

geekmania

geekmania

Microsoft 365 Defender – Review 2023

Alex Verboon | baseVISION AG

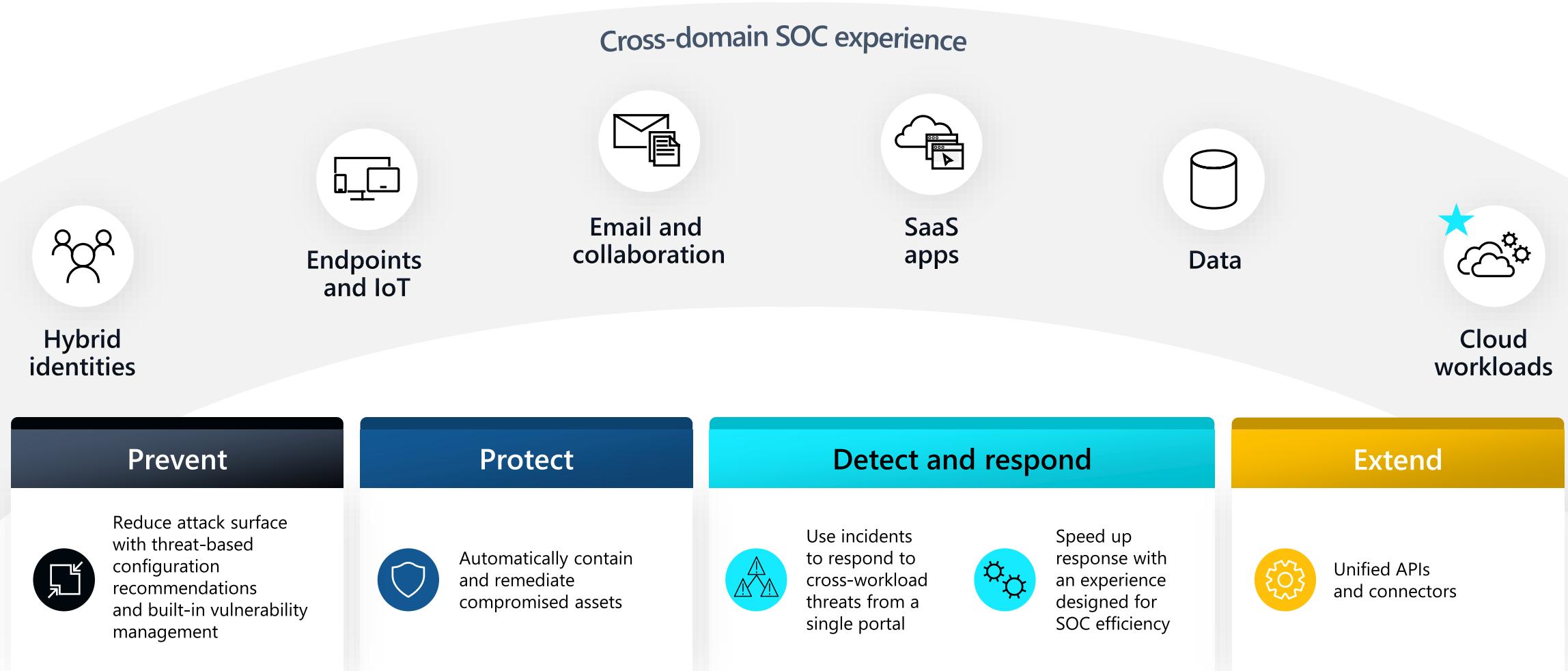
geekmania

Microsoft Defender XDR – Review 2023

Alex Verboon | baseVISION AG

Microsoft Defender XDR

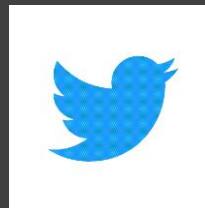
Build a unified defense with XDR





- **Alex Verboon**
CTO - Principal Cyber Security Consultant

- **Contact Me**



<https://twitter.com/alexverboon>



<https://www.linkedin.com/in/verboonalex/>



<https://github.com/alexverboon>



<https://www.verboon.info/>



baseVISION

SECURE & MODERN WORKPLACE

Great
Place
To
Work.[®]

Certified

APR 2022-APR 2023

CH



Microsoft Intelligent
Security Association

Microsoft Security

Microsoft Verified
Managed XDR Solution

Why this session?

How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472

Applies to: Windows Server 2019, all editions, Windows Server 2016, Windows Server, version 1909, all editions, [More](#)

Continuous flow of information

Threats > Ransomware continues to hit healthcare, critical ...

Overview Analyst report Mitigations

Executive summary

At a time when remote work is becoming universal and the strain on IT admins in healthcare are attacks by various ransomware groups have occurred in the first two weeks of April 2020, target providers. While the attacks delivered varying payloads, they all used the same techniques observed deployment of a ransomware payload of the attacker's choice. The actions of these attackers have

Windows introduces cloud settings

Microsoft: Proof of disposal for records - Roll-out Update

- (Updated) Feature Update: Microsoft Secure Score improvement action updates
- (Updated) Outlook on the web - In-product notification of full inbox
- New Azure AD Conditional Access policies now apply to all client apps, including legacy ones
- Exportability of Security reports
- (Updated) Outlook - new resource booking capabilities

Security Baseline (FINAL): Windows 10 and Windows Server Version 2004

Security baseline (FINAL): Windows 10 and Windows Server,...

March 08, 2020 12:14

Threat and vulnerability management Event timeline

7,288



Introducing event timeline – an innovative, new way to...

shirfeldman on 07-06-2020 12:42 PM

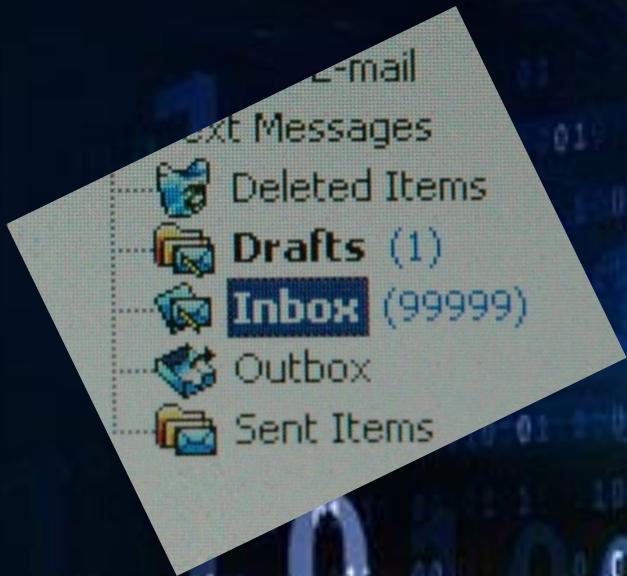
Announcing the public preview of event timeline, a new, interactive way for admins to interpret how risk got introduced...

Windows 10 Servicing Model Timeline

July 8, 2020

Introducing Kernel Data Protection, a new platform security technology for preventing data corruption

The other (important) things in life



Virus & threat protection
Threats found
Windows Defender Antivirus
found threats. Get details.

Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated
All > Active = true										
INC0010001	2020-01-02 07:38:27	test	James Vitolo	● 1 - Critical	New	Inquiry / Help	(empty)	(empty)	2020-01-10 16:52:09	system
INC0035009	2018-06-30 01:06:16	Unable to access the shared folder.	David Miller	● 1 - Low	New	Inquiry / Help	(empty)	(empty)	2018-12-12 23:30:24	admin
INC0050005	2018-08-31 21:35:21	Email server is down.	David Miller	● 1 - Critical	New	Software	(empty)	(empty)	2018-12-12 23:18:55	admin
INC0050001	2018-09-11 20:56:26	Unable to post content on a Wiki page	David Miller	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2018-12-12 23:32:42	admin
INC0070002	2018-10-16 22:47:51	Need access to the common drive.	David Miller	4 - Low	New	Inquiry / Help	(empty)	(empty)	2018-12-12 23:28:49	admin
INC0070001	2018-10-16 22:47:10	Employee payroll application server is down.	David Miller	● 1 - Critical	New	Hardware	Openspace	(empty)	2018-12-12 23:26:28	admin
INC0050009	2018-08-10 09:14:29	Unable to access team file share	Rick Borate	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2018-08-10 09:14:29	admin
INC0050008	2018-08-10 09:37:45	Performance problems with email	Bon Rupper	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2018-08-10 09:37:45	admin
INC0050007	2018-08-10 09:14:59	Performance problems with wifi	Bertie Luby	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2018-08-10 09:14:59	admin
INC0050005	2018-10-08 20:47:23	SAP Sales app is not accessible	Carol Caulkin	● 1 - Critical	In Progress	Service Desk	Beth Anglin	Beth Anglin	2018-12-20 13:08:31	admin
INC0050004	2015-11-02 12:49:08	SAP Materials Management is slow or there is an outage	Christian Mitchell	● 1 - Critical	On Hold	Software	Service Desk	(empty)	2015-11-24 07:47:36	admin
INC0050003	2018-12-06 12:48:46	The SAP HR application is not accessible	Margaret Grey	● 1 - Critical	In Progress	Inquiry / Help	Service	Beth Anglin	2018-12-27 11:42:25	admin
SAP Financial Accounting										



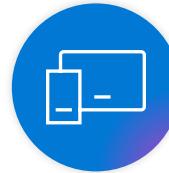
”

So, if you haven't had the time to stay up to date on all things Microsoft Defender XDR this year, this session is for YOU

Defender XDR

Automatic Attack
Disruption

Ransomware continues to be a major threat



300%

Increase in human-operated ransomware
attacks in the past year



70%

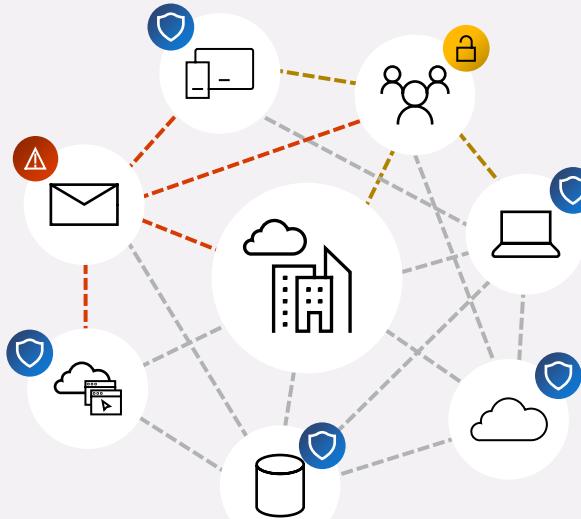
of all successful ransomware attacks targeted
orgs with fewer than 500 employees



5 mins

all that is needed before an attacker can begin
moving laterally after a malicious link is clicked

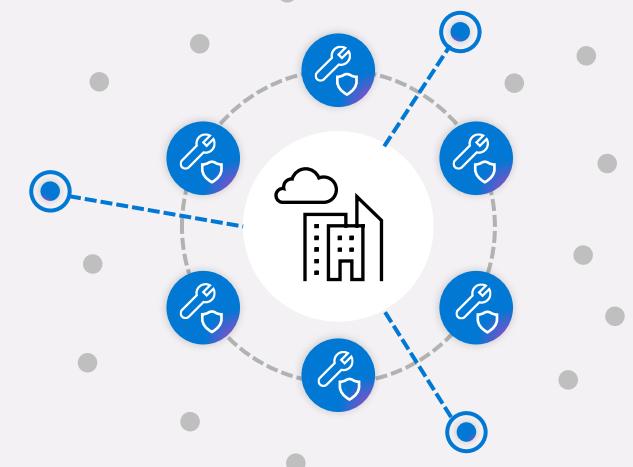
Strong prevention and efficient incident queue triage is no longer enough



Preventing every possible vulnerability is simply unrealistic



Expecting to respond as soon as an alert is triggered is unsustainable

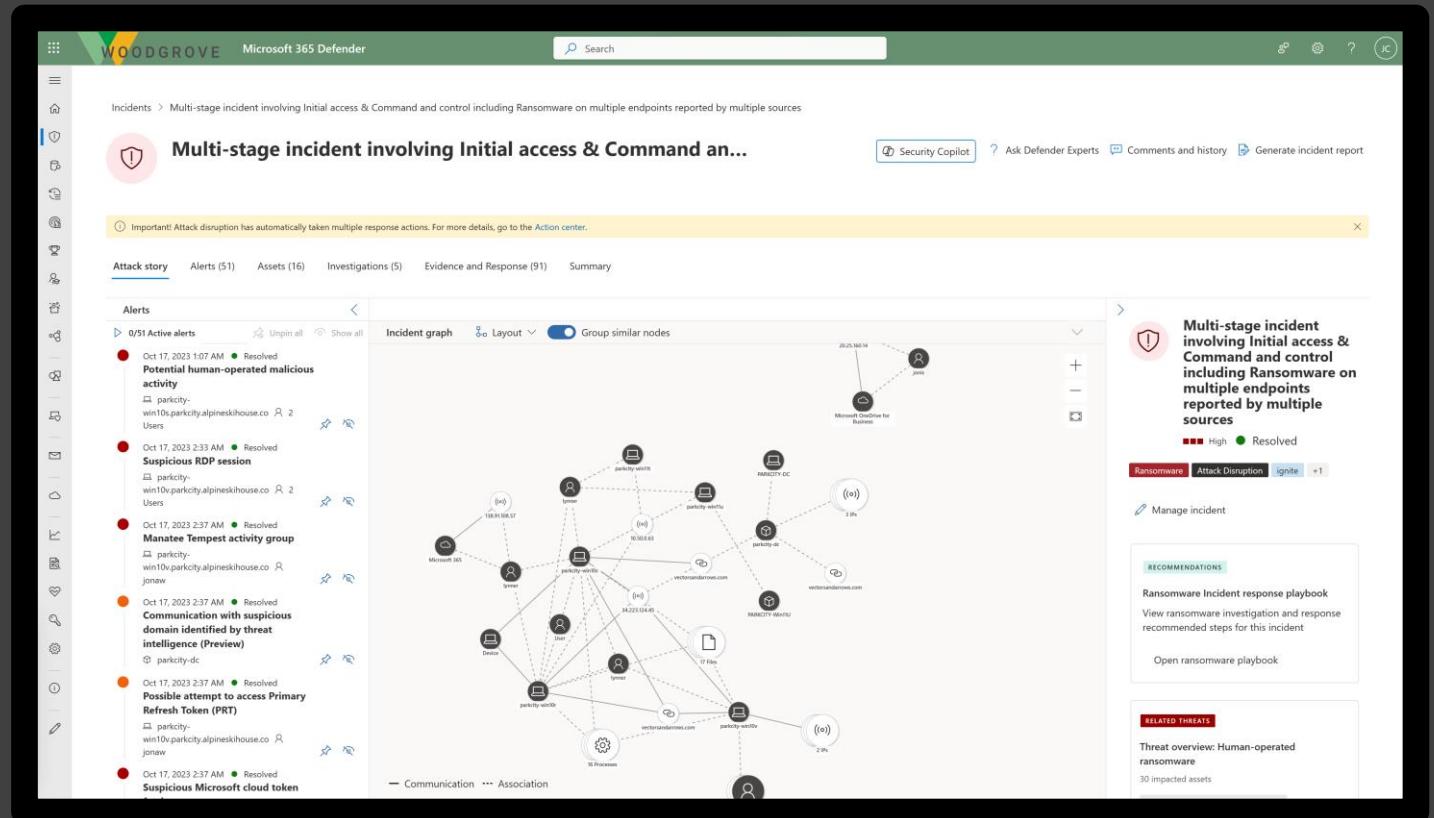


Ensuring full eradication with siloed tools is extremely difficult

Automatically disrupt human-operated ransomware attacks early in the kill chain

Prevent lateral movement by automatically containing compromised users across all devices

On by default for all MDE customers



Attack disruption at machine speed

XDR-level intelligence and AI automatically disrupt advanced attacks incl. ransomware, BEC, and AiTM

The screenshot shows the Microsoft Defender XDR interface with the following details:

- Incident Graph:** Displays a network of nodes representing users, devices, and processes. Nodes include "alice", "parkeyt-win01", "parkeyt-win02", "parkeyt-win03", "payload.exe", and "8 Processes". Relationships are shown with lines labeled "Communication" and "Association".
- Alerts:** A list of 21 active alerts, all marked as "Resolved". Examples include "Suspicious access to LSASS service", "Process memory dump", and "Sensitive credential memory read".
- Incident Summary:** Describes a "Multi-stage incident involving Privilege escalation including Ransomware on multiple endpoints reported by multiple sources".
- Recommendations:** Suggests a "Ransomware Incident response playbook" for the incident.

Detection

Correlates signals from multiple sources into a single, high-confidence incident

Classification

Classify attack scenario and **identify** assets controlled by the attacker

Attack disruption

Automatically isolates infected devices and suspends compromised accounts in real-time



AI-powered automation disrupts lateral movement

Leaves the SOC team in full control of investigating and remediating

Reduces the overall cost and limits the impact of an attack by stopping lateral movement

Automatic attack disruption limits lateral movement early on and reduces the overall impact of an attack, from associated costs to loss of productivity. At the same time, it leaves the SOC team in complete control of investigating, remediating, and bringing assets back online.

- **Device contain** - based on Microsoft Defender for Endpoint's capability, this action is an automatic containment of a suspicious device to block any incoming/outgoing communication with the said device.
- **Disable user** - based on Microsoft Defender for Identity's capability, this action is an automatic suspension of a compromised account to prevent additional damage like lateral movement, malicious mailbox use, or malware execution.
- **Contain user** - This response action automatically contains suspicious identities temporarily. This helps to block any lateral movement and remote encryption related to incoming communication with Microsoft Defender for Endpoint's onboarded devices.

Microsoft 365 Defender Search ⚙️ ? CO

Incidents > Business email compromise (BEC) financial fraud attack launched from a compromised account

Business email compromise (BEC) financial fraud ...

Manage incident Ask Defender Experts Comments and history

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.

Attack story Recommended actions (18) Alerts (8) Devices (0) Users (1) Mailboxes (0) Apps (2) Investigations (1) Evidence and Response (9) Summary

Alerts < >

8/8 Active alerts Unpin all Show all

Date	Type	Details
Dec 2, 2022 1:07 PM	New	Anonymous IP address ↳ Jonathan Wolcott
Dec 2, 2022 1:07 PM	New	Password Spray ↳ Jonathan Wolcott
Dec 2, 2022 1:07 PM	New	Unfamiliar sign-in properties ↳ Jonathan Wolcott
Dec 2, 2022 1:07 PM	New	Atypical travel ↳ Jonathan Wolcott
Dec 2, 2022 1:07 PM	New	Anonymous IP address ↳ Jonathan Wolcott

Incident graph Layout Group similar nodes

The incident graph illustrates the relationships between various entities. A central node is 'Jonathan Wolcott' (user). It connects to an IP address (178. [redacted]) via a dashed line labeled 'Communication'. Another dashed line labeled 'Association' connects 'Jonathan Wolcott' to '2 Cloud Applications'. Two other nodes, each with '(o)' icons, are connected to the IP address node via dashed lines labeled '2 IPs'. The entire graph is contained within a light gray box.

Business email compromise (BEC) financial fraud attack launched from a compromised account

High Active

Attack Disruption Chain Event Detection BEC Fraud

Manage incident

Incident details

Assigned to	Incident ID
Unassigned	22423
Classification	Categories
Not set	Initial access, Defense evasion, Credential access

First activity Last activity

Defender XDR

email notifications for
actions

When there is an important incident, it is crucial to ensure that key stakeholders on the team are promptly informed. Providing immediate notifications for critical activities to relevant team members not only raises awareness but reduces response times and improves alignment among stakeholders.

Example: When Microsoft Defender XDR Attack disruption disables an account or isolates a device, you want to avoid that the helpdesk re-enables the user before the incident is closed.

- **Improve stakeholder alignment** – stakeholders can be notified on certain actions and assets, according to relevance.
- **Gain visibility into remediation actions that take place in real time** – rules can be set to receive emails on automated (e.g., contain device, disable user) or manual actions (e.g., live response, isolate device, delete email)
- **Get notified about actions according to their state** – notifications can be set to be sent when an action fails, succeeds, or both.

Configure
Action
Notifications

The screenshot shows the Microsoft Defender interface for Microsoft 365. The left sidebar contains various icons and navigation links. The main content area is titled "Microsoft 365 Defender". A breadcrumb navigation bar at the top left shows "Settings > Microsoft 365 Defender".

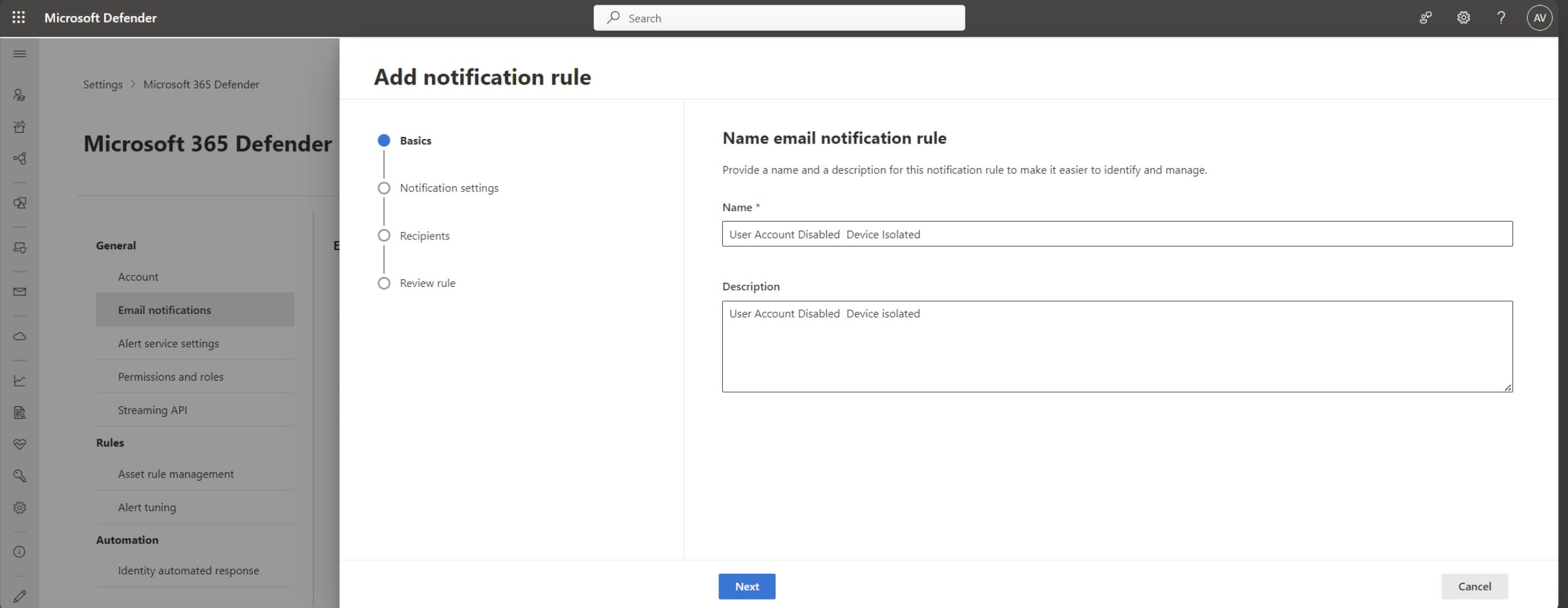
The left sidebar has three main sections:

- General**: Includes "Account", "Email notifications" (which is highlighted with a green box), "Alert service settings", "Permissions and roles", and "Streaming API".
- Rules**: Includes "Asset rule management" and "Alert tuning".
- Automation**: Includes "Identity automated response".

The right side of the screen is titled "Email notifications" and includes tabs for "Incidents", "Actions" (which is highlighted with a green box), and "Threat analytics". Below these tabs is a button "+ Add notification rule". A table lists existing notification rules:

Notification rule	Recipients	Updated
<input type="checkbox"/> Test email notification	oa@verboon.online	Nov 28, 2023 11:01...

Provide a Name and Description. You can setup multiple Action notifications.



The screenshot shows the Microsoft 365 Defender interface with the 'Email notifications' section selected. A modal window titled 'Add notification rule' is open, showing the 'Basics' step. The 'Name email notification rule' section contains fields for 'Name' (User Account Disabled Device Isolated) and 'Description' (User Account Disabled Device isolated). The left sidebar shows navigation options like General, Rules, and Automation.

Microsoft Defender

Settings > Microsoft 365 Defender

Microsoft 365 Defender

General

- Account
- Email notifications**
- Alert service settings
- Permissions and roles
- Streaming API

Rules

- Asset rule management
- Alert tuning

Automation

- Identity automated response

Add notification rule

Basics

- Notification settings
- Recipients
- Review rule

Name email notification rule

Provide a name and a description for this notification rule to make it easier to identify and manage.

Name *

Description

Next Cancel

Select the Action Source and Actions on which to send out an activity notification

The screenshot shows the Microsoft Defender interface for configuring email notifications. On the left, the 'Email notifications' section is selected under 'General' settings. A modal window titled 'Add action' is open, listing various actions for 'Microsoft Defender for Endpoint'. Several actions are checked: 'Isolate device', 'Stop isolation', 'Contain device', and 'Release device containment'. The 'Notification settings' tab is active in the modal, which includes fields for 'Action source', 'Action', 'Device groups scope', and 'Action status'. The 'Action source' dropdown contains 'Automated actions, Manual response actions'. The 'Action' dropdown contains 'Disable User, Contain device, Isolate device, Stop isolation'. The 'Device groups scope' dropdown has 'All device groups (affects all current and future groups)' selected. The 'Action status' dropdown has 'Select' chosen.

Microsoft Defender

Settings > Microsoft 365 Defender

Microsoft 365 Defender

General

- Account
- Email notifications**
- Alert service settings
- Permissions and roles
- Streaming API

Rules

- Asset rule management
- Alert tuning

Automation

- Identity automated response

Add action

- Microsoft Defender for Endpoint
- File quarantine
- Service quarantine
- Driver quarantine
- Release file
- Stop process
- Stop processes
- Remove script persistence
- Live Response command
- Isolate device
- Restrict app execution
- Stop restricting app execution
- Stop isolation
- Collect file
- Offboard device
- Start antivirus scan
- Collect investigation package
- Contain device
- Release device containment
- Contain user
- Release user containment

Notification settings

Set up action notifications by selecting how actions were initiated, action types, and their status.

Action source *

Automated actions, Manual response actions

Action *

Disable User, Contain device, Isolate device, Stop isolation

Device groups scope *

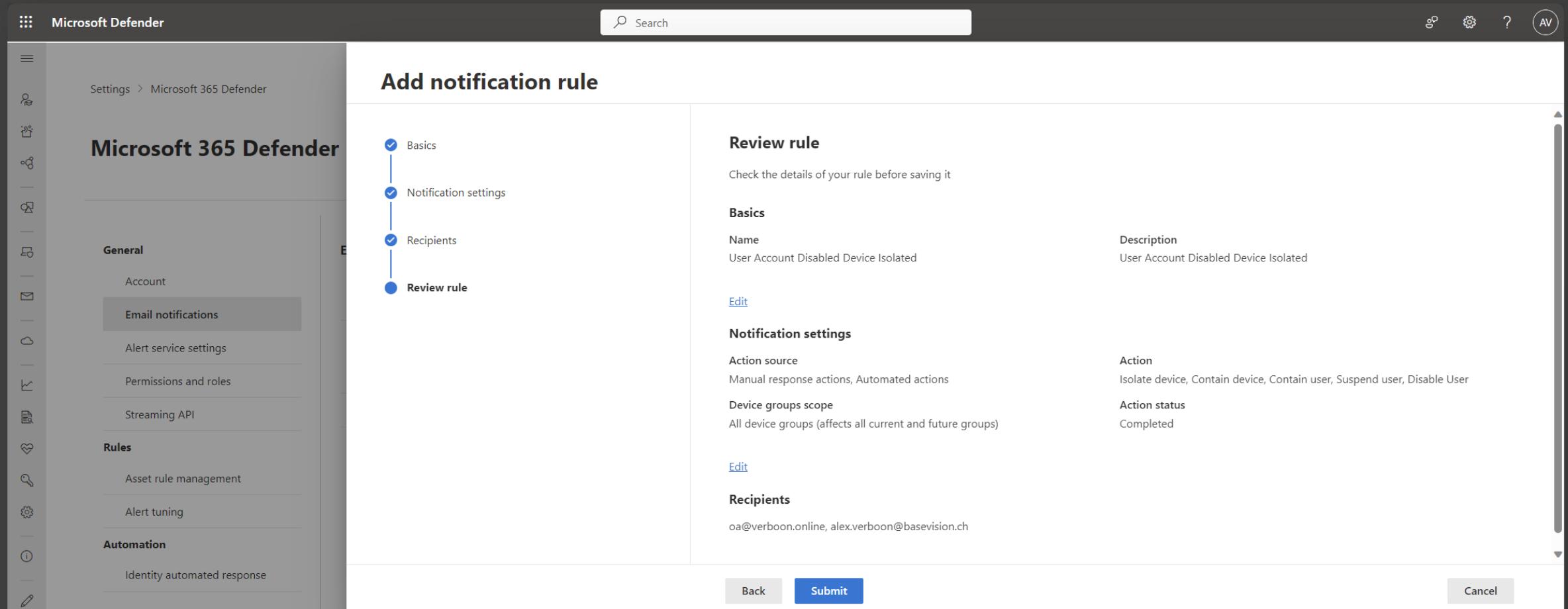
All device groups (affects all current and future groups)
 Selected device groups

Action status *

Select

Back Next Cancel

Review and Submit the Action notification configuration



The screenshot shows the 'Add notification rule' interface in Microsoft 365 Defender. On the left, a navigation sidebar lists 'General', 'Rules', and 'Automation' sections. The 'Email notifications' option under 'General' is selected. The main panel displays a progress bar with four steps: 'Basics' (checked), 'Notification settings' (checked), 'Recipients' (checked), and 'Review rule' (highlighted). The 'Review rule' section contains a summary of the rule details:

Review rule
Check the details of your rule before saving it

Basics

Name	User Account Disabled Device Isolated
Description	User Account Disabled Device Isolated

[Edit](#)

Notification settings

Action source	Manual response actions, Automated actions
Device groups scope	All device groups (affects all current and future groups)

[Edit](#)

Recipients

oa@verboon.online, alex.verboon@basevision.ch

[Back](#) [Submit](#) [Cancel](#)

E-Mail notification

 Microsoft 365

An immediate response action was taken in Microsoft Defender XDR

A user attempted to isolate a device and the attempt succeeded. See the [Devices](#) tab or go to the [Action Center](#) for more details.

Action	Isolate device
Action start time	November 28, 2023
Action status	Completed
Device	clientdlp1
Support ID	eb28a2e5-90e4-4cce-9371-812f6e21ecfb

[!\[\]\(bd2a32f947c5766cd49562c6434da5d4_img.jpg\)](#) [!\[\]\(6d7f1753db5c7f4cdce0eb77d0741b6a_img.jpg\)](#) [!\[\]\(30a67908594c89642bde2d4b1eaf6678_img.jpg\)](#) [!\[\]\(2bae78efd4d0baa6cdfba1ed1469116a_img.jpg\)](#)

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

 Microsoft 365

An immediate response action was taken in Microsoft Defender XDR

A user attempted to disable a user account and the attempt succeeded. See the [Users](#) tab or go to the [Action Center](#) for more details.

Action	Disable user
Action start time	November 28, 2023
Action status	Completed
Support ID	40198d5f-148c-4cc9-93e0-787267b436d4

[!\[\]\(9bb0eeabfc64b565058b9428271cdf15_img.jpg\)](#) [!\[\]\(f159d9550cba63c9a191c936a406412a_img.jpg\)](#) [!\[\]\(1aaa31036622bbfcd5b363a81174d9a7_img.jpg\)](#) [!\[\]\(e551b45089a3dd3ec457d321817b7ac6_img.jpg\)](#)

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Optional – If your SOC isn't monitoring the e-mail queue, you can also generate an Incident when an action notification is sent out.

The screenshot shows the Microsoft Sentinel interface. On the left, there is a list of incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, Owner, and Status. One incident is selected, showing its details on the right. The selected incident is titled "Defender XDR - Response Action Notification" (Incident ID: 629), with a status of "New". It is owned by "Unassigned" and was created on 11/28/23, 03:12 PM. The "Alerts" column shows 1 alert, which is "Microsoft Sentinel". The "Product names" column shows "Microsoft Sentinel". The "Created time" and "Last update time" are both 11/28/23, 03:12 PM. The "Owner" is "Unassigned" and the "Status" is "New". The "Description" field states: "Triggers an Incident when a Microsoft Defender XDR response action notification email is send". The "Alert product names" section lists "Microsoft Sentinel". The "Evidence" section shows 4 events, 1 alert, and 0 bookmarks. A note at the bottom says: "The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. [Learn more >](#)". At the bottom right, there are "View full details" and "Actions" buttons.

EmailEvents

```
| where SenderFromAddress == "defender-noreply@microsoft.com"
| where Subject contains "action"
```

Microsoft
Defender for
Endpoint

Zeek Integration

Zeek is now integrated as a component within Microsoft Defender for Endpoint.

The integration of Zeek into Microsoft Defender for Endpoint provides **new levels of network analysis capabilities** based on deep inspection of network traffic powered by Zeek, a powerful open-source network analysis engine.

Defender for Endpoint can now monitor inbound and outbound traffic with a novel engine that is capable of:

- **Session Awareness** - Being able to aggregate network protocol data across an entire TCP/UDP session, such as NTLM and Kerberos authentications, SSH sessions, FTP connections, and RPC
- **Dynamic Protocol Detection** - Being able to detect attacks even on **non-default ports**, a common pattern attackers use to hide their network traffic.
- **Dynamic Scripting Content** - Being able to add new detections on the fly using Zeek scripts

Device Discovery Enhancements

The integration enhances passive device discovery capabilities by utilizing many widely used protocols that are supported out of the box, including the below:

- **NTLM** - The NTLM authentication protocol involves both client and server devices sending their hostname, domain name, and operating system version. This is highly valuable data when it comes to **device discovery**. Zeek aggregates and reports this information for both sides on the NTLM transaction.
- **SSH** - Zeek monitors SSH protocol traffic and parses out the **server version string**. This string often includes the version of the SSH server software and the host operating system version.
- **FTP** - FTP servers usually respond with a code 220 response after a successful TCP handshake. This means that the server is ready to serve a new user. As part of the code 220 response, a **response message** is sent which typically contains identifying information about the FTP server.

▼ NTLM Secure Service Provider

```
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
Target Name: TEST
Negotiate Flags: 0xe2898215, Negotiate 56, Negotiate K
NTLM Server Challenge: 7d8370da6c118c4f
Reserved: 0000000000000000
```

▼ Target Info

Length: 114
Maxlen: 114
Offset: 64

- > Attribute: NetBIOS domain name: TEST
 - > Attribute: NetBIOS computer name: DC
 - > Attribute: DNS domain name: TEST.local
 - > Attribute: DNS computer name: DC.TEST.local
 - > Attribute: DNS tree name: TEST.local
 - > Attribute: Timestamp
 - > Attribute: End of list

Version 10.0 (Build 17763); NTLM Current Revision 1

▼ SSH Protocol

Protocol: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3

[Direction: server-to-client]

0000	b4	0e	de	50	db	9c	2c	c5	46	30	8b	12	08	00	45	00	...P..., F0...E...
0010	00	4f	ab	8d	40	00	33	06	82	c8	5f	d8	f5	43	c0	a8	.0...@.3..._.C...
0020	03	8f	00	16	07	a5	76	88	32	9b	d6	99	4d	23	50	18v..2...M#P...
0030	01	f6	96	d9	00	00	53	53	48	2d	32	2e	30	2d	4f	70SS H-2.0-Op
0040	65	6e	53	53	48	5f	36	2e	37	70	31	20	44	65	62	69	enSSH_6. 7p1 Debi
0050	61	6e	2d	35	2b	64	65	62	38	75	33	0d	0a		an-5+deb	8u3...	

▼ File Transfer Protocol (FTP)

> 220 SATO SATO PRINTER Ver 2.3.0 FTP server.\r\n

[Current working directory:]

Advanced Hunting - ActionType in the DeviceNetworkEvents table

ActionType

- DnsConnectionInspected
- SslConnectionInspected
- NtLmAuthenticationInspected
- HttpConnectionInspected
- IcmpConnectionInspected
- SshConnectionInspected
- InboundInternetScanInspected
- FtpConnectionInspected
- SmtpConnectionInspected

InboundInternetScanInspected

Identify systems that are scanned from the internet

```
24
25 DeviceNetworkEvents
26 | where ActionType == "InboundInternetScanInspected"
27 | project TimeGenerated, DeviceName, LocalIP, LocalPort, RemoteIP, RemotePort, ActionType
28 | extend current_geoinfo = geo_info_from_ip_address(LocalIP)
29 | extend country = tostring(current_geoinfo.country)
30 | extend city = tostring(current_geoinfo.city)
31 | extend state = tostring(current_geoinfo.state)
32 | join IP_Indicators on $left.LocalIP == $right.TI_ipEntity
33
```

Results Chart Add bookmark

TimeGenerated [UTC] TI_ipEntity DeviceName ↑

TimeGenerated [UTC]	TI_ipEntity	DeviceName
<input checked="" type="checkbox"/> > 7/5/2023, 12:09:59.594 PM	[REDACTED]	[REDACTED]
<input type="checkbox"/> > 7/1/2023, 2:00:45.918 PM	[REDACTED]	[REDACTED]
<input type="checkbox"/> > 6/17/2023, 2:30:49.769 AM	[REDACTED]	[REDACTED]
<input type="checkbox"/> > 6/16/2023, 5:06:20.036 PM	[REDACTED]	[REDACTED]
<input type="checkbox"/> > 7/24/2023, 11:40:35.304 AM	[REDACTED]	[REDACTED]
<input type="checkbox"/> > 6/22/2023, 8:26:33.684 AM	[REDACTED]	[REDACTED]

LocalIP	LocalPort	RemoteIP	RemotePort
162.243.128.11	39124	[REDACTED]	389
138.68.208.7	34266	[REDACTED]	502
192.241.197.21	51713	[REDACTED]	102
192.241.202.13	49806	[REDACTED]	7474
198.199.114.61		[REDACTED]	
162.243.132.16		[REDACTED]	

LocalIP: 162.243.128.11 LocalPort: 39124 RemoteIP: [REDACTED] RemotePort: 389

Community Score: 5 / 88

5 security vendors flagged this IP address as malicious

162.243.128.11 (162.243.128.0/19)
AS 14061 (DIGITALOCEAN-ASN)

FtpConnectionInspected

Identify systems with FTP activity

```
4
5 DeviceNetworkEvents
6 | where ActionType == "FtpConnectionInspected"
7 | extend json = todynamic(AdditionalFields)
8 | extend command = tostring(json.command)
9 | extend reply_code = tostring(json.reply_code)
10 | extend reply_msg = tostring(json.reply_msg)
11 | extend direction = tostring(json.direction)
12 | extend user = tostring(json.user)
13 | extend arg = tostring(json.arg)
14 | extend cwd = tostring(json.cwd)
15 | extend geoinfo = geo info from in address(RemoteTP)
```

Results Chart Add bookmark

	direction	user	arg ↑↓	cwd	country
t.conf	Out	www	ftp://1 [REDACTED]	/pi	France
ed here), 0.56 Kbytes per second	Out	www	ftp://1 [REDACTED]	/pi	France
	Out	www	ftp://1 [REDACTED]	/pi	France
	Out	[REDACTED]	ftp://[REDACTED]arkeepass.kdbx	/	Germany
	Out	[REDACTED]	ftp://[REDACTED]arkeepass.kdbx	/	Germany
	Out	[REDACTED]	ftp://[REDACTED]arkeepass.kdbx	/	Germany

Did you intend to search across the entire table?

⚠ 4 security vendors flagged this IP address as malicious

188.68.47.214 (188.68.32.0/19)

AS 197540 (netcup GmbH)

self-signed

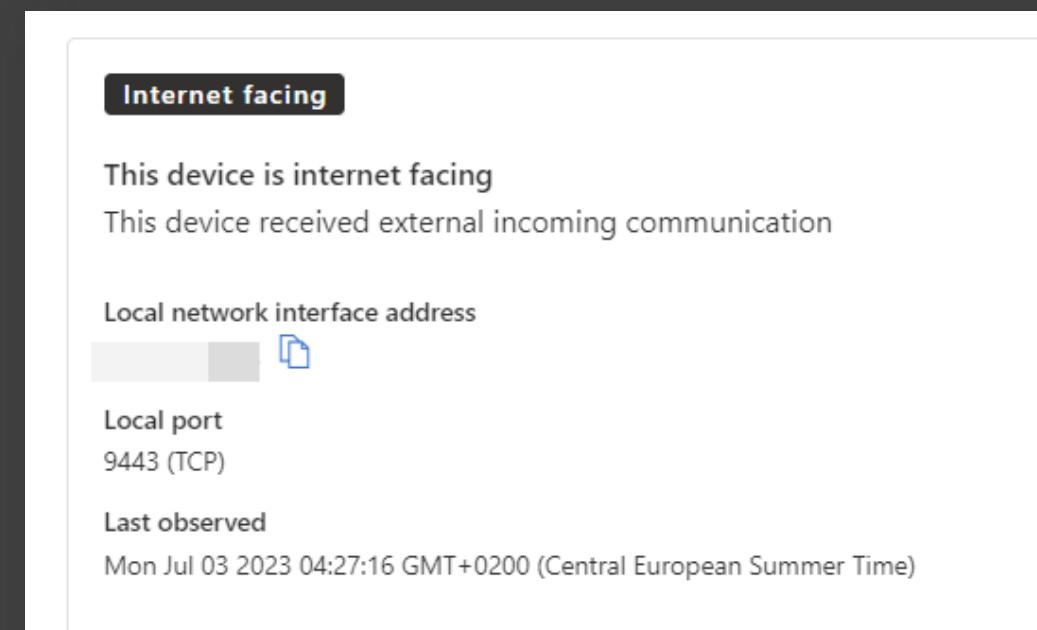
Microsoft
Defender for
Endpoint

Discover Internet Facing
Devices

Microsoft Defender for Endpoint is expanding the device discovery capabilities through Microsoft's existing network telemetry and RiskIQ integration, providing the capability to discover **internet-facing devices**.

Threat actors are constantly scanning the internet to identify **exposed devices**, whether it's part of an opportunistic malicious activity or a wider targeted campaign. These devices serve as highly accessible entry points to an organization's environment.

Microsoft Defender for Endpoint will automatically map and flag onboarded devices that are exposed to the internet in the Microsoft Defender XDR portal, providing more context to security teams and deeper insights into device exploitability



Defender for Endpoint uses different data sources to identify the devices to flag:

- **External scans** are used to identify which devices are approachable from the outside.
- **Device network connections**, captured as part of Defender for Endpoint signals, help to identify external incoming connections that reach internal devices.

Devices can be flagged as internet-facing when a configured firewall policy (host **firewall** rule or enterprise firewall rule) **allows inbound** internet communication.

[Computers & Mobile](#) [Network devices](#) [IoT/OT devices](#)Total
14High risk
0High exposure
2Not onboarded
0Internet facing
14[Export](#)[Search](#)

30

Filters: Internet facing: Yes [X](#)

<input type="checkbox"/> Name	Domain	Risk level ⓘ ↓	Exposure level ⓘ	OS platform	Tags
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing AlwaysOn DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Low	Windows Server 20...	Internet facing AlwaysOn
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing AlwaysOn DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing AlwaysOn DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing AlwaysOn DMZ
<input type="checkbox"/>	[REDACTED]	[REDACTED] No known ri... [REDACTED]	⚠ Medium	Windows Server 20...	Device value: High Internet facing AlwaysOn DMZ

Filter[Clear filters](#)

Internet facing

 No Yes

Query

ⓘ Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't want to see it again X

```
11 DeviceInfo
12 | where Timestamp > ago(7d)
13 | where IsInternetFacing
14 | extend InternetFacingInfo = AdditionalFields
15 | extend InternetFacingReason = extractjson("$.InternetFacingReason", InternetFacingInfo, typeof(string)), InternetFacingLocalPort = extractjson("$.InternetFacingLocalPo
16 | summarize arg_max(Timestamp, *) by DeviceId
17 | summarize arg_max(Timestamp, *) by DeviceId
18 | project
19 DeviceName.
```

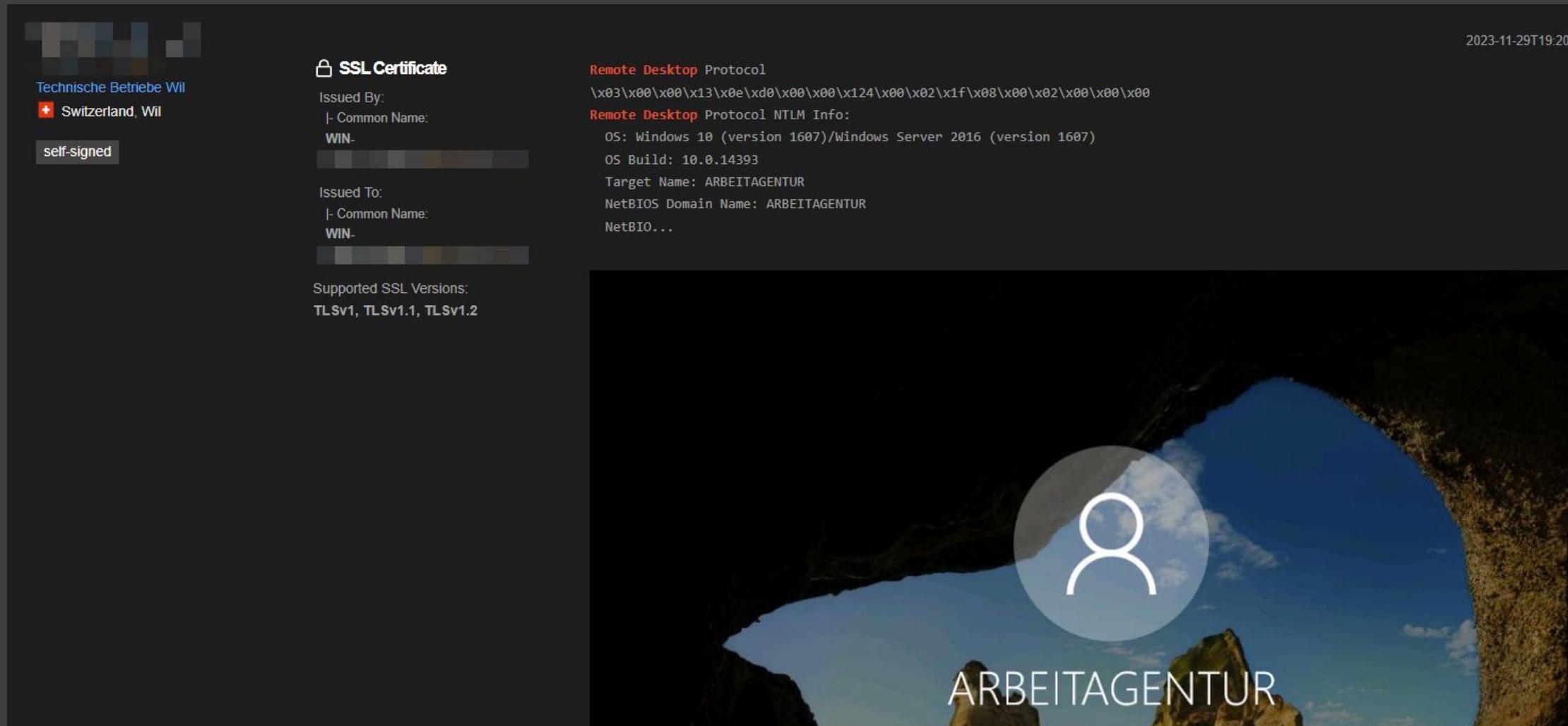
Getting started Results

Export Link to incident Take actions 1 of 1 selected Search 🕒 0:47 Low Chart type Customize columns

<input checked="" type="checkbox"/> DeviceName	<input type="checkbox"/> IsInternetFacing	<input type="checkbox"/> InternetFacingReason	<input type="checkbox"/> InternetFacingLocalIp	<input type="checkbox"/> InternetFacingLocalPort	<input type="checkbox"/> InternetFacingScannedPubli...	<input type="checkbox"/> InternetFacingScannedPubli...
<input checked="" type="checkbox"/> [REDACTED] 1		PublicScan	[REDACTED]	3389	[REDACTED]	81

Internetfacing 3389

Internet Facing



The screenshot shows a detailed view of an SSL certificate. At the top right, the date and time are displayed as 2023-11-29T19:20. On the left, there is a small logo for "Technische Betriebe Wil" and a flag indicating "Switzerland, Wil". Below this, the text "self-signed" is visible. The main content area is titled "SSL Certificate" and includes the following details:

- Issued By:** WIN- [REDACTED]
- Common Name:** WIN-
- Issued To:** WIN- [REDACTED]
- Common Name:** WIN-
- Supported SSL Versions:** TLSv1, TLSv1.1, TLSv1.2

On the right side of the certificate details, there is additional information related to the Remote Desktop Protocol and its NTLM version:

- Remote Desktop Protocol:** \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
- Remote Desktop Protocol NTLM Info:**
 - OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
 - OS Build: 10.0.14393
 - Target Name: ARBEITAGENTUR
 - NetBIOS Domain Name: ARBEITAGENTUR
 - NetBIO...

The background of the screenshot features a scenic landscape with mountains and a blue sky.

Microsoft Defender for Endpoint

Manage security settings
for Windows, macOS,
and Linux natively in
Defender for Endpoint

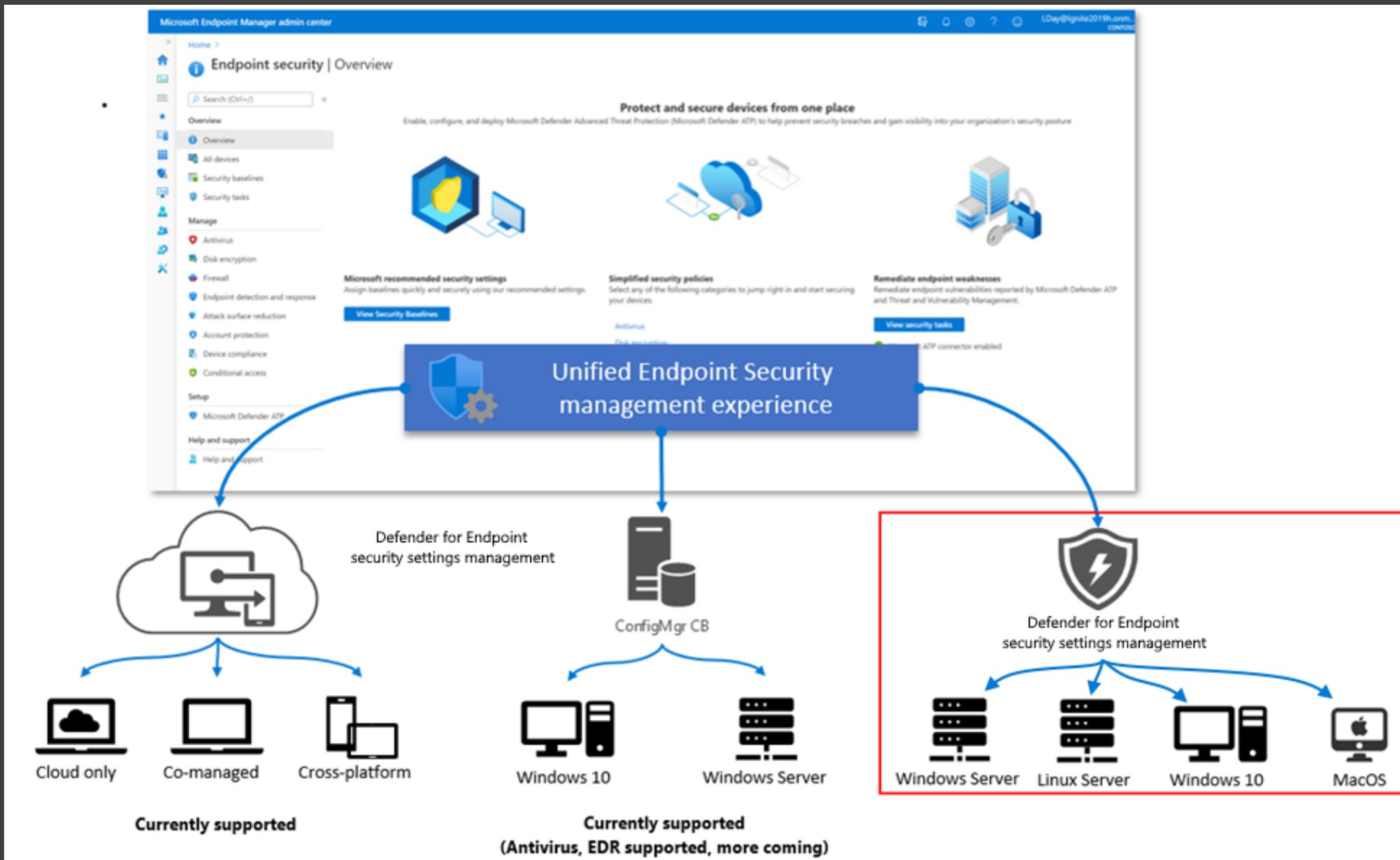
When you use Microsoft Defender for Endpoint, you can deploy policies from Microsoft Intune to manage the Defender security settings on the devices you've onboarded to Defender **without enrolling those devices with Intune**. This capability is known as Defender for Endpoint security settings configuration and is also referred to as security settings management.

Use cases:

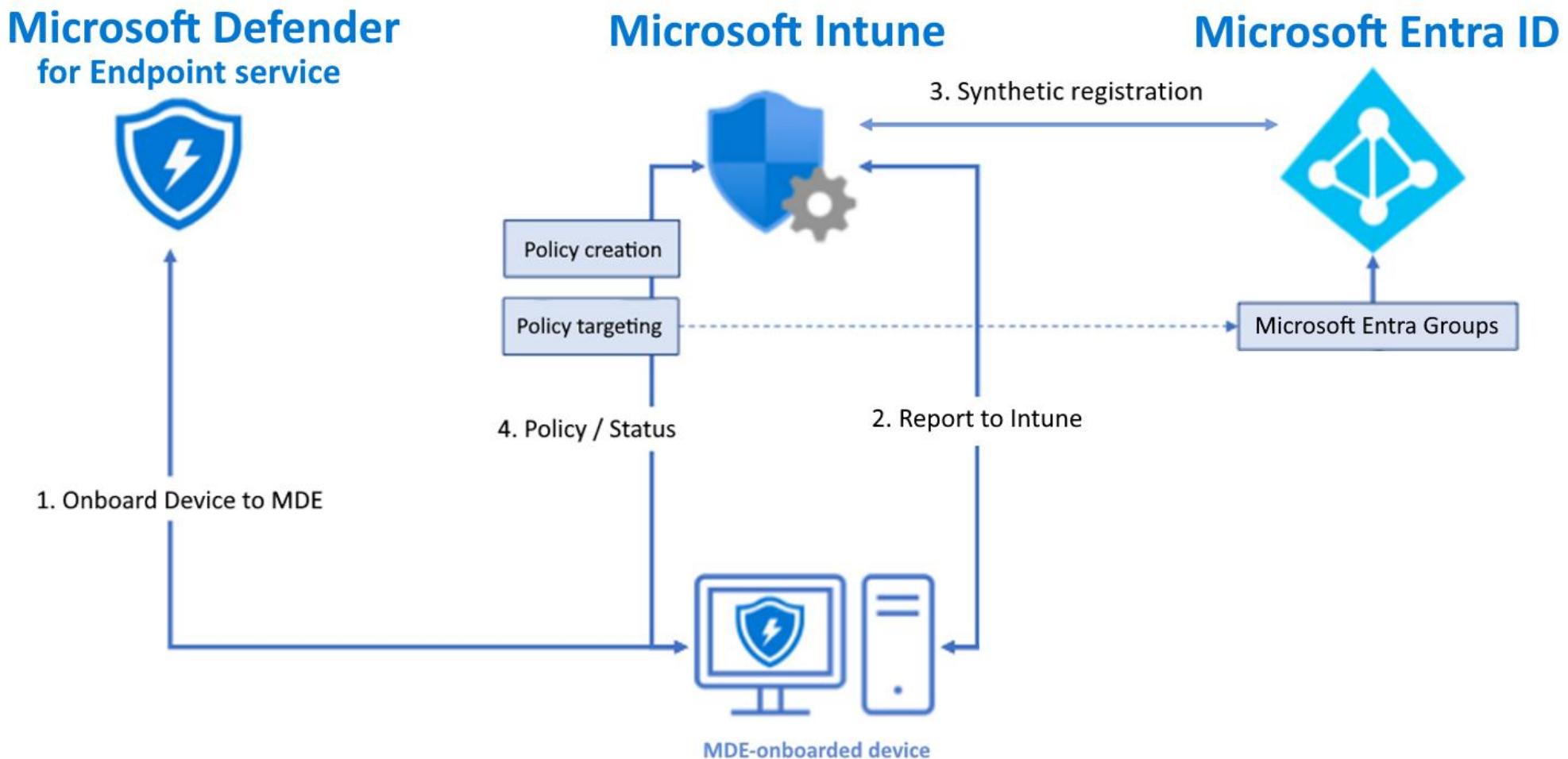
- Windows **Servers** located in a **DMZ**, not domain joined, not managed through Microsoft Configuration Manager
- **Standalone** Windows Clients not managed through Intune
- **Standalone** MacOS devices not managed through Intune
- **Linux Servers**

Or simply, any Microsoft Defender for Endpoint device that is not managed through AD GPO, Intune, Microsoft Configuration manager or any other systems management solution.

- Native security settings management capabilities in Defender for Endpoint that support Windows, macOS, and Linux
- Existing endpoint security policies are automatically ingested in the Microsoft Defender XDR portal
- Create and edit AV policies directly from the Microsoft Defender XDR portal
- Policies are automatically synced with Microsoft Intune to ensure coordination between IT and Security teams for organizations who use Intune as a full management suite.
- A new list on the device page, that shows all security policies and their settings
- Simplified device onboarding: Removal of Azure Active Directory hybrid join as a management prerequisite



How does it work?



Current supported policy types

The following policy types support the *Linux* platform.

Endpoint security policy	Profile	Defender for Endpoint security settings management	Microsoft Intune
Antivirus	Microsoft Defender Antivirus		
Antivirus	Microsoft Defender Antivirus exclusions		
Endpoint detection and response	Endpoint detection and response		

The following policy types support the *macOS* platform.

Endpoint security policy	Profile	Defender for Endpoint security settings management	Microsoft Intune
Antivirus	Microsoft Defender Antivirus		
Antivirus	Microsoft Defender Antivirus exclusions		
Endpoint detection and response	Endpoint detection and response		

Current supported policy types

Windows 10, Windows 11, and Windows Server

To support use with Microsoft Defender security settings management, your policies for Windows devices must use the *Windows 10, Windows 11, and Windows Server* platform. Each profile for the *Windows 10, Windows 11, and Windows Server* platform can apply to devices that are managed by Intune and to devices that are managed by security settings management.

Endpoint security policy	Profile	Defender for Endpoint security settings management	Microsoft Intune
Antivirus	Microsoft Defender Antivirus		
Antivirus	Microsoft Defender Antivirus exclusions		
Antivirus	Windows Security Experience	<i>Note 1</i>	
Attack Surface Reduction	Attack Surface Reduction Rules		
Endpoint detection and response	Endpoint detection and response		
Firewall	Firewall		
Firewall	Firewall Rules		

Enablement – Defender for Endpoint Settings

The screenshot shows the Microsoft 365 Defender interface under the 'Endpoints' section. The left sidebar includes options like 'Identities', 'Endpoints' (selected), 'Vulnerability management', 'Partners and APIs', 'Evaluation & tutorials', 'Configuration management', 'Email & collaboration', 'Investigations', 'Explorer', 'Review', 'Campaigns', 'Threat tracker', 'Exchange message trace', 'Attack simulation training', 'Policies & rules', 'Cloud apps', 'Cloud discovery', 'Cloud app catalog', 'OAuth apps', 'Files', 'Activity log', 'Governance log', and 'Policies'. The main content area shows the 'Endpoints' settings with a 'Search' bar at the top. The 'Enforcement scope' page is displayed, featuring sections for 'Security setting management' (with a note about MDE integration and a toggle switch 'On'), 'Use MDE to enforce security configuration settings from Intune' (with a toggle switch 'On'), 'Enable configuration management' (with a note about testing on specific devices), and a list of OS platforms with selection options ('Windows Client devices', 'Windows Server devices', 'Linux devices', 'macOS devices'). A green box highlights the 'Enforcement scope' link in the sidebar, and another green box highlights the 'MDE-Management' tag in the configuration management section.

Microsoft 365 Defender

Settings > Endpoints > Enforcement scope

Endpoints

SIEM

Rules

- Alert suppression
- Deception rules
- Indicators
- Process Memory Indicators
- Web content filtering
- Automation uploads
- Automation folder exclusions
- Asset rule management

Configuration management

- Enforcement scope** (highlighted with a green box)
- Intune Permissions

Device management

- Onboarding
- Offboarding

Network assessments

- Assessment jobs

Search

Security setting management

Allow security setting in Intune to be enforced by Microsoft Defender for Endpoint (MDE). This configuration setting will apply to devices that are not yet enrolled to Intune.

You'll need to turn on the integration in Microsoft Defender for Endpoint connector settings under Intune. For more information and pre-requisites, see [Security settings management for Microsoft Defender for Endpoint](#).

Use MDE to enforce security configuration settings from Intune

On

Enable configuration management

Choose which OS platforms to apply the settings on, then select which set of devices to implement it on. To test the feature on a specific set of devices, tag them with **MDE-Management**

Windows Client devices
 On all devices On tagged devices

Windows Server devices
 On all devices On tagged devices

Linux devices
 On all devices On tagged devices

macOS devices
 On all devices On tagged devices

Enablement –Microsoft Intune Settings

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Microsoft Defender for Endpoint

Search Refresh Save Discard Delete

The Microsoft Defender for Endpoint connection status is **Connected**. Click here to set up a compliance policy with the Microsoft Defender for Endpoint connector.

Microsoft Intune can enforce Endpoint Security profiles and configuration via supported agents independently of the device being managed by MDM or ConfigMgr. This allows you to protect devices running on these platforms. To protect devices on these platforms, click **Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations**.

Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations **On**

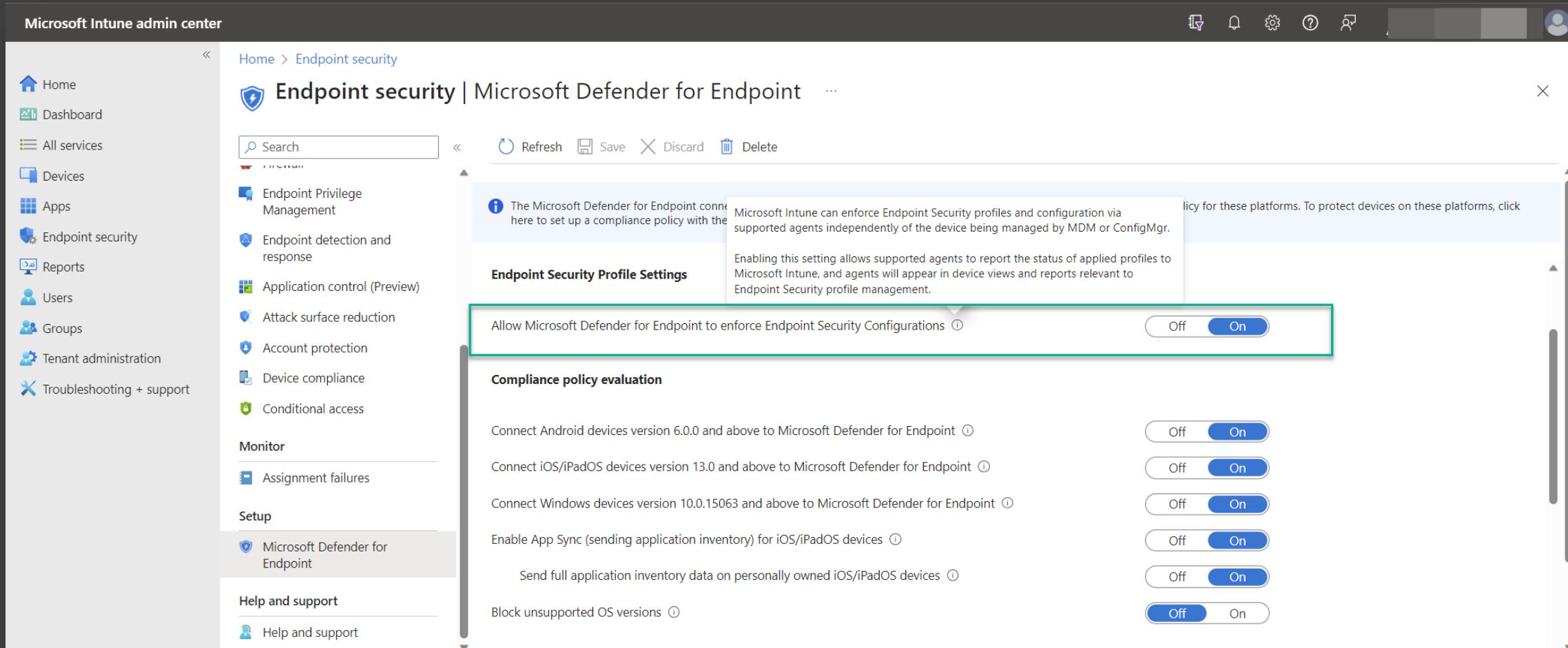
Compliance policy evaluation

- Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint **On**
- Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint **On**
- Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint **On**
- Enable App Sync (sending application inventory) for iOS/iPadOS devices **On**
- Send full application inventory data on personally owned iOS/iPadOS devices **On**
- Block unsupported OS versions **Off**

Microsoft Defender for Endpoint

Help and support

Help and support



Microsoft 365 Defender

Search

Device Inventory

2 devices are not protected
Onboard them now

Computers & Mobile Network devices IoT devices Uncategorized devices

Total 4 | High risk 0 | High exposure 0 | Not onboarded 0

Export Search

Filters: Tags: MDE-Management

Name	Domain	Risk level	Exposure level	OS platform	Windows version	Sensor health state	Onboarding status	Last device update	Tags	Managed by
X1-2	Workgroup	No known risks	Medium	macOS		Active	Onboarded	Aug 2, 2023 12:45 PM	MDE-Management	MDE
servermdc01	Workgroup	No known risks	No data available	Windows Server 20...	1809	Inactive	Onboarded	Jun 2, 2023 4:40 PM	MDE-Management	MDE
client11	AAD joined	No known risks	Medium	Windows 11	22H2	Active	Onboarded	Aug 2, 2023 8:50 PM	MDE-Management	Intune
linuxclient01	Workgroup	Medium	No data available	Linux		Inactive	Onboarded	Jun 6, 2023 8:53 PM	MDE-Management	MDE

Devices are tagged with 'MDE-Management'

Synthetic Device Registration in Azure AD and Device Group Membership

```
1 AuditLogs
2 | where TimeGenerated > ago (190d)
3 | where OperationName contains "Add device"
4 | extend Computer = tostring(TargetResources[0].displayName)
5
6
```

Results Chart Add bookmark

	TimeGenerated [UTC]	Computer	ResourceId	OperationName
<input type="checkbox"/>	5/30/2023, 8:51:02.085 AM	SERVERMDC01	/tenants/f50b6fb5-d3bc-4cff...	Add device
	TenantId	c46c4e10-5d81-409a-9fbb-3857dc9db495		
	SourceSystem	Azure AD		
	TimeGenerated [UTC]	2023-05-30T08:51		
	ResourceId	/tenants/f50b6fb5		
	OperationName	Add device		
	OperationVersion	1.0		
	Category	Device		

Home > avmtp lab | Groups > Groups | All groups > sg-MDEManaged-server

sg-MDEManaged-server | Members



Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Add members

Remove

Refresh

Bulk operations

Columns

Got feedback?

Direct members

All members

Search by name

Add filters

Name

Type

SERVERMDC01

Device

Policies visible in Microsoft Defender for Endpoint

The screenshot shows the Microsoft 365 Defender interface for the device **servermdc01**. The left sidebar includes icons for Devices, Home, Protection, Threats, Compliance, Identity, and Monitoring. The main navigation bar has links for Overview, Incidents and alerts, Timeline, Security recommendations, **Security policies**, Software inventory, Discovered vulnerabilities, and Missing KBs. The **Security policies** tab is selected. A search bar at the top right contains the placeholder "Search". On the right, a detailed view of the **MDE-WindowsServer-EndpointSecurity-Antivirus** policy is displayed, showing 20 items with their status: Success or Not applicable.

Setting name	Setting status	Error code
Allow Archive Scanning	Succeeded	0
Allow Behavior Monitoring	Succeeded	0
Allow Cloud Protection	Succeeded	0
Allow Email Scanning	Succeeded	0
Allow Full Scan On Mapped N...	Succeeded	0
Allow Network Protection Do...	Not applicable	0
Allow On Access Protection	Succeeded	0
Allow Realtime Monitoring	Succeeded	0
Allow Scanning Network Files	Succeeded	0
Allow Script Scanning	Succeeded	0
Allow User UI Access	Succeeded	0
Cloud Block Level	Succeeded	0

Microsoft 365 Defender

Search

Devices > servermdc01 > Configuration Management > Endpoint Security Policies > MDE-WindowsServer-EndpointSecurity-Antivirus

MDE-WindowsServer-EndpointSecurity-Antivirus

Antivirus

Delete Edit View in Intune

Overview Policy settings values Policy settings status Applied devices Assigned groups

Policy details

Description: Defender Antivirus Settings for MDE Managed Servers

Policy type: Microsoft Defender Antivirus

Policy category: Antivirus

Platform: windows10

Target: mdm.microsoftSense

Last Modified: May 30, 2023 11:31 AM

Policy settings status

Setting	Status	Count
Allow Archive Scanning	Success	1
Allow Behavior Monitoring	Success	1
Allow Cloud Protection	Success	1
Allow Email Scanning	Success	1
Allow Full Scan On Mapped Network Drives	Success	1

Success: 1
Error: 0
Conflict: 0
Not Applicable: 0

See all policy settings status See all applied devices

Applied devices check-in status

Success: 1
Error: 0
Conflict: 0
Not Applicable: 0

Assigned groups

Included

Group	Filter	Filter Mode
sg-MDEManaged-server	None	None



Devices > servermdc01 > Configuration Management > Endpoint Security Policies > MDE-WindowsServer-EndpointSecurity-Antivirus



MDE-WindowsServer-EndpointSecurity-Antivirus

Antivirus

Overview Policy settings values Policy settings status Applied devices Assigned groups

Settings

Allow Behavior Monitoring	Allowed. Turns on real-time behavior monitoring.
Allow Archive Scanning	Allowed. Scans the archive files.
Allow Cloud Protection	Allowed. Turns on the Microsoft Active Protection Service.
Allow Email Scanning	Allowed. Turns on email scanning.
Allow Full Scan On Mapped Network Drives	Not allowed. Disables scanning on mapped network drives.
Allow Realtime Monitoring	Allowed. Turns on and runs the real-time monitoring service.
Allow Scanning Network Files	Not allowed. Turns off scanning of network files.
Allow Script Scanning	Allowed.
Allow User UI Access	Allowed. Lets users access UI.
Cloud Block Level	High
Cloud Extended Timeout	50
Enable Network Protection	Enabled (block mode)
PUA Protection	PUA Protection on. Detected items are blocked. They will show in history along with other threats.
Real Time Scan Direction	Monitor all files (bi-directional).
Submit Samples Consent	Send all samples automatically.
Allow On Access Protection	Allowed.
Allow Network Protection Down Level	Network protection will be enabled downlevel.
Engine	

Microsoft 365 Defender

Devices > servermdc01 > Configuration Management > Endpoint Security Policies > MDE-WindowsServer-EndpointSecurity-Antivirus

MDE-WindowsServer-EndpointSecurity-Antivirus

Antivirus

Overview Policy settings values Policy settings status Applied devices Assigned groups

Device Name ↑	Check-in status	Last check-in time
SERVERMDC01	Success	May 30, 2023 12:32 PM

Search

Microsoft 365 Defender

Devices > servermdc01 > Configuration Management > Endpoint Security Policies > MDE-WindowsServer-EndpointSecurity-Antivirus

MDE-WindowsServer-EndpointSecurity-Antivirus

Antivirus

Overview Policy settings values Policy settings status Applied devices Assigned groups

Included

Group	Filter	Filter Mode
sg-MDEManaged-server	None	None

Excluded

Group
No results.

Search

- ≡ Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Dashboard
- Endpoint security policies

Device configuration management

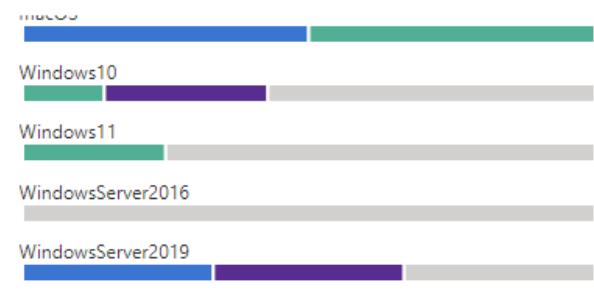
Device security management

17.9% devices security setting enforced by MDE

Understand which security configuration management tool is used on your devices. Data based on endpoints that were last seen in the past six months.

Tool	Count
MDE	5
Intune	4
ConfigMgr	3
Unknown	16

Security configuration by operating system:



Legend: MDE (Blue), Intune (Green), ConfigMgr (Purple), Unknown (Grey)

[View all devices](#)

Device Configuration Management Dashboard

View and manage all security profiles from the Microsoft 365 Defender portal

The screenshot shows the Microsoft 365 Defender portal interface. The left sidebar includes sections for Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints (selected), Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management (Dashboard selected), and Endpoint security policies. The main content area is titled "Endpoint Security Policies" and displays three tabs: Windows policies (selected), Mac policies, and Linux policies. A green box highlights the "Windows policies" tab. Below the tabs are buttons for "+ Create new Policy" and "Export". A search bar and filter options are also present. The main table lists the following policies:

Policy Name	Policy type	Policy category	Assigned	Platform	Target	Last modified
Defender for Endpoint Onboarding	Endpoint detection and response	Endpoint detection and response	true	windows10	mdm,microsoftSense	Aug 18, 2022 1:57 ...
MDE-WindowsServer-EndpointSecurity...	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	May 30, 2023 11:31...
MDE-WindowsServer-EndpointSecurity...	Attack Surface Reduction Rules	Attack surface reduction	true	windows10	mdm,microsoftSense	Jun 2, 2023 7:43 AM
MDE-WindowsServer-EndpointSecurity...	Microsoft Defender Firewall	Firewall	true	windows10	mdm,microsoftSense	May 30, 2023 8:22 ...
Windows-COPE-EndpointSecurity-Antiv...	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	Jun 15, 2023 11:34 ...
Windows-COPE-EndpointSecurity-ASR	Attack Surface Reduction Rules	Attack surface reduction	false	windows10	mdm,microsoftSense	May 24, 2023 8:10 ...
Windows-COPE-EndpointSecurity-ASR	Attack Surface Reduction Rules	Attack surface reduction	true	windows10	mdm,microsoftSense	Aug 2, 2023 9:13 PM

Devices managed by this capability check-in with Microsoft Intune every 90 minutes to update policy.

The screenshot shows the Microsoft 365 Defender portal interface. On the left, there's a navigation sidebar with various sections like Microsoft 365 Defender, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Dashboard, Endpoint security policies, and Email & collaboration. The main area displays a device overview for 'servermdc01'. The device icon is a blue circle with a white laptop. The status bar at the top says 'Devices > servermdc01'. Below the icon, the device name 'servermdc01' is displayed in bold. A risk summary shows 'No known risks'. The 'MDE-Management' tab is selected. The 'Overview' tab is active, showing device details such as Domain (Workgroup), OS (Windows Server 2019 64-bit (Release 1809 Build 17763.4377)), SAM name (Asset group Windows Server), Health state (Inactive), Data sensitivity (None), IP addresses (First seen 172.22.123.12, May 22, 2023 10:37:31 AM), and Last seen (Aug 3, 2023 8:56:48). To the right, a context menu is open, showing options like 'Device value', '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', 'Collect Support Logs', 'Action center', 'Download force release from isolation script', 'Go hunt', 'Turn on troubleshooting mode', and 'Policy sync'. The 'Policy sync' option is highlighted with a red box.

Microsoft 365 Defender

Devices > servermdc01

servermdc01

No known risks MDE-Management Windows Server

Overview Incidents and alerts Timeline Security recomm

Device details

Domain	OS
Workgroup	Windows Server 2019 64-bit (Release 1809 Build 17763.4377)
SAM name	Asset group Windows Server
Health state	Data sensitivity None
IP addresses	First seen 172.22.123.12 May 22, 2023 10:37:31 AM See IP addresses info
Last seen	Onboarding status Aug 3, 2023 8:56:48 Onboarded

Device value 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
- Collect Support Logs
- Action center
- Download force release from isolation script
- Go hunt
- Turn on troubleshooting mode
- Policy sync

Defender for
Endpoint

Deception

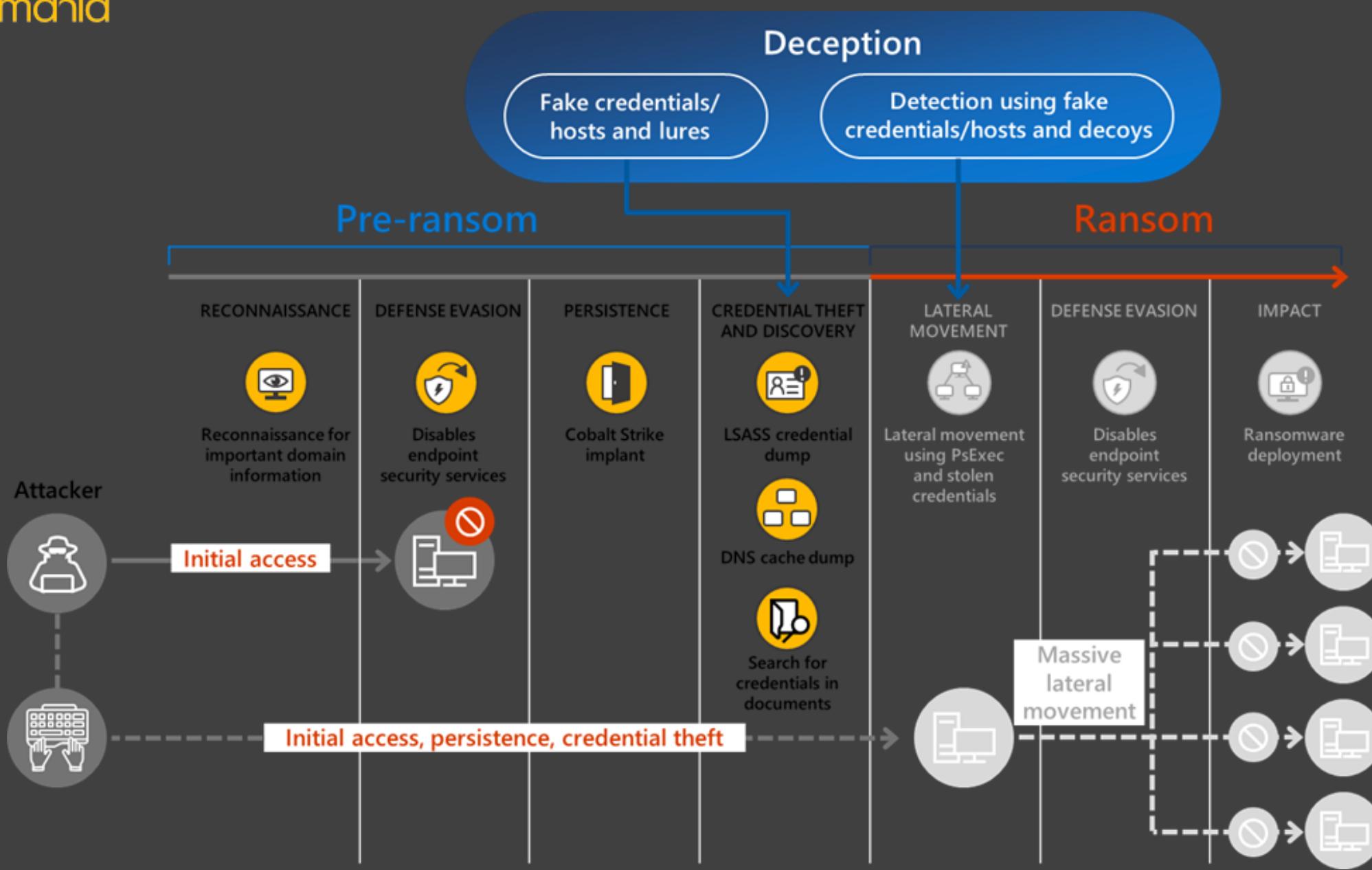
Microsoft Defender for Endpoint now includes deception as a built-in capability.

You can now create an artificial attack surface that entices adversaries to access assets you created just for them, and triggers high-fidelity, early-stage signal when accessed.

As a built-in capability, deception is generated and deployed automatically to add a new layer of protection for devices in your organization, while enabling the SOC team to speed up their response.

Deception in Defender for Endpoint provides customers with:

- **High confidence detections and automatic disruption of threats** – Detects human operated lateral movement in the early stages of a cyber-attack and triggers attack disruption to contain the threat.
- **AI-powered generation of authentic decoys and lures** – Defender for Endpoint uses machine learning to autogenerate and deploy authentic decoys and lures into your network that mirror production assets
- **Built into the existing endpoint agent** - no additional deployment or management of sensors on your network.
- **Integrated into the XDR SOC experience** – for easy, end to end investigation of attacks



What is deception?

Deception technologies help create an artificial cyber-attack surface within your network that consists of decoys and lures that look like high value assets to any outside adversary. The goal is to deceive attackers and lead them into accessing assets.

- **Decoys** – fake assets that trigger an alert when an attacker engages such as fake users and hosts
- **Lures** – are digital breadcrumbs that lead attackers to decoys and make them look more authentic, such as documents, batch files, and more.
 - **Basic lures** – planted documents, link files, and the like that have no or minimal interaction with the customer environment.
 - **Advanced lures** – planted content like cached credentials and interceptions that respond or interact with the customer environment. For example, attackers might interact with decoy credentials that were injected responses to Active Directory queries, which can be used to sign in.

Enable the Deception Feature

The screenshot shows the Microsoft 365 Defender interface under the 'Endpoints' settings. A green box highlights the 'Advanced features' section in the left sidebar. Another green box highlights the 'Deception' feature in the main list of options.

Endpoints

General

- Advanced features** (highlighted by a green box)
- Licenses
- Email notifications
- Auto remediation

Permissions

- Roles
- Device groups

APIs

- SIEM

Rules

- Alert suppression

Live Response unsigned script execution (On)

Enables using unsigned PowerShell scripts in Live Response.

Always remediate PUA (On)

When turned on, potentially unwanted applications (PUA) are remediated on all devices in your tenant. By default, PUA remediation is turned on.

Deception (On) (highlighted by a green box)

Manage and deploy lures and decoys to catch attackers in your environment. After you turn this on, go to Rules > Deception rules to run deception campaigns.

Share endpoint alerts with Microsoft Compliance Center (On)

Fowards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance [insider risk management](#) policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

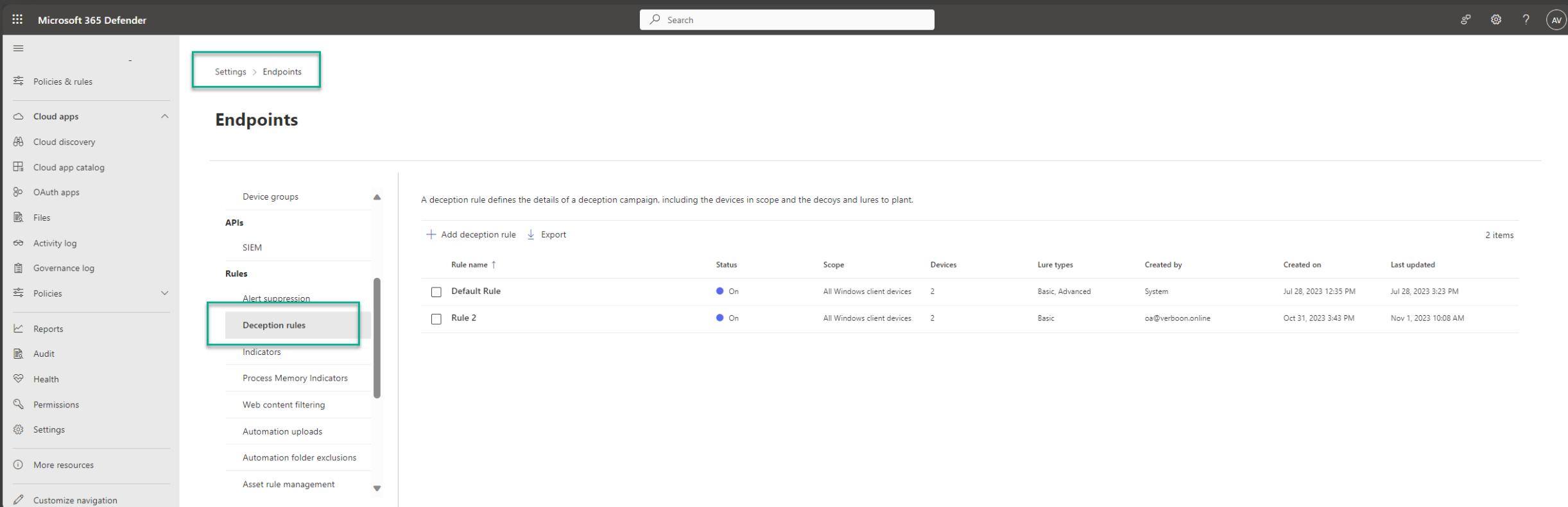
Microsoft Intune connection (On)

Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

Save preferences

Deception Rules



The screenshot shows the Microsoft 365 Defender interface, specifically the Endpoints section under Policies & rules. The left sidebar includes options like Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled 'Endpoints' and contains a search bar and a 'Deception rules' section. A callout box highlights the 'Deception rules' link in the sidebar. The 'Deception rules' section displays two items: 'Default Rule' and 'Rule 2'. Both rules are set to 'On' status, target 'All Windows client devices', and have 2 lure types (Basic, Advanced). The table includes columns for Rule name, Status, Scope, Devices, Lure types, Created by, Created on, and Last updated.

Microsoft 365 Defender

Search

Policies & rules

Cloud apps

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Reports

Audit

Health

Permissions

Settings

More resources

Customize navigation

Settings > Endpoints

Endpoints

A deception rule defines the details of a deception campaign, including the devices in scope and the decoys and lures to plant.

+ Add deception rule Export

Rule name ↑	Status	Scope	Devices	Lure types	Created by	Created on	Last updated
Default Rule	On	All Windows client devices	2	Basic, Advanced	System	Jul 28, 2023 12:35 PM	Jul 28, 2023 3:23 PM
Rule 2	On	All Windows client devices	2	Basic	oa@verboon.online	Oct 31, 2023 3:43 PM	Nov 1, 2023 10:08 AM

Device groups

APIs

SIEM

Rules

Alert suppression

Deception rules

Indicators

Process Memory Indicators

Web content filtering

Automation uploads

Automation folder exclusions

Asset rule management

2 items

Search

Demo Deception

Name and lure types

Scope

Decoys

Lures

Summary

Provide a name and choose lure types

Rule name *

Demo Deception

Description *

Demo Deception

Lure types ⓘ

Basic

- Plant documents, link files, and other files containing decoy information that attackers might utilize.

Advanced

- Plant cached user credentials and inject responses to Active Directory queries with decoy information that attackers might utilize.

Next

Search

Demo Deception

- Name and lure types
- Scope
- Decoys
- Lures
- Summary

Define rule scope

Choose the devices where you'd like to plant lures.

(i) Deception is currently applied only to Windows client devices.

Plant lures to *

All Windows client devices

Devices with specific tags

[Back](#) [Next](#)

Search

Demo Deception

- Name and lure types
- Scope
- Decoys
- Lures
- Summary

Manage decoy accounts and hosts

Decoys are nonexistent accounts and hosts. Attempts to use decoy information during lateral movement or other attacker activity will generate alerts.

+ Add new ▾ Edit Delete

Alias or Host name	Details	Type
jomt	Joe; mtplab	Account
albr	Alex; Brown	Account
Alex.Doe	Alex; Doe	Account
alinuxclient0020.verboon.online		Host
alinuxclient0020.verboon.online		Host
alinuxclient0043.verboon.online		Host
alinuxclient042.verboon.online		Host
alinuxclient026.verboon.online		Host

[Back](#) [Next](#)

Search

Demo Deception

- Name and lure types
- Scope
- Decoys
- Lures
- Summary

Lures

- Use autogenerated lures
Generated by the system
- Use custom lures only
Use lures created by your organization

[+ Add new lure](#)

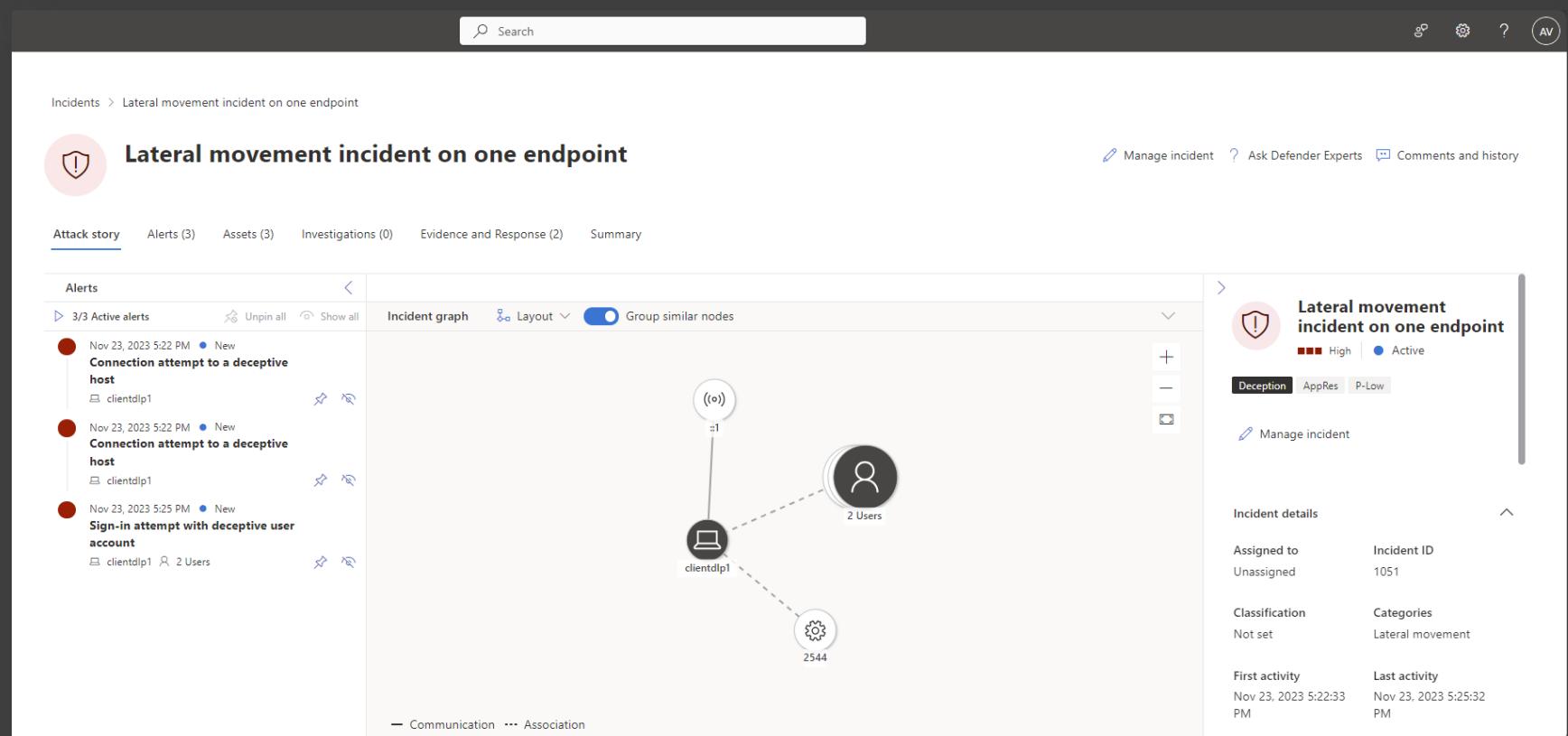
Lure name	Path	Plant on all devices in...	Plant as hidden
lure1.txt	C:\temp	✓	✓
lure2.txt	C:\temp	✓	✗
Finance Figures 2023.xlsx	C:\temp	✓	✗

[Back](#)[Next](#)

Incidents and alerts activated by deception

Alerts based on deception detection contain deceptive in the title. Some examples of alert titles are:

- Sign-in attempt with a deceptive user account
- Connection attempt to a deceptive host



3/3 Active alerts Unpin all Show all

Incident graph Layout Group similar nodes

Nov 23, 2023 5:22 PM • New
Connection attempt to a deceptive host
clientdlp1

Nov 23, 2023 5:22 PM • New
Connection attempt to a deceptive host
clientdlp1

Nov 23, 2023 5:25 PM • New
Sign-in attempt with deceptive user account
clientdlp1 2 Users

Communication --- Association

11/23/2023 5:25:32 PM

Attempted log on with a deceptive username Deception

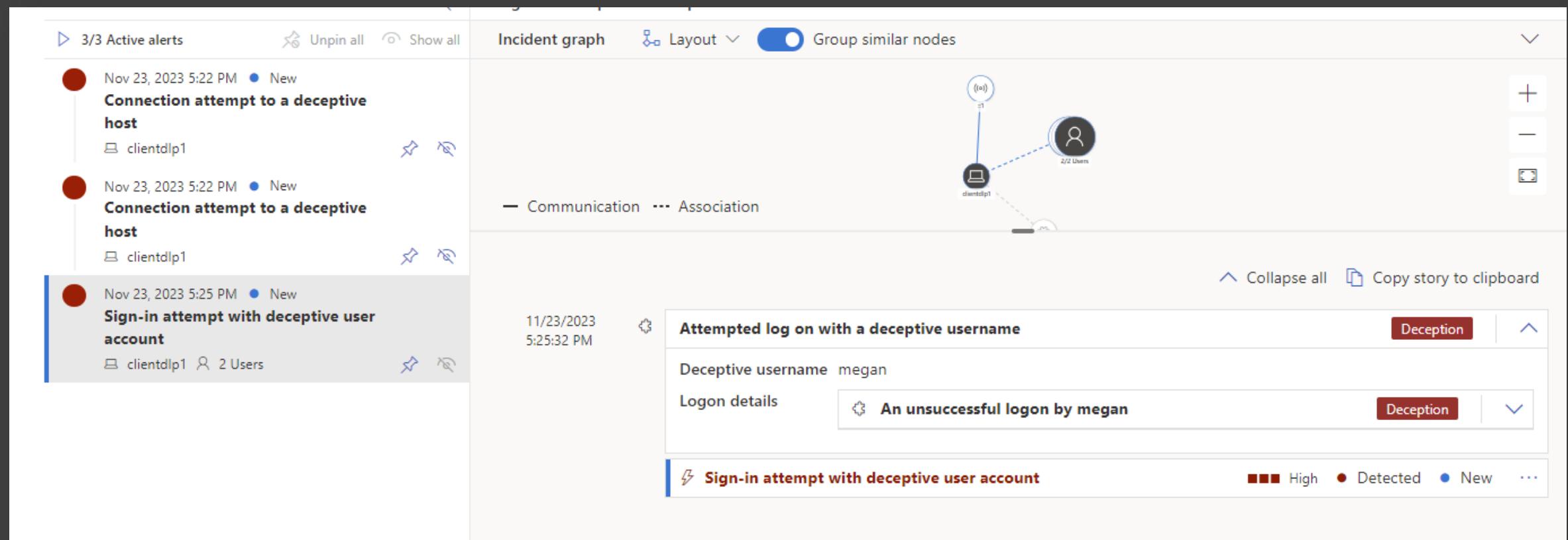
Deceptive username megan

Logon details An unsuccessful logon by megan Deception

Sign-in attempt with deceptive user account High Detected New ...

+ - []

Collapse all Copy story to clipboard



Microsoft
Defender for
Cloud Apps

App Governance

App Governance is a security and policy management capability designed for OAuth-enabled apps registered in Entra ID.

It delivers full visibility, remediation, and governance into how these apps and their users access, use, and share sensitive data stored in Microsoft 365 through actionable insights and automated policy alerts.

It also proactively helps organizations **maintain their app hygiene** by providing a view into OAuth apps that are unused, expiring or have unused credentials and ways to remediate these potential vulnerabilities.

App Governance add-on is now included in Defender for Cloud Apps at no additional cost.

If not already enabled, enable App Governance within the Microsoft Defender for Cloud Apps Settings

The screenshot shows the Microsoft Defender for Cloud Apps Settings interface. On the left, a navigation sidebar includes options like Campaigns, Threat tracker, Attack simulation training, Policies & rules, Cloud apps (selected), Cloud discovery, Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Reports, Health, Permissions, Settings (selected), More resources, and Customize navigation.

The main content area is titled "Cloud apps" under "Settings". It displays the "Service status" for "App governance". A callout box highlights the "Use app governance" toggle switch, which is currently off. Below it, a green banner indicates "App governance is on. Sign in again to start using it." The "Go to app governance" button is visible. A large "We're gathering insights to help you find and stop risky cloud apps" message is displayed, along with a note about preparation time and available insights.

Service status

Get comprehensive visibility and control over cloud apps that authenticate through Azure Active Directory, Google, and Salesforce. [Learn more about app governance](#)

Use app governance

Service status

App governance is on. Sign in again to start using it. X

Get comprehensive visibility and control over cloud apps that authenticate through Azure Active Directory, Google, and Salesforce. [Learn more about app governance](#)

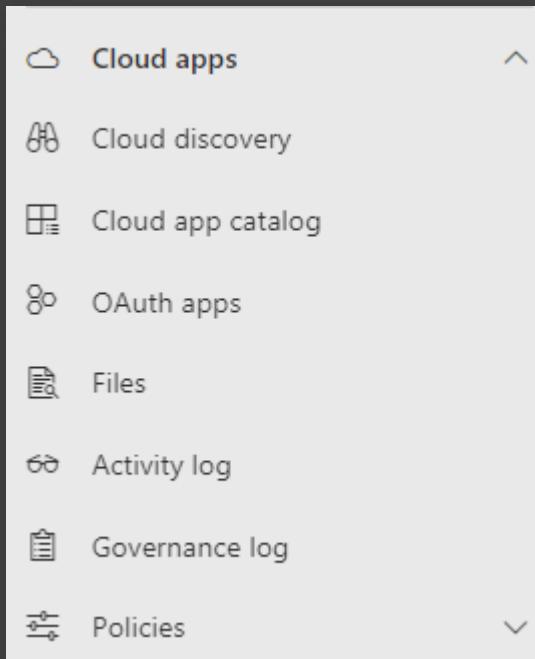
Use app governance

[Go to app governance](#)

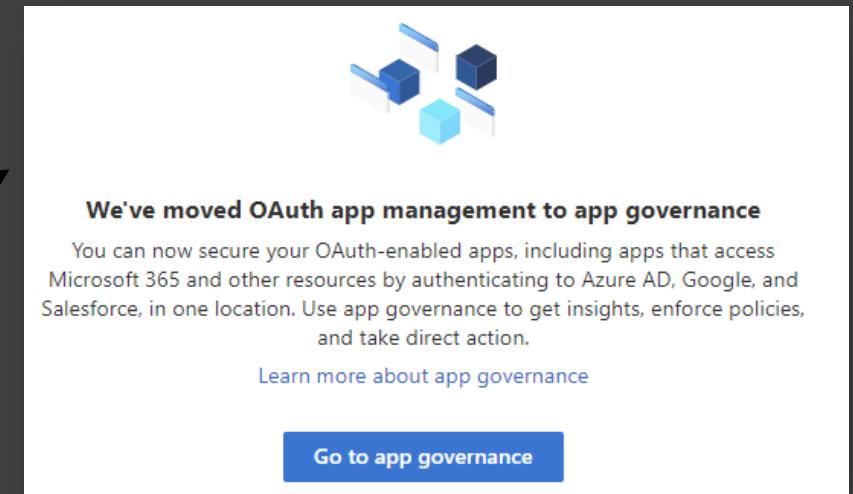
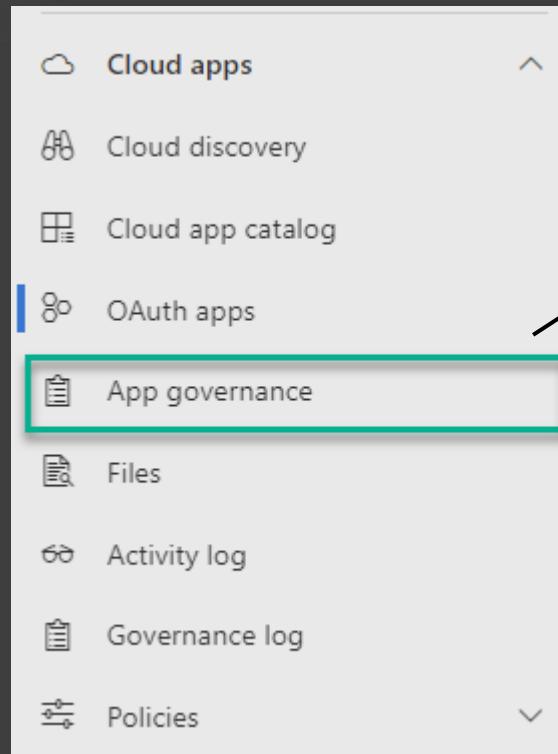
We're gathering insights to help you find and stop risky cloud apps

It can take up to 10 hours to prepare app governance. While you wait, learn more about our powerful insights, detecting malicious apps, and using predefined and custom policies.

Before App Governance enablement



After App Governance enablement



Before App Governance enablement

The screenshot shows the Microsoft Threat Intelligence Center interface. On the left, a navigation bar includes 'Threat tracker', 'Exchange message trace', 'Attack simulation training', 'Policies & rules', 'Cloud apps', 'Cloud discovery', 'Cloud app catalog', 'OAuth apps', 'Files', 'Activity log', 'Governance log', 'Policies', and 'Policy management'. The 'Policies & rules' section is expanded, showing various policy types like 'Activity policy', 'Cloud Discovery anomaly detection policy', 'File policy', etc. A modal window titled 'Filters' is open, showing a search bar for 'Name: Policy name', a dropdown for 'Type: Select type' (set to 'ACTIVE'), and buttons for 'Create policy', 'Export', and 'Status: ACTIVE'.

After App Governance enablement

The screenshot shows the Microsoft Threat Intelligence Center interface after App Governance has been enabled. The 'Policies & rules' section has been moved under the 'App governance' category. The 'App governance' section now includes policies such as 'Malicious OAuth app consent', 'Misleading publisher name for an OAuth app', 'Misleading OAuth app name', and 'Suspicious application consent'. A modal window titled 'Policy' is open, showing a search bar for 'Name: Policy name', a dropdown for 'Type: Select type' (set to 'ACTIVE'), and a list of policy types including 'Activity policy', 'Cloud Discovery anomaly detection policy', 'File policy', 'Ransomware activity', 'Malware detection policy', 'Anomaly detection policy', 'App discovery policy', 'Access policy', 'Session policy', 'OAuth app policy', 'OAuth app anomaly detection policy', and 'Malicious OAuth app consent'. The 'Malicious OAuth app consent' policy is highlighted with a green box.

The OAuth related policies are moved into App Governance

App Governance Overview

App governance

Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.

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 Identities Premium. Try Workload Identities

Overview [Azure AD](#) [Alerts](#) [Policies](#)

Apps

280 apps found 98 overprivileged apps 78 highly privileged apps

[View all apps](#)

Incidents

0 unresolved incidents 0 threat incidents 0 policy incidents

[View all incidents](#)

Latest incidents

Last Activity	Severity	Incident name	Source

Predefined policies

Your predefined policies ...

Watch out for alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.

Active predefined policies 12/12

[View predefined policies](#)

Apps that accessed Microsoft 365 services

Last 30 days

Service	Count
Teams	0/1
OneDrive	0/5

Sensitive data accessed

No items to show

Data usage

Data usage for various services and resources that were accessed using Graph API

Services

Service	March	April	May	June
OneDrive	~1500 GB	~1000 GB	~1000 GB	~2000 GB
Teams	~500 GB	~500 GB	~500 GB	~500 GB

App categories

All apps Highly privileged Overprivileged Unverified publisher ...

App name	App status	Permission type	Consent type	Publisher	Last modified
APD KardexPlus Task Managem...	Enabled	Delegated	Admin	N/A	Jan 1, 1970 1:0...
APD Mail Service	Enabled	Mixed	Admin	N/A	Jan 1, 1970 1:0...
Intranet (SP2010, mySite)	Enabled	Delegated	Admin	N/A	Jan 1, 1970 1:0...

[View all apps](#)

Resource types

Resource Type	March	April	May	June
Files	~1000 GB	~1000 GB	~1000 GB	~2000 GB
Chat and channel messages	~500 GB	~500 GB	~500 GB	~2000 GB

[View all incidents](#)

All Apps in Entra ID

App governance

Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.

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 Identities Premium. [Try Workload Identities](#)

Overview **Azure AD** Alerts Policies

Export 280 items Search Customize columns

Filter Save the query Reset Filters

API access: Any	Privilege level: Any	Permission usage: Any	Permission type: Any	Publisher verified: Any	Services accessed: Any	Sensitivity labels accessed: Any				
App name ↑	App status	Graph API access	Permission type	Consent type	Publisher	Last modified	Added on	Permission usage	Data usage	Privilege level
3CX Login OAuth	Enabled	Yes	Delegated	User (1)	N/A	Jan 1, 1970 1:00 AM	Dec 28, 2020 4:49 PM	N/A	0 (0%)	Low
aadapp-rc-prod	Enabled	Yes	Mixed	Admin	N/A	Jan 1, 1970 1:00 AM	Nov 3, 2021 7:27 PM	Some unused	0 (0%)	High
Abacus Mail	Enabled	Yes	Delegated	Admin	N/A	Jan 1, 1970 1:00 AM	Sep 29, 2022 4:09 PM	Some unused	0 (0%)	High
Across Terminology crossTerm Now - Dev	Enabled	No	Delegated	Admin	N/A	Jan 1, 1970 1:00 AM	Jan 27, 2022 10:28 AM	N/A	0 (0%)	None
Across Terminology crossTerm Now - Prod	Enabled	No	Delegated	Admin	N/A	Jan 1, 1970 1:00 AM	Jan 27, 2022 10:25 AM	N/A	0 (0%)	None
AD Rights Management (RMS)	Enabled	No	Delegated	Admin	N/A	Jan 1, 1970 1:00 AM	Dec 4, 2019 1:59 PM	N/A	0 (0%)	None
AddEvent.com	Enabled	Yes	Delegated	User (12)	N/A	Jan 1, 1970 1:00 AM	Jan 1, 1970 1:00 AM	Some unused	0 (0%)	Low
Adobe Acrobat	Enabled	Yes	Delegated	Admin	Adobe Inc.	Jan 1, 1970 1:00 AM	May 19, 2023 6:04 PM	Some unused	0 (0%)	High
Adobe Acrobat	Enabled	Yes	Delegated	User (4)	N/A	Jan 1, 1970 1:00 AM	Jan 1, 1970 1:00 AM	N/A	0 (0%)	Low
Adobe Acrobat Reader	Enabled	Yes	Delegated	User (1)	Adobe Inc.	Jan 1, 1970 1:00 AM	Mar 23, 2021 12:26 PM	Some unused	0 (0%)	High

App governance

Get in-depth visibility and control over OAuth apps integrated with Azure Ac

Starting June 1, 2023, management of unused apps, unused credentials, and expirin

Overview Azure AD

Export

Filter Save the query Reset Filters

API access: Any Privilege level: Any Permission usage: All

App name	App status	①
Cohesity-API-05	Enabled	
Cohesity-API-01	Enabled	
Cohesity-API-03	Enabled	
Cohesity-API-02	Enabled	
Cohesity-API-04	Enabled	
Cloud Sync for SharePoint	Enabled	



Cohesity-API-05

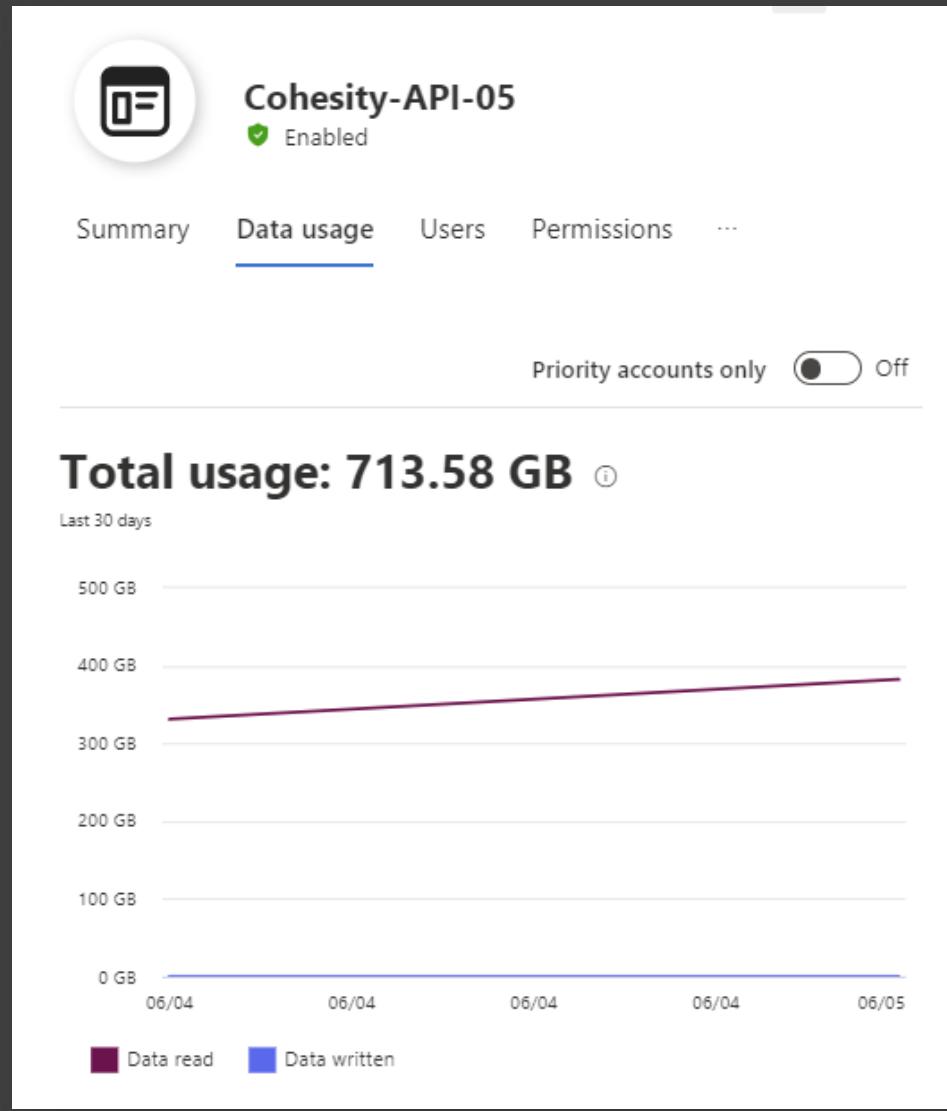
Enabled

Summary Data usage Users Permissions Sensitivity labels

App name	App ID
Cohesity-API-05	0d9f342e-1f8a-4ba1-b8d1-c06438b68f35
View in Azure AD	
Graph API access	Consent type
Yes	Admin
Added on	Last modified
12/6/2021	1/1/1970
Last action	Publisher verification
-	Unverified
Learn more about publisher verification	
Certification	Community use
No certification	Rare
Learn more about Microsoft 365 certification	
App activities	Consent grants
All app activities in the last 30 days	All app consent grants in the last 30 days
View app activities in hunting	
View consent grants in hunting	

Get insights about Apps

- Summary
- Data Usage
- Users
- Permissions
- Sensitivity labels



Usage details

Last 30 days

OneDrive

Resource	Uploaded	Downloaded	Total
Files	0 (0)	86642 (711.39 GB)	86642 (711.39 GB)

SharePoint

Resource	Uploaded	Downloaded	Total
Files	0 (0)	134 (2.19 GB)	134 (2.19 GB)

The screenshot shows the 'Summary' tab for the service principal 'Cohesity-API-05'. It displays key statistics and navigation links.

Cohesity-API-05 Enabled

Summary Data usage Users Permissions ...

Summary ⓘ

Total consented users: 5174 | Priority accounts: 40

Permissions

Cohesity-API-05
Enabled

Summary Data usage Users Permissions ...

Permission summary

Total permissions **29** | High privilege **7** | Unused permissions **8**

Graph API permissions ⓘ

Permission	Privilege level	In use	Type
Files.Read.All	High	No	Application
Sites.ReadWrite.All	High	No	Application
Channel.Create	Low	No	Application
Sites.FullControl.All	High	No	Application
Files.ReadWrite.All	High	No	Application
Sites.Read.All	Low	No	Application
Channel.ReadBasic.All	Low	No	Application

Permission	API	Type
TermStore.ReadWrite.All	Office 365 SharePoint Online	Application
TermStore.ReadWrite.All	Office 365 SharePoint Online	Delegated
MyFiles.Read	Office 365 SharePoint Online	Delegated
AllSites.Read	Office 365 SharePoint Online	Delegated
User.ReadWrite.All	Office 365 SharePoint Online	Delegated
AllSites.Manage	Office 365 SharePoint Online	Delegated
Sites.Search.All	Office 365 SharePoint Online	Delegated
MyFiles.Write	Office 365 SharePoint Online	Delegated
Sites.Manage.All	Office 365 SharePoint Online	Application
AllSites.FullControl	Office 365 SharePoint Online	Delegated

Advanced Hunting

Cohesity-API-05
Enabled

Summary Data usage Users Permissions Sensitivity labels

App name
Cohesity-API-05

App ID
0d9f342e-1f8a-4ba1-b8d1-c06438b68f35
[View in Azure AD](#)

App activities
All app activities in the last 30 days
[View app activities in hunting](#)

Consent grants
All app consent grants in the last 30 days
[View consent grants in hunting](#)

Cohesity-API-05
Enabled

Summary Data usage Users Permissions Sensitivity labels

App name
Cohesity-API-05

App ID
0d9f342e-1f8a-4ba1-b8d1-c06438b68f35
[View in Azure AD](#)

App activities
All app activities in the last 30 days
[View app activities in hunting](#)

Consent grants
All app consent grants in the last 30 days
[View consent grants in hunting](#)

Query

ⓘ Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```

1 // Find all the activities involving the cloud app in last 30 days
2 let now = now();
3 let appId = (i : dynamic)
4 {
5     case
6     (
7         i.Workload == "SharePoint", i.ApplicationId,
8         i.Workload == "Exchange", iff(isempty(i.ClientAppId), i.AppId, i.ClientAppId),
9         i.Workload == "OneDrive", i.ApplicationId,
10        i.Workload == "MicrosoftTeams", i.AppAccessContext.ClientAppId,
11        "Unknown"
12    )
13 };
14 CloudAppEvents
15 | where ((RawEventData.Workload == "SharePoint" or RawEventData.Workload == "OneDrive") and (ActionType == "FileUploaded" or ActionType == "FileDownloaded"))
16 | extend AppId = appId(RawEventData)
17 | where AppId == [REDACTED]
18 | where Timestamp between (datetime("2023-05-07 00:00:00Z")..30d)
19 | extend tostring(RawEventData.Id)
20 | summarize arg_max(Timestamp, *) by RawEventData_Id
21 | sort by Timestamp desc
22 | project Timestamp, OAuthApplicationId = AppId, ReportId, AccountId, AccountObjectId, AccountDisplayName, IPAddress, UserAgent, Workload = tostring(
23 | limit 1000
24

```

Advanced hunting

ⓘ Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

> [Run query](#) [Save](#) [Share link](#)

Query

```

1 // Find all the consent grant activities related to the cloud app in last 30 days
2 CloudAppEvents
3 | where RawEventData.ApplicationId == [REDACTED]
4 | where RawEventData.Workload == "AzureActiveDirectory"
5 | where ActionType == "Consent to application."
6 | where Timestamp between (datetime("2023-05-07 00:00:00Z")..30d)
7 | extend tostring(RawEventData.Id)
8 | summarize arg_max(Timestamp, *) by RawEventData_Id
9 | sort by Timestamp desc
10 | project Timestamp, OAuthApplicationId = tostring(RawEventData.ObjectId), ReportId, AccountId, AccountDisplayName, ActionType, tostring(RawEventData.
11 | limit 1000

```

Mitre Att&ck Mapping

MITRE Att&ck	Description
Initial Access	App redirects to phishing URL by exploiting OAuth redirection vulnerability
Initial Access	OAuth App with suspicious Reply URL
Initial Access	App created recently has low consent rate
Initial Access	App with bad URL reputation
Initial Access	Encoded app name with suspicious consent scopes
Initial Access	OAuth App with Read scopes has suspicious Reply URL
Initial Access	App with unusual display name and unusual TLD in Reply domain
Initial Access	New app with mail permissions having low consent pattern
Initial Access	New app with low consent rate accessing numerous emails
Initial Access	Suspicious app with mail permissions sending numerous emails
Persistence	App made anomalous Graph calls to Exchange workload post certificate update or addition of new credentials
Persistence	App with suspicious OAuth scope was flagged high-risk by Machine Learning model, made graph calls to read email and created Inbox Rule
Persistence	App with suspicious OAuth scope made graph calls to read email and created inbox rule
Persistence	App accessed from unusual location post certificate update
Persistence	App accessed from unusual location made anomalous Graph calls post certificate update
Persistence	App created recently has a high volume of revoked consents

Mitre Att&ck Mapping

MITRE Att&ck	Description
Privilege escalation	OAuth app with suspicious metadata has Exchange permission
Defense Evasion	App impersonating a Microsoft logo
Defense Evasion	App is associated with a typosquatted domain
Discovery	App performed drive enumeration
Discovery	Suspicious enumeration activities performed using Azure Active Directory PowerShell
Discovery	Recently created multitenant application enumerates users information frequently
Exfiltration	OAuth App using unusual user agent
Exfiltration	App with an unusual user agent accessed email data through Exchange Web Services
Collection	App made unusual email search activities
Collection	App made anomalous Graph calls to read e-mail
Collection	App creates inbox rule and made unusual email searches activities
Collection	App made OneDrive / SharePoint search activities and created inbox rule
Collection	App made numerous searches and edits in OneDrive
Collection	App made high volume of importance mail read and created inbox rule
Collection	Privileged app performed unusual activities in Teams
Collection	Anomalous OneDrive activity by app that just updated or added new credentials
Collection	Anomalous SharePoint activity by app that just updated or added new credentials

predefined policies

Policy name	Description	Severity
Unusual activity from an app with priority account consent	Find unusual increases in either data usage or Microsoft Graph API access errors exhibited by application that has been given consent by a priority account. The attempts potentially indicate known tactics used by adversaries to access and retrieve sensitive information from the organization.	Medium
New app with low consent rate	This detection identifies an OAuth application that was created recently and found to have low consent rate. This can indicate a malicious or risky app that lure users in illicit consent grants via phishing or other redirection methods of attack.	Medium
App created numerous inbox rules	An app made a high volume of Graph API calls to create Exchange inbox rules. This app might be involved in data collection and exfiltration or other attempts to access and retrieve sensitive information	Medium
Increase in data usage by an overprivileged or highly privileged app	An App with high privileged or over privileged permissions that exhibit sudden increases in data usage. This app might be involved in data collection and exfiltration or other attempts to access and retrieve sensitive information	Medium
Increase in app API calls to EWS	This detection generates alerts for non-Microsoft OAuth apps that exhibit a significant increase in calls to the Exchange Web Services (EWS) API. This app might be involved in data exfiltration or other attempts to access and retrieve sensitive data.	Medium
Increase in app activity on SharePoint	This detection generates alerts for non-Microsoft OAuth apps that exhibit significant increases in Graph API calls to SharePoint within a 30-day window. This app might be involved in data exfiltration or other attempts to access and retrieve sensitive data.	Medium
Suspicious app with access to multiple M365 services	This detection generates alerts for non-Microsoft OAuth apps, with access to multiple Microsoft 365 services, that exhibit a significant increase in Graph API calls within a few days after its certificates/secrets are updated or new credentials are added. By checking the apps for compromise, you can prevent lateral movement, data exfiltration, and other malicious activities that traverse cloud folders, emails, and other services.	Medium
Access to sensitive data	Find apps that access data with sensitivity labels.	Medium
Increase in app activity on Exchange	This detection generates alerts for non-Microsoft OAuth apps that exhibit significant increase in Graph API calls to Exchange. This app might be involved in data exfiltration or other attempts to access and retrieve sensitive data.	Medium
App sent Exchange email numerous times	An app made a large number of Graph API calls to send email messages using Exchange Online. This app might be involved in data collection and exfiltration or other attempts to access and retrieve sensitive information.	Medium
Increase in app activity on OneDrive	This detection generates alerts for non-Microsoft OAuth apps that exhibit significant increases in Graph API calls to OneDrive within a 30-day window. This app might be involved in data exfiltration or other attempts to access and retrieve sensitive data.	Medium
App searched Exchange content numerous times	A cloud app made a high volume of Graph API calls to search Exchange email content. This app might be involved in data collection or other attempts to access and retrieve sensitive information	Medium

Secure Score

Home

Incidents & alerts

Incidents

Alerts

Hunting

Actions & submissions

Threat intelligence

Secure score

Learning hub

Email & collaboration

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

Filters: Product: App governance X

Rank	Recommended action	Score impact	Points achieved	Status
1	Regulate apps with priority account consent	+0.58%	7/7	Completed
2	Regulate cloud app access to sensitive data	+0.58%	7/7	Completed

Filter

Clear filters

...
Yes

Product

App governance

Azure Active Directory

Citrix ShareFile

Defender for Endpoint

Defender for Identity

Defender for Office

Apply Cancel

Microsoft
Defender for
Endpoint

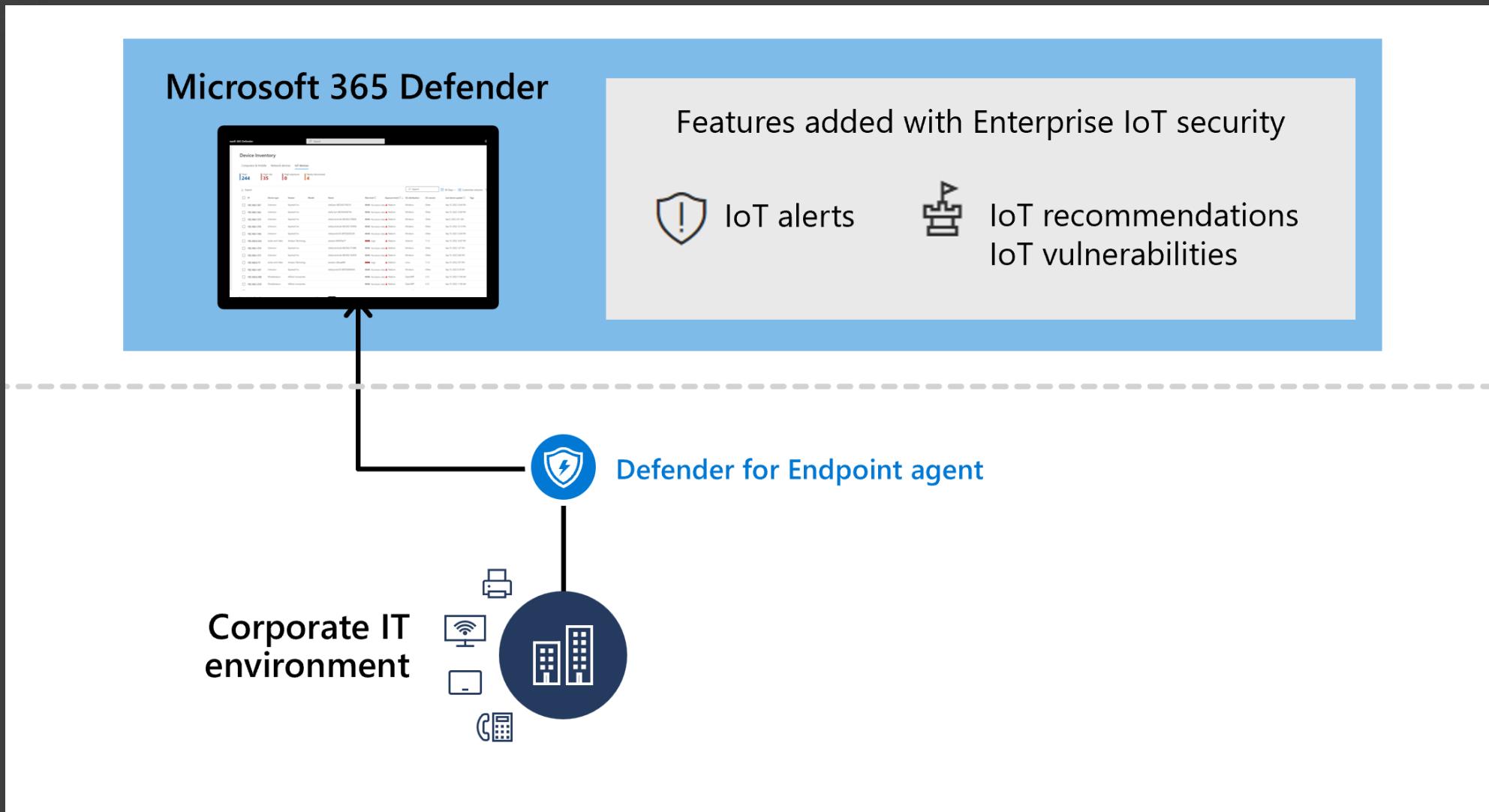
Enterprise IoT security is
now included in
Microsoft 365 E5 and E5
Security plans

To help organizations achieve a more holistic endpoint security strategy that traverses both IT and eloT devices easily, Microsoft announced that the eloT security capabilities of Microsoft Defender for IoT are now included with Microsoft 365 E5 and E5 Security plans at no additional cost for new and existing customers.

This will enable security teams to:

- Eliminate critical blind spots by discovering **unmanaged** enterprise IoT devices
- Identify **anomalies** across the eloT device estate with continuous monitoring
- Harden posture across eloT with **vulnerability** assessments with actionable guidance to help remediate at-risk devices

Architecture and extra features added with Enterprise IoT security in Microsoft 365 Defender



Enable Enterprise IoT in Defender for Endpoint (It's FREE with E5 Security)

The screenshot shows the Microsoft 365 Defender interface with the 'Device discovery' settings page selected. The left sidebar lists various security categories like Policies & rules, Cloud apps, and Activity log. The main content area is titled 'Device discovery' and includes sections for Discovery setup, Exclusions, Monitored networks, Enterprise IoT, and Authenticated scans. The 'Enterprise IoT' section is highlighted with a grey background. It contains a descriptive text about enabling enterprise IoT security, mentioning unmanaged IoT devices, vulnerability data, and recommendations. A toggle switch is set to 'On', and a callout bubble provides a tooltip: 'Gain access to vulnerability data and recommendations for your IoT devices'. A 'Save' button is at the bottom.

Microsoft 365 Defender

Search

Policies & rules

Cloud apps

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Reports

Audit

Settings > Device discovery

Device discovery

Discovery setup

Exclusions

Monitored networks

Enterprise IoT

Authenticated scans

On

Gain access to vulnerability data and recommendations for your IoT devices

Save

EIOT Device Inventory

Computers & Mobile Network devices IoT devices Uncategorized devices

Total **586** | High risk **0** | High exposure **2** | Newly discovered **6**

[Export](#)

<input type="checkbox"/> IP	Name	Device type	Vendor	Model	Risk level ⓘ	Exposure level ⓘ ↑	OS distribution	OS version	Last device update ⓘ
<input type="checkbox"/> 10.30.2.215	[REDACTED]	Printer	HP		██████ No known ri...	▲ High	Unix	Other	Nov 20, 2023 6:01 AM
<input type="checkbox"/> 10.30.0.91	[REDACTED]	Printer	HP		██████ No known ri...	▲ High	Unix	Other	Nov 20, 2023 5:02 AM
<input type="checkbox"/> 10.1.41.95	[REDACTED]	Miscellaneous	WonderMedia Tech...	SmartStream	██████ No known ri...	▲ Low	Linux	Other	Nov 20, 2023 1:21 AM
<input type="checkbox"/> 10.1.47.160	[REDACTED]	Communication	Beward R&D Co., Ltd	1.3 MP H.264 Vand...	██████ No known ri...	▲ Low	EmbeddedOs	Other	Nov 20, 2023 9:20 AM
<input type="checkbox"/> 10.49.12.52	[REDACTED]	Printer	Canon	LBP214	██████ No known ri...	▲ Low	EmbeddedOs	Other	Nov 20, 2023 12:02 AM
<input type="checkbox"/> 172.30.30.34	[REDACTED]	Miscellaneous	WonderMedia Tech...	SmartStream	██████ No known ri...	▲ Low	Linux	Other	Nov 20, 2023 1:19 AM
<input type="checkbox"/> 10.49.12.4	[REDACTED]	Printer	Canon	MF745C	██████ No known ri...	▲ Low	EmbeddedOs	1003	Nov 20, 2023 12:03 AM

Security Recommendations

The screenshot shows a web-based security management interface. On the left is a vertical sidebar with icons for navigation. The main header area includes a user profile icon, a blurred computer name, and a status bar indicating 'No known risks' and 'Active'. Below the header is a navigation bar with tabs: Overview, Incidents and alerts, Timeline, Security recommendations (which is highlighted with a red box), Software inventory, Discovered vulnerabilities, Security policies, and Advanced features. Underneath the tabs is a section for 'Export' and 'Filters: Status: Active +1' with a close button. The main content area displays a table of security recommendations:

Security recommendation	Weaknesses	Related component	Threats	Remediation type
<input type="checkbox"/> Update Samba	49	Samba		Software update
<input type="checkbox"/> Disable insecure administration protocol – Telnet	1	Network		Configuration change
<input type="checkbox"/> Remove insecure administration protocols SNMP V1 and SNMP V2	1	Network		Configuration change

Vulnerabilities

HNZ-ZAB-01

■■■■ No known risks ● Active

Overview Incidents and alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Security policies Advanced features

Export

Name	Severity ↓	CVSS	Related Software	Published on	First detected ⓘ	Updated on	Threats	Tags
<input type="checkbox"/> CVE-2021-44142	■■■■ Critical	9.9	Oracle Ctdb (+ 349 more)	Jan 31, 2022 1:00 AM	Jan 31, 2022 1:00 AM	Nov 7, 2023 4:39 AM	⌚ ⚡	
<input type="checkbox"/> CVE-2004-1154	■■■■ High	10.0	Samba (+ 2 more)	Jan 10, 2005 6:00 AM	Aug 18, 2021 2:03 PM	Oct 30, 2018 5:25 PM	⌚ ⚡	
<input type="checkbox"/> CVE-2022-42898	■■■■ High	8.8	Oracle Krb5 (+ 186 more)	Nov 15, 2022 1:00 AM	Nov 15, 2022 1:00 AM	Oct 8, 2023 11:15 AM	⌚ ⚡	
<input type="checkbox"/> CVE-2003-0085	■■■■ High	10.0	Samba (+ 2 more)	Mar 31, 2003 7:00 AM	Aug 18, 2021 2:03 PM	Oct 19, 2018 5:29 PM	⌚ ⚡	
<input type="checkbox"/> CVE-2004-2687	■■■■ High	9.3	Samba (+ 2 more)	Dec 31, 2004 6:00 AM	Aug 18, 2021 2:03 PM	Sep 5, 2008 6:00 AM	⌚ ⚡	
<input type="checkbox"/> CVE-2012-1182	■■■■ High	10.0	Oracle Samba (+ 138 more)	Apr 10, 2012 2:00 AM	Aug 18, 2021 2:03 PM	Jun 15, 2023 2:00 AM	⌚ ⚡	
<input type="checkbox"/> CVE-2017-9461	■■■■ High	7.5	Oracle Samba (+ 60 more)	Feb 9, 2017 1:00 AM	Aug 18, 2021 2:03 PM	Nov 7, 2023 3:50 AM	⌚ ⚡	

Microsoft Defender for Endpoint

Tamper protection for
exclusions

Tamper protection is a feature of Microsoft Defender for Endpoint that prevents antivirus tampering and misconfiguration by malicious apps and actors. Microsoft Intune and Microsoft Defender for Endpoint integrate to allow enterprises to selectively enable and disable tamper protection in their environment.

Microsoft has enabled functionality that protects path, process, and extension exclusions deployed through Intune.

When tamper protection is combined with the `DisableLocalAdminMerge` setting **exclusions and `DisableLocalAdminMerge` will be protected by tamper protection.**

This means that any exclusions configured by other processes will be explicitly ignored and only intended exclusions are applicable on the device.

Enable tamper protection at the tenant level

Home > Endpoint security | Antivirus > Security Experience

Security Experience | Properties ...

Search <<

Overview

Basics Edit

Overview

Name

Manage

Description

Properties

Platform

Monitor

Assignments Edit

Device status

Included groups

Intune-Device-SecureCore

User status

Excluded groups

--

Per-setting status

Scope tags Edit

Default

Configuration settings Edit

^ Settings

^ Windows Security

Enable tamper protection to prevent Microsoft Defender being disabled ⓘ

Enable



OR

Enable tamper protection through Intune

Windows-COPE-EndpointSecurity-Antivirus | Properties ...

Search <<

Overview

Basics Edit

Overview

Name

Windows-COPE-EndpointSecurity-Antivirus

Manage

Description

Security baseline for Windows 10, version 21H2

Properties

Platform

Windows 10 and later

Monitor

Assignments Edit

Device status

Included groups

Intune-Device-SecureCore
My-Cloud-Configured-PCs

User status

Excluded groups

--

Per-setting status

Scope tags Edit

Default

Configuration settings Edit

Settings

Cloud protection

Microsoft Defender Antivirus Exclusions

Disable local admin merge ⓘ

Yes

0 items

Defender Processes to exclude ⓘ

Disable local admin merge

This policy setting controls whether or not exclusion list settings configured by a local administrator are merged with managed settings. This setting applies to lists such as threats and exclusions. If you disable or do not configure this setting, unique items defined in preference settings configured by the local administrator will be merged into the resulting effective policy. In the case of conflicts, management settings will override preference settings. If you enable this setting, only items defined by management will be used in the resulting effective policy. Managed settings will override preference settings configured by the local administrator.

Windows-COPE-EndpointSecurity-Antivirus | Properties

Search < Microsoft Defender Antivirus Exclusions

Disable local admin merge: Yes

Defender Processes to exclude: 0 items

File extensions to exclude from scans and real-time protection: 2 items

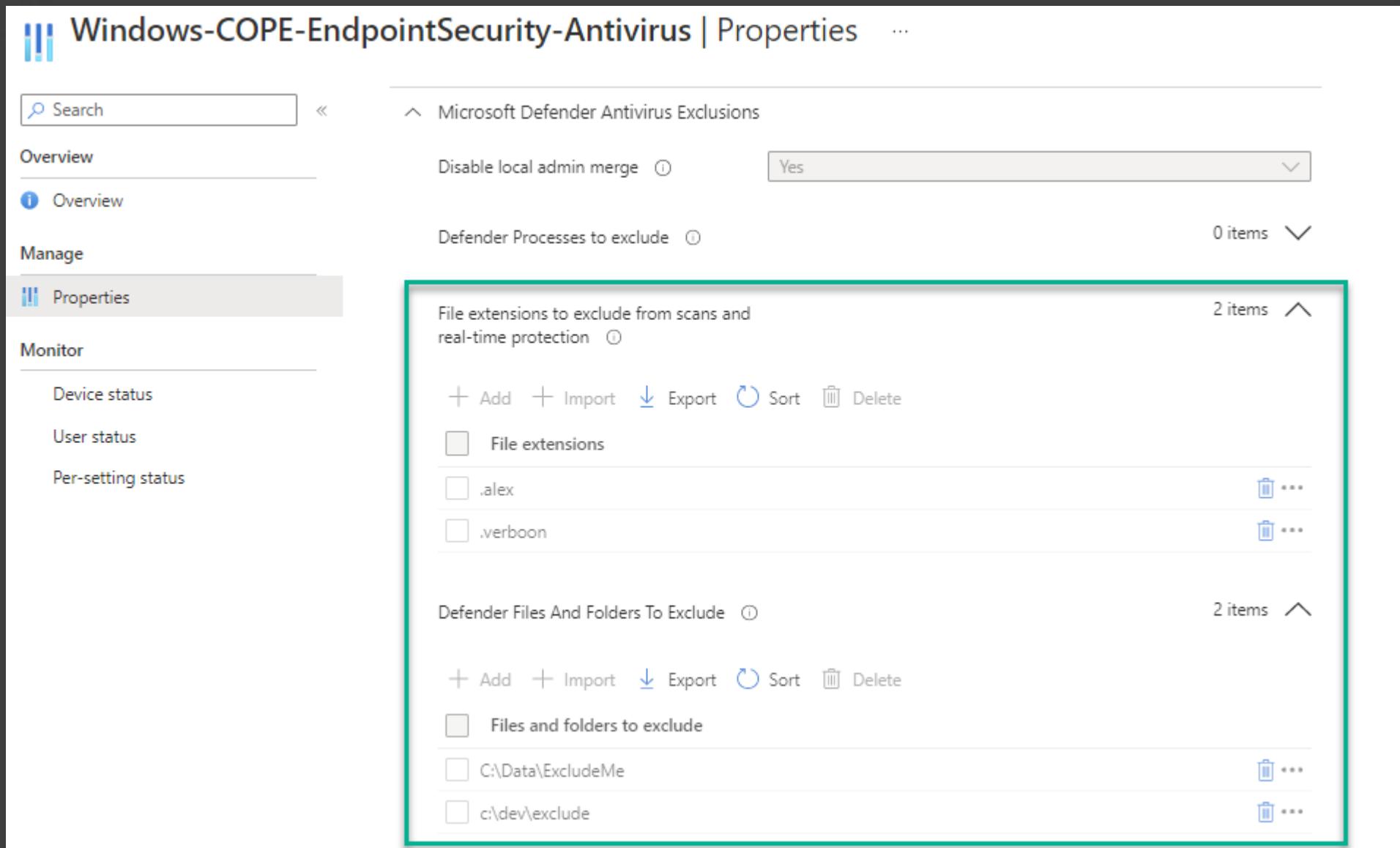
+ Add + Import Export Sort Delete

- File extensions
- .alex
- .verboon

Defender Files And Folders To Exclude: 2 items

+ Add + Import Export Sort Delete

- Files and folders to exclude
- C:\Data\ExcludeMe
- c:\dev\exclude



Exclusion
settings

*Just an
example for
illustration
purposes*

Verify Tamper Protection is enabled, and Exclusions configured within Intune are set

The image shows two screenshots of the Windows Security settings interface.

Left Screenshot: Tamper Protection

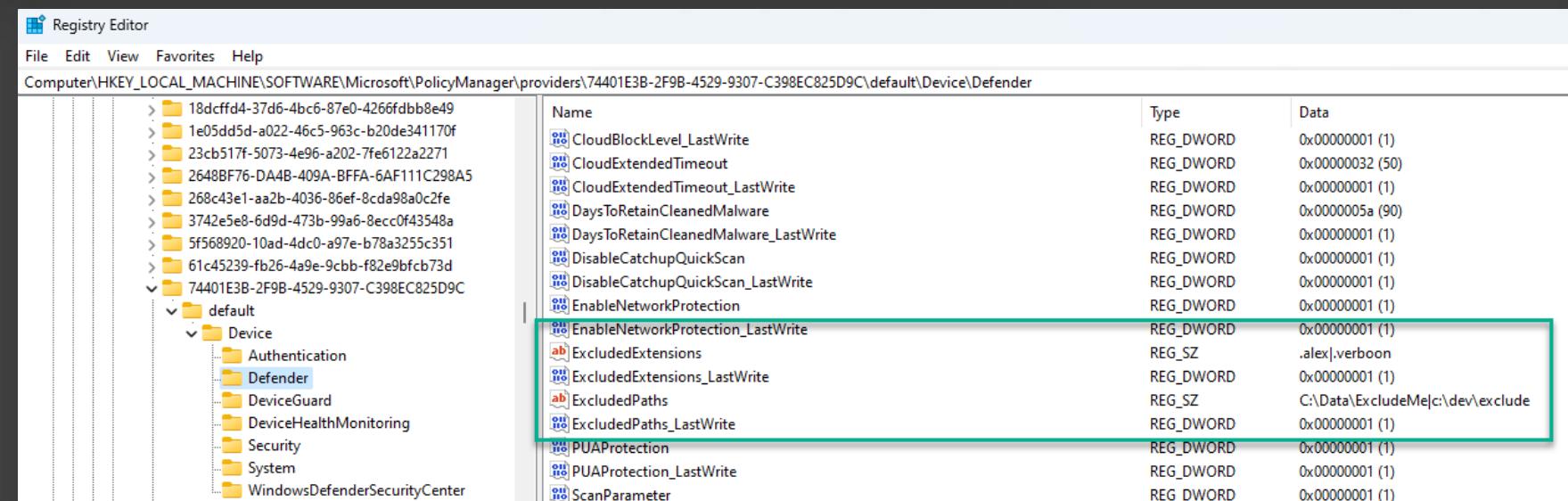
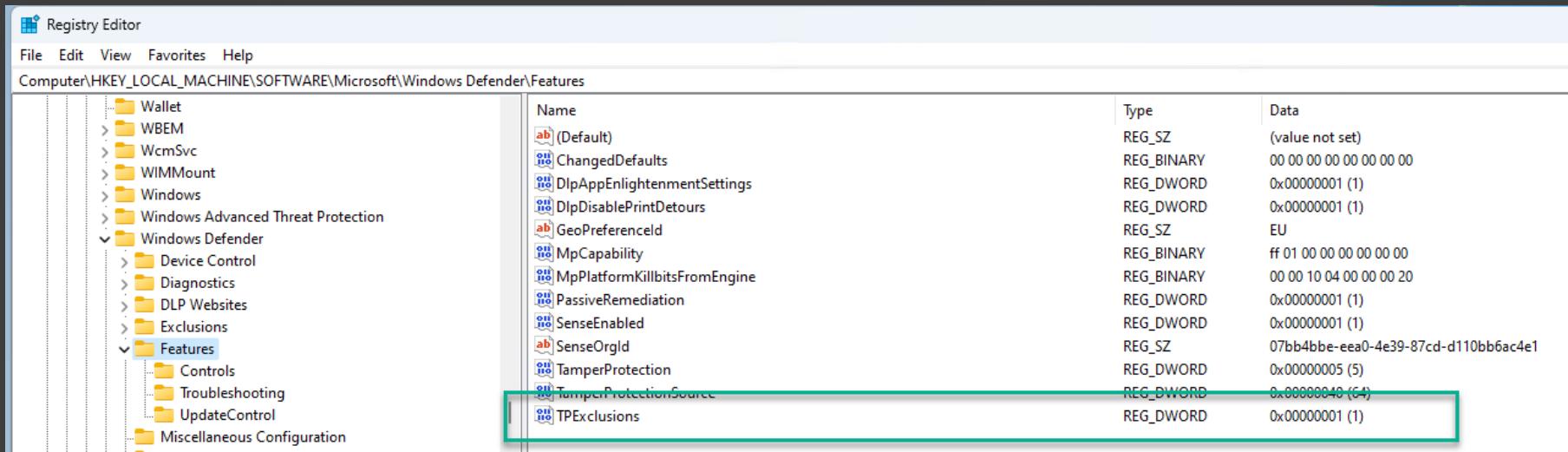
- Header: Windows Security
- Left sidebar:
 - Home
 - Virus & threat protection (selected)
 - Account protection
 - Firewall & network protection
 - App & browser control
 - Device security
 - Device performance & health
 - Family options
 - Protection history
- Main content:
 - Automatic sample submission:** Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information. (Toggle switch: On)
 - Submit a sample manually**
 - Tamper Protection:** Prevents others from tampering with important security features. (Toggle switch: On)

This setting is managed by your administrator.
 - [Learn more](#)

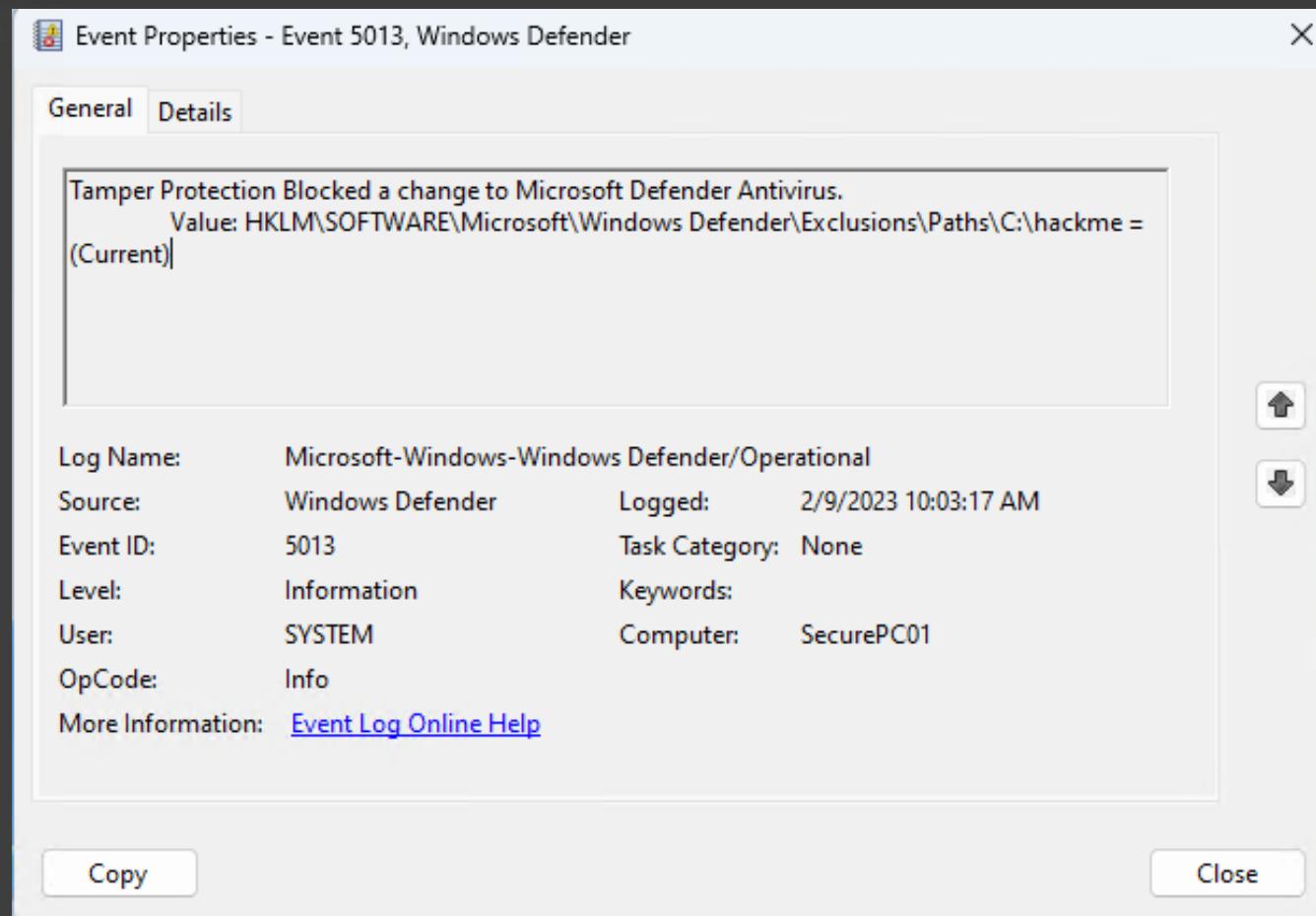
Right Screenshot: Exclusions

- Header: Windows Security
- Left sidebar:
 - Home
 - Virus & threat protection
 - Account protection
 - Firewall & network protection
 - App & browser control
 - Device security
 - Device performance & health
 - Family options
 - Protection history
- Main content:
 - Exclusions:** Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.
 - Changing exclusions has been disabled by your administrator.**
 - Add an exclusion**
 - Excluded items (boxed):**
 - C:\Data\ExcludeMe
 - Folder
 - C:\dev
 - Folder
 - c:\dev\exclude
 - Folder
 - .alex
 - File type
 - .verboon
 - File type

HKLM\SOFTWARE\Microsoft\Windows Defender\Features, find the value **TPExclusions**. A value of 1 signifies exclusions are being protected.
A value of 0 or the absence of the value indicates it's not yet enabled



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Add-MpPreference -ExclusionPath "C:\hackme"
```



Tamper detection

Feb 9, 2023 10:03:17.712 AM Event of type [TamperingAttempt] observed on device

Feb 9, 2023 10:03:17.712 AM Tamper protection in Microsoft Defender for Endpoint blocked the modifi... T1562.001: Disable or Modify Tools

Feb 9, 2023 10:03:17.646 AM powershell.exe executed WMI ExecMethod for MSFT_MpPreference::Add T1047: Windows Management Instrumentation

Feb 9, 2023 10:03:17.500 AM powershell.exe ran Powershell command: 'Add-MpPreference'

Feb 9, 2023 10:03:17.067 AM powershell.exe process contains suspicious patterns in AMSI content assoc... T1562.001: Disable or Modify Tools

Feb 9, 2023 10:03:17.067 AM powershell.exe executed a script

Timeline

Overview Incidents and alerts Timeline Security recommendations Software inventory Browser extensions Discovered vulnerabilities Missing KBs Security baselines Certificate inventory

Export Search

Filters: Marked events: true

Event time	Event	Additional information	User	Entities	Action type
Feb 9, 2023 10:03:17.712 AM	Event of type [TamperingAttempt] observed on device				TamperingAttempt
Feb 9, 2023 10:03:17.712 AM	Tamper protection in Microsoft Defender for Endpoint blocked the modifi... T1562.001: Disable or Modify Tools	system	wininit.exe > services.exe > MsMpEng.exe > Reg... TamperProtectionConfigChangeAttempt		
Feb 9, 2023 10:03:17.646 AM	powershell.exe executed WMI ExecMethod for MSFT_MpPreference::Add T1047: Windows Management Instrumentation	admin	userinit.exe > explorer.exe > powershell.exe	ProcessCreatedUsingWmiQuery	
Feb 9, 2023 10:03:17.500 AM	powershell.exe ran Powershell command: 'Add-MpPreference'	admin	svchost.exe > powershell.exe > PowerShell com...	PowerShellCommand	
Feb 9, 2023 10:03:17.067 AM	powershell.exe process contains suspicious patterns in AMSI content assoc... T1562.001: Disable or Modify Tools	admin	userinit.exe > explorer.exe > powershell.exe	AmsiContentPattern	
Feb 9, 2023 10:03:17.067 AM	powershell.exe executed a script	admin	userinit.exe > explorer.exe > powershell.exe	AmsiContentDetails	

Command line: "MsMpEng.exe"

Image file path: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2211.5-0\MsMpEng.exe

Image file SHA1: c10208460ae2504a99018c01905714dc6b6e763d

Image file SHA256: 1f4b65de4d94487916127bf82ce51d871a6c994bd9d4d60fe1a194f38231453

Execution details: Token elevation: Default, Integrity level: System

Signer: Microsoft Windows Publisher

Issuer: Microsoft Windows Production PCA 2011

VirusTotal detection ratio: 0/70

set registry value: software\microsoft\windows defender\exclusions\

Registry key: software\microsoft\windows defender\exclusions\

Value name: hackme

Value type: RegistryValueEntity

Use Advanced hunting to detect tampering attempts

Advanced hunting

detect zenmap execution | X Spoolsv Spawning Rundll32 | X New query | X New query | X New query | X New query | X Create new

> Run query Save Share link

Query

```
1 DeviceEvents
2 | .where ActionType == @"TamperingAttempt"
3 | .extend AF = parse_json(AdditionalFields)
4 | .evaluate bag_unpack(AF)
5 | .project Timestamp, DeviceName, ActionType, Status, TamperingAction, Target, RegistryValueName, AdditionalFields
6
7
```

Getting started Results

Export

<input type="checkbox"/> Timestamp	DeviceName	ActionType	Status	TamperingAction	Target	RegistryValueName	AdditionalFields
<input type="checkbox"/> Feb 9, 2023 10:03:17 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\hackme		{"TamperingAction": "Re...
<input type="checkbox"/> Feb 9, 2023 9:47:27 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tag2		{"TamperingAction": "Re...
<input type="checkbox"/> Feb 9, 2023 9:47:23 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tag2		{"TamperingAction": "Re...
<input type="checkbox"/> Feb 9, 2023 9:47:19 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tag2		{"TamperingAction": "Re...

Microsoft
Defender for
Endpoint
TVM Add-on

Threat and Vulnerability
Management
Firmware assessments

Firmware and hardware attacks are on the rise. Attackers are increasingly targeting firmware and device drivers of hardware components to gain high privilege and persistence. **Visibility** into the threat posture of firmware and timely remediation of firmware vulnerabilities are paramount for enterprise security.

Microsoft Defender Vulnerability Management new firmware assessments feature provides customers with full visibility into device manufacturer, processor and BIOS information.

The public preview of hardware and firmware assessments feature introduces the following new capabilities:

- New inventory for system models, processors, and BIOS across Windows, Linux and MacOS.
- Vulnerability assessment for processors and BIOS weaknesses for HP, Dell, and Lenovo.
- Evaluation of the UEFI Secure Boot mode setting for Windows and Linux.
- Ability to retrieve system model, processor, and BIOS information using export API and Advanced Hunting.

Hardware Models

Microsoft 365 Defender

Search

Inventories

Software Browser extensions Certificates Hardware & Firmware

Filter by device groups (63)

Laptop, desktop and server models

Processors Bios

Lenovo models | HP models | Dell models | Microsoft models | Other models

The weaknesses information in this page correspond to processors and BIOS only. Exposed devices for CPU and BIOS vulnerabilities are determined only based on security advisories from Lenovo, Dell, and HP. Status of these vulnerabilities for other system vendors is not known.

3 | 1 | 0 | 1 | 10

Export 14 items Search Filter Customize columns

Name	Model family	OS platform	Vendor	Weaknesses	Threats	Exposed devices	Impact
Thinkstation P720	ThinkStation P720	Windows	Lenovo	35	0/0	1/1	<0.01
Thinkpad T460s	ThinkPad T460s	Windows	Lenovo	29	0/0	1/1	<0.01
Hp Elitedesk 800 G4 Twr	103C_53307F HP EliteDesk	Windows	HP	1	0/0	1/1	<0.01
Virtual Machine	Virtual Machine	Windows	Microsoft	0	0/0	0/99	0.00
Macmini8,1	Not Available	macOS	Apple Inc.	0	0/0	0/2	0.00
Thinkserver Rs140	To be filled by O.E.M.	Windows	Lenovo	0	0/0	0/3	0.00
Macbookpro15.2	Not Available	macOS	Apple Inc.	0	0/0	0/1	0.00
Parallels Virtual Platform	Parallels VM	Linux	Parallels Softw...	0	0/0	0/3	0.00
Macbookpro16.1	Not Available	macOS	Apple Inc.	0	0/0	0/3	0.00

Firmware Inventory

Microsoft 365 Defender

Search

Home

Incidents & alerts

Hunting

Actions & submissions

Threat analytics

Secure score

Learning hub

Trials

Partner catalog

Assets

Devices

Identities

Endpoints

Vulnerability management

Dashboard

Recommendations

Remediation

Inventories

Weaknesses

Event timeline

Baselines assessment

Partners and APIs

Inventories

Filter by device groups (72/72)

Software Browser extensions Certificates Hardware & Firmware

Laptop, desktop and server models

Processors Bios

Lenovo BIOS | HP BIOS | Dell BIOS | Microsoft BIOS

The weaknesses information in this page correspond to processors and BIOS only. Exposed devices for CPU and BIOS vulnerabilities are determined only based on security advisories from Lenovo, Dell, and HP. Status of these vulnerabilities for other system vendors is not known.

Export

13 items Search Filter Customize columns

Name	OS platform	Vendor	Weaknesses	Threats	Exposed devices	Impact	Tags
Thinkstation P720 Firmware	Windows	Lenovo	58	0	1 / 1	<0.01	
Virtual Machine Firmware for Linux	Linux	Microsoft	0	0	0 / 21	0.00	
Parallels18.1 Firmware for Mac	macOS	Parallels	0	0	0 / 1	0.00	
Macmini8,1 Firmware for Mac	macOS	Apple	0	0	0 / 1	0.00	
Parallels15.1 Firmware for Mac	macOS	Parallels	0	0	0 / 1	0.00	
Macbookpro16,1 Firmware	Windows	Apple	0	0	0 / 1	0.00	
Virtual Machine Firmware	Windows	Microsoft	0	0	0 / 62	0.00	
Macbookpro14,3 Firmware for Mac	macOS	Apple	0	0	0 / 1	0.00	
Macbookpro16,1 Firmware for Mac	macOS	Apple	0	0	0 / 2	0.00	

Missing updates & Vulnerabilities

Microsoft 365 Defender

Search

Inventories > Thinkstation P720 Firmware

Thinkstation P720 Firmware

Overview Security recommendations (1) Discovered vulnerabilities (35) Installed devices (1) Version distribution (1) Missing software (1)

Export

Bulletin ID ↓

Link	ID
Multi-Vendor BIOS Security Vulnerabilities (September 2022)	LEN-94953
Multi-vendor BIOS Security Vulnerabilities (February 2022)	LEN-77639
Intel Processors MMIO Stale Data Advisory	LEN-77468
Multi-vendor BIOS Security Vulnerabilities (September 2021)	LEN-67440
Intel BSSA DFT Advisory	LEN-61893
Multi-vendor BIOS Security Vulnerabilities (November 2020)	LEN-49266

Intel Processors MMIO Stale Data Advisory

ID	Devices missed on
LEN-77468	1

Exposed devices (1)

Name	OS platform	Last seen	Tags
[REDACTED]	Windows Server 2019	Nov 24, 2022 1:0...	

Related CVEs (4)

Name	Severity	Threats
CVE-2022-21127	Medium	0
CVE-2022-21123	Medium	0
CVE-2022-21125	Medium	0

Show more

Missing updates & Vulnerabilities

Security recommendations > Latitude 5520 Firmware

Latitude 5520 Firmware

LF

Overview Security recommendations (1) Discovered vulnerabilities (58) Installed devices (287) Version distribution (18) Missing security updates (11)

Export

Bulletin

ID	Name	OS platform	Last seen	Tags
dsa-2022-327	[Redacted]	Windows 10	23 Jan 2023 13:36	
dsa-2022-312	[Redacted]	Windows 10	20 Jan 2023 14:26	
dsa-2022-224	[Redacted]	Windows 10	23 Jan 2023 13:14	

Show more

Related CVEs (2)

Name	Severity	Threats
CVE-2022-34400	High	[Redacted]

DSA-2022-327: Dell Client Security Update for Multiple Dell Client BIOS Vulnerabilities

ID: dsa-2022-327

Devices missed on: 265

Exposed devices (265)

Export

Name OS platform Last seen Tags

dsa-2022-327 [Redacted] Windows 10 23 Jan 2023 13:36

dsa-2022-312 [Redacted] Windows 10 20 Jan 2023 14:26

dsa-2022-224 [Redacted] Windows 10 23 Jan 2023 13:14

Show more

Related CVEs (2)

Export

Name Severity Threats

CVE-2022-34400 High [Redacted]

Direct Links to Vendor support

Dell Technologies Dell Support durchsuchen 

Anmelden Kontakt CH/DE Warenkorb

Produkte Lösungen Services Support

/ Support / Wissensdatenbankartikel

Artikelnummer: 000205716

Druck E-Mail Warnmeldung English

DSA-2022-327: Dell Client Security Update for Multiple Dell Client BIOS Vulnerabilities

Zusammenfassung: Dell Client Consumer platform remediation is available for multiple Dell BIOS vulnerabilities that may be exploited by malicious users to compromise the affected systems.

Mithilfe von Cookies können wir Ihre Nutzererfahrung auf unserer Website personalisieren und verbessern, wie in unserem Cookie Consent Tool beschrieben. Sie können allen Cookies auf unserer Website zustimmen, indem Sie auf „Alle akzeptieren“ klicken, oder nicht notwendige Cookies ablehnen, indem Sie auf „Alle ablehnen“ klicken. Wenn Sie alle oder einige nicht notwendige Cookies ablehnen, kann dies Ihre Nutzererfahrung sowie die Bereitstellung bestimmter Dienste, Funktionen oder Angebote beeinträchtigen. Möglicherweise sehen Sie dann keine Werbung mehr, die Sie interessiert. Einzelheiten zu unserem Umgang mit Daten finden Sie in unserem [Datenschutzhinweis](#).

Artikelinhalt

Auswirkungen

High

Details

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2022-34403	Dell BIOS contains a Stack based buffer overflow vulnerability. A local authenticated attacker may potentially exploit this vulnerability by using an SMI to send larger than expected input to a parameter to gain arbitrary code execution in SMRAM.	7.5	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Support kontaktieren

<

Run query Save Share link

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceTvmHardwareFirmware  
2 | where ComponentType == 'Hardware'  
3 | summarize count() by Manufacturer, ComponentName  
4
```

Getting started Results

Export

Manufacturer	ComponentName	count_
dell	latitude_5520	287
dell	latitude_5590	168

Column name	Data type	Description
DeviceId	string	Unique identifier for the device in the service
DeviceName	string	Fully qualified domain name (FQDN) of the device
ComponentType	string	Type of hardware or firmware component
Manufacturer	string	Manufacturer of hardware or firmware component
ComponentName	string	Name of hardware or firmware component
ComponentFamily	string	Component family or class, a grouping of components that have similar features or characteristics as determined by the manufacturer
ComponentVersion	string	Component version (for example, BIOS version)
AdditionalFields	string	Additional information about the components in JSON array format

All data also available through advanced hunting

Microsoft Defender XDR

New file analysis and
pivoting capabilities

The **new file page** in Microsoft 365 Defender improves the way security teams can analyze and pivot across devices and cloud applications. This enhancement enables defenders to gain deeper insights into files, their prevalence across the organization, and their impact on security incidents

- New Interface
- Enhanced pivoting
- File history
- Cloud apps" list
- File content information
- Deep Analysis

New Interface

File > Defender detected and removed 'HackTool:Win32/NetCat' in file 'netcat-win32-1.12.zip'

Defender detected and removed 'HackTool:Win32/NetCat' in file 'netcat-win32-1.12.zip'

Signer: ⚠ Unsigned • Size: 111.89 KB

[Manage indicator](#) [Download file](#)

[Overview](#) [Incidents & Alerts](#) [Observed in organization](#) [File names](#) [File content](#)

File Details

Object details

SHA1
b1735341e8f16f5bcc96ab34331fe9747fb07e1 [View](#)

SHA256
413f85a1dbac60ab5516742d76beff4f4da22b8
ef1a424f10f36ec77e6d274b1 [View](#)

MD5
5cae15c12e26d4ac8f32cd7026a5cb7a [View](#)

File size
111.89 KB

Signer
⚠ Unsigned file
⚠ This file's signer is unknown

PE metadata

Original name	Company
-	-

Product Description

Incidents & Alerts

2 active alerts, 1 incident

High (0) Medium (0) 2 more

[View Incidents & Alerts](#)

Malware detection

2 malware types found

Malware	Source	Alerts
HackTool:Win32/N...	Windows Defe...	1 alerts
PUA:Win32/Presen...	Windows Defe...	1 alerts

[View more details](#)

Observed devices (last 30 Days)

1 device

08/02

Devices

Date (First / Last)
Aug 2, 2023 (First) [View all devices](#)

VirusTotal

31/66 (High risk)

VirusTotal Ratio

[View in VirusTotal](#)

File names

1 file name

File name	Number of devices
netcat-win32-1.12.zip	1

[View all file names](#)

The "Observed in organization" section of the file page offers an in-depth view of devices and cloud applications where the file has been detected.

The screenshot shows the Microsoft Defender interface for a detected file. The top navigation bar includes 'File' > 'Defender detected and removed 'HackTool:Win32/NetCat' in file 'netcat-win32-1.12.zip''. Below the title, it says 'Signer: Unsigned • Size: 111.89 KB'. The main content area features a chart titled 'Devices' showing one asset observed. A table below lists details for this device, including its name, tags, execution status, file names, first seen date, and initiating process name.

Defender detected and removed 'HackTool:Win32/NetCat' in file 'netcat-win32-1.12.zip'

Signer: Unsigned • Size: 111.89 KB

Overview Incidents & Alerts Observed in organization File names File content

All assets

Devices

Observed on cloud apps

Devices

1

08/02

Export

1 Week

Customize columns

Filters: Risk level: Any Exposure level: Any OS Platform: Any Filters

Device name	Tags	Was executed	File names	File first seen	First initiating process name
[REDACTED]	:	false	netcat-win32-1.12.zip	Aug 2, 2023 11:56 AM	chrome.exe

The File **capabilities** feature leverage the expertise of the Microsoft research team to correlate file activities observed during detonation with **MITRE ATT&CK** techniques, empowering defenders to understand the potential capabilities of a file, even if it hasn't executed anywhere.

The screenshot shows the Microsoft Threat狩獵 (MTHunting) interface for the file `ransomware_testfile_unsigned.exe`. The file is marked as Unsigned and has a size of 79.87 KB. The **File content** tab is selected, displaying detonation results from the Microsoft Sandbox. A note indicates that the results show files detonated in the last 30 days. On the left, a sidebar lists file capabilities: **File Capabilities (1)** (T1083: File and Directory Discovery), **Process writes (0)**, and **Dynamic linking (0)**. The main table details the observed attack technique, tactics, and associated file details.

Attack technique	Tactics	Details
T1083: File and Directory Discovery	• Discovery	This file may attempt to enumerate files because API(s) were observed in the file: FindFirstFile and FindNextFile

With **File content information**, security professionals gain access to detailed information about PE files, including observed execution of MITRE ATT&CK techniques.

File content includes Process writes, Process creation, Network activities, File writes, File deletes, Registry reads, Registry writes, Strings, Imports and Exports.

The screenshot shows a user interface for analyzing a file. At the top, there's a navigation bar with 'File >' and other options like 'Manage indicator', 'Download file', and '...'. Below that, a circular icon contains a document symbol, with text indicating 'Signer: ▲ Unsigned • Size: 4.1 KB'. A message box says 'File was submitted for Deep analysis. Status: Success. See report'. The main content area has tabs: 'Overview', 'Incidents & Alerts', 'Observed in organization', 'File names', and 'File content' (which is underlined). A sidebar on the left lists various file capabilities: 'File Capabilities (0)', 'Process writes (2)', 'Process creations (3)' (which is selected), 'Network activities (0)', 'File writes (1)', 'File deletes (0)', 'Registry reads (1063)', 'Registry writes (4)', and 'Strings (0)'. The main table displays three items from the 'Process creations' section:

File name	File path	Full command line	Child process id
Malware.exe	C:\Input	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	5192
Malware.exe	C:\Input	"C:\Windows\System32\cmd.exe" /c for /I %i in (0) do (timeout 1 && del "C:\Input\Malware.exe" && IF NOT EXIST "C:\Input\M..." 5240	
cmd.exe	C:\Windows\System32	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	5548

At the bottom right of the table area, it says 'Showing 3 out of 3 items' and has a 'Search' input field with a magnifying glass icon.

Below is the original c# code of the demo app and then the information from the file content analysis

```
C: > Temp > c > C# filemelt.cs
1  using System;
2  using System.Diagnostics;
3  public class Programm
4  {
5      public static void Main()
6      {
7
8      ProcessStartInfo processInfo = new ProcessStartInfo();
9
10     processInfo.CreateNoWindow = true;
11     processInfo.FileName = "cmd.exe";
12     processInfo.Arguments = String.Format(
13         "/c for /l %i in (0) do ( timeout 1 && del \"{0}\" && IF NOT EXIST \"{0}\" (exit /b))",
14         System.Diagnostics.Process.GetCurrentProcess().MainModule.FileName
15     );
16     Process.Start(processInfo);
17 }
18 }
```

Showing 3 out of 3 items

Child process

Process writes (2)

Process creations (3)

Network activities (0)

File writes (1)

Malware.exe	C:\Input	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	5192
Malware.exe	C:\Input	"C:\Windows\System32\cmd.exe" /c for /l %i in (0) do (timeout 1 && del "C:\Input\Malware.exe" && IF NOT EXIST "C:\Input\M... 5240	
cmd.exe	C:\Windows\System32	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	5548

The file page also provides seamless access **to deep analysis** capabilities. This initiates a thorough examination of the file, providing insights into its behaviour and potential risks.

Files > File

Deep analysis

Submitting file to deep analysis collects the file from the device or from Microsoft sample store if the file already exists.
Collecting the file can take up to 3 hours depending on file and device availability. The collected file is analyzed in a secured environment and a detailed report is created.

 Results available

Latest available result: Aug 2, 2023, 9:40:45 PM

Behaviors

- ^ Environment Awareness
- ^ Interaction With System Processes
- ^ Miscellaneous
- ▽ Script Execution
 - ▽ Launches cmd.exe (1) ⓘ

Time	Process [PID]	Oper...	Target	Details
Aug 2, 2023 9:37 P...	[no name].exe [3232]	[2036] cmd.exe	"C:\Windows\System32\cmd.exe" /c for /l %i in (0) do (timeout 1 && del "C:\users\[deep_analysis_user]\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\LYZUZR0H\[no name].exe" && IF NOT E	

Resubmit

Microsoft
Defender XDR

RBAC

The Microsoft Defender XDR Role Based Access Model is a new central role-based access control (RBAC) capability to help unify roles and permissions management across the following Microsoft Defender XDR solutions.

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365,
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps (Planned)

Once in place, there is no need any more to just assign the Global Administrator , Security Administrator or multiple other Azure Roles to access the various security features within Microsoft Defender XDR

Microsoft 365 Defender

General

[Account](#)[Email notifications](#)[Alert service settings](#)[Permissions and roles](#)[Streaming API](#)

Rules

[Asset rule management](#)[Alert tuning](#)[Critical asset management](#)

Automation

Endpoints & Vulnerability Management

 Active

Email & Collaboration

Enforcing Exchange Online permissions will impact the Email & Collab capabilities that were previously configured in the Exchange admin center. [Exchange admin center](#).

 Active - Defender for Office 365 Active - Exchange Online permissions ⓘ

Identity

Enabling this setting will also enforce these permissions on the Microsoft Defender for Identity portal. [Learn more about role groups for MDI](#).

 Active

Additional data sources

Secure Score

Enabling this setting will stream additional 'non-workload' sources for Secure Score. [Learn more about data sources in Secure Score](#).

 Active[Go to Permissions and roles](#)

Microsoft Defender

Search

Settings > Microsoft 365 Defender > Microsoft Defender XDR

Permissions and roles

Roles give users permission to view data and complete tasks in Microsoft Defender XDR. Help keep your organization secure by assigning the least-permissive role to users.

Import your existing roles from other data sources.

Export Create custom role Import roles Delete roles

Add filter

Role name	Description	Data source	Last updated	Assigned to
eCorp SOC-Responder	SOC Responder	All Scopes	11/29/2023, 8:26:29 PM	0 users, 1 groups
eCorp Security Admins	eCorp Security Admins	All Scopes	11/23/2023, 3:46:27 PM	1 users, 0 groups
eCorp-Security Reader	eCorp Security Reader	All Scopes	1/23/2023, 5:28:15 PM	0 users, 1 groups

Settings > Microsoft 365 Defender >

eCorp Security Admins

Role ID: 130586f6-c41e-4703-8330-fce23eca0866

Delete role

Basics

Role name: eCorp Security Admins
Description: eCorp Security Admins
[Edit name and description](#)

Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. [Learn more](#)

Assignments

Assignment name	Data sources	Users & groups
eCorp-Security-Admins	All Scopes	1 users

[Add new assignment](#)

Permissions

Permission group	Description	Permissions sele...
Security operations	Manages day-to-day oper...	<input checked="" type="radio"/> Yes Edit
Security posture	Manages the organization'	<input checked="" type="radio"/> Yes Edit
Authorization and settings	Manages the security and ...	<input checked="" type="radio"/> Yes Edit

Assignments

Security operations

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

- Clear all permissions
- All read-only permissions
- All read and manage permissions
- Select custom permissions

Security data

- Read-only
- Select all permissions
- Select custom permissions
 - Security data basics (read) ⓘ
 - Alerts (manage) ⓘ
 - Response (manage) ⓘ
 - Basic live response (manage) ⓘ
 - Advanced live response (manage) ⓘ
 - File collection (manage) ⓘ
 - Email quarantine (manage) ⓘ
 - Email advanced actions (manage) ⓘ

Raw data (Email & collaboration)

- Read only

Security posture

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

- Clear all permissions
- All read-only permissions
- All read and manage permissions
- Select custom permissions

Posture management

- Read-only
- Select all permissions
- Select custom permissions
 - Vulnerability management (read) ⓘ
 - Exception handling (manage) ⓘ
 - Remediation handling (manage) ⓘ
 - Application handling (manage) ⓘ
 - Security baselines assessment (manage) ⓘ
 - Secure Score (read) ⓘ
 - Secure Score (manage) ⓘ

Authorization and settings

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

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

- Clear all permissions
- All read-only permissions
- All read and manage permissions
- Select custom permissions

Authorization

- Read-only
- Read and manage

Security settings

- Read-only
- Select all permissions
- Select custom permissions
 - Detection tuning (manage) ⓘ
 - Core security settings (read) ⓘ
 - Core security settings (manage) ⓘ

System settings

Tip: Don't forget the Role permissions in MDE

The screenshot shows the 'Endpoints' settings page in Microsoft Defender for Endpoint. The left sidebar has sections for General, Licenses, Email notifications, Auto remediation, and Permissions, with 'Roles' selected. The main area is titled 'Endpoints' and contains a table for defining admin roles. The table has columns for Role, Assigned security groups, Description, and Permissions. It lists five items: 'Microsoft Defender for Endpoint administrator (default)', 'Security Operators', 'SOC-Readers', and 'test'. The 'test' row is highlighted with a grey background.

Role	Assigned security groups	Description	Permissions
Microsoft Defender for Endpoint administrator (default)	sg-SecurityAdmins, SOC-Contributor, SOC-Responder	Default role with full permissions to the service. It cannot be modified or ...	Administrator
Security Operators	MDATP-SecurityOps	MDATP Security Operators	Security operations-view data, Defender ...
SOC-Readers	SOC-Reader	SOC Readers	Security operations-view data, Defender ...
test	OranjeFans		Security operations-view data, Defender ...

geekmania