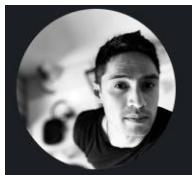

Defender XDR + Sentinel

Deployment Guide

By Ray Reyes
Data Security ANZ Lead, Microsoft



Updated: 6th August 2024

This article is for Customers, Partners, and Colleagues

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

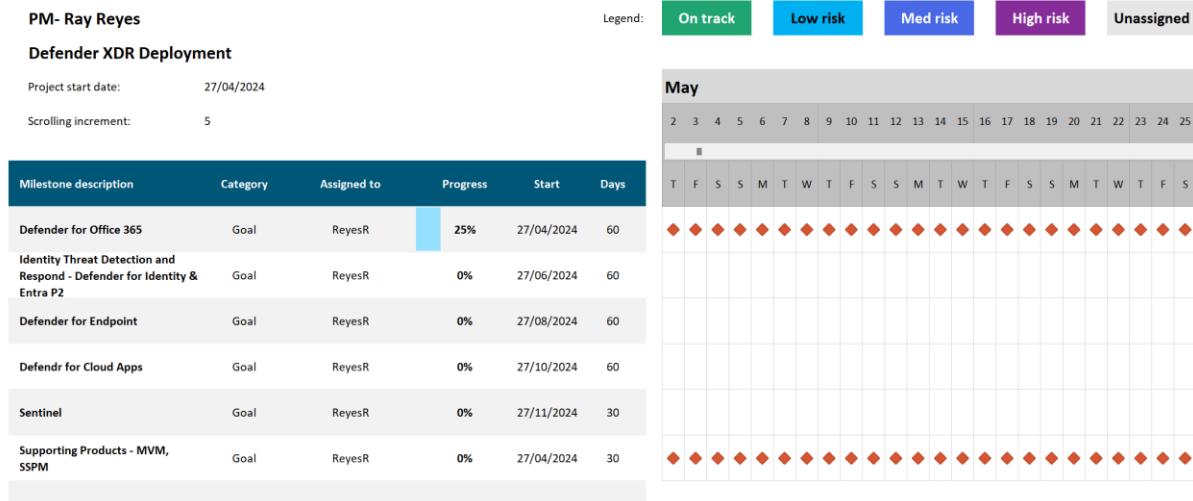
Highlights

- 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?’



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 period** 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?

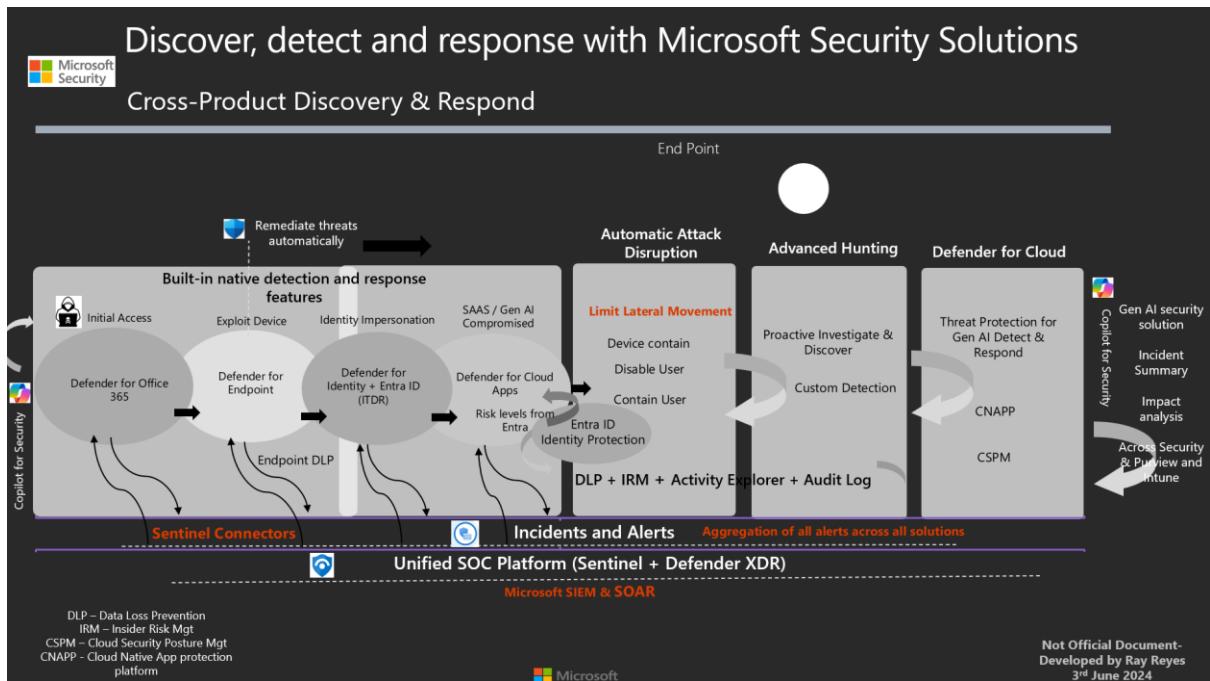
Microsoft Defender XDR is a unified pre- and post-breach enterprise defence suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. What will go through on 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.

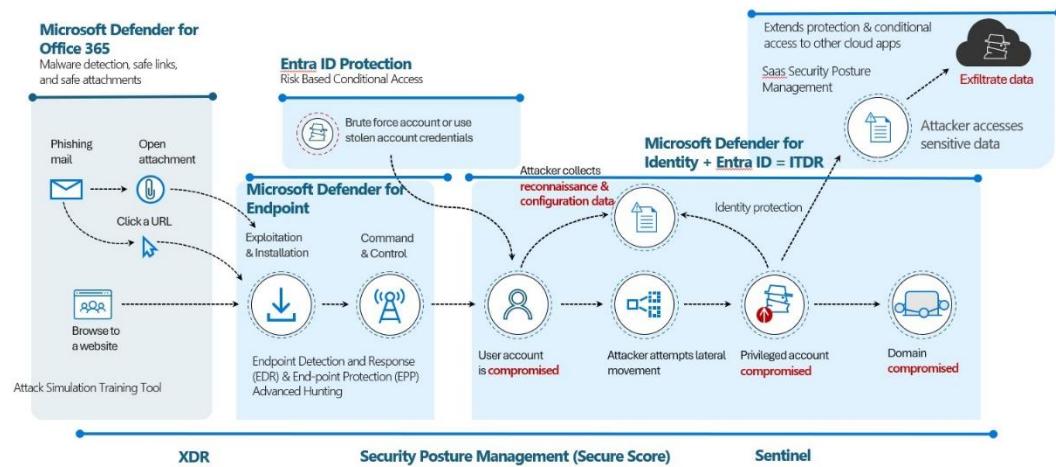
IF we look at a common Attack Kill Chain. The most common initial access to an environment is through Phishing emails. There is a tonne of various techniques from your credential harvesting technique to more sophisticated ones like QR Code

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

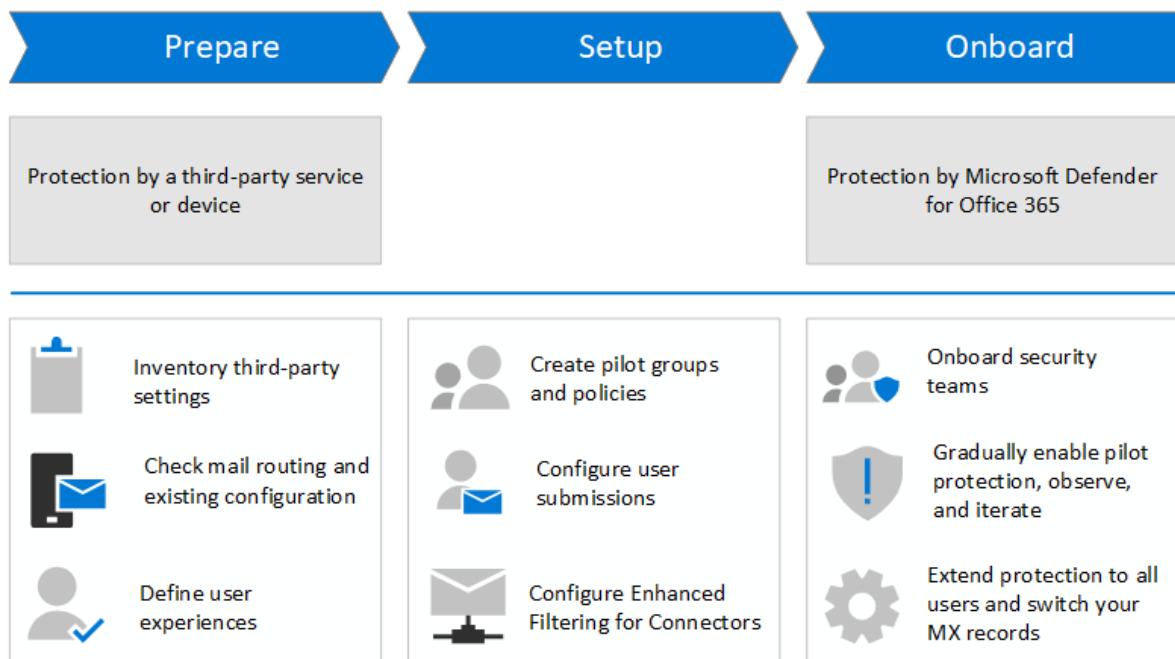
Protection across the attack kill chain



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](#)



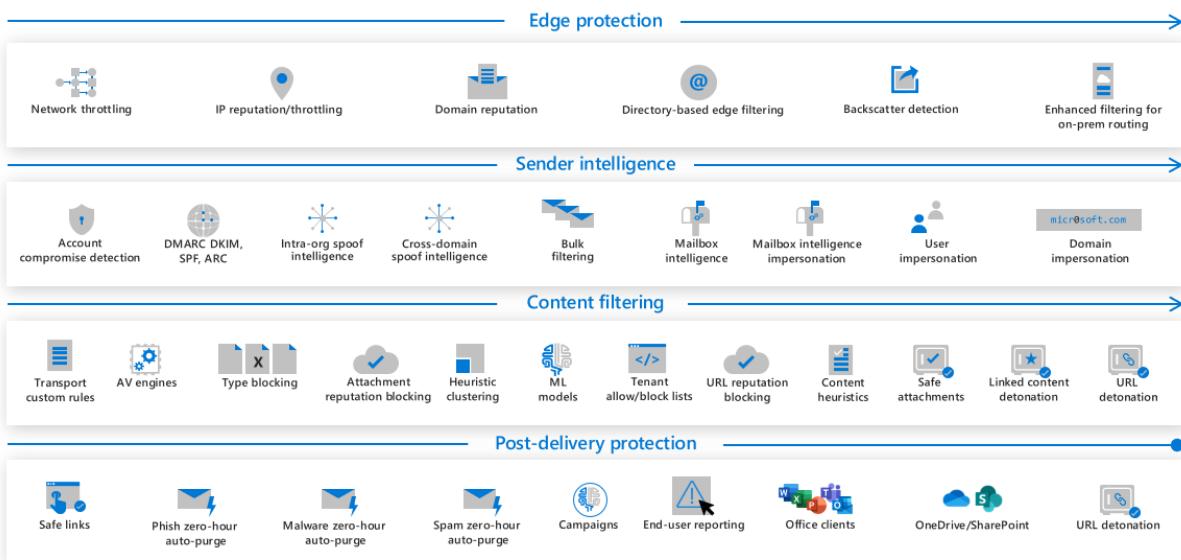
But before we get into the nitty gritty of configuration, there are few key things you need to know and understand

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.

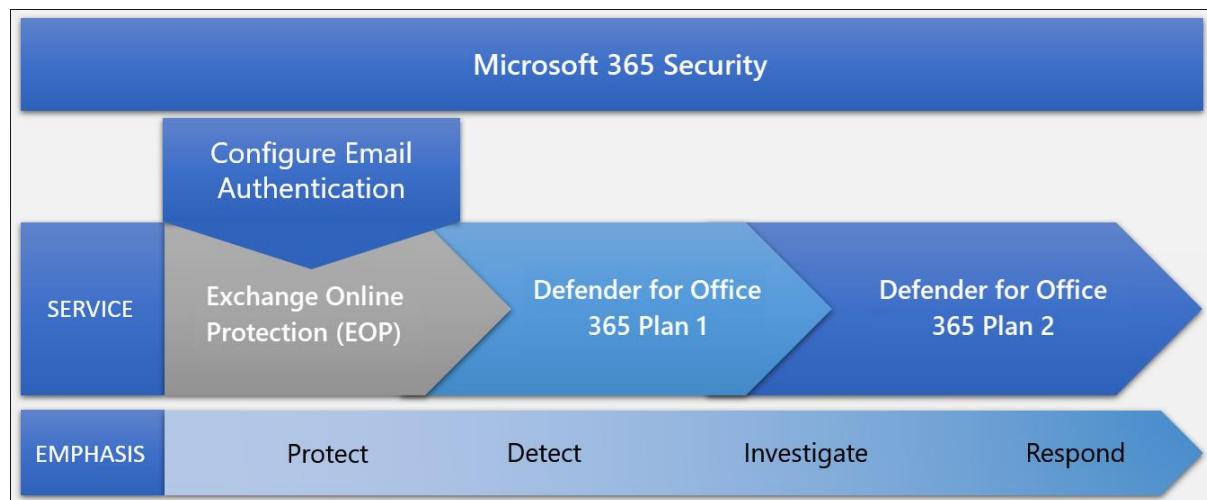


Microsoft Defender for Office 365 protection stack



- Edge Protection – still a crucial part of the stack, this phase is designed to block automatically as the 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.

The screenshot shows the Microsoft Defender Configuration Analyzer interface. The left sidebar lists various security categories like Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Reports, Learning hub, Trials, More resources, System, and Customize navigation. The main area is titled "Configuration analyzer" and contains a message about the analyzer's purpose and how to stay updated with recommendations. Below this, there are tabs for "Standard recommendations", "Strict recommendations", and "Configuration drift analysis and history". The "Standard recommendations" tab is selected. It displays four counts: 20 for Anti-spam, 16 for Anti-phishing, 2 for DKIM, and 1 for Outlook. A table below lists 39 items, each with columns for Recommendation, Policy, Policy group/setting name, Policy type, Current configuration, Last modified, and Status. The table includes rows for various anti-spam and anti-phishing configurations such as "Move to Junk Email folder", "Invalid date", and "Not started".



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

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

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

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

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

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



The screenshot shows the Microsoft Defender Threat policies page. On the left is a navigation sidebar with sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Reports, and Learning hub. The main content area is titled "Threat policies" and includes sections for "Templated policies" (Preset Security Policies, Configuration analyzer) and "Policies" (Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, Safe Links). Below these are sections for "Rules" (Tenant Allow/Block Lists, Email authentication settings, Advanced delivery, Enhanced filtering, Quarantine policies).

This screenshot shows the "Preset security policies" section within the Threat policies. It features three tabs: "Built-in protection" (selected), "Standard protection", and "Strict protection". The "Built-in protection" tab shows a shield icon and a note: "Built-in Microsoft Office 365 security applied to all users in your organization to protect against malicious links and attachments." It lists features: Additional machine learning models, More aggressive detonation evaluation, Visual indication in the experience, and a note: "Note: Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants." The "Standard protection" tab shows a group of people icon and a note: "A baseline protection profile that protects against spam, phishing, and malware threats." It lists features: Balanced actions for malicious content, Balanced handling of bulk content, Attachment and link protection with Safe Links and Safe Attachments, and a note: "Standard protection is on". The "Strict protection" tab shows a group of people with a lock icon and a note: "A more aggressive protection profile for selected users, such as high value targets or priority users." It lists features: More aggressive actions on malicious mail, Tighter controls over bulk senders, and More aggressive machine learning, with a switch labeled "Strict protection is off". A "Manage protection settings" button is also present.

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

This screenshot shows the "Safe attachments" policy setup page. The left sidebar includes sections like connectors, Investigation & response, Alerts, Advanced hunting, Custom detection rules, Items & submissions, Threat intelligence, Assets, and Microsoft Sentinel. The main content area is titled "Safe attachments" and includes a note: "We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. View preset security policies". It shows a table of existing policies: "Defender for Office 365 Evaluation" (Status: On), "Safe Attachment policy Test" (Status: On), and "Built-in protection (Microsoft)" (Status: On). The right side has a "Global settings" section with options: "Protect files in SharePoint, OneDrive, and Microsoft Teams" (switch on), "Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams" (switch on), "Help people stay safe when trusting a file to open outside Protected View in Office applications" (switch on), and "Allow people to click through Protected View even if Safe Documents identified the file as malicious" (switch on). Buttons for "Save" and "Cancel" are at the bottom.

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

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



Apply strict protection

<ul style="list-style-type: none"><input checked="" type="radio"/> Exchange online protection<input type="radio"/> Defender for Office 365 protection<input type="radio"/> Impersonation protection<input type="radio"/> Policy mode<input type="radio"/> Review	<h3>Apply Exchange Online Protection</h3> <p>Add the users, groups, and domains to protect using Exchange Online Protection capabilities, including inbound anti-spam, anti-malware, and anti-phishing. Learn more about preset security policies</p> <p>Apply protection to:</p> <p><input type="radio"/> All recipients <input checked="" type="radio"/> Specific recipients</p> <p>Users [Text input field]</p> <p>And</p> <p>Groups [Text input field]</p> <p>And</p> <p>Domains [Text input field]</p> <p><input type="radio"/> None</p> <p><input type="checkbox"/> Exclude these recipients</p>
--	---

Onboard MDO – Steps 1-8

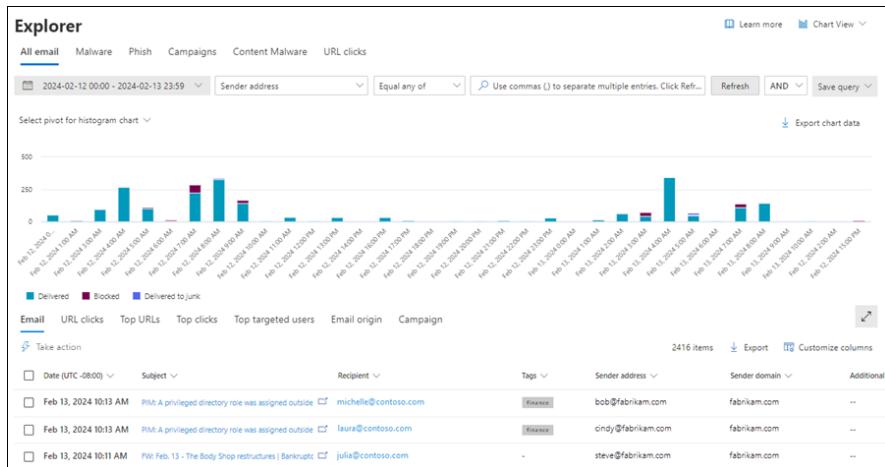
In this section, we will do a lot of fine tuning, make a decision to add more users to your pilot group but first things first, ensure that the right folks have the right permission. Just like with all of our Defender stack, each one has certain roles you can assign, for the simple reason that you may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

Policies & rules > Threat policies > Anti-phishing

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing policies to increase the prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority [phishing policies](#).

0 impersonated domain(s) and user(s) over the past 7 days. [View impersonations](#)

+ Create Export Refresh

Name	Status
Standard Preset Security Policy	On
Defender for Office 365 Evaluation	On
Anti-phishing test group	On
Office365 AntiPhish Default (Default)	Always on

Edit protection settings

Set your phishing thresholds and desired impersonation and spoof protections for this policy. [Learn more](#)

Phishing email threshold 1 - Standard

This is the default value. The severity of the action that's taken on the message depends on the degree of confidence that the message is phishing (low, medium, high, or very high confidence).

Impersonation

Enable users to protect (0/350) [Enable impersonation protection for up to 350 internal and external users.](#) [Learn more about adding users to impersonation protection](#) [Manage 0 senders](#)

Enable domains to protect (0) [Enable impersonation protection for these internal and external sender domains.](#) [Manage 0 custom domains](#)

Add trusted senders and domains (0) Add trusted senders and domains so they are not flagged as an impersonation-based attack [Manage 0 trusted sender\(s\) and domain\(s\)](#)

Enable mailbox intelligence (Recommended) Enables artificial intelligence (AI) that determines user email patterns with their frequent contacts to identify potential impersonation attempts. [Learn more](#)

Enable Intelligence for impersonation protection (Recommended) Enables advanced impersonation results based on each user's individual sender map and allows you to define specific actions on impersonated messages

Spoof

Enable spoof intelligence (Recommended) Choose how you want to filter email from senders who are spoofing domains. To control which senders are allowed to spoof your domains or external domains, use the [Instant Allow/Block List Spoofing page](#). [Learn more about Spoof Intelligence](#)

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



The screenshot shows the Microsoft Defender for Office 365 interface. On the left, there's a navigation bar with 'Home' and 'Incidents & alerts'. The main area is titled 'Multi-stage incident involving Initial access & Collection on one endpoint reported by multiple sources'. It shows '16/19 active alerts', '6 MITRE ATT&CK tactics', and '1 other alert categories'. Below this is a chart with colored bars representing different alert types. A sidebar on the right is titled 'Incident Information' and contains sections for 'Tags summary', 'Incident tags' (with 'Chain Event Detection' and 'CAAttack' selected), 'Incident details' (Status: Active, Severity: High, Incident ID: 11479, First activity: Jan 28, 2022, Last activity: Jan 28, 2022, Classification: Not set, Determination: Not set, Assigned to: Unassigned), and 'Evidence' (21 entities found).

Be Proactive

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

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

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

USERS

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

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

SOC Team + Change Management

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

Once the dust settles from your MDO migration. Attack Sim needs to be part of your MDO adoption or Phase 2 of your MDO migration. One of the coolest and critical 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

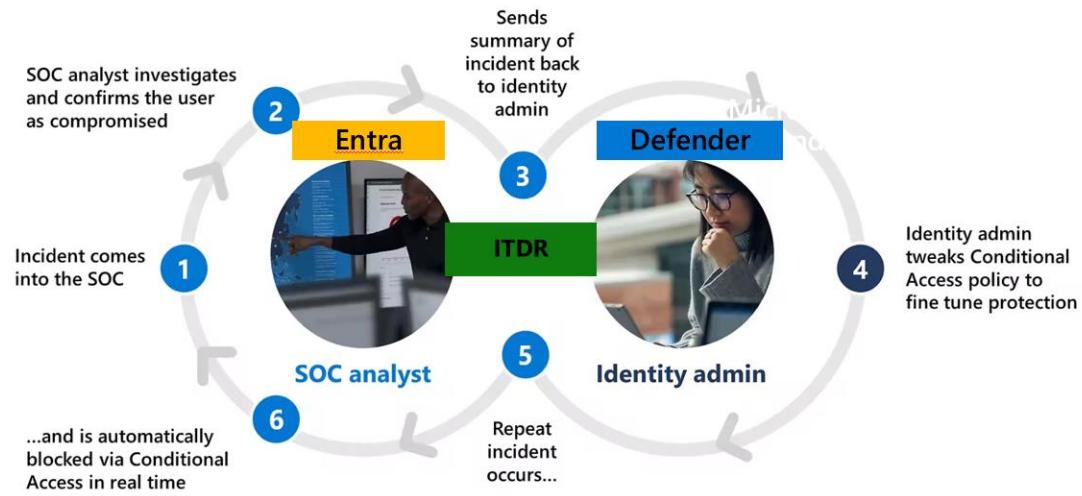
- Capacity planning! Crucial on the early stages on this deployment, importance on ensuring opening up those pre-reqs, network ports 443 and sizing tool for all your servers you want to install the sensors on.
- Don't run the sensors on those servers that need more specs, upgrade them before you install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

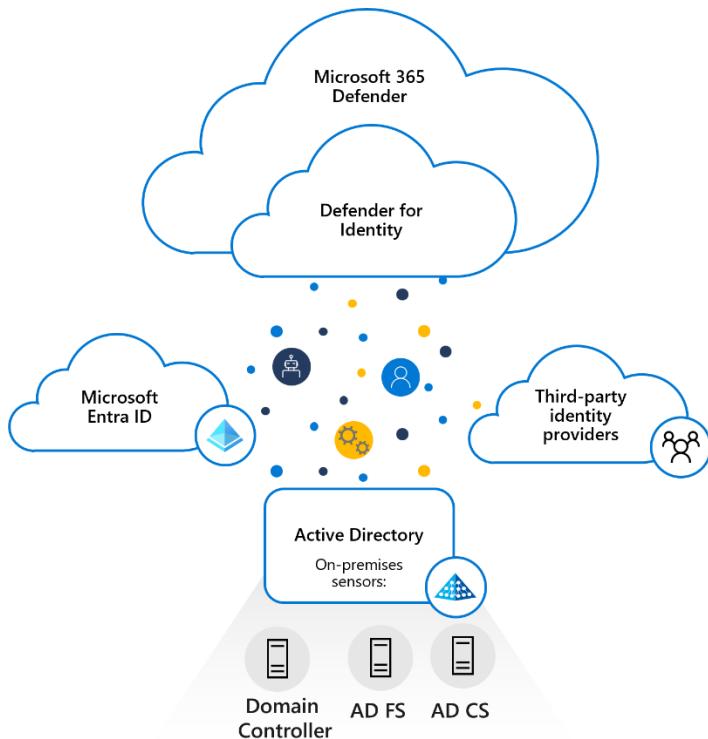
The time deploying this product depends on how large your organisation is based on the number of DCs, ADFS, ADCS and where I often see customers hit some delays are upgrading some of the servers that require more specs, and the back and forth change request can slow things down in the beginning. One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

Step 3. Install and configure the sensor in DC

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



Microsoft Defender for Identity

Sensor	Type	Domain	Service status	Sensor status	Version	Delayed update	Health status	Health issues	Created
DC2	Domain controller Sensor	domain1.test.local	Running	Up to date	2.185.15524.950	Disabled	● Healthy	0	Jul 21, 2022 6:08 PM
STANDALONE	Standalone Sensor	domain1.test.local	Running	Up to date	2.184.15495.42267	Enabled	● Healthy	0	Mar 6, 2022 3:22 PM
DC4	Domain controller Sensor	domain1.test.local	Running	Up to date	2.185.15524.950	Disabled	● Healthy	0	Jul 21, 2022 6:07 PM

Install sensor on ADFS and ADCS if this is still applicable to you, we won't dive too deep on this but touch base on the detection you can enable [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.



MDI detects identity attacks throughout different phases:

Initial Access	Credential Access	Lateral Movement	Defense Evasion
Suspicious VPN Connection	Suspected NTLM authentication tampering	Suspected use of Metasploit hacking framework	Suspected DCShadow attack (domain controller promotion)
Discovery	Suspected brute-force attack (SMB)	Suspected WannaCry ransomware attack	Suspected DCShadow attack (domain controller replication request)
Account enumeration reconnaissance	Suspected AD FS DKM key read	Remote code execution attempt over DNS	Suspected SID-History injection
Network mapping reconnaissance (DNS)	Suspected AS-REP Roasting attack	Abnormal Exchange attribute change	
User and IP address reconnaissance (SMB)	Suspicious Kerberos delegation attempt using BronzeBit method	Suspected Netlogon privilege elevation attempt	
Security principal reconnaissance (LDAP)	Suspected brute-force attack (Kerberos, NTLM)		
User and group membership reconnaissance (SAMR)	Suspected DFSCoerce attack using Distributed File System Protocol		
Active Directory attributes Reconnaissance using LDAP	Suspected DCSync attack		
Honeytoken activity	Suspected Golden Ticket usage		
Privilege Escalation	Suspected Kerberos SPN exposure		
Suspicious modification of dNSHostName attribute	Suspected brute-force attack (LDAP)		
Suspicious Kerberos delegation attempt	Suspected NTLM relay attack (Exchange Server account)		
Suspicious modification of the RBCD attribute	Suspected skeleton key attack		
Suspicious modification of a SAMNameAccount	Malicious request of Data Protection API (DPAPI) master key		
Suspicious modification of the trust relationship of AD FS server	Suspected rogue Kerberos certificate usage		
	Suspicious Kerberos ticket request		

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.

Suspicious Domain-Controller certificate request (ESC8)

DC1
Source Host

...
CLIENT2
Related Host

...
DC2
Destination Host

Alert story

What happened

DC1 (Domain Controller) on CLIENT2 requested a certificate from DC2.

Alert graph

```

graph LR
    DC1((DC1)) -- "On" --> CLIENT2((CLIENT2))
    CLIENT2 -- "successfully requested the certificate from" --> DC2((DC2))
    
```

Important information

- This attack method is primarily combined with NTLM relay attack, in which DC authentication is coerced and relayed to ADCS server.
- The attack can be mitigated by revoking the certificate.
- The AD CS server which processed the requests was DC2.
- DC1 is a Domain Controller.
- Certificates details:
 - Issue date: 11/8/23 11:42 AM. Subject Key Identifier: c7 9e 20 ac f3 c4 b6 c7 5a 12 fe 96 ce bd 53 e6 00 fa b3 c5. Request ID: 404. Enrollment Method: Certsrv

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](#)

The screenshot shows the 'Adjust alerts thresholds' page in Microsoft Defender for Identity. On the left, a sidebar lists various categories like General, Sensors, Directory services accounts, Manage action accounts, VPN, Health issues, Entity tags, Actions and exclusions, and Notifications. The 'Adjust alerts thresholds' option is highlighted. The main area displays a table of alerts with columns for Alert name, Threshold level, and Information. Each alert entry includes a dropdown menu for changing the threshold level. The 'Information' column provides a brief description of each alert's behavior based on the threshold level. At the top of the main area, there is a toggle button for 'Recommended test mode' and a 'Revert to default' button.

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

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



The screenshot shows the Microsoft 365 Defender interface for identity protection. On the left, there's a navigation sidebar with various options like Cloud apps, Cloud discovery, OAuth apps, App governance, Files, Activity log, Governance log, Policies, Reports, Health, Permissions, Settings (which is selected), More resources, and Customize navigation. The main area is titled 'Microsoft Defender for Identity' under 'General'. It includes sections for Health issues, About, Report management, Entity tags (with 'Sensitive' highlighted), Actions and exclusions (Global excluded entities, Exclusions by detection rule, Automated response exclusions), and Notifications. To the right, a modal window titled 'Tag user accounts' is open, prompting the user to 'Select which accounts to tag as Sensitive'. It lists users such as Oscar King, Guest, Karla Dickens, Dan Williams, MSOL_6b1f8fac19d3, Stevie Beavers, Clem Jones, antoine j DEL:545680, and DefaultAccount. There are columns for Name, Domain, and UPN Name. A red box highlights the 'Tag users' button and the 'Add selection' button at the bottom of the modal.

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 P1 features at a glance

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



Entra P2 features at a glance

Identity Protection		Identity Governance		
Identity Protection	Risk-based Conditional Access	Access Reviews	Privileged Identity Management	Entitlement Management
<p>Detect risky sign-ins and risky user accounts.</p> <p>Provide easy Access to remediation actions such as password resets.</p>	<p>Use Conditional Access policies to mitigate risky sign-ins and risky users by either:</p> <ul style="list-style-type: none"> - Blocking sign-ins - Requiring MFA challenges - Requiring password resets 	<p>Ensure the right users have the right access to the right resources by using advanced identity governance features to control group and roles memberships.</p>	<p>Enforce on-demand, just-in-time administrative access when needed.</p>	<p>Allow employees to request and have time-Limited Access across groups, apps and SPO sites.</p> <p>Allow users from Business Partners to do the same via an approval workflow.</p>

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	<ul style="list-style-type: none"> 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. 	<p>Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more</p> <table border="1"> <tr> <td>User risk level</td><td>Not configured</td></tr> <tr> <td>Sign-in risk level</td><td>Not configured</td></tr> </table>	User risk level	Not configured	Sign-in risk level	Not configured
User risk level	Not configured						
Sign-in risk level	Not configured						
Sign-in Risk	Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner	<ul style="list-style-type: none"> 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](https://entra.microsoft.com/#home)

The screenshot shows the Microsoft Entra admin center homepage. On the left, there's a navigation sidebar with links like Home, What's new, Diagnose & solve problems, Favorites, Identity, Protection, and Identity governance. Under Protection, the Conditional Access link is highlighted with a yellow box. The main content area features a large blue and white graphic with the word "Contoso". Below it, there's a section titled "Learn about Microsoft Entra" and "Explore the Microsoft Entra product family". A call-to-action button at the bottom says "View all products" and "Read documentation".

This screenshot shows the "Conditional Access | Overview" page. The left sidebar has the same navigation as the previous screen. The main content area is titled "New" and shows a "Conditional Access policy" named "Reyes RBCA". It includes sections for "Assignments" (Users: All users, Target resources: No target resources selected), "Conditions" (2 conditions selected), and "Access controls" (Grant: 1 control selected, Session: 0 controls selected). To the right, there's a "Sign-in risk" configuration panel with options for "Configure" (Yes or No) and "Sign-in risk level" (High, Medium, Low, No risk). A note says "Sign-in risk level is generated base real-time risk detections".



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.

The screenshot shows the Microsoft Defender interface with the 'Identities' page selected. The left sidebar has sections like Threat intelligence, Assets (with Identities highlighted), Microsoft Sentinel, and Email & collaboration. The main area is titled 'Identities' with a search bar and filters for User name, Affiliation (Internal or External), Type (User or Account), App (Select apps), and Groups (Select user group). A table lists 648 users, sorted by Investigation priority (descending). The columns include User name, Investigation priority, Affiliation, Type, Email, and Apps. Allan Deyoung has the highest priority at 4. Other users listed include Adele Vance, Grady Archie, Alex Wilber, Isaiah Langer, MOD Administrator, Megan Bowen, and Nestor Wilke, all with a priority of 0.

User name	Investigation priority	Affiliation	Type	Email	Apps
Allan Deyoung	4	Internal	User	alland@msdx170521.onmicrosoft.com	Office 365
Adele Vance	3	Internal	User	adelev@msdx170521.onmicrosoft.com	Office 365
Grady Archie	3	Internal	User	gradya@msdx170521.onmicrosoft.com	Office 365
Alex Wilber	3	Internal	User	alexw@msdx170521.onmicrosoft.com	Office 365
Isaiah Langer	0	Internal	User	isaiahl@msdx170521.onmicrosoft.com	Office 365
MOD Administrator	0	Internal	User	admin@msdx170521.onmicrosoft.com	Office 365, SharePoint
Megan Bowen	0	Internal	User	meganb@msdx170521.onmicrosoft.com	Office 365
Nestor Wilke	0	Internal	User	nestorw@msdx170521.onmicrosoft.com	Office 365

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

The screenshot shows the 'Allan Deyoung' user details page. It features a circular profile picture with 'AD' initials. Below it, the name 'Allan Deyoung' is displayed in large red font, with 'IT Admin | Type: User' below it. The page has tabs for Overview, Incidents and alerts, Observed in organization (which is selected and underlined in blue), and Timeline. Under 'Observed in organization', there are sections for Devices (0), Locations (0), Groups, and a highlighted 'Lateral movements' section. The 'Lateral movements' section is highlighted with a yellow background and contains a small icon and some text.



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.

The screenshot shows the Microsoft Entra ID user details page for a user named Allan Deyoung. The user is an IT Admin and is categorized as a User. The page displays Entity details, Incidents and alerts (which shows 'No incidents and alerts'), and Active Directory account controls. A context menu is open on the right side, listing various response actions such as 'Confirm user compromised', 'Suspend user in Azure AD', and 'Require user to sign in again'. A red arrow points from the text above to this menu.

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

The screenshot shows the Microsoft Defender XDR Settings page under Alert service settings. It displays options for Microsoft Entra ID Protection, where 'High-impact alerts only (Default)' is selected, and Microsoft Defender for Cloud alerts. A red arrow points from the text above to this page.



New ITDR Dashboard

The screenshot shows the Microsoft Defender ITDR Dashboard. On the left is a navigation sidebar with categories like Hunting, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Exposure management, Assets, Endpoints, Identities, Dashboard, Health issues, Tools, Email & collaboration, and Investigations. The main area has a title 'ITDR Dashboard' with a sub-section 'This dynamic dashboard is offering a centralized view of critical insights and real-time data about identity threat detection and response. By providing an intuitive interface that showcases important information related to unauthorized access, account compromise, insider threats and abnormal activities, our dashboard enables you to proactively monitor and manage potential identity-related security risks.' Below this is a large map-like visualization showing user distribution across three environments: Cloud Users (1,209), On-Premises Users (1,010), and Hybrid Users (1,024). At the bottom, there's a 'Top Insights' section with two items: '0 users were identified in a risky lateral movement path' and '7 users are considered dormant in AD and should be removed from sensitive groups'. Below these are sections for 'ITDR Deployment Health', 'Identity posture (Secure score)', and 'Highly privileged identities'. The secure score is listed as 'Identity: 47.07%'. The highly privileged identities section shows counts for 'Entra ID Global Admin' (17), 'Entra ID Security Administrator' (5), and 'Tagged as sensitive' (16).

Important to note and consider

Microsoft Entra Suite

Important Update. 06.08.2024

What is Microsoft Entra Suite?

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

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

The Microsoft Entra Suite includes the following products:

Microsoft Entra Suite

- Microsoft Entra Private Access**
Zero Trust Network Access
- Microsoft Entra Internet Access**
Secure Web Gateway
- Microsoft Entra ID Governance**
Identity Governance and Administration
- Microsoft Entra ID Protection**
Identity Protection
- Microsoft Entra Verified ID (Premium capabilities)**
Identity Verification



- [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?

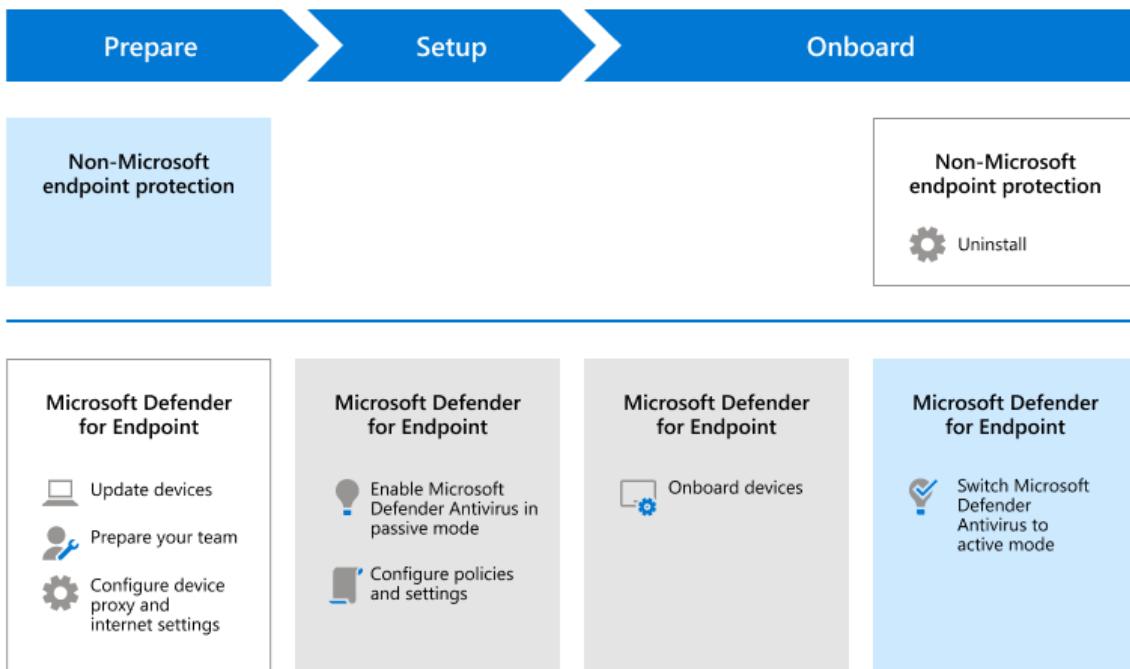
But before we jump talking about what these P2 features mean we need to onboard the devices first to MDE

Microsoft Defender for Endpoint					
[...] Expand table					
					
Core Defender Vulnerability Management	Attack surface reduction	Next-generation protection	Endpoint detection and response	Automated investigation and remediation	Microsoft Threat Experts
Centralized configuration and administration, APIs					
Microsoft Defender XDR					

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

The Migration Process

Migration process



Preparing Phase

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

Setup Phase

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

Onboarding Phase

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

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

Endpoint	Deployment tool
Windows	Local script (up to 10 devices) Group Policy Microsoft Intune/ Mobile Device Manager Microsoft Configuration Manager VDI scripts
Windows servers	Integration with Microsoft Defender for Cloud
Linux servers	
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 onboard 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 for Intune | Microsoft Learn](#)

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

The screenshot shows the Microsoft Defender for Endpoint interface. On the left, there's a navigation sidebar with various options like Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Reports, Learning hub, Trials, More resources, System, Audit, Permissions, Health, and Settings. The 'Settings' option is currently selected. In the main area, the 'Endpoints' section is open under 'Advanced features'. A list of features is shown with toggle switches: 'Live Response' (On), 'Live Response for Servers' (On), 'Live Response unsigned script execution' (Off), 'Deception' (Off), 'Share endpoint alerts with Microsoft Compliance Center' (Off), 'Microsoft Intune connection' (On), 'Authenticated telemetry' (On), 'Preview features' (On), and 'Endpoint Attack Notifications' (On). An 'Apply' button is at the bottom right.

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

The screenshot shows the Microsoft Defender for Endpoint security dashboard. At the top, there's a search bar, refresh, save, discard, and delete buttons. Below that, the 'Overview' section includes links for 'Overview', 'All devices', and 'Security baselines'. To the right, there's a 'Connection status' card showing 'Available' and 'Last synchronized' at '29/04/2024, 6:52:53 pm'. A blue shield icon with a lightning bolt is displayed next to the status information.



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

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

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



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

How to create a profile and using the MDE Baseline

The screenshot shows two pages from the Microsoft Intune admin center:

- Endpoint security | Security baselines**: A list of security baselines:

	Version
Security Baselines	
Security Baseline for Windows 10 and later	Version 23H2
Microsoft Defender for Endpoint Baseline	Version 6
Security Baseline for Microsoft Edge	Version 117
Windows 365 Security Baseline	November 2021
Microsoft 365 Apps for Enterprise Security Baseline	Version 2306
- Microsoft Defender for Endpoint baseline | Profiles**: A list of profiles:

Profile Name	Current Baseline	Assigned
MDE Baseline	Version 6	No

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

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

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



Microsoft Intune admin center

Home > Endpoint security | Security baselines > Microsoft Defender for Endpoint baseline | Profiles > Guide v6 | Properties >

Edit profile

1 Configuration settings (2) Review + save

Settings

Search for a setting

Attack Surface Reduction Rules

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

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

Microsoft Intune admin center

Home > Endpoint security | Security baselines > Microsoft Defender for Endpoint baseline | Profiles >

Create profile

Microsoft Defender for Endpoint baseline

Basics Configuration settings Scope tags Assignments (5) Review + create

Included groups

Add groups Add all users Add all devices

Groups	Group Members <small>(1)</small>	Remove
MDE Test group	0 devices, 0 users	Remove

Excluded groups

i When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

Add groups

Groups	Group Members <small>(1)</small>	Remove
No groups selected		



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

The screenshot shows the Microsoft Defender interface under the 'Reports' section. The left sidebar contains navigation links for Overview, Attack surface, Exposure insights, Secure score, Data connectors, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Reports, Learning hub, Trials, and More resources. The main content area is titled 'Reports' and displays a list of reports categorized by type. The 'Attack surface reduction rules' report is highlighted with a yellow box. Other visible reports include Security report, Query resources, Device health, Vulnerable devices, Monthly security summary, Web protection, Firewall, Device control, and Email & collaboration reports.

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

The screenshot shows the Microsoft Defender interface under the 'Detections' tab of the 'Attack surface reduction rules' report. The left sidebar is identical to the previous screenshot. The main content area shows a bar chart with 'Audited detections' (0) and 'Blocked detections' (5). Below the chart is a table with 5 items, each showing details about a blocked detection:

Detected file	Detected on	Blocked/Audited?	Rule	Source app	Device	Device group	User	Publisher
WaAppAgent.exe	28 Apr 2024 17:51	Blocked	Block credential stealing from the ...	WaAppAgent.exe	client2.Rc.lab	UnassignedGroup	SYSTEM	Microsoft Corporation
Dropbox.exe	27 Apr 2024 21:09	Blocked	Block credential stealing from the ...	Dropbox.exe	client2.Rc.lab	UnassignedGroup	SYSTEM	Microsoft Corporation
WaAppAgent.exe	23 Apr 2024 04:03	Blocked	Block credential stealing from the ...	WaAppAgent.exe	client2.Rc.lab	UnassignedGroup	SYSTEM	Microsoft Corporation
Dropbox.exe	23 Apr 2024 04:02	Blocked	Block credential stealing from the ...	Dropbox.exe	client2.Rc.lab	UnassignedGroup	SYSTEM	Microsoft Corporation
WaAppAgent.exe	23 Apr 2024 03:58	Blocked	Block credential stealing from the ...	WaAppAgent.exe	client2.Rc.lab	UnassignedGroup	SYSTEM	Microsoft Corporation



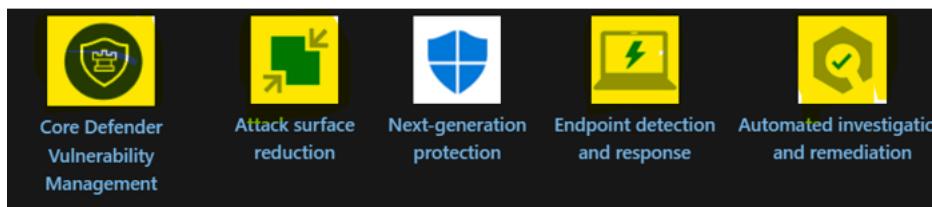
You can get the location you need on the bottom right.

The screenshot shows the Microsoft Defender interface with the left sidebar expanded. Under 'Investigation & response', 'Attack surface reduction' is selected. The main area displays a table of detected files:

File name	Detections	Devices
WaAppAgent.exe	3	1
Dropbox.exe	2	1

Below the table, there's a summary section with a bar chart comparing 'Actual detections' (4) and 'Detections after exclusions' (2). A pie chart shows '1 affected device'. At the bottom, there are buttons for 'Add exclusions' and 'Get selected exclusion paths'.

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



Incidents > Multi-stage incident involving Initial access & Collection on one endpoint reported by multiple sources

Multi-stage incident involving Initial access & Collection on one endpoint reported by multiple sources...

Manage incident Ask Defender Experts Comments and history

Attack story Recommended actions (21) Alerts (11) Assets (0) Investigations (0) Evidence and Response (25) Summary

Alerts

Incident graph Layout Group similar nodes

Communication Association

Link to incident Take actions Manage alerts Open in advanced hunting

1 of 3 selected Search Customize columns

Timestamp	Alert ID	Title	Category	Severity	ServiceSource	DetectionSource	AttackTechnique	DeviceID
May 1, 2024 10:00:00	6438370002567	User compromised in Al...	CredentialAccess	High	Microsoft Defender for ...	Microsoft 365 Defender	[Initial Web Session Co...	00000000-0000-0000-0000-000000000000
May 1, 2024 10:00:00	64383700448101	Suspicious URL clicked	InitialAccess	High	Microsoft Defender for ...	Microsoft 365 Defender	[Spanning Tree (ST)	00000000-0000-0000-0000-000000000000
May 1, 2024 10:00:00	6438370024520	Connection to a suspicious...	CredentialAccess	High	Microsoft Defender for ...	EDR	[Phishing (T1566)]	00000000-0000-0000-0000-000000000000

Incident details

Assigned to Incident ID

Classification Categories

First activity Last activity

Impacted assets

Devices (0) Risk Score

Users (0)

App (0) Application ID Risk

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

Microsoft Defender

Device Inventory > client1

client1

Low Criticality: None Active Priority Group

Overview Incidents and alerts Timeline Security recommendations Inventories Discovered vulnerabilities Missing KBs Security policies

VM details

Domain: ItLab OS: Windows 10 64-bit (Release 21H2 Build 19044.2570)

SAM name: CLIENT1\$ Asset group:

Health state: Active Created on: 4 Jun 2021 07:17:29

Data sensitivity: None IP addresses: 10.96.82.5 See IP addresses info

First seen: 26 Jun 2022 Last seen: 29 Apr 2024 03:53:10

Onboarding status: Onboarded Resources

Device AAD id: Device id: 8e2950fb-086-302d8130cc5f360fb

Defender engine version: 1.1.24030.4 Endpoint DLP status: Not available

Risk level: Low

Exposure level: High

Active alerts (Last 180 days): 2 active alerts, 2 active incidents

Security assessments: 31 active security recommendations

Most logons: 1 logger (F user, Local admin)

Least logons: F user, Local admin

Newest logon: F user, Local admin

View all incidents and alerts View all recommendations

Device health status: Full scan status is unknown

Type State Date & time

Last full scan: No scan performed

Last quick scan: Completed 23 Apr 2024 10:32:42

Security intelligence: Version 1.409.589.0 28 Apr 2024 20:07:43

Engine: Version 1.1.24030.4 28 Apr 2024 20:07:44

Platform: Version 4.18.24030.9 23 Apr 2024 04:10:28

Defender Antivirus mode: Active 29 Apr 2024 03:51:01

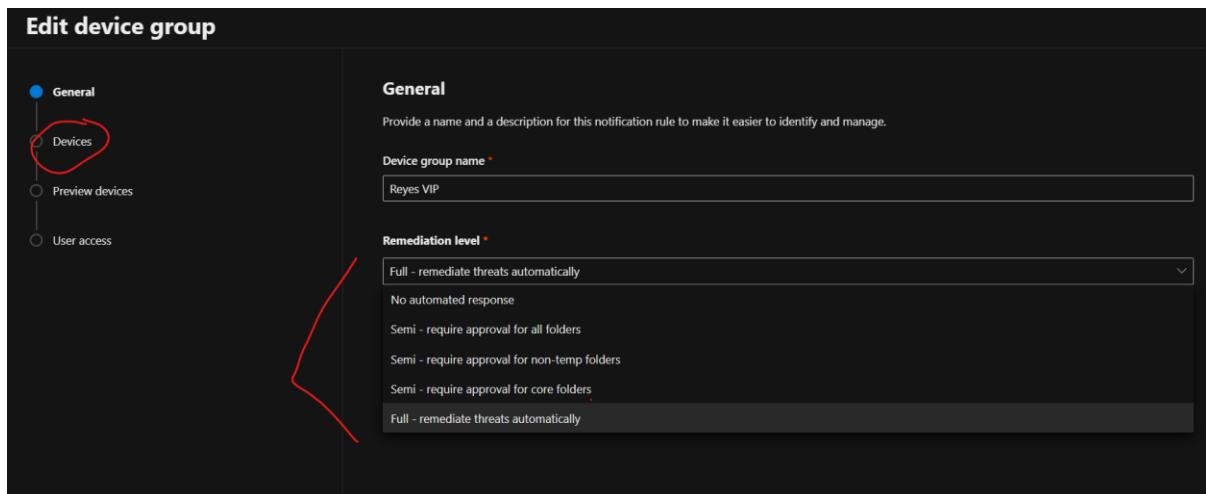
Actions menu (right side):

- View in map
- Device value
- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Ask Defender Experts
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync



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 Event 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.

The screenshot shows the Microsoft Defender interface under the 'Vulnerability management' section. The 'Remediation' tab is selected. On the left, the navigation menu includes 'Investigation & response', 'Threat intelligence', 'Assets', 'Microsoft Sentinel', 'Endpoints', 'Vulnerability management' (with 'Dashboard' and 'Recommendations' selected), 'Partners and APIs', and 'Configuration management'. The main content area is titled 'Inventories' and shows 'Windows 10' details. It includes sections for 'Software details' (44 items), 'Exposed devices' (3/3), 'Associated CVEs' (10 Critical, 282 High, 123 Medium, 6 Low), and 'Threat context' (Exploits available: Yes). A note at the bottom states: 'Some devices are running Windows 10 versions which will reach their end-of-support soon. Support and service will no longer be available for these versions after the upcoming dates. [details about Windows 10 version distribution](#)'.

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.

The screenshot shows the Microsoft Defender interface under the 'Vulnerability management' section. The 'Recommendations' tab is selected. The left navigation menu is identical to the previous screenshot. The main content area is titled 'Security recommendations' and shows a list of 58 items. Each item includes a checkbox, a title, and columns for 'OS platform', 'Weaknesses', 'Related component', 'Threats', 'Exposed devices', and 'Remediation' (status: Software update). Examples of recommendations include 'Update Microsoft Windows 10 (OS and built-in applications)', 'Update Microsoft .net Framework', and various security controls like 'Block executable files from running unless they meet a prevalence, age, or trusted list criterion'.

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>

The screenshot shows the Microsoft Defender interface under 'Settings > Endpoints'. On the left, a sidebar lists various security categories like Home, Exposure management, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, More resources, System, and Customize navigation. The 'Endpoints' section is selected. On the right, the 'Advanced features' tab is active. It contains several toggle switches for different features:

- Apply streamlined connectivity settings to devices managed by Intune and Defender for Cloud**: On
- Live Response**: On
- Live Response for Servers**: On
- Live Response unsigned script execution**: Off
- Deception**: On
- Share endpoint alerts with Microsoft Compliance Center**: On
- Microsoft Intune connection**: On
- Authenticated telemetry**: On

Each feature has a tooltip providing more information. At the bottom right is a 'Save preferences' button.

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](https://learn.microsoft.com/en-us/defender-endpoint/onboarding/windows-server)

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

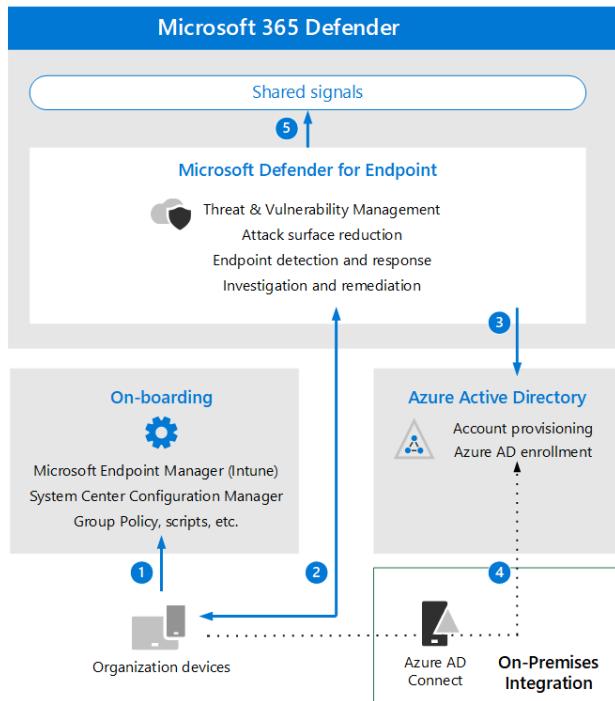
We have moved our demos in public docs. None of these actual files or links are malicious, they're intended to showcase what it would look like in the real world. This is good training for SOC juniors who may not have seen what the reaction of the security tools does.

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

Demonstrations			Expand table
#	Demonstration name	Protection area	
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





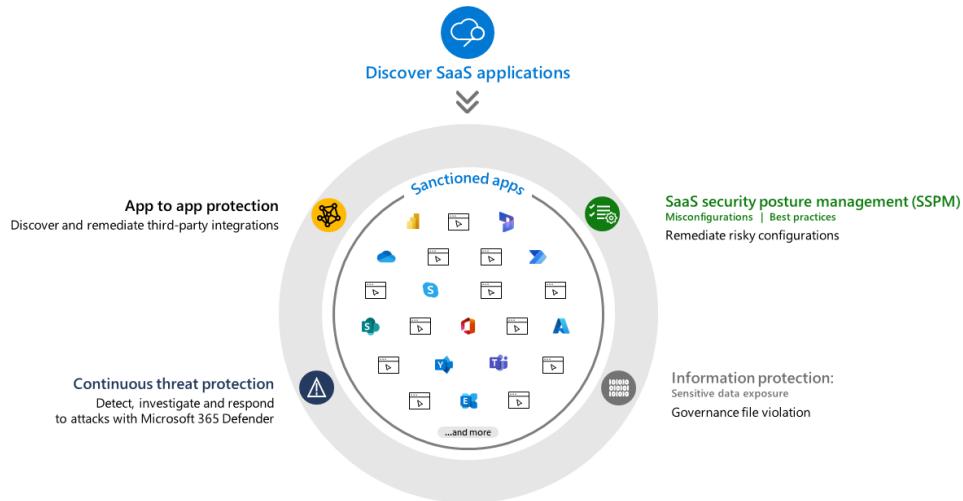
Phase 4. Microsoft Defender for Cloud Apps (MDA)

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.

Settings > Cloud apps

System

- About
- Organization details
- Mail settings
- Scoped deployment and privacy
- Preview Features
- IP address ranges
- User groups
- API tokens
- SIEM agents
- Playbooks
- My account**
- My email notifications
- Cloud Discovery**
- Score metrics**
- Snapshot reports

The level of the FedRAMP-compliant solution provided by this app.

CSA STAR level	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
Privacy Shield	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
ISO 27017	High (x4)	<input checked="" type="checkbox"/> Exclude N/A
FFIEC	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
ISO 27002	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
GAPP	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
COBIT	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A

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.

Settings > Cloud apps

System

- About
- Organization details
- Mail settings
- Scoped deployment and privacy
- Preview Features
- IP address ranges
- User groups
- API tokens
- SIEM agents
- Playbooks
- My account**
- My email notifications
- Cloud Discovery**
- Score metrics**
- Snapshot reports

HITRUST CSF

Does this app comply with HITRUST CSF, a set of controls that harmonizes the requirements of information security regulations and standards?

Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
-------------	---

Jericho Forum Commandments

Does this app follow Jericho Forum Commandments, a set of principles to be observed when architecting systems for secure operation in de-perimeterized environments?

Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
-------------	---

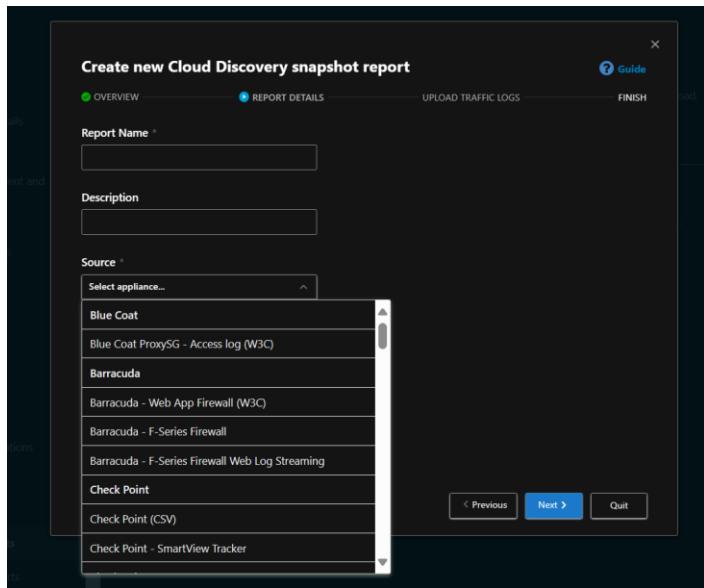
Legal

Category importance: Medium (x2)

Field	Importance	N/A values
Data ownership	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
DMCA	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A
Data retention policy	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/A

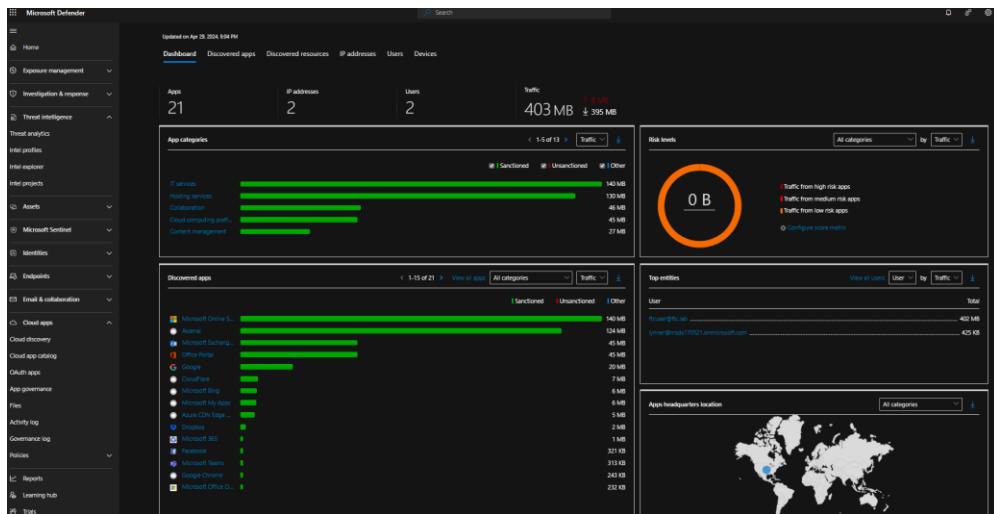
Snapshot reports is simply that, it's a sample report based on what source you may be thinking of using to digest the data from and the point of this is to give you what results it can digest. Again, our recommended log collector is MDE which is our native built-in agent which doesn't require much work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





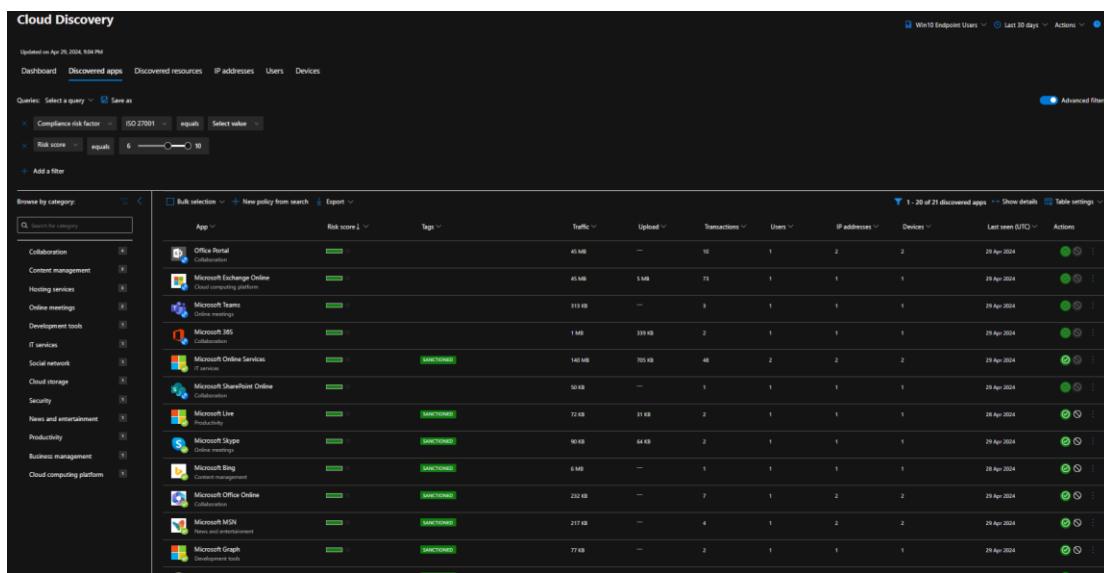
So with your devices already onboarded to MDE, it's a simple toggle. [Integrate Microsoft Defender for Endpoint - Microsoft Defender for Cloud Apps | Microsoft Learn](#)

Once you've enabled MDE, the data being absorbed 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 start 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 key feature in MDA is Connected Apps. We recommend connecting at minimum your M365 and Azure to get a deeper visibility on those platforms 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



The screenshot shows the Microsoft Defender interface. On the left, there's a navigation sidebar with various sections like Partners and APIs, Configuration management, Email & collaboration, Cloud apps, Reports, System, and more. The 'Cloud apps' section is expanded, showing sub-options like Preview Features, IP address ranges, User groups, API tokens, SaaS agents, Playbooks, My account, and Cloud Discovery. Under Cloud Discovery, there are Score metrics, Snapshot reports, Continuous reports, Automatic log upload, App Tags, Exclude entities, Microsoft Defender for Endpoint, User enrichment, Anonymization, and Delete data. Below these are Connected apps, App Connectors (which is highlighted), Conditional Access App Control apps, Information Protection, Admin quarantine, and Microsoft Information Protection. The main content area is titled 'App Connectors' and describes them as providing greater visibility and control over cloud apps. It includes a table showing 1-5 of 5 connected apps: Microsoft 365 Collaboration (Connected, 29 Apr 2024 08:20, 590 accounts), Microsoft Azure (Connected, 19 Sep 2022 18:26, 29 Apr 2024 08:24, 8 accounts), Salesforce (Connection error, 29 Feb 2024 04:08, — accounts), Dropbox (No recent status, 24 Jan 2024 11:44, — accounts), and Box (Connection error, 29 Feb 2024 04:10, — accounts). There are filters and table settings buttons at the top of the table.

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](#)

The screenshot shows the Microsoft Defender interface again. The left sidebar has sections like Exposure management, Investigation & response, Microsoft Sentinel, and Cloud apps. The 'Cloud apps' section is expanded, showing sub-options like Preview Features, IP address ranges, User groups, API tokens, SaaS agents, Playbooks, My account, and Cloud Discovery. Under Cloud Discovery, there are Score metrics, Snapshot reports, Continuous reports, Automatic log upload, App Tags, Exclude entities, Microsoft Defender for Endpoint, User enrichment, Anonymization, and Delete data. Below these are Connected apps, App Connectors, Conditional Access App Control apps, Information Protection, Admin quarantine, and Microsoft Information Protection. The main content area is titled 'Microsoft Secure Score' and shows a table of actions you can take to improve your Microsoft Secure Score. The table has columns for Rank, Recommended action, Score Impact, Points achieved, Status, Regressed, New found?, Category, Product, Last update, Microsoft update, and Notes. Actions listed include: Lockout effective period (Impact +0.2%, Points 0/7, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Require a minimum 1 day password lifetime (Impact +0.09%, Points 0/5, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Enforce login IP ranges on every request (Impact +0.09%, Points 0/5, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Disable Caching and Autocomplete on Login Page via Session settings (Impact +0.09%, Points 0/4, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Block OneDrive for Business sync from unmanaged devices (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product SharePoint Online, Last update 2/6/2024, Microsoft update None, Notes None); Ensure SharePoint external sharing is managed through domain whitelists/blacklists (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product SharePoint Online, Last update 2/6/2024, Microsoft update None, Notes None); Ensure that SharePoint guest users cannot share items they don't own (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product SharePoint Online, Last update 2/6/2024, Microsoft update None, Notes None); Enable clickjacking protection for customer Visualforce pages with standard head (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Enable clickjacking protection for customer Visualforce pages with headers disable (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Require HttpOnly attribute (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); Force (admin) relogin after Login As user (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None); and Enable XSS protection (Impact +0.02%, Points 0/3, Status No, Regressed Yes, New found? Yes, Category App, Product Salesforce - Salesforce1, Last update 1/4/2024, Microsoft update None, Notes None).



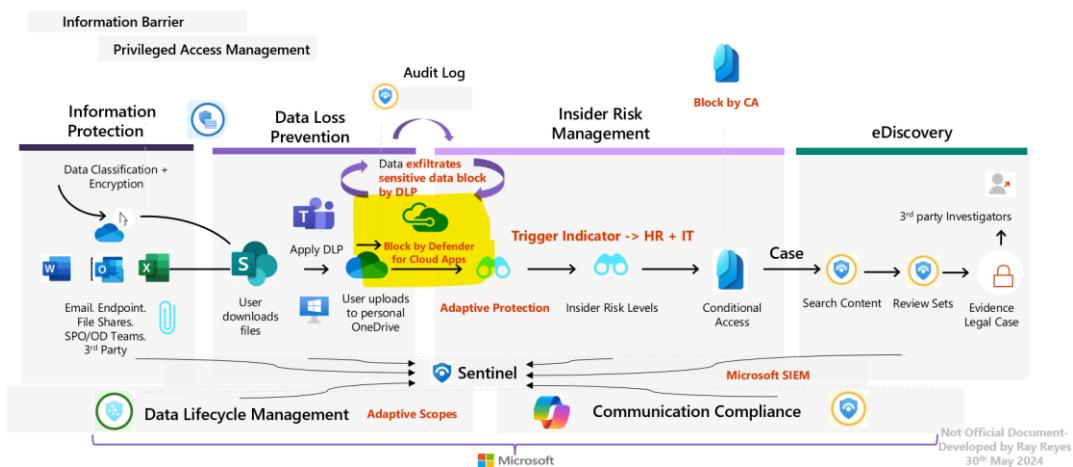
Information Protection

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

How Purview can fight against a Typical Internal Data Exfiltration

Microsoft Purview

A typical process using all Purview features



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](#)



The screenshot shows the Microsoft Defender Policy templates page. On the left is a navigation sidebar with various security categories like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, and Policies. Under Policies, 'Policy templates' is selected. The main area is titled 'Policy templates' and contains a search bar and filters for Type (Select type), Severity (orange, red, dark red), and Name (Template name). A dropdown menu for 'Category: Select risk category' is open, listing Threat detection, Privileged accounts, Compliance, DLP, Cloud Discovery, Sharing control, Access control, and Configuration control. Below this is a list of policy templates with descriptions and severity levels:

- Administrative activity from a non-corporate IP address
- Potential ransomware activity
- Block upload of potential malware (based on Microsoft Threat Intelligence)
- Block download of potential malware (based on Microsoft Threat Intelligence)
- Non-password protected shared links (Box)
- File shared with unauthorized domain
- Mass download by a single user
- Multiple failed user log on attempts to an app
- New popular app
- New high volume app
- New high upload volume app
- New risky app
- Collaboration app compliance check

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

The screenshot shows the 'Edit file policy' page. The left sidebar is identical to the previous one. The main area has a title 'Edit file policy' and a message 'Matched policies filter is no longer available.' It includes fields for 'Policy template' (No template), 'Policy name' (Reyes Co Publicly Shared Files), 'Policy severity' (orange, red, dark red), 'Category' (DLP), and a 'Description' text area. Below these are sections for 'Files matching all of the following' (Access level equals Public, External, Public (Internet)), 'Apply to' (all files), 'Select user groups' (all file owners), 'Inspection method' (None), and 'Alerts'. At the bottom is a checkbox for 'Create an alert for each matching file'.



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

The screenshot shows the Microsoft Defender policy creation interface. On the left, there's a navigation sidebar with options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Reports, Learning hub, Trials, More resources, and System. The main area is titled 'Policy name' with 'Rayes Co - Apply Sensitivity Label'. It includes 'Policy severity' (High) and 'Category' (DLP). A 'Description' field is empty. Below this, under 'Files matching all of the following', there are several filters. One filter is expanded, showing 'App equals' selected, with a dropdown menu listing various Microsoft 365 services: Microsoft Online Services, Microsoft 365, Microsoft Viva Engage, Microsoft OneDrive for Business, Microsoft SharePoint Online, Microsoft Exchange Online, Microsoft Skype for Business, and Microsoft Teams. Other filters include 'Select user groups: all file owners' and 'Inspection method: Data Classification Service'. There are also sections for 'Alerts' (checkbox for 'Create an alert for each matching file') and 'Governance actions' (checkbox for 'Microsoft OneDrive for Business'). At the bottom right, there's a 'Search' bar and a 'Save' button.

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.

The screenshot shows the Microsoft Defender policy templates interface. The left sidebar is identical to the previous screenshot. The main area is titled 'Policy templates' with a note to 'Manage all OAuth app policies, including policies for Azure AD, Google, and Salesforce go to [see previous]'. It features a 'Filters' section with 'Type: Select type' (All), 'Severity: High', 'Name: Threat detection', and 'Category: Threat detection'. Below this is a table of templates:

Template	Severity	Linked policies	Published
Administrative activity from a non-corporate IP address	High	0	8 Jan 2024 00:00
Internal reconnaissance activity	High	0	8 Jan 2024 00:00
Block upload of potential malware based on Microsoft Threat Intelligence	High	0	8 Jan 2024 00:00
Block download of potential malware based on Microsoft Threat Intelligence	High	0	8 Jan 2024 00:00
Mass download by a single user	High	0	8 Jan 2024 00:00
Multiple failed user log on attempts to an app	High	0	8 Jan 2024 00:00
Login from a risky IP address	High	0	8 Jan 2024 00:00
Access level change (Shared)	Medium	0	8 Jan 2024 00:00
Detect unauthorized accounts updating shared file expiration dates for files within a sensitive folder (Safex)	Medium	0	8 Jan 2024 00:00
Activities from suspicious user agents	Low	0	8 Jan 2024 00:00
External user added (Shared)	Low	0	8 Jan 2024 00:00
Mass deletion (Shared)	Low	0	8 Jan 2024 00:00

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.

This screenshot shows the 'Conditional Access App Control apps' section in the Microsoft Defender for Cloud Apps settings. It lists various Microsoft services and cloud providers as registered apps, each with a status (Connected or Not connected), possible controls (e.g., 'Block access to this app'), and last activity dates. The list includes Microsoft 365 Defender - General, Microsoft 365 Admin Center - General, Microsoft Exchange Online - General, Microsoft SharePoint Online - General, Microsoft OneDrive - General, Microsoft Teams - General, Microsoft Office 365 - General, and Office 365 - General.

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

This screenshot shows the Microsoft Entra admin center interface for creating a Conditional Access policy. The left sidebar navigation includes Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, Show more, Protection, and Conditional Access. The main content area is titled 'Session Control' under 'Conditional Access policy'. It includes sections for 'Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.' and 'Control access based on all or specific network access traffic, cloud apps or actions.' A 'Learn more' link is provided. The policy configuration includes fields for 'Name' (set to 'Session Control'), 'Assignments' (specific users included), 'Target resources' (1 app included, with 'Salesforce' selected), 'Conditions' (2 conditions selected), 'Access controls' (Grant: Block access), and 'Session' (Use Conditional Access App Control). A note at the bottom states 'Control access based on all or specific network access traffic, cloud apps or actions.'

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.

The screenshot shows the Microsoft Defender App governance interface. On the left, there's a navigation sidebar with various security modules like Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, and Email & collaboration. Under the App governance section, there are tabs for Overview, Azure AD, Salesforce, Alerts, and Policies. The Overview tab is selected, displaying a summary of apps found (14 apps found), overprivileged apps (4 overprivileged apps), and highly privileged apps (5 highly privileged apps). It also shows latest incidents (1 unresolved incidents, 0 threat incidents, 1 policy incidents) and a list of apps with columns for App name, App status, Permission type, Consent type, Publisher, Last modified, Added on, Permission usage, Data usage, and Privilege level. A section for 'Your predefined policies are...' shows 'No items to show'. Another section for 'Sensitive data accessed' also shows 'No items to show'. The right side of the interface has sections for 'Data usage' and 'No items to show'.

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

This screenshot shows a detailed view of app permissions for the 'WD Antivirus Testground' application. The interface includes a search bar at the top and a navigation bar with tabs for Summary, Data usage, Users, Permissions, and Sensitivity labels. The Permissions tab is active, showing a summary of total permissions (3), high privilege (0), and unused permissions (0). Below this is a table for Graph API permissions, listing profile, openid, and email with their respective privilege levels (Low, Medium, High) and usage status (In use, Not available, Delegated). The main table lists various apps with their details: App name, App status, Graph API access, Permission type, Consent type, Publisher, Last modified, Added on, Permission usage, Data usage, and Privilege level. The 'WD Antivirus Testground' app is highlighted. At the bottom right, there's a green button labeled 'Disable app'.



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

The screenshot shows the Microsoft App governance interface. At the top, there are several informational banners: "Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.", "We've automatically turned on app governance. Learn more about our data security and privacy practices.", and "Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload Identity Premium. Try Workload Identity". Below these, a navigation bar includes "Overview", "Azure AD", "Salesforce", "Alerts", and "Policies". The "Policies" tab is selected, showing two sections: "Regulate app use" and "Secure app permissions". Each section has a "Create policy" button and a table of policy items. The "Regulate app use" table lists 14 items, and the "Secure app permissions" table lists 14 items. Both tables include columns for "Name", "Status", "Severity", "Active alerts", "Total alerts", "Last alert", "Last modified", "Scope", and "Created by".

[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.

The screenshot shows the Microsoft Defender XDR interface. At the top, there's a shield icon and the text "M365D Demo 10-20-22 Multi-stage incident involving Initial access & Lateral movement...". Below this, a navigation bar includes "Attack story", "Alerts (18)", "Devices (2)", "Users (6)", "Mailboxes (1)", "Apps (1)", "Investigations (3)", "Evidence and Response (31)", and "Summary". The "Alerts and categories" section shows "17/18 active alerts", "7 MITRE ATT&CK tactics", and "1 other alert categories". It also features a bar chart of alert severity. The "Scope" section displays "2 impacted devices", "6 impacted users", "1 impacted mailbox", and "1 impacted app". The "Top impacted entities" table lists various entities with their risk levels and tags. The "Evidence" section shows "31 entities found" with a progress bar indicating "Pending approval" and "Other". At the bottom, there are links for "View alerts" and "View all entities".



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)’**

The screenshot shows the Microsoft Conditional Access policy configuration interface. On the left, there's a navigation sidebar with options like Email & collaboration, Review, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Policy management (which is selected and highlighted with a red box), Policy templates, Reports, and Audit. The main area is titled 'Activities matching all of the following' and contains two filter conditions: 'Device' (selected) and 'Tag' (selected). The 'Device' condition has 'does not equal' and 'Intune compliant, Hybrid Azure AD joined' dropdowns. The 'Tag' condition has 'App' selected and 'Automatic Azure AD onboarding' dropdown. Below these filters is a 'Actions' section with 'Test' (selected) and 'Monitor all activities' option, and 'Block' option with 'A default block message is displayed when possible'. There's also an 'Alerts' section with a checked 'Create an alert for each matching event with the policy's severity' checkbox, and 'Save as default settings' and 'Restore default settings' buttons. A modal window titled 'Microsoft Office 365 SharePoint' lists various SaaS applications: Microsoft Flow Service, Microsoft Forms, Microsoft Intune, Microsoft Intune Enrollment, Microsoft Office 365 SharePoint (which is selected and highlighted with a blue box), Microsoft Rights Management Services, Microsoft StaffHub, Microsoft Stream Service, and Microsoft Teams Services.

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.



The screenshot shows the Microsoft 365 Defender interface for an incident titled "Business email compromise (BEC) financial fraud attack". The left sidebar has a shield icon and navigation links like Home, Incidents, Alerts, Devices, Users, Mailboxes, Apps, Investigations, Evidence and Response, and Summary. The main area has a search bar and tabs for Attack story, Recommended actions (18), Alerts (8), Devices (0), Users (1), Mailboxes (0), Apps (2), Investigations (1), Evidence and Response (9), and Summary. A yellow banner at the top says "Important! A potentially compromised account was automatically disabled by Microsoft 365 Defender's Attack Disruption. See the 'Users' tab or go to the Action center for more information." Below it, the "Attack story" tab is selected, showing a list of 8/8 active alerts from Dec 2, 2022, 1:07 PM, such as "Anonymous IP address" and "Unfamiliar sign-in properties". To the right is an "Incident graph" with nodes for "jwolcott@contoso.com", "178.129.125.123", "2 IPs", and "2 Cloud Applications", connected by lines representing "Communication" and "Association". On the far right, there's a summary section with a shield icon, the incident title, alert levels (High and Active), and tabs for "Attack Disruption", "Chain Event Detection", and "BEC Fraud". Below that are sections for "Manage incident", "Incident details" (Assigned to Unassigned, Incident ID 22423, Classification Not set, Categories Initial access, Defense evasion, Credential access), and activity logs for First activity and Last activity.

Deployment requirements for AAD

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

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

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

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

Operationalizing our Core Defender products

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

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





SOC Operational Guide in Defender XDR

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

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

Reference

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

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

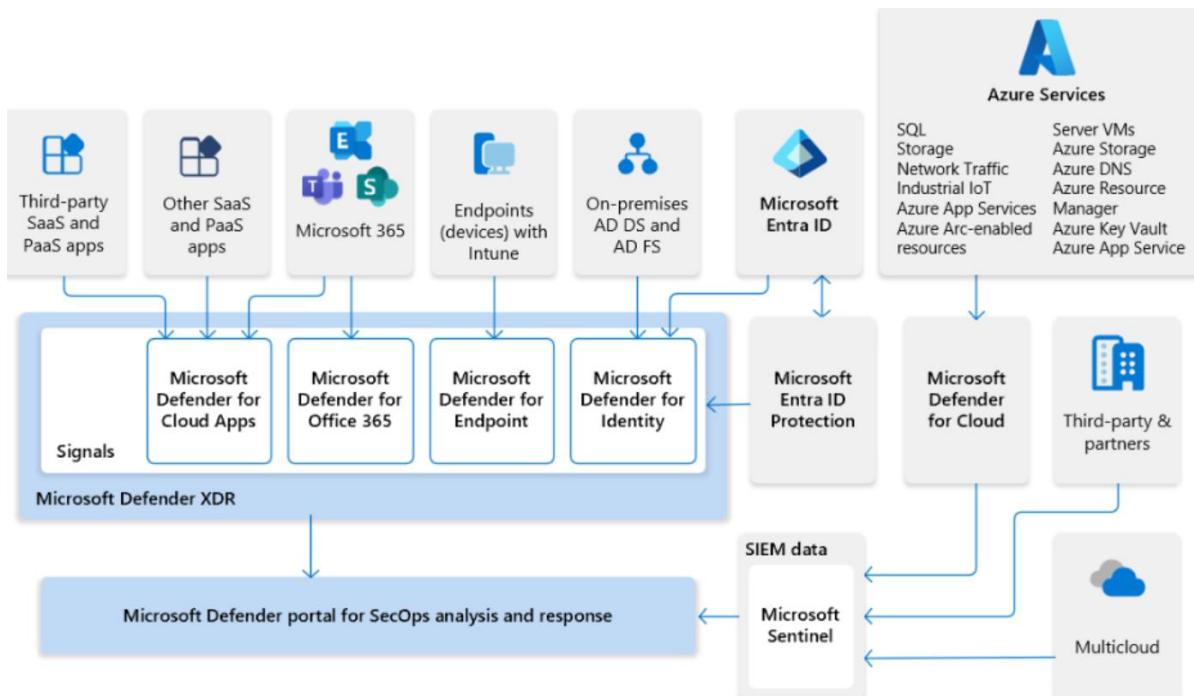
MDI - <https://learn.microsoft.com/en-us/defender-for-identity/ops-guide/ops-guide-daily>

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

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.

Unified security operations platform

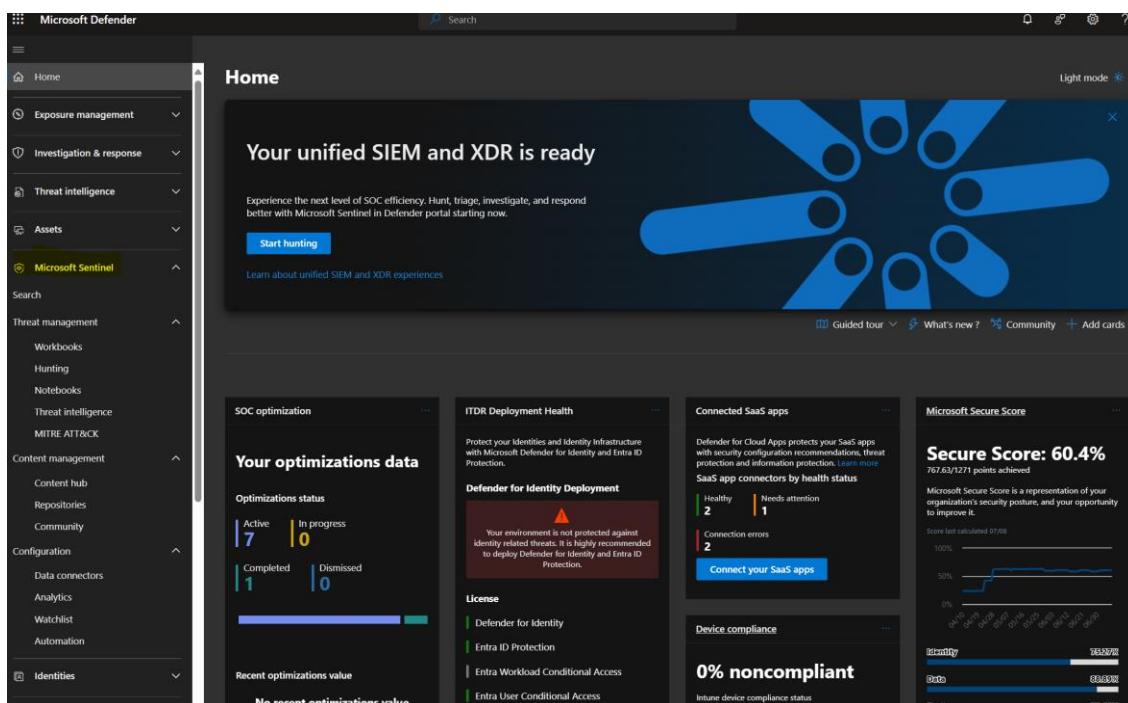
Artificial intelligence
AI-powered SOC

Extended detection and response (XDR)
Defense and protection across workloads

Security information and event management (SIEM)
Flexible detection across digital estate

Exposure management
Reduced exposure across digital estate

Threat intelligence
Comprehensive threat insights



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

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

		
Analytics Logs Powerful all inclusive logs ideal for real-time monitoring, alerting and dashboards. <ul style="list-style-type: none">✓ Standard cost✓ Including unlimited queries✓ 30 days retention included, can extend retention to 2 yrs.✓ Long-term retention up to 12 yrs.	Basic Logs Medium-touch telemetry data needed for troubleshooting and incident response. <ul style="list-style-type: none">✓ Reduced cost✓ Additional charges for queries✓ 30 days retention included✓ Long-term retention up to 12 yrs.	Auxiliary Logs Low-touch telemetry data intended for high verbose logs, auditing and compliance. <ul style="list-style-type: none">✓ Minimal cost✓ Additional charges for queries✓ 30 days retention included✓ Long-term retention up to 12 yrs.

Analytic Logs

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

Auxiliary logs

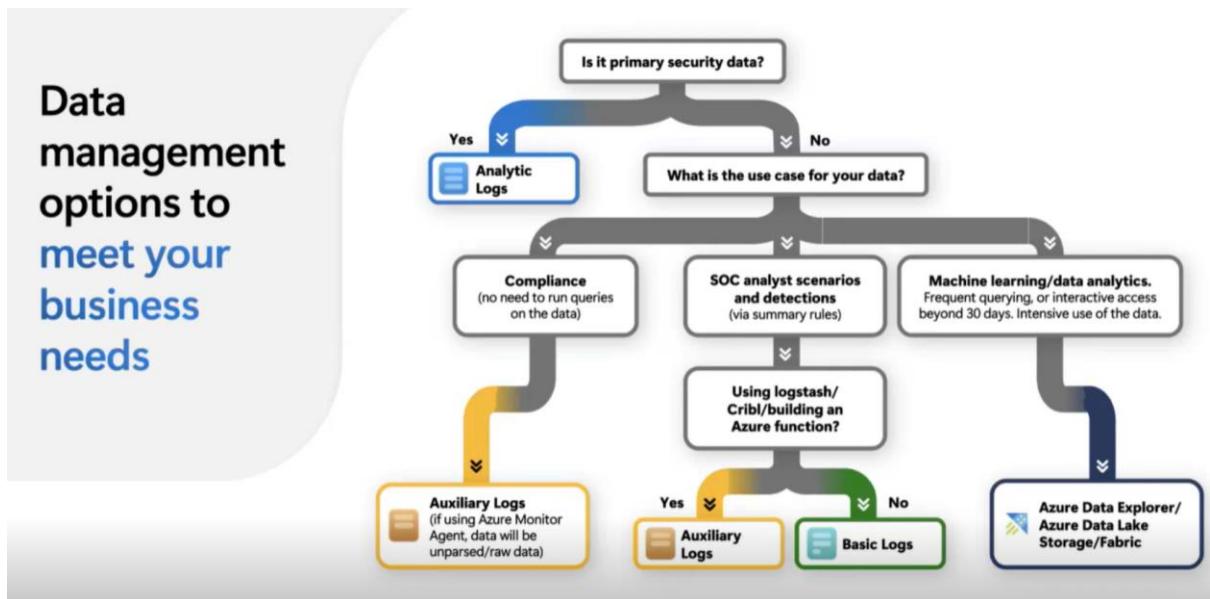
- keeps data in the interactive retention state for 30 days
- this state has very low retention costs as compared to the Analytics plan
- While this data remains in the interactive retention state, you can run [summary rules](#) on this data to create tables of aggregate

Basic Logs

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



This is a simple decision tree when



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

Onboard Sentinel

- a. Go to Azure Portal, find Microsoft Sentinel. Create and add a new workspace. Bear in mind that the workspace you choose means that the data is isolated to that workspace
3. **Configure Content** – This is the fun part of setting up Sentinel, from choosing your data connectors, to automation to playbooks. These are the features that really help separate Sentinel from other SIEMs
4. Determine and setup your Data Connectors
There 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.

The screenshot shows the Microsoft Defender Content hub interface. On the left, there's a navigation sidebar with various sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, and More resources. The main area displays a summary of content: Solutions (361), Standalone contents (278), Installed (16), and Updates (5). Below this, there's a search bar and filters for Status, Content type, Support, Provider, Category, and Content sources. A large table lists individual connectors with columns for Content title, Status, Content source, Provider, Support, Category, and Content type. Examples include AWS Amazon Web Services, Azure Activity, Cisco Umbrella, DNS Essentials, Google Cloud Platform IAM, Log4j Vulnerability Detection, Microsoft Defender for Cloud, Microsoft Defender XDR, Microsoft Entra ID, Network Session Essentials, SAP applications, Security Threat Essentials, Sentinel SOAR Essentials, and SOC Handbook.

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

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

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

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

The screenshot shows the Microsoft Defender Analytics page. The left sidebar includes Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Identities, Endpoints, Email & collaboration, and more. The main area has tabs for Active rules (47) and Rule templates. A yellow box highlights the 'Rule templates' tab. Another yellow box highlights the '+ Create' button. Below these are tabs for Analytics workbooks, Rule runs (Preview), Enable, Disable, Delete, Import, Export, and Columns. A 'Scheduled query rule' table lists various rules with columns for Name, Rule type, Status, Tactics, Techniques, Source name, and Last modified. Examples include 'Medium Office policy tampering', 'Low Failed login attempts to Az...', 'Medium Linked Malicious Storage Artifacts', 'Medium High count of connections by client ...', 'Low TestAV AR', 'Low Palo Alto - possible interna...', 'Medium T1 map Email entity to Emai...', 'Medium New External User Granted Admin R...', and 'High [DO NOT TOUCH] Squid URL TI match'. A red box highlights the 'Create' button in the toolbar.



message to that effect.

The screenshot shows the Microsoft Sentinel Analytics Rule creation interface. At the top, there's a header with a clock icon and the title "User login from different countries within 3 hours (Uses Authentication Normalization)". Below the header, there's a table with three columns: "High Severity" (Content Source), "Gallery Cont...", and "Scheduled Rule Type". The "Content Source" column has a "Gallery Cont..." link. The "Rule Type" column has a "Scheduled" entry. Under the "Description" section, it says: "This query searches for successful user logins from different countries within 3 hours. To use this analytics rule, make sure you have deployed the ASIM normalization parsers". Below that, under "MITRE ATT&CK", there's a link to "Initial Access (1)". The "Rule query" section contains the following PowerShell-like code:

```
let timeframe = ago(3h);
let threshold = 2;
imAuthentication
| where TimeGenerated > timeframe
| where EventType == 'Logon'
    and EventResult == 'Success'
```

The "Rule frequency" section is collapsed. A note box says: "Note: You haven't used this template yet; You can use it to create analytics rules." A blue "Create rule" button is highlighted with a red border.

6. Setup Automation Rules

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

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

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

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



The screenshot shows the Microsoft Sentinel Incident page for an incident with ID 602768. The main pane displays the incident details for a "Brute force attack" (Incident ID: 602768). It includes sections for Owner (Unassigned), Status (New), Severity (High), Description (A suspicious activity was detected in the organization. IPs are attached.), Alert product names (Microsoft Sentinel), Tasks (1/6 completed), Evidence (Events: 1, Alerts: 1, Bookmarks: 0), and Entities (3). The Timeline tab shows a single event from Nov 27, 4:41 PM: "Brute force attack" (Medium | Detected by Microsoft Sentinel). The right pane, titled "Incident tasks", lists several recommended actions: "Reset user password" (checked), "Validate and scope the alert", "Run query to explore last activities", "Stop suspicious process and isolate affected machines", "Block IP addresses and URLs", and "Open a task in ServiceNow for the IT department".

In Defender Portal. Sentinel – Configuration

The screenshot shows the Microsoft Defender Portal's Automation section. The left sidebar includes navigation links for Microsoft Sentinel, Threat management (Workbooks, Hunting, Notebooks, Threat Intelligence, MITRE ATT&CK), Content management, Configuration (Data connectors, Analytics, Watchlist, Automation), Identities, and Endpoints. The main pane is titled "Automation" and displays statistics: 4 Automation rules, 4 Enabled rules, and 14 Enabled playbooks. Below this, there are tabs for "Automation rules", "Active playbooks" (selected), and "Playbook templates (Preview)". A search bar and filter options are available. The "Playbook templates (Preview)" section lists several templates, including "Playbook with incident trigger", "Playbook with alert trigger", "Playbook with entity trigger", "Blank playbook", "Restrict MDE URL - Entity Triggered", "AD4IoT-NewAssetServiceNowTicket", and "MDT-IIntel-Reputation".

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



Microsoft Defender

Automation

Automation rules | Enabled rules | Enabled playbooks | More content at Content Hub

Automation rules Active playbooks Playbook templates

+ Create Automation rule

Add filter

	Trigger	Logic Apps Conn...	Entities	Tags	Last modified	Source name
Playbook with incident trigger	Microsoft Sentinel Incident	Microsoft Sentinel +	Notification	Incid	05/08/2022, 10:0...	SentinelSOARess...
Playbook with alert trigger	Microsoft Sentinel Alert	Microsoft Sentinel +	Notification	Incid	05/08/2022, 10:0...	SentinelSOARess...
Playbook with entity trigger	Microsoft Sentinel Entity	Microsoft Sentinel +	Notification	Incid	05/08/2022, 10:0...	SentinelSOARess...
Blank playbook	Microsoft Sentinel Entity (Pre)	Microsoft Sentinel +	DNS	Remediation	26/02/2023, 10:0...	MicrosoftDefend...
Restrict MDE URL - Entity Triggered	Microsoft Sentinel Entity (Pre)	Microsoft Sentinel +	FileHash	Remediation	14/07/2022, 10:0...	MicrosoftDefend...
Restrict MDE FileHash - Alert Triggered	Microsoft Sentinel Alert	Microsoft Sentinel +	Host	Remediation	22/12/2022, 10:0...	MicrosoftDefend...
Isolate MDE Machine using entity trigger	Microsoft Sentinel Entity (Pre)	Microsoft Sentinel +	Host	Remediation	22/12/2022, 10:0...	MicrosoftDefend...
Relate alerts to incident by IP	Microsoft Sentinel Incident	Azure Monitor Logs ↔ IP	grouping	20/03/2022, 10:0...	SentinelSOARess...	
Send Teams Adaptive Card on incident creation	Microsoft Sentinel Incident	Microsoft Teams +1		Notification	04/08/2022, 10:0...	SentinelSOARess...
Isolate endpoint - MDE - Incident Triggered	Microsoft Sentinel Incident	Microsoft Defender +	Host	Remediation	14/07/2022, 10:0...	MicrosoftDefend...
Isolate MDE Machine - Alert Triggered	Microsoft Sentinel Alert	Microsoft Defender +	Host	Remediation	14/07/2022, 10:0...	MicrosoftDefend...
Run MDE Antivirus - Alert Triggered	Microsoft Sentinel Alert	Microsoft Defender +	Host	Remediation	14/02/2022, 10:0...	MicrosoftDefend...
Confirm Microsoft Entra ID Risky User - Incident Triggered	Microsoft Sentinel Incident	Microsoft Entra ID +	Account	Remediation	25/07/2022, 10:0...	Microsoft Entra L...
Incident tasks - Microsoft Defender XDR Phishing Playbook ...	Microsoft Sentinel Incident	Microsoft Sentinel	Tasks	16/02/2023, 10:0...	SentinelSOARess...	
Post Message Teams	Microsoft Sentinel Alert	Microsoft Teams +1		Notification	04/08/2022, 10:0...	SentinelSOARess...
Dismiss Microsoft Entra ID Risky User - Alert Triggered	Microsoft Sentinel Alert	Microsoft Entra ID +	Account	Remediation	25/07/2022, 10:0...	Microsoft Entra L...
Isolate MDE Machine using entity trigger	Microsoft Sentinel Entity (Pre)	Microsoft Sentinel +	Host	Remediation	22/12/2022, 10:0...	MicrosoftDefend...
Restrict MDE Domain - Alert Triggered	Microsoft Sentinel Alert	Microsoft Sentinel +	DNS	Remediation	14/07/2022, 10:0...	MicrosoftDefend...
Send email with formatted incident report	Microsoft Sentinel Incident	Office 365 Outlook +		Notification	14/07/2021, 10:0...	SentinelSOARess...
Restrict MDE to Address - Alert Triggered	Microsoft Sentinel Alert	Microsoft Sentinel ↔ IP		Remediation	14/07/2022, 10:0...	MicrosoftDefend...

No template
Select a template to ...

Automation > Playbook editor



Basics	
Subscription	Visual Studio Enterprise Subscription
Resource group	Sentinel
Region	australiaeast
Playbook name	Play
Diagnostics logs workspace	Sentinel1

Connections

- Microsoft Sentinel

Connect with managed identity
Note: Grant permissions to the managed identity after deployment.

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



The screenshot shows the Microsoft Logic App Designer interface. On the left, there's a sidebar with navigation links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Development Tools (Logic app designer is selected), Logic app code view, Run History, Versions, API connections, Quick start guides, Settings, Monitoring, Automation, and Help. Below the sidebar is a toolbar with Search, Run, Save, Discard, Parameters, Code view, Errors, Info, File a bug, and Enable Legacy Designer. The main area has a title bar "Play | Logic app designer" and a "Microsoft incident" card. To the right, a modal window titled "Add an action" is open, showing a search bar, runtime selection (Select a runtime), and action type (Actions). It lists various actions in a grid, such as "jexacts gen. Document & more", "10to8 Appointment Scheduling", "IMe Corporate", "Ipt (Independent Publisher)", "24 pull request (Independent Pu...)", "365 Training", "3E Events", "Abbreviations", "Abortion Policy (Independent P...)", "Abstract Company Enrichment (I...", "Abstract Email Validator (Indepe...)", "Abstract Exchange Rates (Indep...)", "Abstract Holidays (Independent ...)", "Abstract IBAN Validator (Indepe...)", "Abstract IP Geolocation (Indepe...)", and "Abstract Phone Validator (Inde...)".

8. Setup Workbooks

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

These are the commonly use workbooks

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

9. Setup Watchlist

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

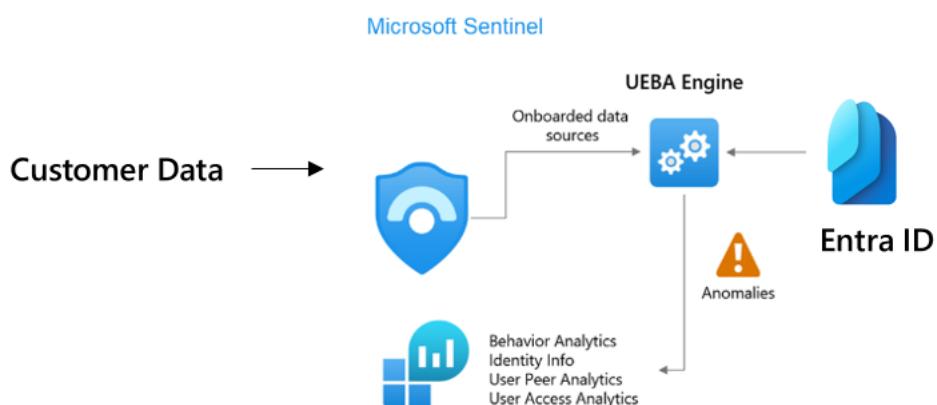
Think of watchlist as something like you can leverage for VIP users or assets. Watchlist is a feature that allows you to correlate the data source and the events in Sentinel. You can upload a file with the list and be able to dive deeper into the assets and monitor using correlated data and events.



The screenshot shows the Microsoft Sentinel interface. On the left, there's a navigation sidebar with various sections like Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Data connectors, Analytics, Watchlist (which is selected and highlighted in blue), and Automation. The main area is titled "Watchlists" and displays a summary: "Watchlists 34" and "Watchlist Items 559K". Below this, there are two tabs: "My Watchlists" (selected) and "Templates (Preview)". A search bar says "Search by name, alias and description" and a "Add filter" button. A table lists several watchlists with columns for Name, Alias, Source, Create..., and Last up... . One row is expanded to show details: HighValueAssets, high_value, HighValue/..., 3/17/2022, 3/17/2022, zscaler, Watchlist.c..., 6/9/2022, 1, 6/9/2022, 2, SAP - Privileged Users, SAP - Privil..., ContentHu..., 1/15/2024, 2/29/2024, SAP - Transactions for ABAP Ge..., SAP - Trans..., ContentHu..., 1/15/2024, 2/29/2024, SAP - Sensitive Tables, SAP - Sens..., ContentHu..., 1/15/2024, 2/29/2024, SAP - Sensitive Profiles, SAP - Sens..., ContentHu..., 1/15/2024, 2/29/2024, SAPAlertRulesMetadata, SAPAlertRu..., ContentHu..., 1/15/2024, 2/29/2024, and SAP - Sensitive ABAP Programs, SAP - Sens..., ContentHu..., 1/15/2024, 2/29/2024.

10. Enable User and Entity Behavioural Analytics (UEBA)

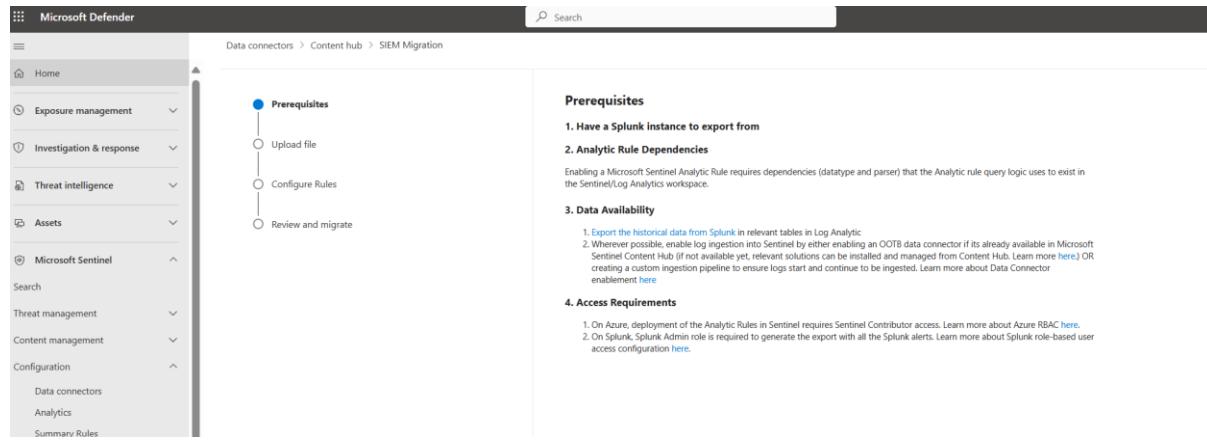
From a Sentinel perspective, UEBA has the same purpose where it builds baseline behavioural profiles of your organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon from all the logs you collect from the data sources. Using a variety of techniques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



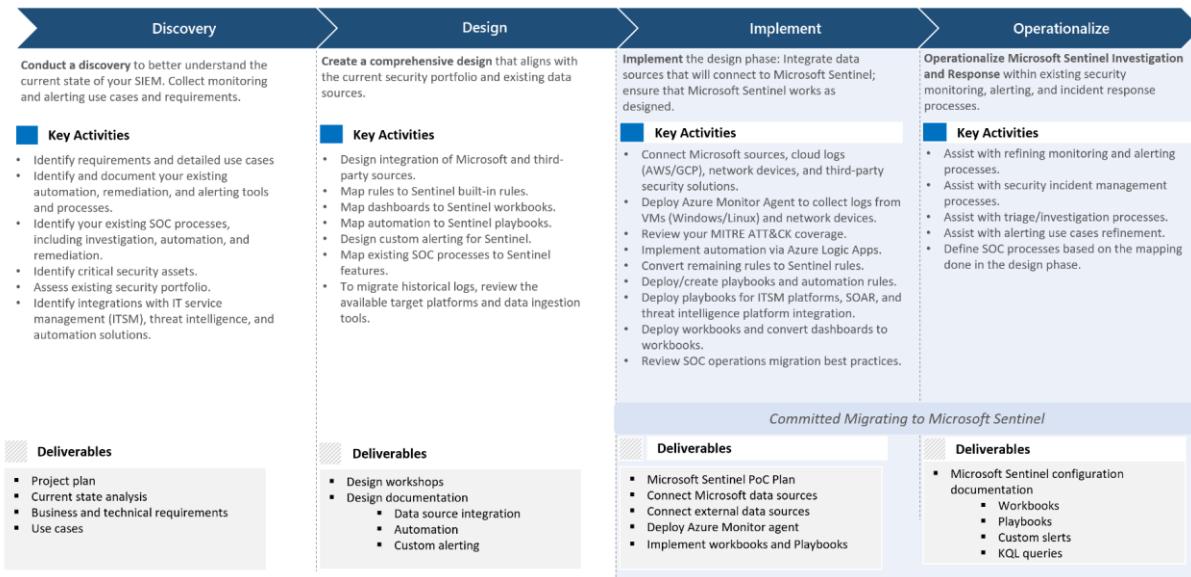
Migration from 3rd party SIEM to Sentinel

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

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



Microsoft Sentinel Migration – phases & key activities



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 probe threats in email or identity, you can simply go into the table and find the closest query. If the query you are looking for is not there, you can also go into the queries tab and community queries which potentially could have queries that the community has uploaded to share.

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



Community Queries

The screenshot shows the Microsoft Defender XDR interface. On the left is a navigation sidebar with various sections like Home, Exposure management, Investigation & response, Hunting (Advanced hunting, Custom detection rules), Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, and Activity log. The main area is titled "Advanced hunting" and shows a query editor. The sidebar on the right is titled "Community queries" and lists several pre-defined Kusto queries under categories such as Campaigns, Collection, Command and Control, Credential Access, Defense evasion, Delivery, Discovery, Email Queries, Execution, Extrication, Exploits, Fun, General queries, Impact, and Initial access. One specific query, "Account brute force (0)", is selected and its code is visible in the main query editor.

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



Devices	^
<input type="checkbox"/> Isolate device	
<input type="checkbox"/> Collect investigation package	
<input type="checkbox"/> Run antivirus scan	
<input type="checkbox"/> Initiate investigation	
<input type="checkbox"/> Restrict app execution	
Files	^
<input type="checkbox"/> Allow/Block	
<input type="checkbox"/> Quarantine file	
Users	^
<input type="checkbox"/> Mark user as compromised	
<input type="checkbox"/> Disable user	
<input type="checkbox"/> Force password reset	
Emails	^
<input type="checkbox"/> Move to mailbox folder	
<input type="checkbox"/> Delete email	

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?

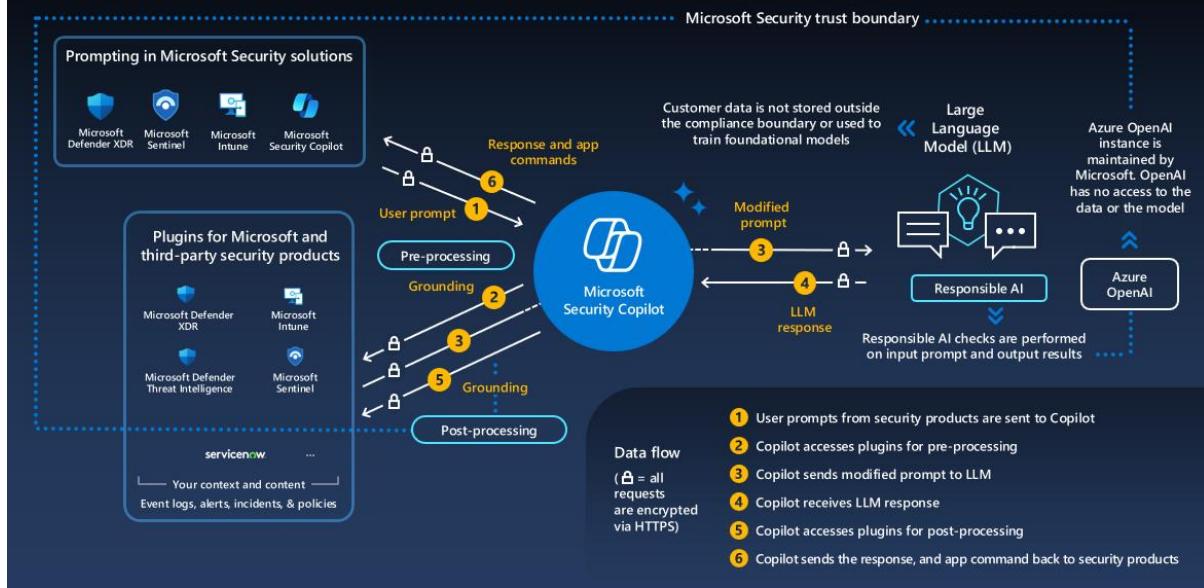
The new, embedded experience in Microsoft Defender XDR supercharges security teams with generative AI capabilities to take their efficiency to a new level for the following set of powerful use cases:

- 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



Microsoft Copilot for Security



Copilot for Security primary use cases

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

Incident summarization

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

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

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

Alerts Incident graph Layout Group similar nodes

Mar 15, 2024 2:26 PM • Resolved Activity from a Tor IP address

Mar 15, 2024 2:26 PM • Resolved Suspicious inbox manipulation rule

Mar 15, 2024 2:26 PM • Resolved Activity from a Tor IP address

Mar 15, 2024 2:26 PM • Resolved Suspicious inbox manipulation rule

Mar 15, 2024 2:26 PM • Resolved A potentially malicious URL click was detected

Mar 15, 2024 2:26 PM • Resolved A potentially malicious URL click was detected

Mar 15, 2024 2:27 PM • Resolved Anonymous IP address

Mar 15, 2024 2:27 PM • Resolved Anonymous IP address

Mar 15, 2024 2:27 PM • Resolved Compromised user account in a

Cloud Applications (2) User (3) No subject (3)

Copilot

Incident summary Mar 16, 2024 1:53 PM

The high severity BEC financial fraud attack occurred between 2024-03-15 14:26:31 UTC and 2024-03-15 14:40:38 UTC. It was tagged as Attack Disruption, BEC Fraud, and Credential Phish, triggering an automatic Attack Disruption action.

- DefenseEvasion: The incident began at 2024-03-15 14:26:31 UTC when a suspicious inbox rule was set on the inbox of user 'name'. This rule, named 'RSS Feeds', forwards messages to a folder named RSS Feeds. The attack involved the IPs 111.111.11.111 and 111.111.11.111 and the cloud app Microsoft Exchange Online. At the same time, 'name' accessed the Tor IP address 111.111.11.111, indicating potential evasion of detection.
- NetworkAccess: At 2024-03-15 14:34:01 UTC, 'name' clicked on a potentially malicious URL in a mail message titled 'Updater'. The URL was <http://192.168.1.100/test.html?00000000000000000000000000000000>. Shortly after, at 14:37:02 UTC, an attempted sign-in was detected from the anonymous IP 111.111.11.111.
- CredentialAccess: At 2024-03-15 14:37:15 UTC, 'name' logged on to Office365, indicating a potential compromise of the user account. The session was associated with the IP 111.111.11.111.
- Collection and DefenseEvasion: At 2024-03-15 14:39:11 UTC, 'name' performed a New-Mailbox operation on the Microsoft Exchange Online, indicating a BEC financial fraud attempt. This action was associated with the IP 111.111.11.111. At the same time, a suspicious inbox manipulation rule was set, involving the same IP and the cloud app Microsoft Exchange Online.

AI-generated content may be incorrect. Check at the source.

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

The screenshot displays a detailed timeline of security events for a device named 'Device1'. The timeline covers from Oct 2023 to Mar 2024. A specific event on Feb 16, 2024, at 6:17:23 AM is selected, showing a command-line analysis of the process 'Zimba4!u!exe' with PID 1954. The analysis highlights the command 'netstart -p -s Schedule' and the file path 'C:\Windows\System32\svchost.exe'. The event details show the user 'Devices\adhadmin' and the process 'svchost.exe'.

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

The screenshot shows a guided response for a financial fraud attack. The guided response interface includes sections for threat overview, activity profile, incident details, remediation, and containment. It provides specific actions such as 'Delete similar emails' and 'Disable the account Name'.

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



Sentinel Plug-in

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

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

Medium | Active | Unassigned

Attack story Alerts (228) Assets (2) Investigations (0) Evidence and Response (1) Summary Similar incidents (0)

Incident graph Layout Group similar nodes

Communication Association

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

What happened

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

ANALYTICS RULE

Analytics rule details

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

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

Copilot Manage incident ...

Incident summary Jul 1, 2024 10:30 PM

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

- Exfiltration: The incident began at 2024-06-30 02:27:15 UTC

See more

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

Guided response Jul 1, 2024 10:39 PM

Completed recommendation...

Status: All

Investigation New

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

Hi,

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

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

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 replaced. 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



