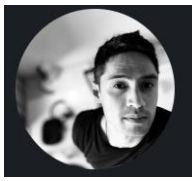
Defender XDR + Sentinel

Deployment Guide

By Ray Reyes
Data Security ANZ Lead, Microsoft



Updated: 6th August 2024

<u>This article is for Customers, Partners, and Colleagues</u>

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 Vulnerability Management (MDVM)
- Microsoft Defender for Cloud Apps (MDA)
- Microsoft Sentinel

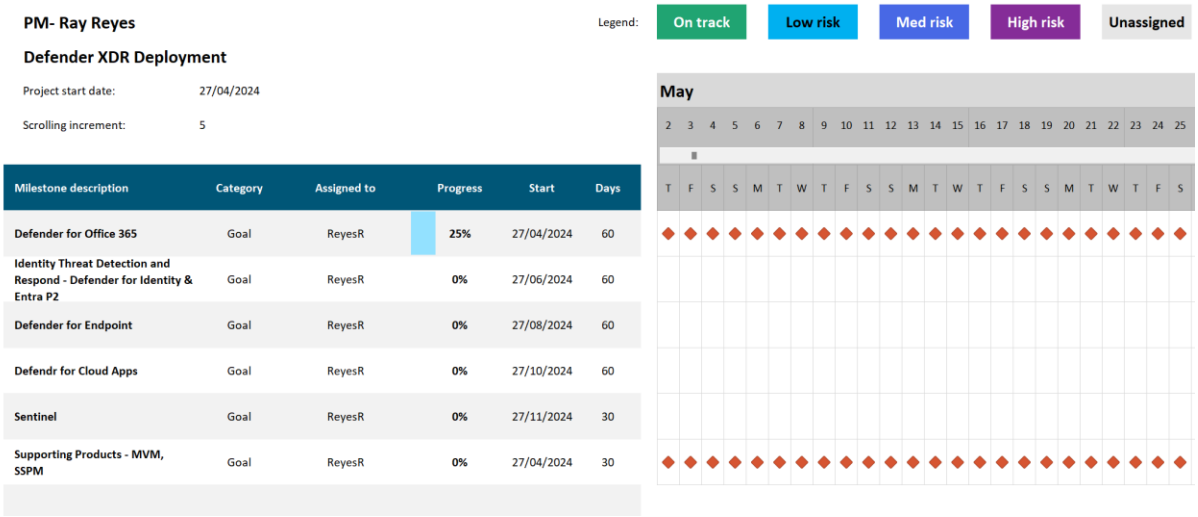
Highlights

- Copilot for Security
- Advanced Hunting
- App Governance

Background

My role at Microsoft is helping customers deploy workloads in E5 Security and Purview. The reason for this paper is to answer in depth two common questions we get in my role.

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



PM- Ray Reyes

Defender XDR Deployment

Project start date: 27/04/2024

Scrolling increment: 5

Legend: On track | Low risk | Med risk | High risk | Unassigned

Milestone description	Category	Assigned to	Progress	Start	Days
Defender for Office 365	Goal	ReyesR	25%	27/04/2024	60
Identity Threat Detection and Respond - Defender for Identity & Entra P2	Goal	ReyesR	0%	27/06/2024	60
Defender for Endpoint	Goal	ReyesR	0%	27/08/2024	60
Defendr for Cloud Apps	Goal	ReyesR	0%	27/10/2024	60
Sentinel	Goal	ReyesR	0%	27/11/2024	30
Supporting Products - MVM, SSPM	Goal	ReyesR	0%	27/04/2024	30

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 written based on my experience helping customers deploy our 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 an option with a personalised touch.

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 perio**d from MDI to MDO and MDE, which about a minimum 30 days for Machine Learning to collect any data. During the learning period, it's important to have active participation from your users to feedback and help you fine tune policies. As most of our deployment guide, we apply around **Crawl, Jog and Run** approach

Let's define these 3 phases:

Walk

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.

Jog

This is when you bring the people from the business, power users 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 is 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

Run

Time to bulk deploy.

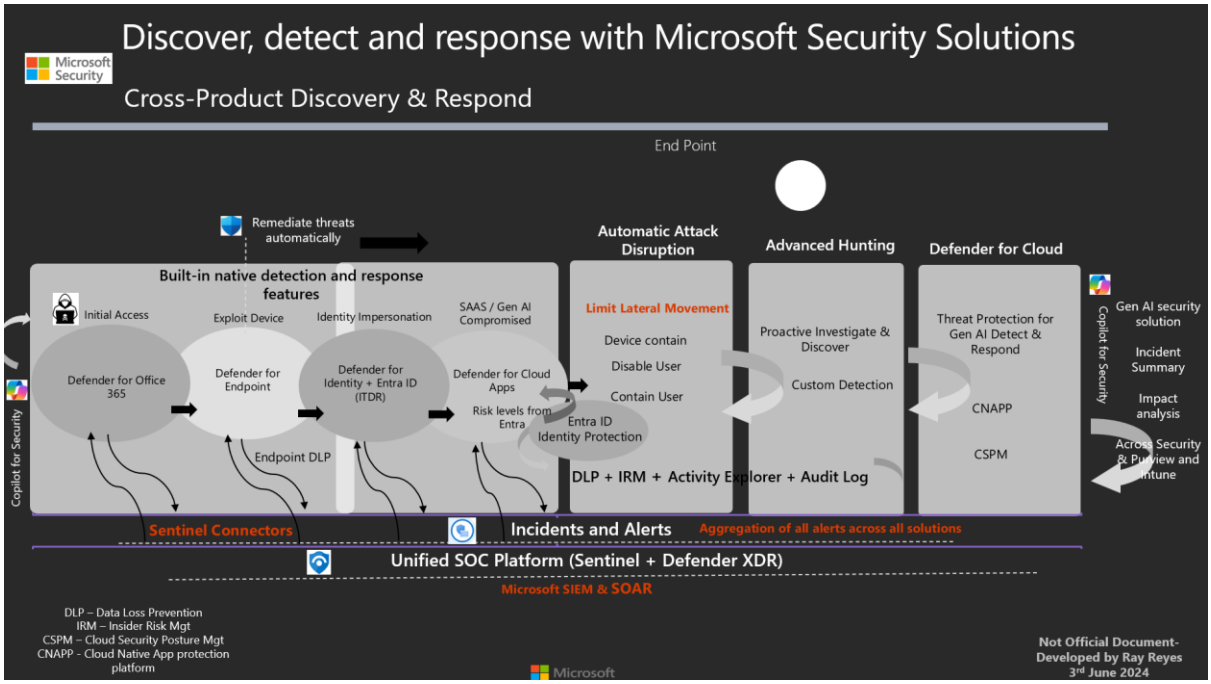
What is Microsoft Defender XDR?

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
- Zero Trust Coverage
- Enablement of Automatic Attack Disruption

- XDR + Sentinel better together story



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

Scenario

The story we will follow for this guide is a **customer that is migrating to 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, lets 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 license for it.

Customer 'We've just subscribed 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 fresh mindset. What customers tend to do is try to feature match their current protection against the Microsoft Defender XDR, we just do things slightly differently, we detect differently, we process logs differently, we can engineer our detection fasters or enable them in the OS (we own windows so things do get engineered fast) and features might be different.

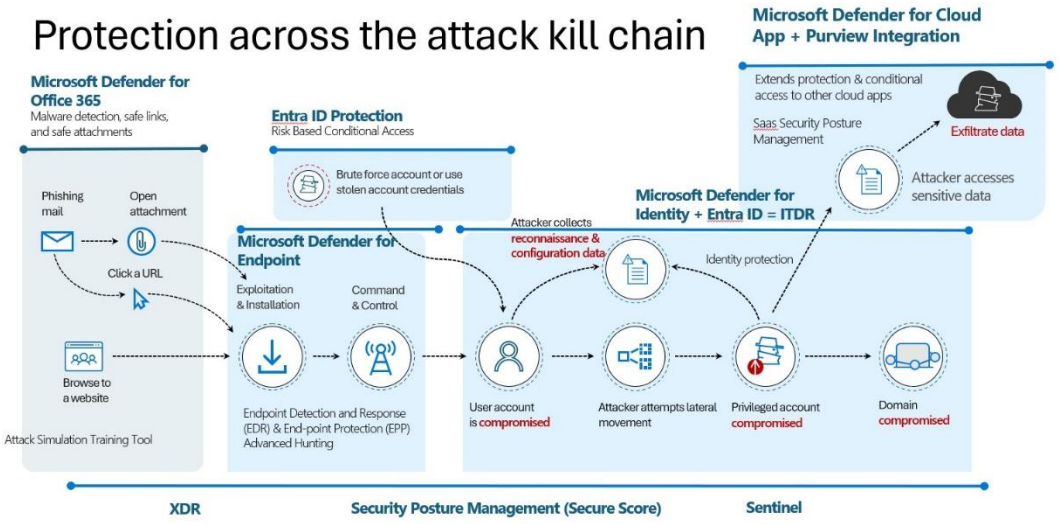
Another key takeaway and one I often come across with customers, it's how the migration is 'urgent' so the deployment timeline is 'aggressive' migration. The downside is, there is no time for change management, no time for machine learning to kick in, no time for a 'phase' deployment, no time for pilot users to feedback issues or report false positives or assess reports. So, if you're a customer who's reading this, plan way 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. There is a tonne of various techniques from your credential harvesting technique to more sophisticated ones like QR Code

Phase 1 - Microsoft Defender for Office 365

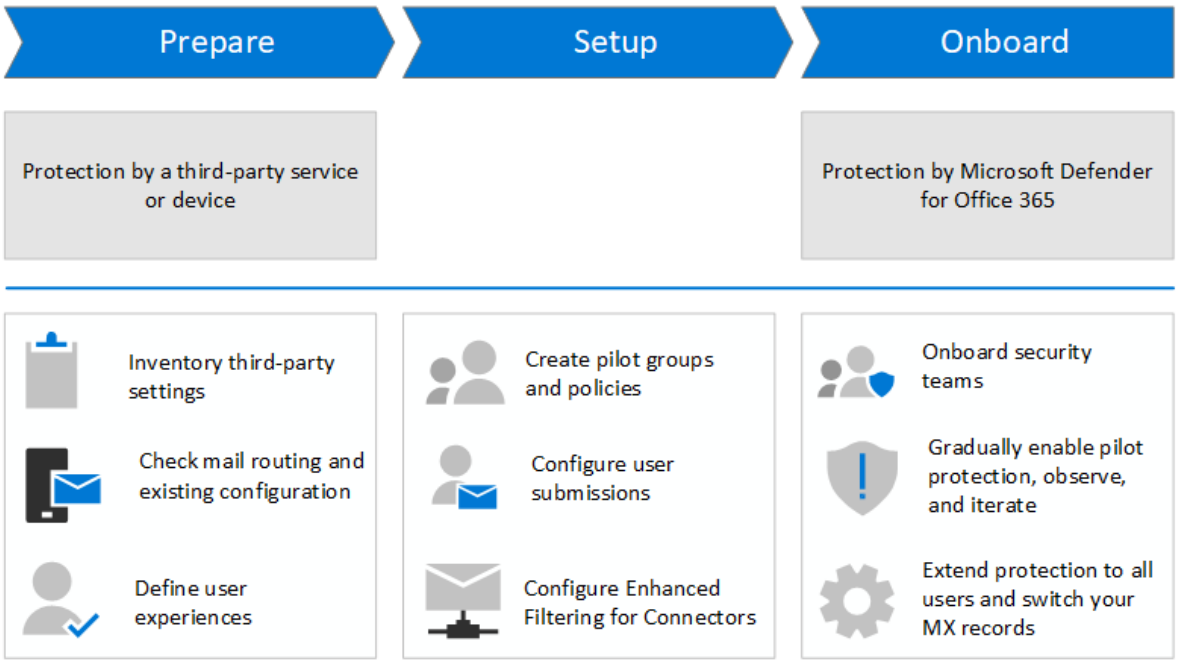
Key Watch outs

- 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.

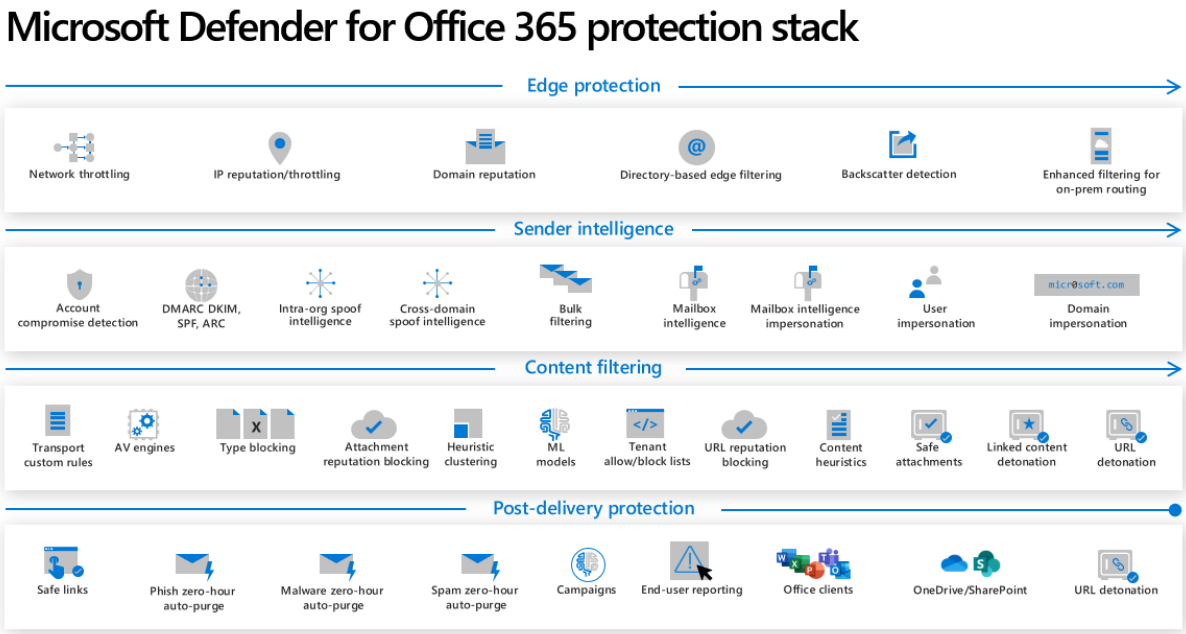
If you're coming from a 3rd party protection, we have a comprehensive guide in migration in our public docs [Migrate from a third-party protection service to Microsoft Defender for Office 365 | Microsoft Learn]



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

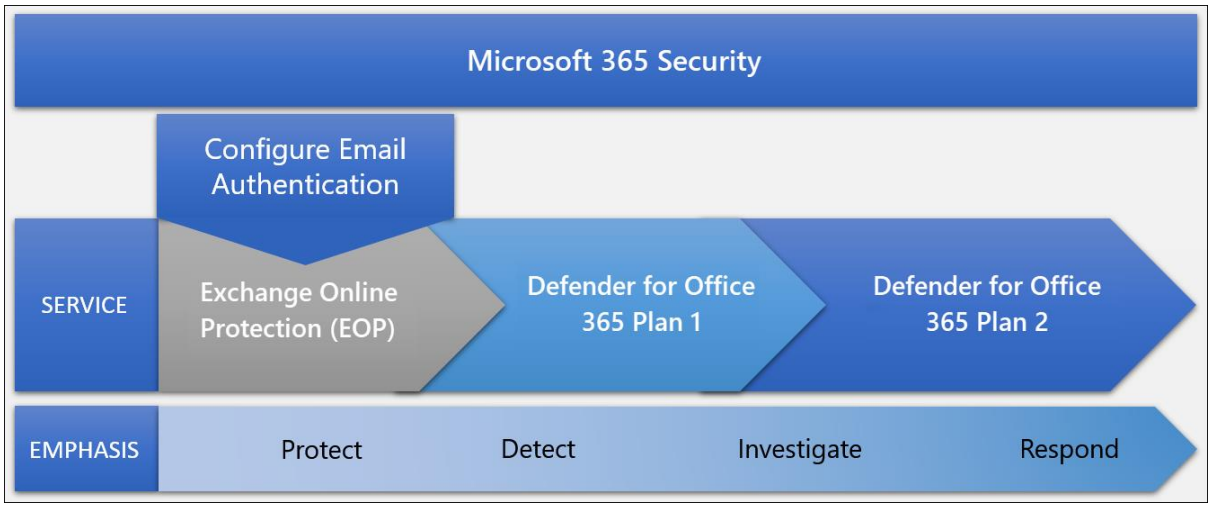
The protect stack is layered in 4 phases. Highlighting that these are a mixture of EOP, P1 and P2 subscription features***, but if you're an E5 customer, nee bother***.

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



- Edge Protection – still a crucial part of the stack, this phase is design to block automatically tho 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 cover 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 m365 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.

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 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**)

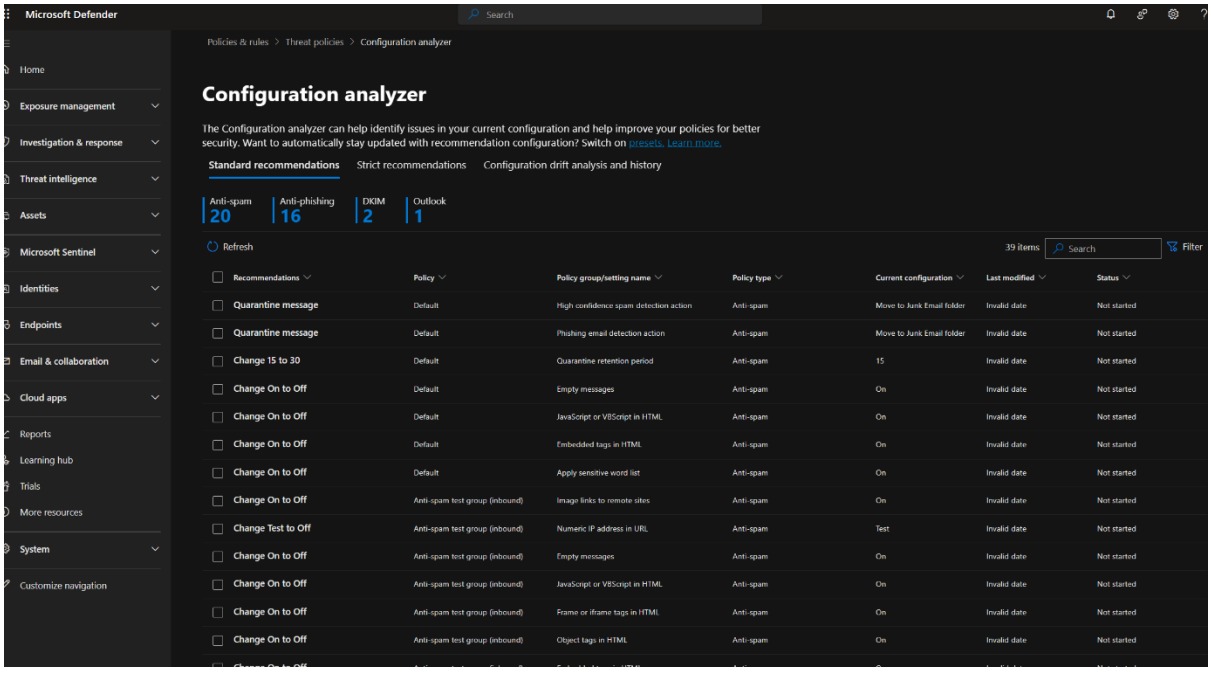
- ***A Safe Attachments pilot group**: For example, **MDOPilot_SafeAttachments***
- ***A Safe Links pilot group**: For example, **MDOPilot_SafeLinks***
- ***A pilot group for Standard anti-spam and anti-phishing policy settings**: For example, **MDOPilot_SpamPhish_Standard***
- ***A pilot group for Strict 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 M365 can fully be tested by your pilot.

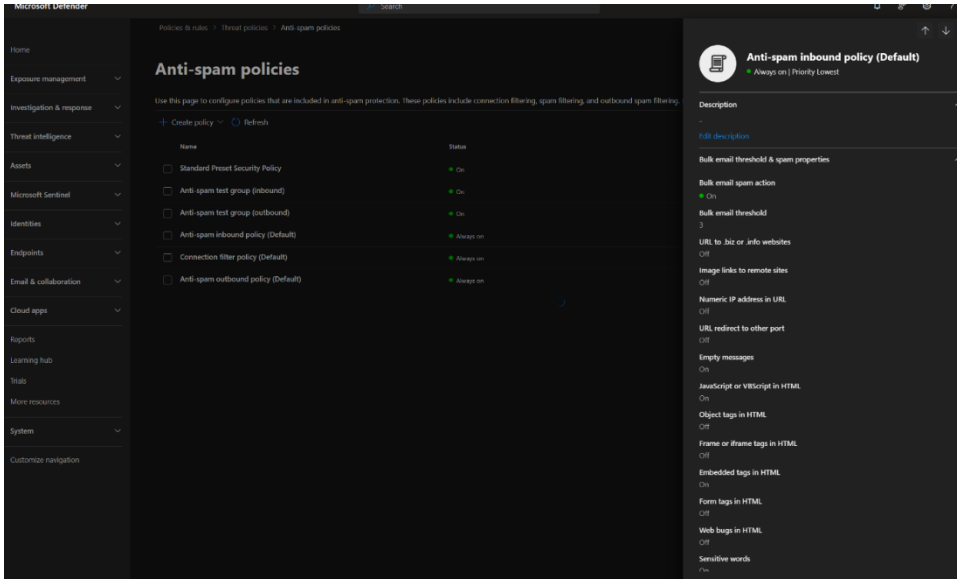
When building your pilot policies for the above you can use our config-analyzer which is our best practice configuration recommendation which will be your best friend going forward

The goal of config analyzer 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.



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



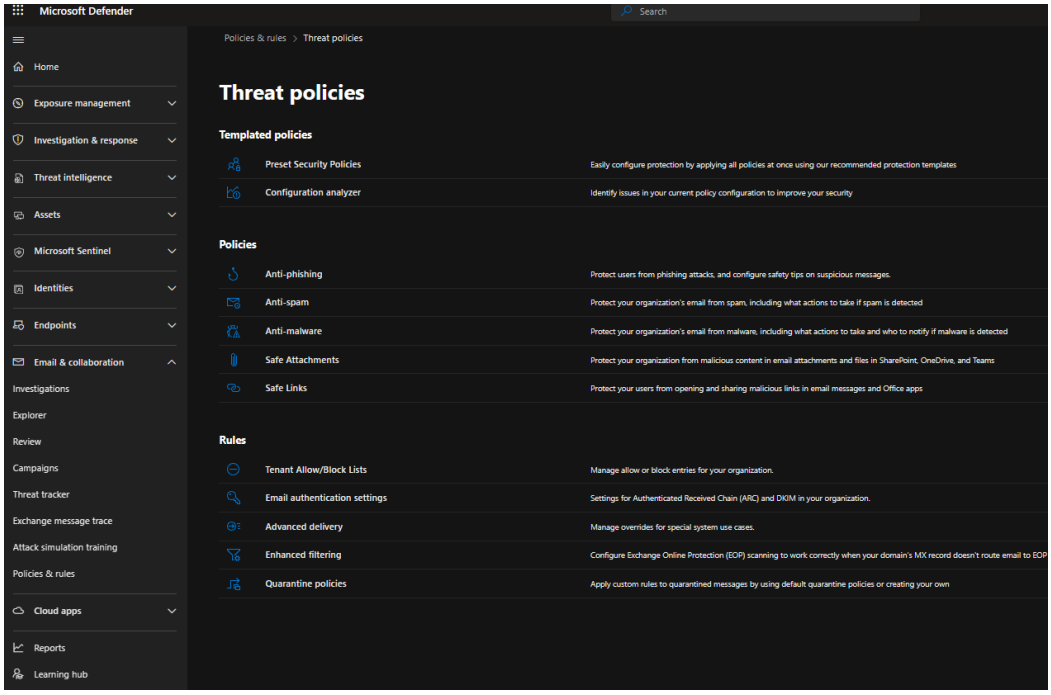
Important note: when deploying policies, our recommendation is to use **users or groups** for your pilot phase and domains when you're ready for general deployment. We don't recommend mixing all 3.

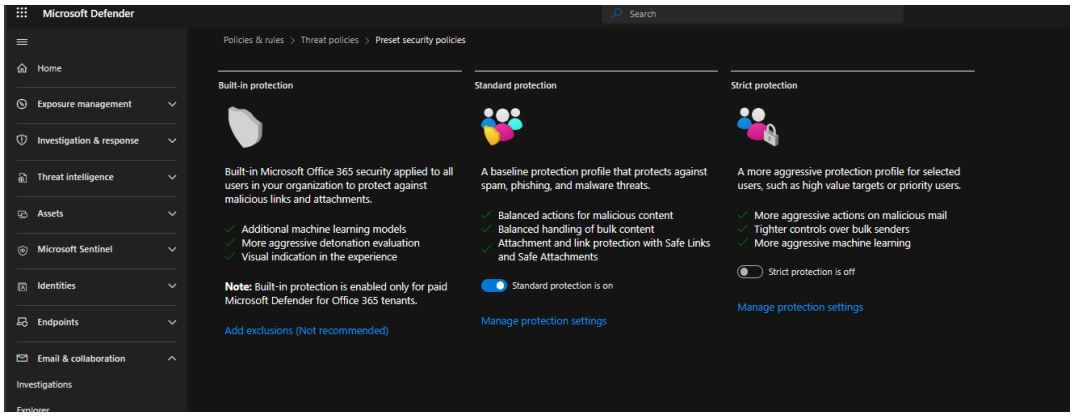
<u>Exchange Online Protection (EOP) and Microsoft Defender for Office 365 (MDO) Policies</u>

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.

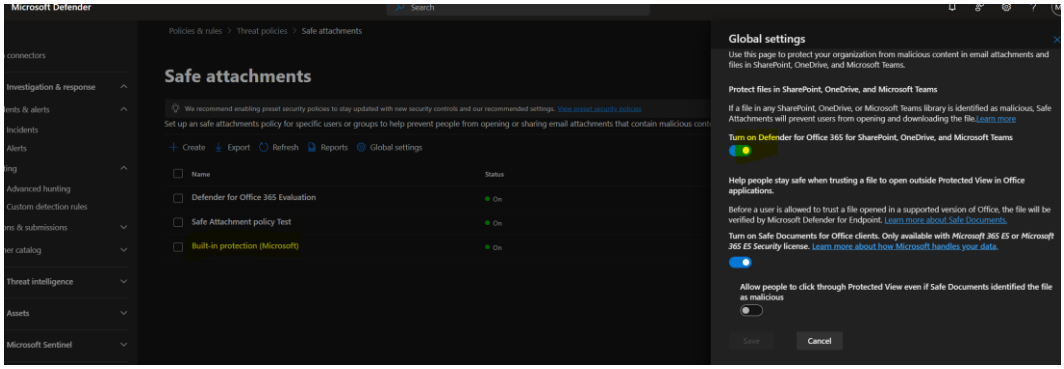
Preset security policies - Microsoft Defender for Office 365 | Microsoft Learn

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



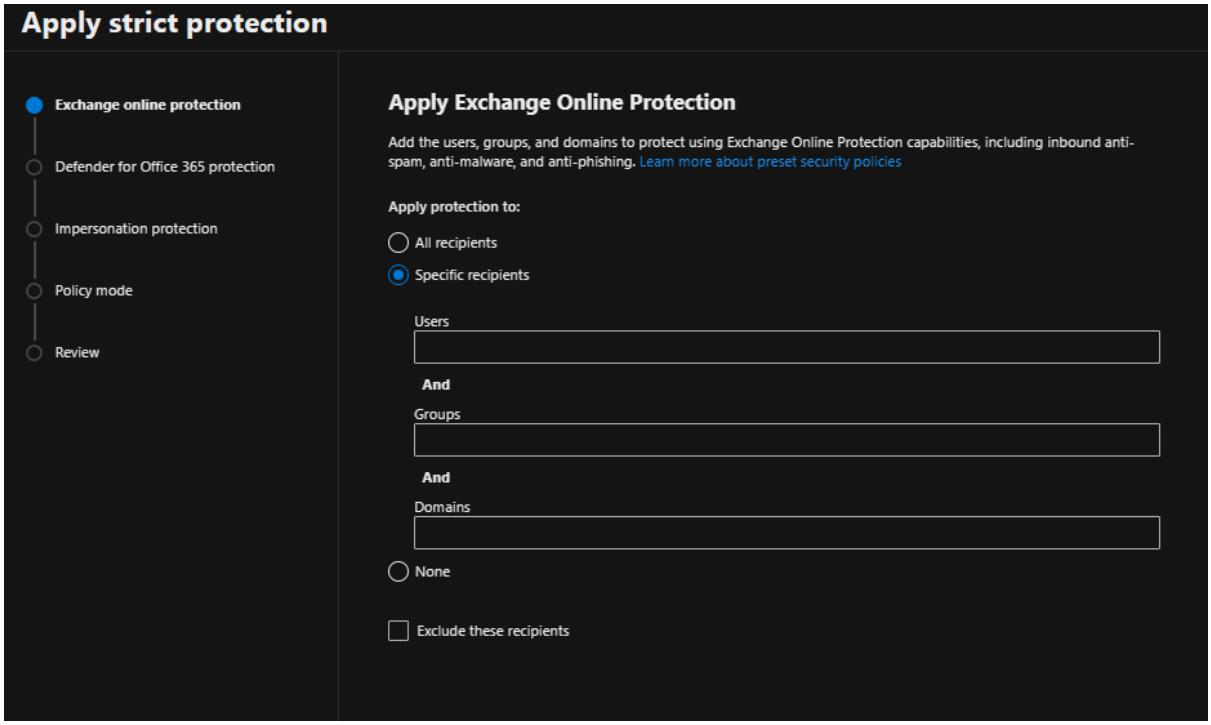


By default, both Safe attachments and Safe links are enabled. However, you can still customised users or groups for granular or more specific use case policy



[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]



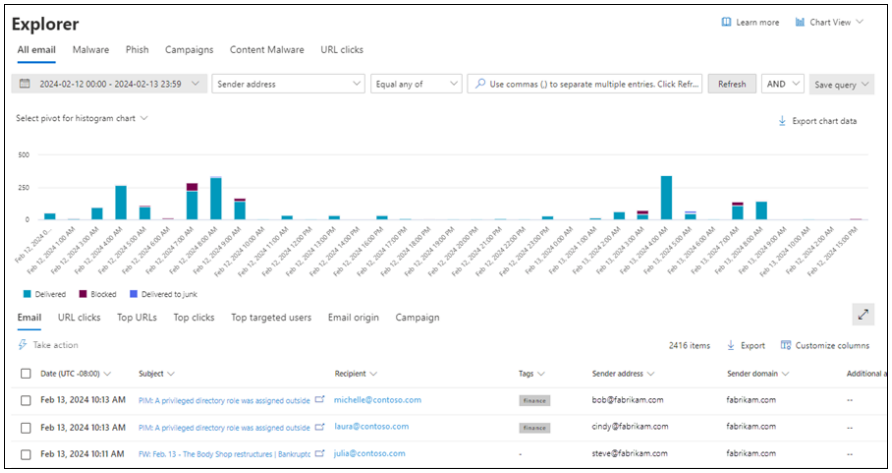
Onboard MDO – Steps 1-8

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 is 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.

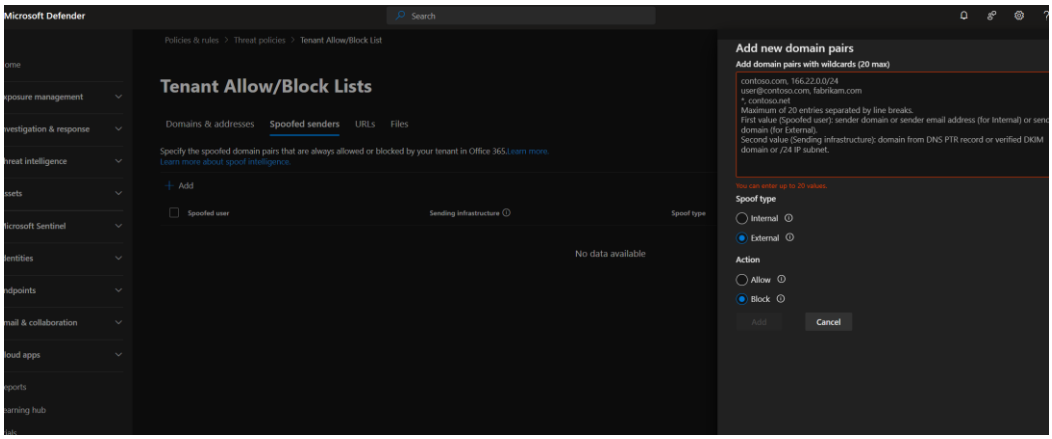
As your users report false positives, there's a few features you can leverage to confirm the validity of their concern, these are a mixture of P1 and P2 features so look carefully. As an example. Threat explorer is a great feature to dive deeper on emails that could be malicious and the validity of it.



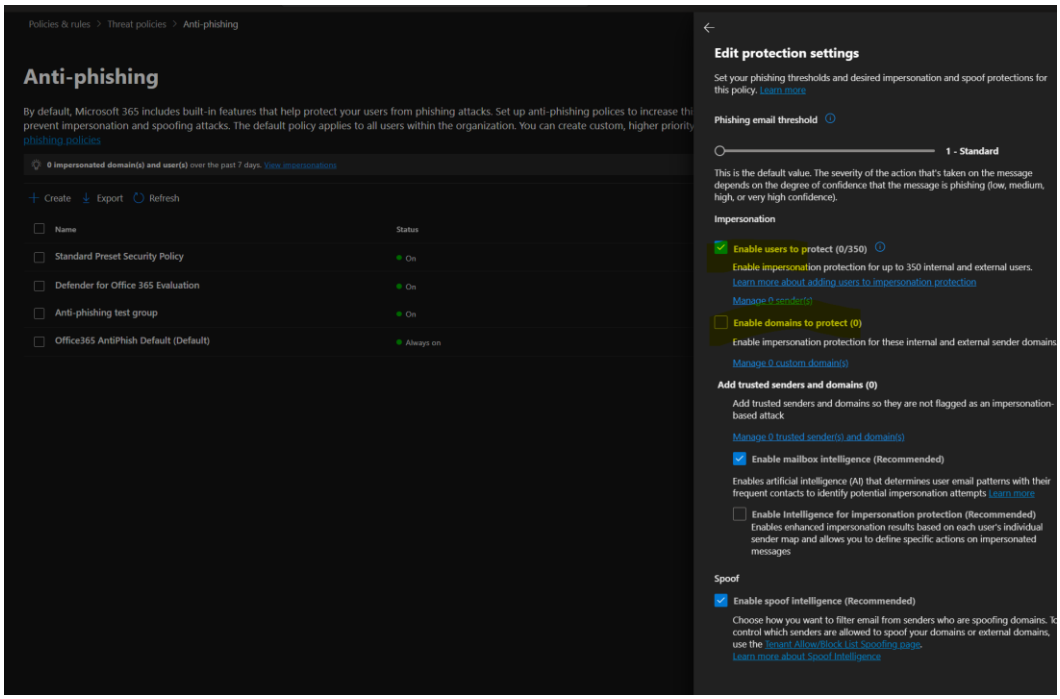
- Quarantine
- Threat Explorer (Explorer)
- Email security reports
- Defender for Office 365 reports
- Mail flow insights
- Mail flow reports

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

Tune Spoof in Tenant Allow/Block List



Impersonation users and domains



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.

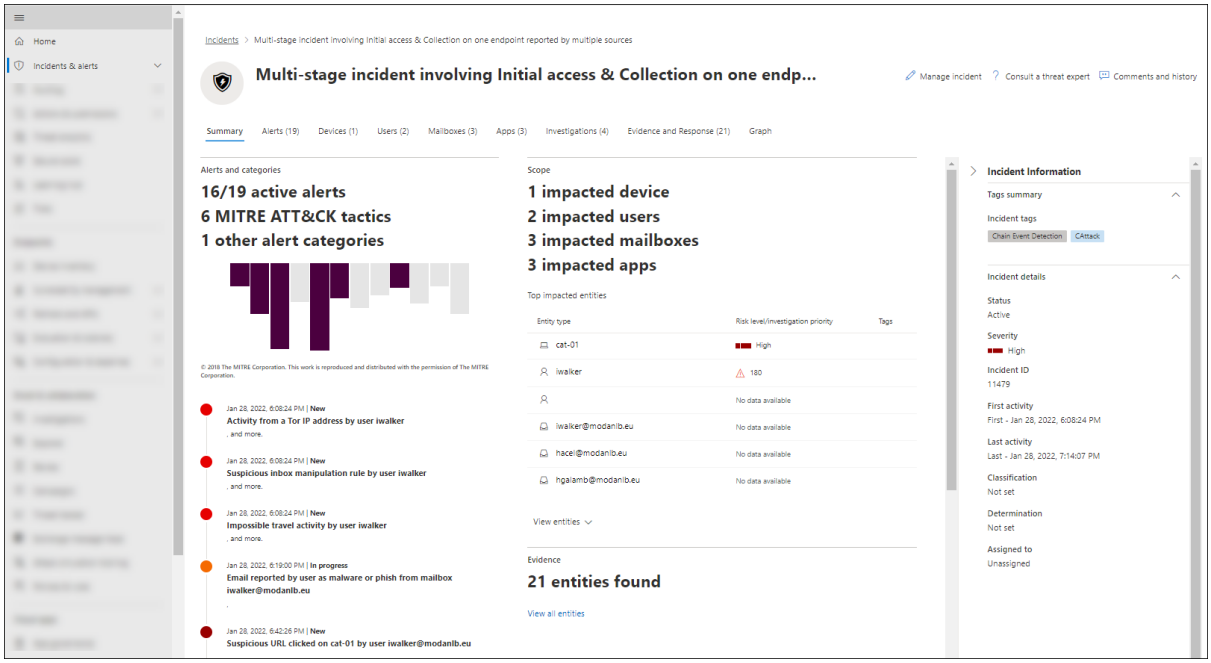
Essentially you have two steps in this section, apply the policy to all and **then Turn off the mail flow so it can now point to M365**.... Turn off the SCL = 1 mailflow rule

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 procactive. 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

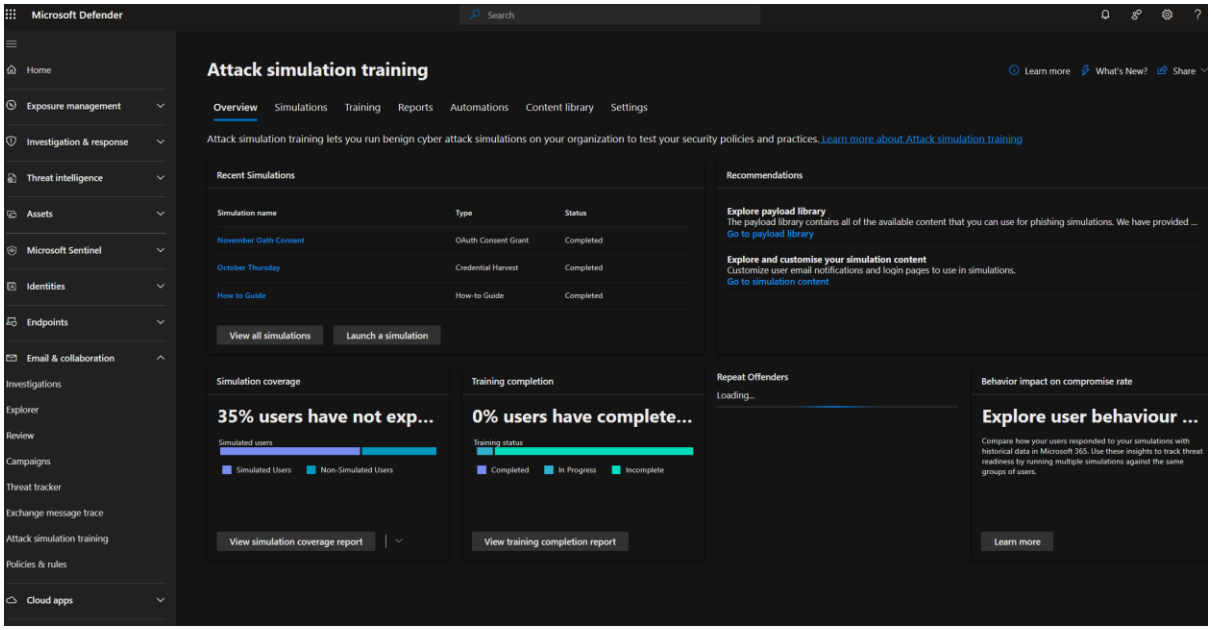
Manage submissions - Microsoft Defender for Office 365 | Microsoft Learn

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 feature 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)

'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 logins and access, investigating suspect posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure' -' Gartner'

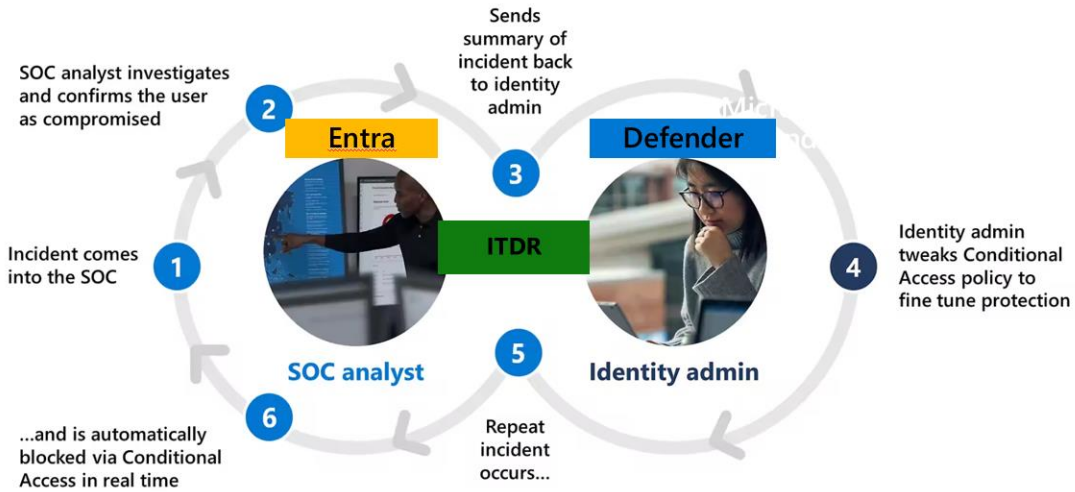
Key Watch outs

- Capacity planning! Crucial on the early stages on this deployment, importance on ensuring opening up 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 gpo 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've always had solutions to cover on-prem, our cloud and 3rd party identies. You can safely say, it's 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.

So, from a 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

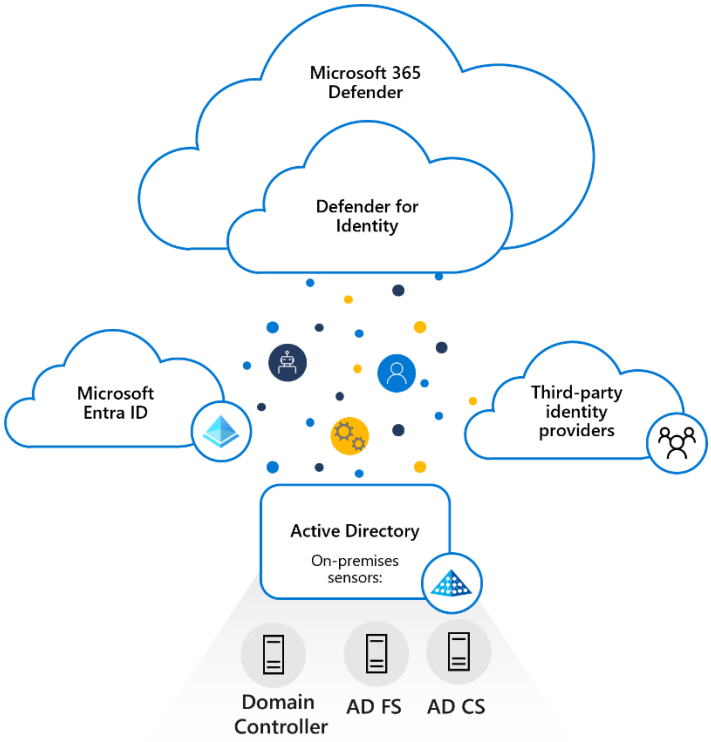
The time deploying this product depends on how large your organisation is based on the number of DCs, ADFS, ADCS and where I often see customers hit some delays are upgrading some of the servers that require more specs, and the back and forth change request can slow things down in the beginning. One 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, lets take a 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 light weight bit of code.

In the domain controller, we collect and parsed network data from the Domain Controller, and sending that telemetry to the cloud services…. In the Domain Controller, what we're 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 parsed 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.



So **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

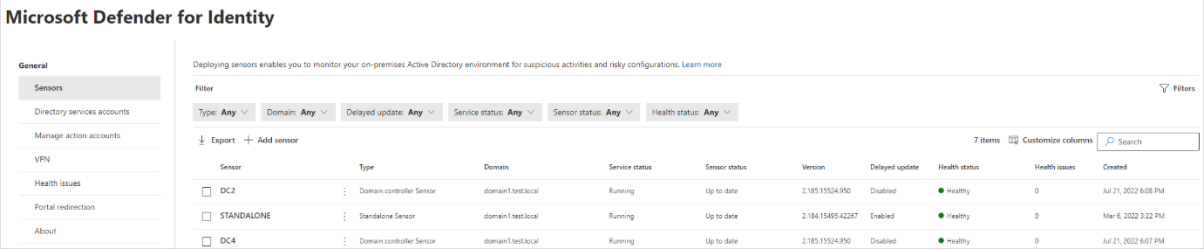
** Outbound connection to MDI instance hosted at *.atp.azure.com

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 perio

Step 3. Install and configure the sensor in DC

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



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 Configuring sensors for AD FS and AD CS - Microsoft Defender for Identity | Microsoft Learn

Important Update 06.8.2024.

When I wrote this article, this new capability was still being tested and was just getting into preview. Since then, it has gone to General Availability. So for customers, who've already onboarded their domain controllers to Defender for Endpoint, you can activate Microsoft Defender for Identity capabilities directly on a domain controller instead of using a Microsoft Defender for Identity sensor.

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

Activate Microsoft Defender for Identity capabilities directly on a domain controller - Microsoft Defender for Identity | Microsoft Learn

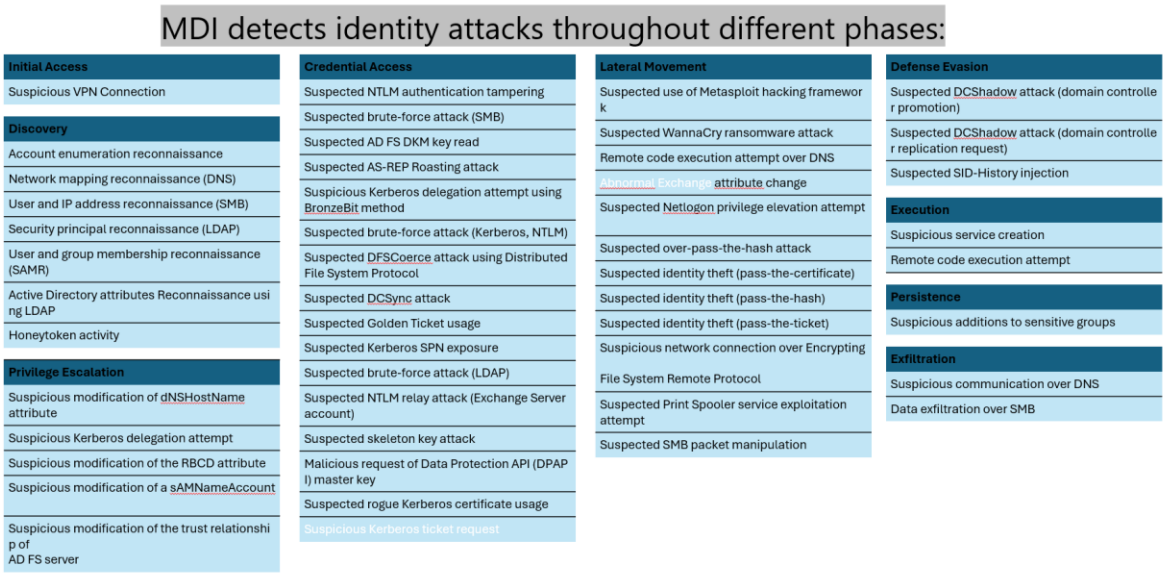
Step 4. Once if you've confirmed that the sensor is installed and is healthy, its time to enable the windows event collection so we can start collecting this logs to Defender. The good news is that in the past we had to do this manually and a few months ago we've recently released the NEW Powershell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

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

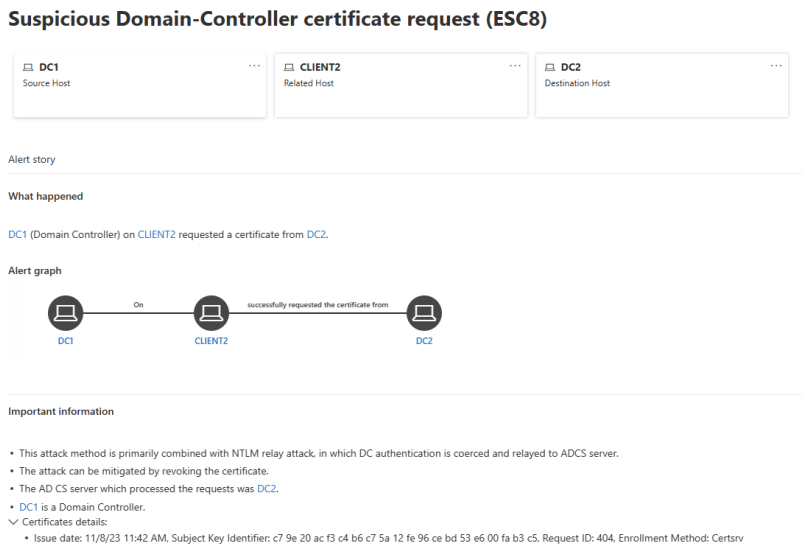
Watch this video for a full demo

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.



A few months ago we've also released some new detection for ADCS, if ADCS is prominent in your environment, highly recommend you turn this on. ADCS has the ability to 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.



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]

For more information, see:

- DefenderForIdentity Module
- Defender for Identity in the PowerShell Gallery

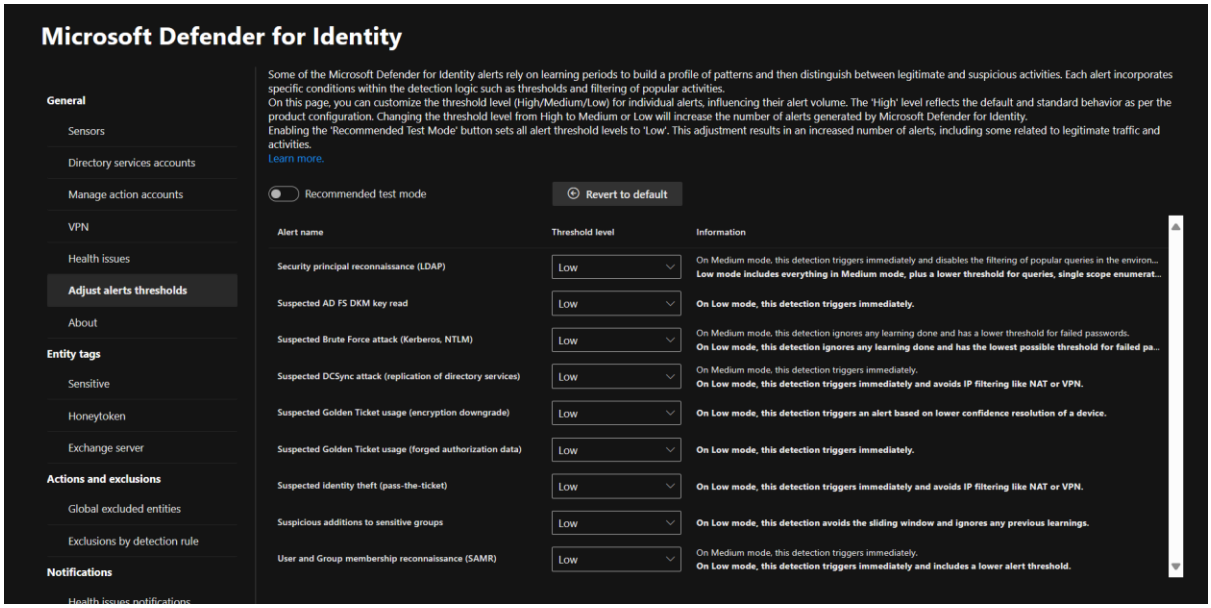
For example, the following command defines all settings for the domain, creates group policy objects, and links them.

Set-MDIConfiguration -Mode Domain -Configuration All

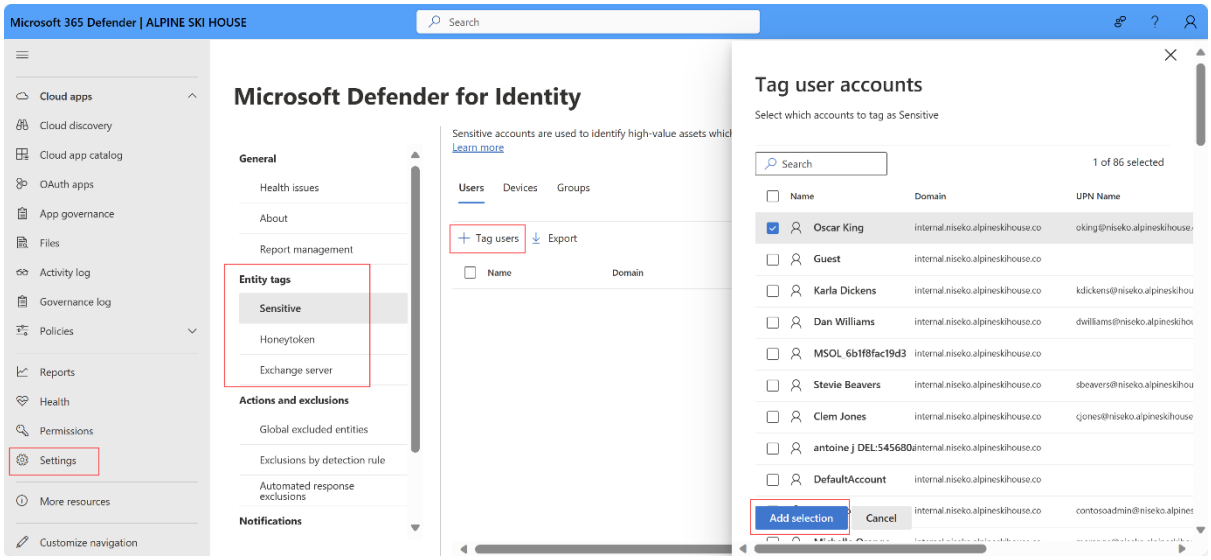
Once we've configured and run PS modules, there are few key features to go through

First, is 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

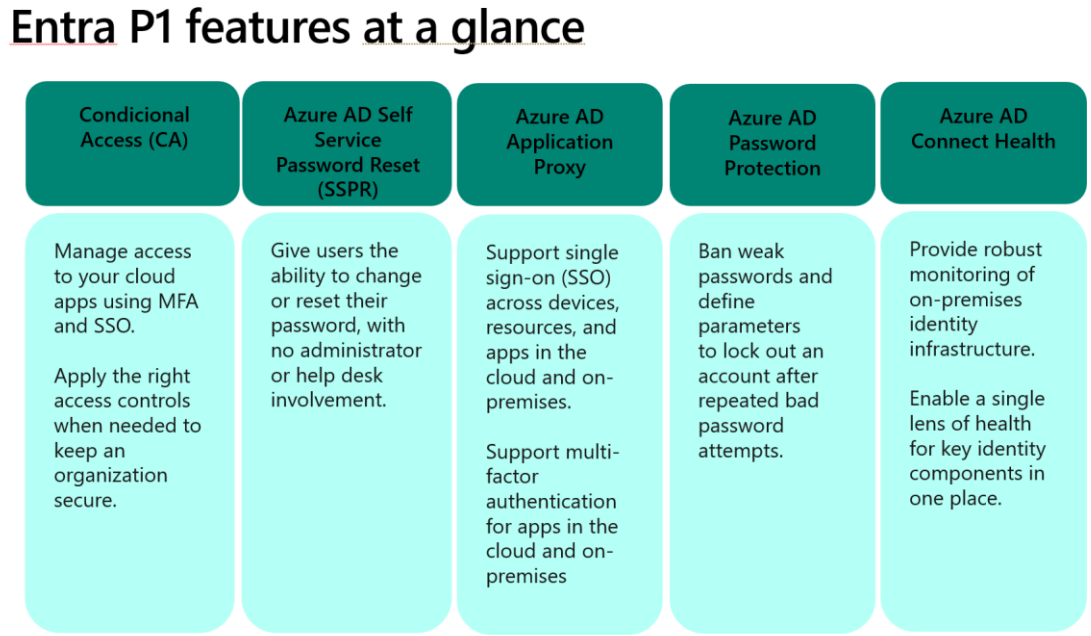


To get a sense that your sensitive accounts are truly set as a priority for alerts, you can tag them here to get priority on alerts. There is already a list of accounts that are automatically tag such as Domain Admins, Admins, Power Users..



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, lets 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 P2 features at a glance

Identity Protection		Identity Governance		
Identity Protection	Risk-based Conditional Access	Access Reviews	Privileged Identity Management	Entitlement Management
Detect risky sign-ins and risky user accounts. Provide easy Access to remediation actions such as password resets.	Use Conditional Access policies to mitigate risky sign-ins and risky users by either: - Blocking sign-ins - Requiring MFA challenges - Requiring password resets	Ensure the right users have the right access to the right resources by using advanced identity governance features to control group and roles memberships.	Enforce on-demand, just-in-time administrative access when needed.	Allow employees to request and have time-Limited Access across groups, apps and SPO sites. Allow users from Business Partners to do the same via an approval workflow.

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

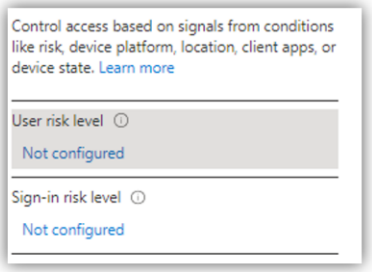
[What are risks in Microsoft Entra ID Protection - Microsoft Entra ID Protection | Microsoft Learn]

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.**



*Both user and sign-in risk conditional access policies require Premium P2 licenses for users

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

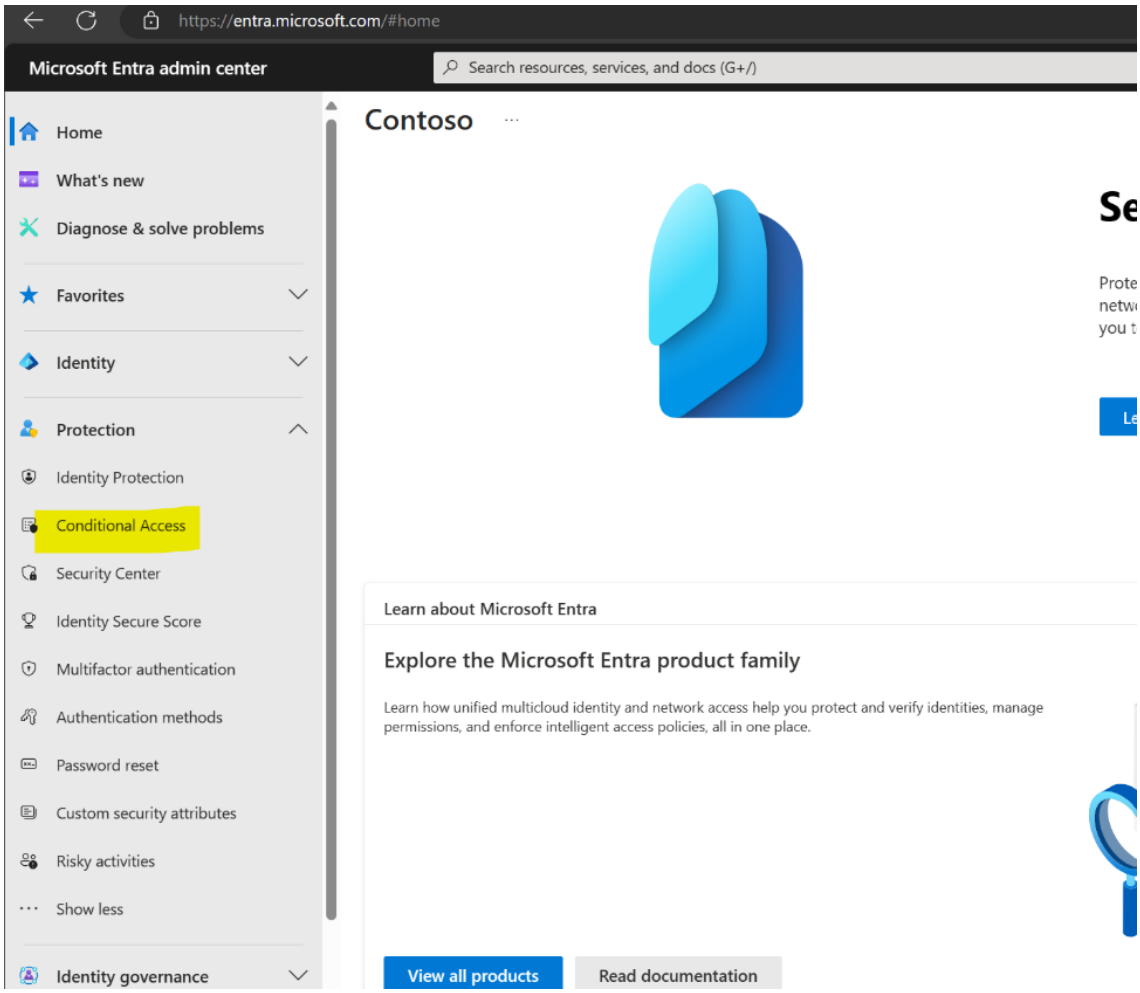
Risk detection	Detection type	Type
Atypical travel	Offline	Premium
Anomalous Token	Real-time or Offline	Premium
Suspicious browser	Offline	Premium
Unfamiliar sign-in properties	Real-time	Premium
Malicious IP address	Offline	Premium
Suspicious inbox manipulation rules	Offline	Premium
Password spray	Offline	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

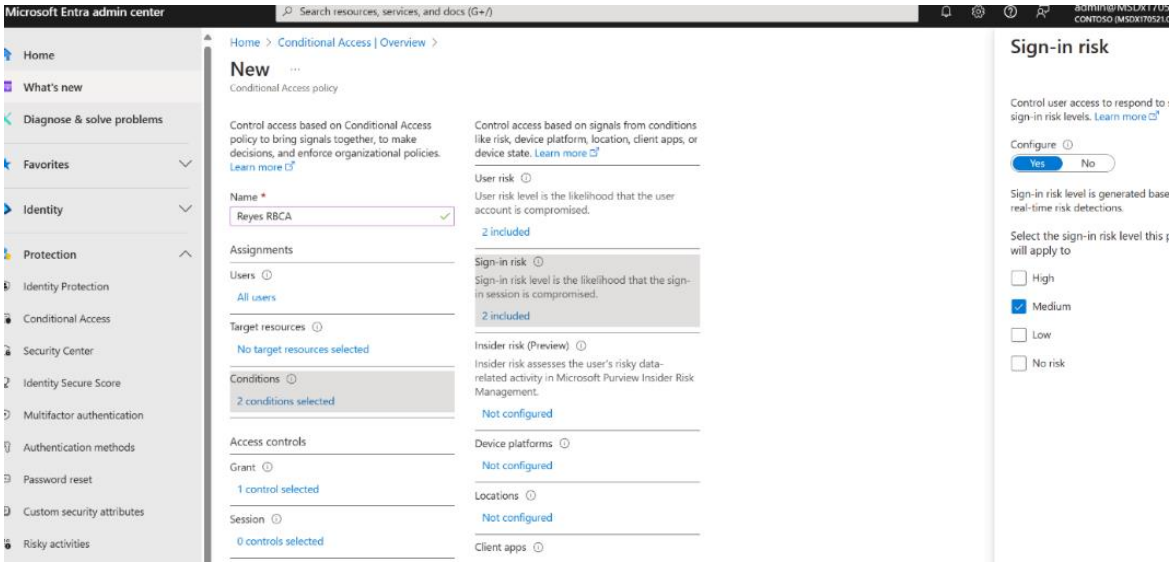
User risk detections

Expand table

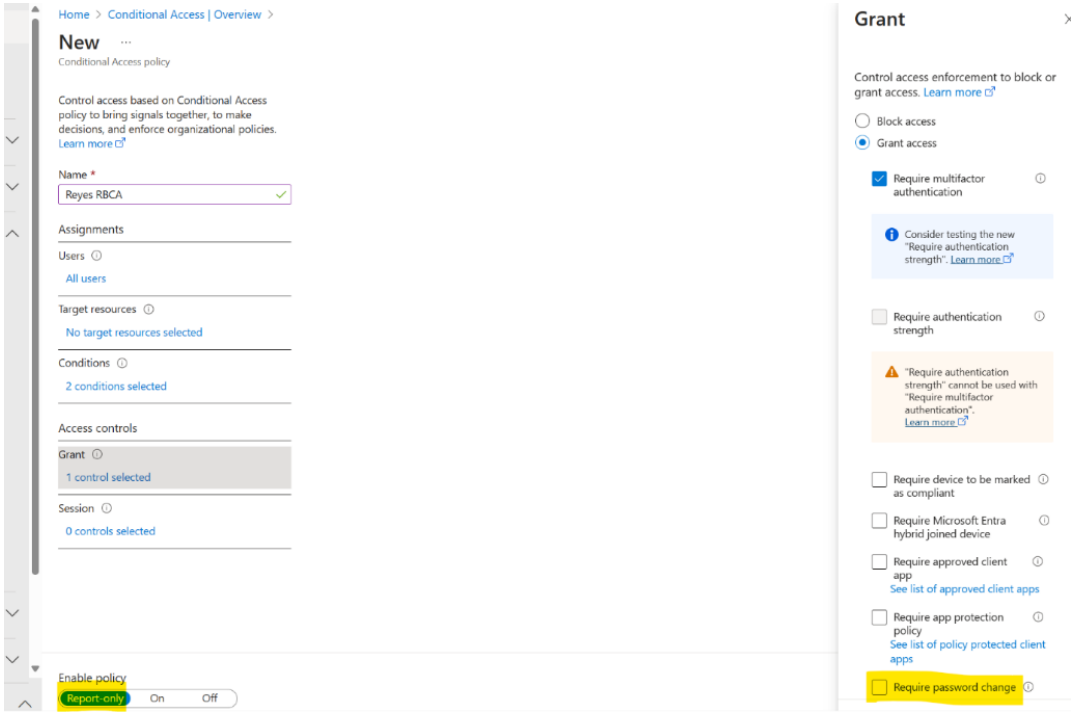
Risk detection	Detection type	Type
Possible attempt to access Primary Refresh Token (PRT)	Offline	Premium
Anomalous user activity	Offline	Premium
User reported suspicious activity	Offline	Premium
Suspicious API Traffic	Offline	Premium
Suspicious sending patterns	Offline	Premium
Additional risk detected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

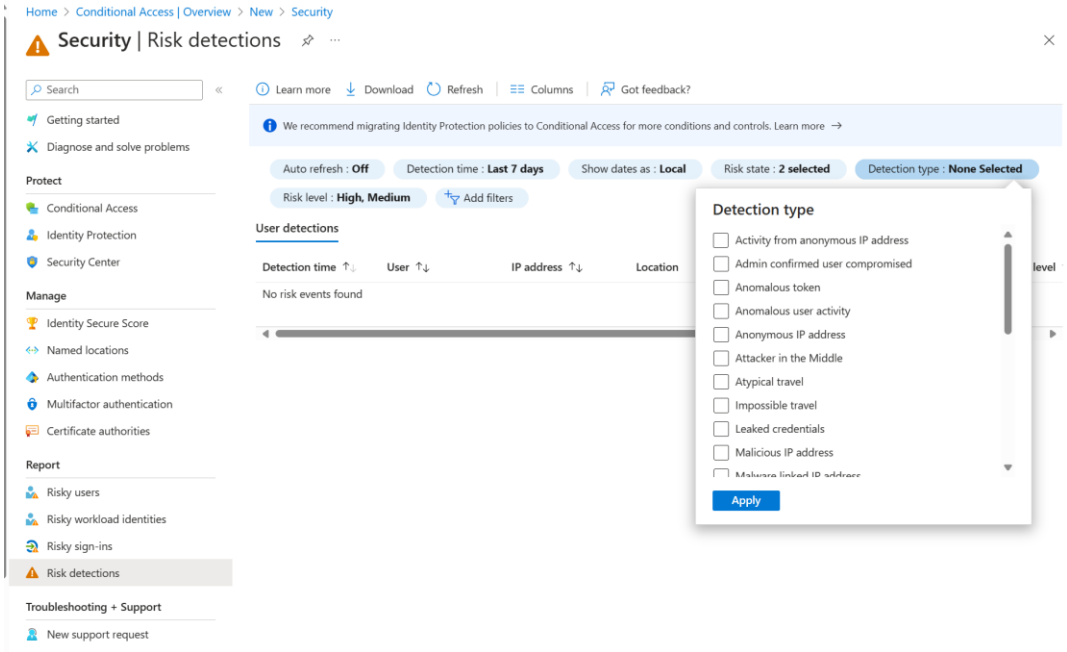
Enabling Risk Based Conditional Access can be found in entra.microsoft.com





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





Understanding Alerts and using Incidents to Triage

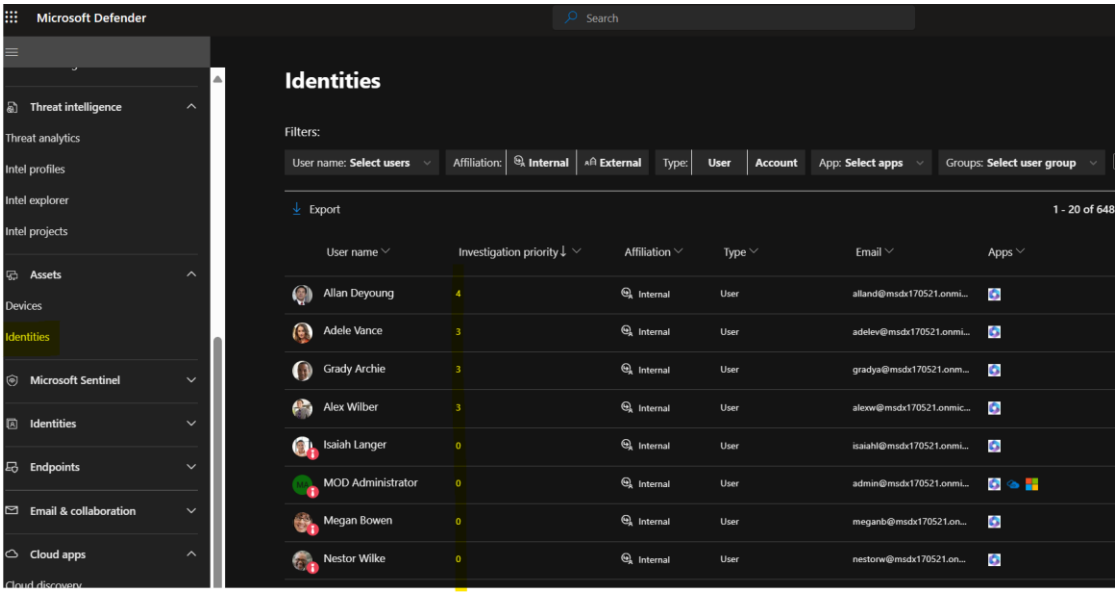
[Security alerts - Microsoft Defender for Identity | Microsoft Learn]

In Microsoft Defender XDR:

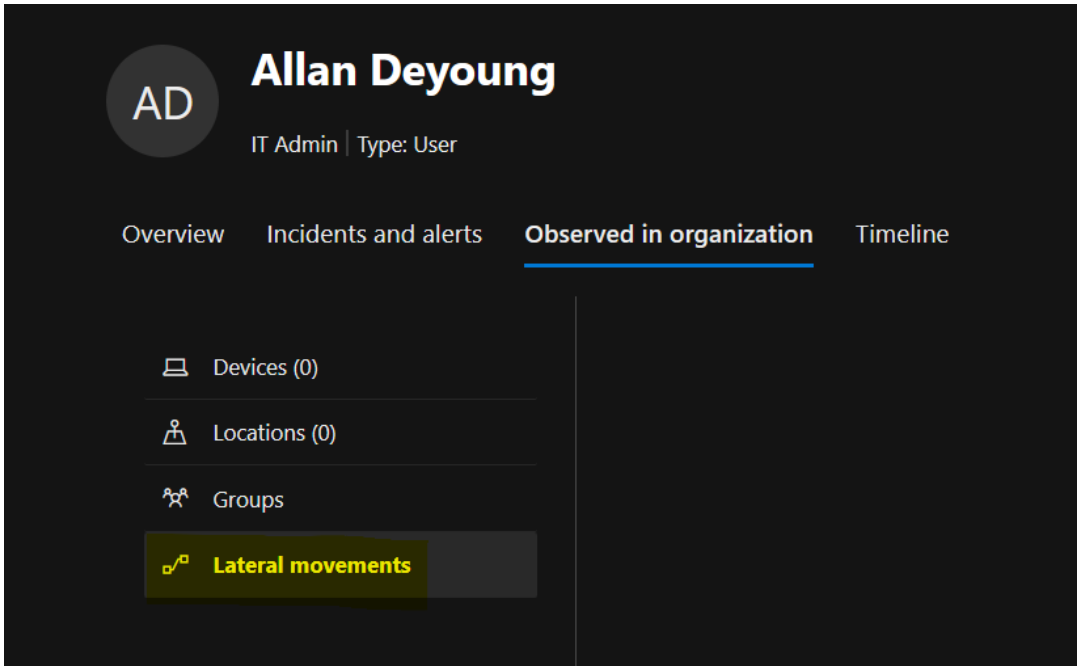
1. Check the **Users at risk** widget on the **Home** page or the **Entra ID users at risk** on the **Identities > Dashboard** page.

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.

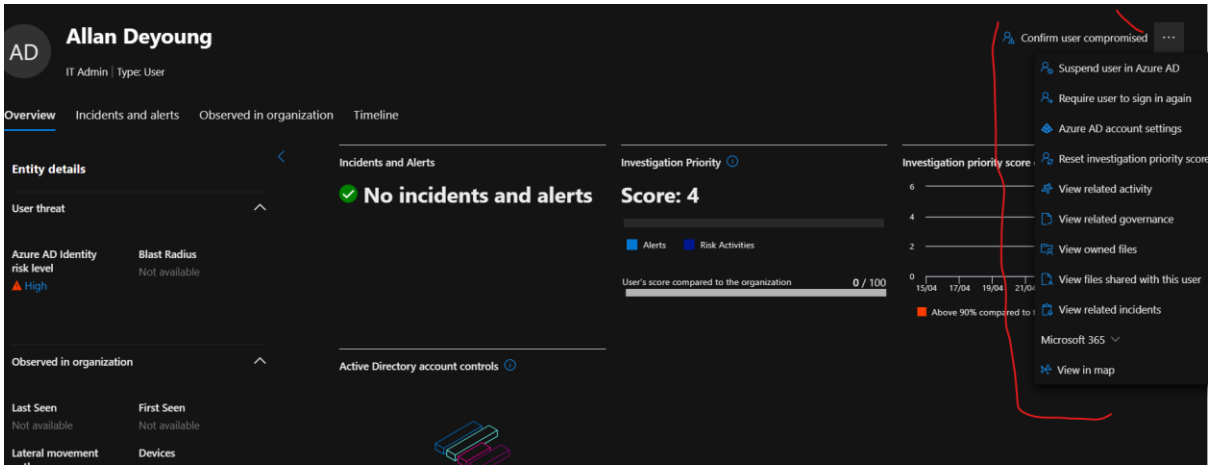


As an example, if Allan's investigation priority score is high and you get an alert, you can dive deeper in Allan's User's Page in Assets / Identities and look at a possible LMP

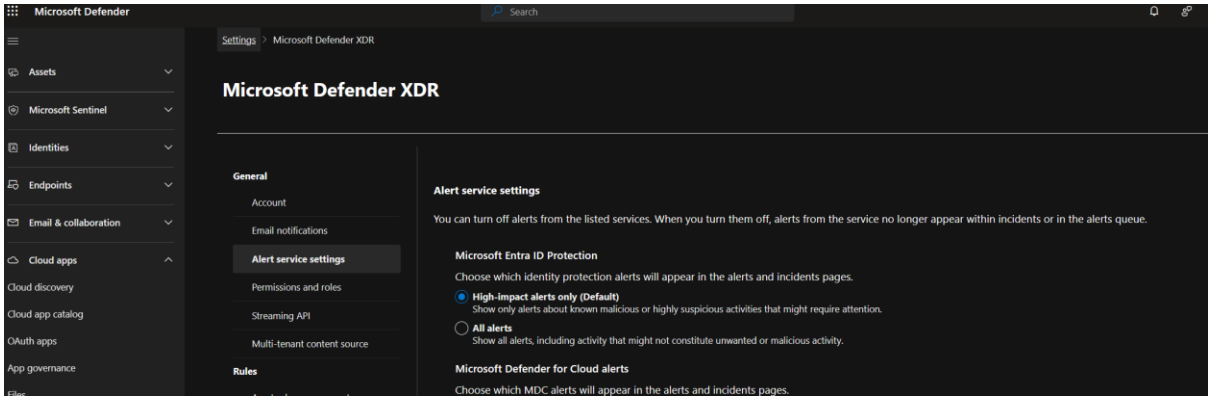


We've created a possible Lateral Movement story that could be a high confidence chance that an identity has been compromised

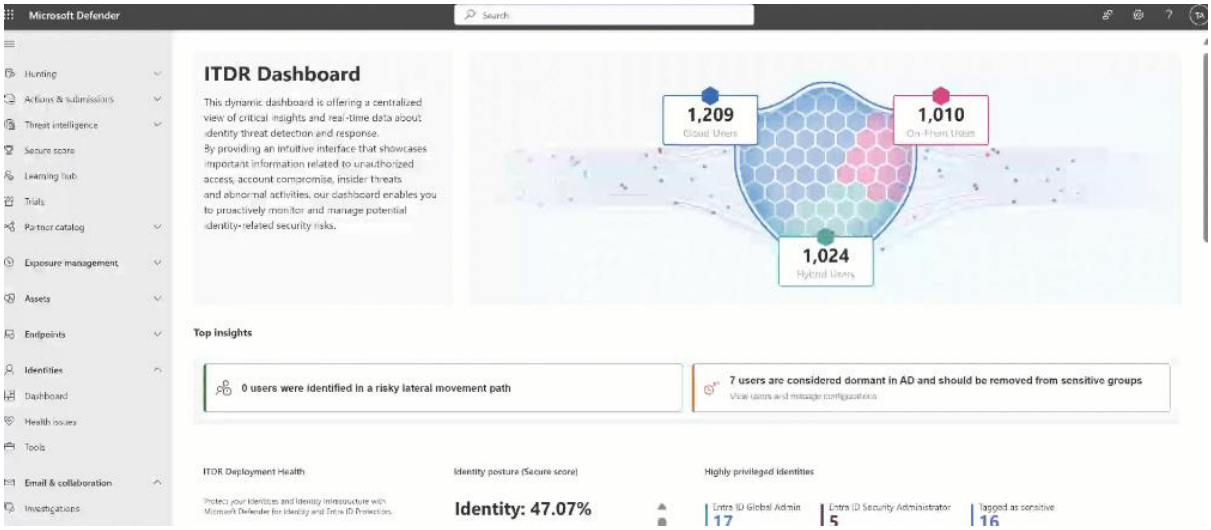
If you have identified Allan has been compromised, we have a bunch of native response actions we can take. This is when on-prem and cloud has that integration where if you click on compromised this can increase Allan's score in Entra and in turn puts his account at high risk which will force him to reset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



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



New 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]

- 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)

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

Key Watch outs

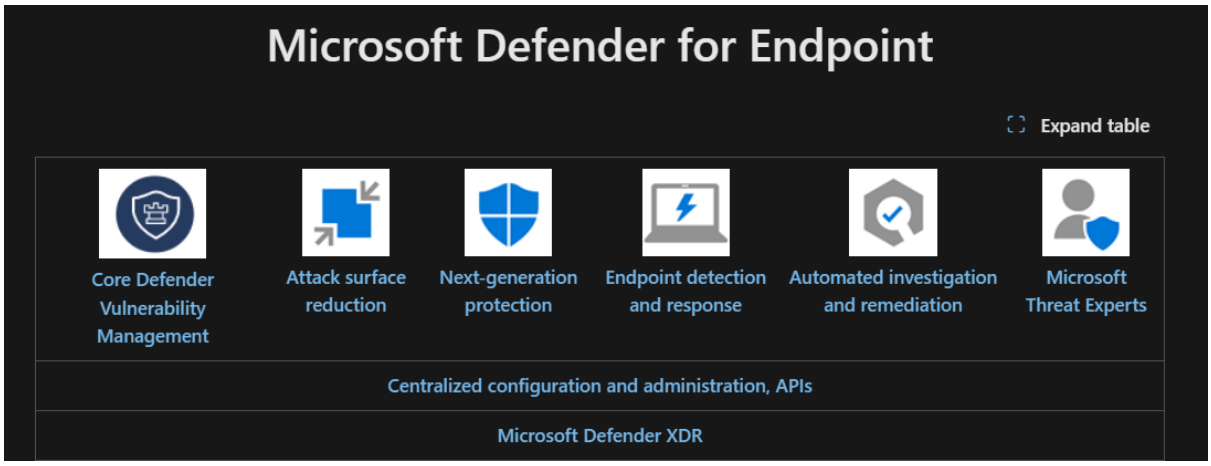
- Intune is our recommended device management tool, SCCM is not going anywhere but managing policies through SCCM does take a little bit more work. Not all policies are in SCCM, in fact most advanced policies still need to be deployed via GPO
- We recommend at least 30 days to put your ASR in audit mode 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 cause 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.

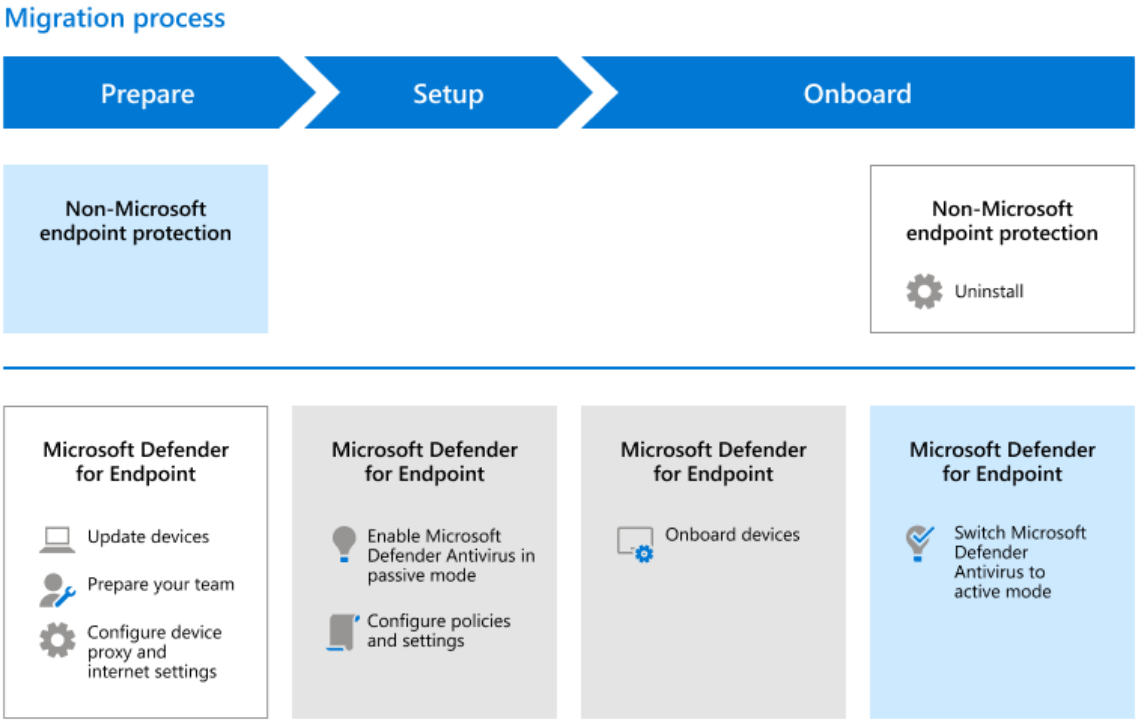
When we talk about MDE P2 features, we talk about these pillars below. Our bread and butter, they're the finest features known to any endpoint protection and I've managed and deployed plenty of endpoint protection over the course of my career Security roles and I'm not even in sales or marketing, just 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



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



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

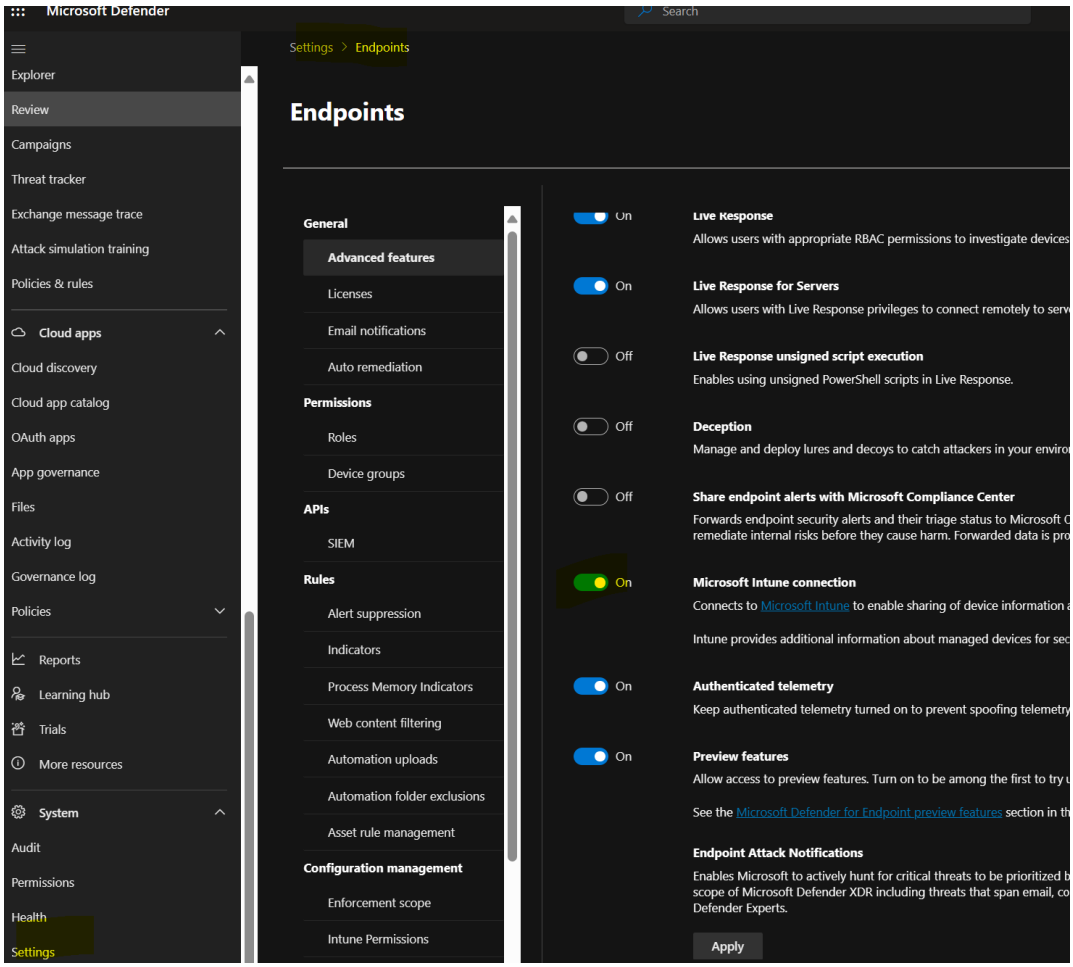
Onboarding Mac OS Microsoft Defender for Endpoint on Mac - Microsoft Defender for Endpoint | Microsoft Learn

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

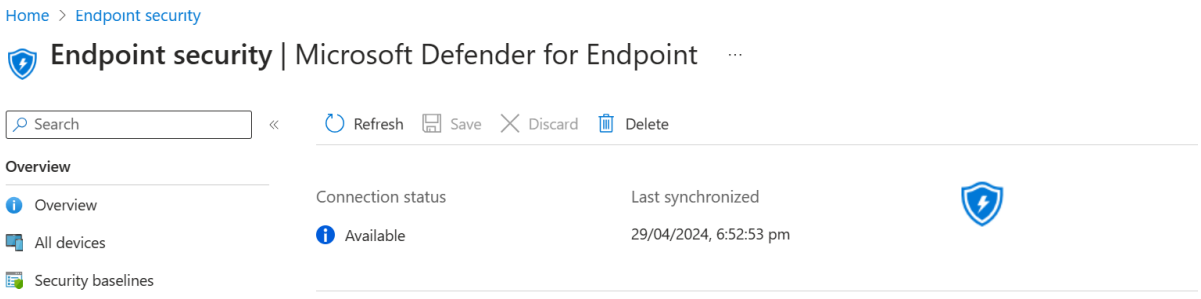
Ok so lets dive a little deeper on onboarding and configuring MDE with Intune, as this is the our recommendation approach and also the most common approach most of my customers are taking. Some even using this to progress their device management migration ahead of schedule from SCCM to Intune

[Configure Microsoft Defender for Endpoint in Microsoft Intune | Microsoft Learn]

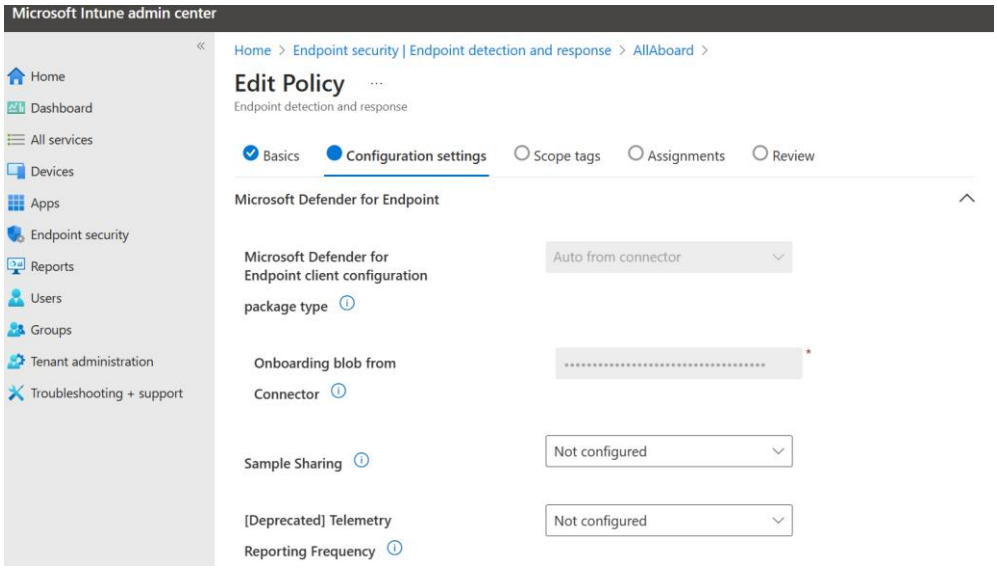
Step 1. Enable to cross over service between MDE to Intune.

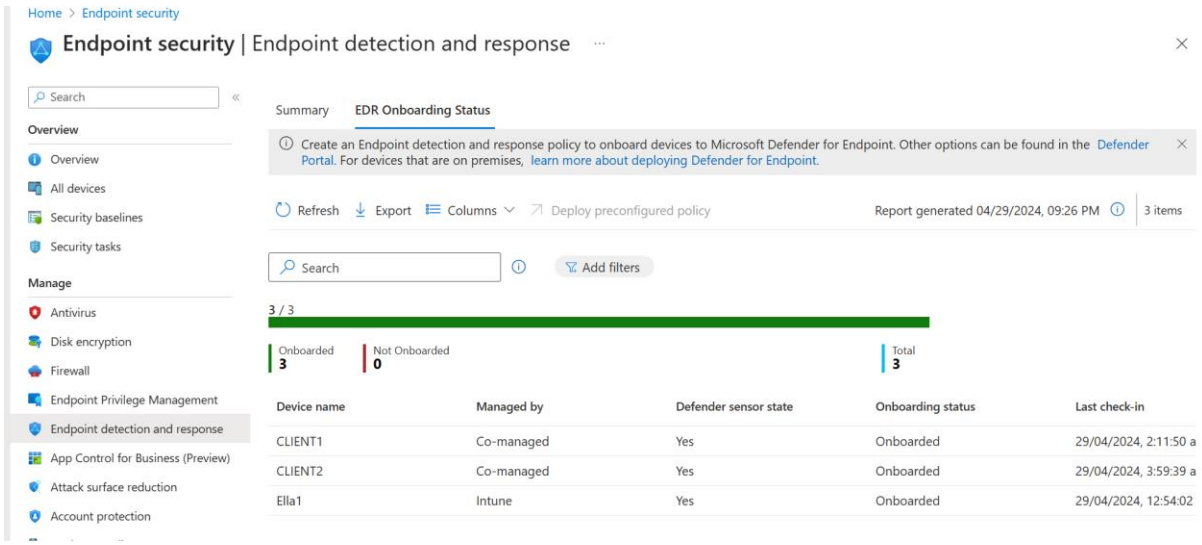


Confirm the connection has been established in Intune. The sync happens once everyday



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

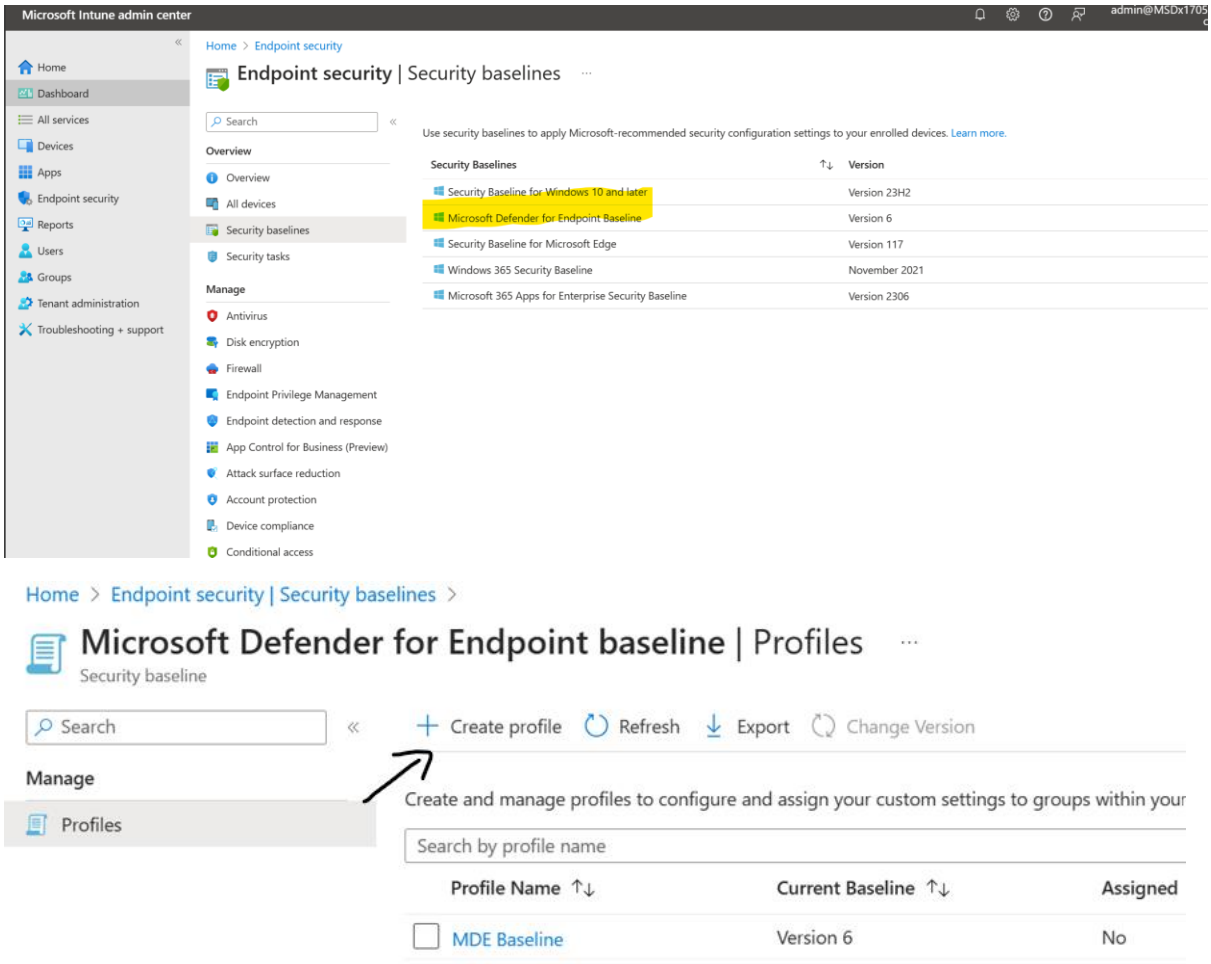




Once you've established the pilot devices you're testing is done, we can now start creating our policies. Because you're coming from a 3rd party protection you may have some idea on what settings you want to re-create in MDE.

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. So test, test and test. Use a test group to test this against

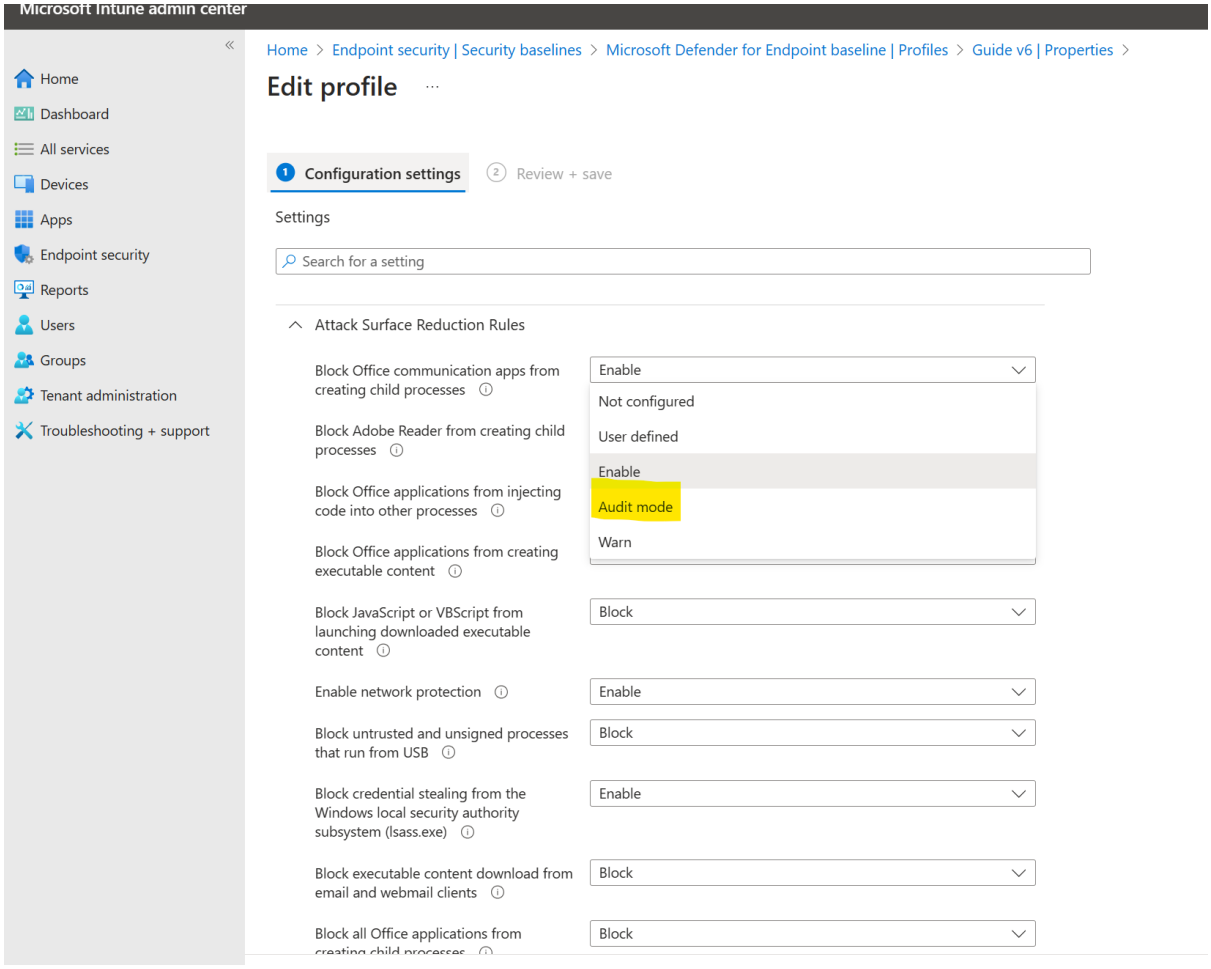
How to create a profile and using the MDE Baseline



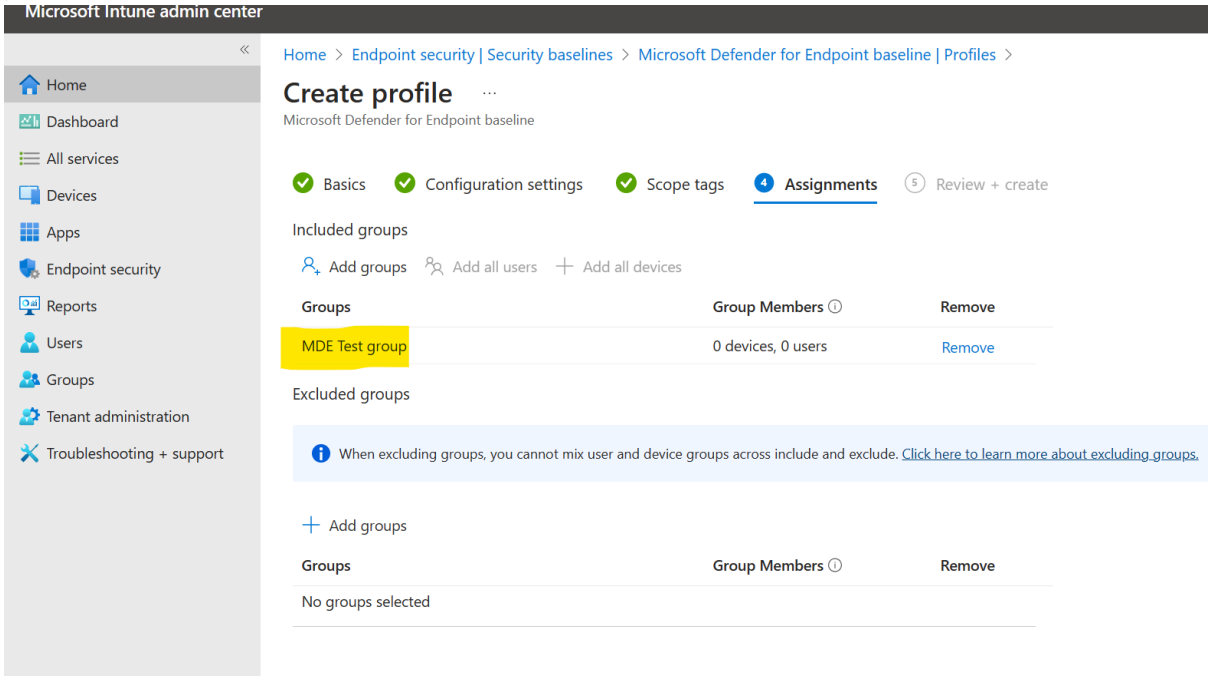
You will see all the settings that has been recommended, enabled. When you're testing, it's a good idea to **put the settings in audit mode**, this will give you a chance to see what will be affected or has been blocked. This is a stage where a lot of fine tuning happens from creating exclusions, talking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

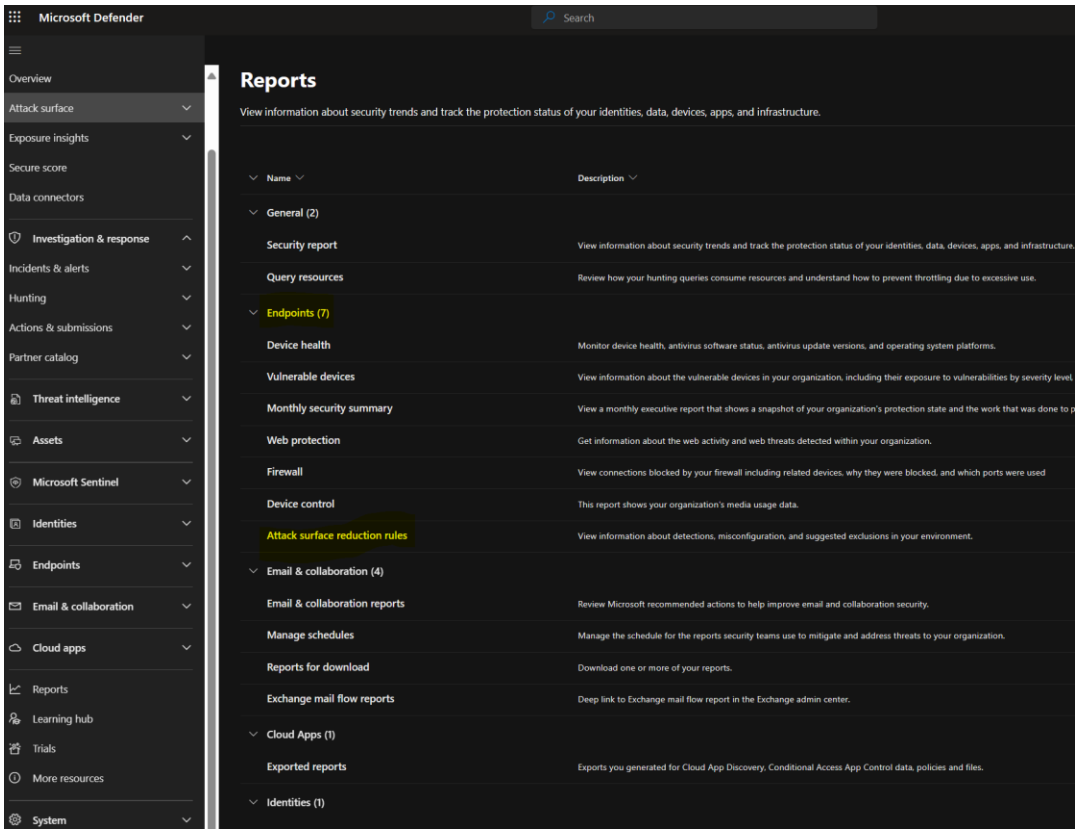
Important to note, that the baseline is not recommended for VM or VDI



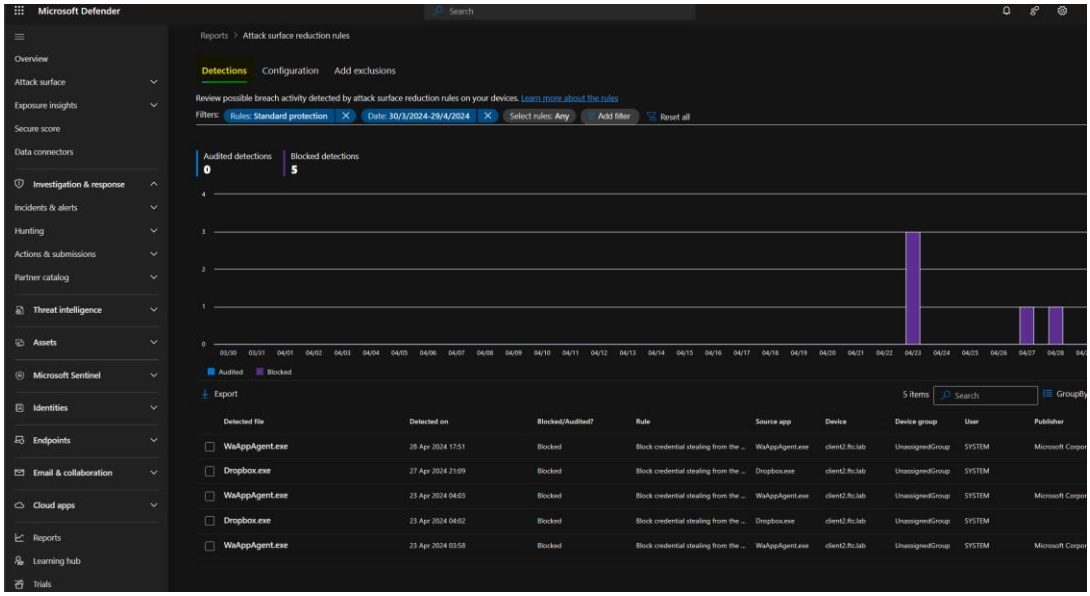
At first, it's a good idea to use a test group (preferably your IT), this is your walk phase, then add a little more to your pilot. Increase the numbers over time across your business. Chose your pilot users wisely so you get a good sense that everything is being tested and being feedback to you



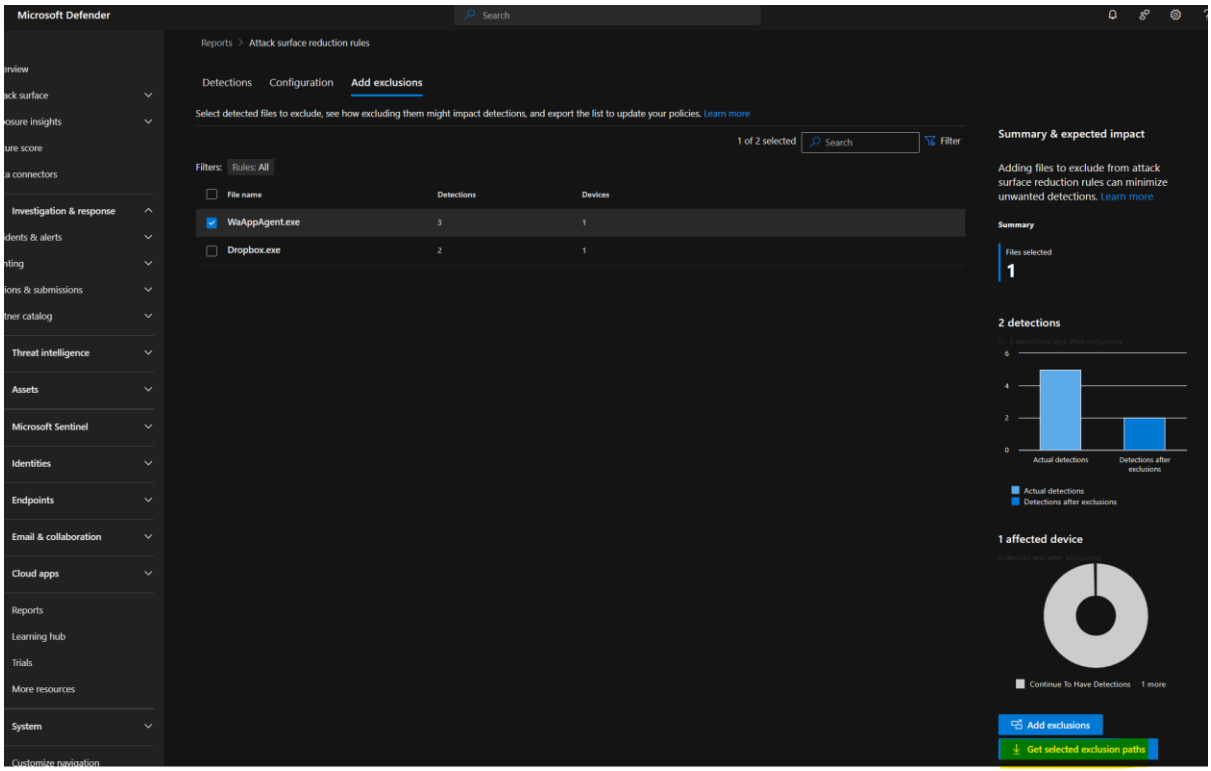
Reporting. When you're in the early stages you will be visiting the reports quite a bit. As an example if we look at the ASR rules. This is to see what is being detected and being blocked. Some may be relevant to your business and you will need to create exclusions.



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



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

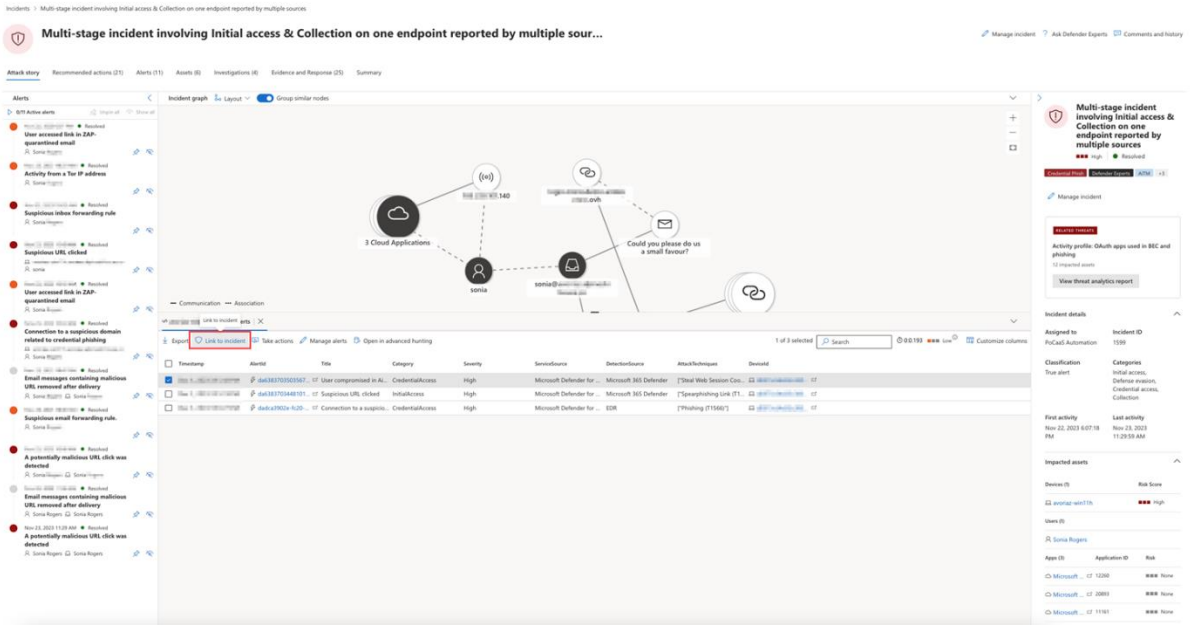


Let's take a look at 4 key feature of MDE

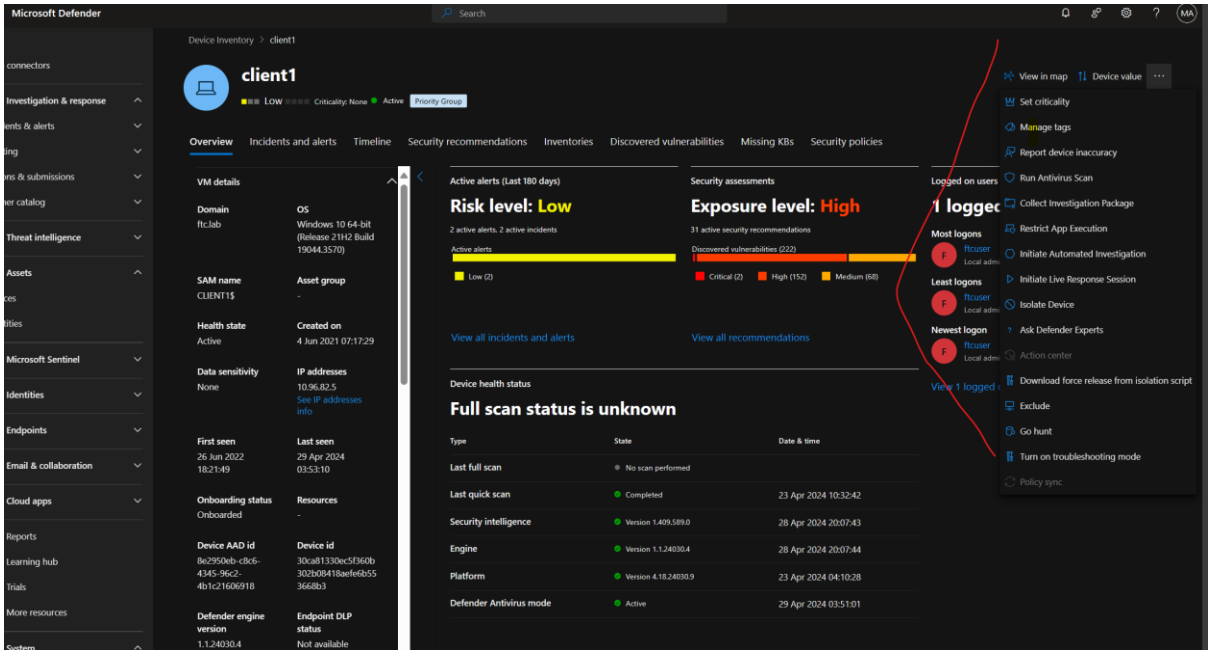
Attack Surface Reduction - Understand and use attack surface reduction - Microsoft Defender for Endpoint | Microsoft Learn

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 alerts that was correlated to this story. We can collect 6 months of data if we want to go that far

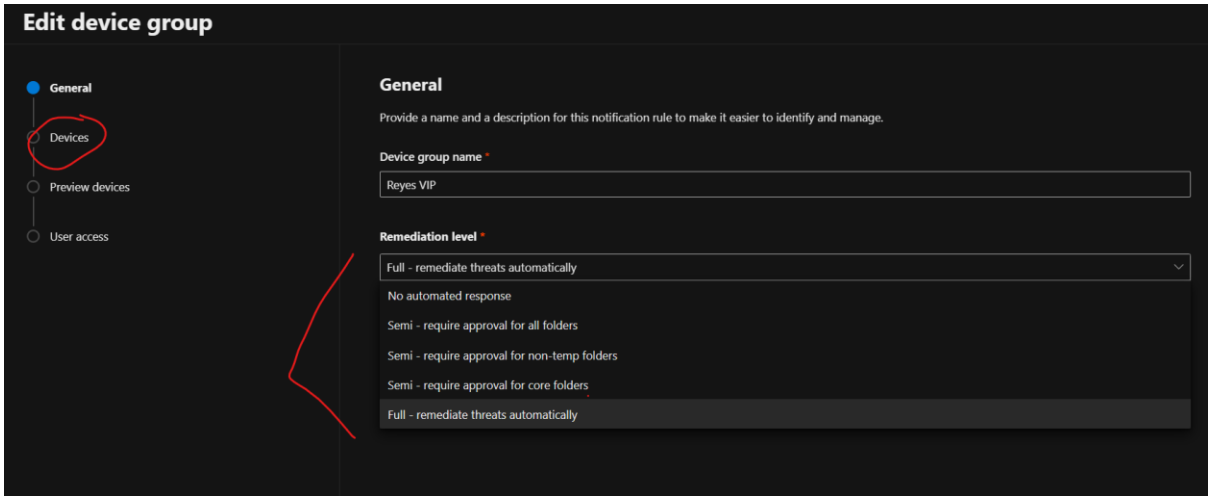


We also have a bunch of built-in native responses from scanning to isolating a device to running a Live Response which is a remote shell to a device and you can run a bunch of commands investigation



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

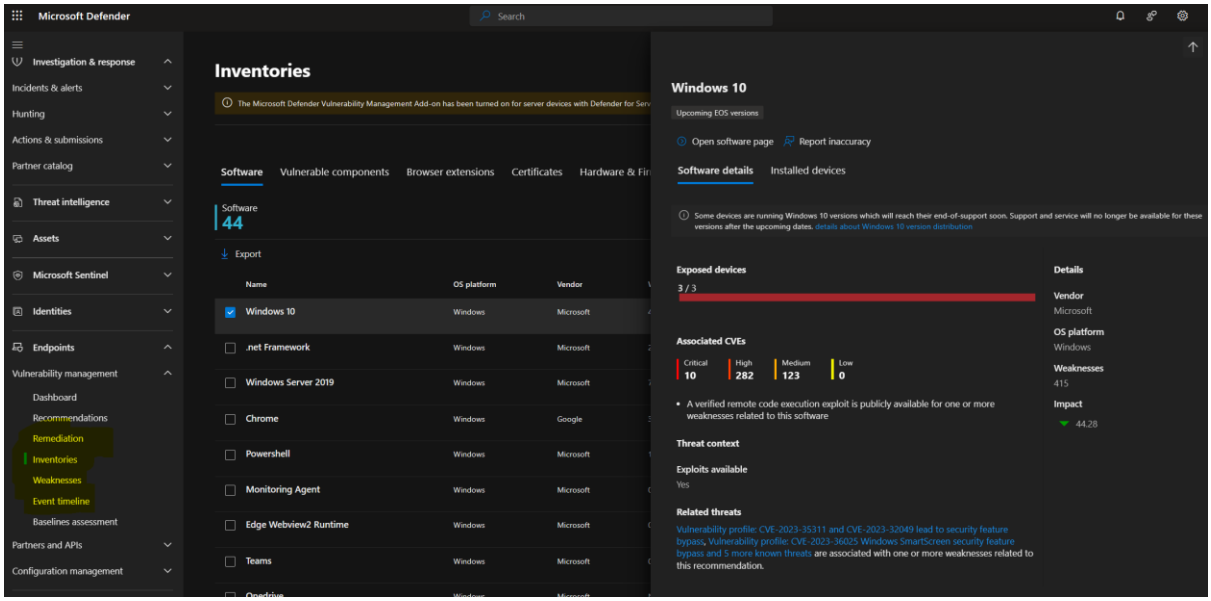
As you may have guessed, this feature essentially remediates alerts/Incidents automatically when an alert is triggered. You can also run AIR manually from the native respond buttons. Our recommendation is to use the **Full – remediation** which gives us a higher confidence to resolve malware and free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



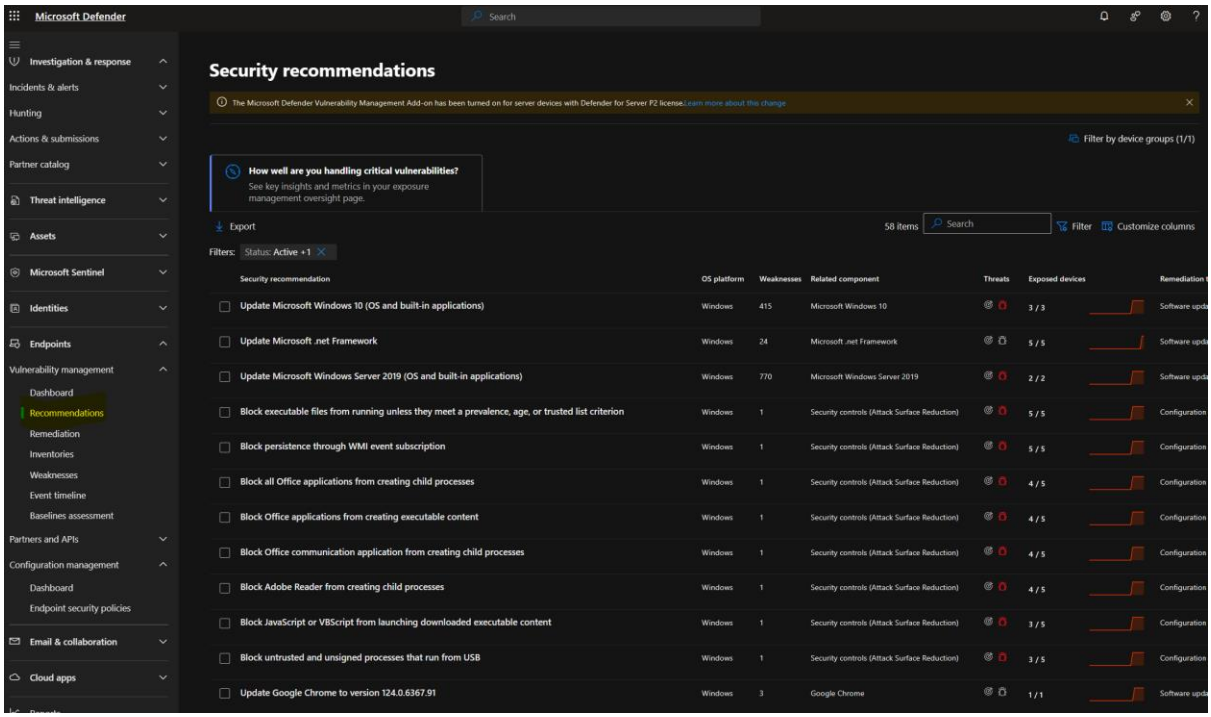
Microsoft Defender Vulnerability Management

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 mssense.exe 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.



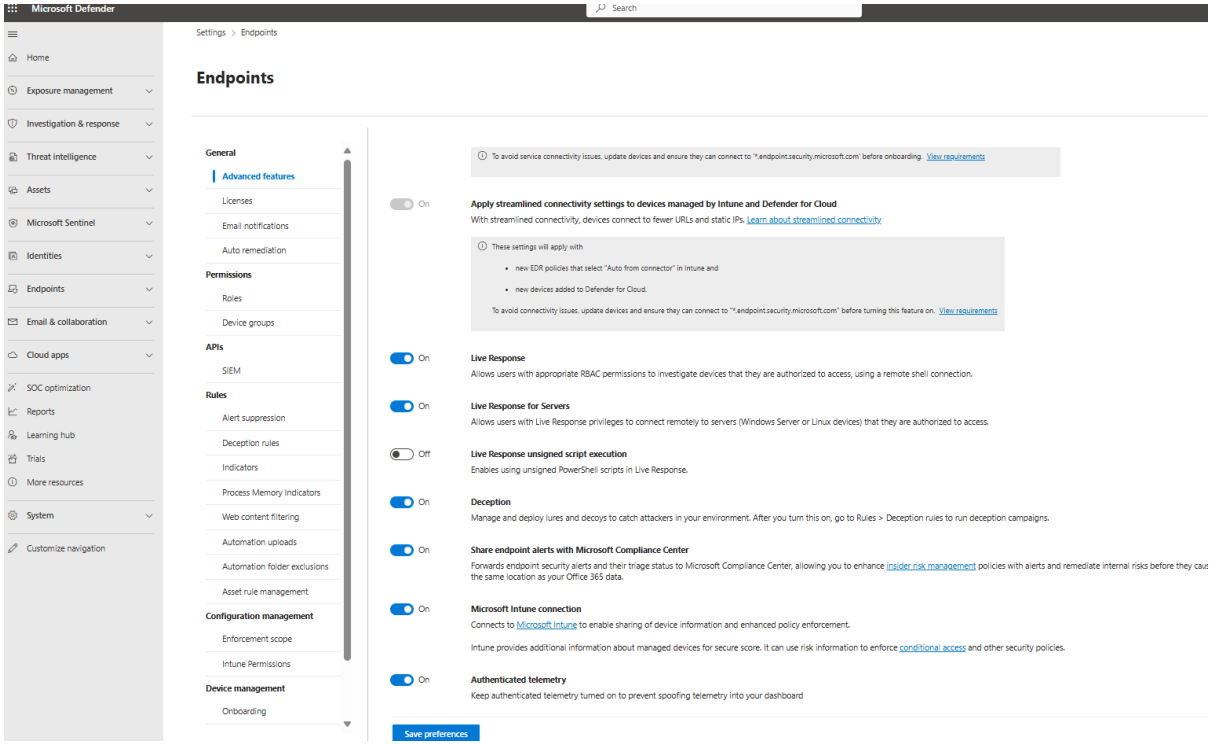
Once you've done your last group for your pilot phase, you can assess that all the recommendation has been actioned or at least be aware there's still items being recommended. You can go to Secure Score.



Once the onboarded is complete. It's important to assess all the Advanced Features under MDE – Settings. We have some default settings that is 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

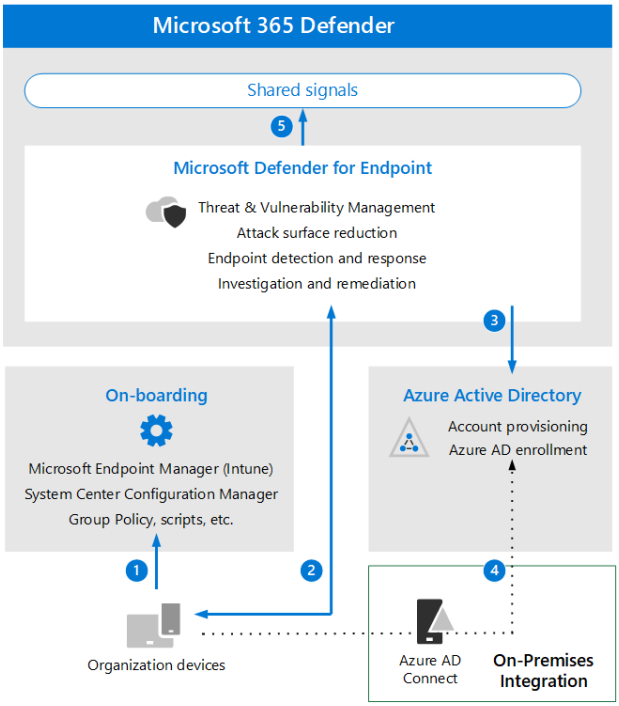
Demonstrations

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



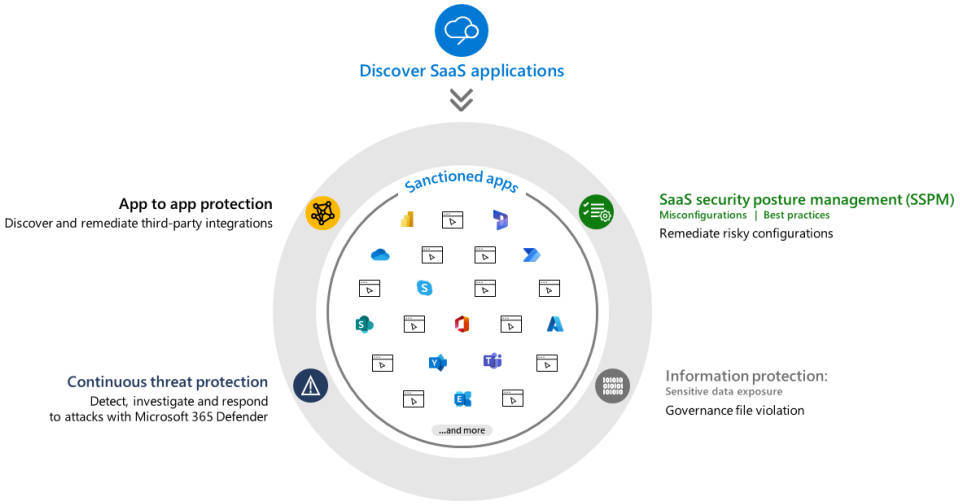
Phase 4. Microsoft Defender for Cloud Apps (MDA)

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 5 main components that make up MDA, which we will use to adopt and deploy MDA



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

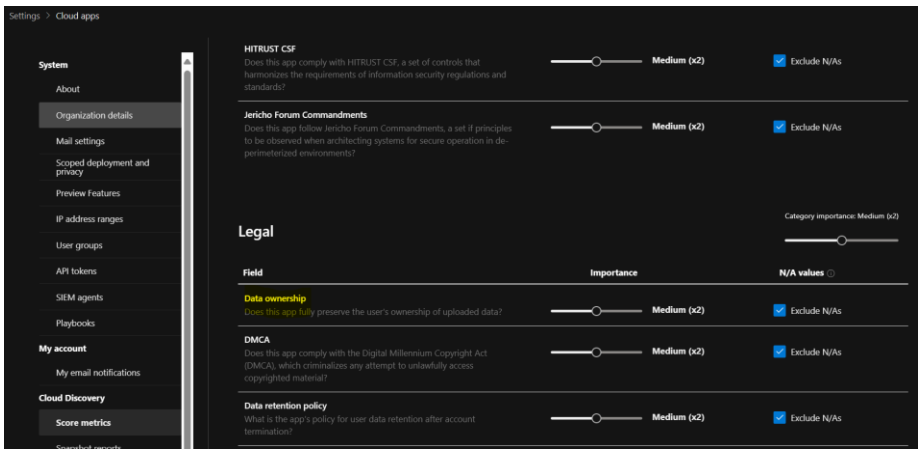
1. Discover and assess cloud apps
2. Apply cloud governance policies
3. Limit exposure of shared data and enforce collaboration policies
4. Discover, classify, label, and protect regulated and sensitive data stored in the cloud
5. Enforce DLP and compliance policies for data stored in the cloud
6. Block and protect download of sensitive data to unmanaged or risky devices
7. Secure collaboration with external users by enforcing real-time session controls
8. Detect cloud threats, compromised accounts, malicious insiders, and ransomware
9. Use the audit trail of activities for forensic investigations
10. Secure IaaS services and custom apps

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

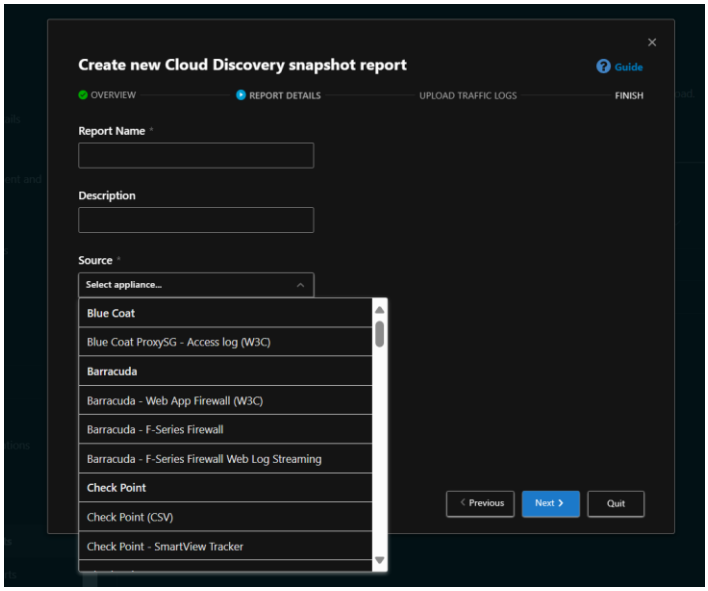
Cloud Discovery features

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.

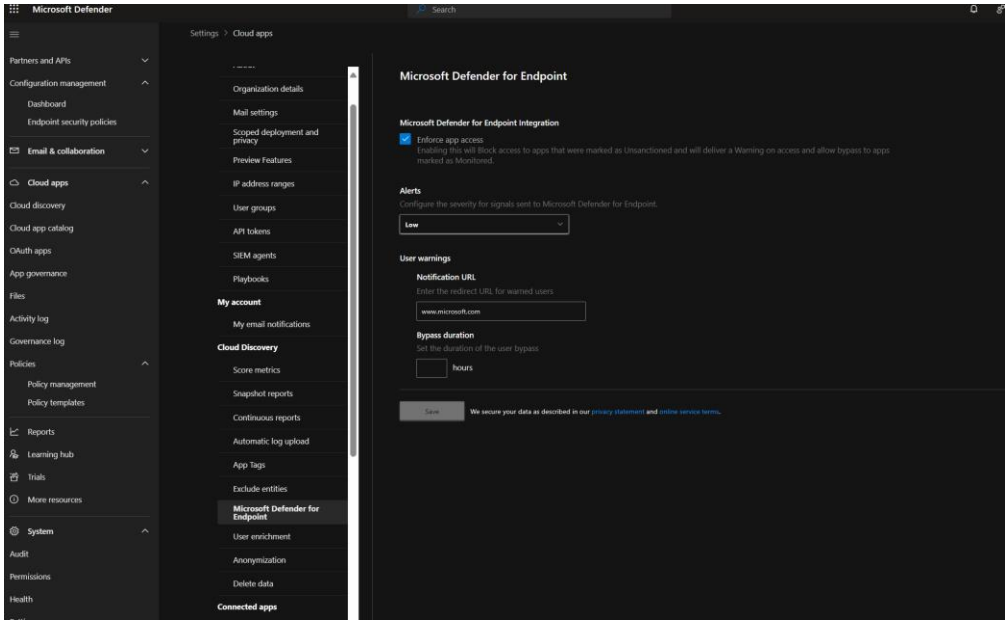
One very cool metric is Data Ownership which I don't see any other CASBs (at least me). This metric allows you to unsanctioned any apps that basically starts to own your data if you upload data into their cloud service. Which is very important to most, if not all organisation as they want to own their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



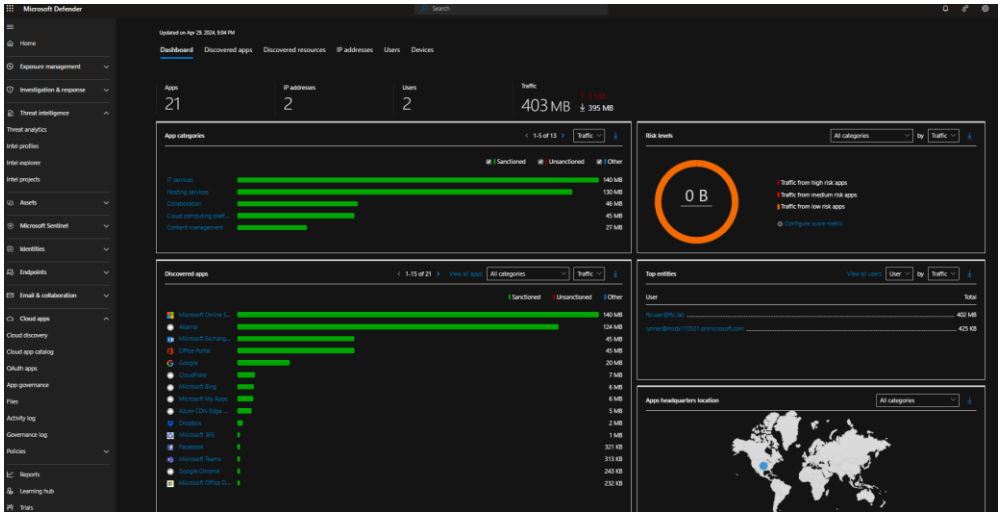
Snapshot reports is simply that, it's a sample report based on what source you may be thinking of using to digest the data from and the point of this is to give you what results it can digest. Again, our recommended log collector is MDE which is our native built-in agent which doesn't require much work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



So with your devices already onboarded to MDE, it's a simple toggle. [Integrate Microsoft Defender for Endpoint - Microsoft Defender for Cloud Apps | Microsoft Learn]

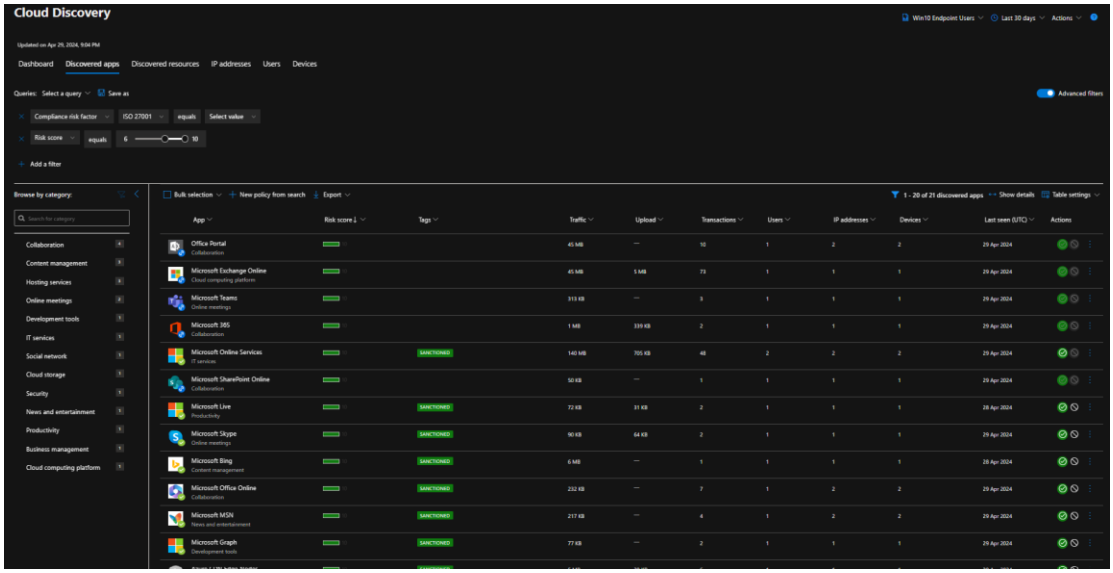


Once you've enabled MDE, the data being absorb will slowly start to be interpreted in MDA and Cloud Discovery will start to fill up. MDA absorbs the network traffic, so as soon as users starts to access websites, you'll absorb all that traffic. You'll be able to see all sorts of information from apps,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



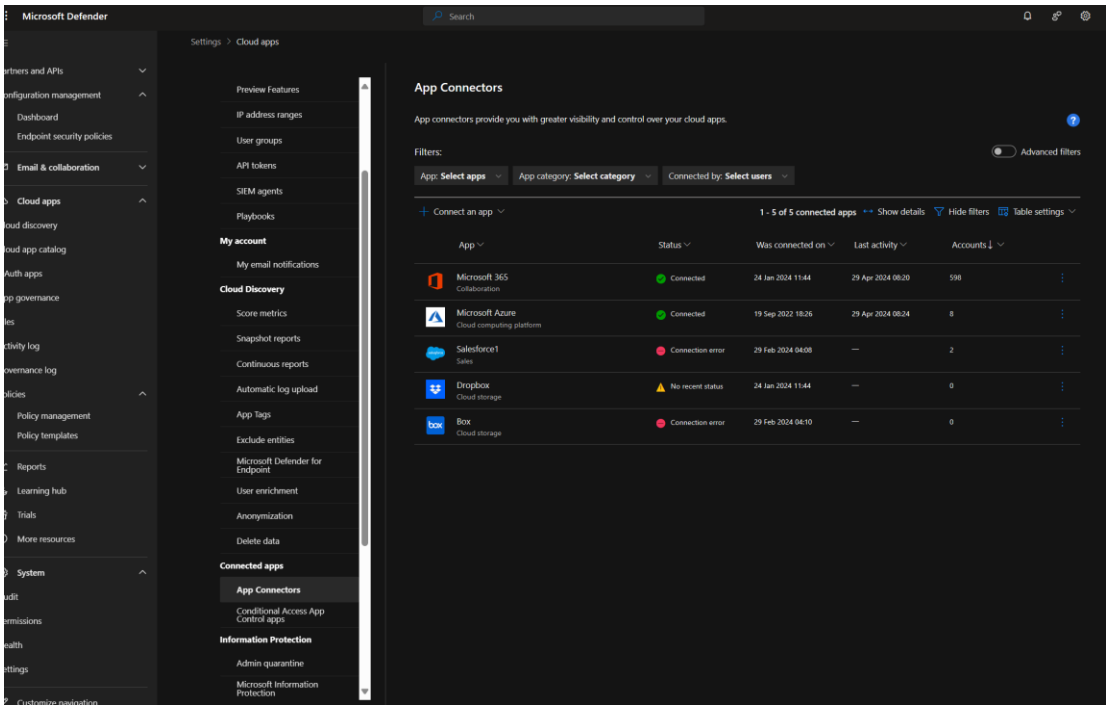
One of the first key steps you can take when rolling out MDA is to view your Saas landscape. This is sometimes a scary moment when discovering you have 1000s of apps that are unknown to anyone, but they're installed on user's devices.
You can filter your search based on acceptable score metric, what 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 un-sanctioning it or creating a Conditional Access for it.



Another the key feature in MDA is Connected Apps. We recommend connecting at minimum your M365 and Azure to get a deeper visibility on those 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]

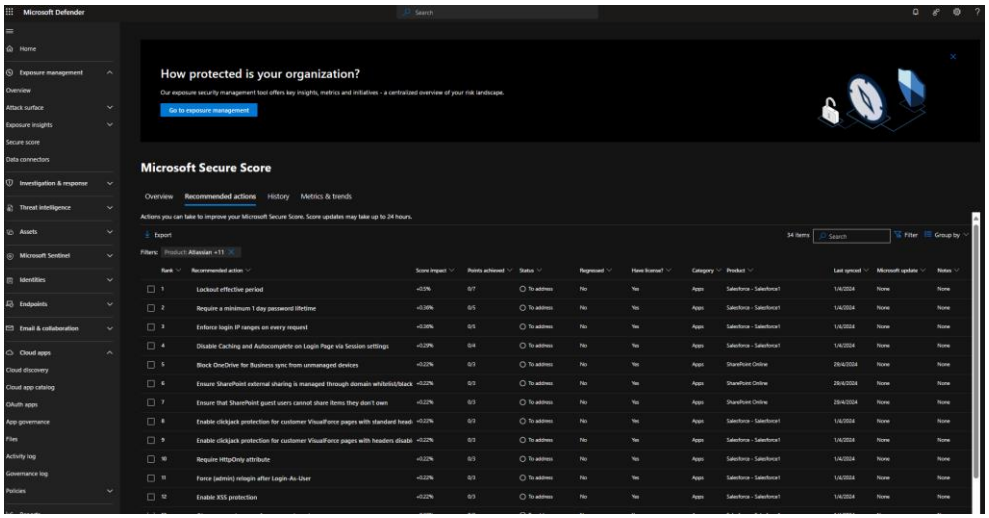


SaaS Security Posture Management

Using this feature as a proactive security investigation.

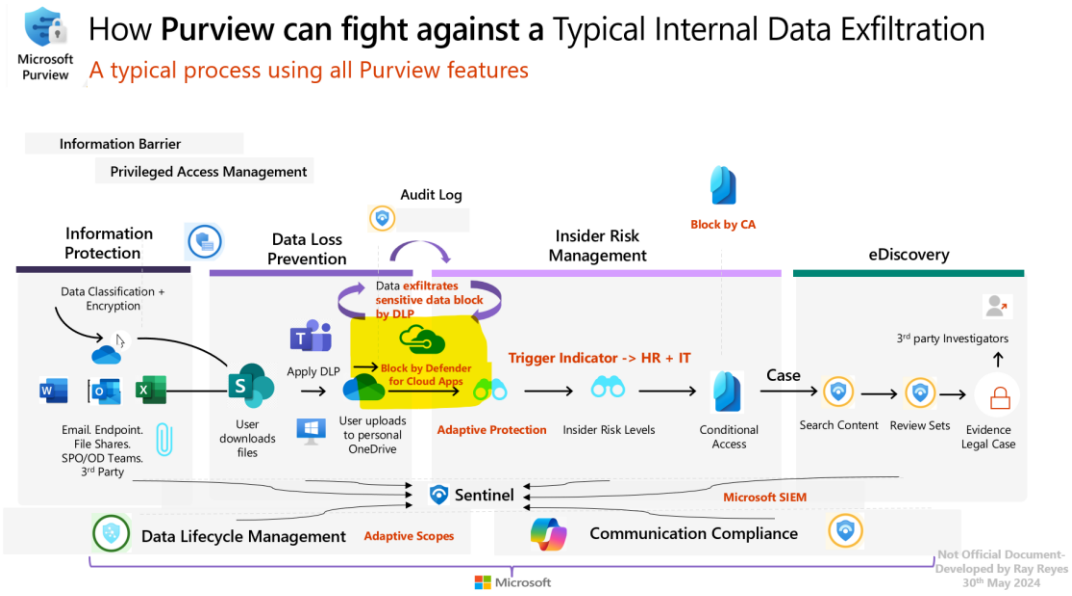
By working closely with 3rd party apps and building integration with our platform and theirs, we need to be able to detect and respond to mis-configuration. SSPM allows us to recommend at a deepest level when 3rd party apps are not configured correctly.

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



Information Protection

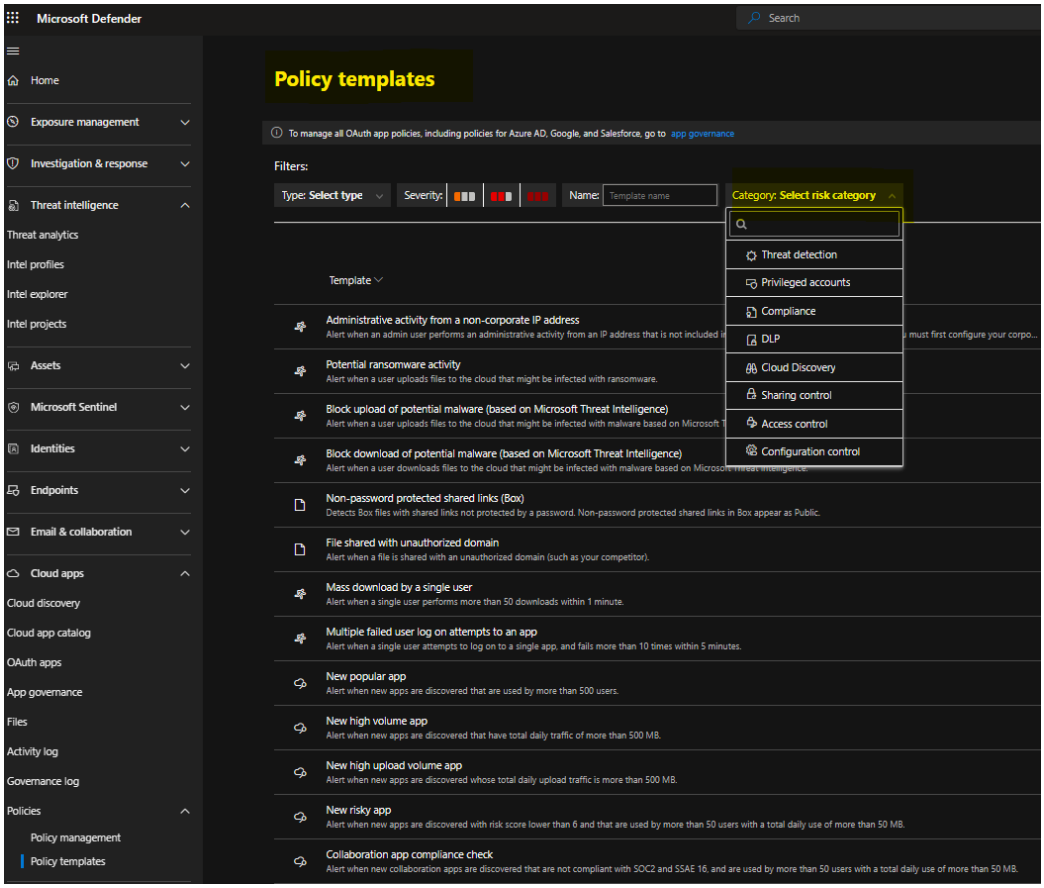
I love this section of crossover platforms. As you can see from this inforgraphic, MDA can play a huge part on Data Extraction



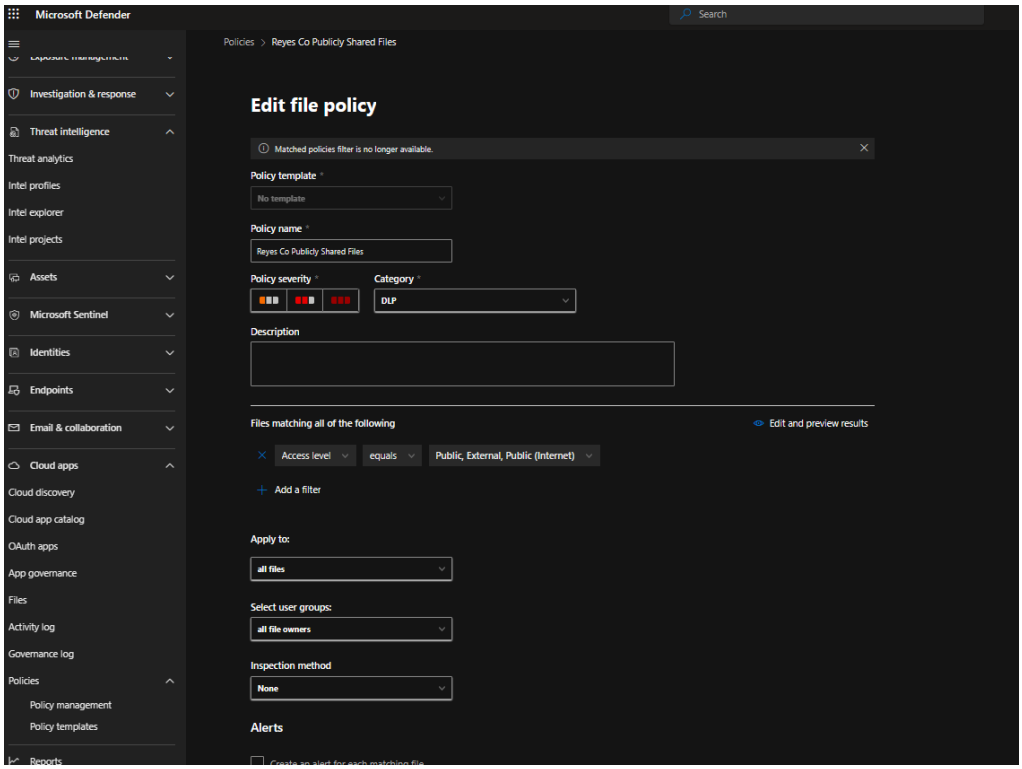
We have a bunch of Information Protection policies we can apply in MDA
[Information protection policies - Microsoft Defender for Cloud Apps | Microsoft Learn]

To learn more about how to deploy DLP and all the Purview stack – [here's another article]

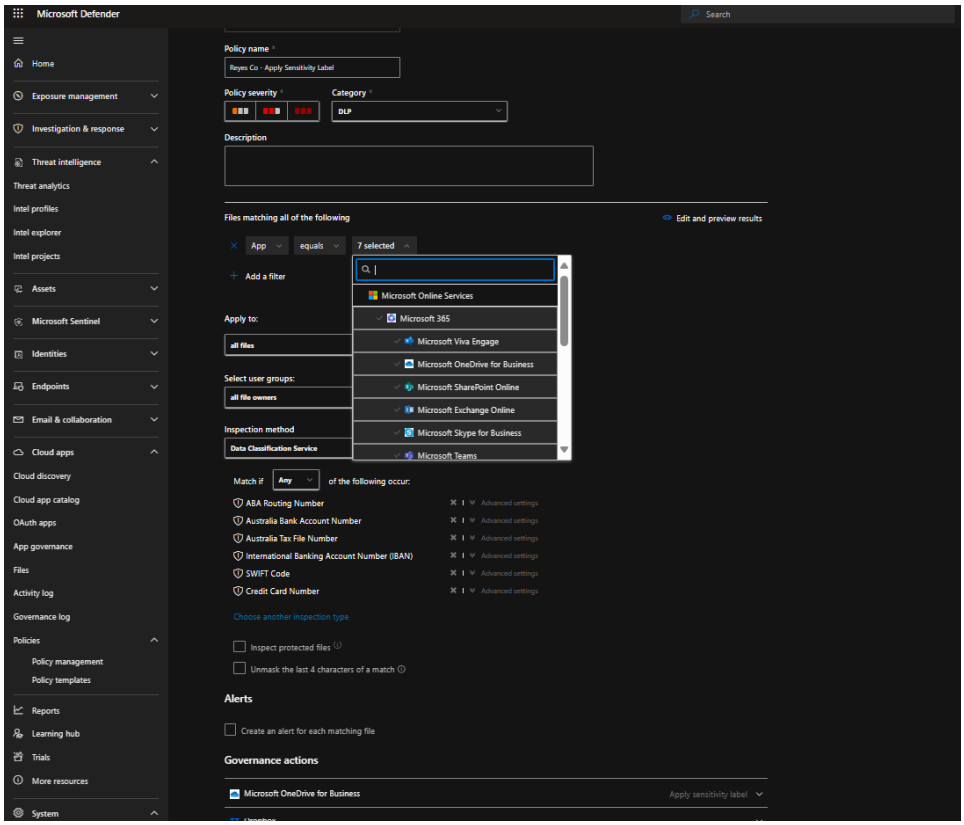
You can find all the policy templates under Cloud Apps – Policies – Policy Template
You can switch categories to see any templates that could be useful or you can also create your own – All the template policies [Control cloud apps with policies - Microsoft Defender for Cloud Apps | Microsoft Learn]



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

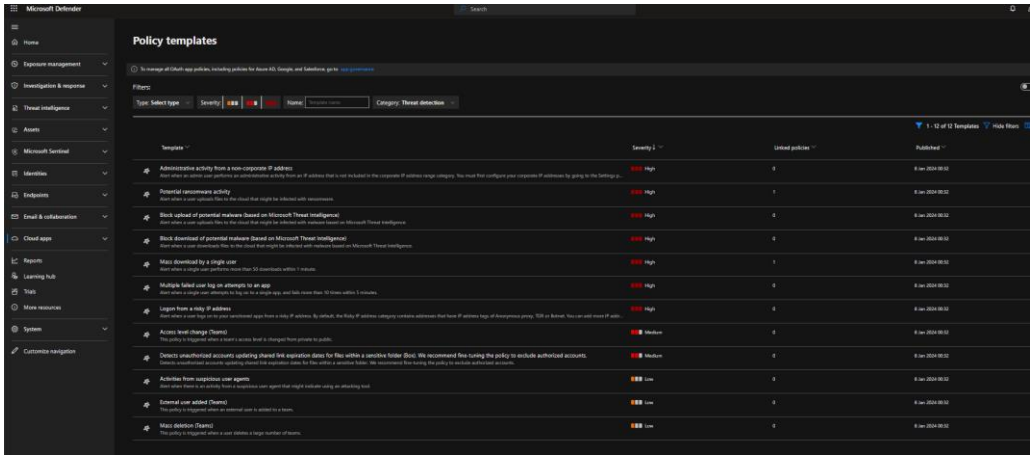


Applying labels across the connected apps is easy to apply. The integration with Purview would be clear when you click on the data classification. This will showcase your label taxonomy you've created when deploying Purview



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:

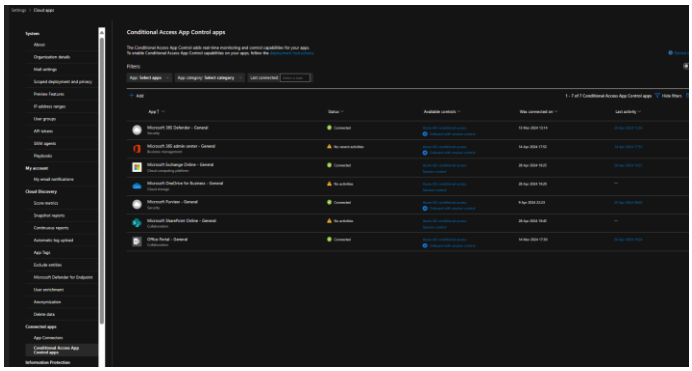
Use access policies to:

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

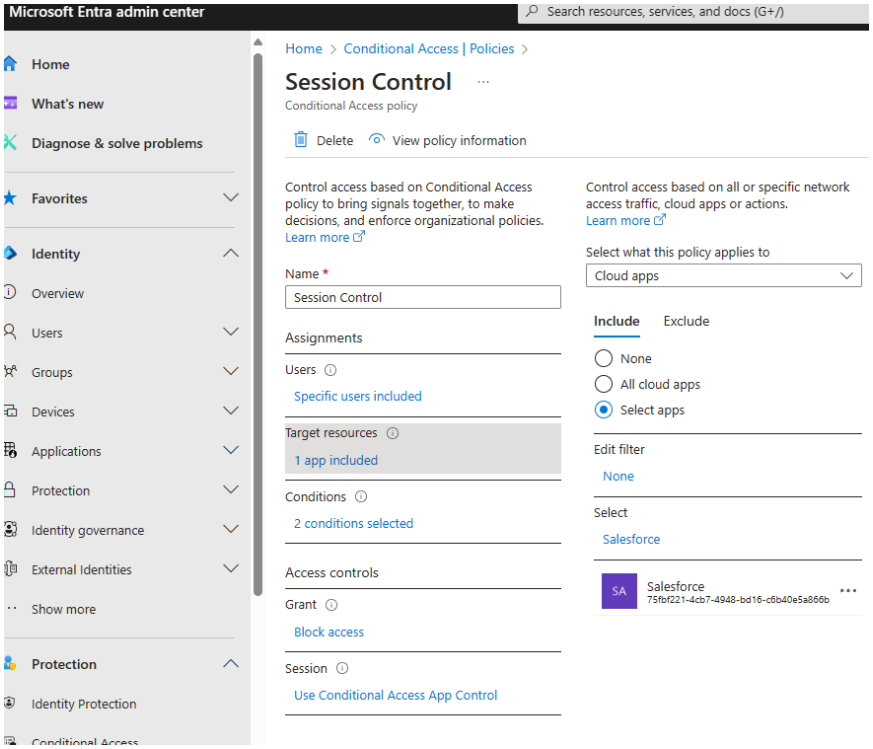
Use session policies to:

- 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.

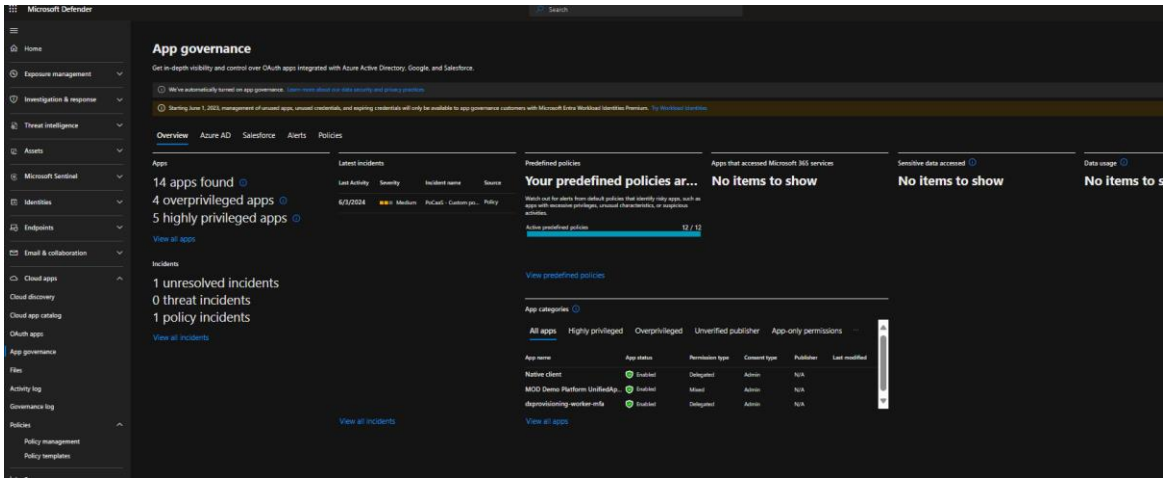


Creating the CA Policy in entra is very much like all the other Conditional Access.



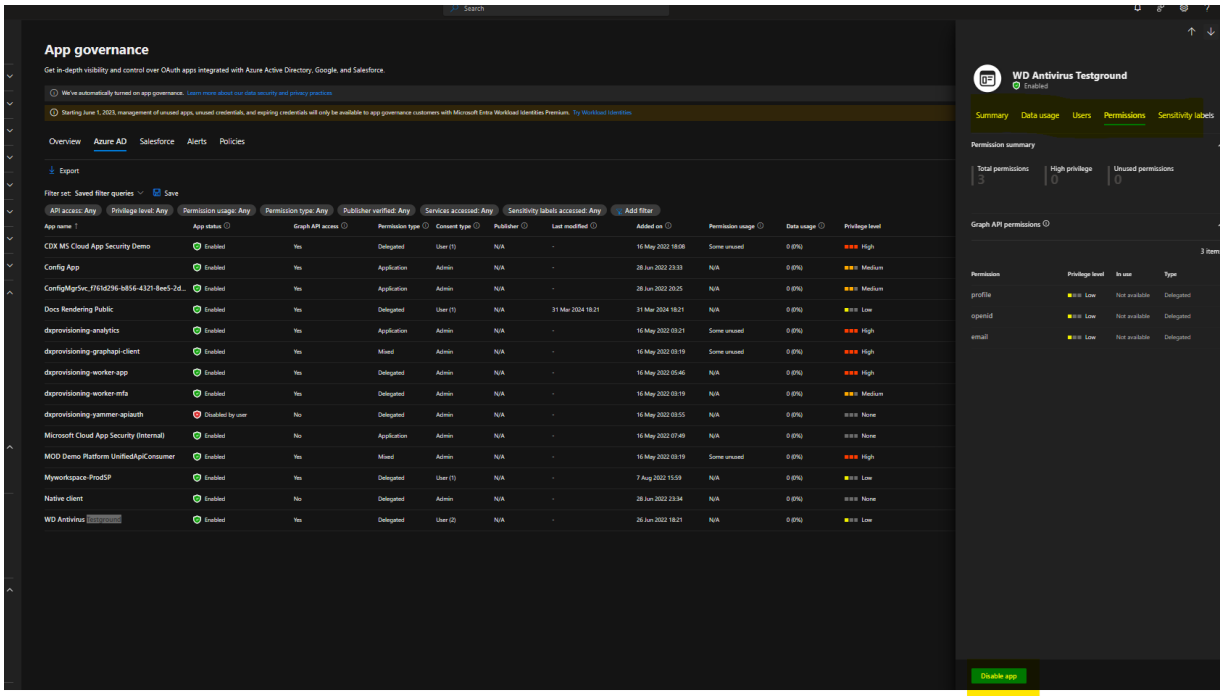
Our last component to highlight on Defender for Cloud Apps is **App Governance**. Previously an add-on to MDA, this is now included as part of your MDA subscription. Designed specifically for oauth-enabled apps registered in Entra, Google and Salesforce. App governance delivers visibility, remediation, and governance into how these apps and their users access, use, and

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

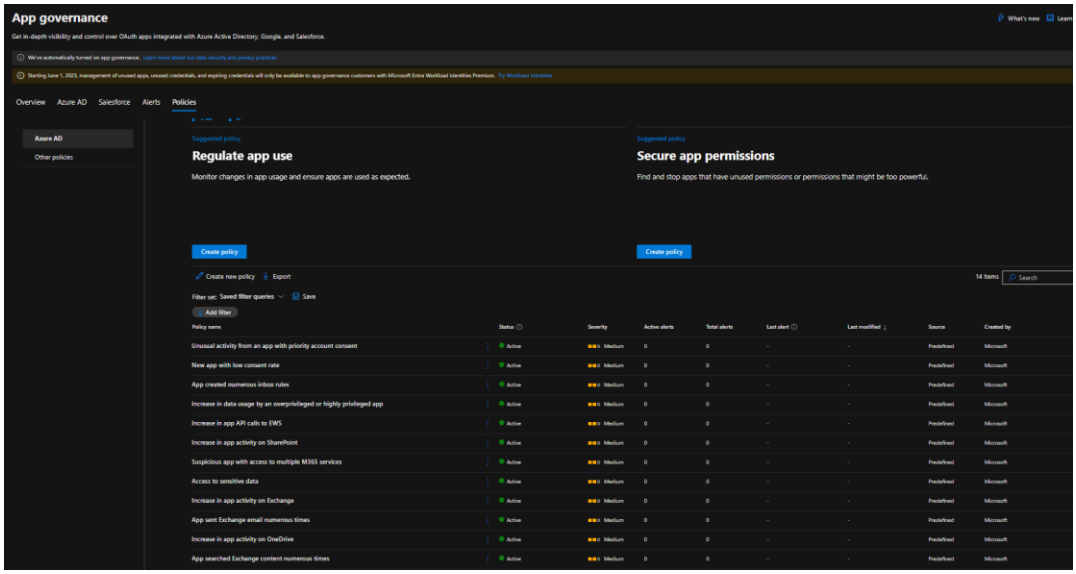


By opening an app you can dig deeper if an app is compliant or you have random permissions in this app. One for the SOC is known to have attackers apply malware onto apps and unidentified accounts can be seen with full rights to the application. If this is a business critical app, is something to investigate.

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



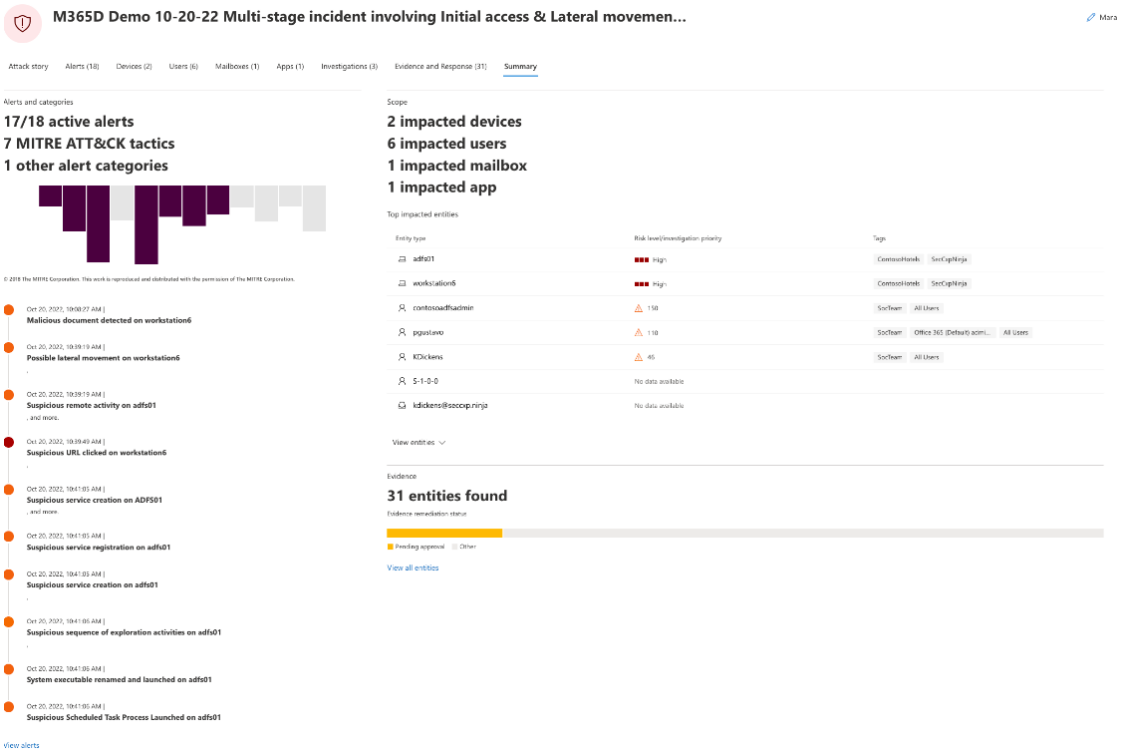
We have some crossover policies and policy templates turned on by default



[Investigate incidents in Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn]

The beauty of turning on all the Defender stack.

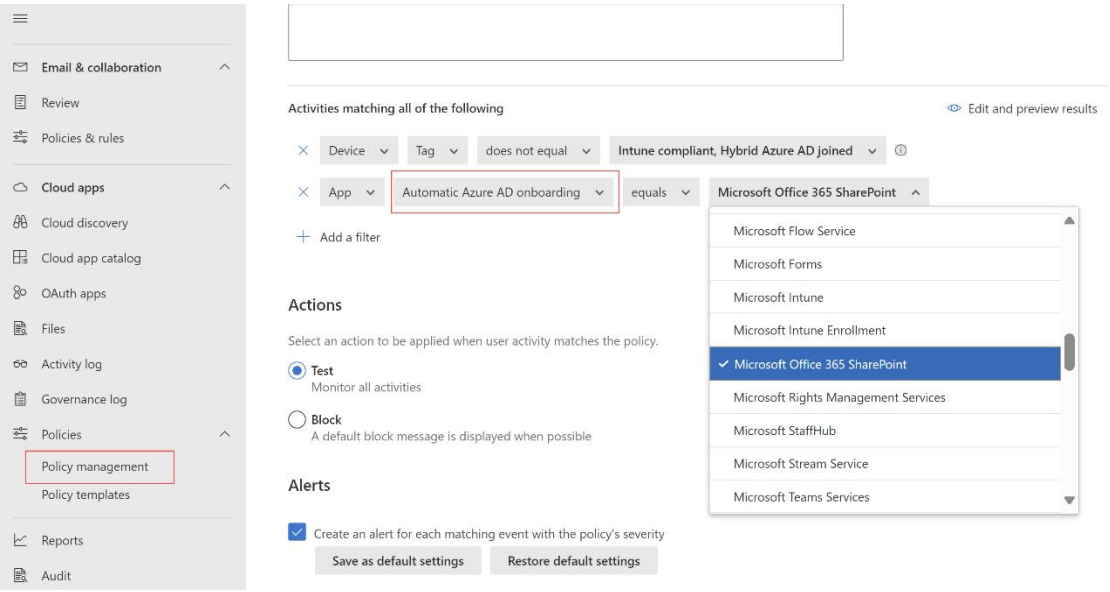
When you get an alert that is then correlated into an incident, an alert that was generated from multiple instances from email, endpoint, to identity, you can see the whole attack story. You can trace it back from the source and potentially run some of our native responses, isolate a device, disable 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 a 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)’**



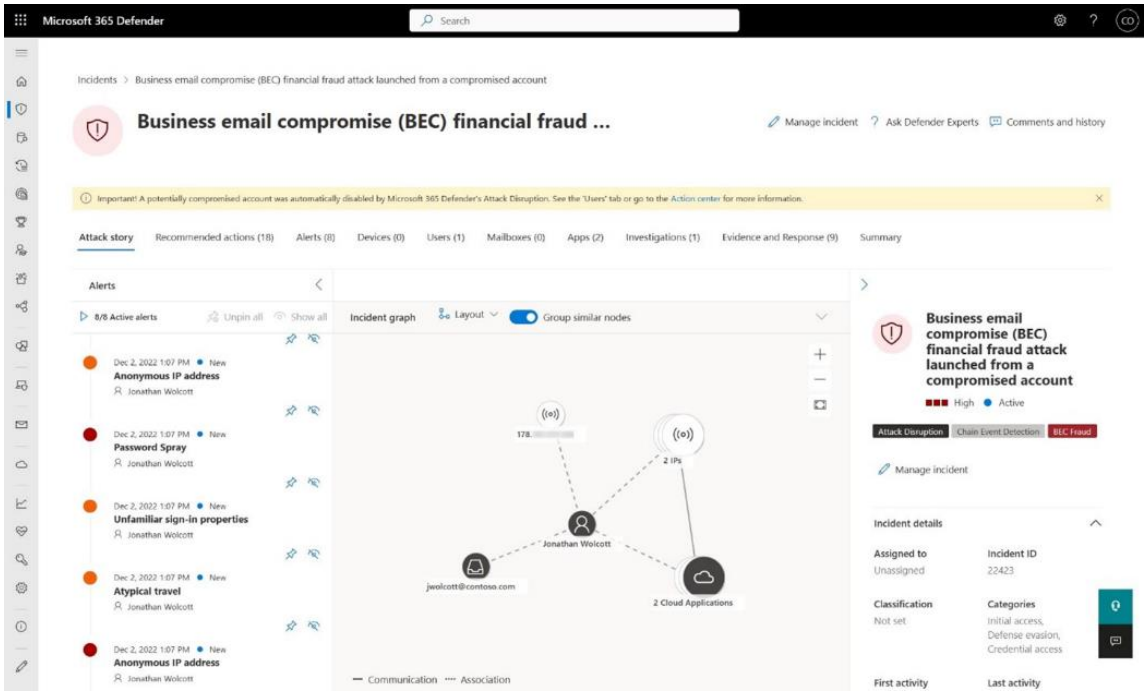
Automatic Attack Disruption (AAD)

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 center 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.

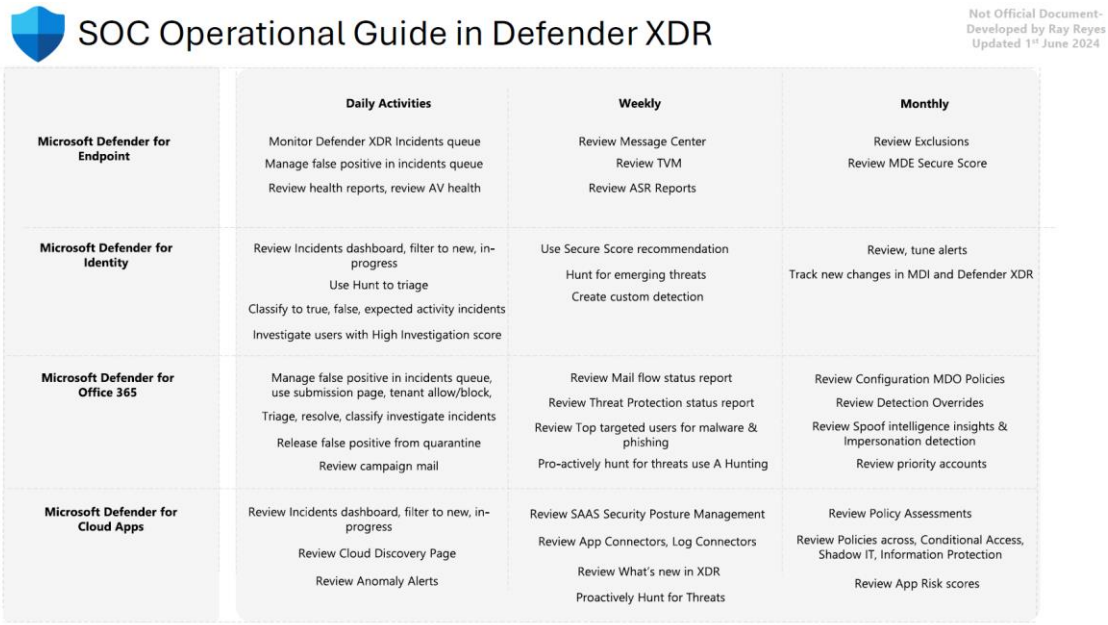
Similarly, the relevant product should be deployed to execute an automated response action. For example, Microsoft Defender for Endpoint is required to automatically contain a device.

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 a 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.



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

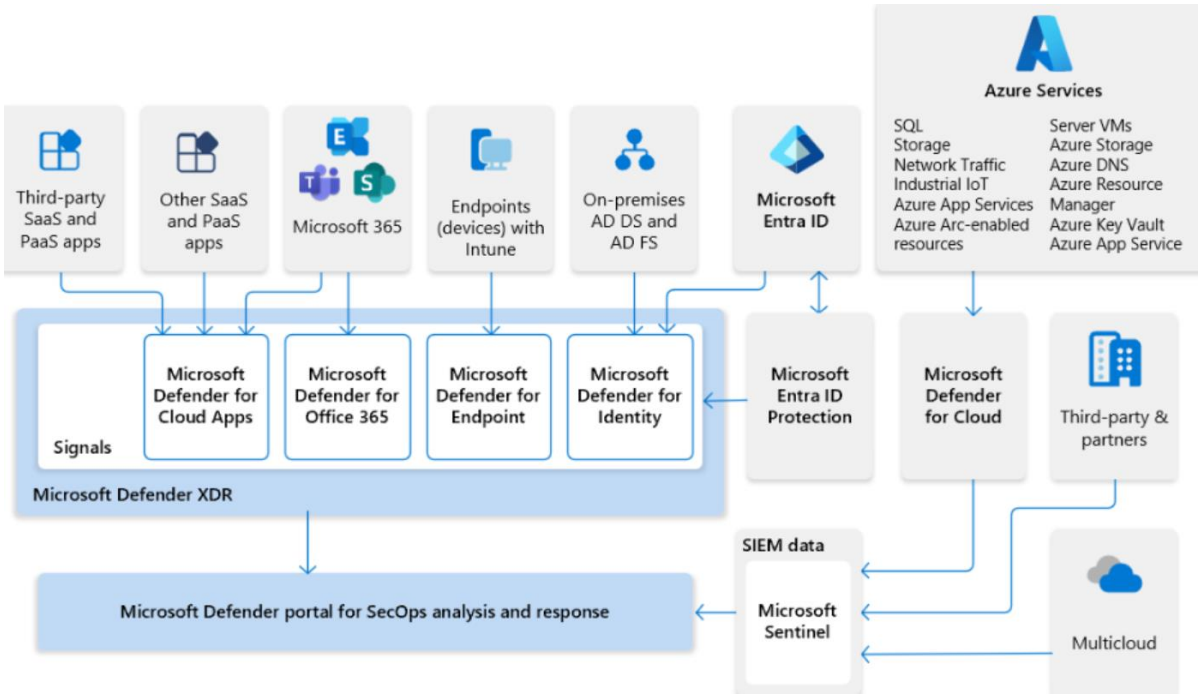
MDI - https://learn.microsoft.com/en-us/defender-for-identity/ops-guide/ops-guide-daily

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

Microsoft Sentinel

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

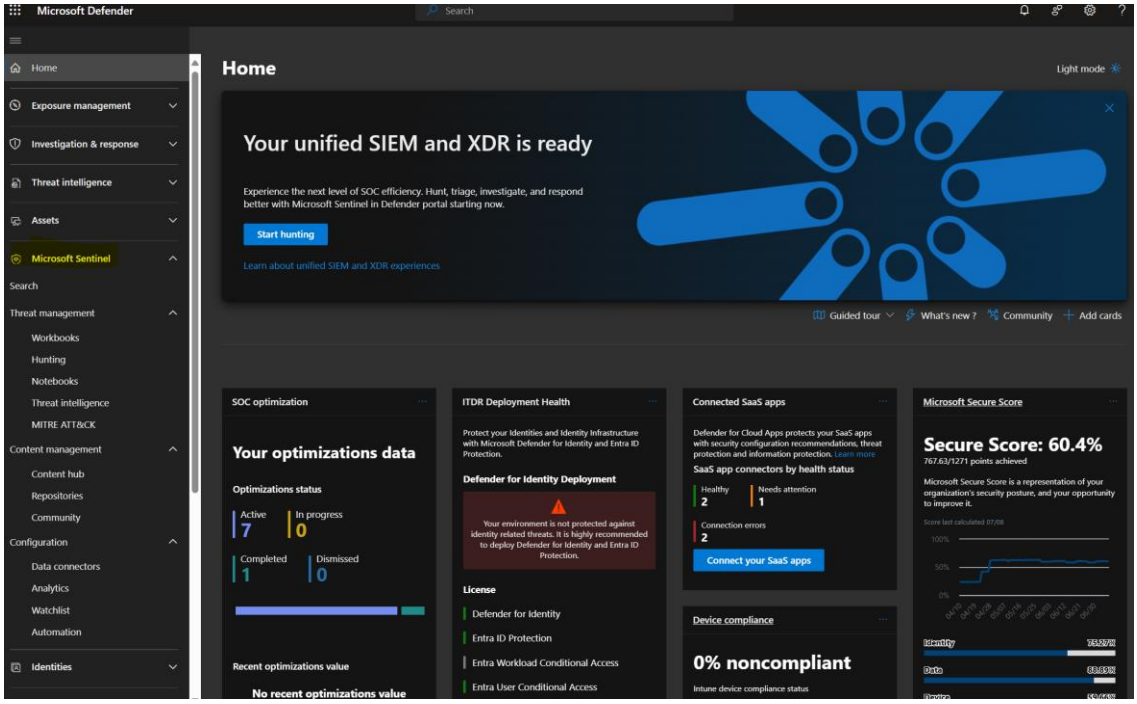
- Cyberattack timelines are automatically fully correlated in a single incident, allowing analysts to move faster to respond to breaches, with a more comprehensive view of an attack
- **Detect and investigate faster with more accuracy.** Bringing the depth of XDR signal from Defender and the flexibility 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.

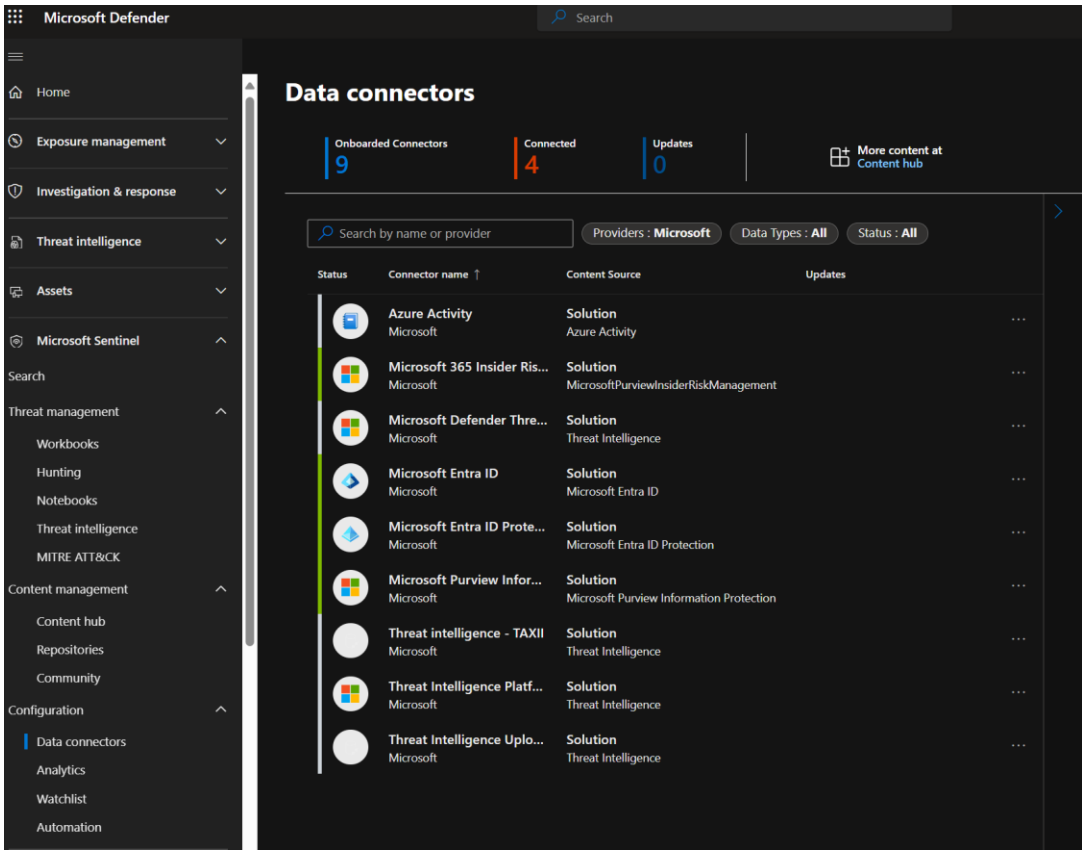
Microsoft Sentinel customers can adopt the new experience easily while continuing to use the classic experience in Microsoft Azure if needed. It's never been easier to add SIEM capabilities

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



[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

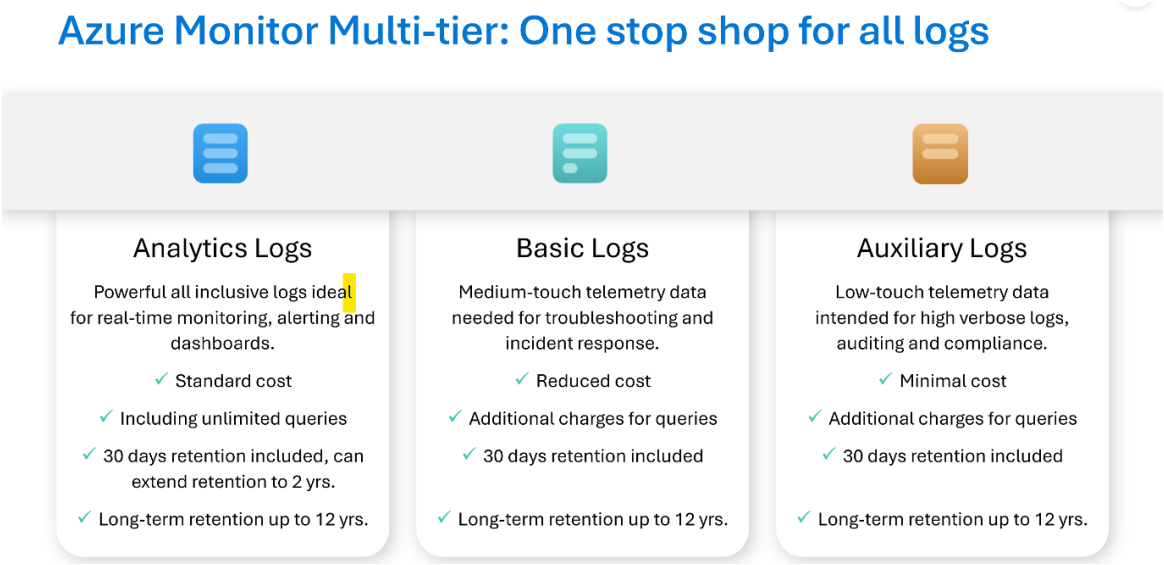
- **Primary security data** is data that contains critical security value. This data is used for real-time proactive monitoring, scheduled alerts, and analytics to detect security

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



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

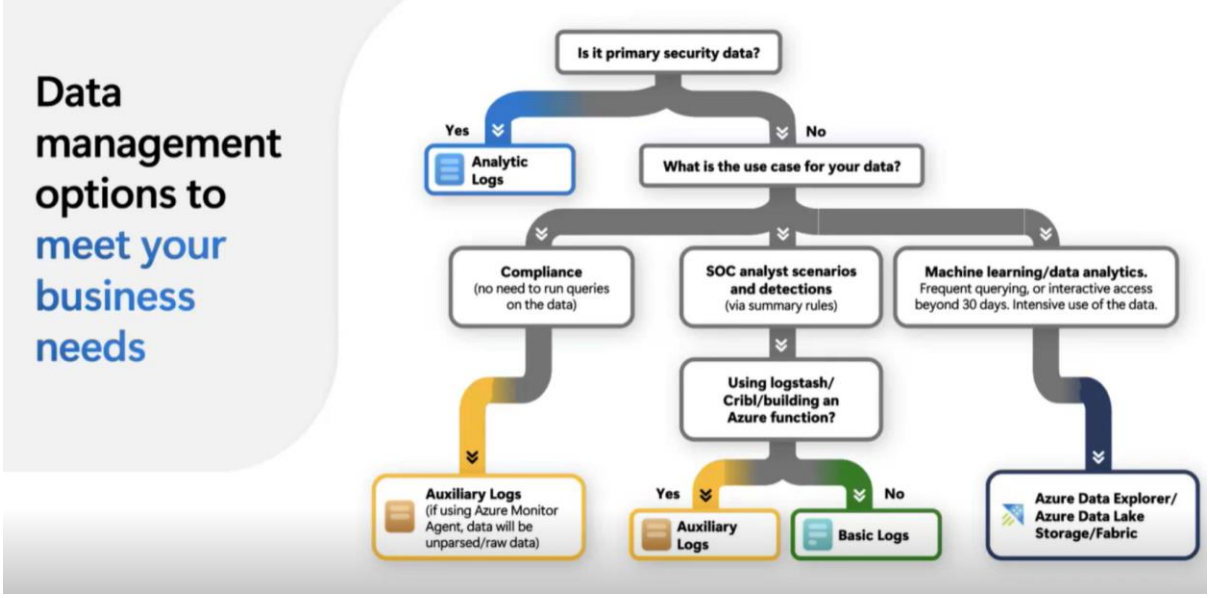
Auxilary logs

- 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

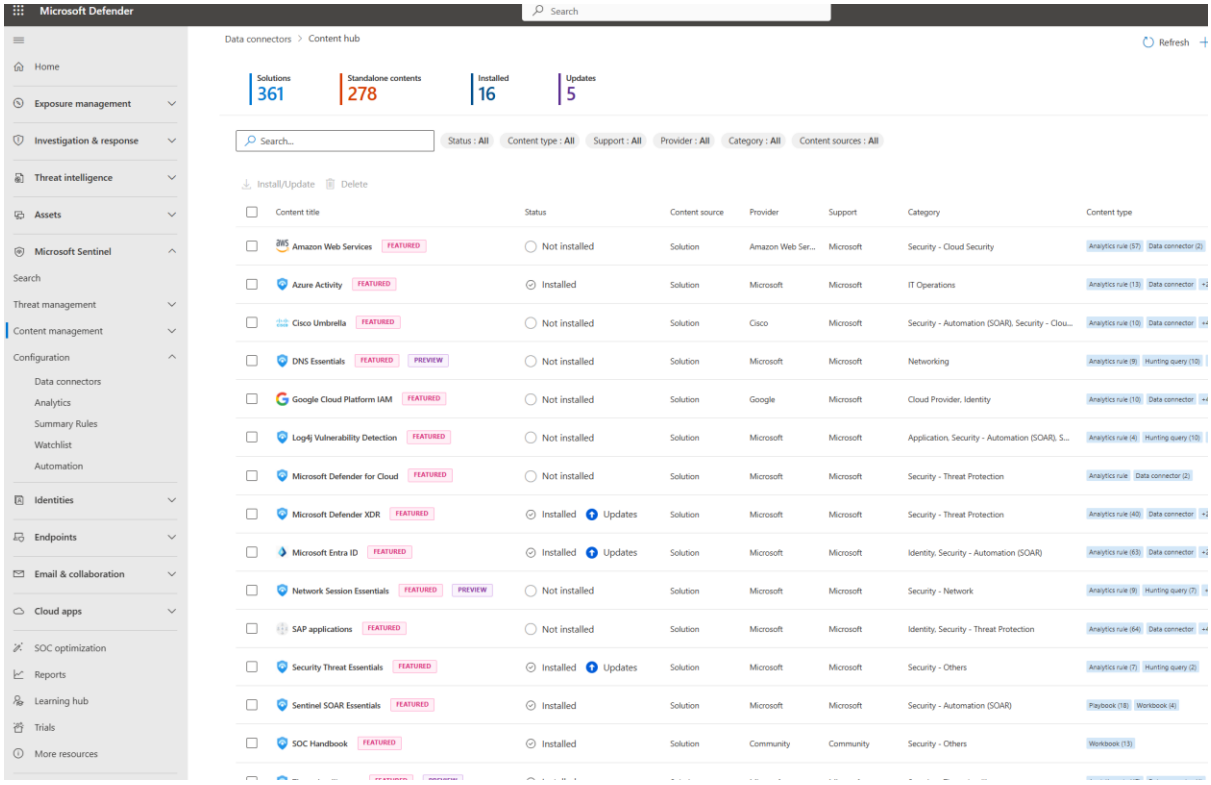


Plan costs and understand pricing and billing - Microsoft Sentinel | Microsoft Learn

Onboard Sentinel

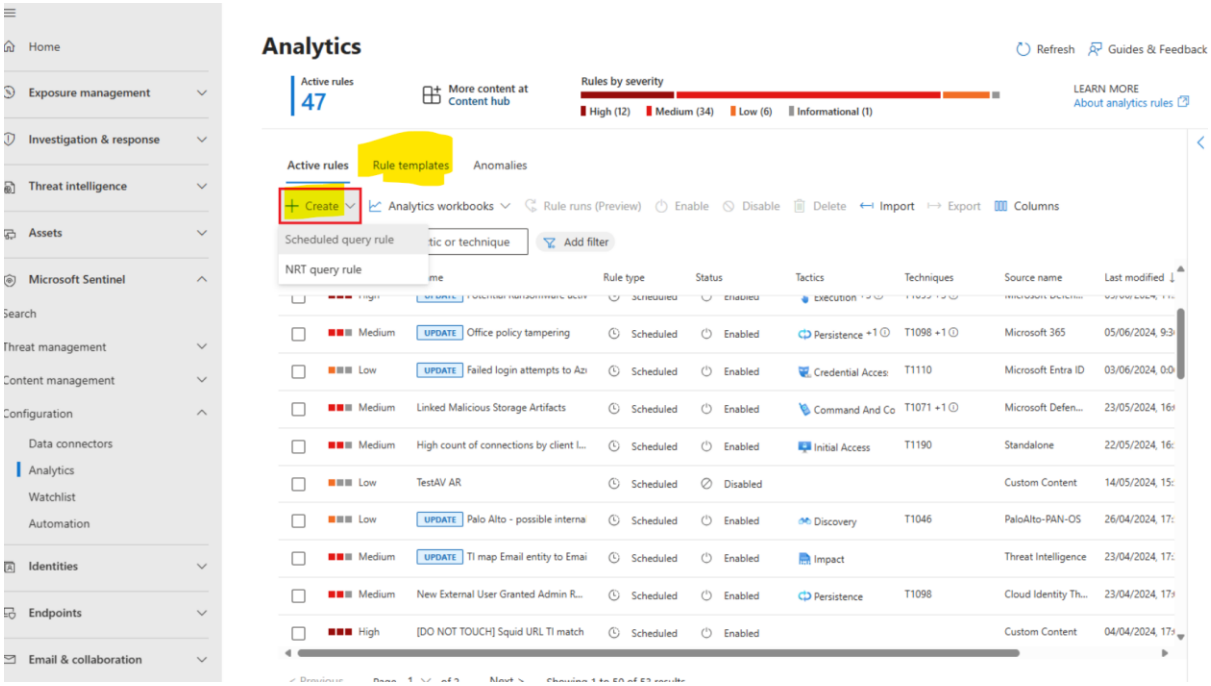
a. Go to Azure Portal, find Microsoft Sentinel. Create and add a new workspace. Bear in mind that the workspace you choose means that the data is isolated to that workspace

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 are 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.

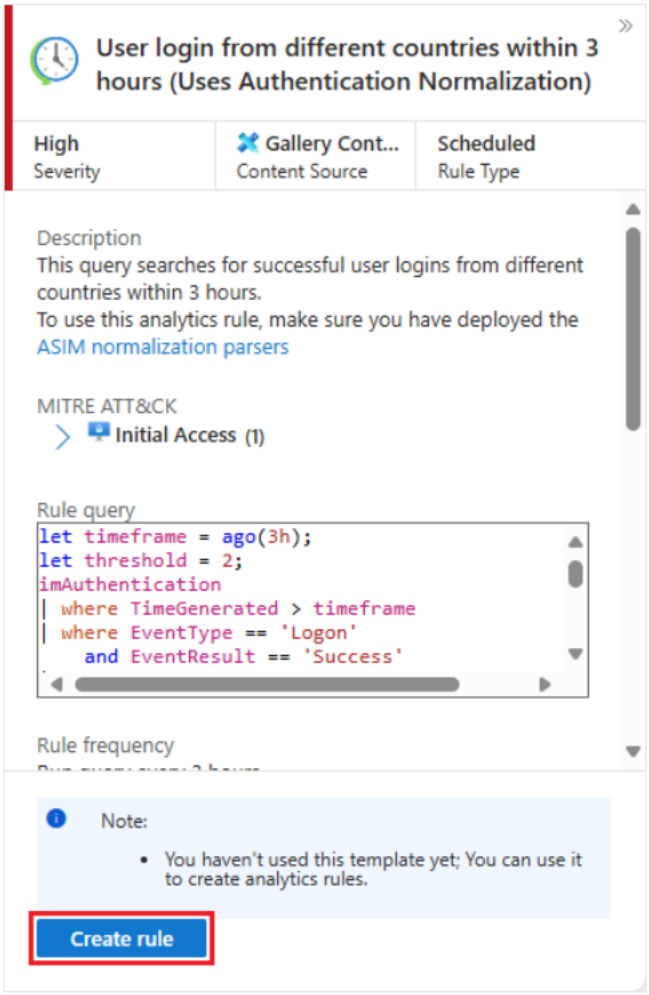


5. Setup Analytics Rules - [Threat detection in Microsoft Sentinel | Microsoft Learn]
   Once you've setup your connectors, you're going to need to know what you're looking for, detect and report rules you put in place.
   You can do this in two ways. Using the [built-in analytics rule wizard] or **[analytics rule templates]**

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



message to that effect.

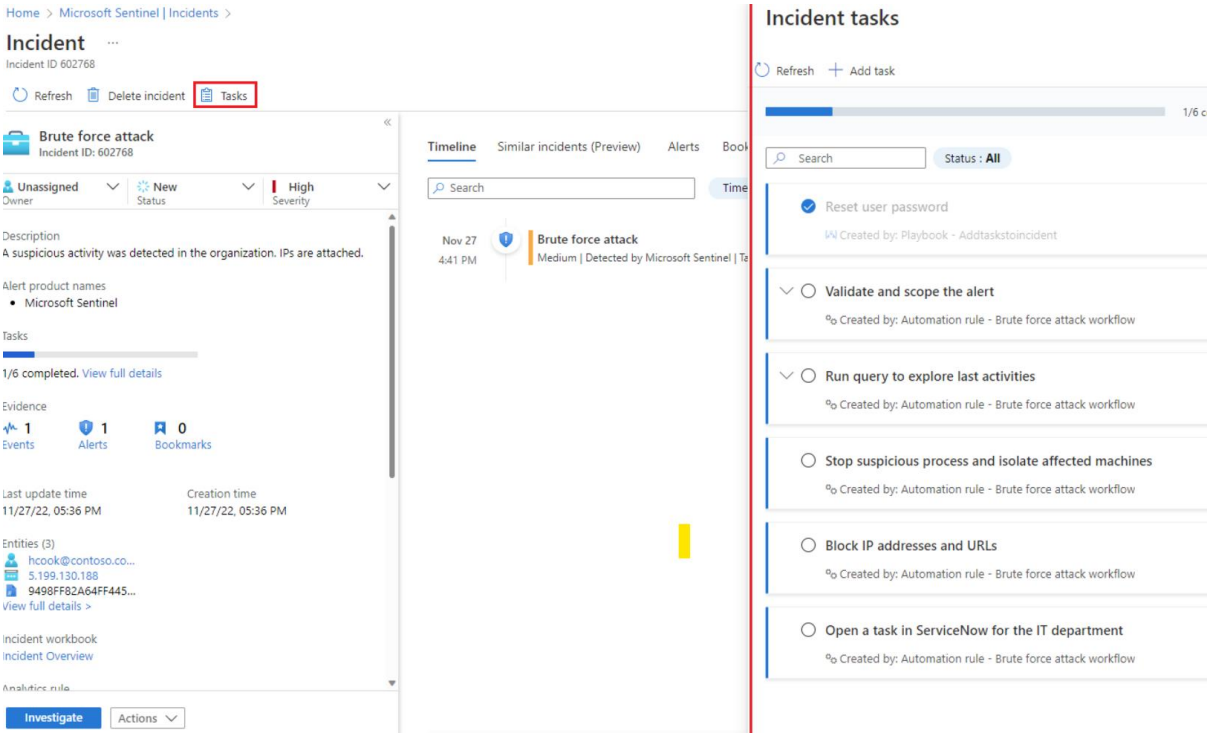


6. **Setup Automation Rules**
   Automation rules helps streamline the use of automation in Microsoft Sentinel, enabling you to simplify complex workflows for your threat response orchestration processes.

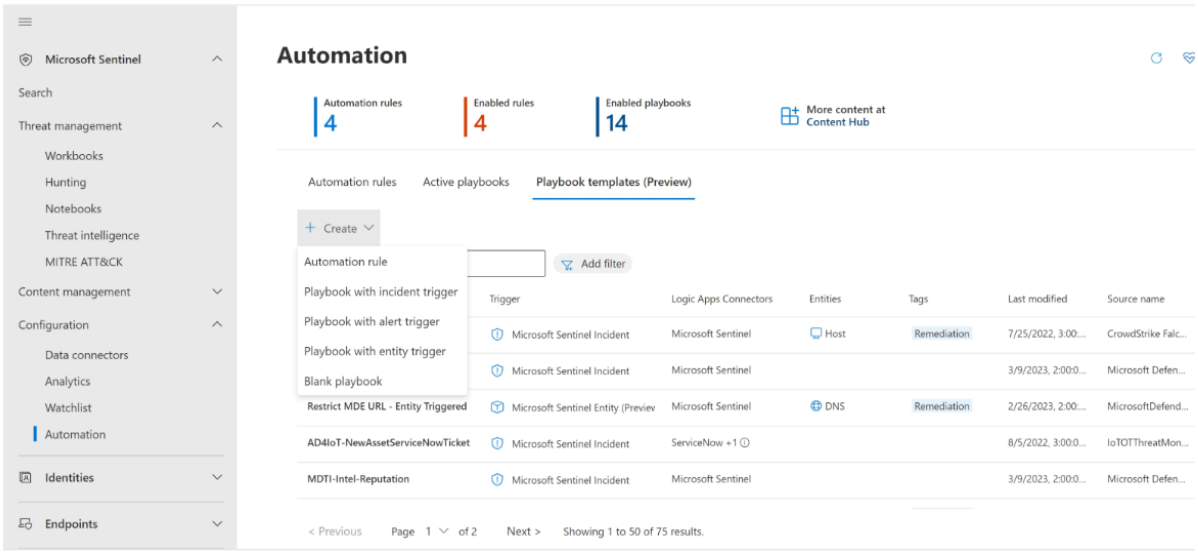
   There are 3 key components in Automation Rules. Triggers, Condition and Action. A common triage and respond flow.

   These 3 key components can be use 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]



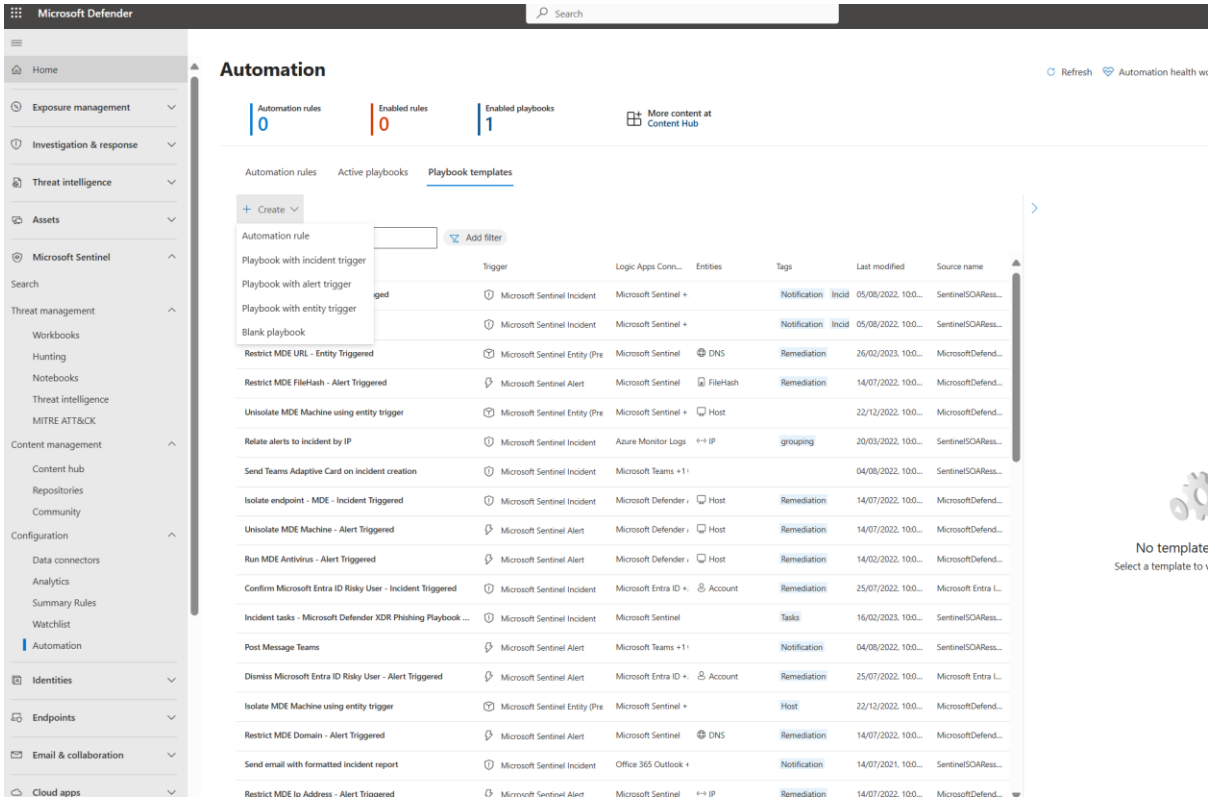
In Defender Portal. Sentinel – Configuration

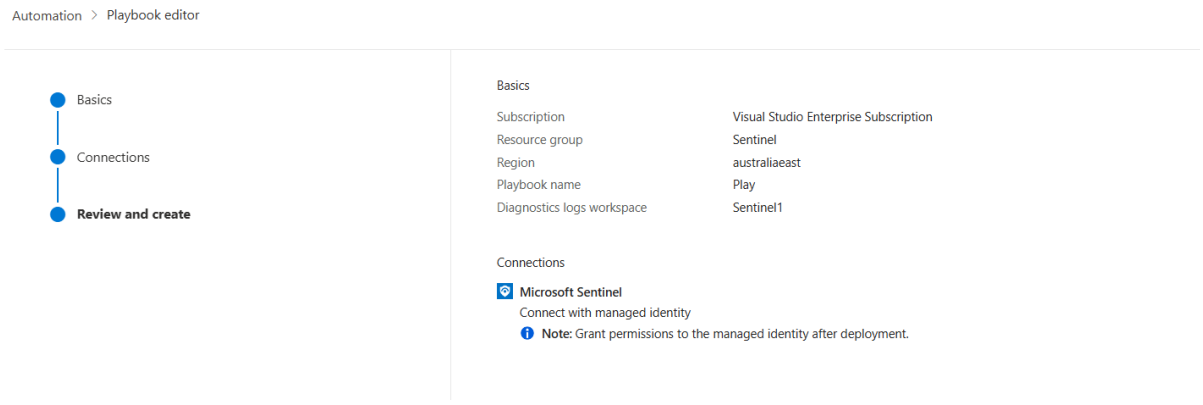


7. Setup Playbook

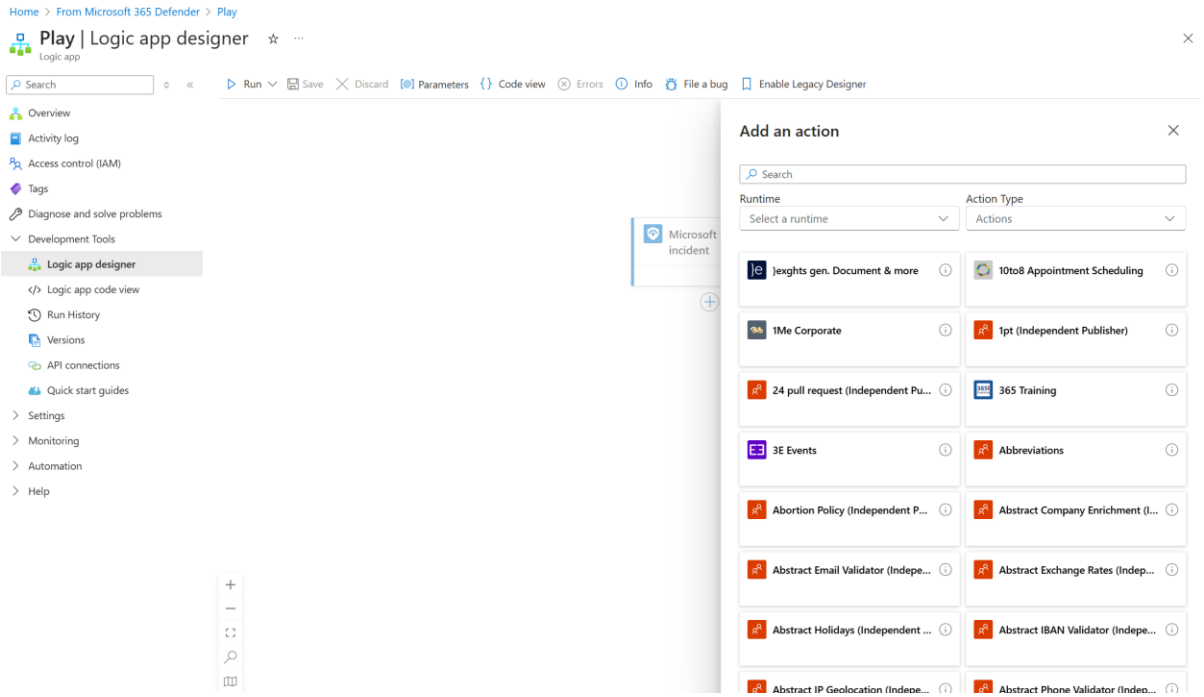
Playbooks in Sentinel is one of our bread and butter feature and a SOCs best friend. With the sheer volume of alerts and incidents, sometimes I can be overwhelming for any SOC to go through each alerts. Playbook can help SOCs to run a set of collection of remediation actions that you run from Microsoft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

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





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



8. Setup Workbooks

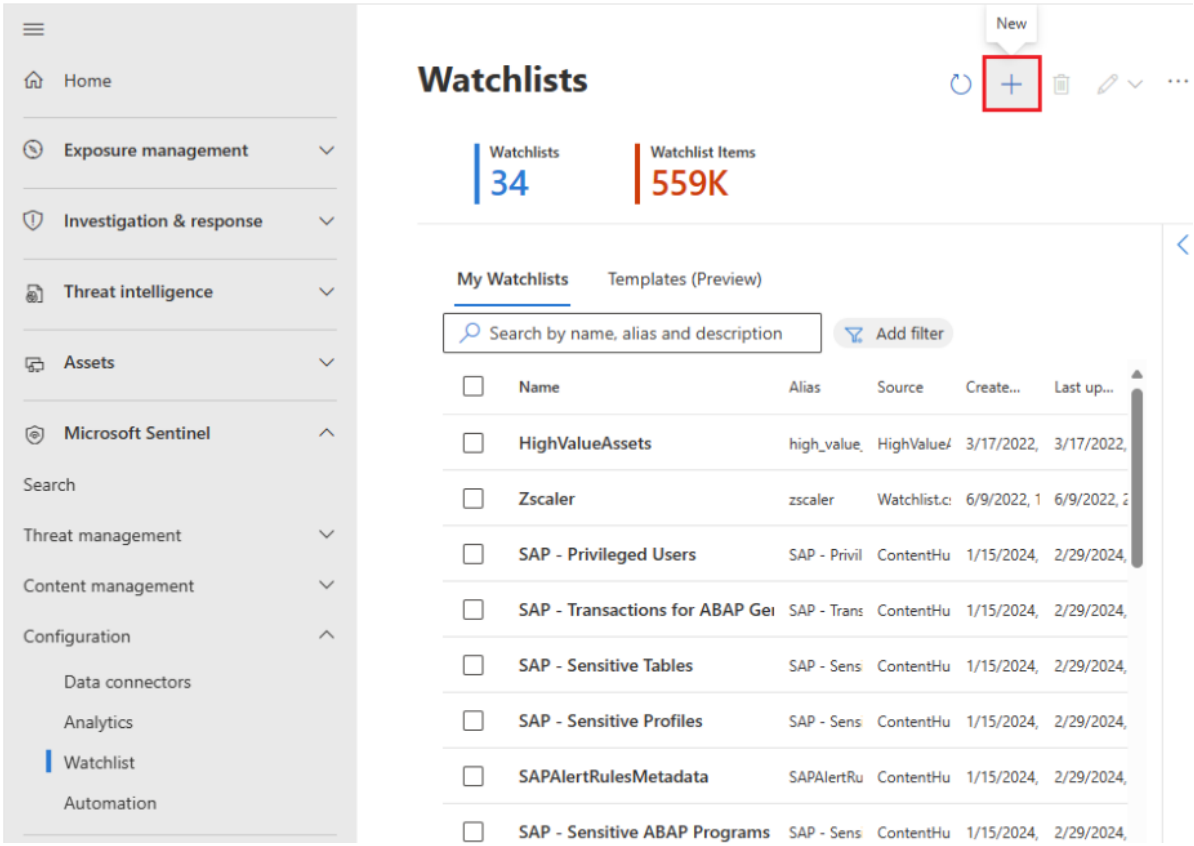
When you think of Workbooks, think of visual reports within Microsoft Sentinel. To give you a better insight to the reports from the logs you receive based on data connectors you've turned on. There isn't much to this. Just like some of the steps above, you can create your own or use the templates we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

These are the commonly use workbooks
Commonly used Microsoft Sentinel workbooks | Microsoft Learn

9. Setup Watchlist

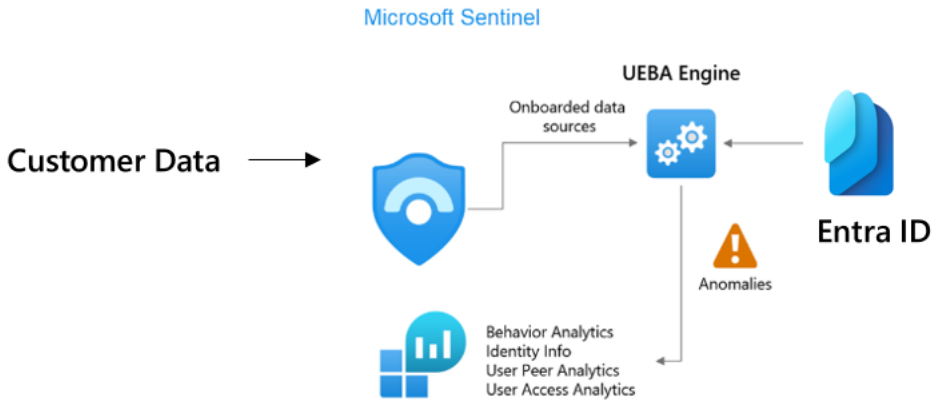
Watchlists in Microsoft Sentinel - Microsoft Sentinel | Microsoft Learn

Think of watchlist as something like you can leverage for VIP users or assets. Watchlist is an 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)

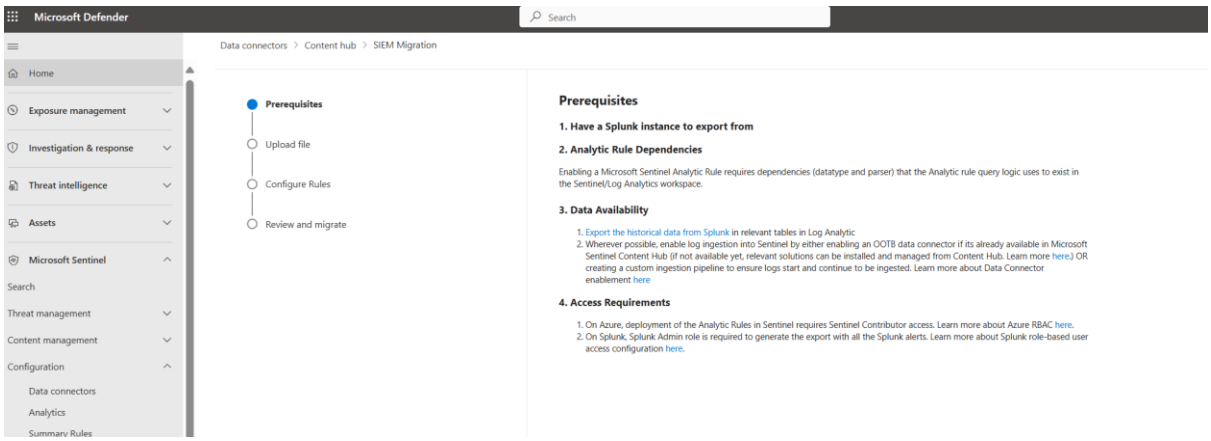
From a Sentinel perspective, UEBA has the same purpose where it builds baseline behavioural profiles of your organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon from all the logs you collect from the data sources. Using a variety of techniques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

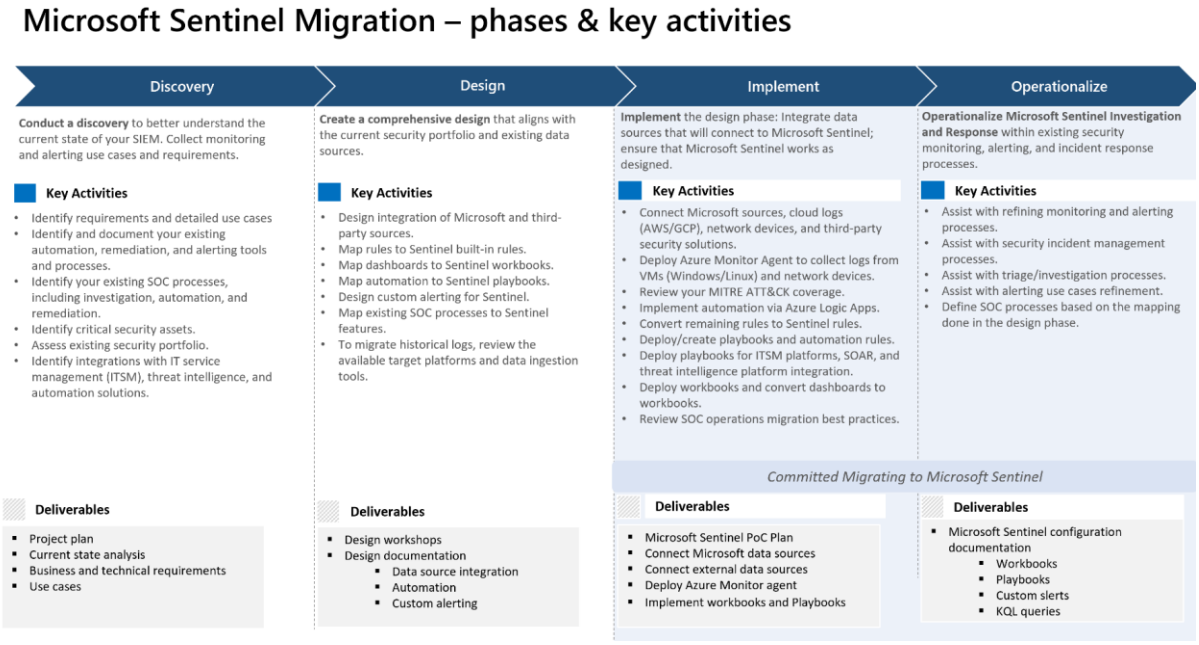


Migration from 3rd party SIEM to Sentinel

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]





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.

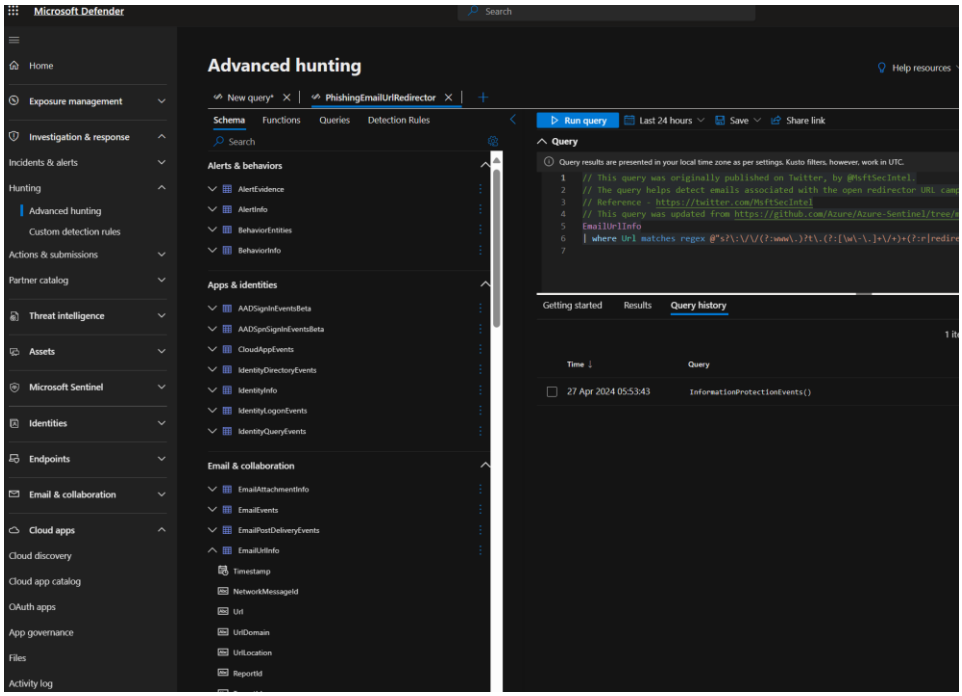
- **Runs playbooks to act on alerts**, gathering information, performing actions on items, and sending notifications to various platforms.
- **Integrates with partner platforms**, such as ServiceNow and Jira, to provide essential services for SOC teams.
- **Ingests and fetches enrichment feeds** from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

Advanced Hunting (AH)

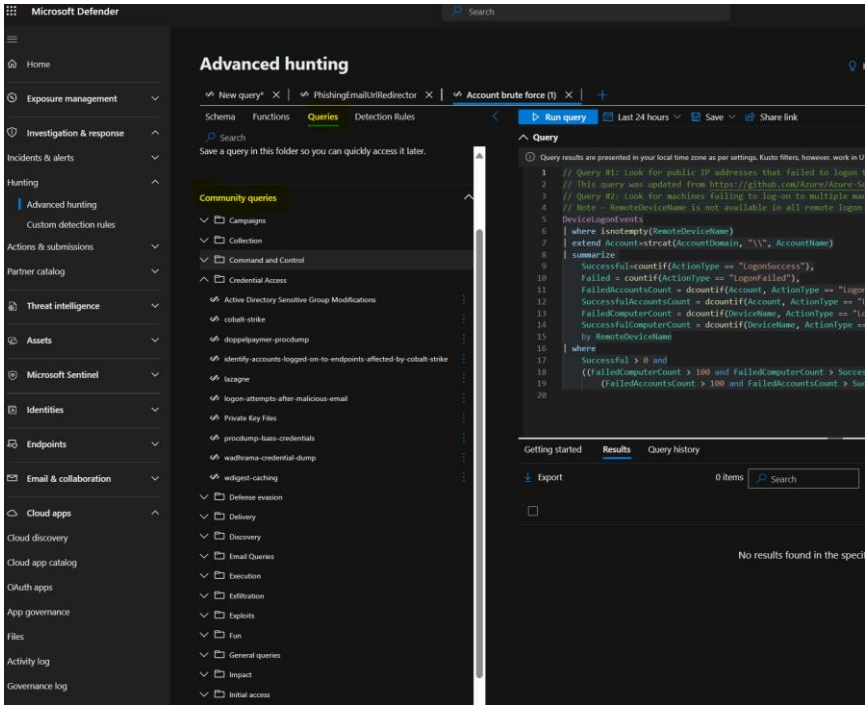
Our AH is our query-based threat hunting using KQL language. It allows you up to 30 days of raw data to discover. Essentially, the telemetry we absorb from our defender stack, is converted to schema tables so we can query it using KQL . We have a number of schemas from Identity, Email, Endpoint, Sentinel 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 template already located in our tables. If you want to hunt and probs threats in email or identity, you can simple go into tha 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

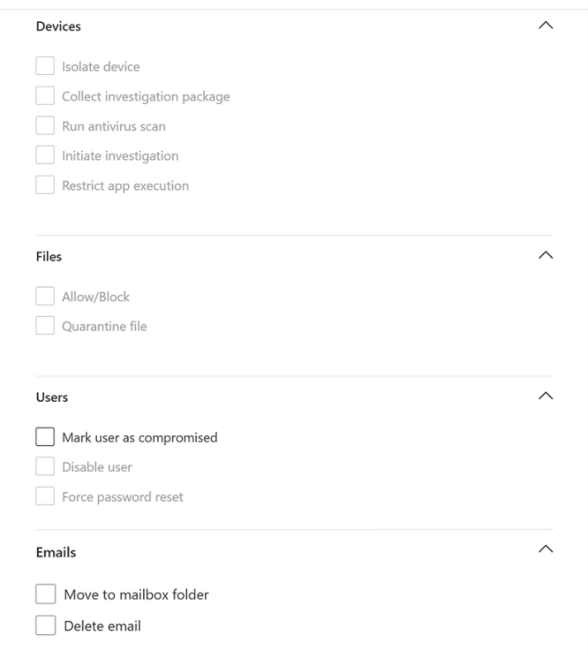


Sample Queries

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



Copilot for Security (CFS) – Just FYI section

*It's important to note that CFS 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. Copilot for Security 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.

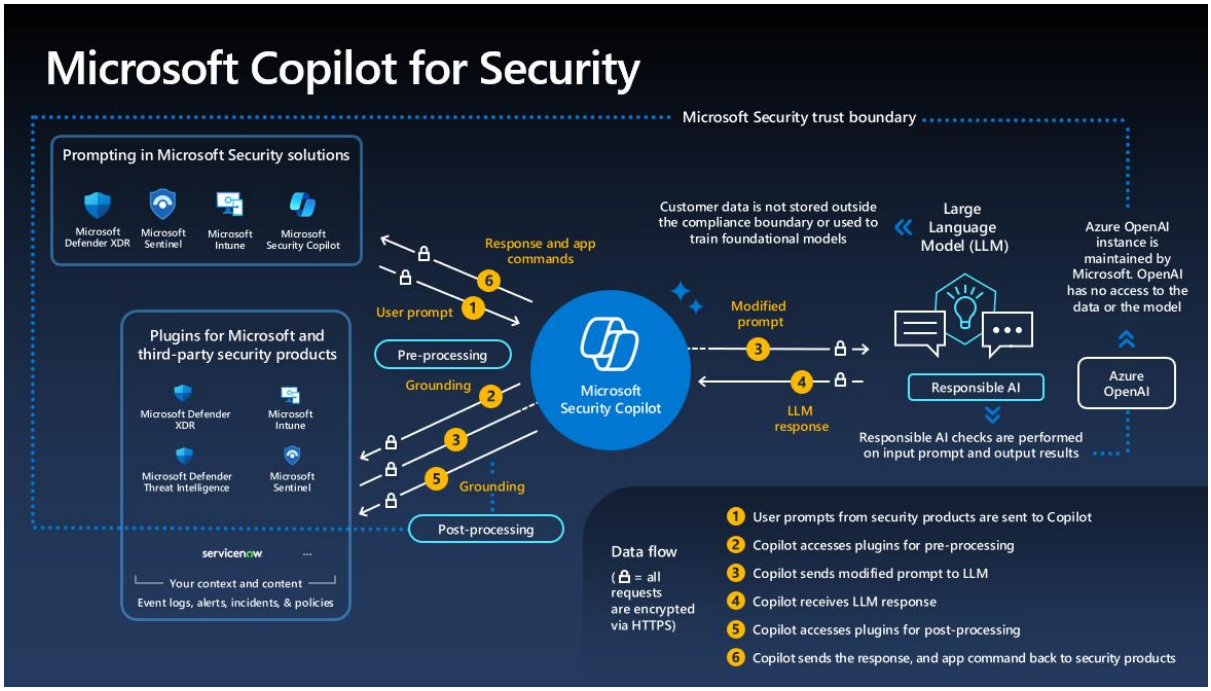
Microsoft Copilot for Security is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale

How does Copilot for Security 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

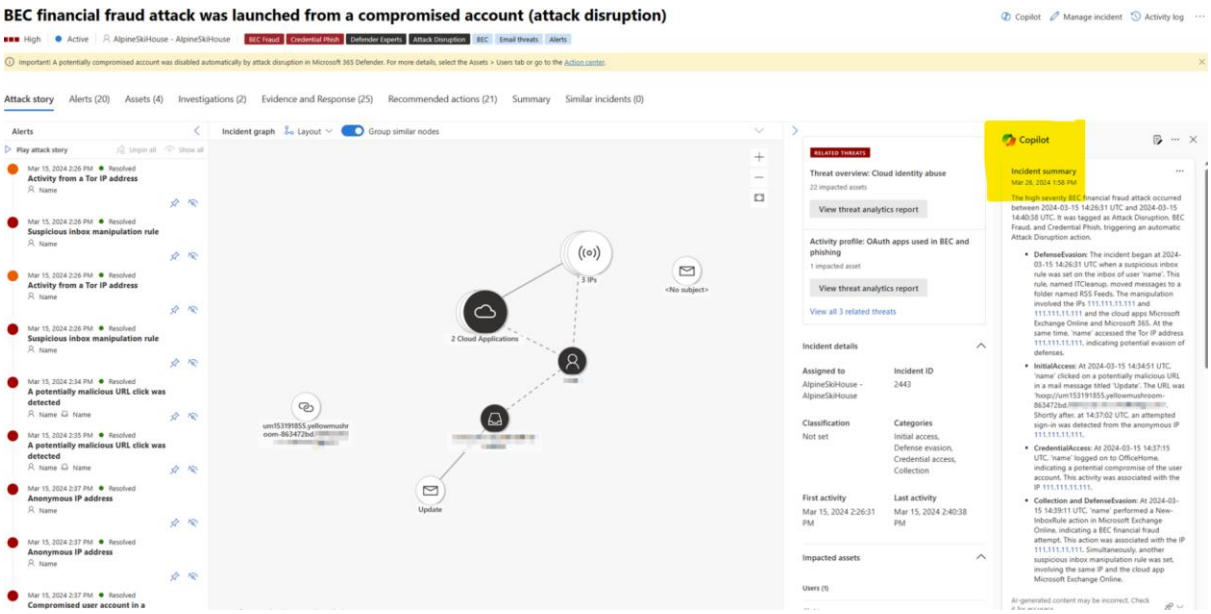
CFS Architecture



Copilot for Security primary use cases

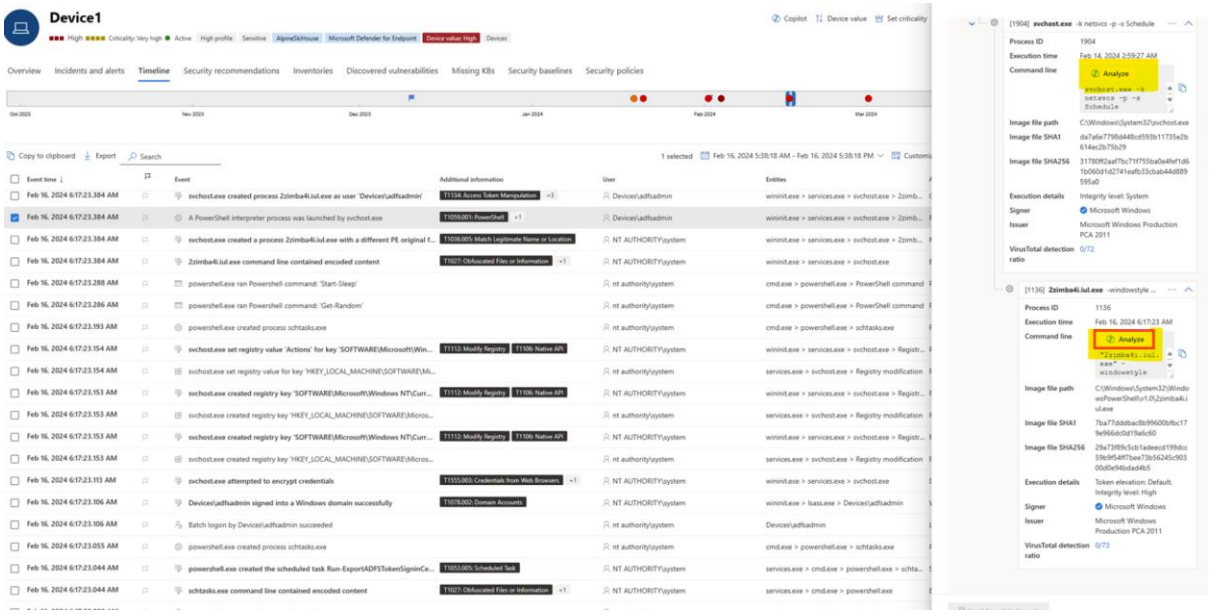
Copilot for Security focuses on making the following highlighted use cases easy to use:

Incident summarization



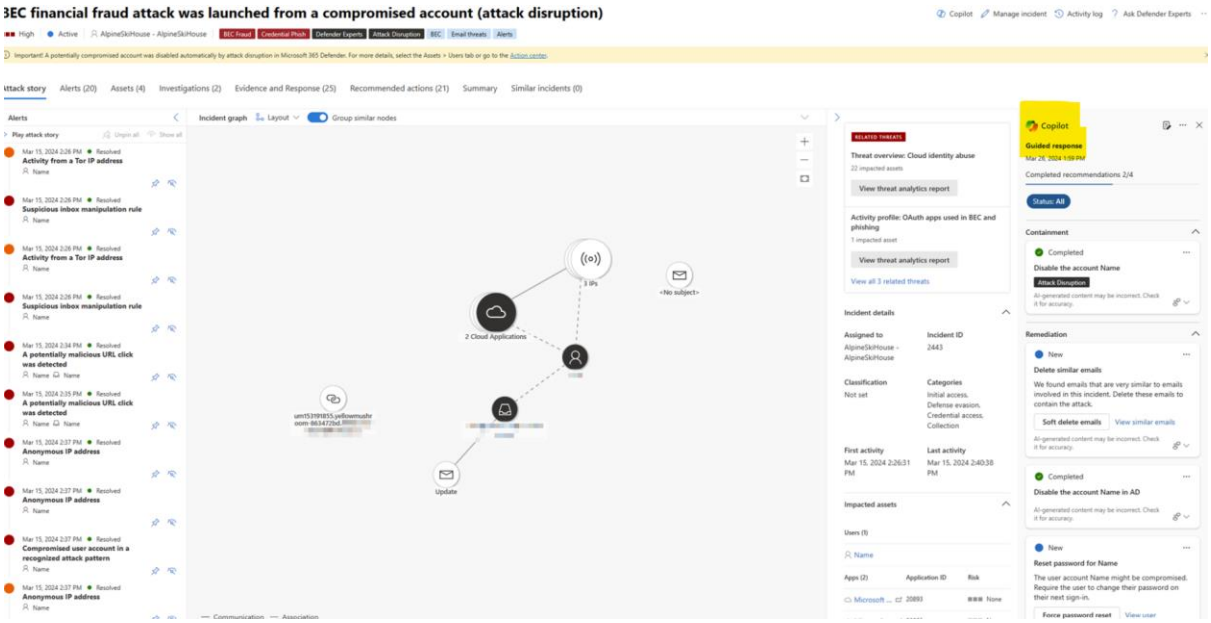
Gain context for incidents and improve communication across your organization by leveraging generative AI to swiftly distill complex security alerts into concise, actionable summaries, which then enable quicker response times and streamlined decision-making.

Analyse code



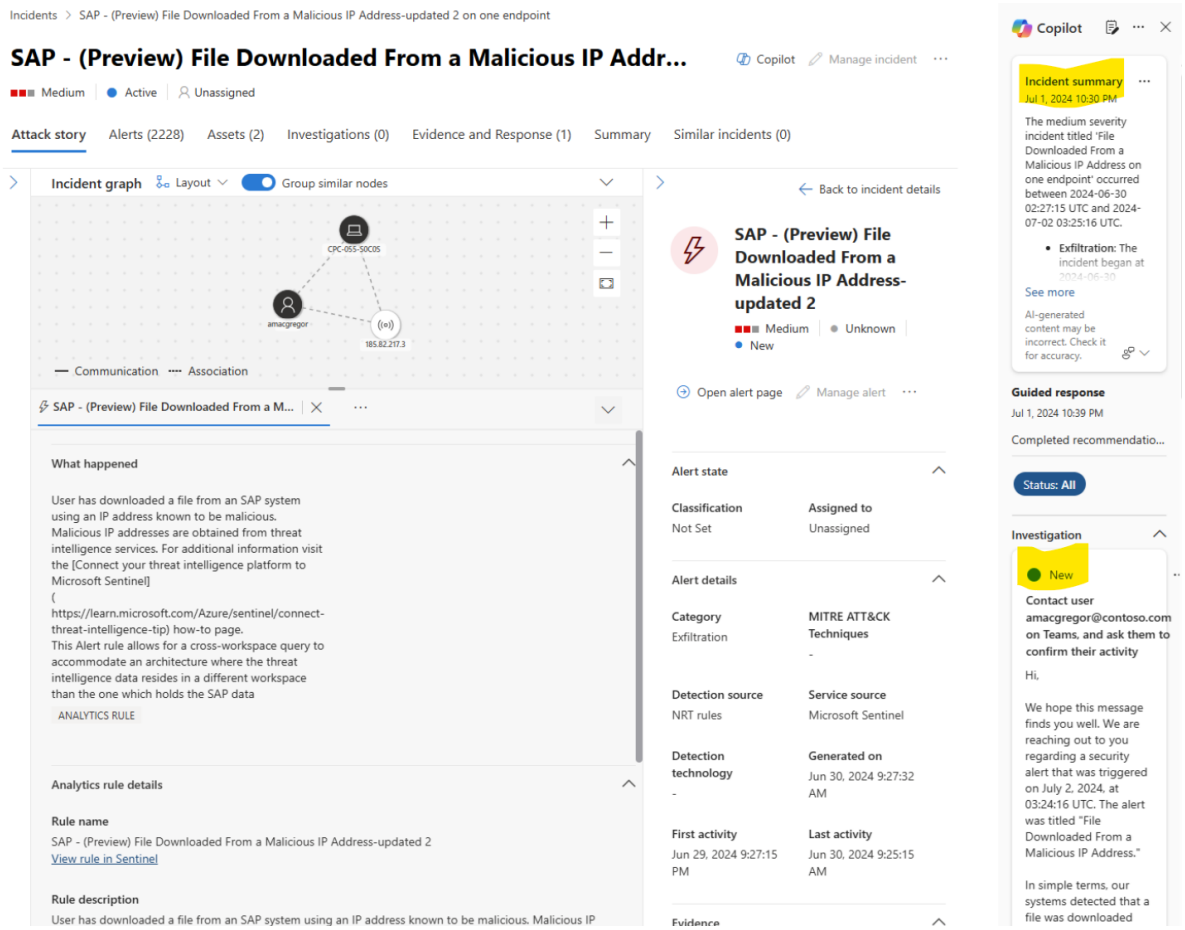
Utilize AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively.

Guided response



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



CFS also 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 guide. I will try to update this guide every 6 months, as our technology matures, and new technology comes into our family of security products. It's important to note that some features could be out of date or about to be replace. So please do refer to when this guide was created on the first page

I hope this guide helps you get started and help you understand the deployment guidance on our security products

Regards,

Ray Reyes