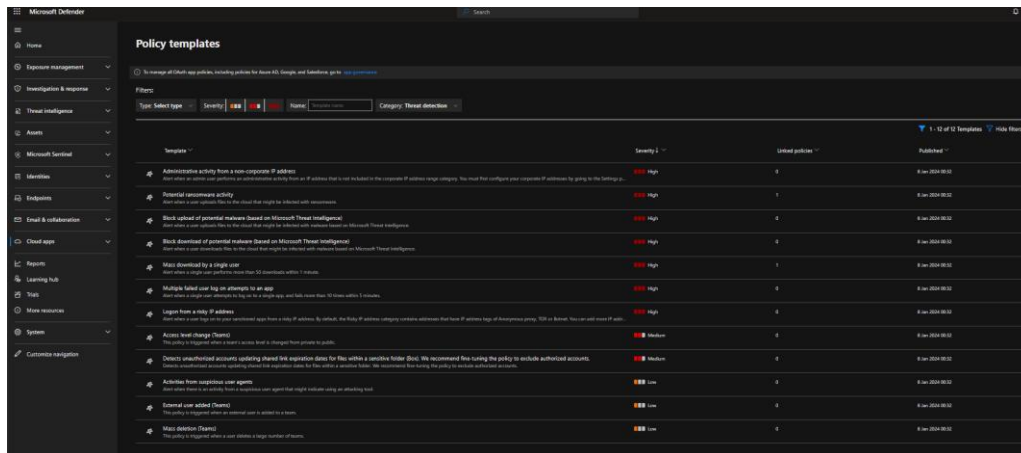


Two common ones you can test and apply are: 1. What's being shared publicly so you can see what's been shared outside the business 2. Apply Sensitive Info types on content throughout apps that is relevant to your organisation, in this scenario it would be ones that we've used to connectors for



Threat Protection

We have a bunch of policy template for Threat Protection. If a policy has been triggered, the alert/s will be correlated in our alert/incidents page in Defender XDR, and you can triage this like any other incident and be able to trace the attack story.



Last of the policy templates is the integration with our very own Entra's Conditional Access.

[Conditional access app control - Microsoft Defender for Cloud Apps | Microsoft Learn](#)

Microsoft Defender for Cloud Apps integrates with any identity provider (IdP) to deliver this protection with [access](#) and [session](#) policies.

For example:

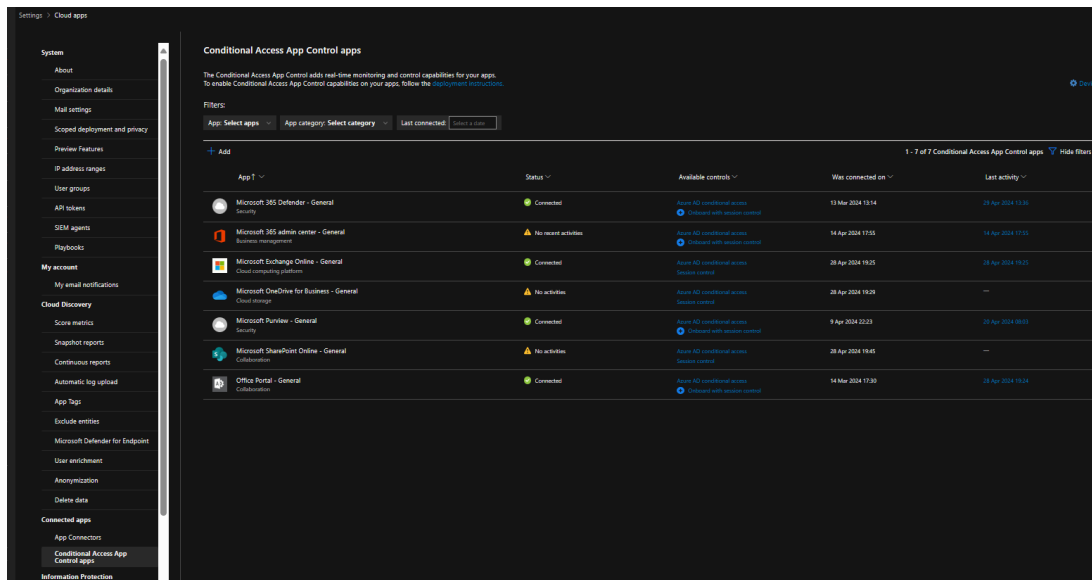
Use access policies to:

- Block access to Salesforce for users coming from unmanaged devices
- Block access to Dropbox for native clients.

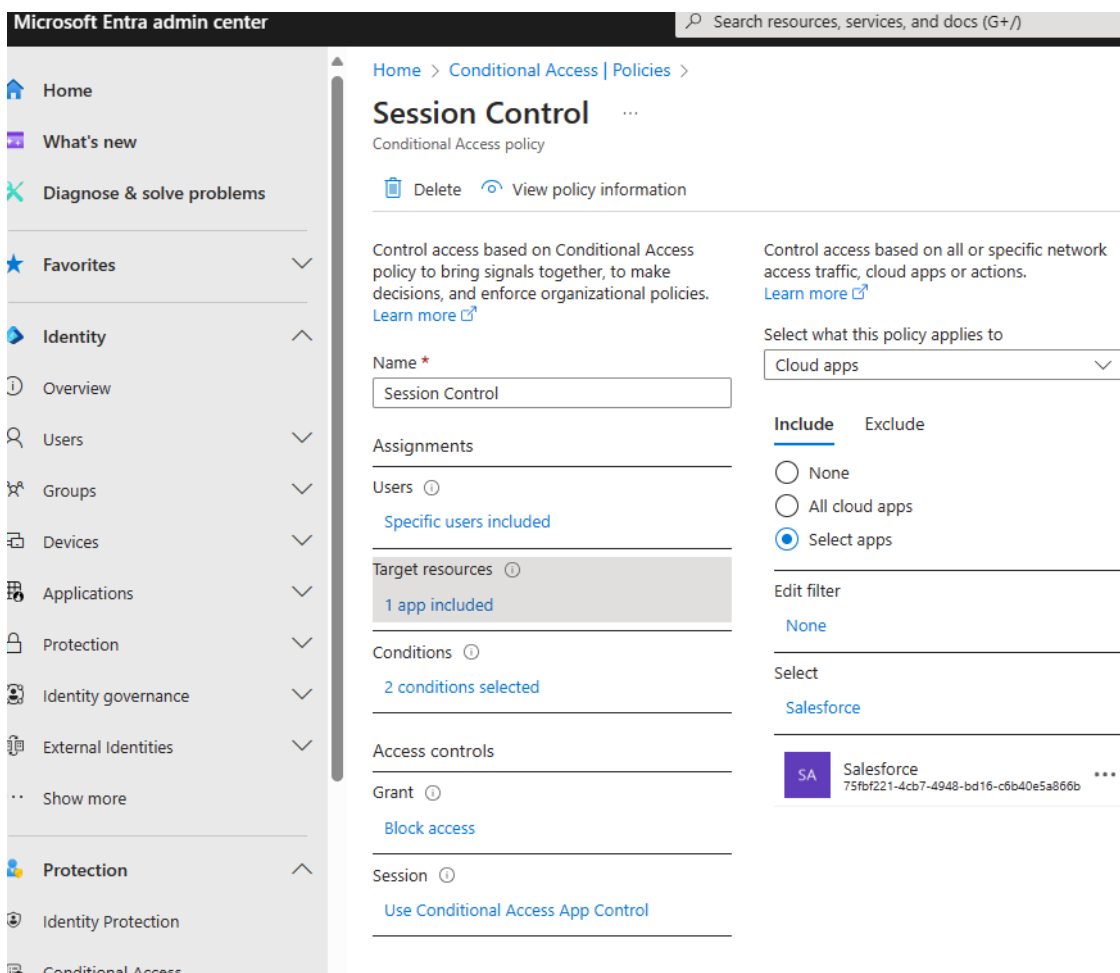
Use session policies to:

- Block downloads of sensitive files from OneDrive to unmanaged devices
- Block uploads of malware files to SharePoint Online

Any web apps can work with access and session control. Two steps you need to do 1. Pre-onboard the app in the Settings under Defender for Cloud Apps in Defender XDR. 2. Create a Conditional Access session in Entra.

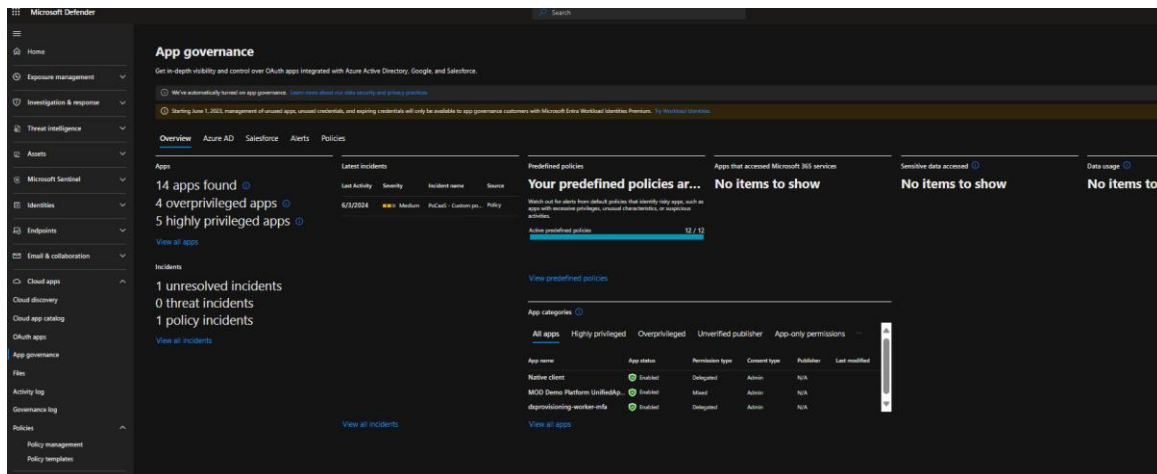


Creating the CA Policy in Entra is very much like all the other Conditional Access.



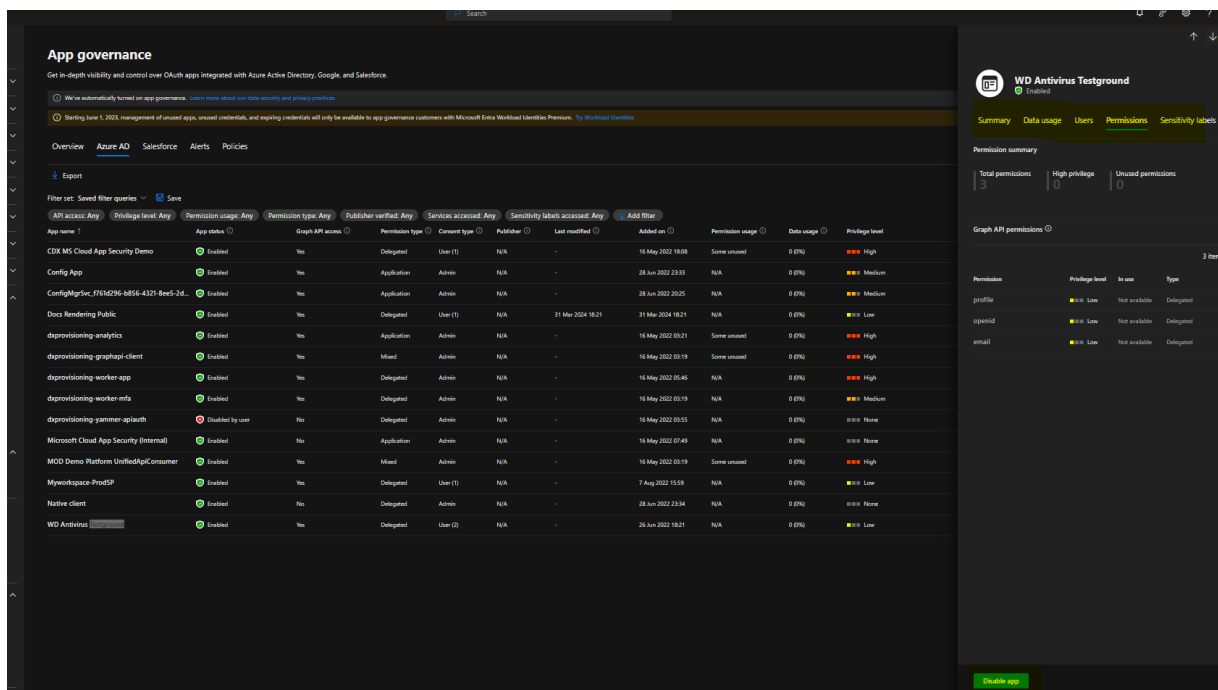
Another key feature of Defender for Cloud Apps is **App Governance**. Designed specifically for oauth-enabled apps registered in Entra, Google and Salesforce. App governance delivers visibility, remediation, and governance into how these apps and their user's access, use, and

share sensitive data in Microsoft 365 and other cloud platforms through actionable insights and automated policy alerts and actions.

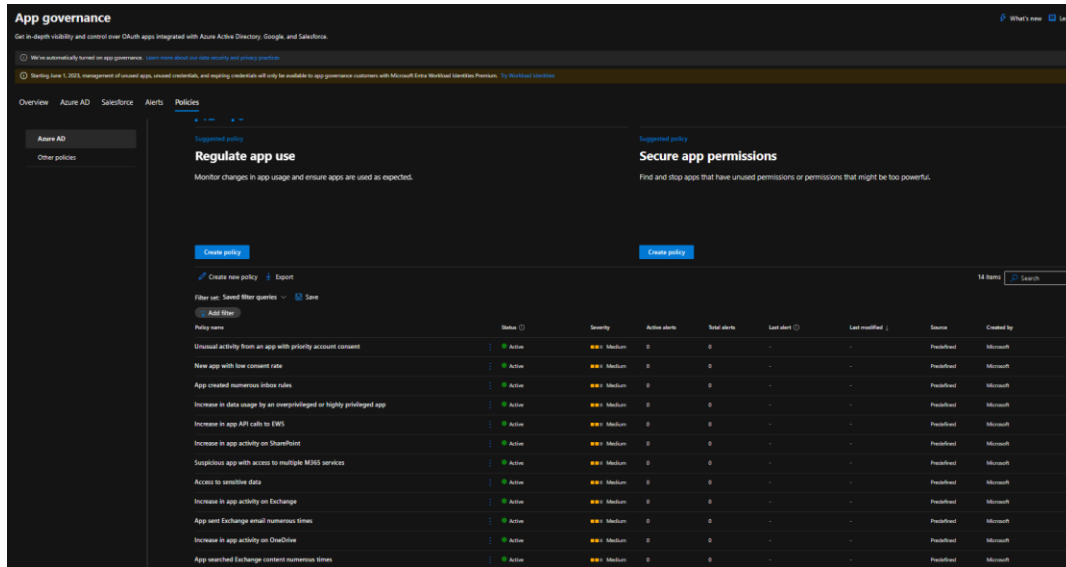


By opening an app, you can dig deeper if an app is compliant or you have random permissions in this app. One for the SOC is known to have attackers apply malware onto apps and unidentified accounts can be seen with full rights to the application. If this is a business-critical app, is something to investigate.

You can also create custom policies you feel will help govern your applications further

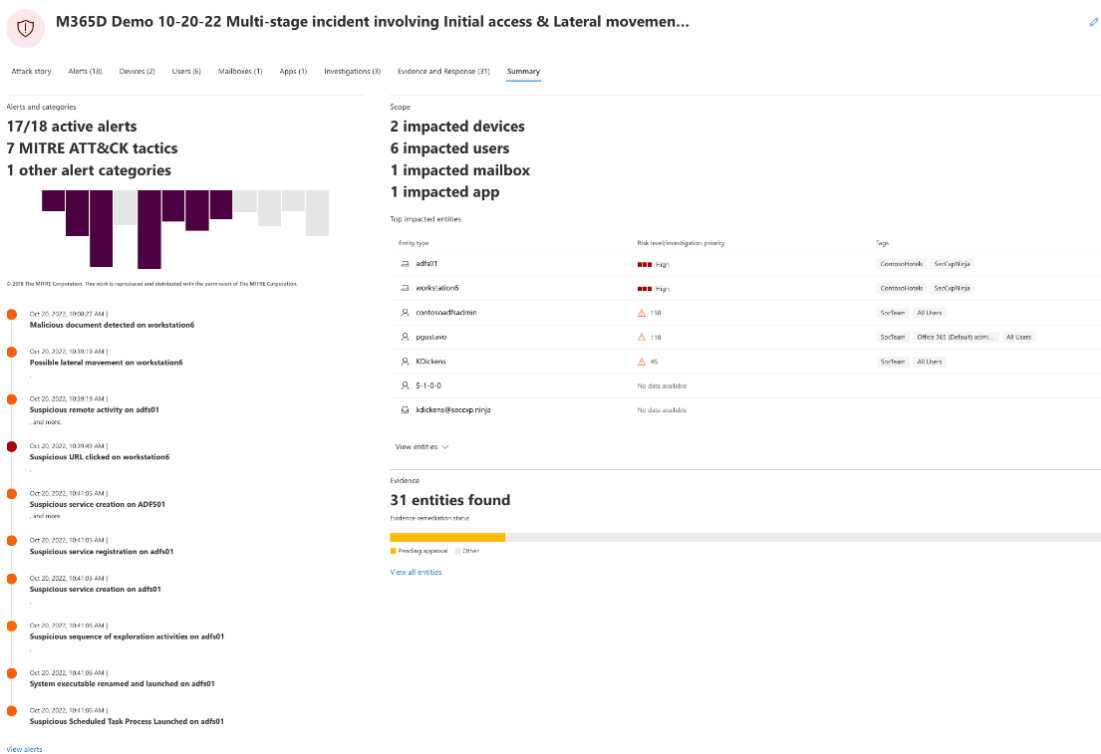


We have some crossover policies and policy templates turned on by default



[Investigate incidents in Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn](#)

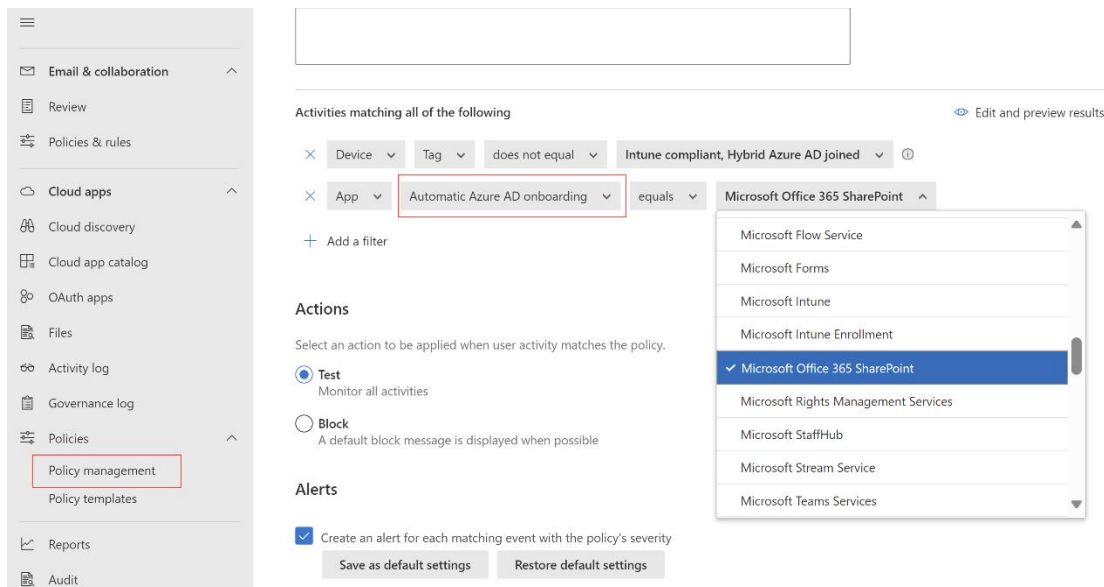
When you get an alert that is then correlated into an incident, an alert that was generated from multiple instances from email, endpoint, to identity, you can see the whole attack story. You can trace it back from the source and potentially run some of our native responses, isolate a device, disable a user. You'll be able to see all the alerts relating to the incident, the assets impacted, investigations and evidence and resources related to the incident.



For all Defender products, do not forget to check in our monthly 'What's new' this is an important piece as part of your monthly checks. It could be a feature you been waiting for or a new feature that can potentially solve a bottle neck.

An example for June 2024 updates. We have added MacOS as part of our in-browser protection which have garnered feedback from the community.

Another example is our **'Microsoft Entra ID apps are automatically onboarded for Conditional Access app control (Preview)'**



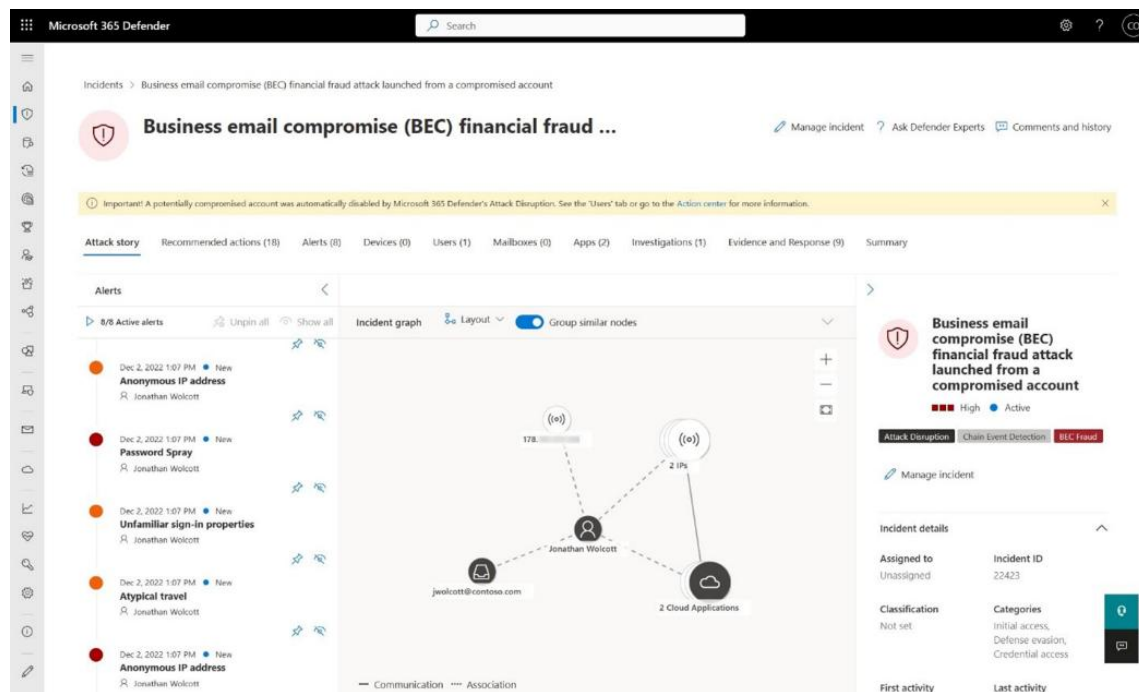
Automatic Attack Disruption (AAD)

Automatic attack disruption is designed to contain attacks in progress, limit the impact on an organization's assets, and provide more time for security teams to remediate the attack fully.

You can see when AAD enabled by the yellow bar across the incident or see all the work in action centre if AAD is being triggered

Automatic attack disruption operates in three key stages:

- It uses Defender XDR's ability to correlate signals from many different sources into a single, high-confidence incident through insights from endpoints, identities, email and collaboration tools, and SaaS apps.
- It identifies assets controlled by the attacker and used to spread the attack.
- It automatically takes response actions across relevant Microsoft Defender products to contain the attack in real-time by isolating affected assets.



Deployment requirements for AAD

Deployment across Defender products (e.g., Defender for Endpoint, Defender for Office 365, Defender for Identity, and Defender for Cloud Apps)

The wider the deployment, the greater the protection coverage is. For example, if a Microsoft Defender for Cloud Apps signal is used in a certain detection, then this product is required to detect the relevant specific attack scenario.

Similarly, the relevant product should be deployed to execute an automated response action. For example, Microsoft Defender for Endpoint is required to automatically contain a device.

Microsoft Defender for Endpoint's device discovery is set to 'standard discovery'

Operationalizing our Core Defender products

Ever heard the saying, “the car is only as good as the driver”. In the case of Microsoft Defender XDR, that is pretty accurate. Our Security tools are some of the best out there, if not the best, we put a lot of thought in easing the life of SOC by trying to automate a lot of detections and alerts and building our posture assessments with our products and 3rd party but once all of those are in place, you must rely on some very technical and experience SOC Team.

We have put some guides on Daily, Weekly and Monthly activities that the operation team should consider. I've put them on one slide to make it easier to see for each core product.



SOC Operational Guide in Defender XDR

Not Official Document-
Developed by Ray Reyes
Updated 1st June 2024

	Daily Activities	Weekly	Monthly
Microsoft Defender for Endpoint	Monitor Defender XDR Incidents queue Manage false positive in incidents queue Review health reports, review AV health	Review Message Center Review TVM Review ASR Reports	Review Exclusions Review MDE Secure Score
Microsoft Defender for Identity	Review Incidents dashboard, filter to new, in-progress Use Hunt to triage Classify to true, false, expected activity incidents Investigate users with High Investigation score	Use Secure Score recommendation Hunt for emerging threats Create custom detection	Review, tune alerts Track new changes in MDI and Defender XDR
Microsoft Defender for Office 365	Manage false positive in incidents queue, use submission page, tenant allow/block, Triage, resolve, classify investigate incidents Release false positive from quarantine Review campaign mail	Review Mail flow status report Review Threat Protection status report Review Top targeted users for malware & phishing Pro-actively hunt for threats use A Hunting	Review Configuration MDO Policies Review Detection Overrides Review Spoof intelligence insights & Impersonation detection Review priority accounts
Microsoft Defender for Cloud Apps	Review Incidents dashboard, filter to new, in-progress Review Cloud Discovery Page Review Anomaly Alerts	Review SAAS Security Posture Management Review App Connectors, Log Connectors Review What's new in XDR Proactively Hunt for Threats	Review Policy Assessments Review Policies across, Conditional Access, Shadow IT, Information Protection Review App Risk scores

Reference

MDE - <https://learn.microsoft.com/en-us/defender-endpoint/mde-sec-ops-guide>

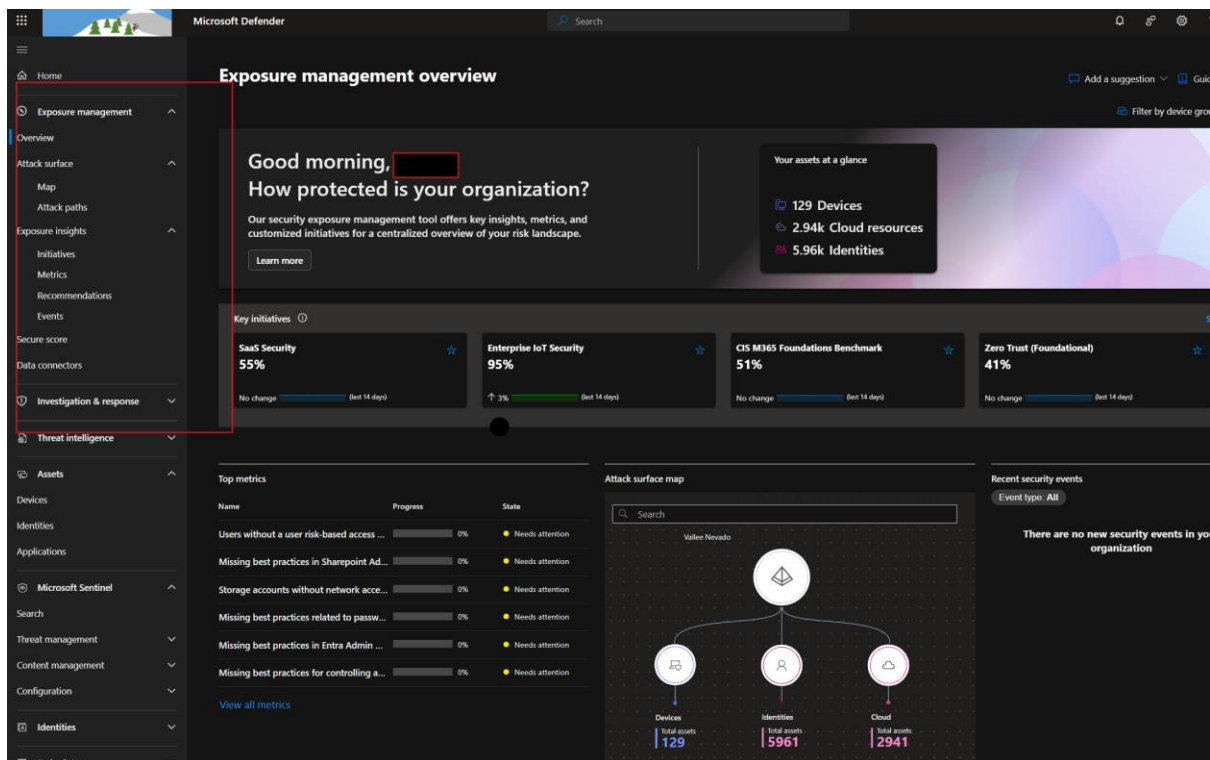
MDO - <https://learn.microsoft.com/en-us/defender-office-365/mdo-sec-ops-guide>

MDI - <https://learn.microsoft.com/en-us/defender-for-identity/ops-guide/ops-guide-daily>

MDA - <https://learn.microsoft.com/en-us/defender-cloud-apps/ops-guide/ops-guide-daily>

Continuing Operationalising Defender XDR - Microsoft Security Exposure Management

provides a unified view of security posture across company assets and workloads. Security Exposure Management enriches asset information with security context that helps you to proactively manage attack surfaces, protect critical assets, and explore and mitigate exposure risk.



With *Security Exposure Management* you can:

- Get a unified view across the organization: Security Exposure Management continuously discovers assets and workloads and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.
- Manage and investigate attack surfaces: Visualize, analyse, and manage cross-workload attack surfaces.
- The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business.
- Graph schemas provide contextual information about specific organizational entities such as devices, identities, machines, and storage.
- Query the enterprise exposure graph to explore assets, assess risk, and hunt for threats across on-premises, hybrid, and multi-cloud environments.
- Visualize your environment and graph queries with the attack surface map.
- Discover and safeguard critical assets: Security Exposure Management marks predefined assets and assets you customize, as critical. This enables you to focus and prioritize on those critical assets to ensure security and business continuity.
- Manage exposure: Security Exposure Management provides tools to manage security exposure and mitigate exposure risk.
- Exposure insights aggregate security posture data and provide rich context around the security posture state of your asset inventory.

You leverage these insights to prioritize security efforts and investments.

Insights include security events, recommendations, metrics, and security initiatives.

As you manage exposure risk, attack paths show you how an attacker might breach your attack surface.

Security Exposure Management generates attack paths based on data collected across assets and workloads. It simulates attack scenarios and identifies weaknesses that an attacker could exploit.

You can use the enterprise exposure graph and attack surface map to visualize and understand potential threats.

You can also focus on choke points through which many attack paths flow.

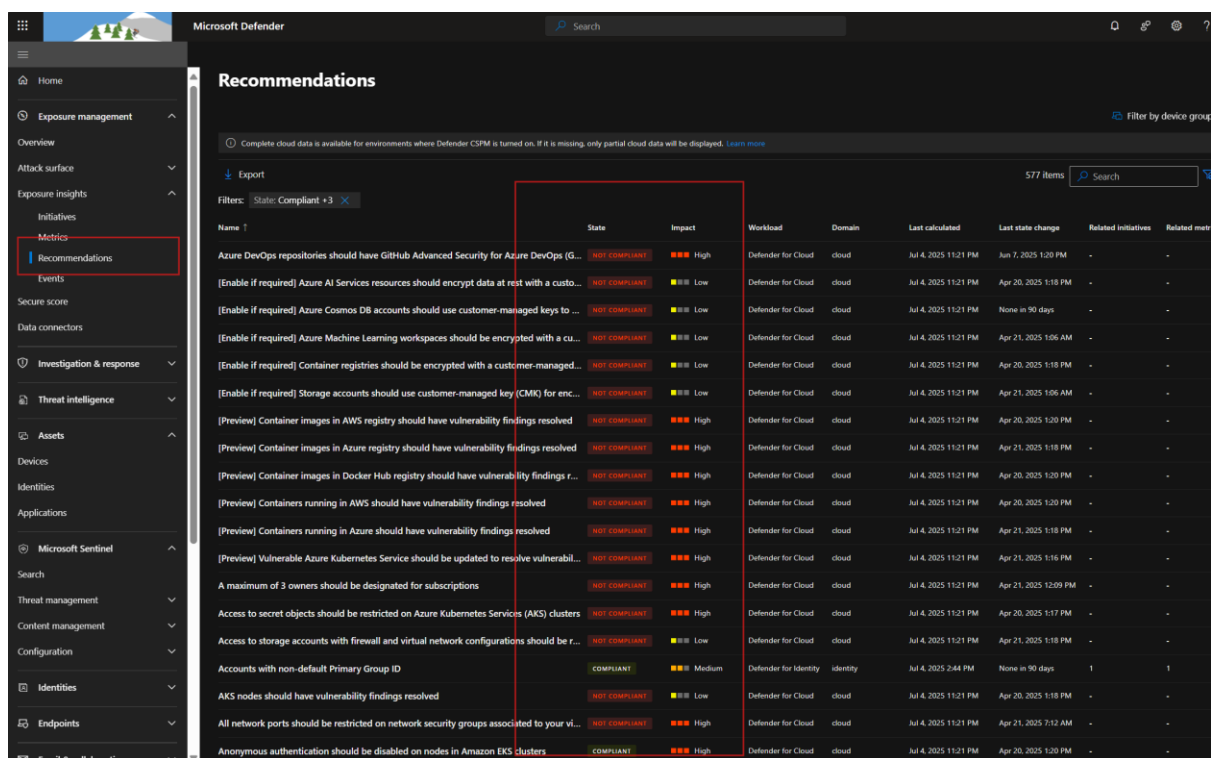
Actionable recommendations help you to mitigate identified attack paths.

Connect your data: Security Exposure Management supports a variety of data connectors to integrate with different security solutions and data sources.

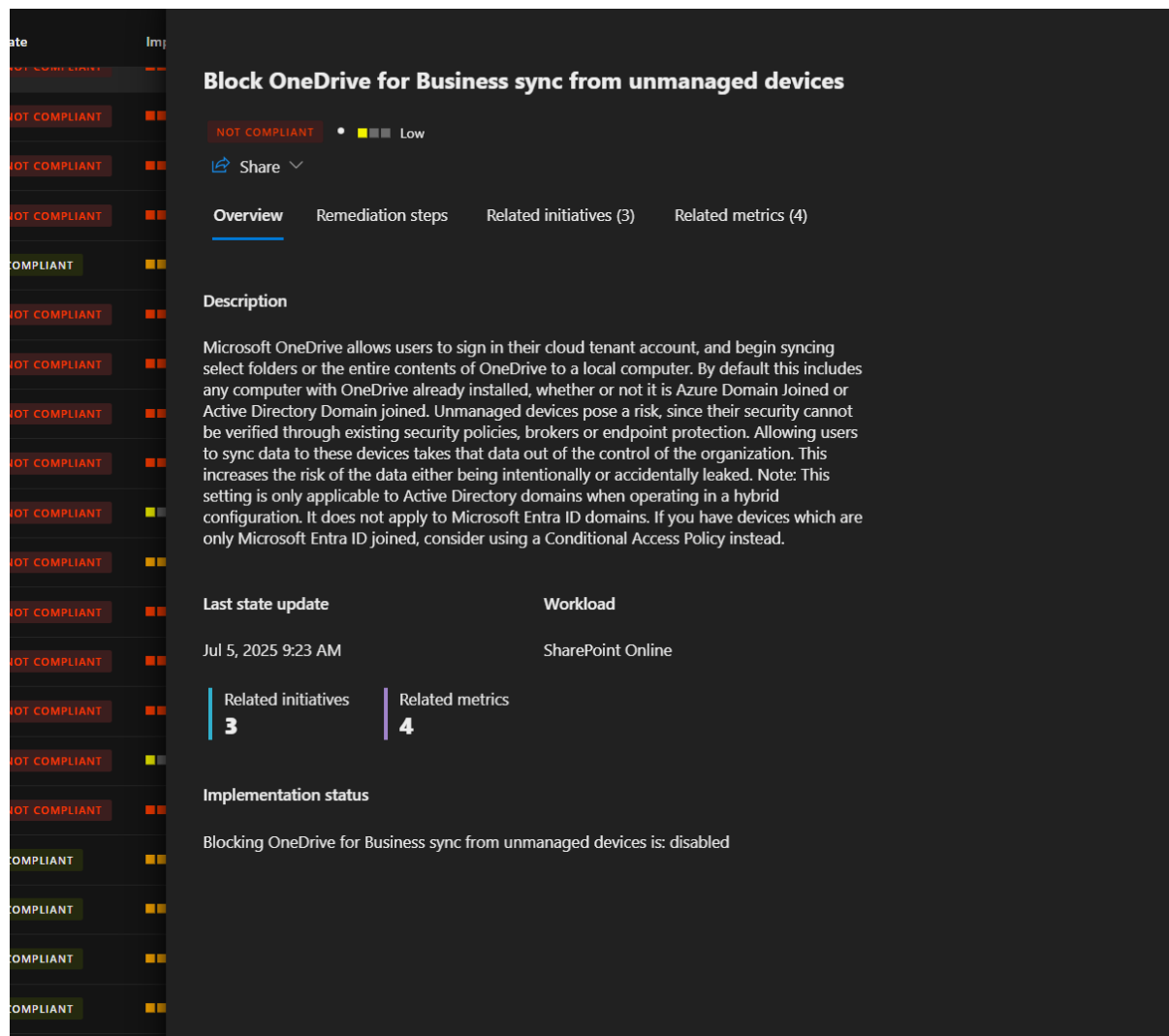
Consolidate security data from multiple sources into a single, unified view.

Gain deeper insights into your security posture by integrating data from various environments.

Simplify the management of security data across different platforms and solutions.



Name	State	Impact	Workload	Domain	Last calculated	Last state change	Related initiatives	Related more
Azure DevOps repositories should have GitHub Advanced Security for Azure DevOps (G...	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Jun 7, 2025 1:00 PM	-	-
[Enable if required] Azure AI Services resources should encrypt data at rest with a custo...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:18 PM	-	-
[Enable if required] Azure Cosmos DB accounts should use customer-managed keys to ...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	None in 90 days	-	-
[Enable if required] Azure Machine Learning workspaces should be encrypted with a cu...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:06 AM	-	-
[Enable if required] Container registries should be encrypted with a customer-managed...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:18 PM	-	-
[Enable if required] Storage accounts should use customer-managed key (CMK) for enc...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:06 AM	-	-
[Preview] Container images in AWS registry should have vulnerability findings resolved	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:30 PM	-	-
[Preview] Container images in Azure registry should have vulnerability findings resolved	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:18 PM	-	-
[Preview] Container images in Docker Hub registry should have vulnerability findings r...	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:20 PM	-	-
[Preview] Containers running in AWS should have vulnerability findings resolved	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:20 PM	-	-
[Preview] Containers running in Azure should have vulnerability findings resolved	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:18 PM	-	-
[Preview] Vulnerable Azure Kubernetes Service should be updated to resolve vulnerabil...	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:16 PM	-	-
A maximum of 3 owners should be designated for subscriptions	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 12:09 PM	-	-
Access to secret objects should be restricted on Azure Kubernetes Services (AKS) clusters	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:17 PM	-	-
Access to storage accounts with firewall and virtual network configurations should be r...	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 1:18 PM	-	-
Accounts with non-default Primary Group ID	COMPLIANT	Medium	Defender for Identity	identity	Jul 4, 2025 2:44 PM	None in 90 days	1	1
AKS nodes should have vulnerability findings resolved	NOT COMPLIANT	Low	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:18 PM	-	-
All network ports should be restricted on network security groups associated to your vi...	NOT COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 21, 2025 7:12 AM	-	-
Anonymous authentication should be disabled on nodes in Amazon EKS clusters	COMPLIANT	High	Defender for Cloud	cloud	Jul 4, 2025 11:21 PM	Apr 20, 2025 1:20 PM	-	-



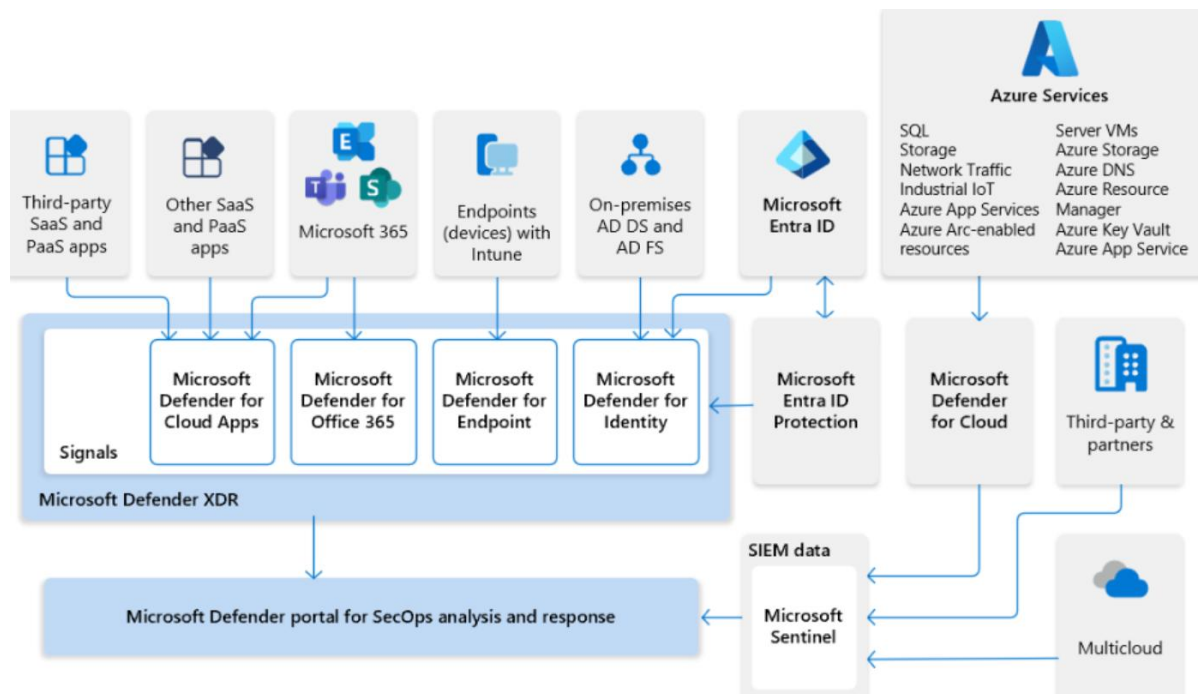
Microsoft Sentinel

What's new since August, 2024

- Microsoft Sentinel in the Azure portal to be retired July 2026
 - Planning your move-> [Migration Plan](#)
- All Microsoft Sentinel use cases generally available in the Defender portal
- Security Copilot generates incident summaries in Microsoft Sentinel in the Azure portal (Preview)

Microsoft Sentinel is Microsoft's Security Information and Events Management (**SIEM**) and a Security Orchestration, Automation and Responsibility (**SOAR**).

What makes Microsoft's SIEM stand out from the rest of other SIEM is our **Defender XDR + SIEM story** which we have designed a single pane (Unified Security Operations) to give a consistent schema for data. And when you think about this in another analogy, **you have the brain that collects all the data and the brute force of the arms and legs of our Microsoft Defender XDR ready to flex on detections.**



Benefits of unified solution

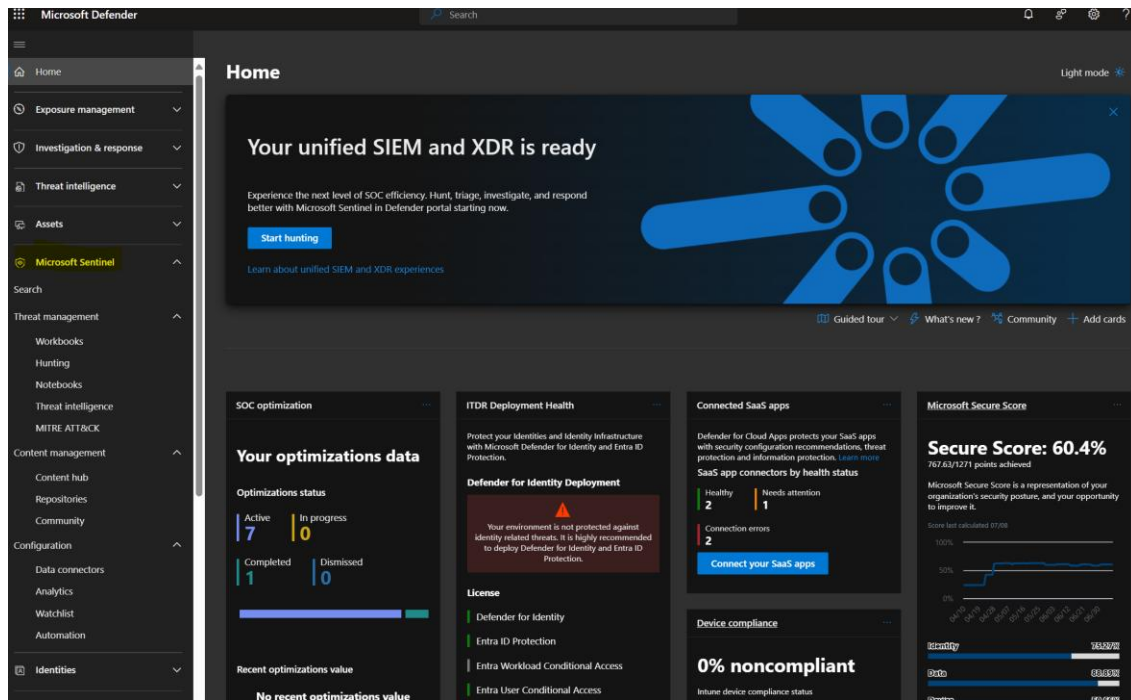
- Cyberattack timelines are automatically fully correlated in a single incident, allowing analysts to move faster to respond to breaches, with a more comprehensive view of an attack
- **Detect and investigate faster with more accuracy.** Bringing the depth of XDR signal from Defender and the flexibility of log sources from Microsoft Sentinel delivers an improved signal-to-noise ratio and enhanced alert correlation
- **Improved threat hunting experience.** With a single experience for data querying, analysts don't have to remember where data is available or jump across portals.
- The unification of SIEM and XDR has delivered to our customers, on average, 50% faster correlation among XDR, log data, custom detections, and threat intelligence—with 99% accuracy.

When you onboard Sentinel to the Microsoft Defender portal, you gain capabilities such as incident management and advanced hunting. Specifically, here's how it works:

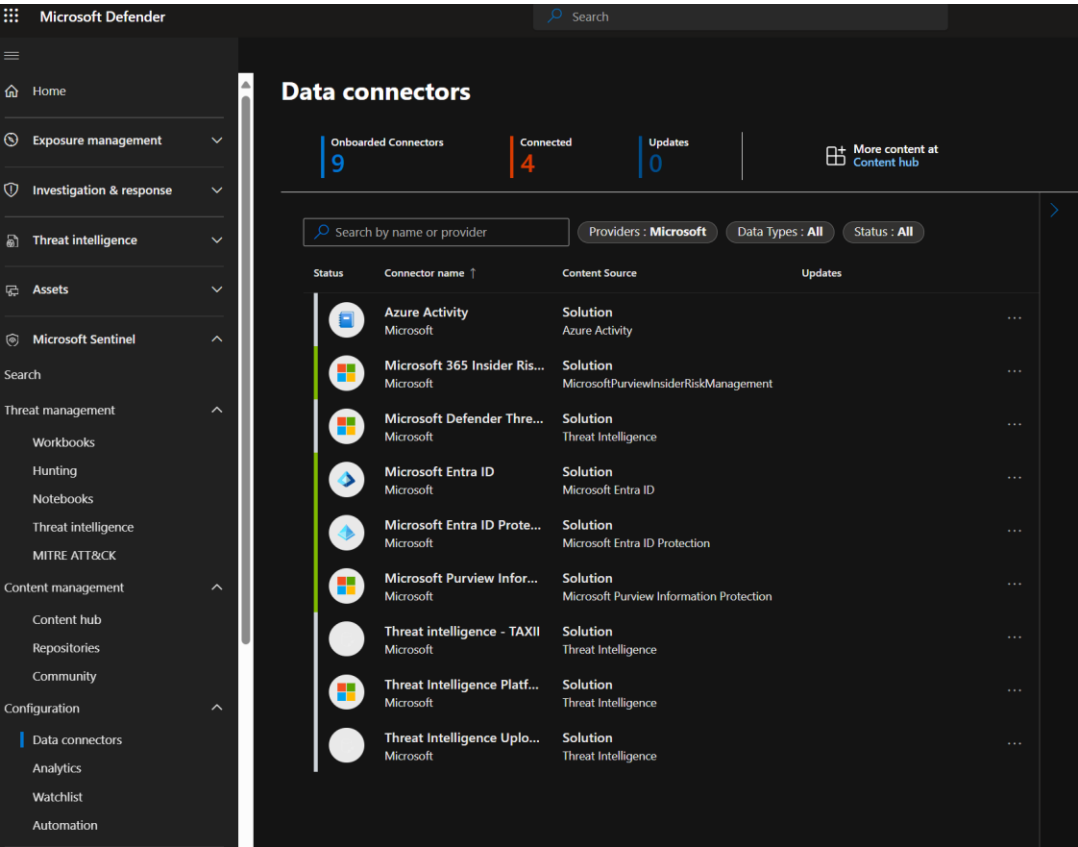
1. **Incident Correlation and Alerts:**
2. Defender XDR incidents (including alerts, entities, and relevant information from Microsoft Defender for Endpoint, Identity, Office 365, and Cloud Apps) are streamed to Sentinel as security information and event management (SIEM) data.
3. You can manage Defender XDR incidents within Sentinel, alongside incidents from other cloud and on-premises systems.
4. Correlate incidents across your organization and take advantage of Defender XDR's unique capabilities for in-depth investigations.

Microsoft Sentinel customers can adopt the new experience easily while continuing to use the classic experience in Microsoft Azure if needed. It's never been easier to add SIEM capabilities

like connectors to hundreds of data sources, and extended retention or additional compliance capabilities to your existing Microsoft Defender XDR environment.



Sentinel is empowered and enriched by the components that send data to your workspace and is made stronger through integrations with other Microsoft services. Any logs ingested into products, such as MDA, MDE, MDI allow these services to create detections, and in turn provide those detections to Microsoft Sentinel. We have several new connectors for our Data Security workloads too to enable that holistic view across our data security and cyber



Step	Article
Plan your migration	You are here
Track migration with a workbook	Track your Microsoft Sentinel migration with a workbook
Use the SIEM Migration experience	SIEM Migration (Preview)
Migrate from ArcSight	• Migrate detection rules • Migrate SOAR automation • Export historical data
Migrate from Splunk	• Start with the SIEM Migration experience • Migrate detection rules • Migrate SOAR automation • Export historical data If you want to migrate your Splunk Observability deployment, learn more about how to migrate from Splunk to Azure Monitor Logs.
Migrate from QRadar	• Migrate detection rules • Migrate SOAR automation • Export historical data
Ingest historical data	• Select a target Azure platform to host the exported historical data • Select a data ingestion tool • Ingest historical data into your target platform
Convert dashboards to workbooks	Convert dashboards to Azure Workbooks
Update SOC processes	Update SOC processes

[Connect Microsoft Sentinel to Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn](#)

Let's go through the high-level steps on deploying Sentinel

1. First order of priority. Go through the [plan guide](#).

- a. This includes planning the required data connectors which will help you forecast cost. This will go along with the Plan cost overall. Ensuring you know the price planning that comes with automation and also bringing your own logs
- b. Workspace design, tenancy consideration
- c. Roles and permissions

2. Plan interactive and long-term data retention and Planning Cost

This section is one of the most important parts of planning your SIEM program. A key challenge for customers is determining what data to prioritize and at the same time trying to ensure cost is kept to a minimum. In most cases, customers feel that all data is important which makes it challenging.

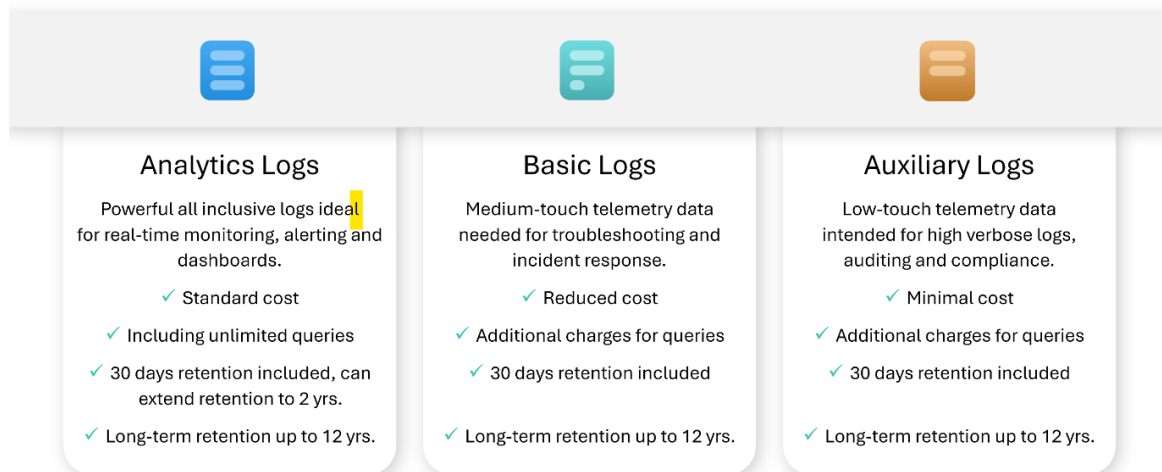
At Microsoft, we recommended to break down the ingested data into two sections

- **Primary security data** is data that contains critical security value. This data is used for real-time proactive monitoring, scheduled alerts, and analytics to detect security threats. The data needs to be readily available to all Microsoft Sentinel experiences in near real time.
- **Secondary security data** is supplemental data, often in high-volume, verbose logs. This data is of limited security value, but it can provide added richness and context to detections and investigations, helping to draw the full picture of a security incident. It doesn't need to be readily available but should be accessible on-demand as needed and in appropriate doses.

Log Storage Plans

Currently, we offer a multi-tier storage plan. Analytics Logs and Basic Logs (sunsetting) – Auxiliary Logs (Preview) will be replacing Basic logs

Azure Monitor Multi-tier: One stop shop for all logs



Analytic Logs

- Keeps data in the interactive retention state for 90 days by default
- extensible for up to two years.
- When the interactive retention period ends, data goes into the long-term retention stat

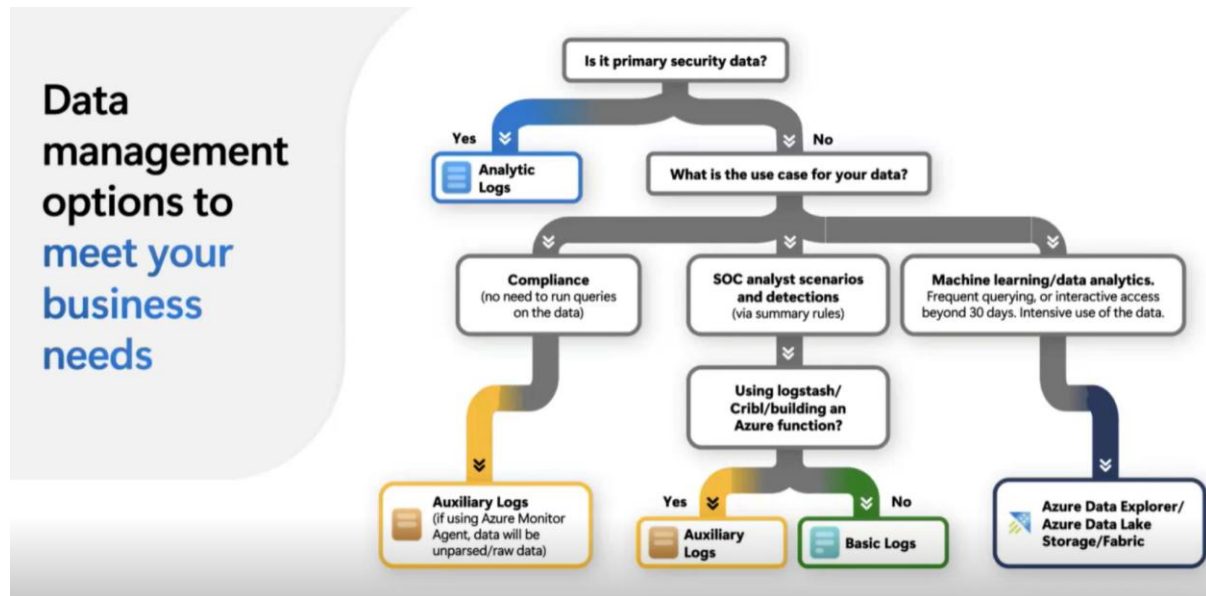
Auxiliary logs

- keeps data in the interactive retention state for 30 days
- this state has very low retention costs as compared to the Analytics plan
- While this data remains in the interactive retention state, you can run [summary rules](#) on this data to create tables of aggregate

Basic Logs

- similar functionality to the auxiliary logs plan, but at a higher interactive retention cost (though not as high as the analytics logs plan)
- basic logs can be an option for long-term, low-cost retention if your organization doesn't use preview features.

This is a simple decision tree when



[Plan costs and understand pricing and billing - Microsoft Sentinel | Microsoft Learn](#)

Onboard Sentinel

- a. Go to Azure Portal, find Microsoft Sentinel. Create and add a new workspace. Bear in mind that the workspace you choose means that the data is isolated to that workspace
3. **Configure Content** – This is the fun part of setting up Sentinel, from choosing your data connectors, to automation to playbooks. These are the features that really help separate Sentinel from other SIEMs
4. Determine and setup your Data Connectors
 There is various approach to Data connectors, and you can probably categorise them into 3.
[Free Data Connectors](#) – this is where you will mostly find our Microsoft Defender stack and Data Security connectors
[Custom Data Connectors](#) – Lots of cool things in here such as connecting to Logstash, logic apps
 and [Partner Connectors](#) – tonne of partner connectors to see here.

The screenshot shows the Microsoft Defender Content Hub interface. The left sidebar contains navigation options: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management (selected), Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, and More resources. The main area displays 'Data connectors > Content hub' with a search bar and filters for Status, Content type, Support, Provider, Category, and Content sources. A table lists various content items with columns for Content title, Status, Content source, Provider, Support, Category, and Content type. Items include Amazon Web Services, Azure Activity, Cisco Umbrella, DNS Essentials, Google Cloud Platform IAM, LogRhythm Vulnerability Detection, Microsoft Defender for Cloud, Microsoft Defender XDR (highlighted with a yellow box), Microsoft Entra ID, Network Session Essentials, SAP applications, Security Threat Essentials, Sentinel SOAR Essentials, and SOC Handbook.

5. Setup Analytics Rules - [Threat detection in Microsoft Sentinel | Microsoft Learn](#)

Once you've setup your connectors, you're going to need to know what you're looking for, detect and report rules you put in place.

You can do this in two ways. Using the [built-in analytics rule wizard](#) or [analytics rule templates](#)

In Defender Portal – Sentinel – Configuration – Analytics. You can create one from templates or from scratch

The screenshot shows the Microsoft Defender Analytics page. The left sidebar is the same as the previous screenshot. The main area is titled 'Analytics' and shows 'Active rules 47'. A 'Rule templates' button is highlighted with a yellow box. Below it, a '+ Create' button is also highlighted with a yellow box. The page displays a list of active rules with columns for Rule type, Status, Tactics, Techniques, Source name, and Last modified. Rules include 'Office policy tampering', 'Failed login attempts to Azure', 'Linked Malicious Storage Artifacts', 'High count of connections by client IP', 'TestAV AR', 'Palo Alto - possible internal', 'TI map Email entity to Email', 'New External User Granted Admin Role', and '[DO NOT TOUCH] Squid URL TI match'.

message to that effect.



6. Setup Automation Rules

Automation rules help streamline the use of automation in Microsoft Sentinel, enabling you to simplify complex workflows for your threat response orchestration processes.

There are 3 key components in Automation Rules. Triggers, Condition and Action. A common triage and respond flow.

These 3 key components can be used for various categories to perform task handling of incidents or alerts. In some ways, help your SOC team to automate a lot of the manual action they need to perform

Here is an example where a SOC can work with rules [Work with incident tasks in Microsoft Sentinel | Microsoft Learn](#)

Home > Microsoft Sentinel | Incidents >

Incident ...
Incident ID: 602768

Refresh Delete incident **Tasks**

Brute force attack
Incident ID: 602768

Unassigned Owner New Status High Severity

Description
A suspicious activity was detected in the organization. IPs are attacked.

Alert product names
• Microsoft Sentinel

Tasks
1/6 completed. View full details

Evidence
1 Events 1 Alerts 0 Bookmarks

Last update time: 11/27/22, 05:36 PM
Creation time: 11/27/22, 05:36 PM

Entities (3)
• hcook@contoso.co...
• 5.199.130.188
• 9498FF82A64FF445...
View full details >

Incident workbook
Incident Overview

Analytic rule
Investigate Actions

Incident tasks

Refresh Add task

Search Status: All

- ☒ Reset user password
Created by: Playbook - Addtaskstoincident
- ☐ Validate and scope the alert
Created by: Automation rule - Brute force attack workflow
- ☐ Run query to explore last activities
Created by: Automation rule - Brute force attack workflow
- ☐ Stop suspicious process and isolate affected machines
Created by: Automation rule - Brute force attack workflow
- ☐ Block IP addresses and URLs
Created by: Automation rule - Brute force attack workflow
- ☐ Open a task in ServiceNow for the IT department
Created by: Automation rule - Brute force attack workflow

In Defender Portal. Sentinel – Configuration

Automation

Automation rules: 4 Enabled rules: 4 Enabled playbooks: 14 More content at Content Hub

Automation rules Active playbooks Playbook templates (Preview)

+ Create

Automation rule

Playbook with incident trigger

Playbook with alert trigger

Playbook with entity trigger

Blank playbook

Trigger	Logic Apps Connectors	Entities	Tags	Last modified	Source name
Microsoft Sentinel Incident	Microsoft Sentinel	Host	Remediation	7/25/2022, 3:00...	CrowdStrike Falc...
Microsoft Sentinel Incident	Microsoft Sentinel			3/9/2023, 2:00...	Microsoft Defen...
Microsoft Sentinel Entity (Preview)	Microsoft Sentinel	DNS	Remediation	2/26/2023, 2:00...	MicrosoftDefend...
Microsoft Sentinel Incident	ServiceNow +1			8/5/2022, 3:00...	IoTOTThreatMon...
Microsoft Sentinel Incident	Microsoft Sentinel			3/9/2023, 2:00...	Microsoft Defen...

< Previous Page 1 of 2 Next > Showing 1 to 50 of 75 results.

7. Setup Playbook

Playbooks in Sentinel is one of our bread-and-butter features and a SOC's best friend. With the sheer volume of alerts and incidents, sometimes it can be overwhelming for any SOC to go through each alert. Playbook can help SOC's to run a set of collection of remediation actions that you run from Microsoft Sentinel as a routine, to help automate and orchestrate your threat response.

We have built-in template Playbooks we highly recommend and you have the ability to create custom playbooks

Automation

Automation rules: 0, Enabled rules: 0, Enabled playbooks: 1

More content at Content Hub

Automation rule

Playbook with incident trigger

Playbook with alert trigger

Playbook with entity trigger

Blank playbook

Trigger	Logic Apps Conn...	Entities	Tags	Last modified	Source name
Microsoft Sentinel Incident	Microsoft Sentinel +		Notification, Incid	05/08/2022, 100...	SentinelSOARess...
Microsoft Sentinel Incident	Microsoft Sentinel +		Notification, Incid	05/08/2022, 100...	SentinelSOARess...
Microsoft Sentinel Entity (Pre	Microsoft Sentinel	DNS	Remediation	26/02/2023, 100...	MicrosoftDefend...
Microsoft Sentinel Alert	Microsoft Sentinel	FileHash	Remediation	14/07/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Entity (Pre	Microsoft Sentinel +	Host		22/12/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Incident	Azure Monitor Logs	IP	grouping	20/03/2022, 100...	SentinelSOARess...
Microsoft Sentinel Incident	Microsoft Teams + T			04/08/2022, 100...	SentinelSOARess...
Microsoft Sentinel Incident	Microsoft Defender +	Host	Remediation	14/07/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Alert	Microsoft Defender +	Host	Remediation	14/07/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Alert	Microsoft Defender +	Host	Remediation	14/02/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Incident	Microsoft Entra ID +	Account	Remediation	25/07/2022, 100...	Microsoft Entra L...
Microsoft Sentinel Incident	Microsoft Sentinel		Tasks	16/02/2023, 100...	SentinelSOARess...
Microsoft Sentinel Alert	Microsoft Teams + T		Notification	04/08/2022, 100...	SentinelSOARess...
Microsoft Sentinel Alert	Microsoft Entra ID +	Account	Remediation	25/07/2022, 100...	Microsoft Entra L...
Microsoft Sentinel Entity (Pre	Microsoft Sentinel +		Host	22/12/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Alert	Microsoft Sentinel	DNS	Remediation	14/07/2022, 100...	MicrosoftDefend...
Microsoft Sentinel Incident	Office 365 Outlook +		Notification	14/07/2021, 100...	SentinelSOARess...
Microsoft Sentinel Alert	Microsoft Sentinel	IP	Remediation	14/07/2022, 100...	MicrosoftDefend...

Automation > Playbook editor

Basics

Subscription: Visual Studio Enterprise Subscription

Resource group: Sentinel

Region: australiaeast

Playbook name: Play

Diagnostics logs workspace: Sentinel1

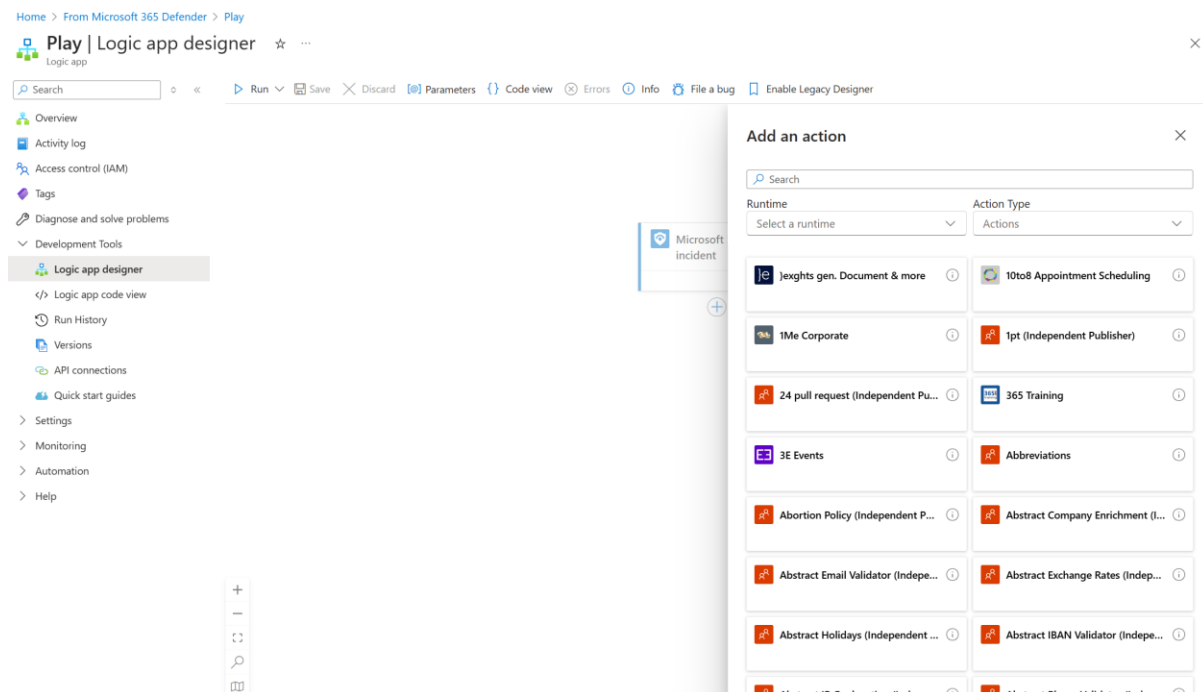
Connections

Microsoft Sentinel

Connect with managed identity

Note: Grant permissions to the managed identity after deployment.

Once you've created the resource, you can go to the playbook



8. Setup Workbooks

When you think of Workbooks, think of visual reports within Microsoft Sentinel. To give you a better insight to the reports from the logs you receive based on data connectors you've turned on. There isn't much to this. Just like some of the steps above, you can create your own or use the templates we have.

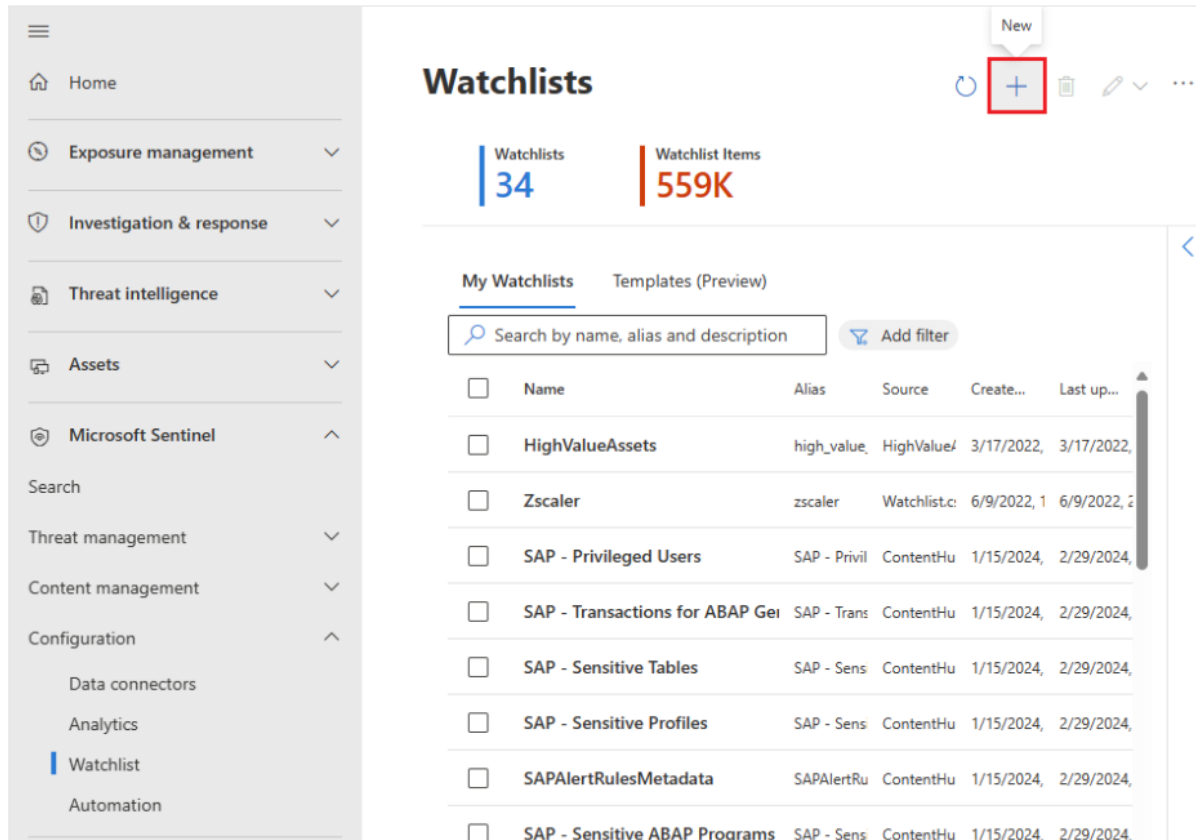
These are the commonly use workbooks

[Commonly used Microsoft Sentinel workbooks | Microsoft Learn](#)

9. Setup Watchlist

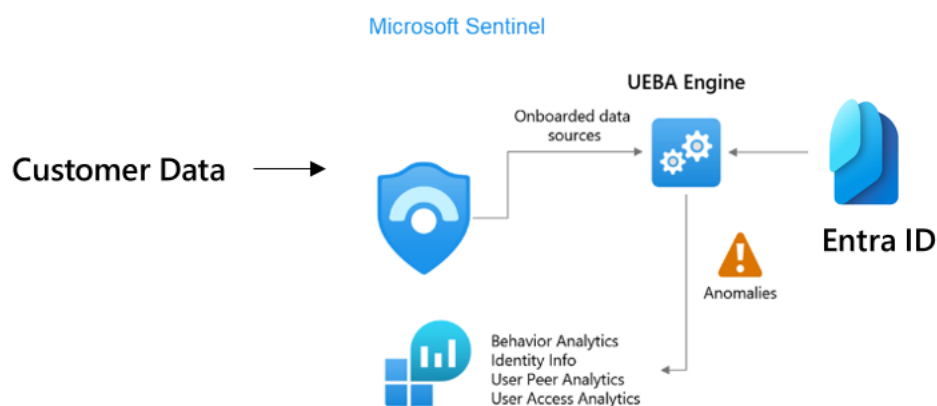
[Watchlists in Microsoft Sentinel - Microsoft Sentinel | Microsoft Learn](#)

Think of watchlist as something like you can leverage for VIP users or assets. Watchlist is a feature that allows you to correlate the data source and the events in Sentinel. You can upload a file with the list and be able to dive deeper into the assets and monitor using correlated data and events.



10. Enable User and Entity Behavioural Analytics (UEBA)

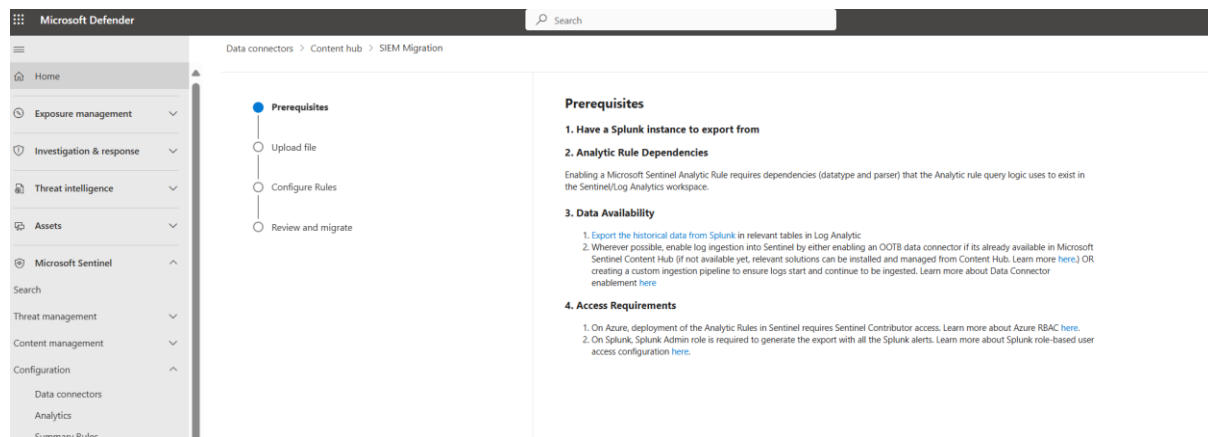
From a Sentinel perspective, UEBA has the same purpose where it builds baseline behavioural profiles of your organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon from all the logs you collect from the data sources. Using a variety of techniques and machine learning capabilities, Microsoft Sentinel can then identify anomalous activity and help you determine if an asset has been compromised



Migration from 3rd party SIEM to Sentinel

If you're migrating from another 3rd party SIEM. We have you covered. On the link below, we have a migration detail for some common SIEM such as arcsight, Splunk. It's important to go through the migration details for your current 3rd party to ensure migration goes smoothly

[Plan your migration to Microsoft Sentinel | Microsoft Learn](#)



Microsoft Sentinel Migration – phases & key activities

Discovery	Design	Implement	Operationalize
Conduct a discovery to better understand the current state of your SIEM. Collect monitoring and alerting use cases and requirements. Key Activities - Identify requirements and detailed use cases - Identify and document your existing automation, remediation, and alerting tools and processes. - Identify your existing SOC processes, including investigation, automation, and remediation. - Identify critical security assets. - Assess existing security portfolio. - Identify integrations with IT service management (ITSM), threat intelligence, and automation solutions. Deliverables - Project plan - Current state analysis - Business and technical requirements - Use cases	Create a comprehensive design that aligns with the current security portfolio and existing data sources. Key Activities - Design integration of Microsoft and third-party sources. - Map rules to Sentinel built-in rules. - Map dashboards to Sentinel workbooks. - Map automation to Sentinel playbooks. - Design custom alerting for Sentinel. - Map existing SOC processes to Sentinel features. - To migrate historical logs, review the available target platforms and data ingestion tools. Deliverables - Design workshops - Design documentation - Data source integration - Automation - Custom alerting	Implement the design phase: Integrate data sources that will connect to Microsoft Sentinel; ensure that Microsoft Sentinel works as designed. Key Activities - Connect Microsoft sources, cloud logs (AWS/GCP), network devices, and third-party security solutions. - Deploy Azure Monitor Agent to collect logs from VMs (Windows/Linux) and network devices. - Review your MITRE ATT&CK coverage. - Implement automation via Azure Logic Apps. - Convert remaining rules to Sentinel rules. - Deploy/create playbooks and automation rules. - Deploy playbooks for ITSM platforms, SOAR, and threat intelligence platform integration. - Deploy workbooks and convert dashboards to workbooks. - Review SOC operations migration best practices. Deliverables - Microsoft Sentinel PoC Plan - Connect Microsoft data sources - Connect external data sources - Deploy Azure Monitor agent - Implement workbooks and Playbooks	Operationalize Microsoft Sentinel Investigation and Response within existing security monitoring, alerting, and incident response processes. Key Activities - Assist with refining monitoring and alerting processes. - Assist with security incident management processes. - Assist with triage/investigation processes. - Assist with alerting use cases refinement. - Define SOC processes based on the mapping done in the design phase. Deliverables - Microsoft Sentinel configuration documentation - Workbooks - Playbooks - Custom alerts - KQL queries

Some holistic best practices

More than ingesting alerts and logs from other sources, Microsoft Sentinel also:

- **Uses the information it ingests with [machine learning](#)** that allows for better event correlation, alert aggregation, anomaly detection, and more.
- **Builds and presents interactive visuals via [workbooks](#)**, showing trends, related information, and key data used for both admin tasks and investigations.

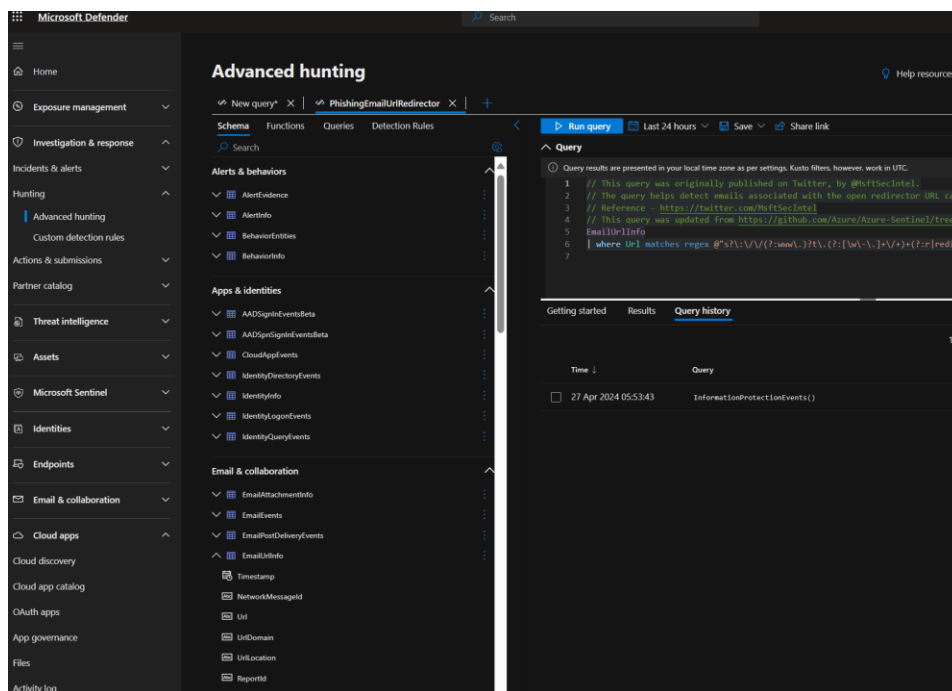
- **Runs [playbooks](#) to act on alerts**, gathering information, performing actions on items, and sending notifications to various platforms.
- **Integrates with partner platforms**, such as ServiceNow and Jira, to provide essential services for SOC teams.
- **Ingests and fetches enrichment feeds** from [threat intelligence platforms](#) to bring valuable data for investigating.

Advanced Hunting (AH)

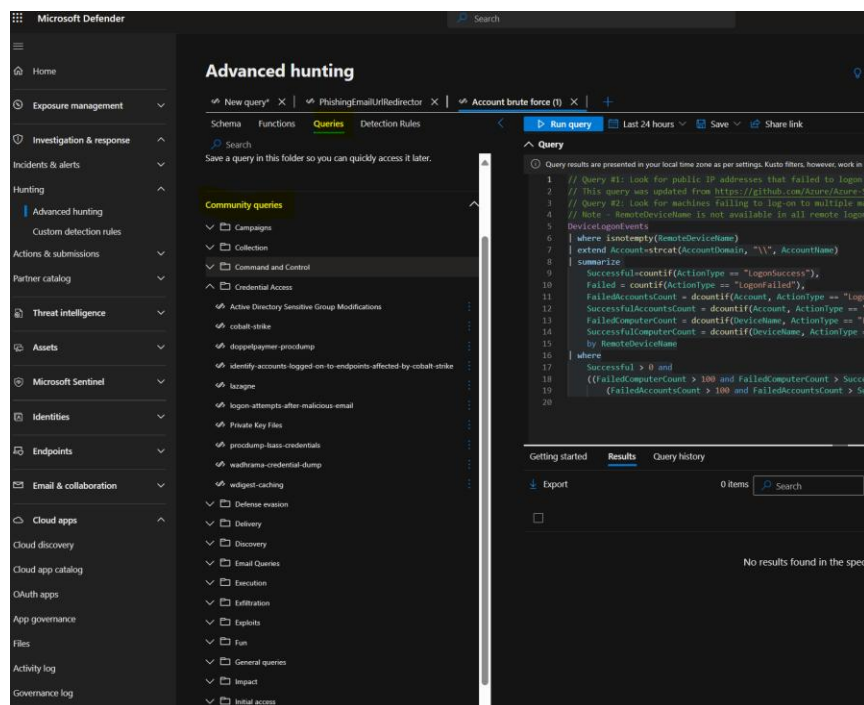
Our AH is our query-based threat hunting using KQL language. It allows you up to 30 days of raw data to discover. Essentially, the telemetry we absorb from our defender stack, is converted to schema tables so we can query it using KQL. We have a number of schemas from Identity, Email, Endpoint, Sentinel etc. Full schema [Data tables in the Microsoft Defender XDR advanced hunting schema - Microsoft Defender XDR | Microsoft Learn](#)

If you're new to KQL, we have two ways to query our schema, guided and advanced (writing KQL from scratch). Guided query is we have a bunch of templates already located in our tables. If you want to hunt and probe threats in email or identity, you can simply go into the table and find the closest query. If the query you are looking for is not there, you can also go into the queries tab and community queries which potentially could have queries that the community has uploaded to share.

[Overview - Advanced hunting - Microsoft Defender XDR | Microsoft Learn](#)



Community Queries

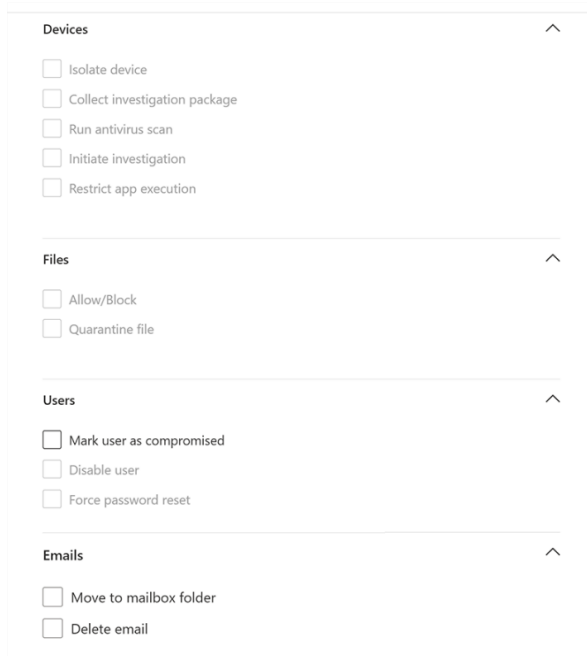


Sample Queries

IdentityLogonEvents where Timestamp > ago(7d) sort by Timestamp desc	Identity
IdentityLogonEvents where Protocol == @"Kerberos" where isnotempty(AccountUpn) extend UPN_Account = split(AccountUpn,'@')[0] project Protocol, AccountUpn, UPN_Account	Identity
DeviceFileEvents where Filename == 'Invoice.pdf.exe'	MDE
DeviceEvents where ActionType =~ "ExploitGuardNetworkProtectionBlocked" summarize count(RemoteUrl) by InitiatingProcessFileName, RemoteUrl, Audit_Only=tostring(parse_json(AdditionalFields).IsAudit) sort by count_RemoteUrl desc	MDE

Customer Detection

You can further take advantage of advance hunting queries by creating custom detection. You can run these queries regularly, if you find matches you can then set responses like below. This is one of those features I guess you rarely hear but I would say this is another great feature I'm comfortable to include as part of an additional auto-remediation in Defender XDR



The image shows a screenshot of a user interface for Microsoft Defender XDR, displaying a list of response actions categorized into four sections: Devices, Files, Users, and Emails. Each section has a title and a list of actions, each preceded by an unchecked checkbox. The 'Devices' section includes 'Isolate device', 'Collect investigation package', 'Run antivirus scan', 'Initiate investigation', and 'Restrict app execution'. The 'Files' section includes 'Allow/Block' and 'Quarantine file'. The 'Users' section includes 'Mark user as compromised', 'Disable user', and 'Force password reset'. The 'Emails' section includes 'Move to mailbox folder' and 'Delete email'. Each section is separated by a horizontal line and has an upward-pointing arrow icon to its right.

Category	Actions
Devices	☐ Isolate device ☐ Collect investigation package ☐ Run antivirus scan ☐ Initiate investigation ☐ Restrict app execution
Files	☐ Allow/Block ☐ Quarantine file
Users	☐ Mark user as compromised ☐ Disable user ☐ Force password reset
Emails	☐ Move to mailbox folder ☐ Delete email

Security Copilot

It's important to note that Security Copilot is **not part of the E5 suite**. This section is highlighting an important product that will continue to be integrated and critical to our Microsoft Security story. It goes without saying that AI should be part of all Security conversation. As cyber threats continue to increase at scale, various techniques that will heavily include AI targets. We need help to triage, summarize and respond to alerts and incidents at a much faster rate. Complex attacks, include lengthy attack stories, complex techniques at a large scale. Security Copilot can help us reduce the need to triage incidents at a slower pace which is a risk in itself as the attack gets deeper while investigation happens.

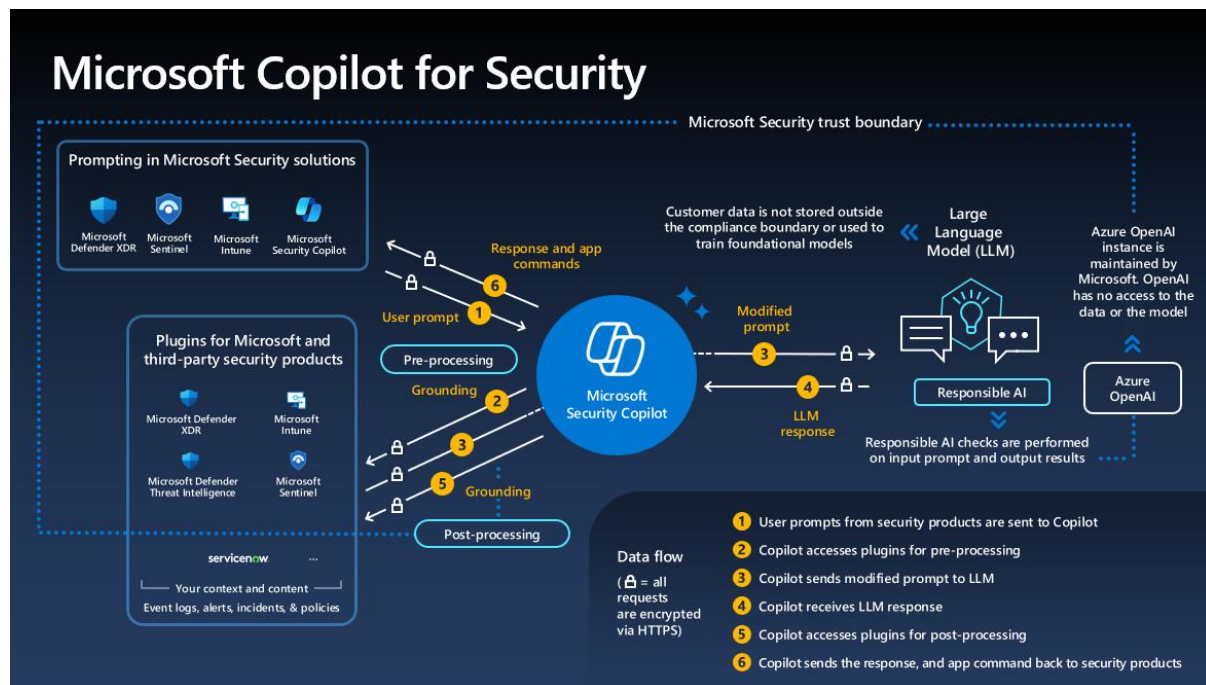
Microsoft Security Copilot is a **generative AI-powered security solution** that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale

How does Security Copilot help Defender XDR & Sentinel much better?

The new, embedded experience in Microsoft Defender XDR supercharges security teams with generative AI capabilities to take their efficiency to a new level for the following set of powerful use cases:

- Respond to threats at the speed of AI with assisted incident investigation and response.
- Scale advanced tasks to all skill levels.
- Perform malicious code analysis in real time
- Apply threat intelligence into your investigation workflows with ease

SECURITY COPILOT Architecture



Security Copilot primary use cases

Security Copilot focuses on making the following use cases easy to accomplish.

- Investigate and remediate security threats - gain context for incidents to quickly triage complex security alerts into actionable summaries and remediate quicker with step-by-step response guidance
- Build KQL queries or analyse suspicious scripts -
- Understand risks and manage security posture of the organization
- Troubleshoot IT issues faster - synthesize relevant information rapidly and receive actionable insights to identify and resolve IT issues quickly
- Define and manage security policies - define a new policy, cross-reference it with others for conflicts
- Configure secure lifecycle workflows -
- Develop reports for stakeholders - get a clear and concise report that summarizes the context and environment

Security Copilot focuses on making the following highlighted use cases easy to use:

Incident summarization

BEC financial fraud attack was launched from a compromised account (attack disruption)

The screenshot displays the Microsoft Defender XDR interface. At the top, a yellow banner states: "Important: A potentially compromised account was disabled automatically by attack disruption in Microsoft 365 Defender. For more details, select the Assets > Users tab or go to the [Action center](#)." Below this, the "Attack story" section shows a list of alerts on the left and an "Incident graph" in the center. The graph illustrates the attack flow: "3 IPs" connected to "2 Cloud Applications", which then connects to a "User" node, leading to an "Update" node. On the right, the "Incident summary" panel provides a detailed overview of the attack, including the threat overview, activity profile, incident details, and impacted assets. The summary describes a high-severity BEC financial fraud attack that occurred between 2024-03-15 14:26:31 UTC and 2024-03-15 14:40:38 UTC, triggered by an automatic Attack Disruption action. It details the initial compromise, credential access, and the subsequent collection and defense evasion.

Gain context for incidents and improve communication across your organization by leveraging generative AI to swiftly distil complex security alerts into concise, actionable summaries, which then enable quicker response times and streamlined decision-making.

Analyse code

The screenshot displays the Microsoft Defender XDR interface. The "Device" section shows a timeline of events from Dec 2023 to Mar 2024. The timeline highlights several events, including "schtasks.exe created process ZimbaKul.exe as user 'Device\jadmin'", "A PowerShell interpreter process was launched by schtasks.exe", "schtasks.exe created a process ZimbaKul.exe with a different PE original...", "ZimbaKul.exe command line contained encoded content", "powershell.exe ran Powershell command: 'Start-Sleep'", "powershell.exe ran Powershell command: 'Get-Random'", "powershell.exe created process schtasks.exe", "schtasks.exe set registry value 'Actions' for key 'SOFTWARE\Microsoft\Win...", "schtasks.exe set registry value for key 'HKY_LOCAL_MACHINE\SOFTWARE\M...", "schtasks.exe created registry key 'SOFTWARE\Microsoft\Windows NT\Cur...", "schtasks.exe created registry key 'HKY_LOCAL_MACHINE\SOFTWARE\Micros...", "schtasks.exe attempted to encrypt credentials", "Device\jadmin signed into a Windows domain successfully", "Batch login by Device\jadmin succeeded", "powershell.exe created process schtasks.exe", "powershell.exe created the scheduled task Run-ExportADFSignedC...", and "schtasks.exe command line contained encoded content". On the right, a detailed view of a specific event is shown, including the process ID, execution time, command line, image file paths, image file SHA1, image file SHA256, execution details, signer, issuer, and virus total detection ratio.

Utilize AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively.

Guided response

3EC financial fraud attack was launched from a compromised account (attack disruption)

High Active | AlignedSkHouse - AlignedSkHouse | [BEC fraud](#) | [Compromised threat](#) | [Defender Update](#) | [Attack Disruption](#) | [BEC](#) | [Email threats](#) | [Alerts](#)

Important: A potentially compromised account was disabled automatically by attack disruption in Microsoft 365 Defender. For more details, select the Assets > Users tab or go to the [Action center](#).

Attack story Alerts (20) Assets (4) Investigations (2) Evidence and Response (25) Recommended actions (21) Summary Similar incidents (0)

Play attack story

Mar 15, 2024 2:28 PM Resolved
Activity from a Tor IP address

Mar 15, 2024 2:28 PM Resolved
Suspicious inbox manipulation rule

Mar 15, 2024 2:28 PM Resolved
Activity from a Tor IP address

Mar 15, 2024 2:28 PM Resolved
Suspicious inbox manipulation rule

Mar 15, 2024 2:28 PM Resolved
A potentially malicious URL click was detected

Mar 15, 2024 2:28 PM Resolved
A potentially malicious URL click was detected

Mar 15, 2024 2:28 PM Resolved
Anonymous IP address

Mar 15, 2024 2:28 PM Resolved
Anonymous IP address

Mar 15, 2024 2:28 PM Resolved
Compromised user account in a recognized attack pattern

Mar 15, 2024 2:28 PM Resolved
Anonymous IP address

Incident graph

Threat overview: Cloud identity abuse
22 impacted assets
[View threat analytics report](#)

Activity profile: OAuth apps used in BEC and phishing
1 impacted asset
[View threat analytics report](#)
[View all 3 related threats](#)

Incident details

Assigned to: AlignedSkHouse - AlignedSkHouse
Incident ID: 2443

Classification: Not set
Categories: Initial access, Defense evasion, Credential access, Collection

First activity: Mar 15, 2024 2:26:31 PM
Last activity: Mar 15, 2024 2:40:38 PM

Impacted assets

Users (0)

Apps (2)

Microsoft - 27 20885 - None

Copilot
Guided response
Mar 26, 2024 1:04 PM
Completed recommendations 2/4
[Status: All](#)

Containment

Completed
Disable the account Name
[View details](#)
All generated content may be incorrect. Check it for accuracy.

Remediation

New
Delete similar emails
We found emails that are very similar to emails involved in this incident. Delete these emails to contain the attack.
[Soft delete emails](#) [View similar emails](#)
All generated content may be incorrect. Check it for accuracy.

Completed
Disable the account Name in AD
The user account Name might be compromised. Require the user to change their password on their next sign in.
[Force password reset](#) [View user](#)
All generated content may be incorrect. Check it for accuracy.

Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation. Relevant deep links to recommended actions allow for quicker response.

Sentinel Plug-in

Incidents > SAP - (Preview) File Downloaded From a Malicious IP Address-updated 2 on one endpoint

SAP - (Preview) File Downloaded From a Malicious IP Addr...

Medium Active Unassigned

Attack story Alerts (2228) Assets (2) Investigations (0) Evidence and Response (1) Summary Similar incidents (0)

Incident graph

Layout Group similar nodes

Communication Association

SAP - (Preview) File Downloaded From a M...

What happened

User has downloaded a file from an SAP system using an IP address known to be malicious. Malicious IP addresses are obtained from threat intelligence services. For additional information visit the [Connect your threat intelligence platform to Microsoft Sentinel] (<https://learn.microsoft.com/Azure/sentinel/connect-threat-intelligence-tip>) how-to page. This Alert rule allows for a cross-workspace query to accommodate an architecture where the threat intelligence data resides in a different workspace than the one which holds the SAP data

ANALYTICS RULE

Analytics rule details

Rule name
SAP - (Preview) File Downloaded From a Malicious IP Address-updated 2
[View rule in Sentinel](#)

Rule description
User has downloaded a file from an SAP system using an IP address known to be malicious. Malicious IP

Alert state

Classification: Not Set
Assigned to: Unassigned

Alert details

Category: Exfiltration
MITRE ATT&CK Techniques: -

Detection source: NRT rules
Service source: Microsoft Sentinel

Detection technology: -
Generated on: Jun 30, 2024 9:27:32 AM

First activity: Jun 29, 2024 9:27:15 PM
Last activity: Jun 30, 2024 9:25:15 AM

Evidence

Copilot

Incident summary
Jul 1, 2024 10:30 PM

The medium severity incident titled "File Downloaded From a Malicious IP Address on one endpoint" occurred between 2024-06-30 02:27:15 UTC and 2024-07-02 03:25:16 UTC.

- Exfiltration: The incident began at 2024-06-30

[See more](#)

AI-generated content may be incorrect. Check it for accuracy.

Guided response
Jul 1, 2024 10:39 PM
Completed recommendation...

Status: All

Investigation

New

Contact user amacgregor@contoso.com on Teams, and ask them to confirm their activity

Hi,

We hope this message finds you well. We are reaching out to you regarding a security alert that was triggered on July 2, 2024, at 03:24:16 UTC. The alert was titled "File Downloaded From a Malicious IP Address."

In simple terms, our systems detected that a file was downloaded

Copilot integrates with other MS Security Solutions

- Sentinel Plugin
- Defender XDR
- Microsoft Entra ID
- Microsoft Intune
- Microsoft Purview
- Microsoft Defender for Cloud
- Microsoft Defender Threat Intelligence

Thank you for taking time to read this high-level guide. As a summary, the objective of this guide is to help customers, partners and partners to get a quick overview on the best practice approach to deploy Microsoft Defender XDR. Is also to highlight its capability of cross-product discovery and respond and how each workload can enrich the full potential of Defender XDR.

Yours truly,

Ray Reyes