geekmania

geekmania

Microsoft 365 Defender – Review 2023

Alex Verboon | baseVISION AG

geekmania

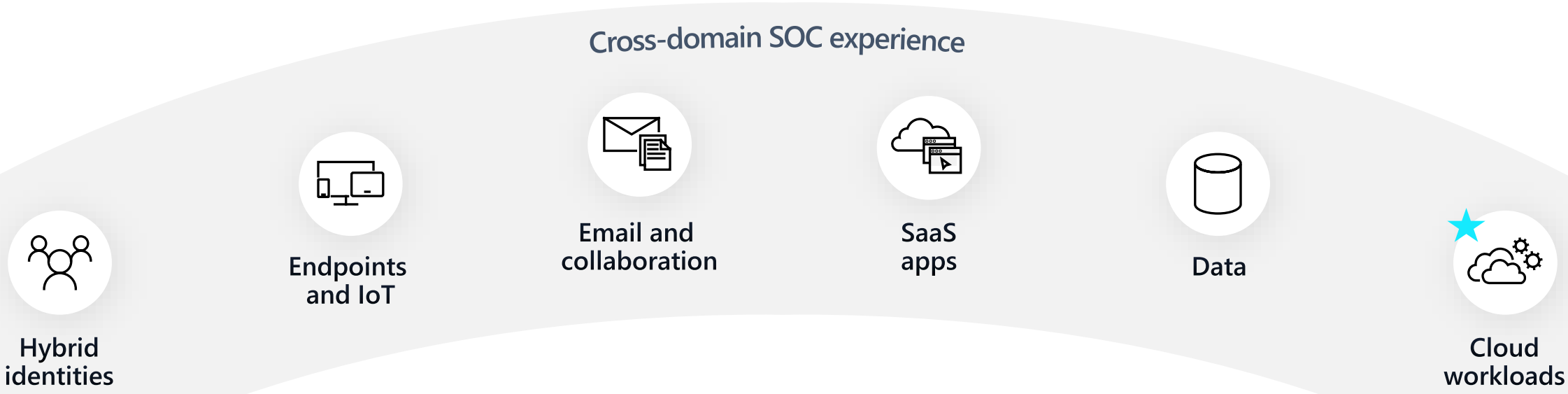
Microsoft Defender XDR – Review 2023

Alex Verboon | baseVISION AG

geekmania

Microsoft Defender XDR

Build a unified defense with XDR



Prevent

Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management

Protect

Automatically contain and remediate compromised assets

Detect and respond

Use incidents to respond to cross-workload threats from a single portal

Speed up response with an experience designed for SOC efficiency

Extend

Unified APIs and connectors

geekmania

Microsoft® MVP Most Valuable Professional

GSEC

baseVISION
SECURE & MODERN WORKPLACE

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

- **Contact Me**

https://twitter.com/alexverboon

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

GitHub https://github.com/alexverboon

https://www.verboon.info/

geekmania

baseVISION

SECURE & MODERN WORKPLACE

Great Place To Work. Certified APR 2022-APR 2023 CH

kununu TOP COMPANY www.kununu.com VON MITARBEITERN EMPFOHLEN!

Microsoft | Schweiz
Partner of the Year 2022
Security

Microsoft | Schweiz
Partner of the Year 2021
Security

Microsoft | Schweiz
Partner of the Year 2018
Empower Employees

Microsoft | Schweiz
Partner of the Year 2016
Cloud Innovation: Public Sector

Microsoft Solutions Partner
Security
Specialist
Identity and Access Management
Threat Protection

Microsoft Solutions Partner
Modern Work
Specialist
Modernize Endpoints

Microsoft Solutions Partner
Infrastructure
Azure

ISO/IEC 27001:2013
BUREAU VERITAS Certification

UKAS MANAGEMENT SYSTEMS
0008

Microsoft Intelligent Security Association

Microsoft Security

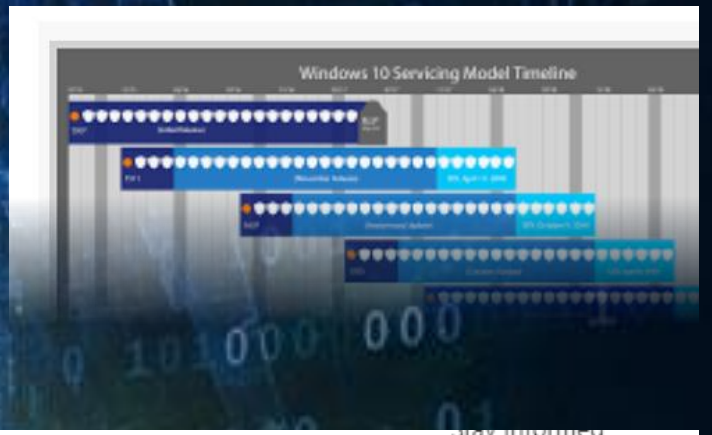
Microsoft Verified Managed XDR Solution

Why this session?

Continuous flow of information

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



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 ar
attacks by various ransomware groups have occurred in the first two weeks of April 2020, targe
providers. While the attacks delivered varying payloads, they all used the same techniques obs
deployment of a ransomware payload of the attacker's choice. The actions of these attackers ha

	...ent: Proof of disposal for records - Roll-out Update	Stay Informed
	(Updated) Feature Update: Microsoft Secure Score improvement action updates	Stay Informed
	(Updated) Outlook on the web - In-product notification of full inbox	Stay Informed
	New Azure AD Conditional Access policies now apply to all client apps, including lega	Stay Informed
	Exportability of Security reports	Stay Informed
	(Updated) Outlook - new resource booking capabilities	Stay Informed
	...Slow	Stay Informed
		Plan For Change

Threat and vulnerability management

7,288

Event timeline

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, i
way for admins to interpret how risk got introduc...

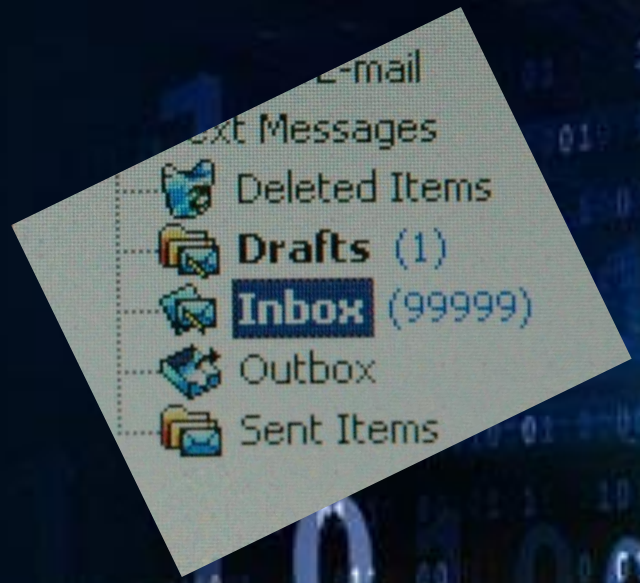
Security Baseline (FINAL): Windows 10 and Windows Server Version 2004

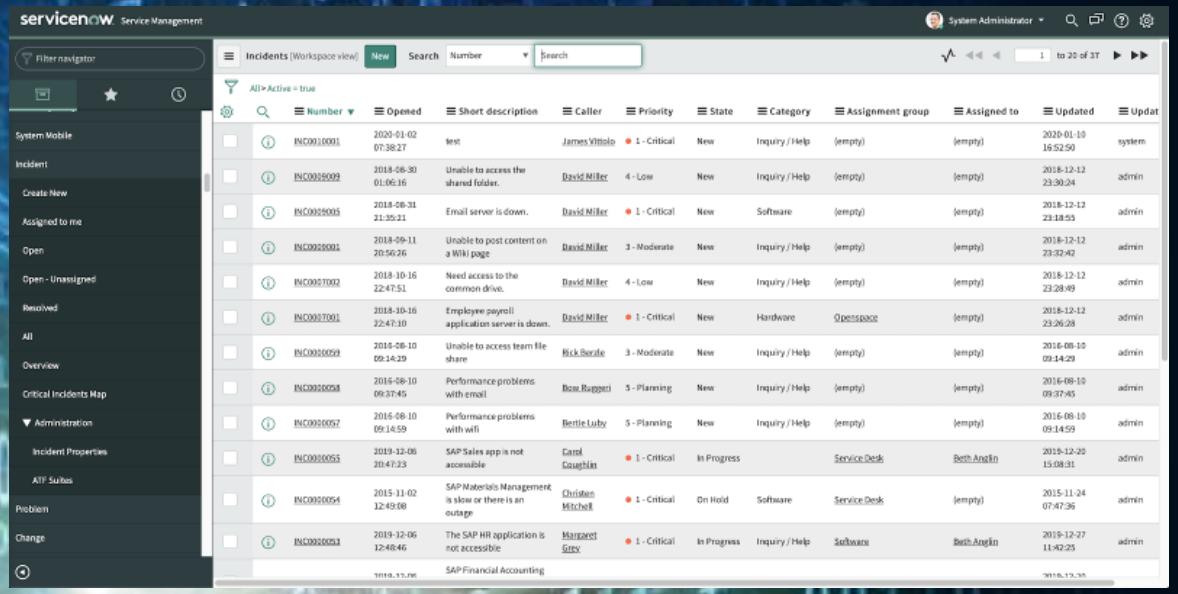
Security baseline (FINAL): Windows 10 and Windows Server,...

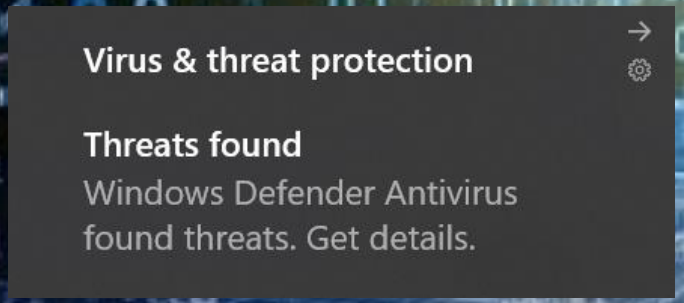
July 8, 2020

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

The other (important) things in life







geekmania

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

geekmania

Defender XDR

Automatic Attack Disruption

Ransomware continues to be a major threat

300%

Increase in human-operated ransomware attacks in the past year

70%

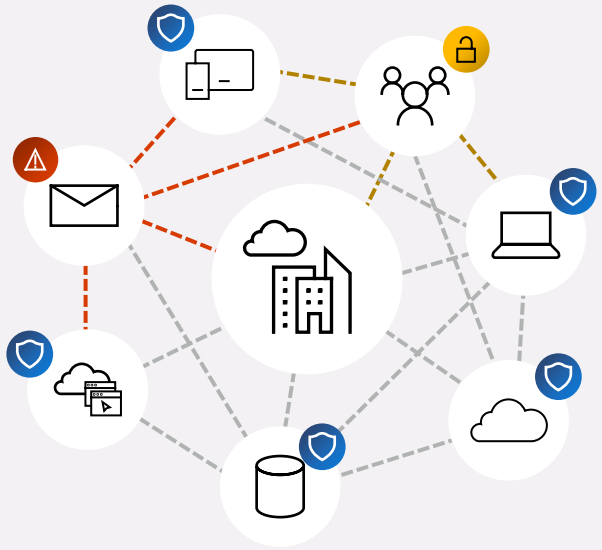
of all successful ransomware attacks targeted orgs with fewer than 500 employees

5 mins

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

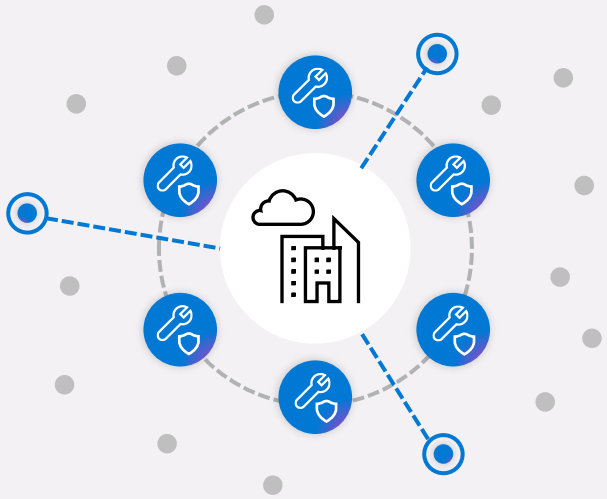
geekmania

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



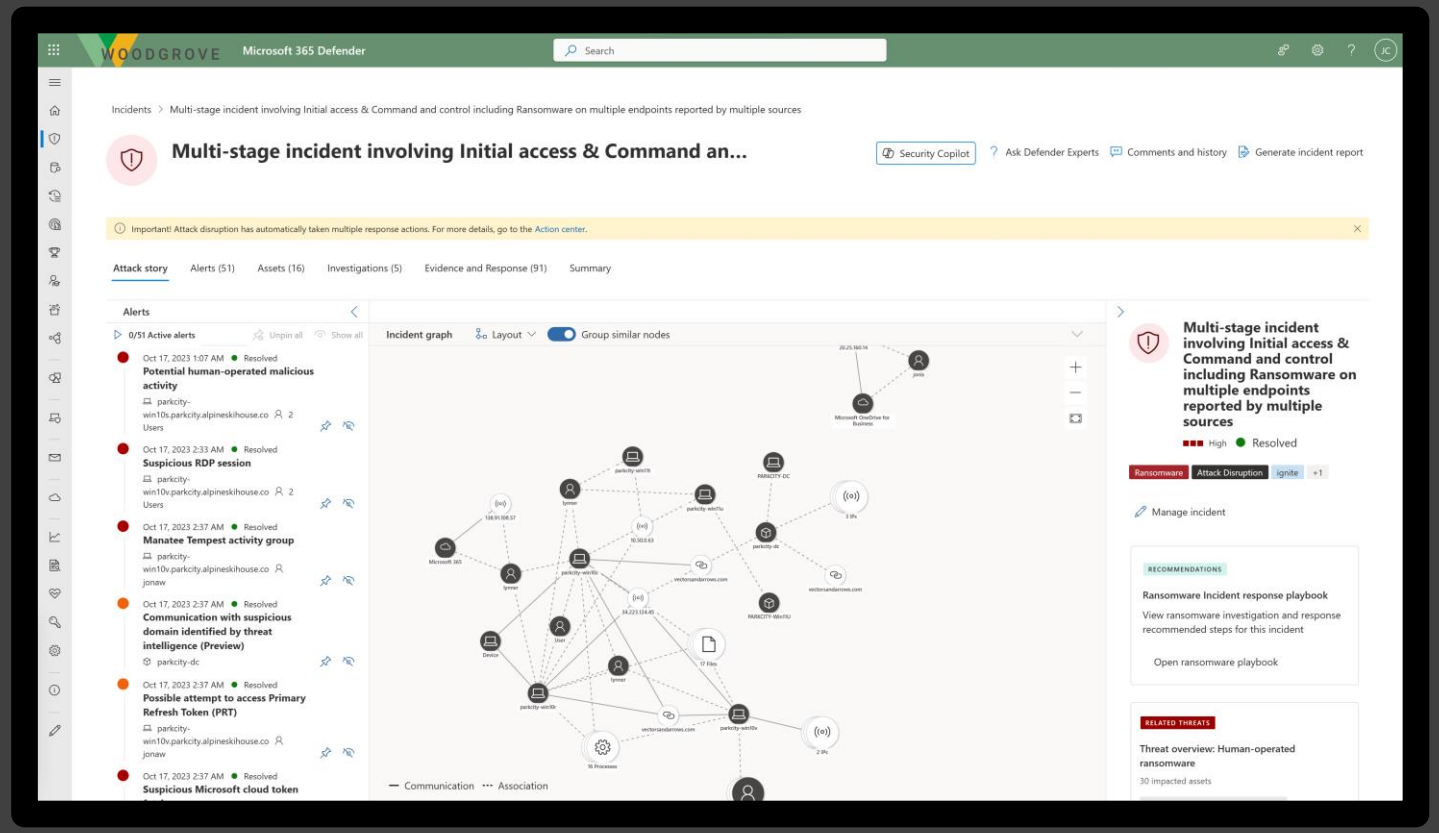
Ensuring full eradication with siloed tools is extremely difficult

geekmania

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

Prevent lateral movement
by automatically containing compromised users across all devices

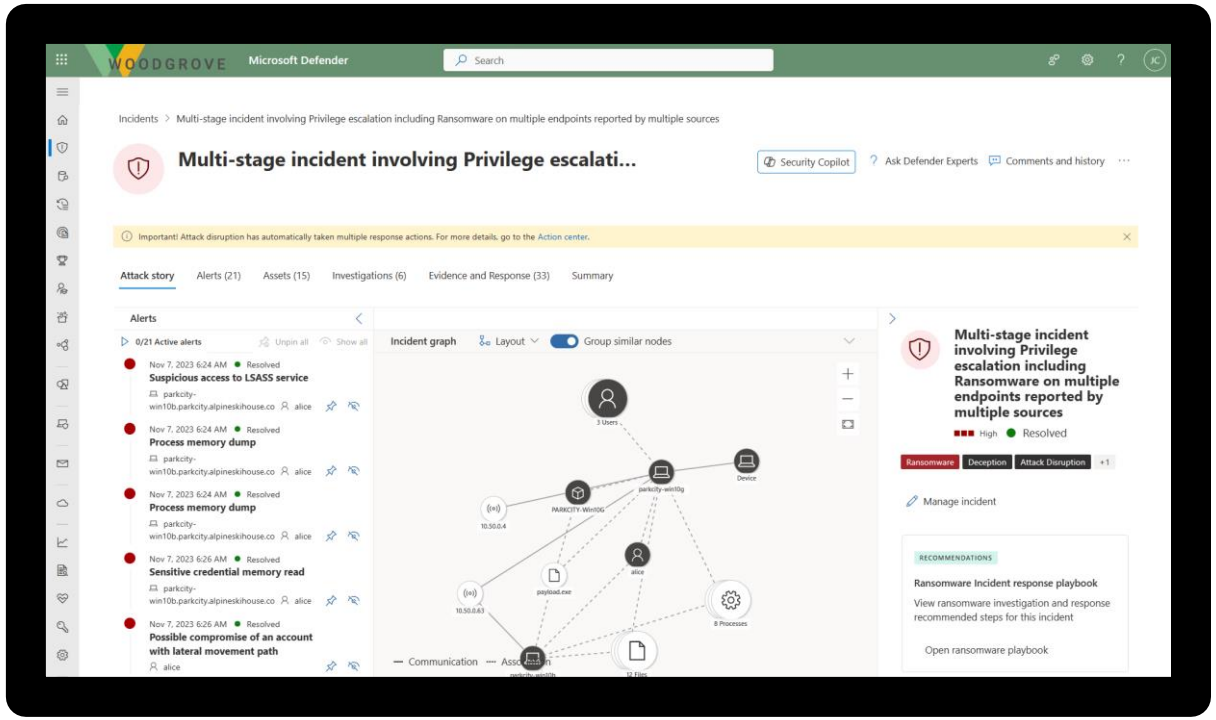
On by default
for all MDE customers



geekmania

Attack disruption at machine speed

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



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

Detection

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

Classification

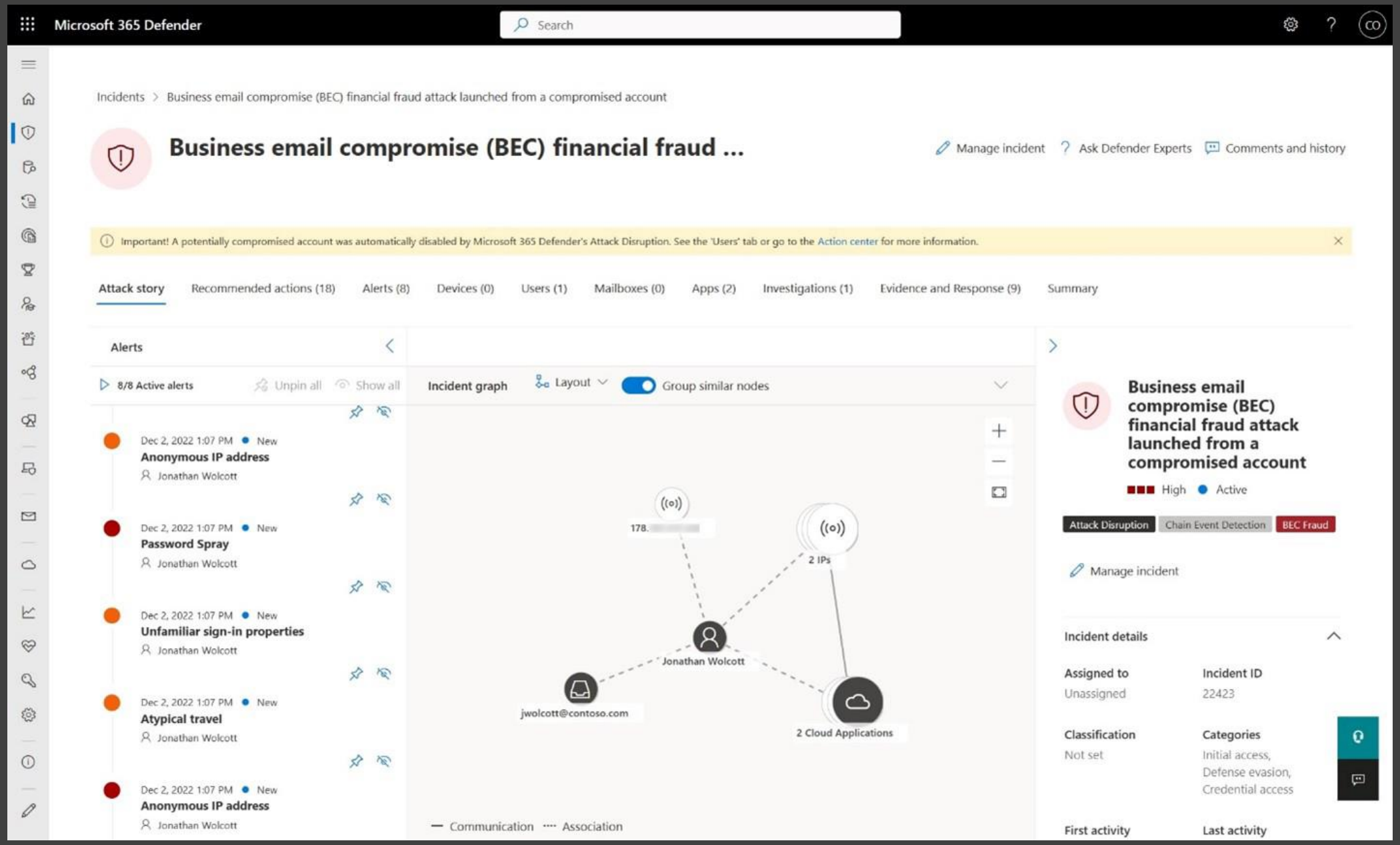
Classify attack scenario and **identify** assets controlled by the attacker

Attack disruption

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

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
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
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
178.
2 IPs
Jonathan Wolcott
jwolcott@contoso.com
2 Cloud Applications
Communication
Association
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
Unassigned
Incident ID
22423
Classification
Not set
Categories
Initial access, Defense evasion, Credential access
First activity
Last activity

geekmania

Defender XDR

email notifications for actions

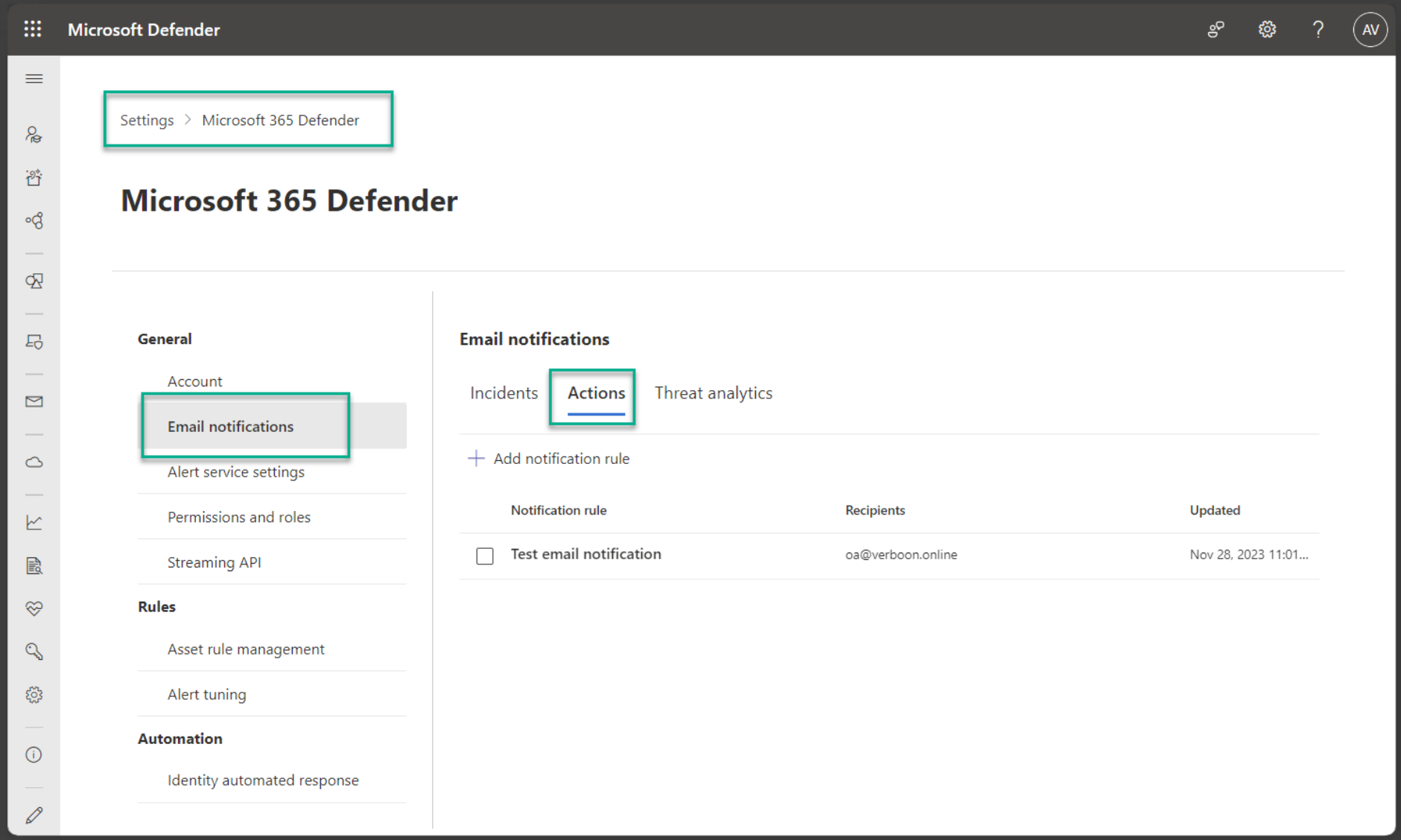
When there is an important incident, it is crucial to ensure that key stakeholders on the team are promptly informed. Providing immediate notifications for critical activities to relevant team members not only raises awareness but reduces response times and improves alignment among stakeholders.

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.

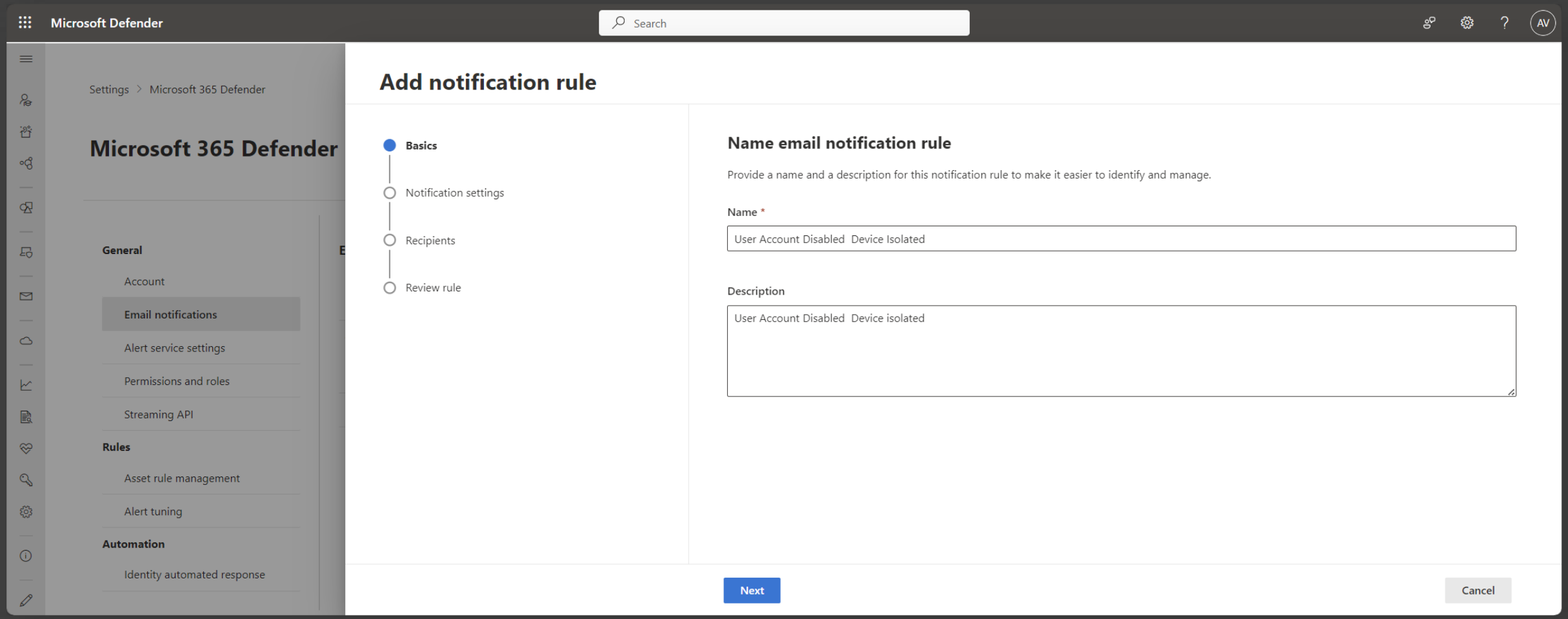
geekmania

Configure Action Notifications



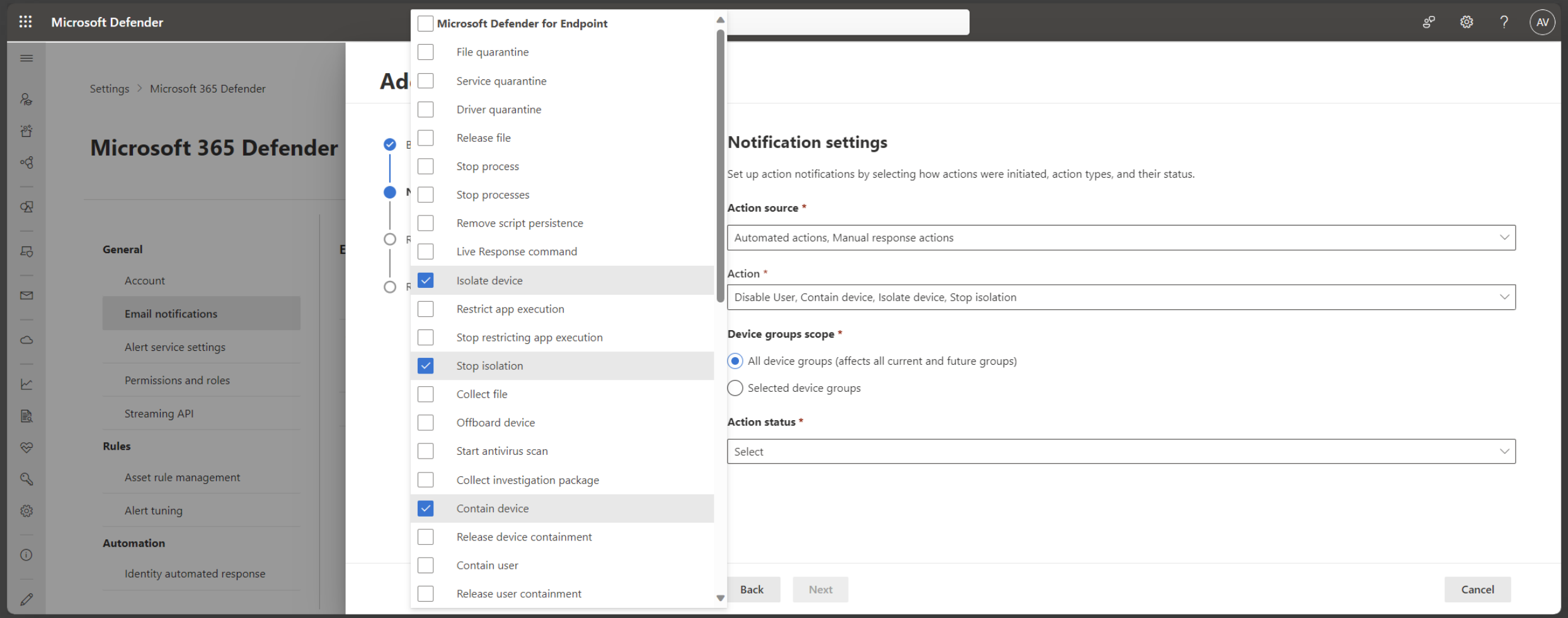
geekmania

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



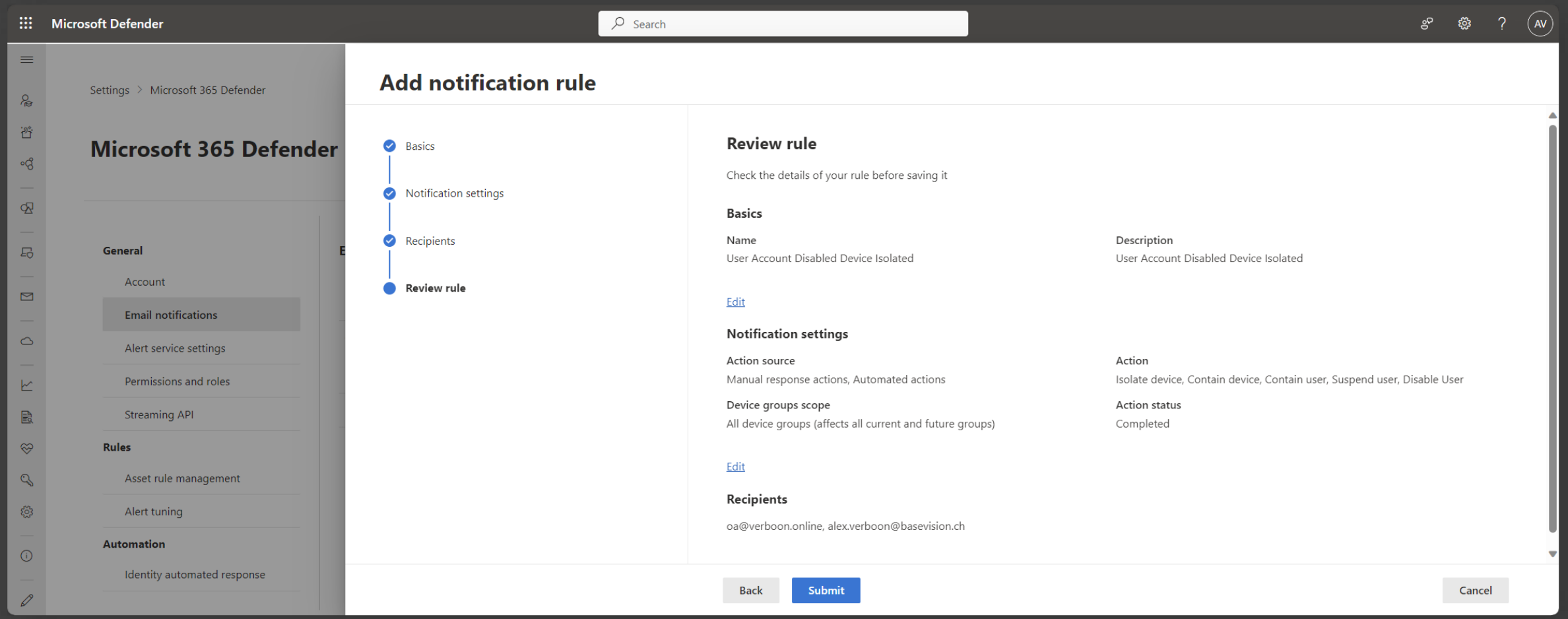
geekmania

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



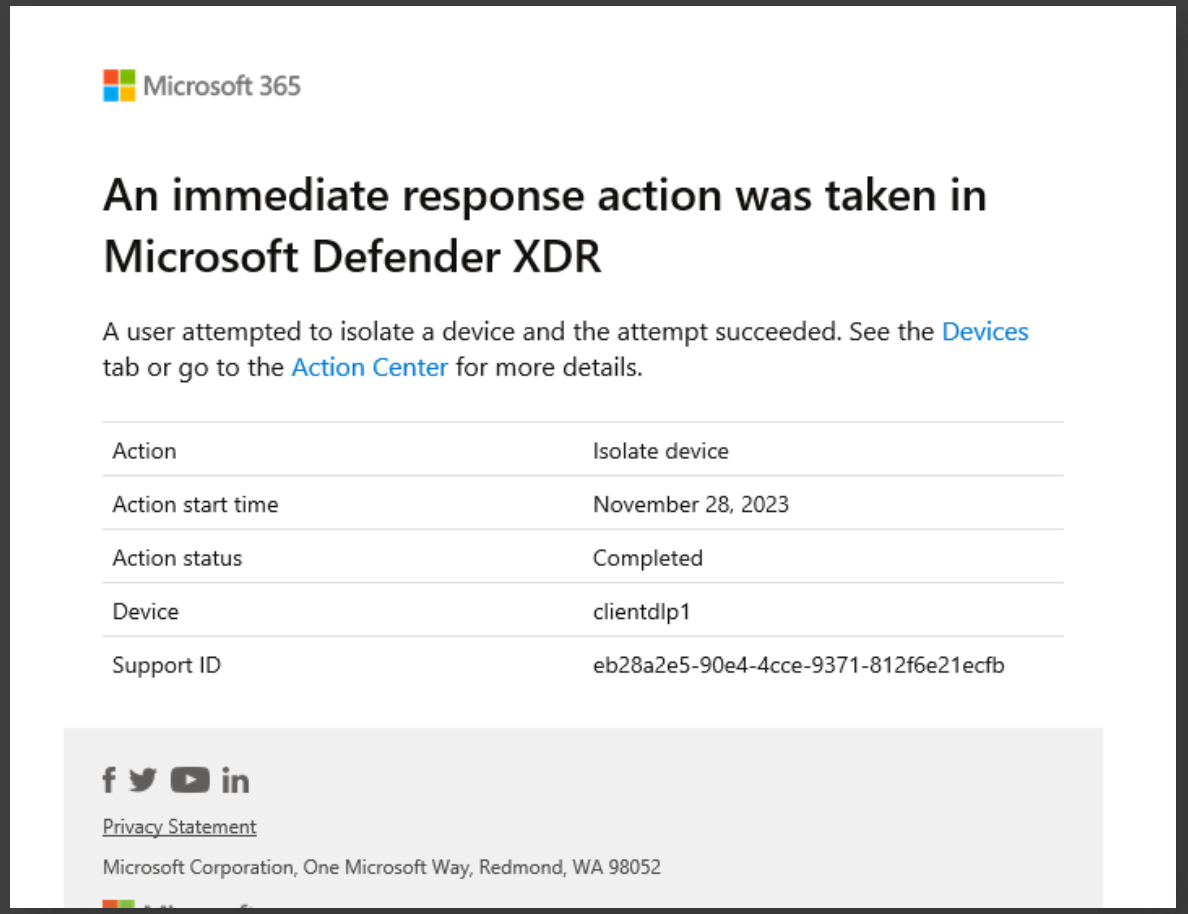
geekmania

Review and Submit the Action notification configuration



geekmania

E-Mail notification



Microsoft 365

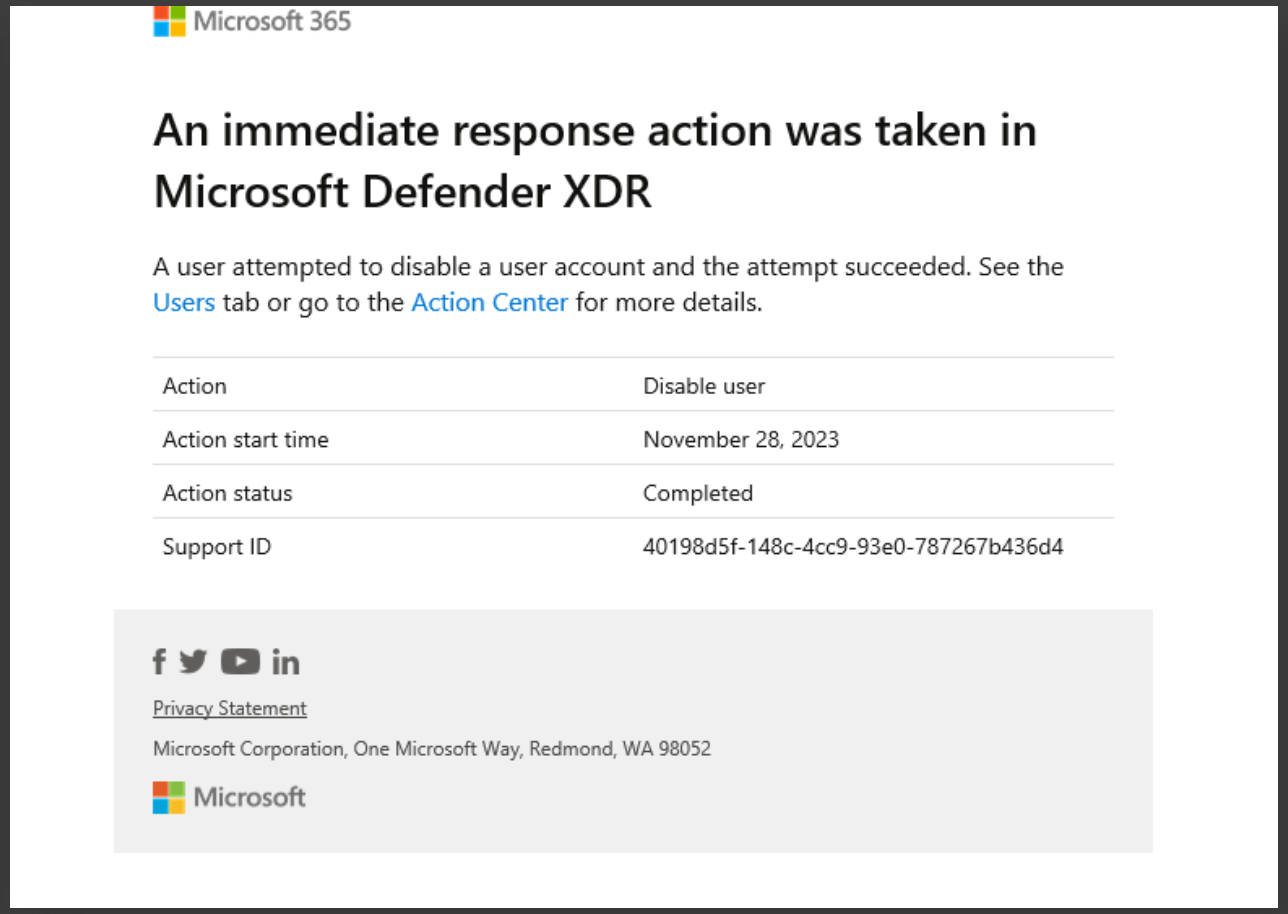
An immediate response action was taken in Microsoft Defender XDR

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

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

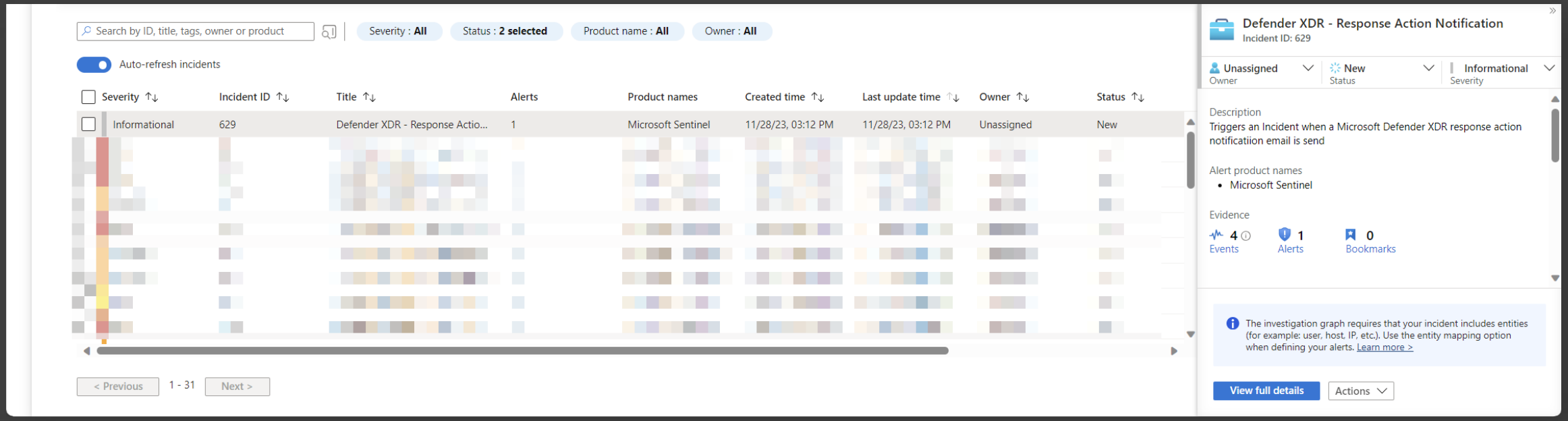
Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

geekmania

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




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

geekmania

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

geekmania

Device Discovery Enhancements

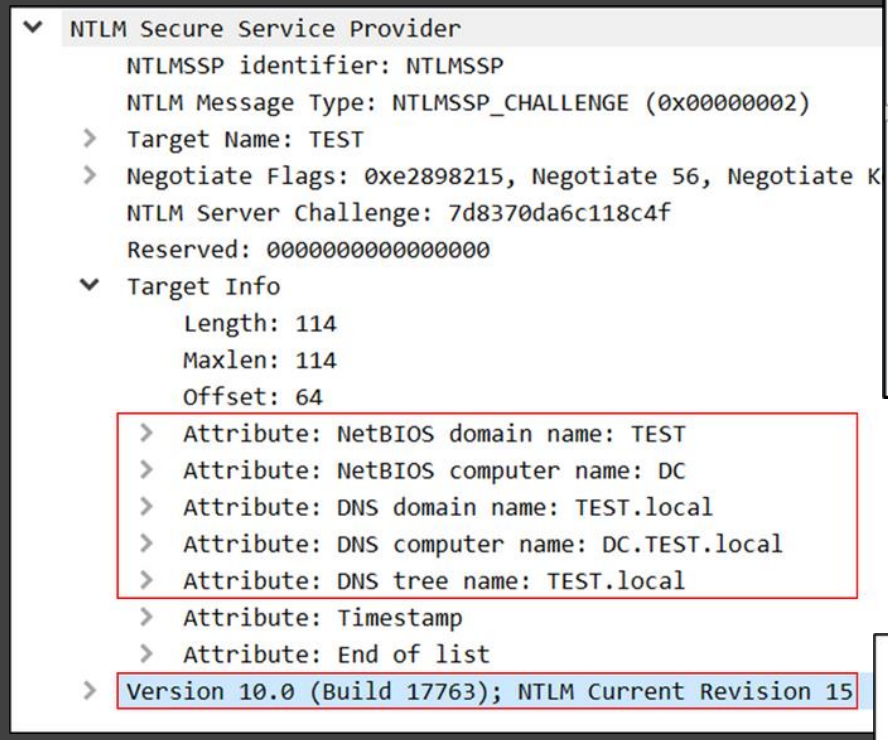
The integration enhances passive device discovery capabilities by utilizing many widely used protocols that are supported out of the box, including the below:

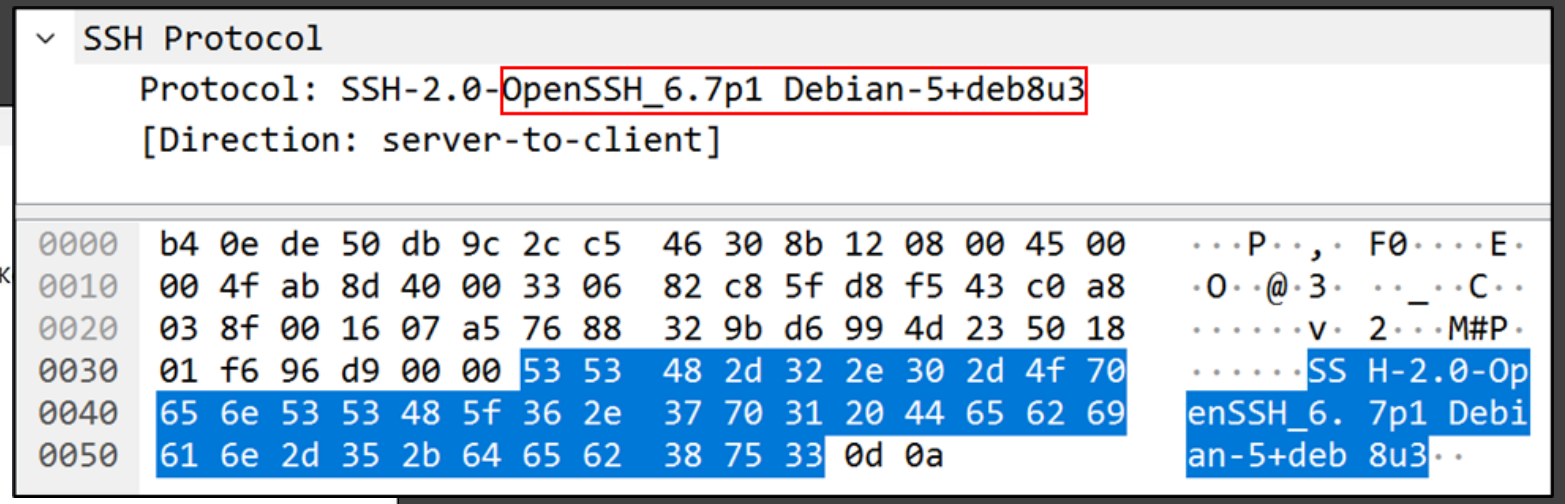
- **NTLM** - The NTLM authentication protocol involves both client and server devices sending their hostname, domain name, and operating system version. This is highly valuable data when it comes to device discovery. Zeek aggregates and reports this information for both sides on the NTLM transaction.

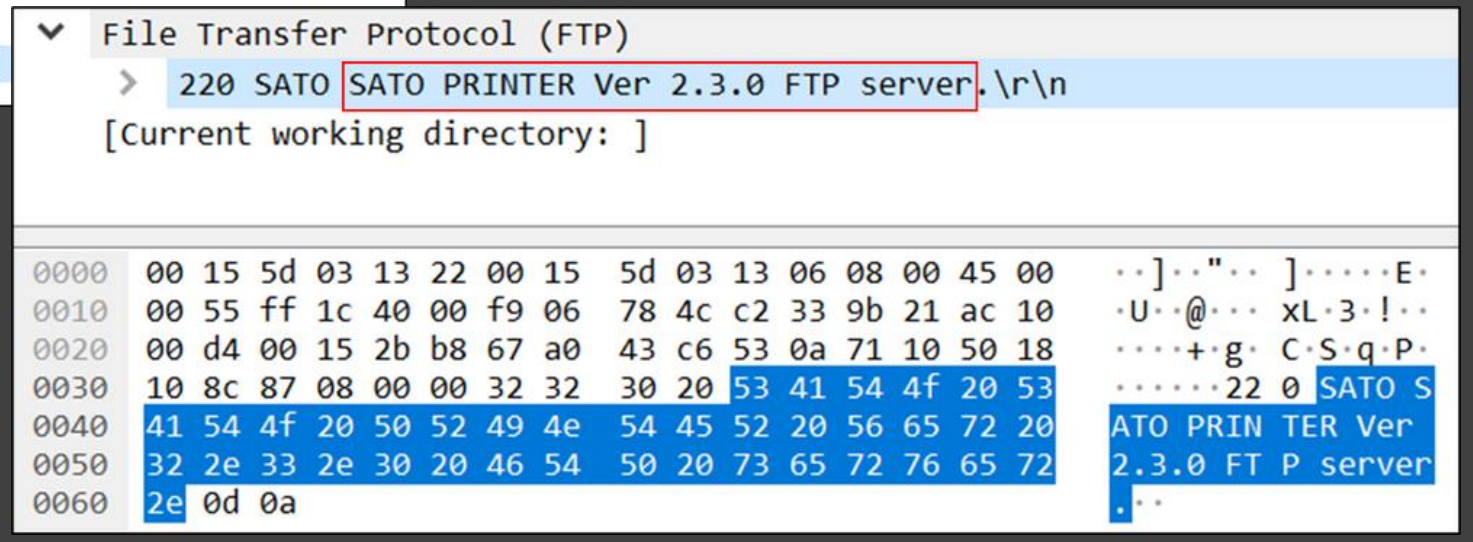
- **SSH** - Zeek monitors SSH protocol traffic and parses out the server version string. This string often includes the version of the SSH server software and the host operating system version.

- **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.

geekmania


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 15


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 ·O··@·3· ··_··C··
0020 03 8f 00 16 07 a5 76 88 32 9b d6 99 4d 23 50 18 ·····v· 2···M#P·
0030 01 f6 96 d9 00 00 53 53 48 2d 32 2e 30 2d 4f 70 ·····SS 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:]
0000 00 15 5d 03 13 22 00 15 5d 03 13 06 08 00 45 00 ··]··"··]·····E·
0010 00 55 ff 1c 40 00 f9 06 78 4c c2 33 9b 21 ac 10 ·U··@··· xL·3·!··
0020 00 d4 00 15 2b b8 67 a0 43 c6 53 0a 71 10 50 18 ····+·g· C·S·q·P·
0030 10 8c 87 08 00 00 32 32 30 20 53 41 54 4f 20 53 ·····22 0 SATO S
0040 41 54 4f 20 50 52 49 4e 54 45 52 20 56 65 72 20 ATO PRIN TER Ver
0050 32 2e 33 2e 30 20 46 54 50 20 73 65 72 76 65 72 2.3.0 FT P server
0060 2e 0d 0a .··

geekmania

Advanced Hunting - ActionType in the DeviceNetworkevents table

ActionType

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

geekmania

InboundInternetScanInspected

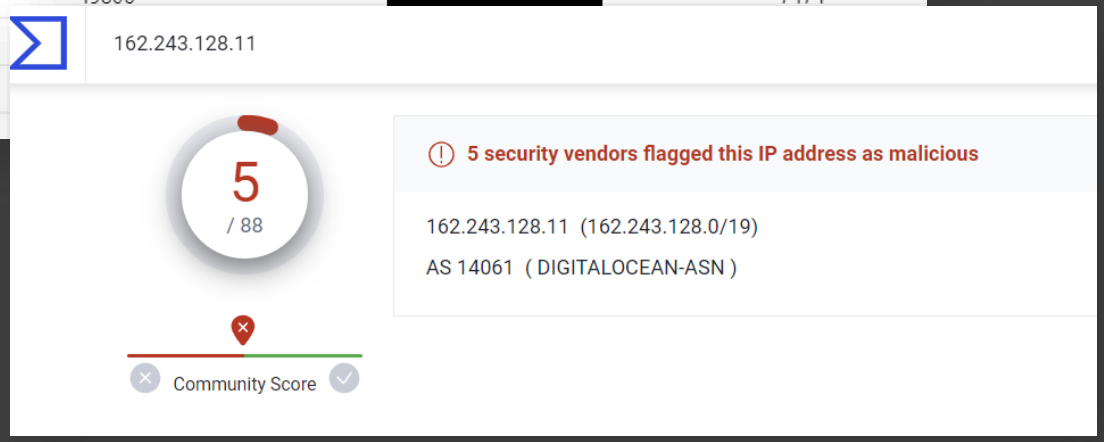
Identify systems that are scanned from the internet

```
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
```

Schema and Filter

Results | Chart | Add bookmark

TimeGenerated [UTC]	TI_ipEntity	DeviceName	LocalIP	LocalPort	RemoteIP	RemotePort
7/5/2023, 12:09:59.594 PM	[redacted]		162.243.128.11	39124	[redacted]	389
7/1/2023, 2:00:45.918 PM			138.68.208.7	34266		502
6/17/2023, 2:30:49.769 AM			192.241.197.21	51713		102
6/16/2023, 5:06:20.036 PM			192.241.202.13	49806		7474
7/24/2023, 11:40:35.304 AM			198.199.114.61			
6/22/2023, 8:26:33.684 AM			162.243.132.16			



geekmania

FtpConnectionInspected

Identify systems with FTP activity

```
DeviceNetworkEvents
| where ActionType == "FtpConnectionInspected"
| extend json = todynamic(AdditionalFields)
| extend command = tostring(json.command)
| extend reply_code = tostring(json.reply_code)
| extend reply_msg = tostring(json.reply_msg)
| extend direction = tostring(json.direction)
| extend user = tostring(json.user)
| extend arg = tostring(json.arg)
| extend cwd = tostring(json.cwd)
| extend geoinfo = geo_info_from_ip_address(RemoteIP)
```

Results | Chart | Add bookmark

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

4 security vendors flagged this IP address as malicious

188.68.47.214 (188.68.32.0/19)

AS 197540 (netcup GmbH)

self-signed

geekmania

Microsoft Defender for Endpoint

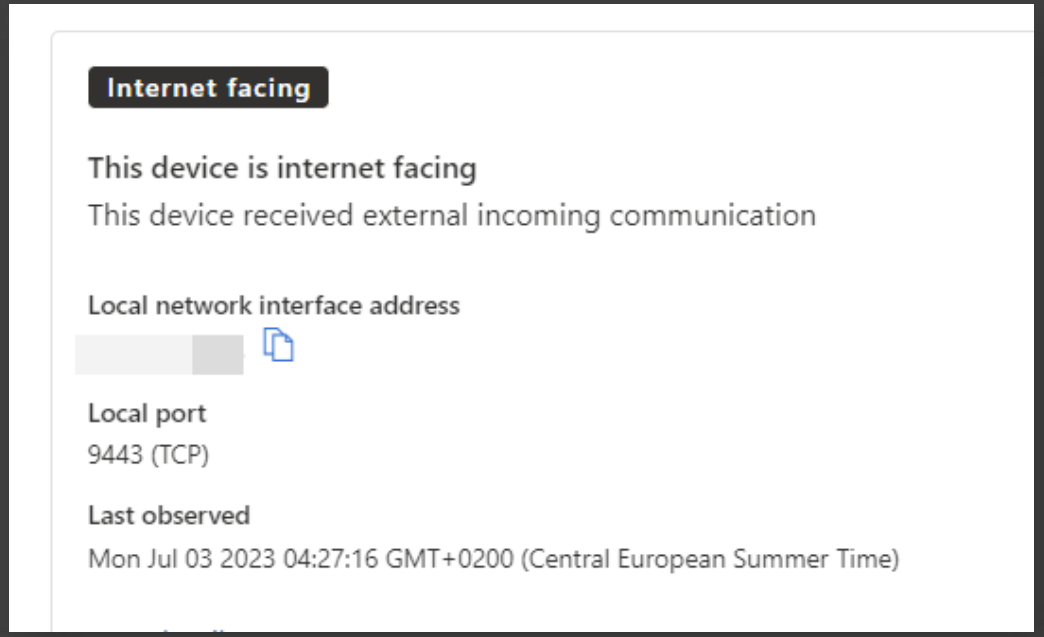
Discover Internet Facing Devices

geekmania

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

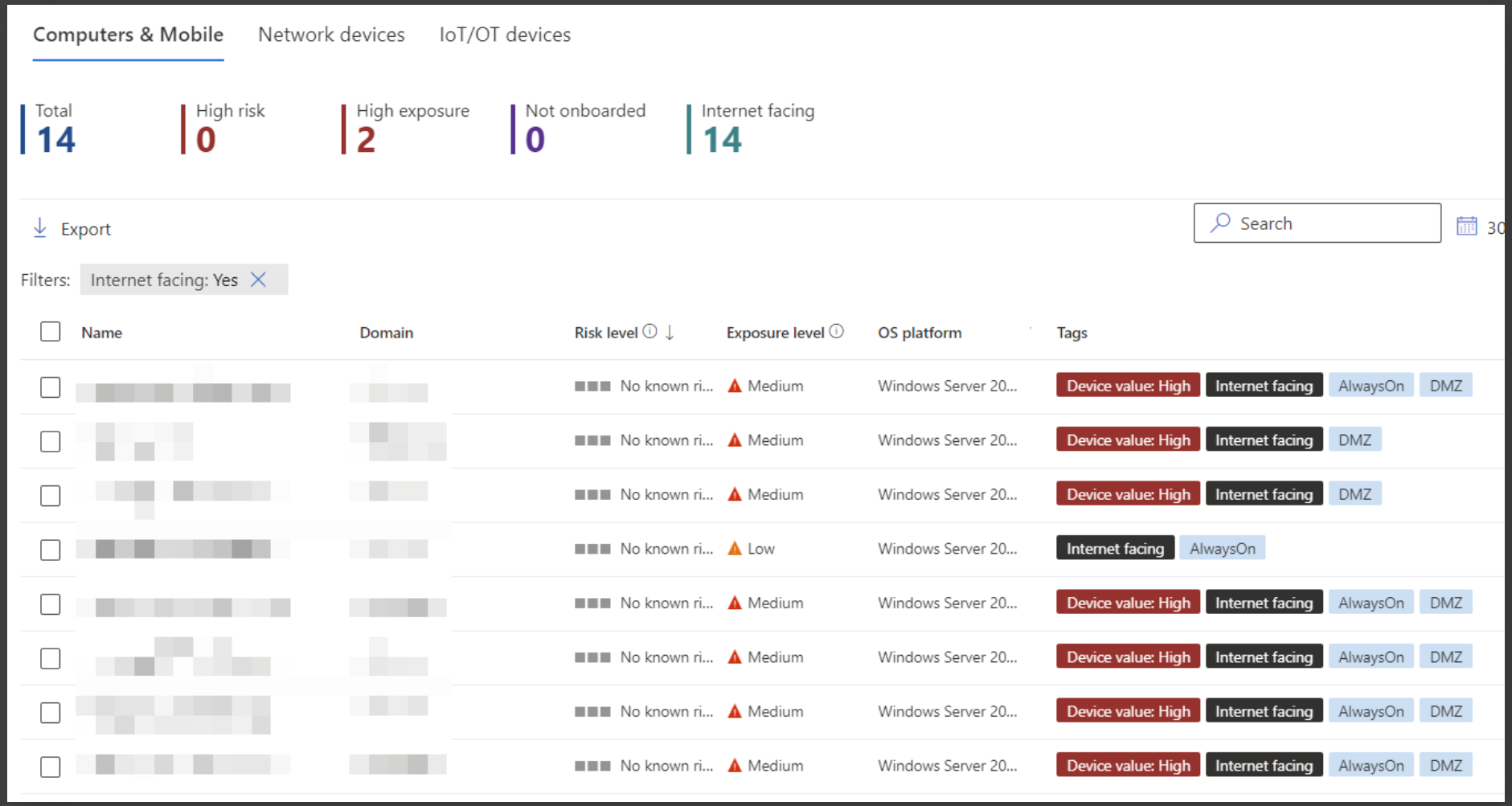


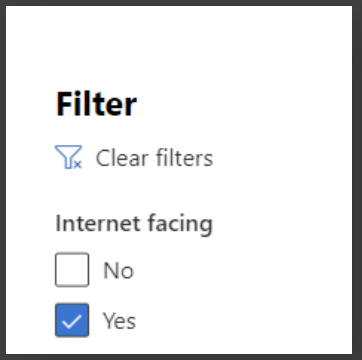
Defender for Endpoint uses different data sources to identify the devices to flag:

- 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.

geekmania


Computers & Mobile
Network devices
IoT/OT devices
Total 14
High risk 0
High exposure 2
Not onboarded 0
Internet facing 14
Export
Search
Filters: Internet facing: Yes
Name
Domain
Risk level
Exposure level
OS platform
Tags
No known ri... Medium Windows Server 20... Device value: High Internet facing AlwaysOn DMZ
No known ri... Medium Windows Server 20... Device value: High Internet facing DMZ
No known ri... Medium Windows Server 20... Device value: High Internet facing DMZ
No known ri... Low Windows Server 20... Internet facing AlwaysOn
No known ri... Medium Windows Server 20... Device value: High Internet facing AlwaysOn DMZ
No known ri... Medium Windows Server 20... Device value: High Internet facing AlwaysOn DMZ
No known ri... Medium Windows Server 20... Device value: High Internet facing AlwaysOn DMZ
No known ri... Medium Windows Server 20... Device value: High Internet facing AlwaysOn DMZ


Filter
Clear filters
Internet facing
No
Yes

geekmania

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

```
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 | 0:0.47 | Low | Chart type | Customize columns

DeviceName	IsInternetFacing	InternetFacingReason	InternetFacingLocalIp	InternetFacingLocalPort	InternetFacingScannedPubli...	InternetFacingScannedPubli...
[redacted]	1	PublicScan	[redacted]	3389	[redacted]	81

Internetfacing 3389

geekmania

Internet Facing

[redacted]

Technische Betriebe Wil

Switzerland, Wil

self-signed

SSL Certificate

Issued By:

|- Common Name:

WIN-[redacted]

Issued To:

|- Common Name:

WIN-[redacted]

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2

2023-11-29T19:20

```
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...
```

geekmania

Microsoft Defender for Endpoint

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

geekmania

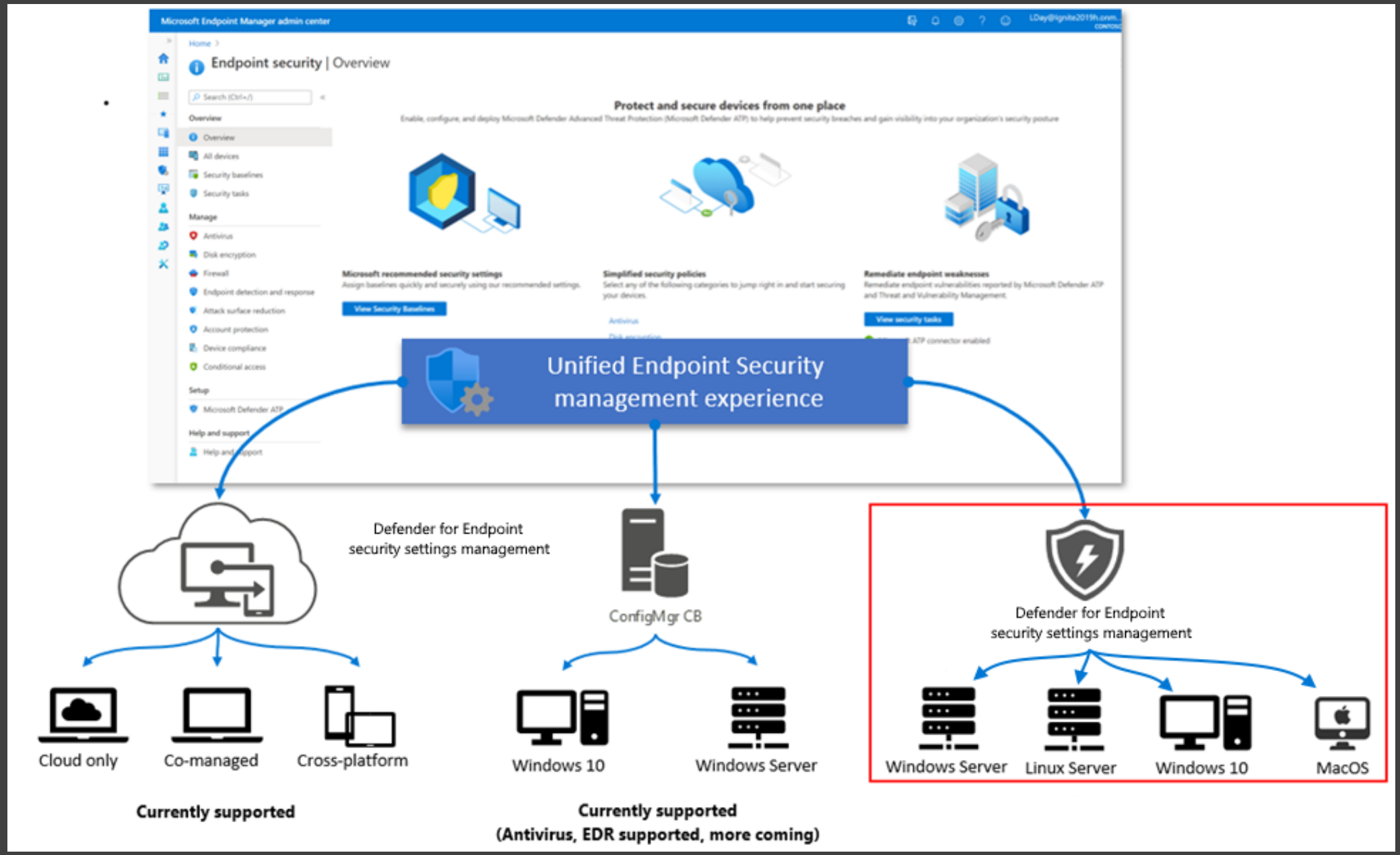
When you use Microsoft Defender for Endpoint, you can deploy policies from Microsoft Intune to manage the Defender security settings on the devices you've onboarded to Defender **without enrolling those devices with Intune**. This capability is known as Defender for Endpoint security settings configuration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

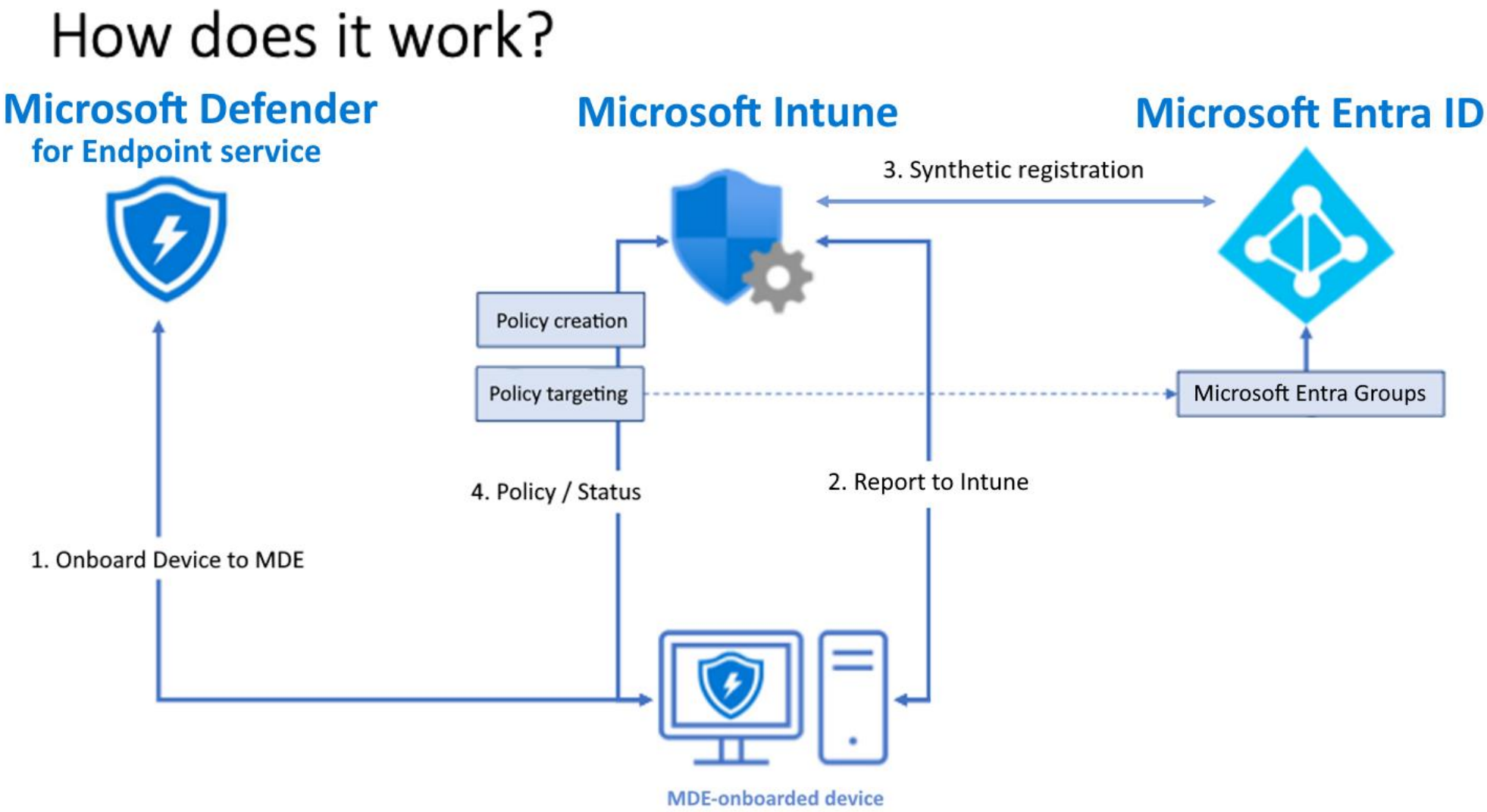
Or simply, any Microsoft Defender for Endpoint device that is not managed through AD GPO, Intune, Microsoft Configuration manager or any other systems management solution.

- 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


Microsoft Endpoint Manager admin center
Endpoint security | Overview
Protect and secure devices from one place
Unified Endpoint Security management experience
Defender for Endpoint security settings management
ConfigMgr CB
Defender for Endpoint security settings management
Cloud only
Co-managed
Cross-platform
Windows 10
Windows Server
Windows Server
Linux Server
Windows 10
MacOS
Currently supported
Currently supported (Antivirus, EDR supported, more coming)

geekmania

Architecture



geekmania

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	✓	✓

geekmania

Current supported policy types

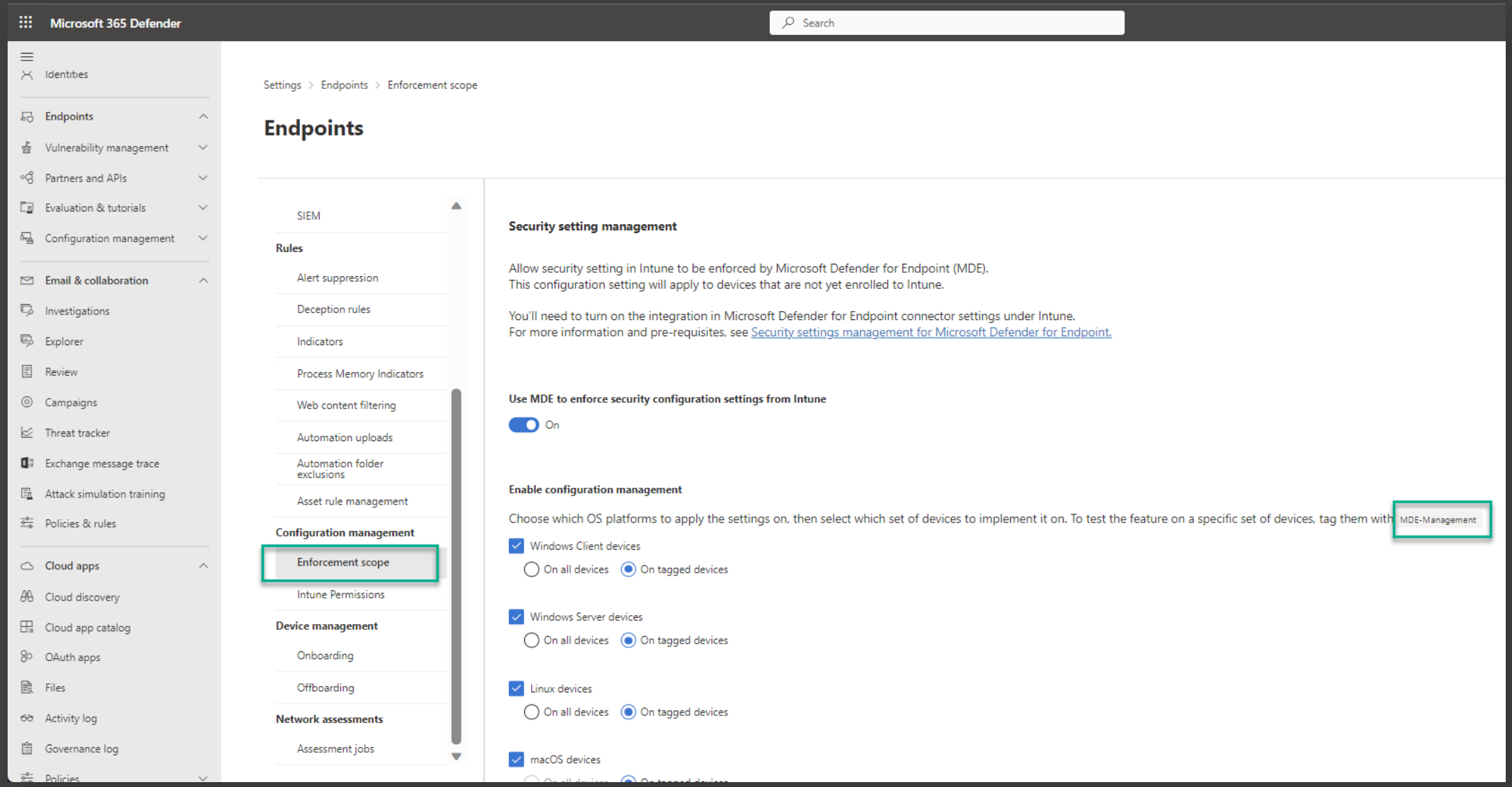
Windows 10, Windows 11, and Windows Server

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	*Note 1*	✓
Attack Surface Reduction	Attack Surface Reduction Rules	✓	✓
Endpoint detection and response	Endpoint detection and response	✓	✓
Firewall	Firewall	✓	✓
Firewall	Firewall Rules	✓	✓

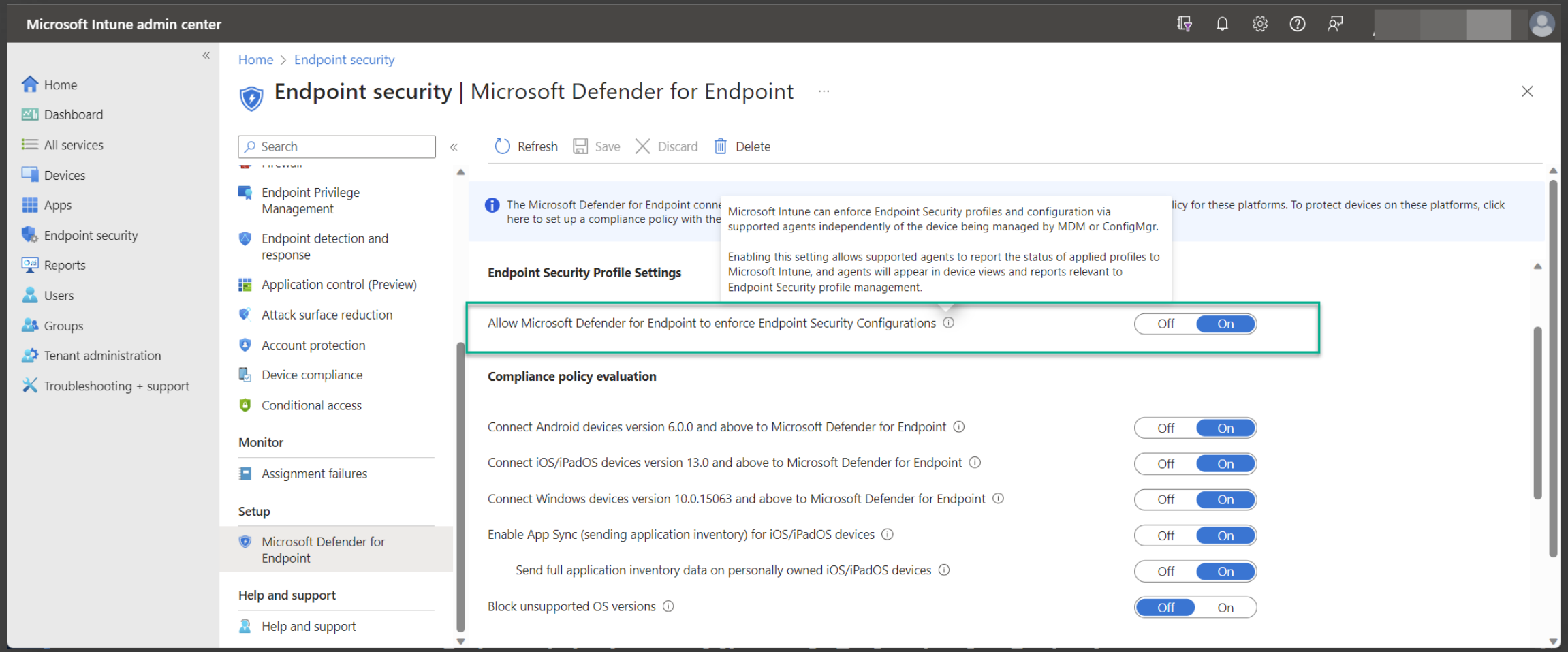
geekmania

Enablement – Defender for Endpoint Settings

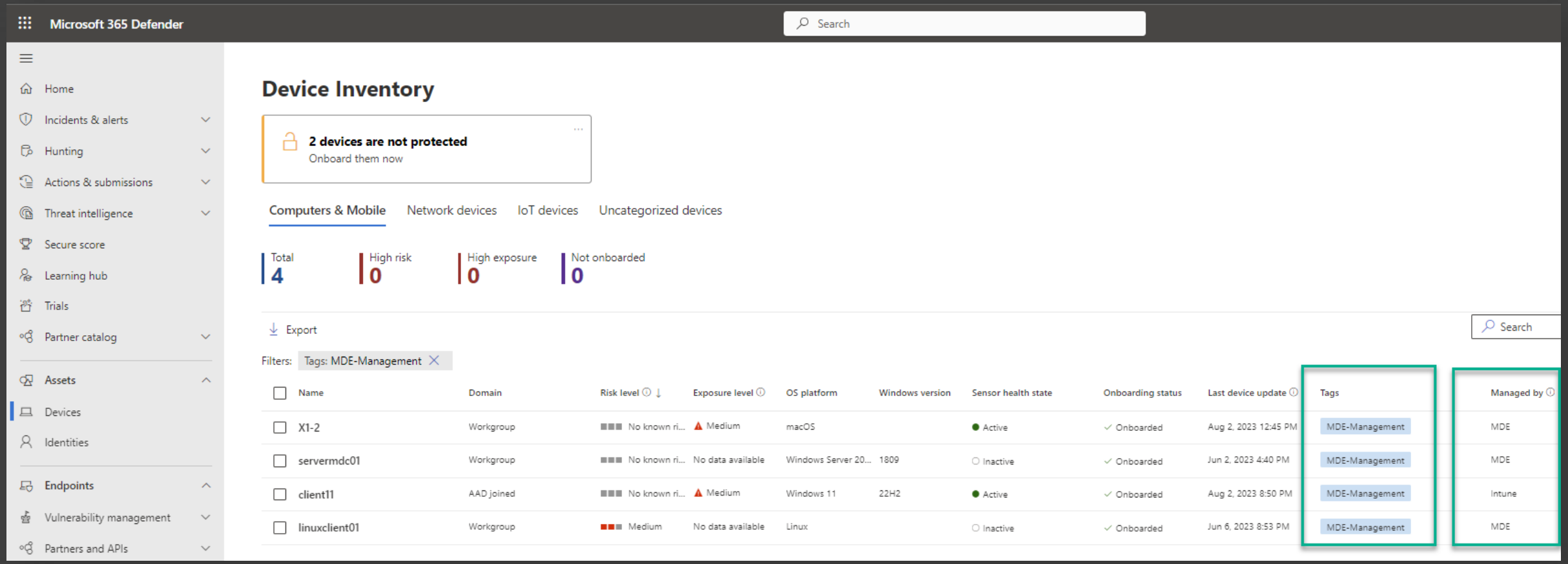


geekmania

Enablement –Microsoft Intune Settings



geekmania



Devices are tagged with '**MDE-Management**'

geekmania

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
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 > avmtplab | Groups > Groups | All groups > sg-MDEManaged-server

sg-MDEManaged-server | Members

Group

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

- Overview
- Diagnose and solve problems

Manage

- Properties
- Members
- Owners

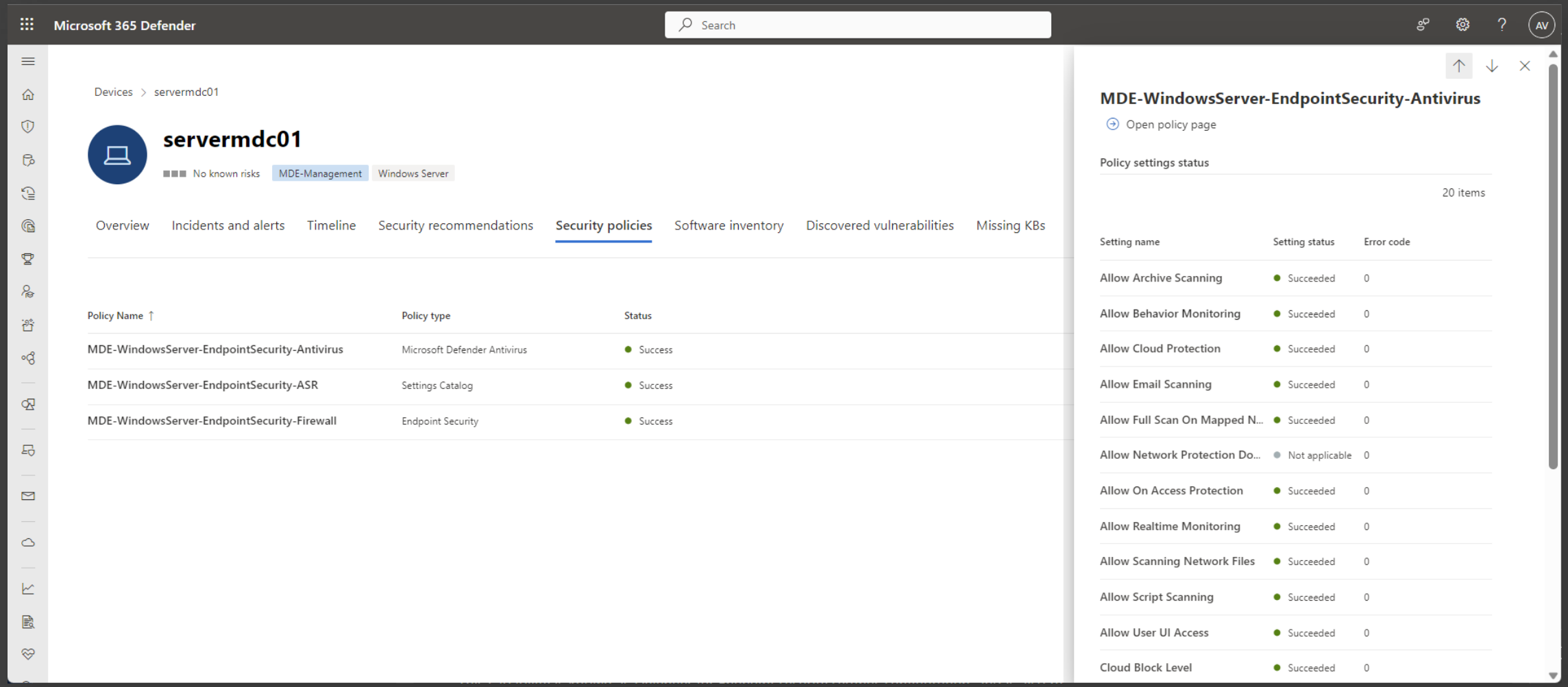
Direct members | All members

Search by name | Add filters

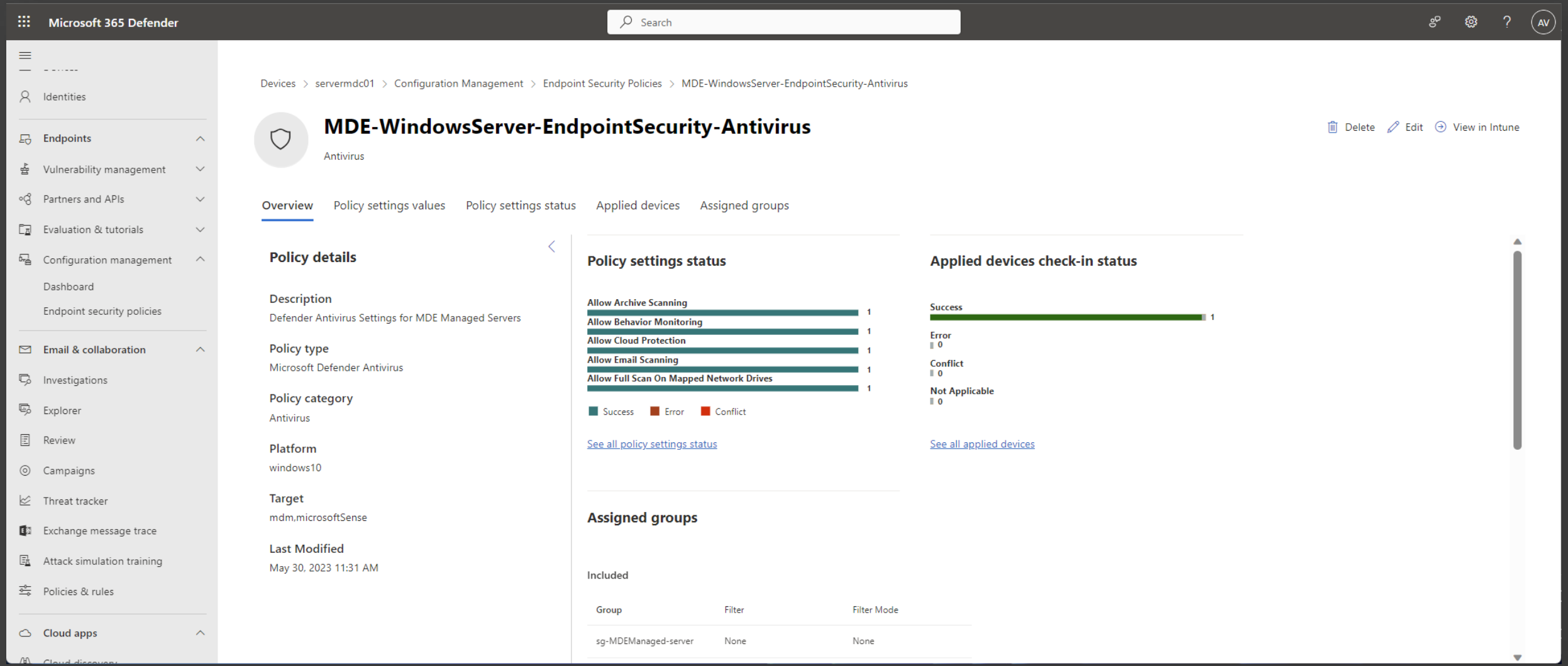
Name	Type
SERVERMDC01	Device

geekmania

Policies visible in Microsoft Defender for Endpoint



geekmania


Microsoft 365 Defender
Search
AV
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Dashboard
Endpoint security policies
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
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
Allow Archive Scanning 1
Allow Behavior Monitoring 1
Allow Cloud Protection 1
Allow Email Scanning 1
Allow Full Scan On Mapped Network Drives 1
Success
Error
Conflict
See all policy settings status
Applied devices check-in status
Success 1
Error 0
Conflict 0
Not Applicable 0
See all applied devices
Assigned groups
Included
Group
Filter
Filter Mode
sg-MDEManaged-server
None
None

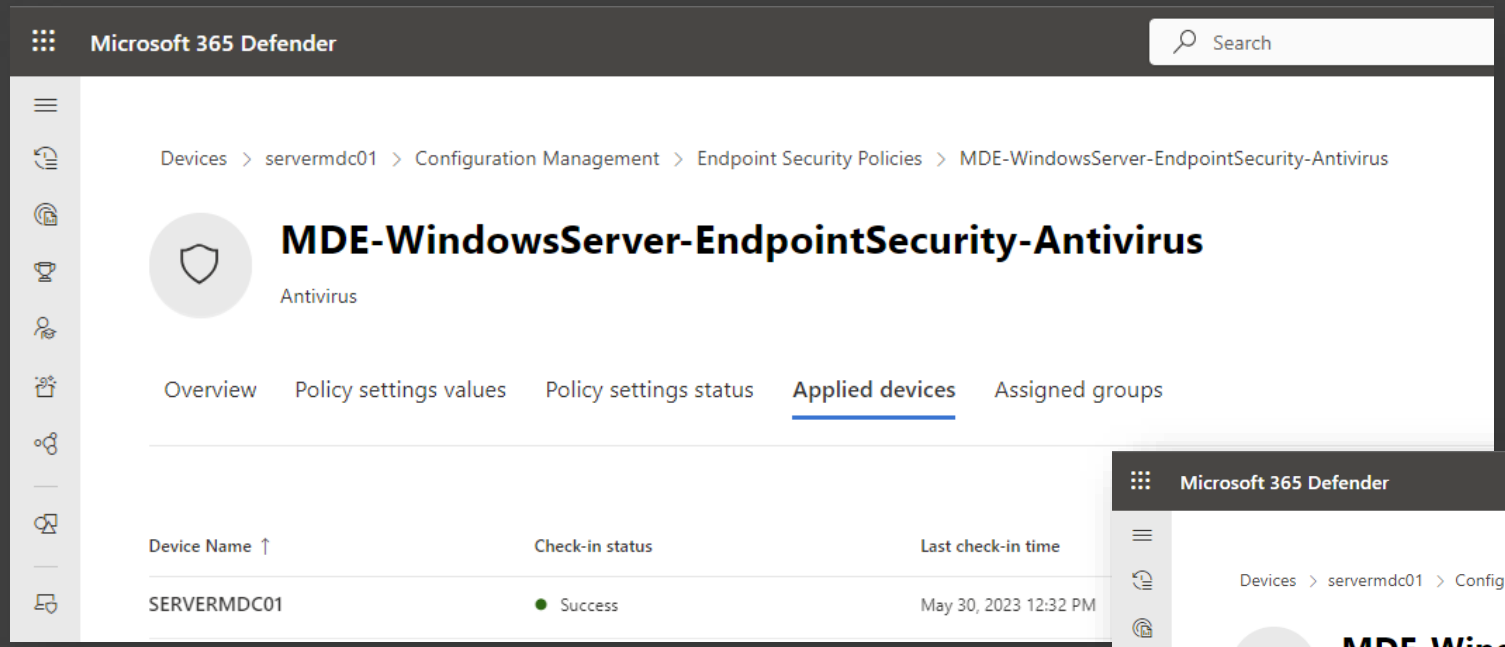
MDE-WindowsServer-EndpointSecurity-Antivirus

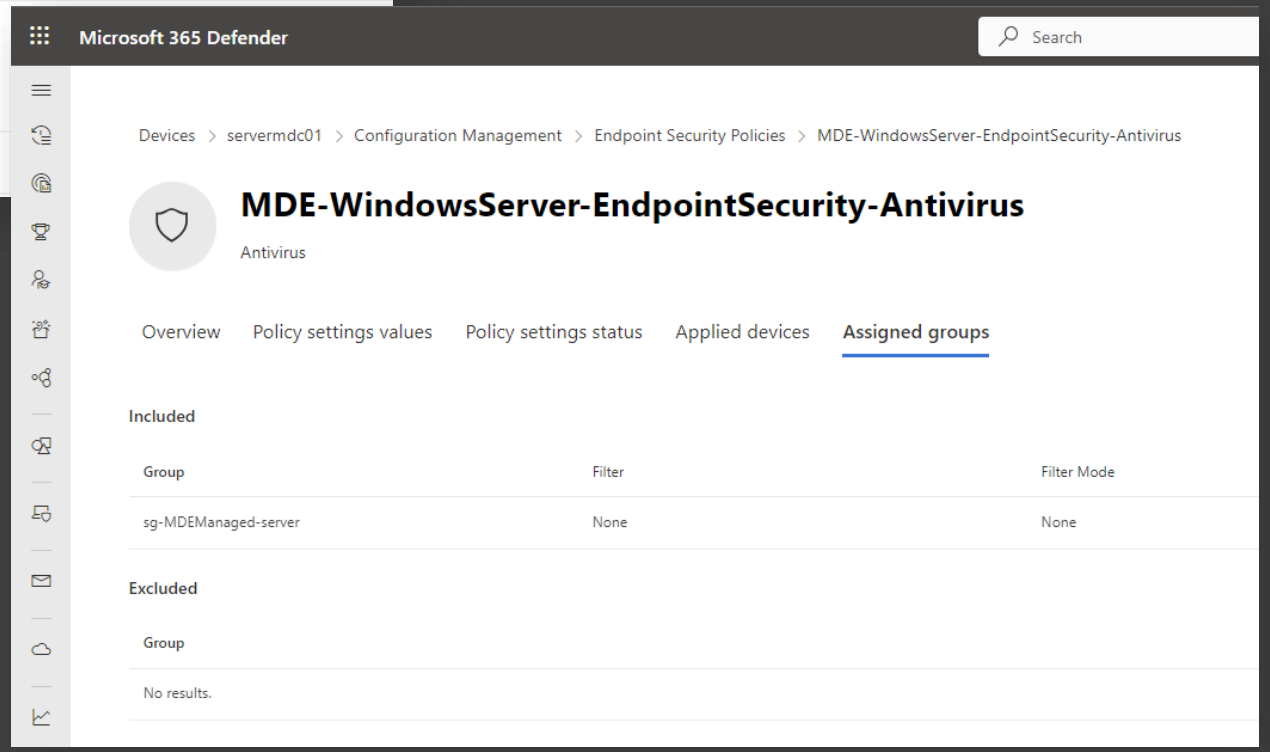
Antivirus

Settings

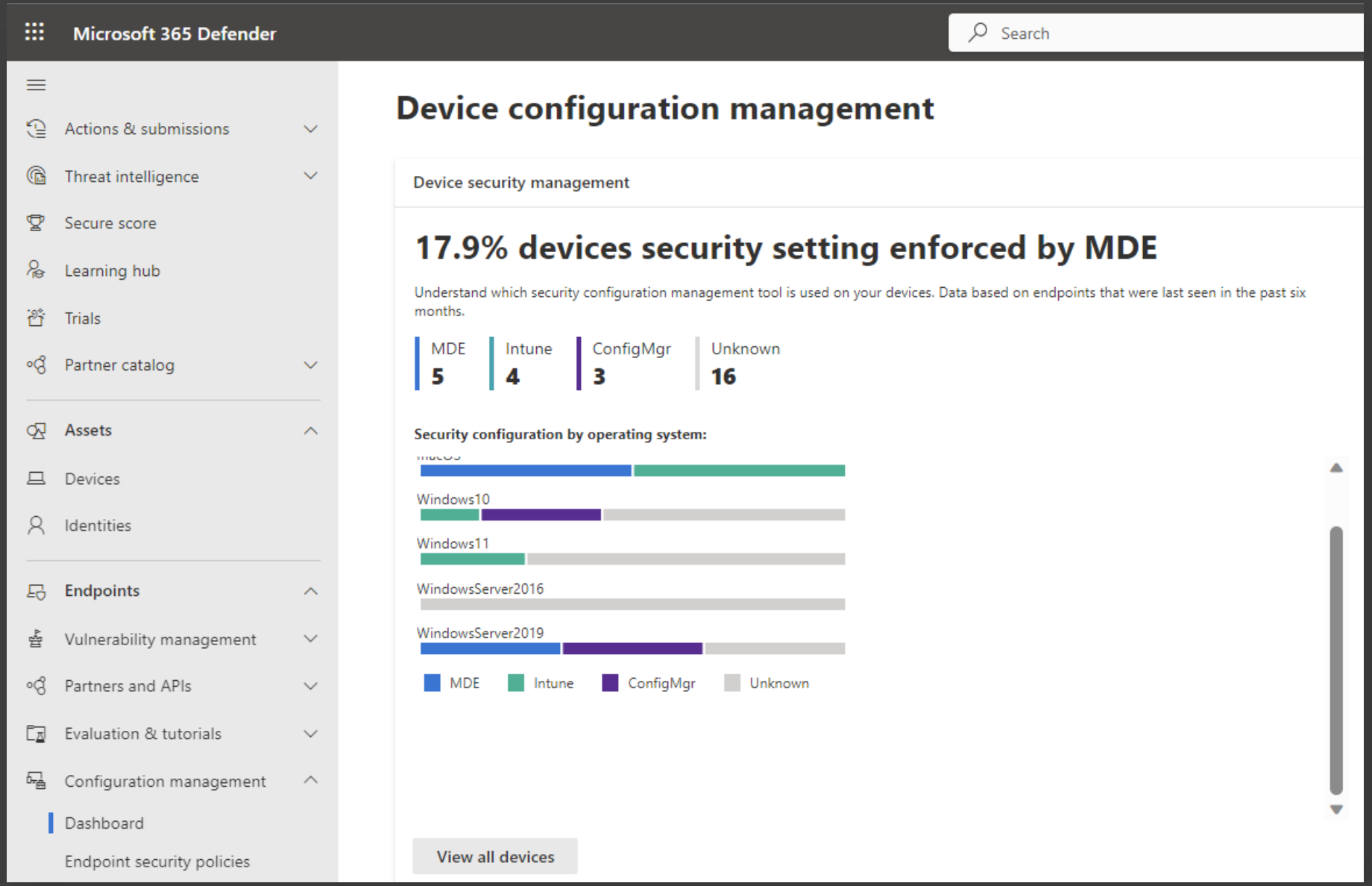
Allow Behavior Monitoring	Allowed. Turns on real-time behavior monitoring.
Allow Archive Scanning	Allowed. Scans the archive files.
Allow Cloud Protection	Allowed. Turns on the Microsoft Active Protection Service.
Allow Email Scanning	Allowed. Turns on email scanning.
Allow Full Scan On Mapped Network 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	

geekmania


Microsoft 365 Defender
Search
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


Microsoft 365 Defender
Search
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.

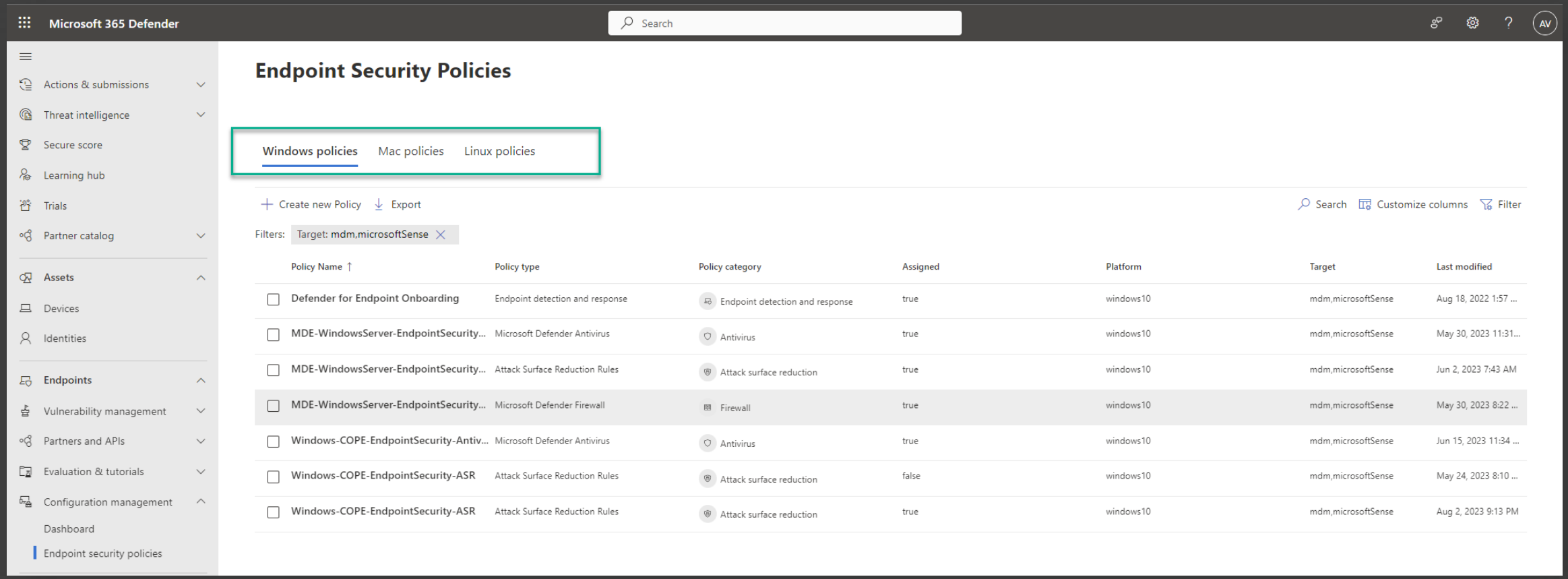
geekmania



Device Configuration Management Dashboard

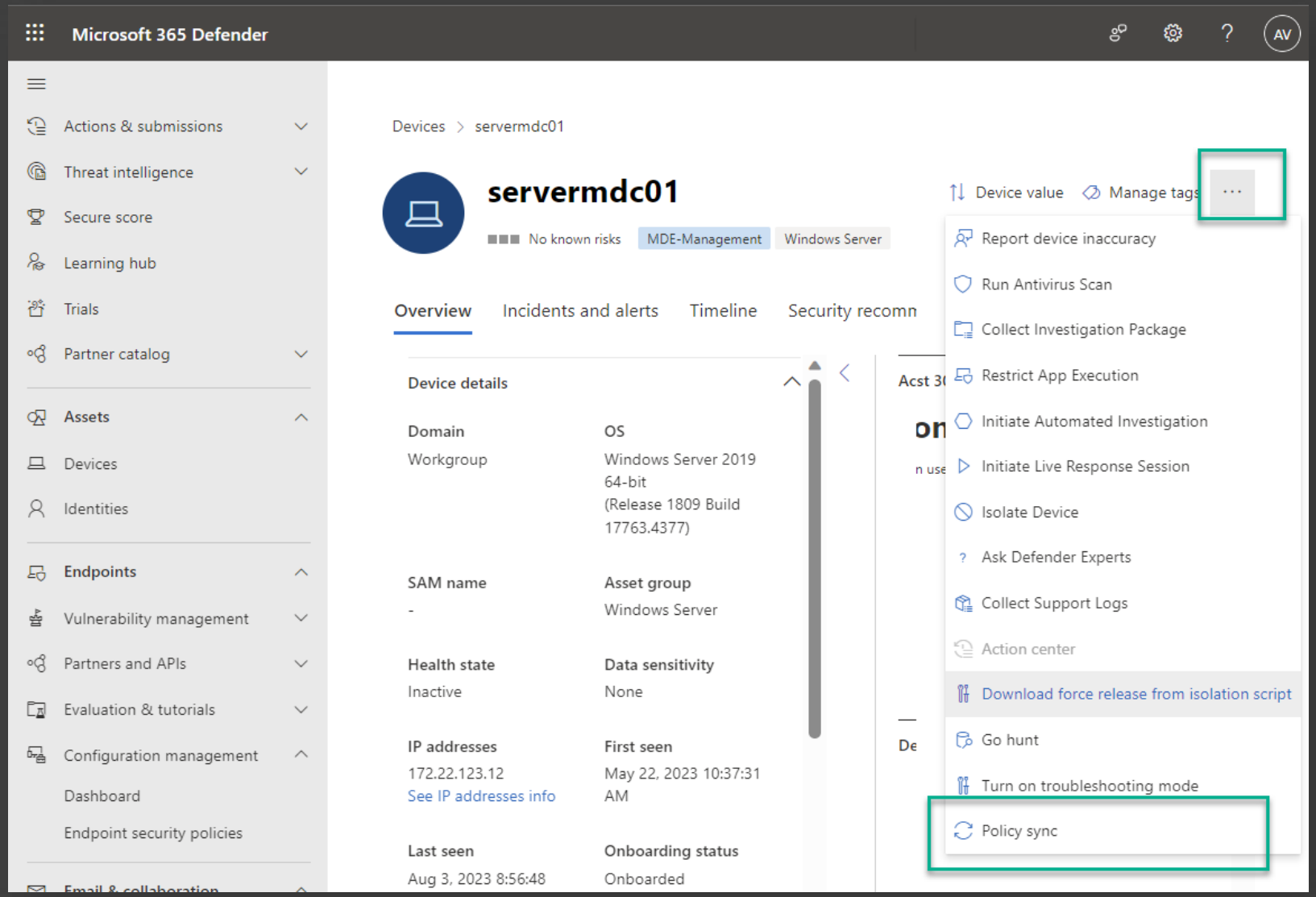
geekmania

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



geekmania

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



geekmania

Defender for Endpoint

Deception

geekmania

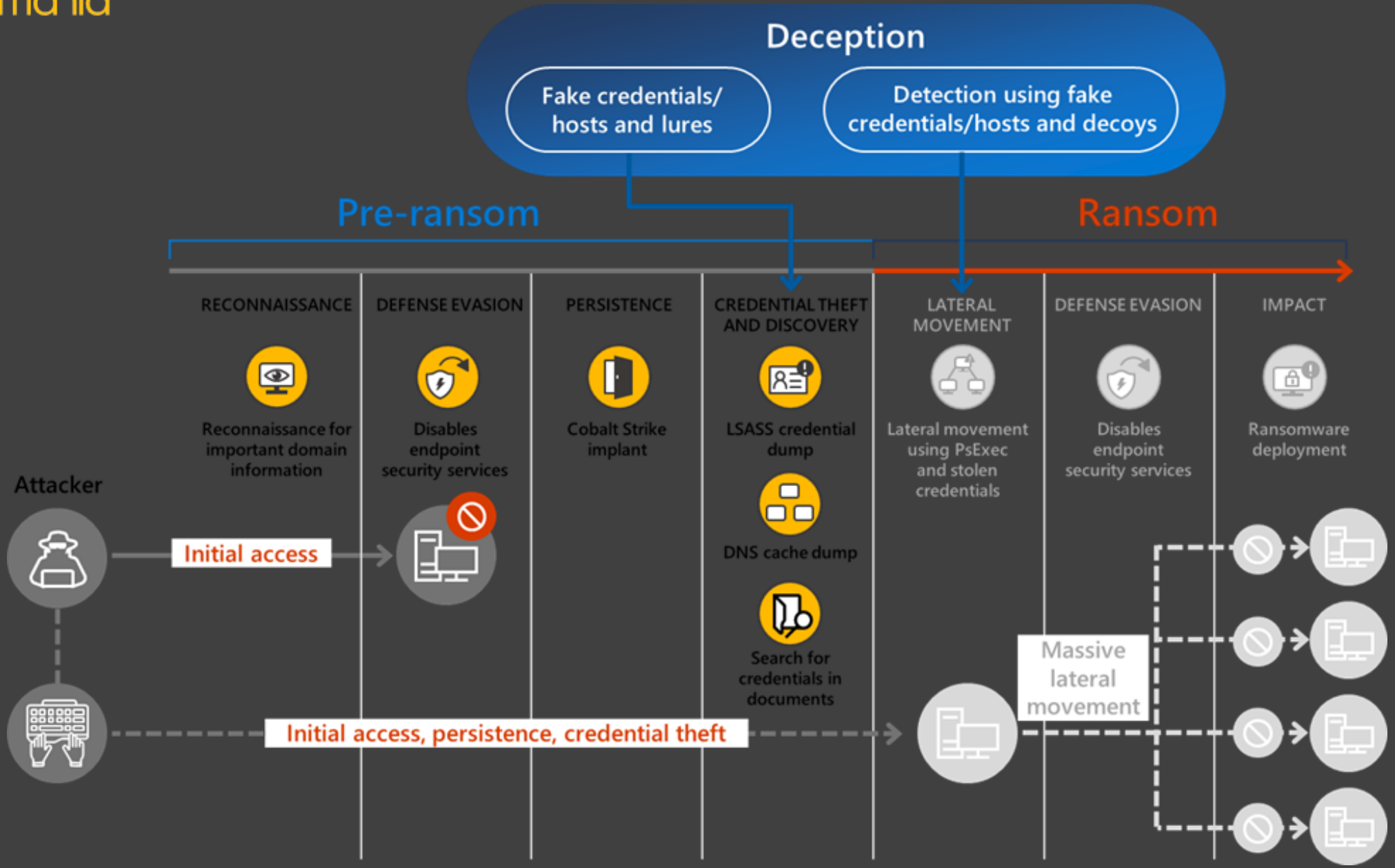
Microsoft Defender for Endpoint now includes deception as a built-in capability.

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

geekmania


Deception
Fake credentials/ hosts and lures
Detection using fake credentials/hosts and decoys
Pre-ransom
Ransom
RECONNAISSANCE
DEFENSE EVASION
PERSISTENCE
CREDENTIAL THEFT AND DISCOVERY
LATERAL MOVEMENT
DEFENSE EVASION
IMPACT
Reconnaissance for important domain information
Disables endpoint security services
Cobalt Strike implant
LSASS credential dump
DNS cache dump
Search for credentials in documents
Lateral movement using PsExec and stolen credentials
Disables endpoint security services
Ransomware deployment
Attacker
Initial access
Initial access, persistence, credential theft
Massive lateral movement

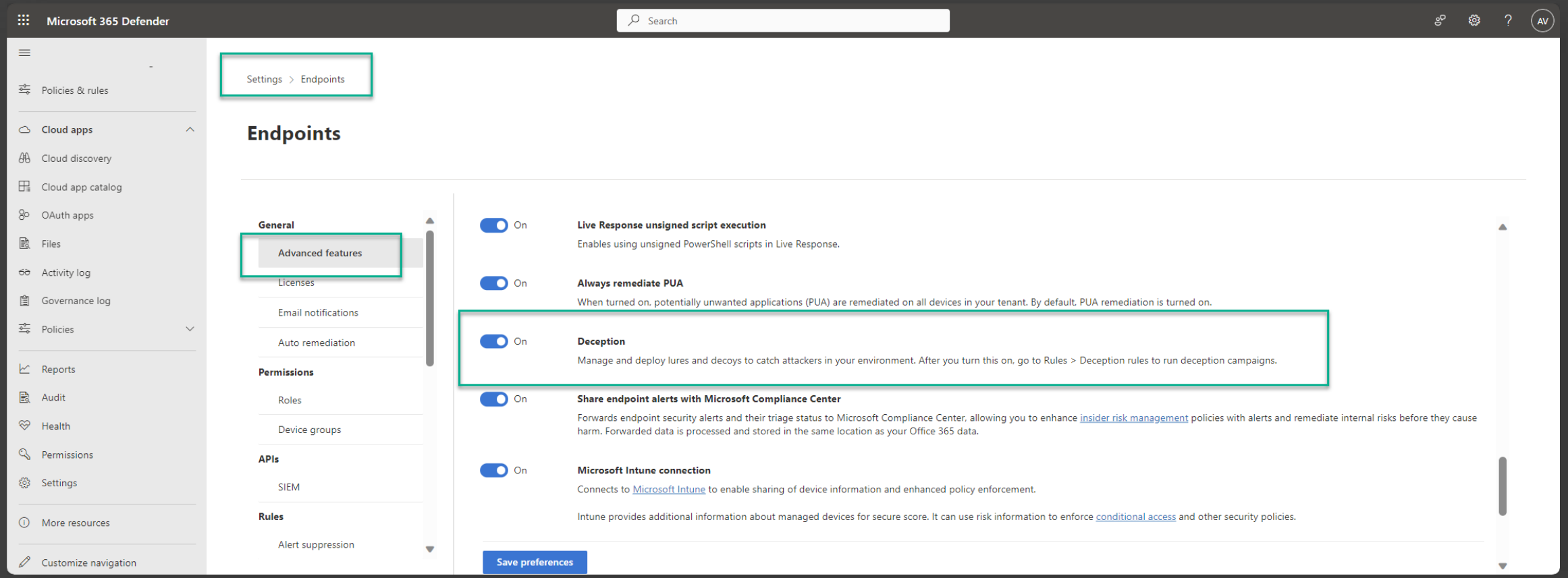
What is deception?

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.

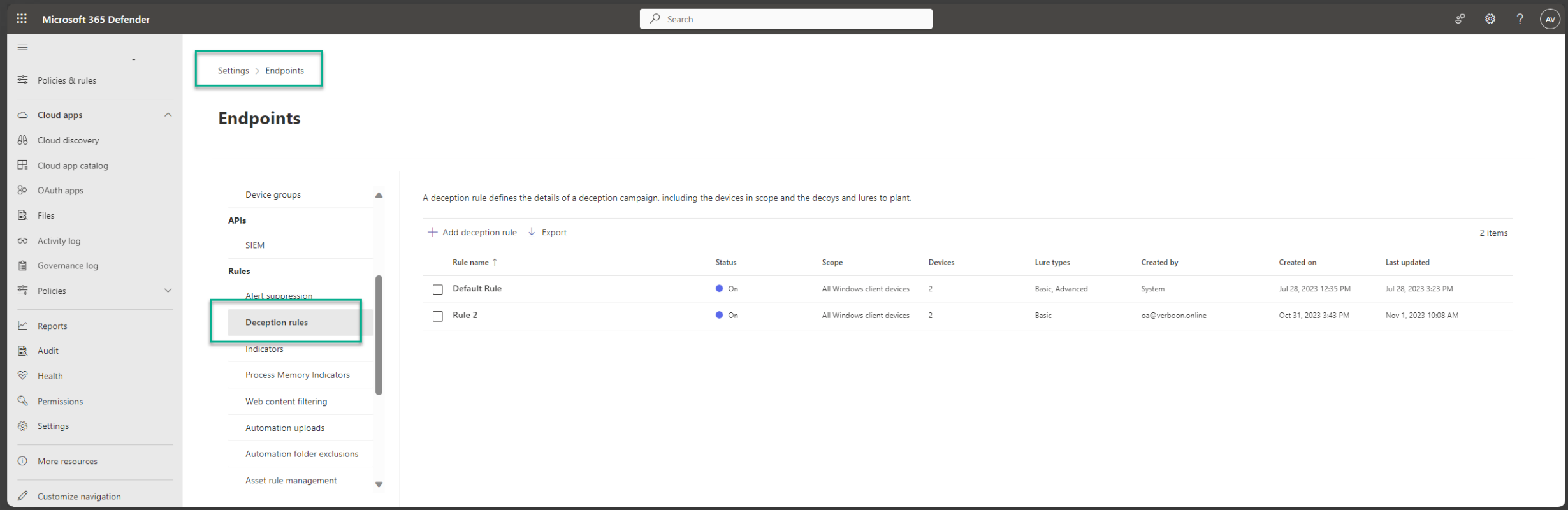
geekmania

Enable the Deception Feature



geekmania

Deception Rules



geekmania

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

geekmania

Search

Demo Deception

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

Define rule scope

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

Deception is currently applied only to Windows client devices.

Plant lures to *

- (•) All Windows client devices
- ( ) Devices with specific tags

Back | Next

geekmania

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
alinuxclient00020.verboon.online		Host
alinuxclient0020.verboon.online		Host
alinuxclient0043.verboon.online		Host
alinuxclient042.verboon.online		Host
alinuxclient026.verboon.online		Host

Back | Next

geekmania

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 | Edit | Delete

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	✓	✗

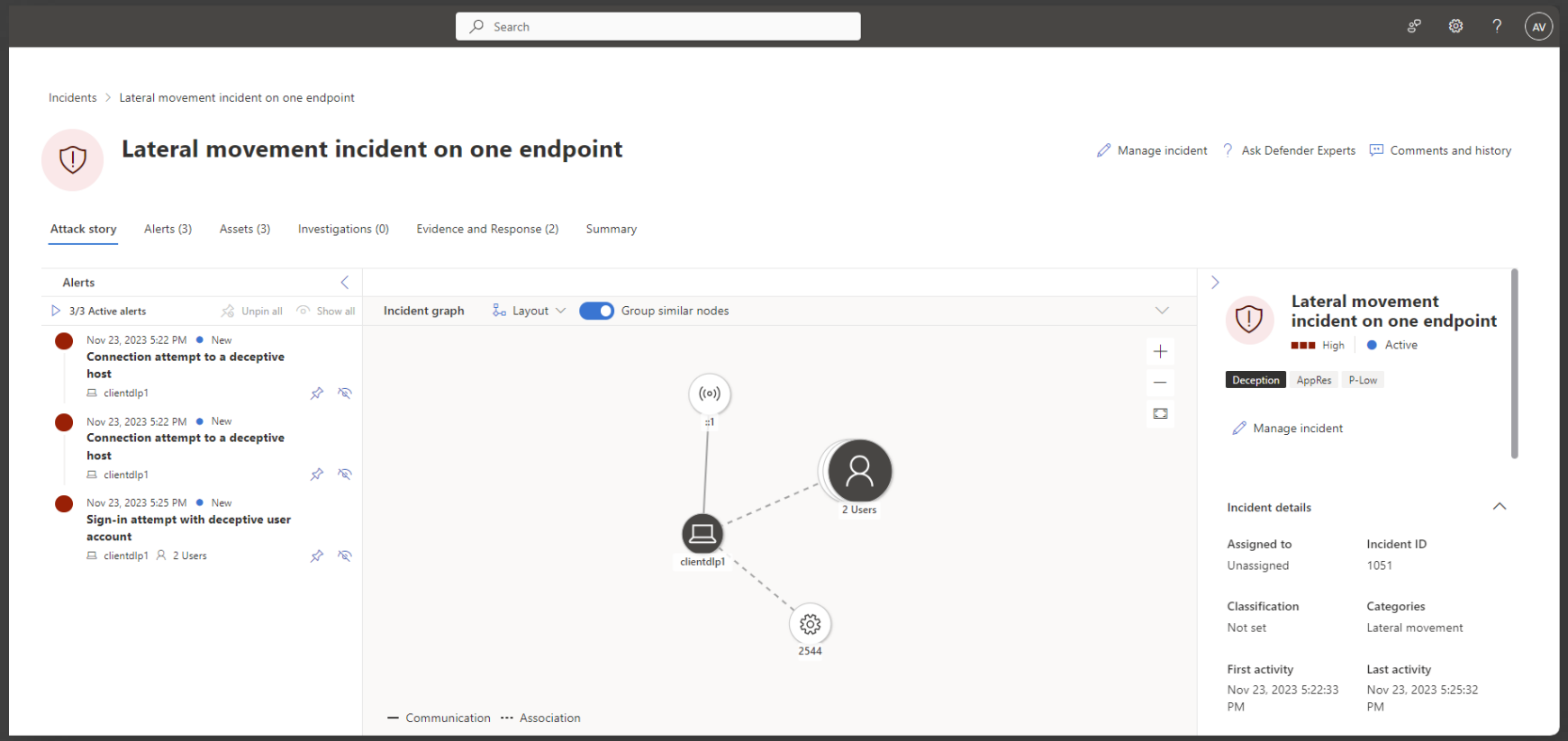
Back | Next

geekmania

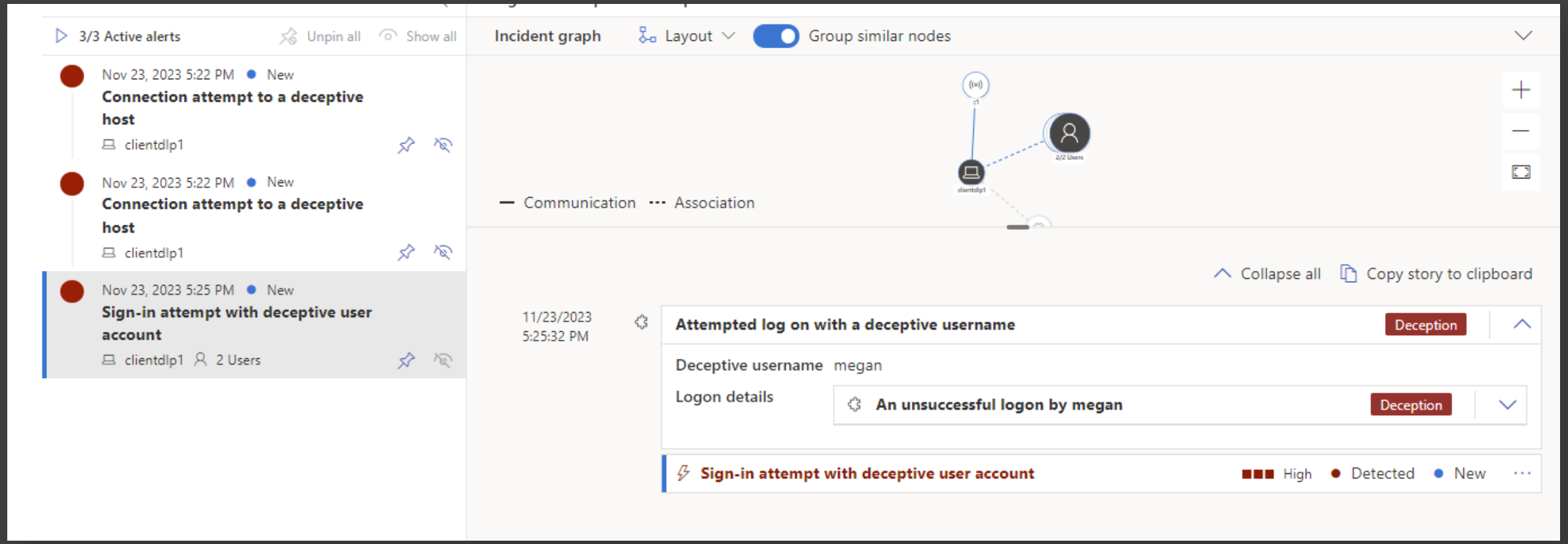
Incidents and alerts activated by deception

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



geekmania


3/3 Active alerts
Unpin all
Show all
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
Incident graph
Layout
Group similar nodes
Communication
Association
Collapse all
Copy story to clipboard
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

geekmania

Microsoft Defender for Cloud Apps

App Governance

geekmania

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

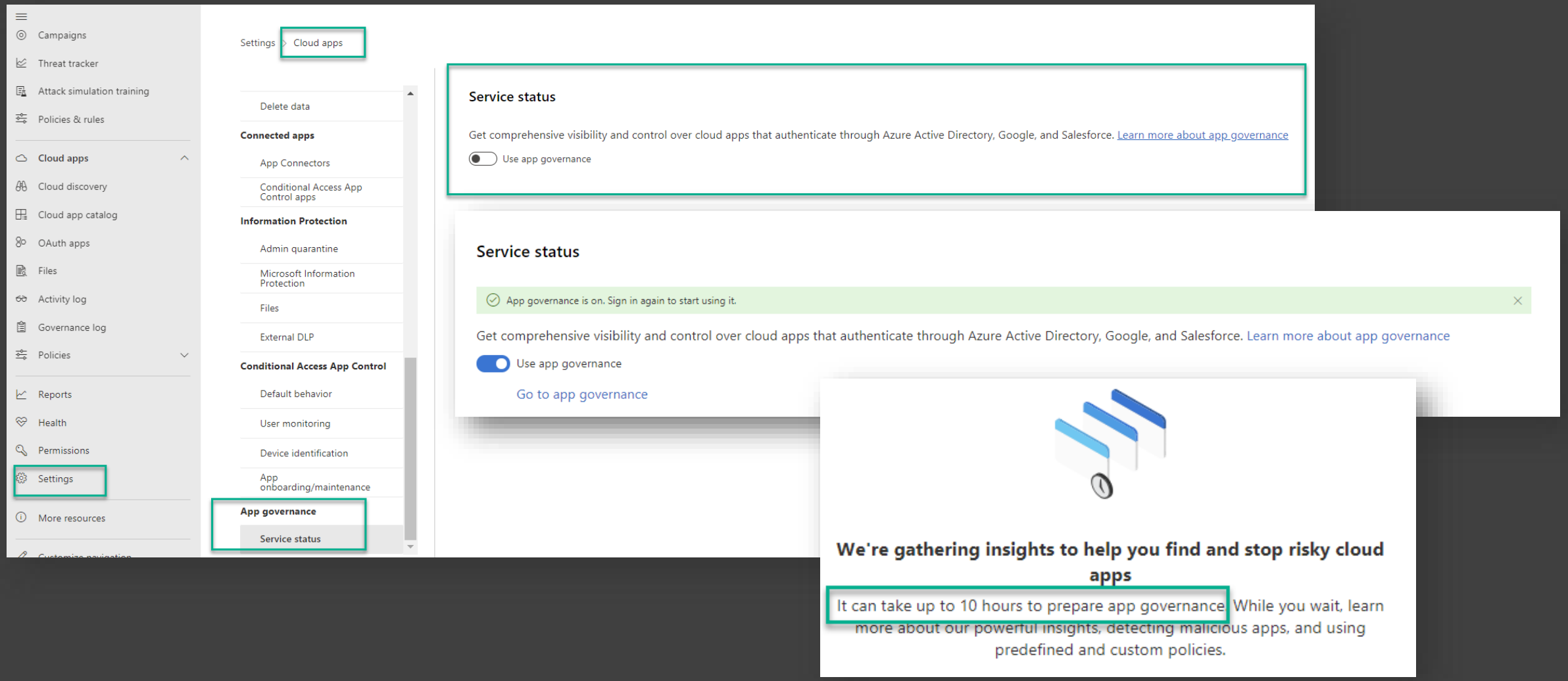
It delivers full visibility, remediation, and governance into how these apps and their users access, use, and share sensitive data stored in Microsoft 365 through actionable insights and automated policy alerts.

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.

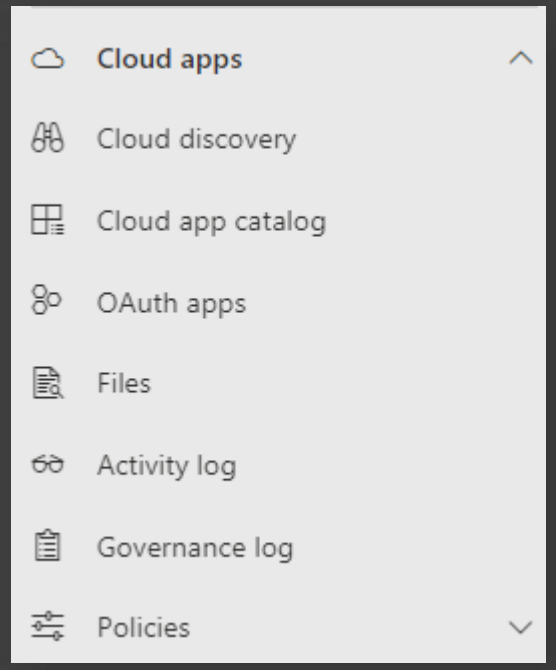
geekmania

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

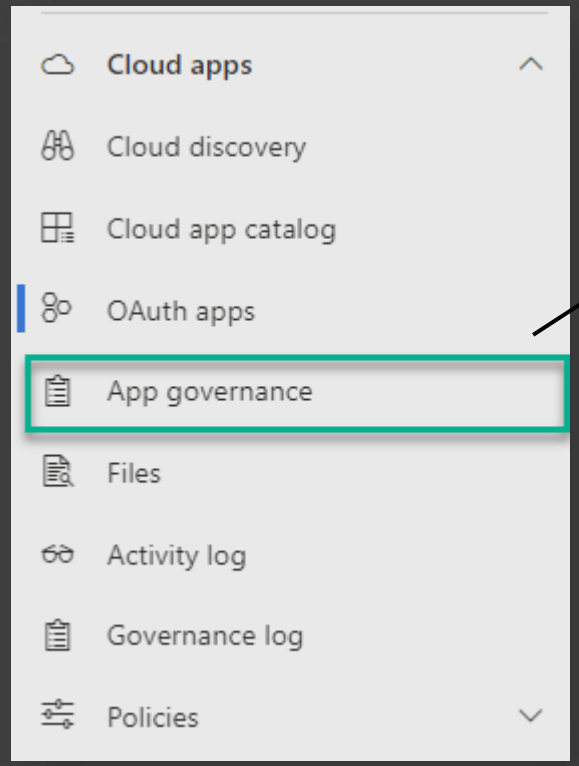


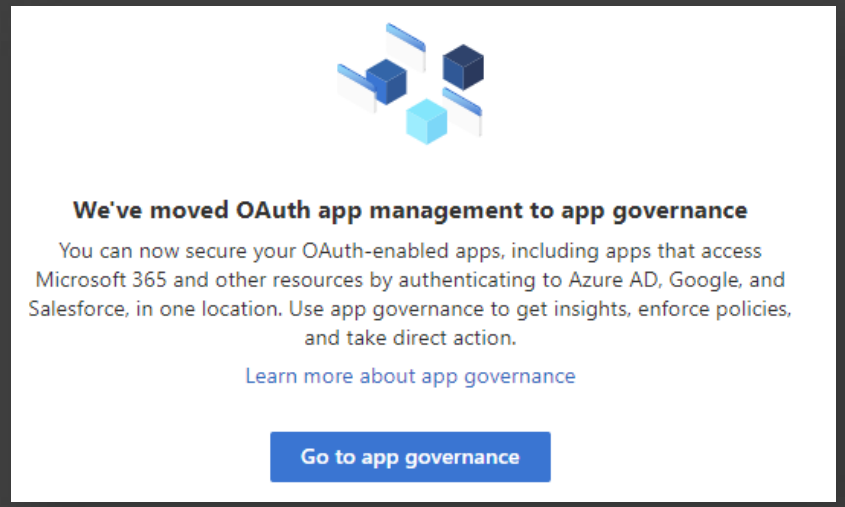
geekmania

Before App Governance enablement



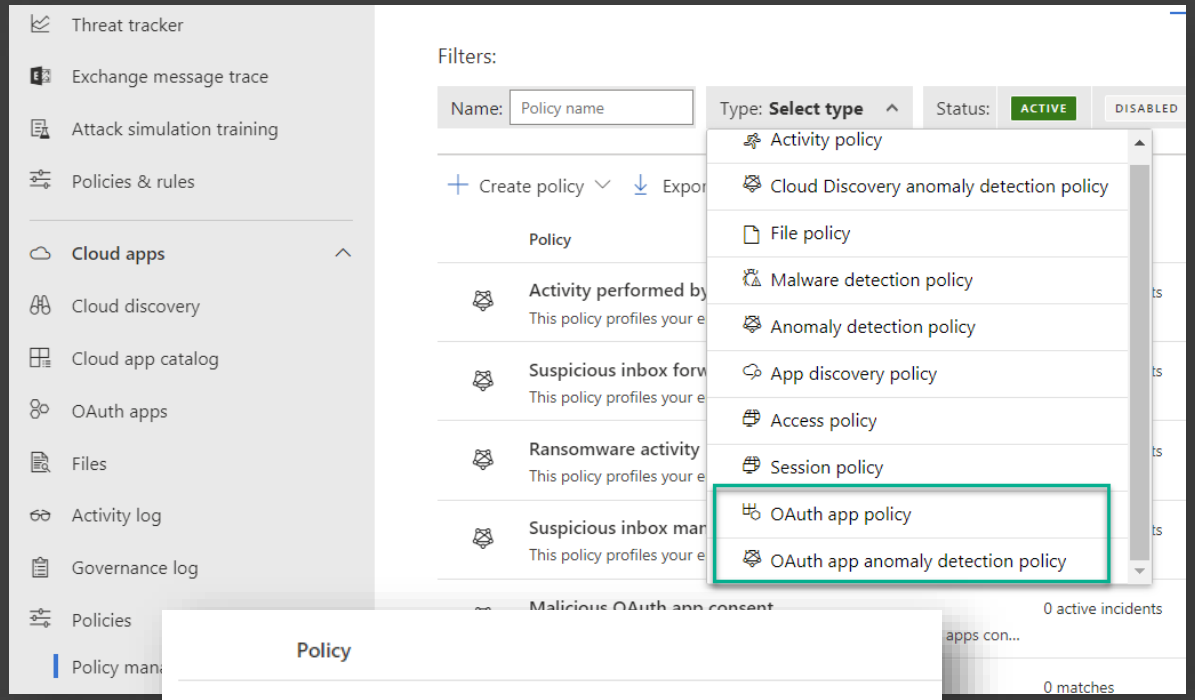
After App Governance enablement

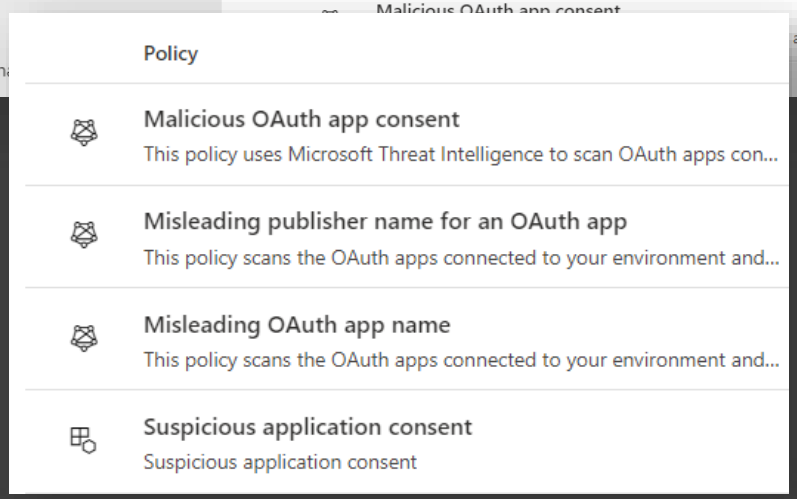




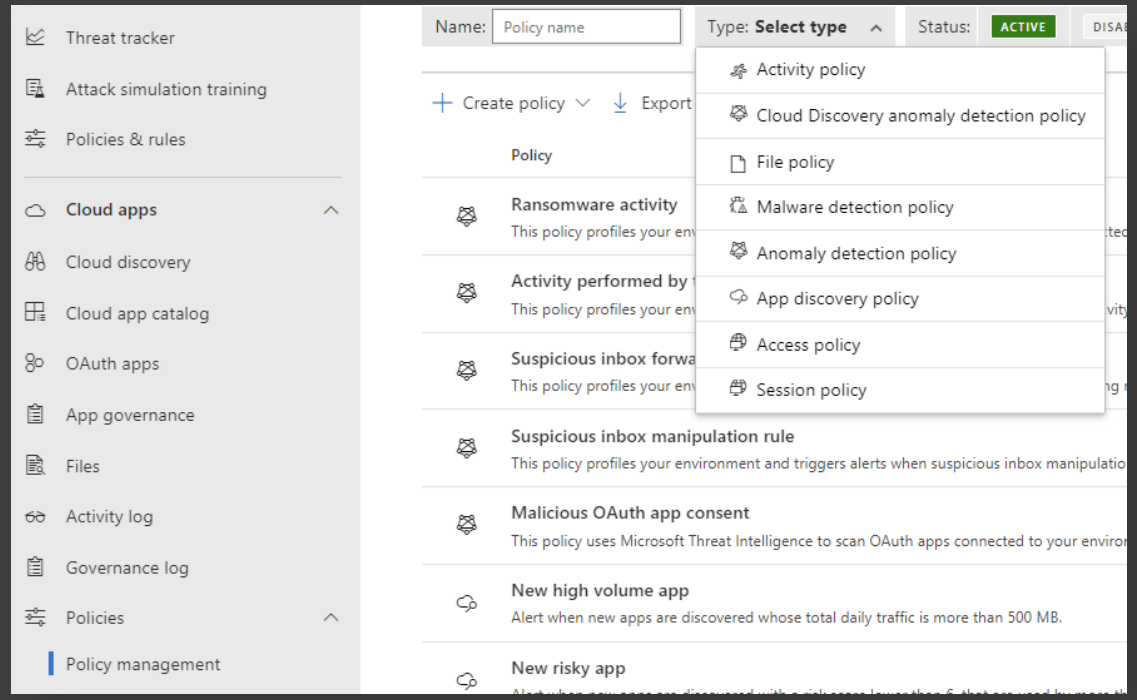
geekmania

Before App Governance enablement





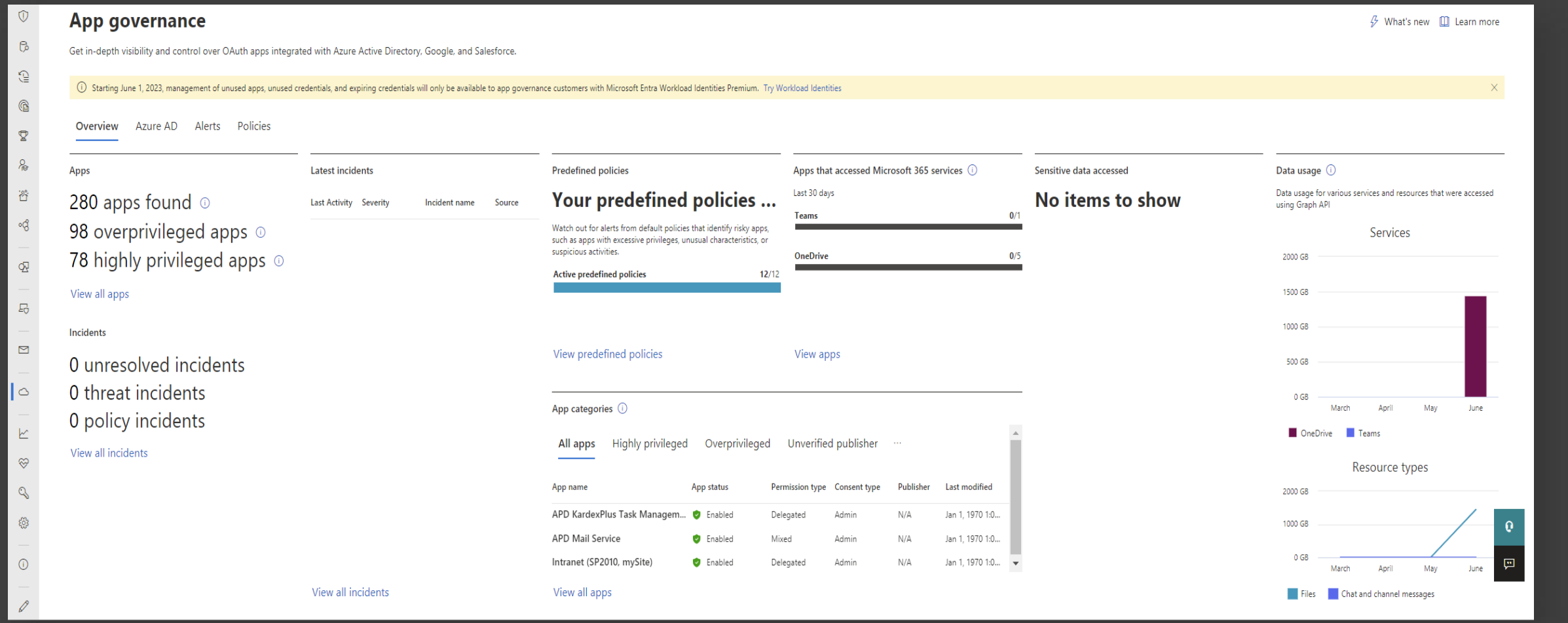
After App Governance enablement



The OAUTH related policies are moved into App Governance

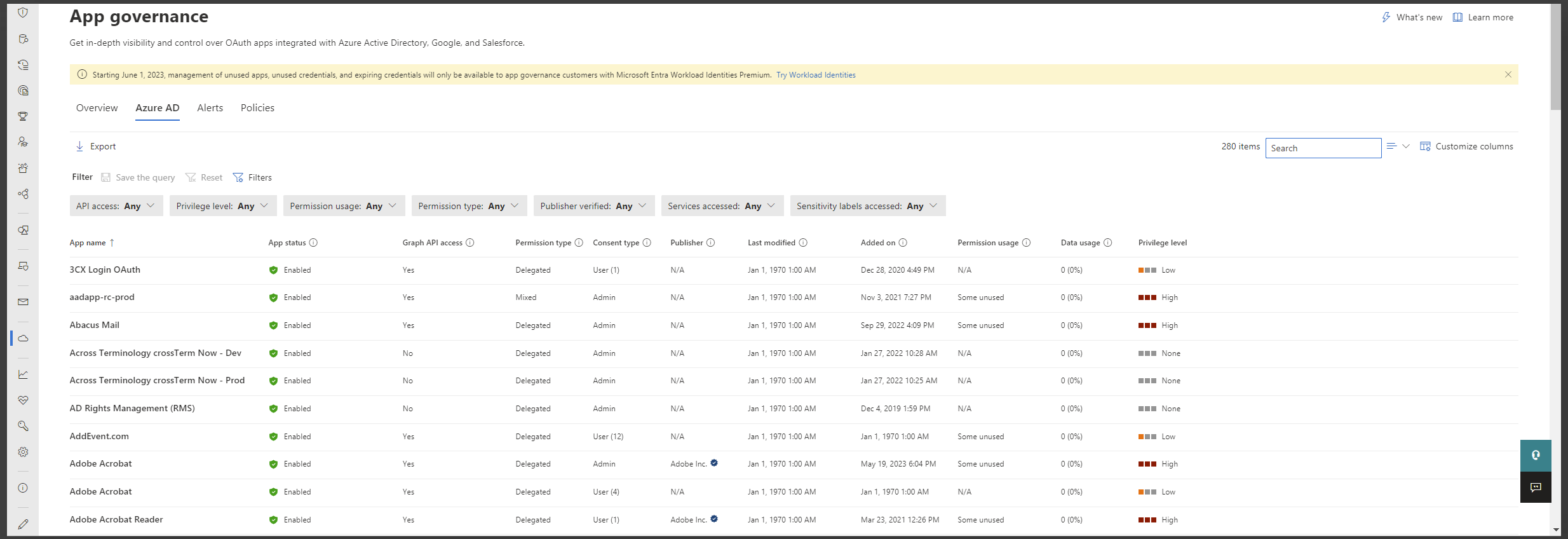
geekmania

App Governance Overview

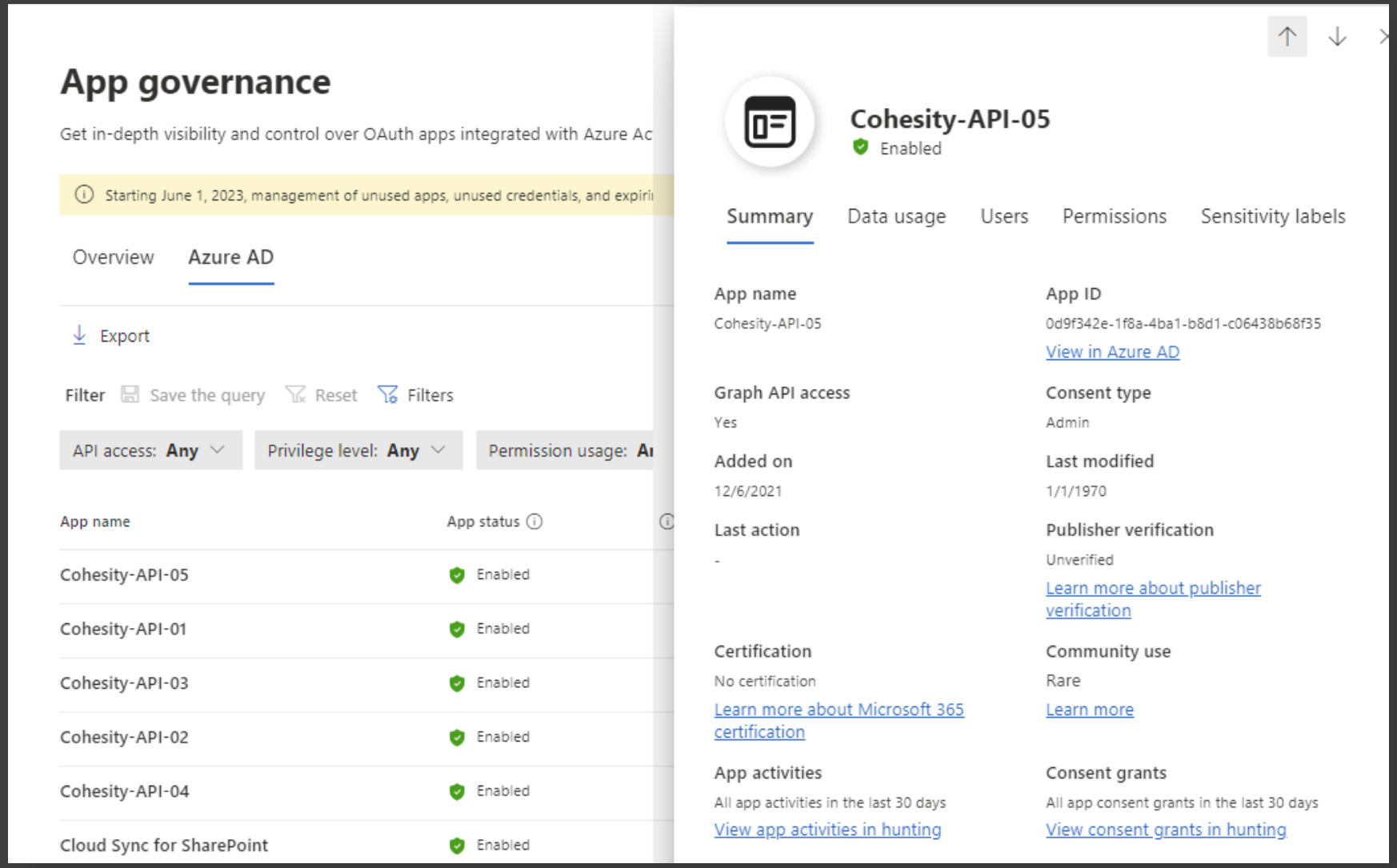


geekmania

All Apps in Entra ID



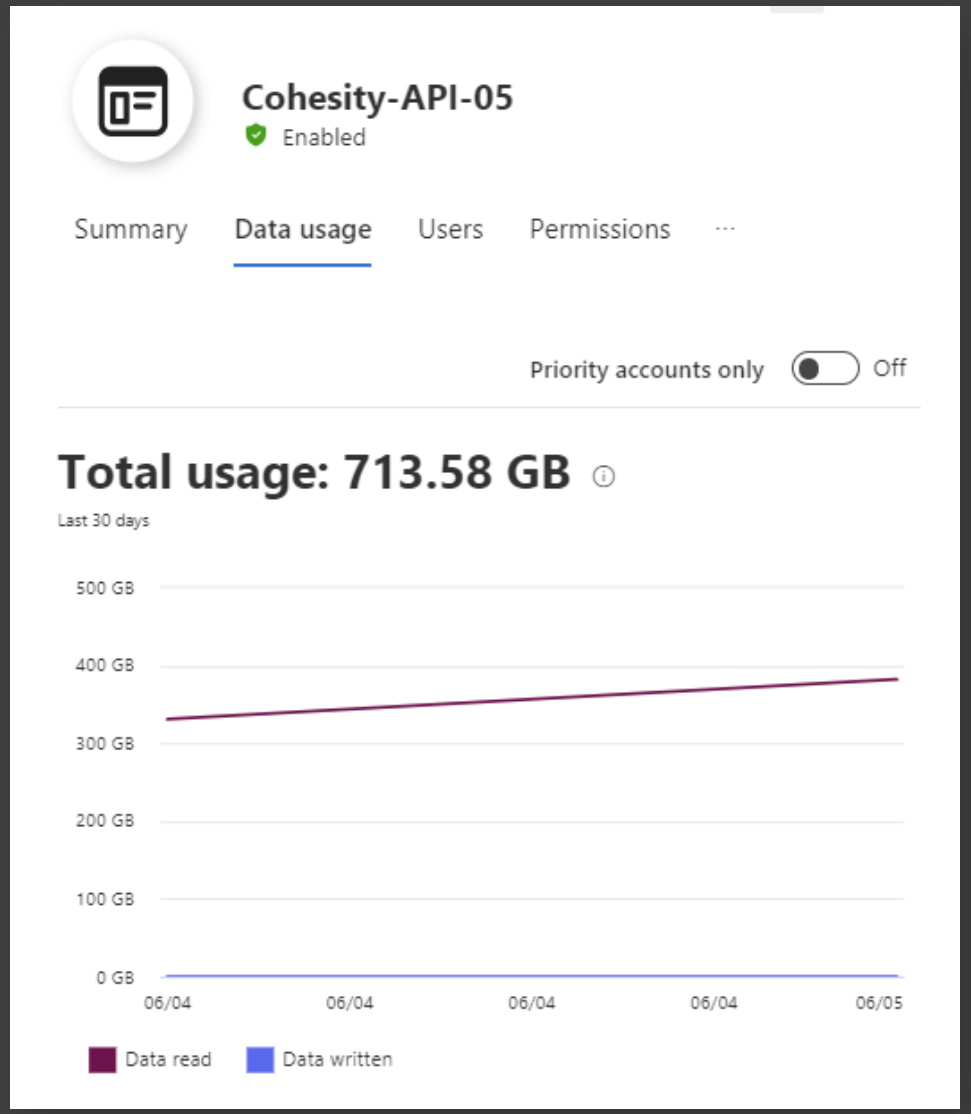
geekmania

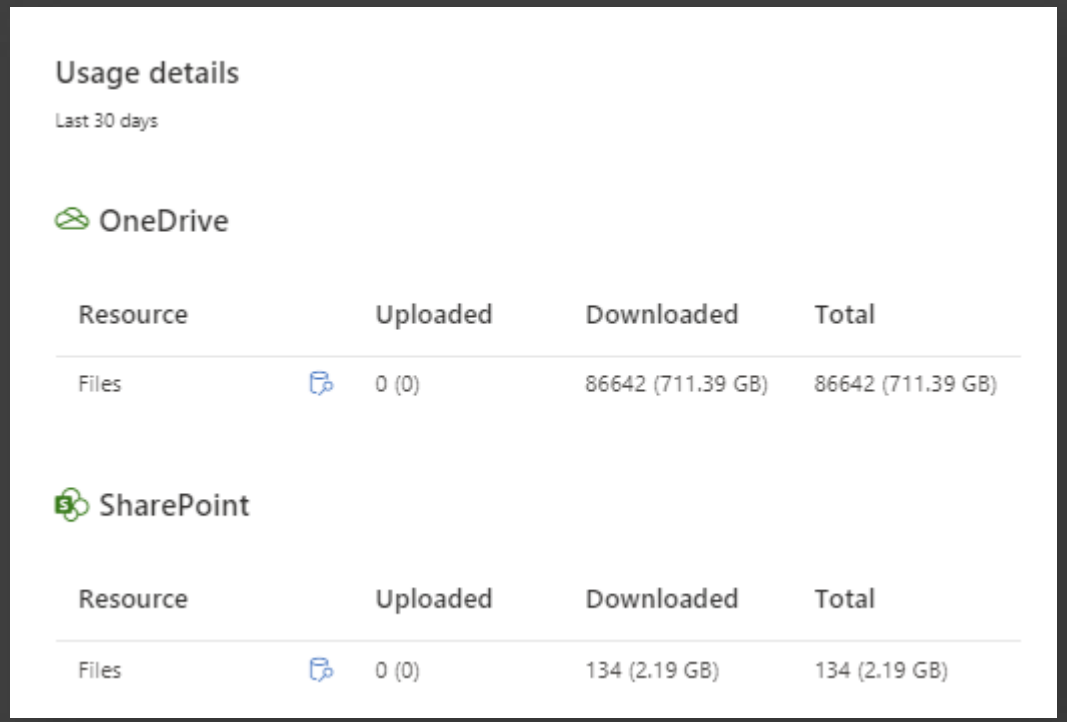


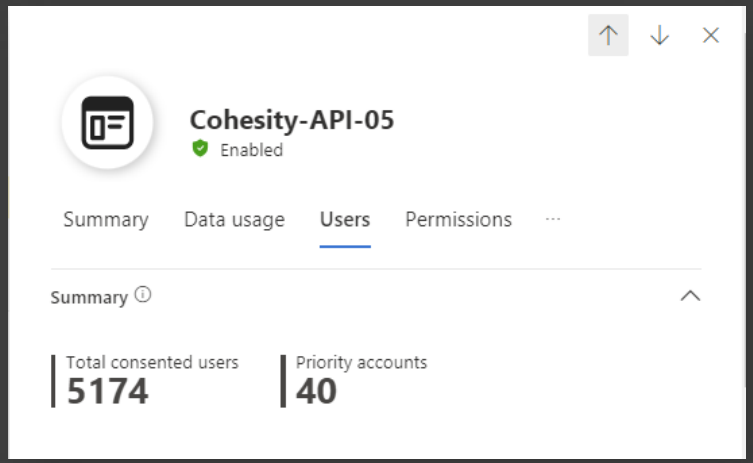
Get insights about Apps

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

geekmania

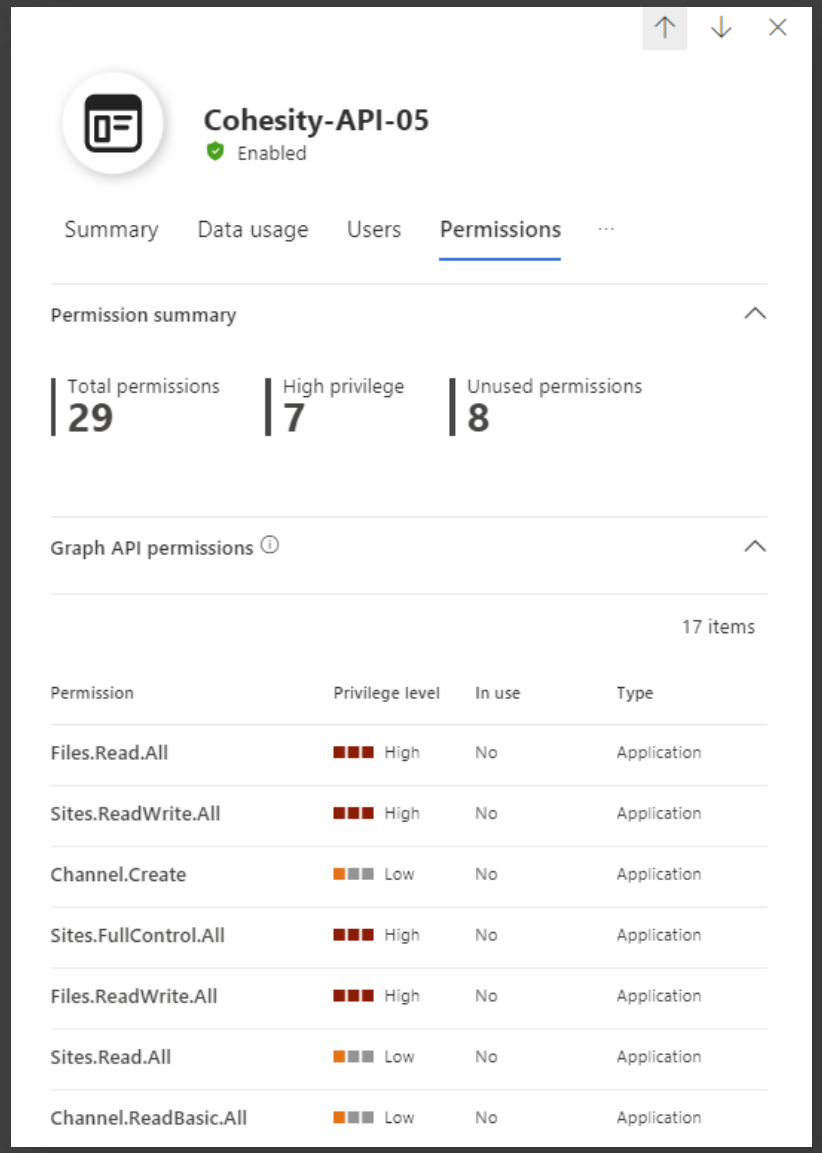

Cohesity-API-05
Enabled
Summary
Data usage
Users
Permissions
Priority accounts only
Off
Total usage: 713.58 GB
Last 30 days
500 GB
400 GB
300 GB
200 GB
100 GB
0 GB
06/04
06/04
06/04
06/04
06/05
Data read
Data written


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)


Cohesity-API-05
Enabled
Summary
Data usage
Users
Permissions
Summary
Total consented users
5174
Priority accounts
40

geekmania

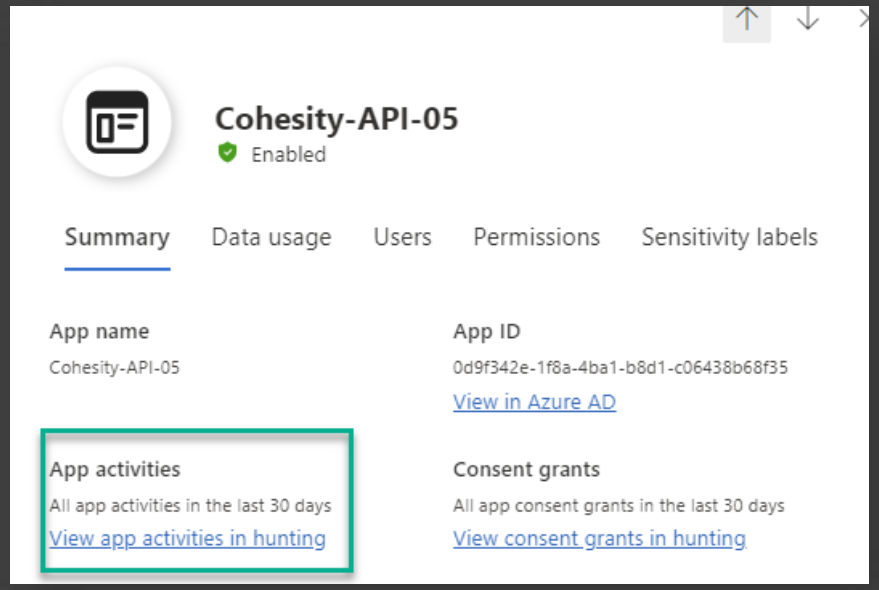
Permissions

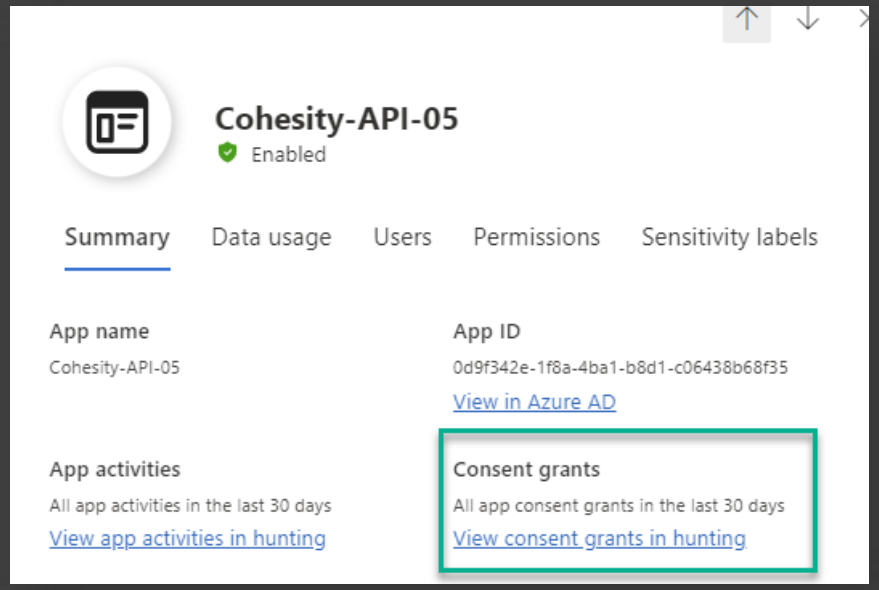


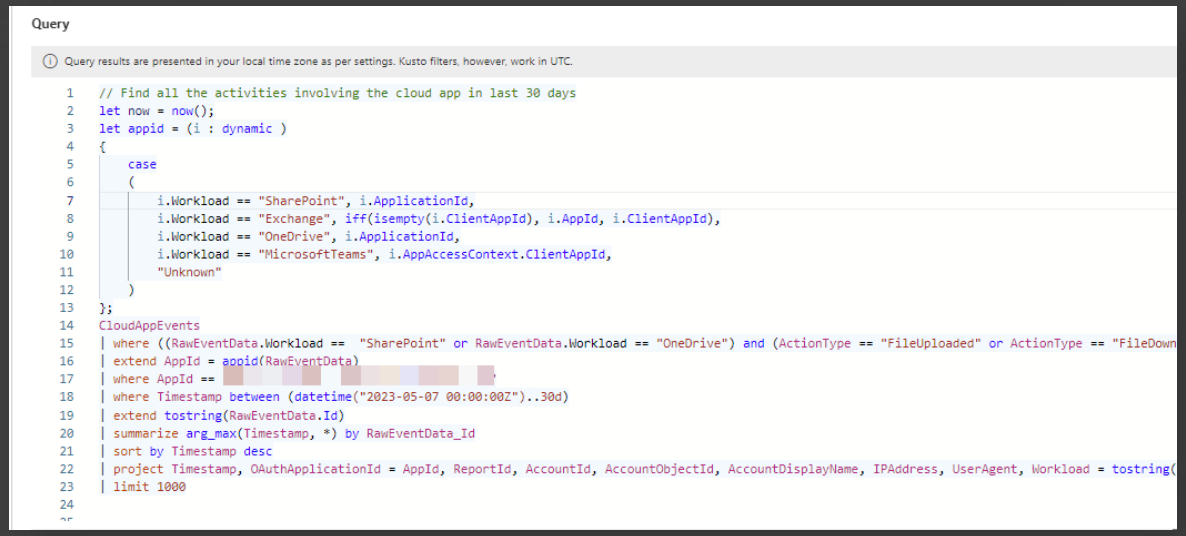
Permission	API	Type
TermStore.ReadWrite.All	Office 365 SharePoint Online	Application
TermStore.ReadWrite.All	Office 365 SharePoint Online	Delegated
MyFiles.Read	Office 365 SharePoint Online	Delegated
AllSites.Read	Office 365 SharePoint Online	Delegated
User.ReadWrite.All	Office 365 SharePoint Online	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

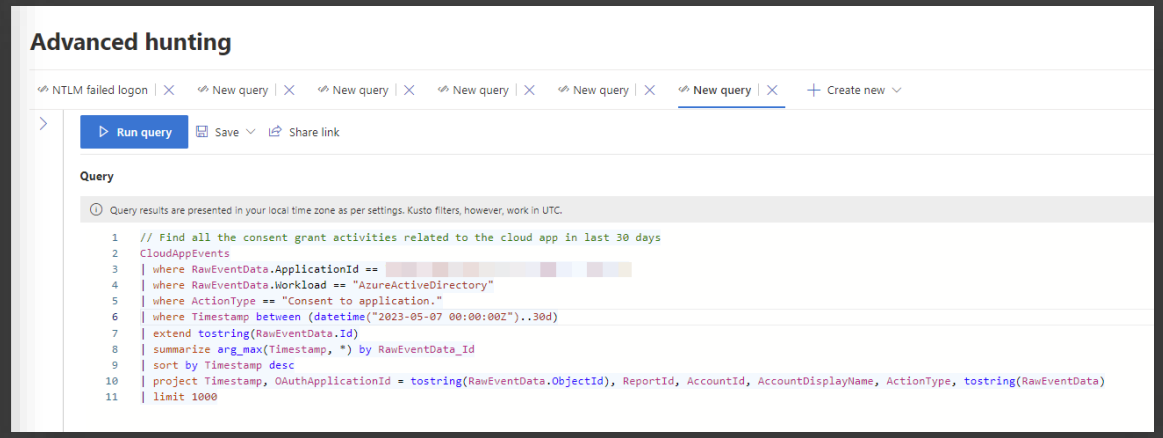
geekmania

Advanced Hunting









geekmania

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

geekmania

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

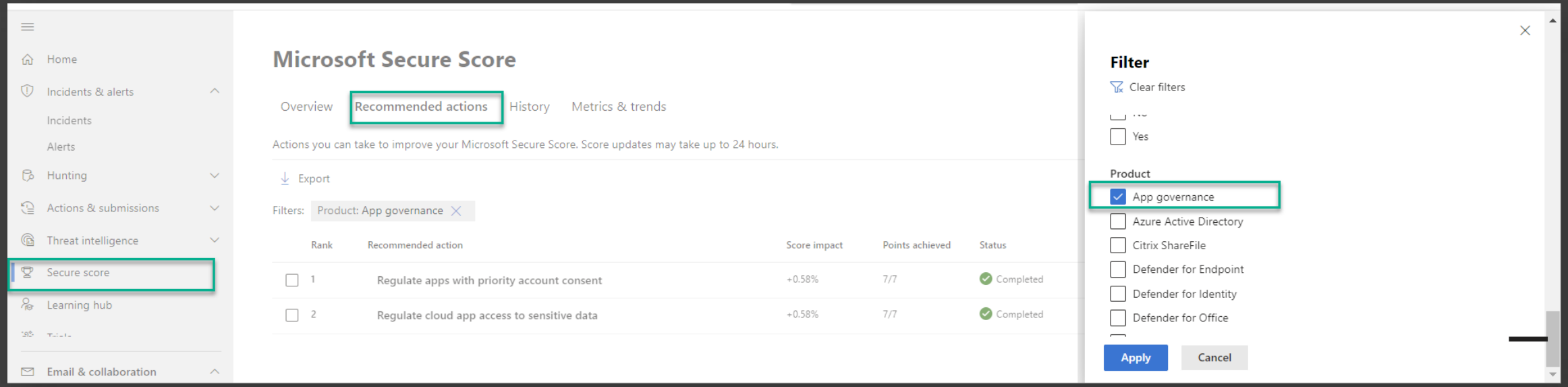
geekmania

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 senstitive 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 orther 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

geekmania

Secure Score



geekmania

Microsoft Defender for Endpoint

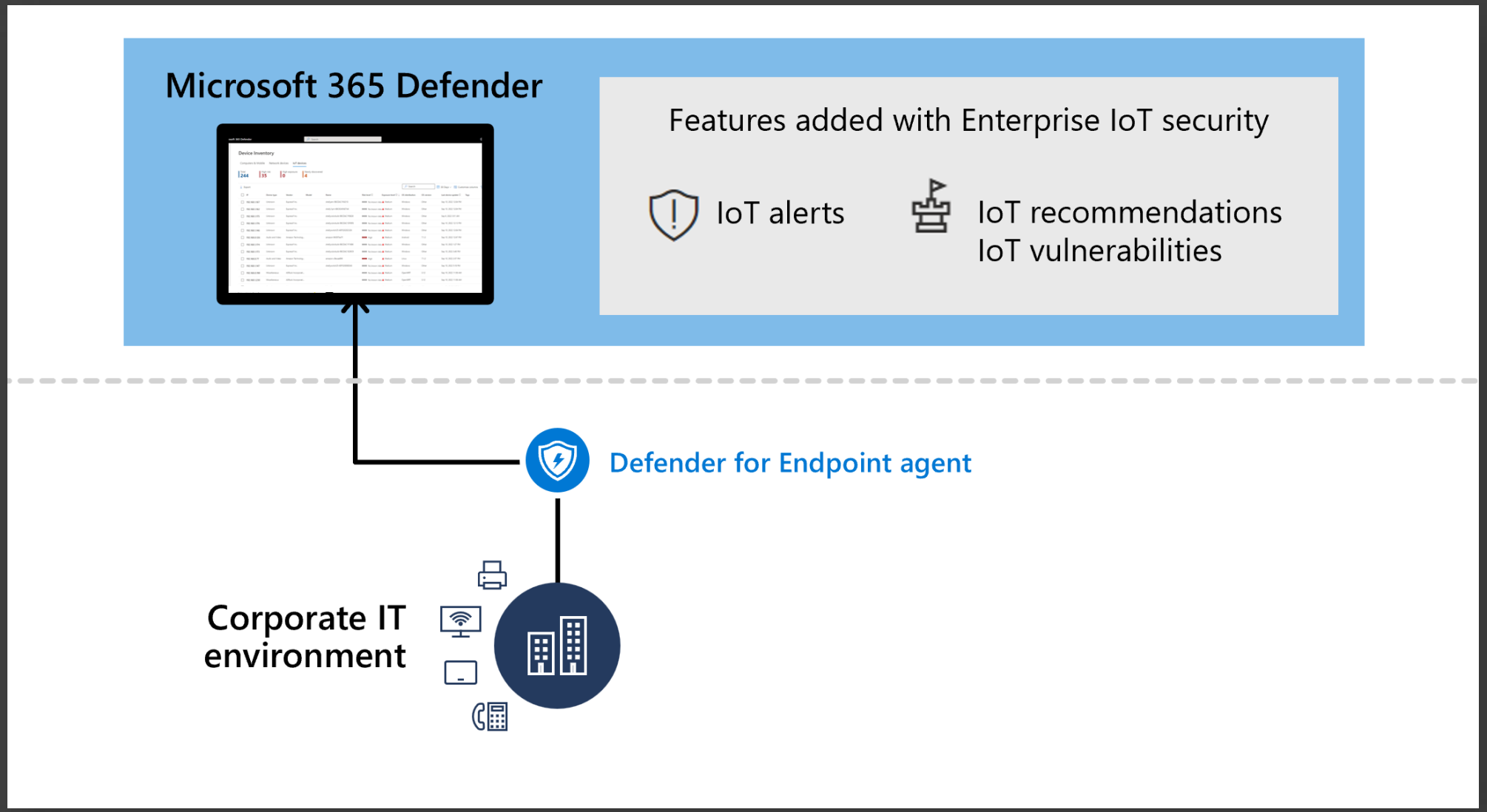
Enterprise IoT security is now included in Microsoft 365 E5 and E5 Security plans

To help organizations achieve a more holistic endpoint security strategy that traverses both IT and eIoT devices easily, Microsoft announced that the eIoT 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:

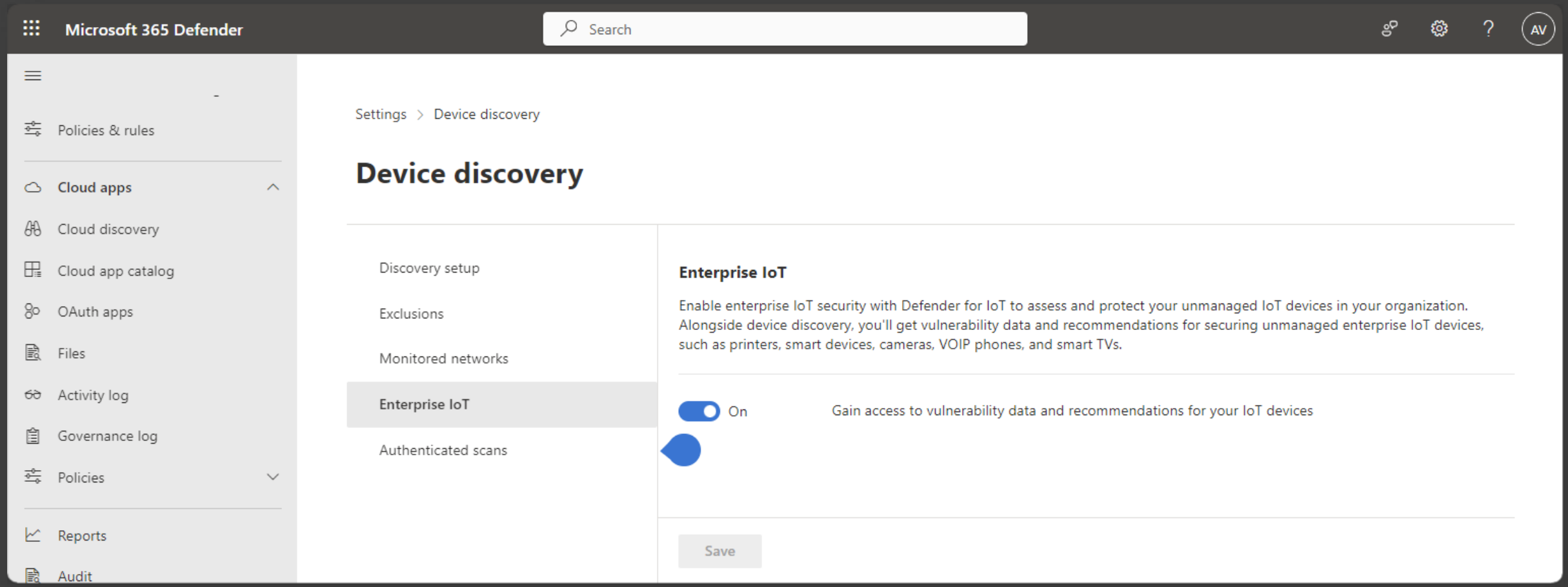
- Eliminate critical blind spots by discovering unmanaged enterprise IoT devices
- Identify anomalies across the eIoT device estate with continuous monitoring
- Harden posture across eIoT with vulnerability assessments with actionable guidance to help remediate at-risk devices

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



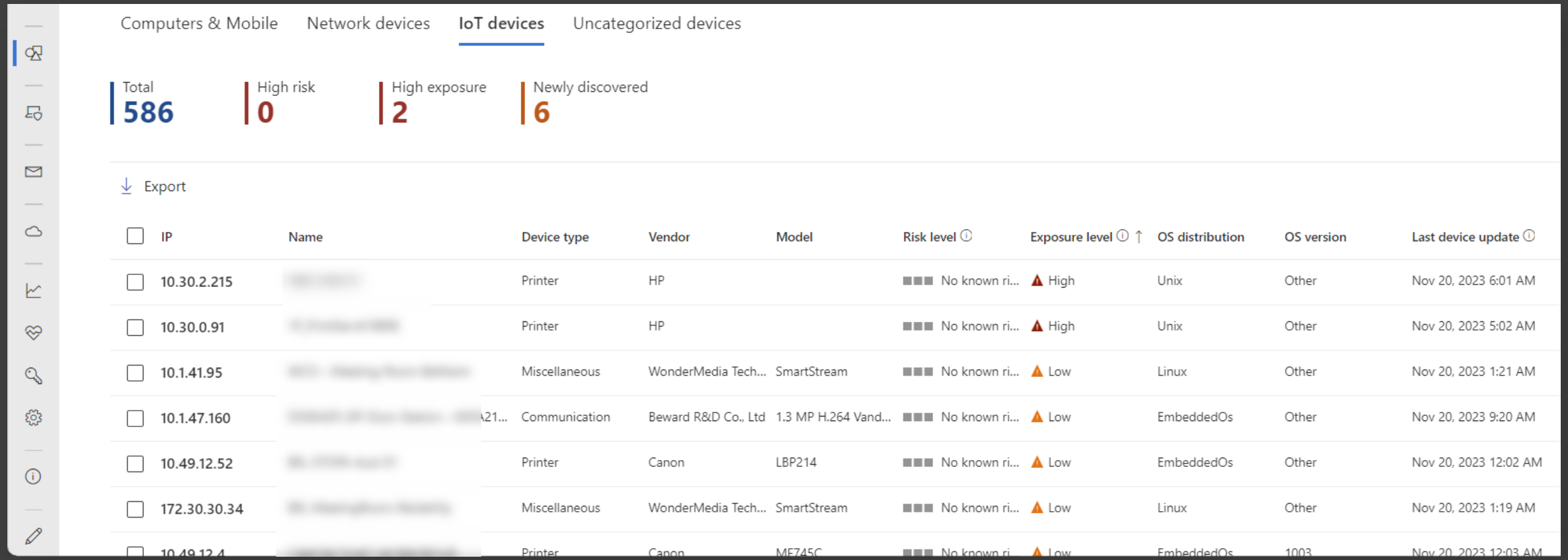
geekmania

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



geekmania

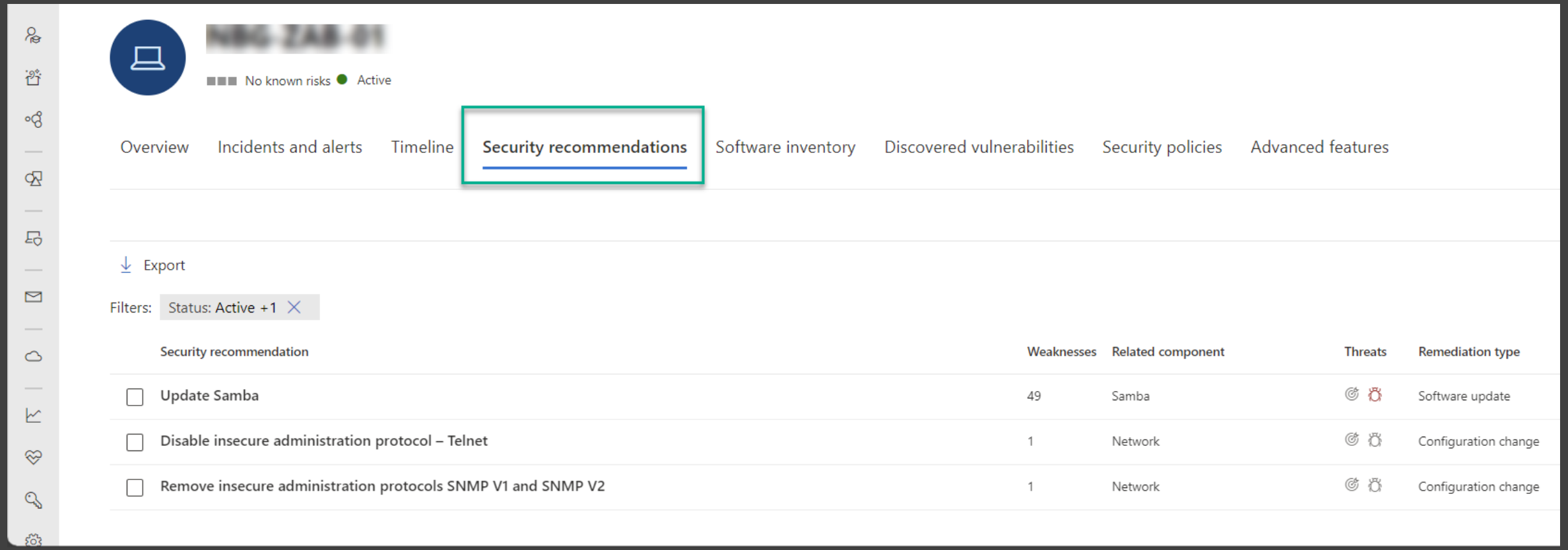
EIOT Device Inventory



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

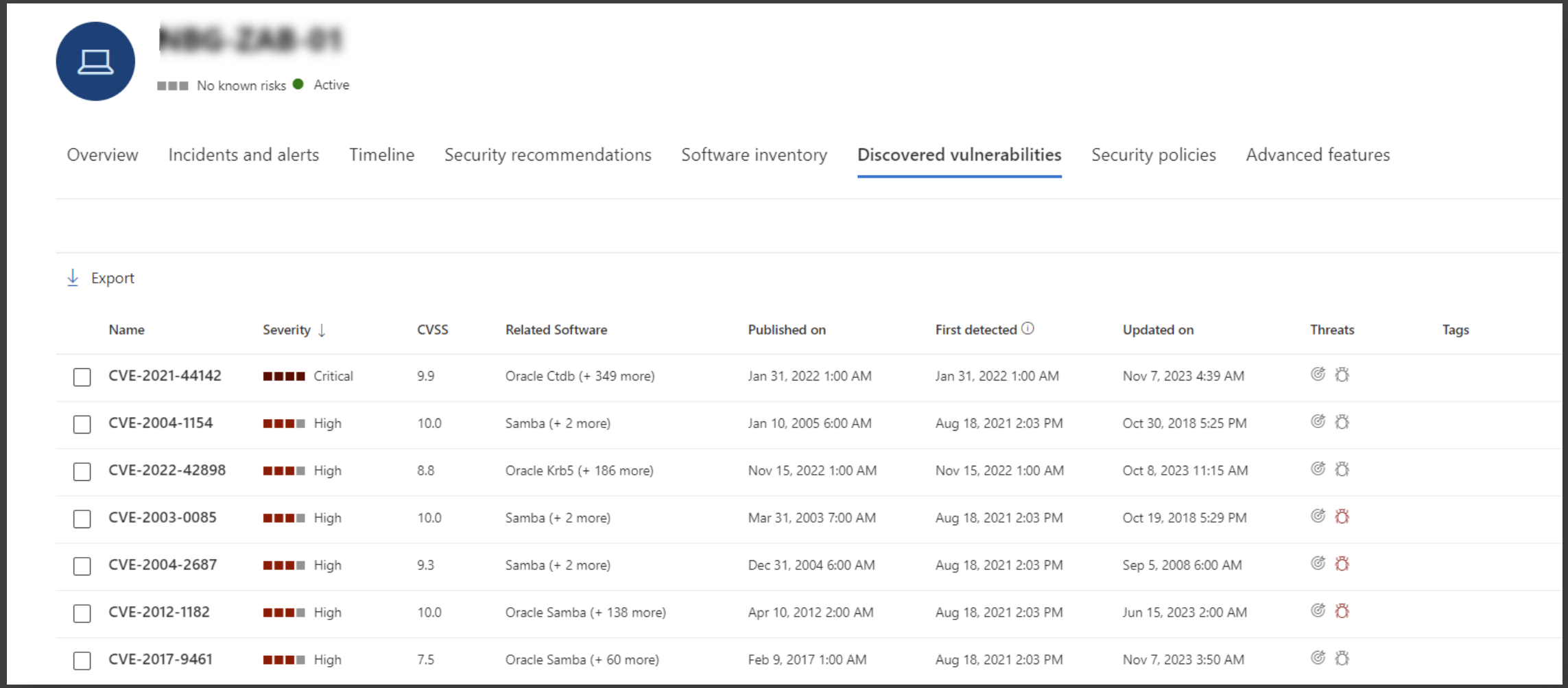
geekmania

Security Recommendations



geekmania

Vulnerabilities



Name	Severity	CVSS	Related Software	Published on	First detected	Updated on	Threats	Tags
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		
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		
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		
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		
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		
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		
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		

geekmania

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.

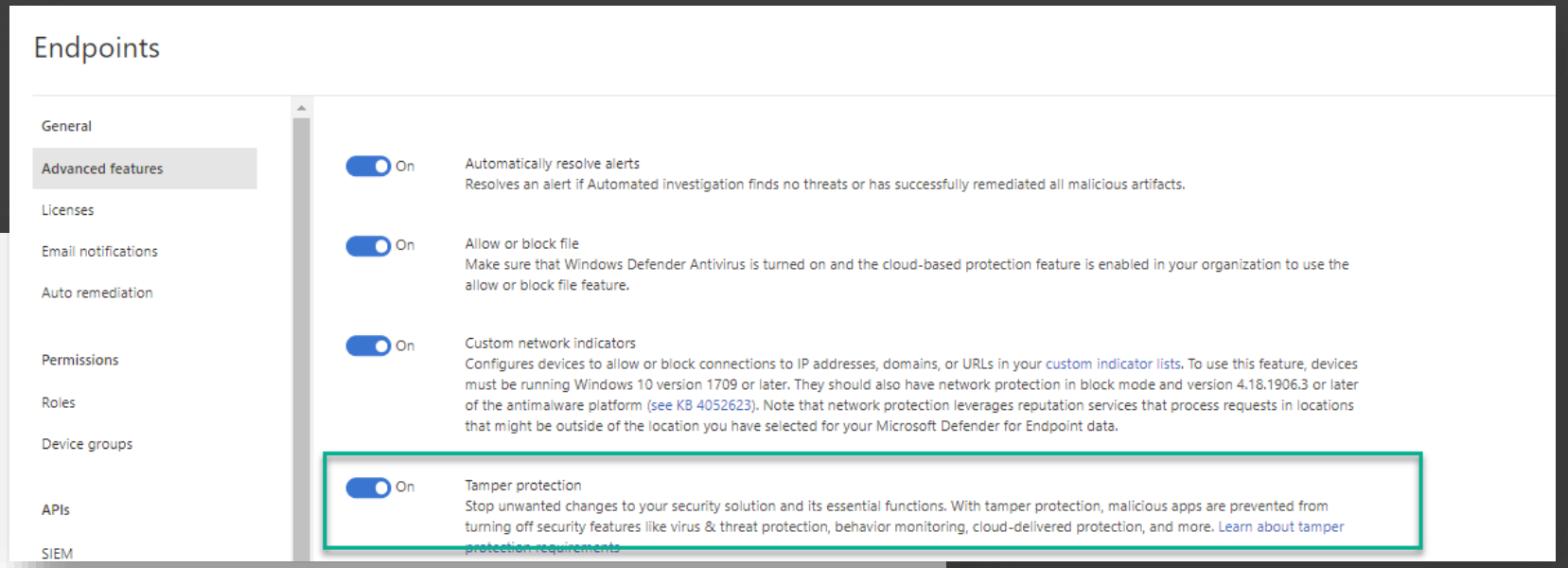
Microsoft has enabled functionality that protects path, process, and extension exclusions deployed through Intune.

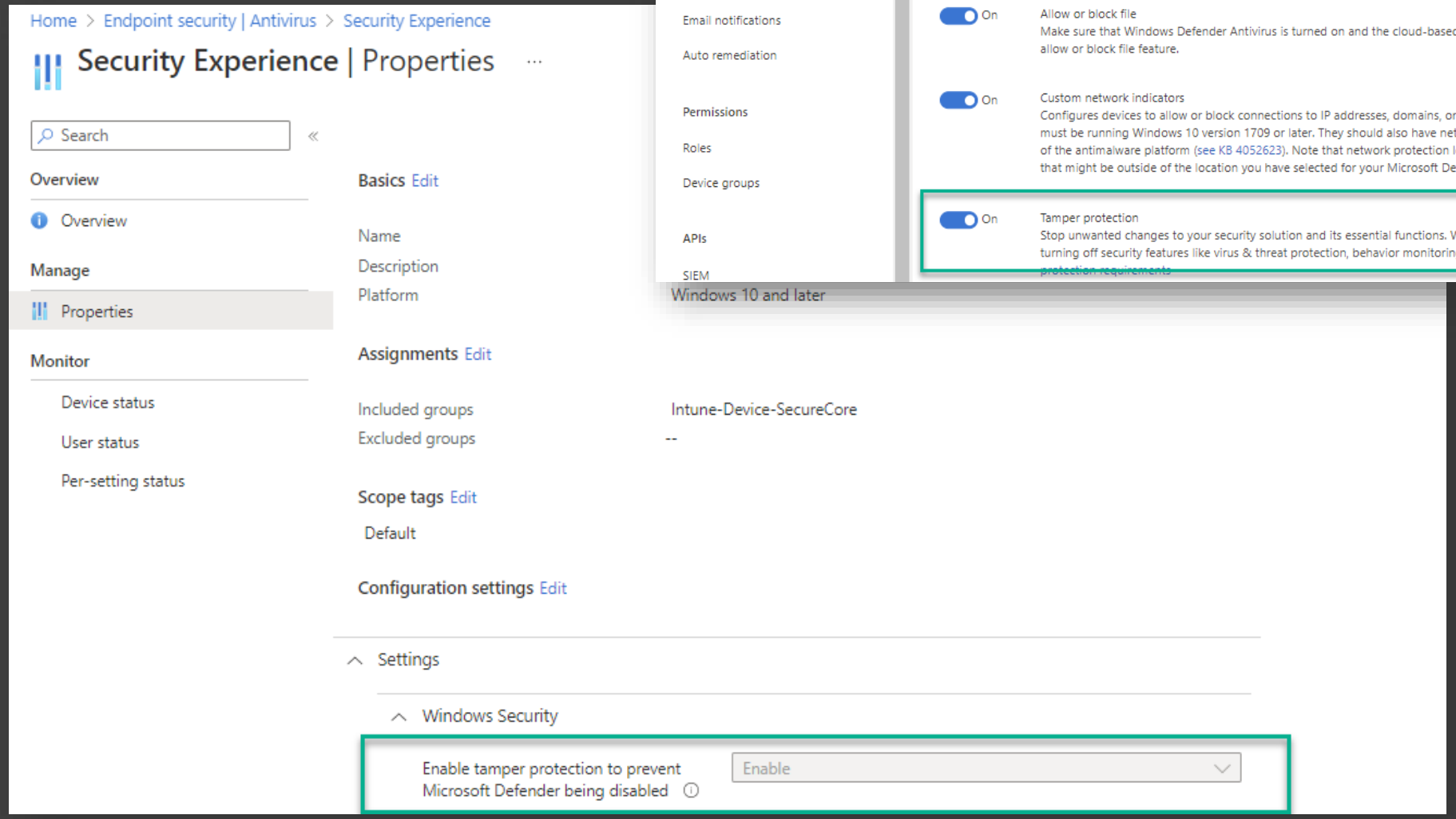
When tamper protection is combined with the DisableLocalAdminMerge setting exclusions and DisableLocalAdminMerge will be protected by tamper protection.

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

geekmania

Enable tamper protection at the tenant level

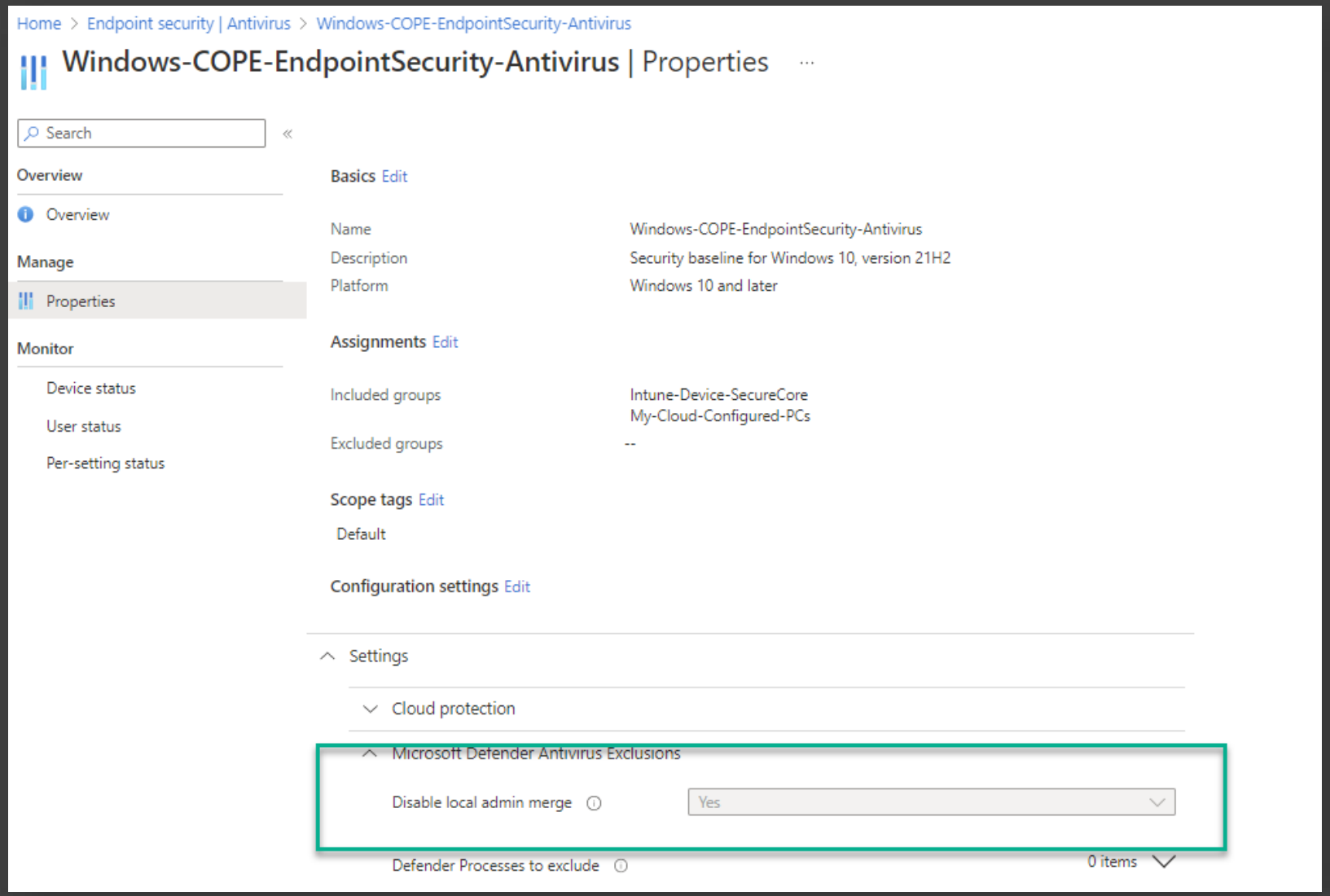




OR

Enable tamper protection through Intune

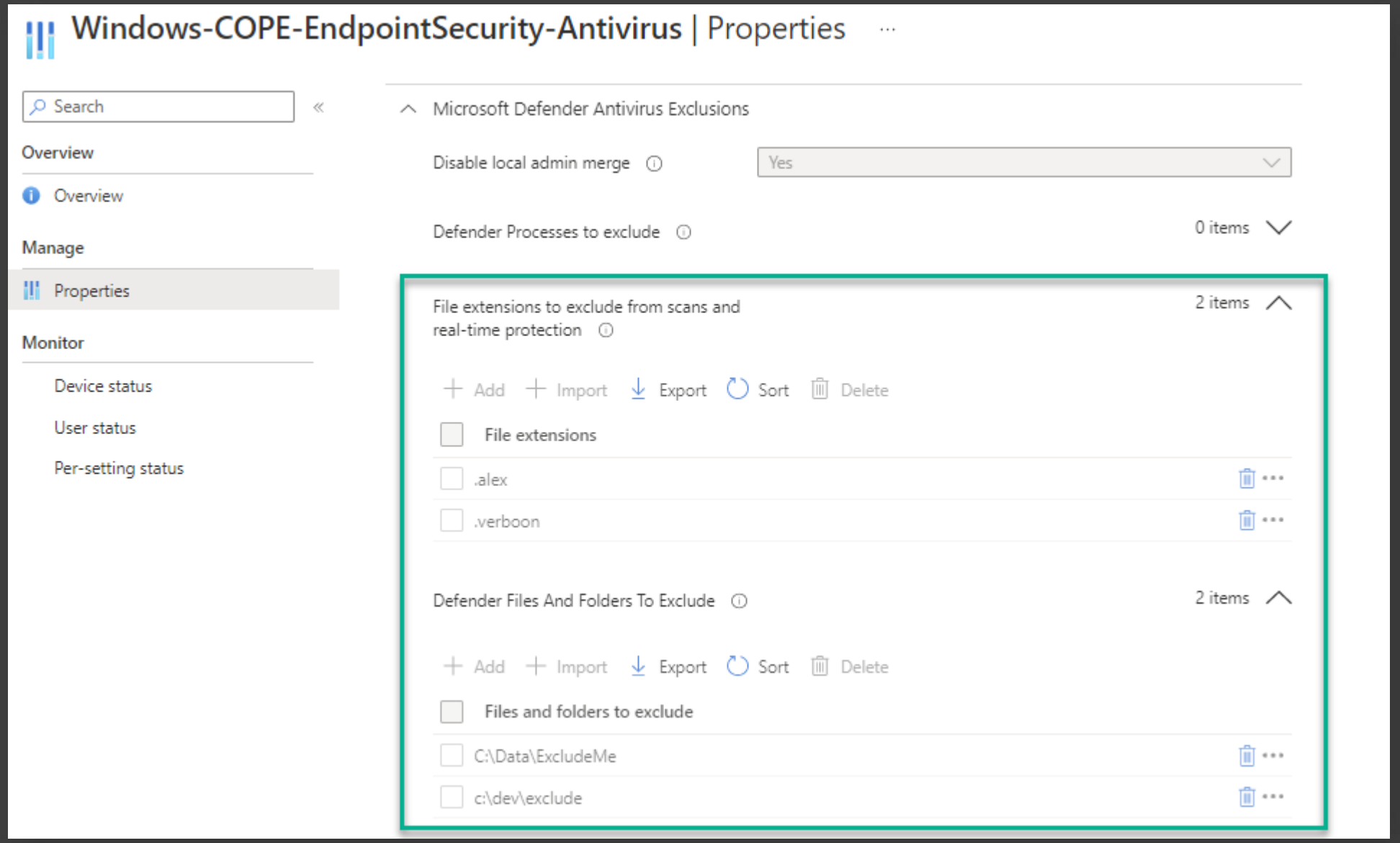
geekmania



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.

geekmania

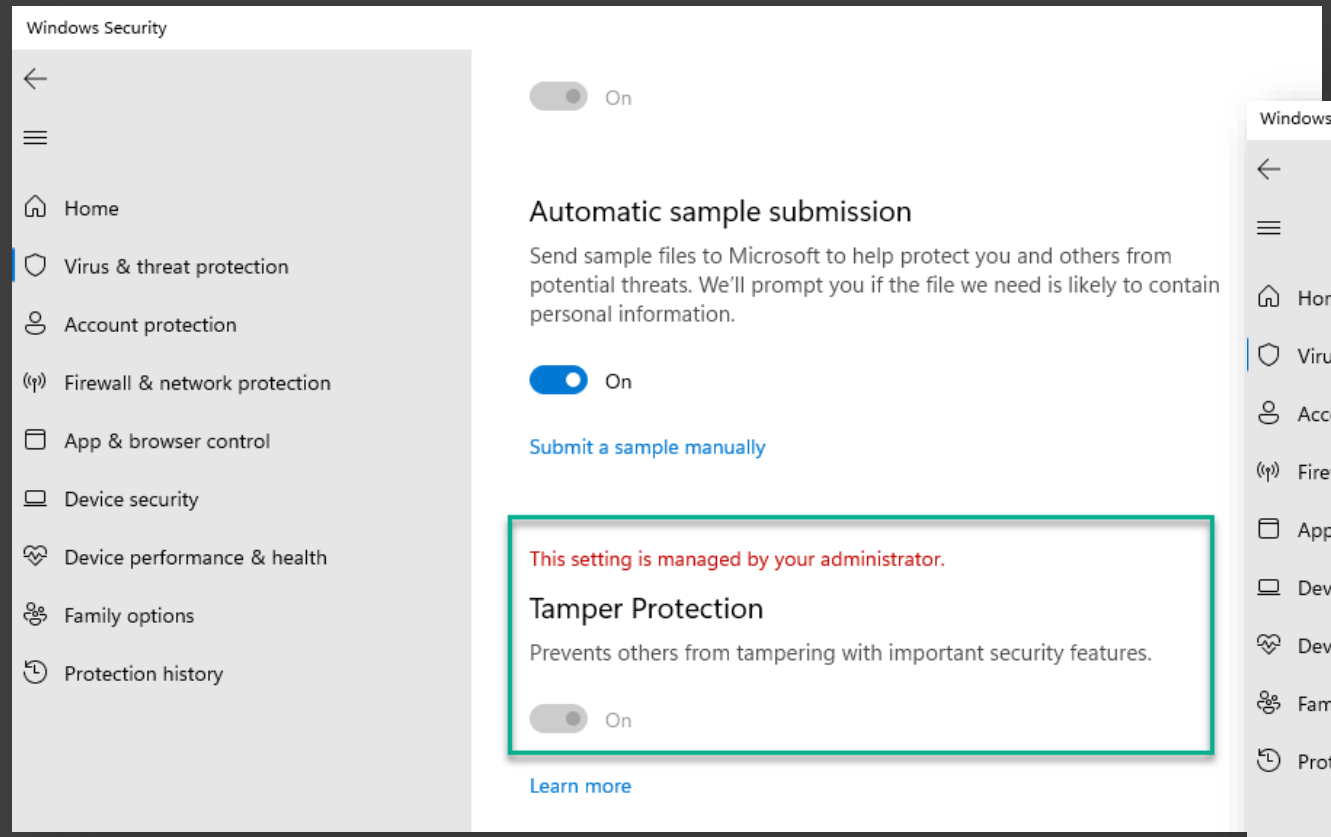


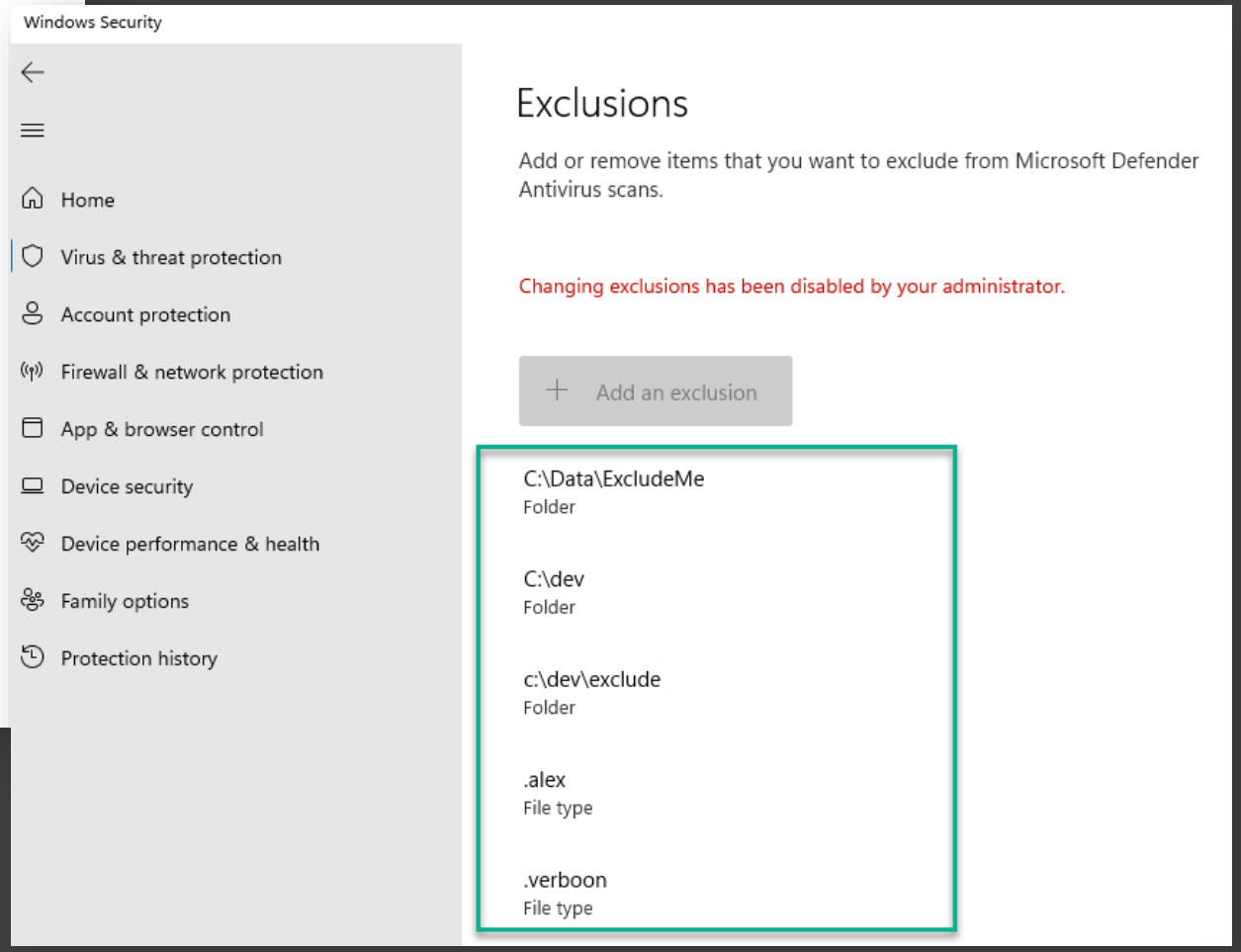
Exclusion settings

Just an example for illustration purposes

geekmania

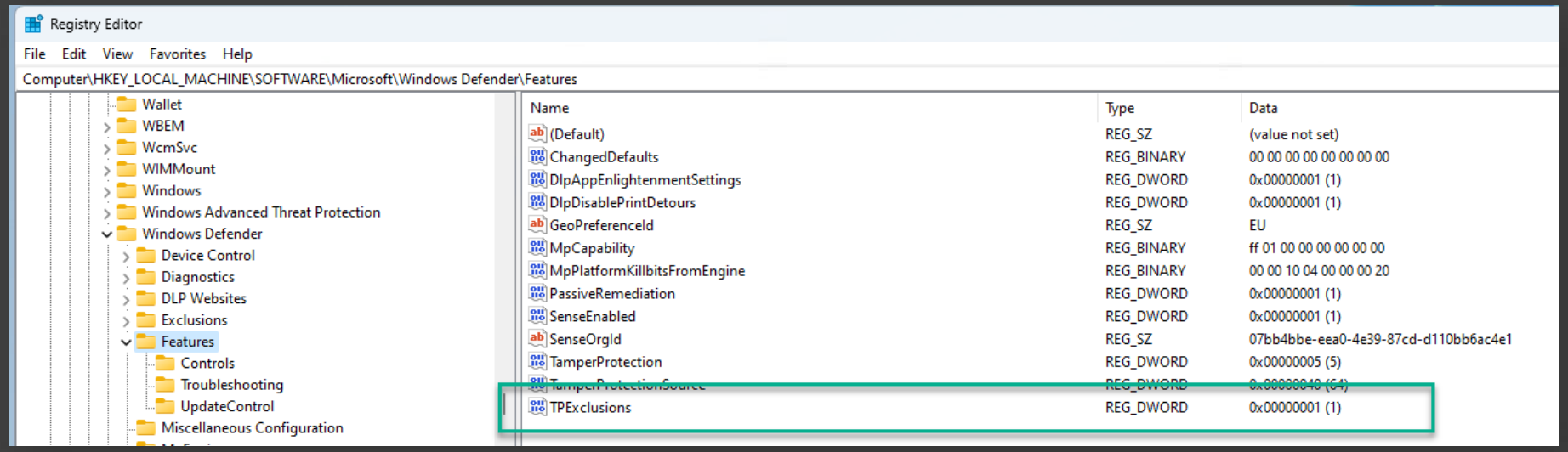
Verify Tamper Protection is enabled, and Exclusions configured within Intune are set

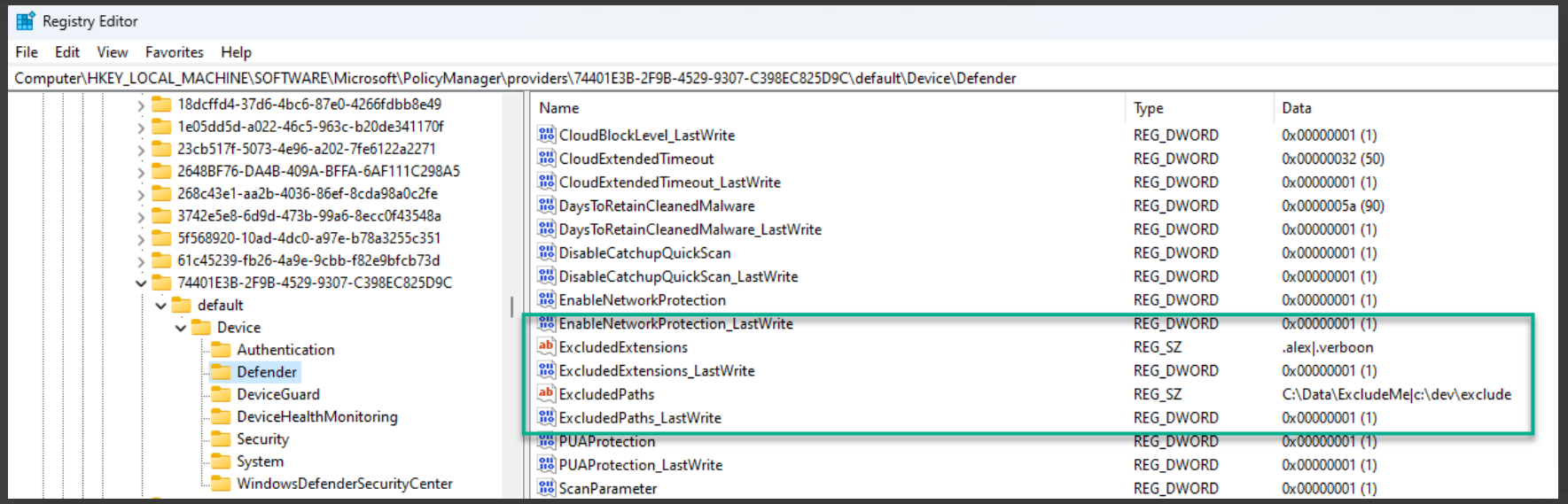




geekmania

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





geekmania

Select Administrator: Windows PowerShell

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

Event Properties - Event 5013, Windows Defender

General | Details

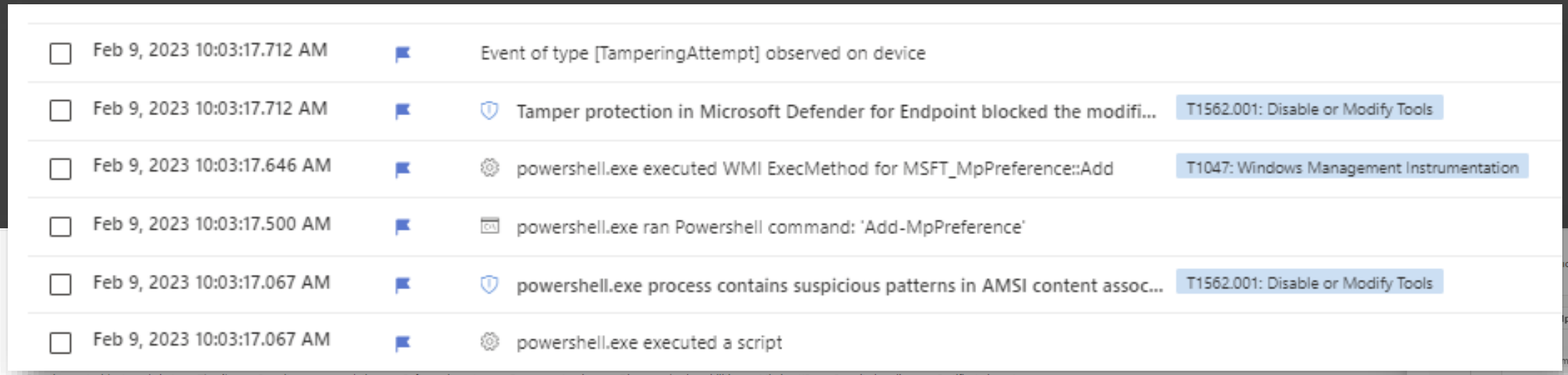
Tamper Protection Blocked a change to Microsoft Defender Antivirus.
Value: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\hackme = (Current)

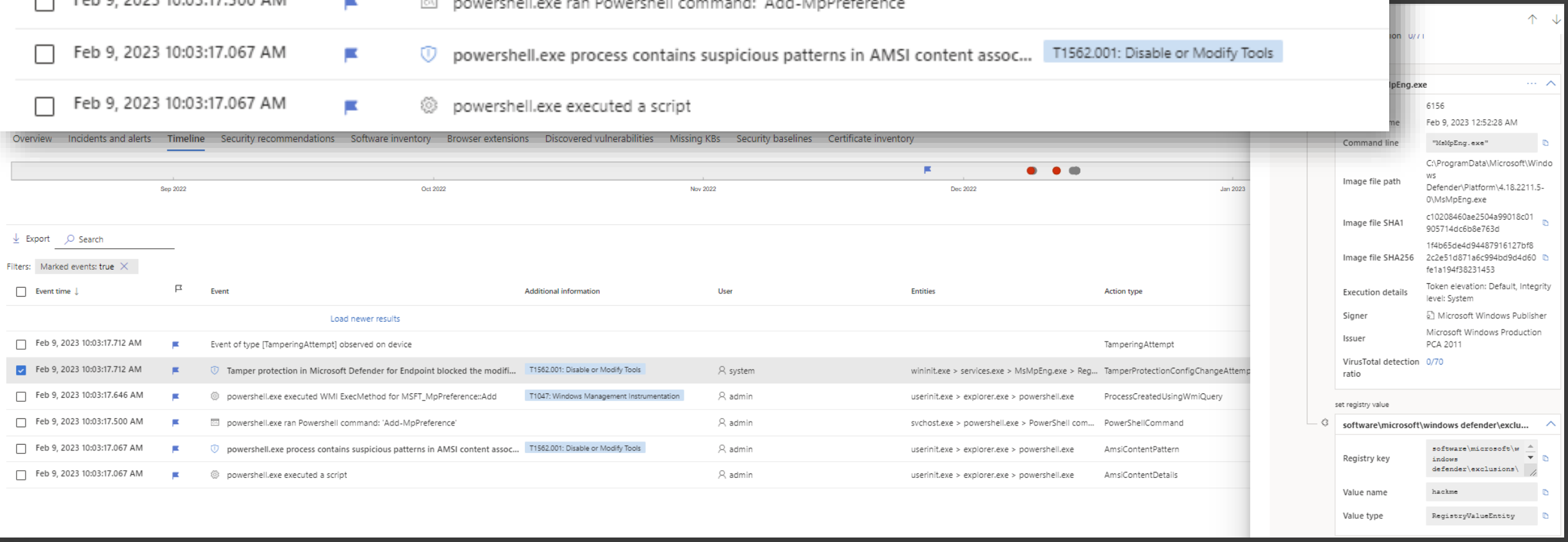
Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	2/9/2023 10:03:17 AM
Event ID:	5013	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	SecurePC01
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

geekmania

Tamper detection





geekmania

Use Advanced hunting to detect tampering attempts

Advanced hunting

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

Run query | Save | Share link

Query

```
DeviceEvents
| where ActionType == @"TamperingAttempt"
| extend AF = parse_json(AdditionalFields)
| evaluate bag_unpack(AF)
| project Timestamp, DeviceName, ActionType, Status, TamperingAction, Target, RegistryValueName, AdditionalFields
```

Getting started | Results

Export

Timestamp	DeviceName	ActionType	Status	TamperingAction	Target	RegistryValueName	AdditionalFields
Feb 9, 2023 10:03:17 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\MICROSOFT...	hackme	{"TamperingAction":"Re...
Feb 9, 2023 9:47:27 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\MICROSOFT...	tag2	{"TamperingAction":"Re...
Feb 9, 2023 9:47:23 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\MICROSOFT...	tag2	{"TamperingAction":"Re...
Feb 9, 2023 9:47:19 AM	securepc01	TamperingAttempt	Blocked	RegistryModification	SOFTWARE\MICROSOFT...	tag2	{"TamperingAction":"Re...

geekmania

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.

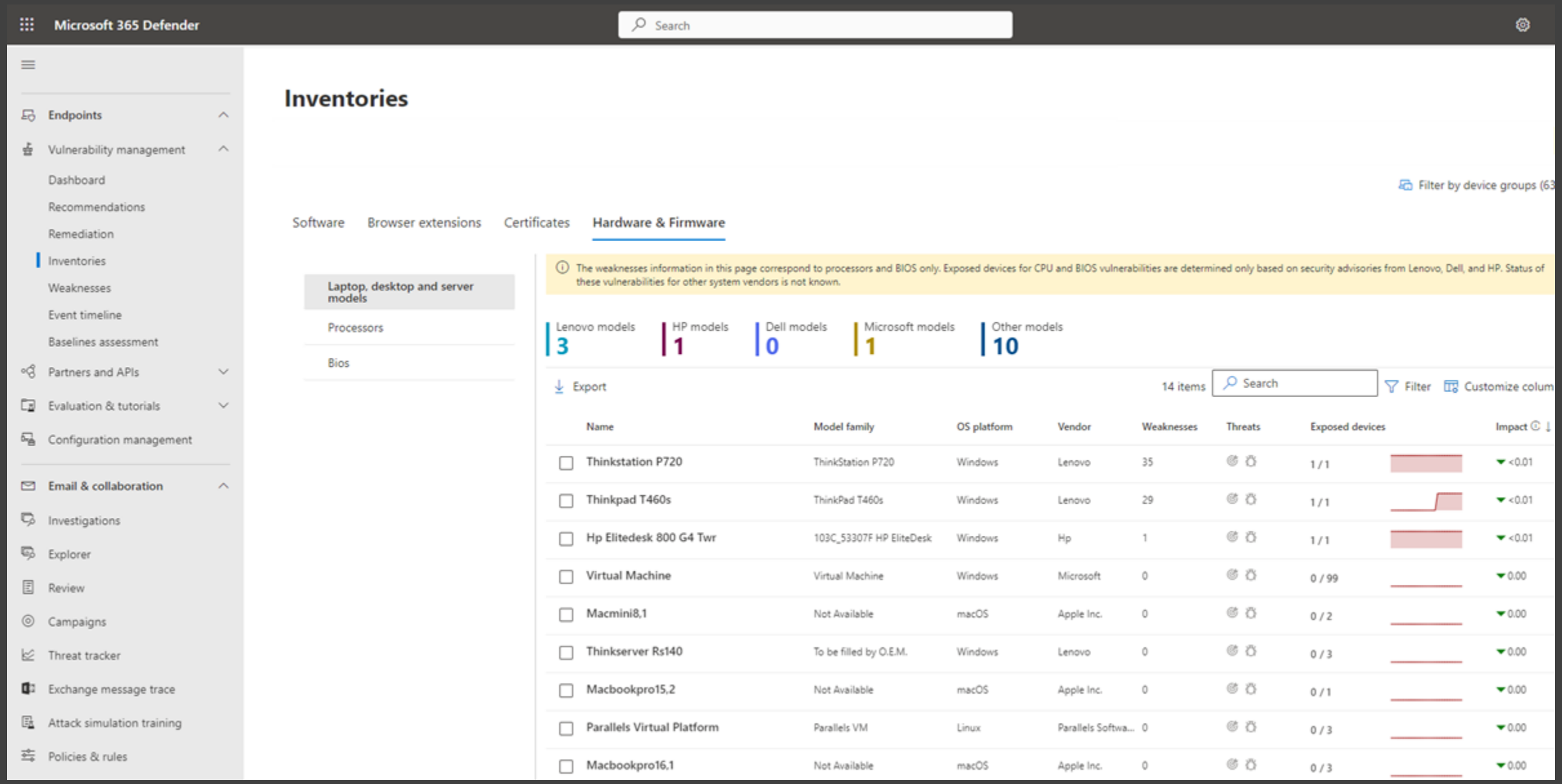
Microsoft Defender Vulnerability Management new firmware assessments feature provides customers with full visibility into device manufacturer, processor and BIOS information.

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.

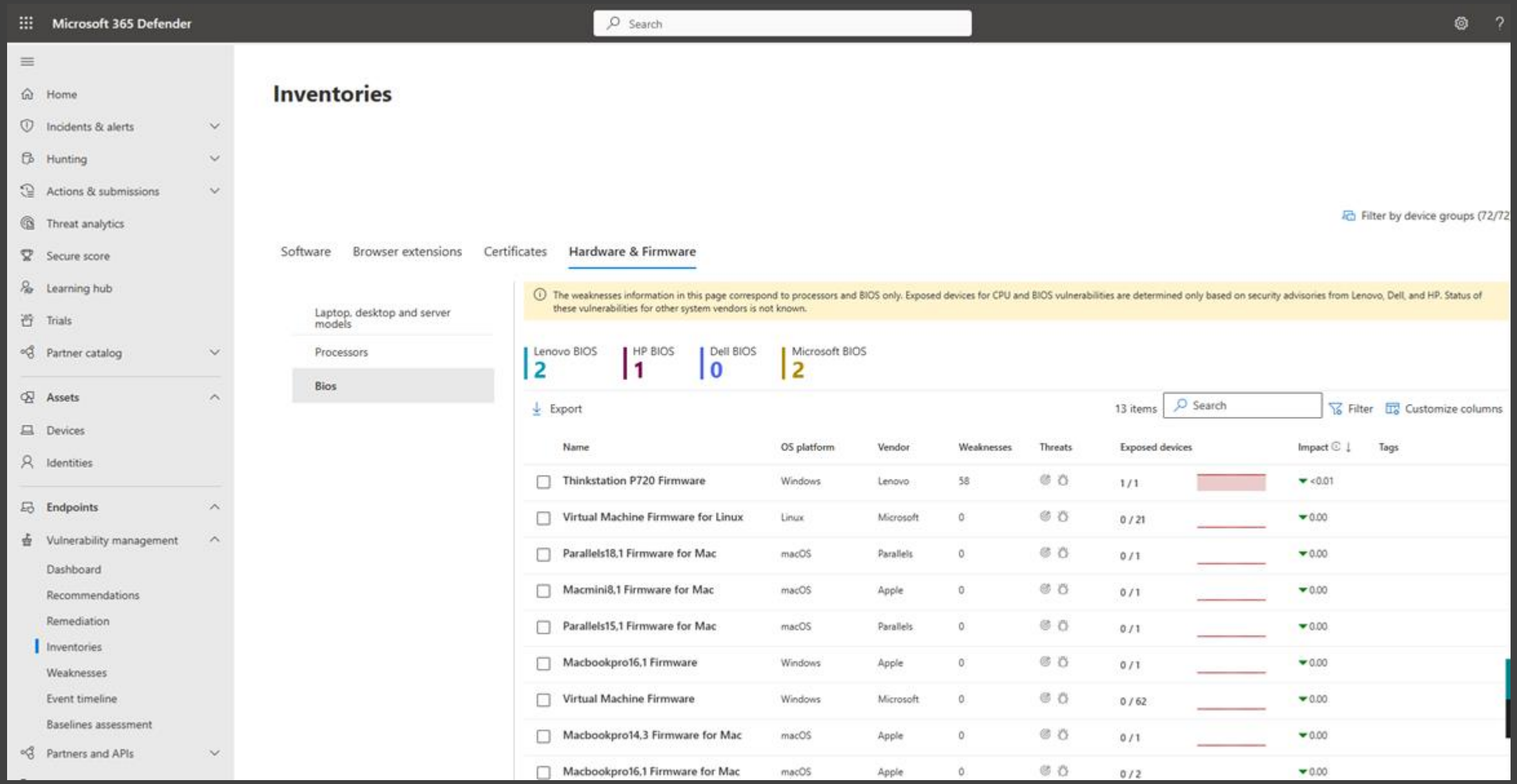
geekmania

Hardware Models



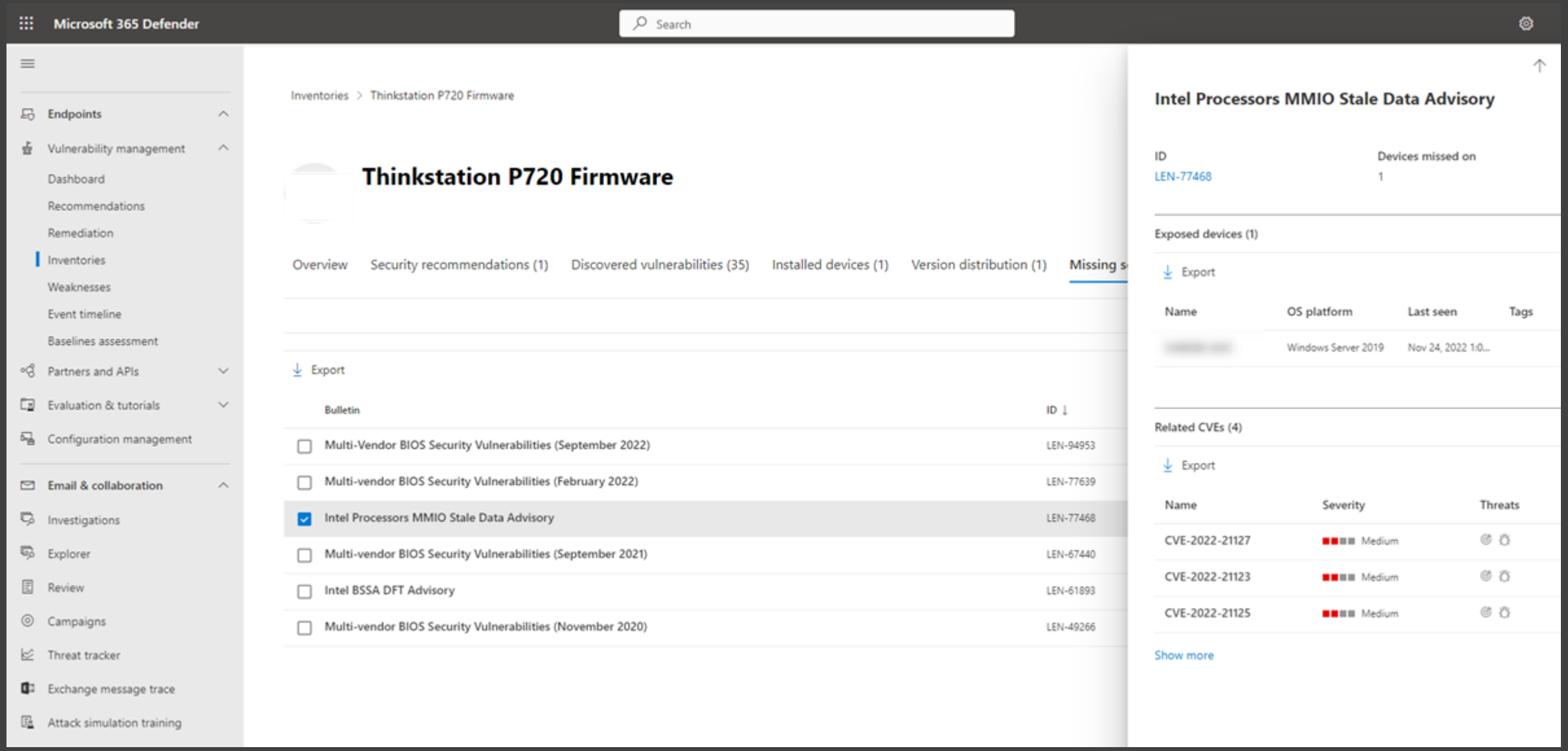
geekmania

Firmware Inventory



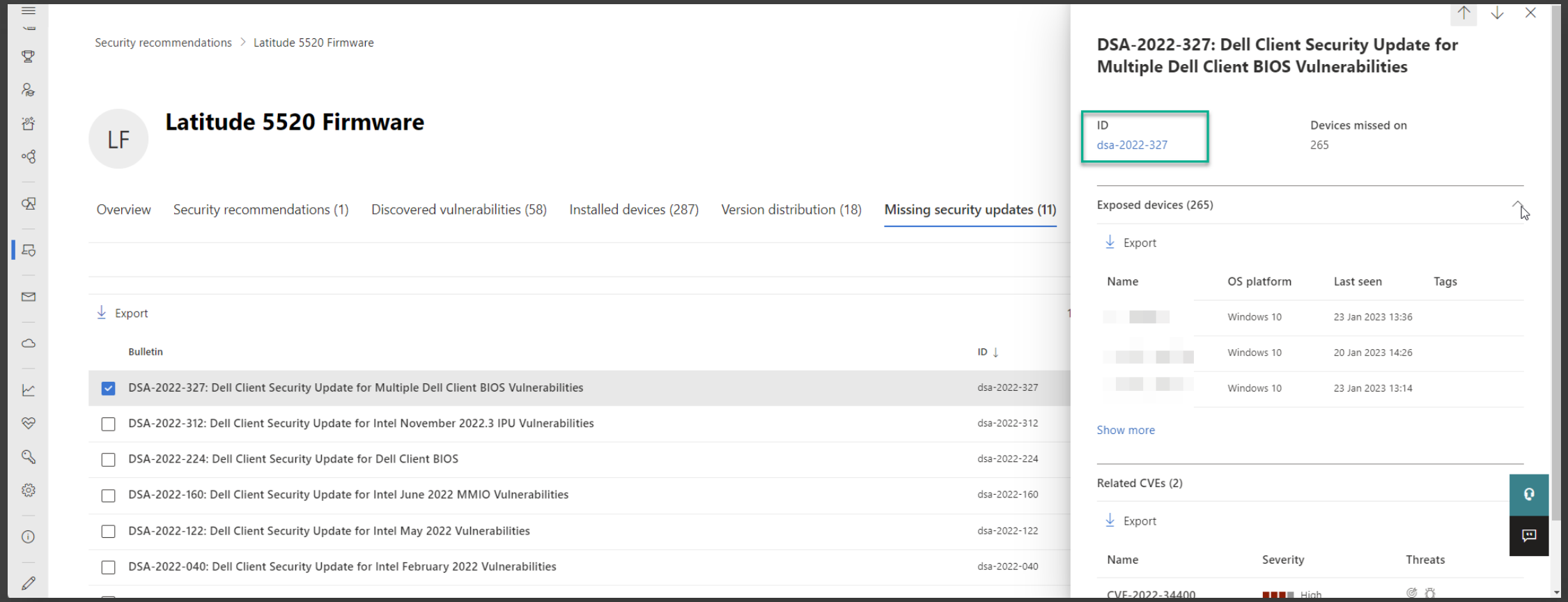
geekmania

Missing updates & Vulnerabilities



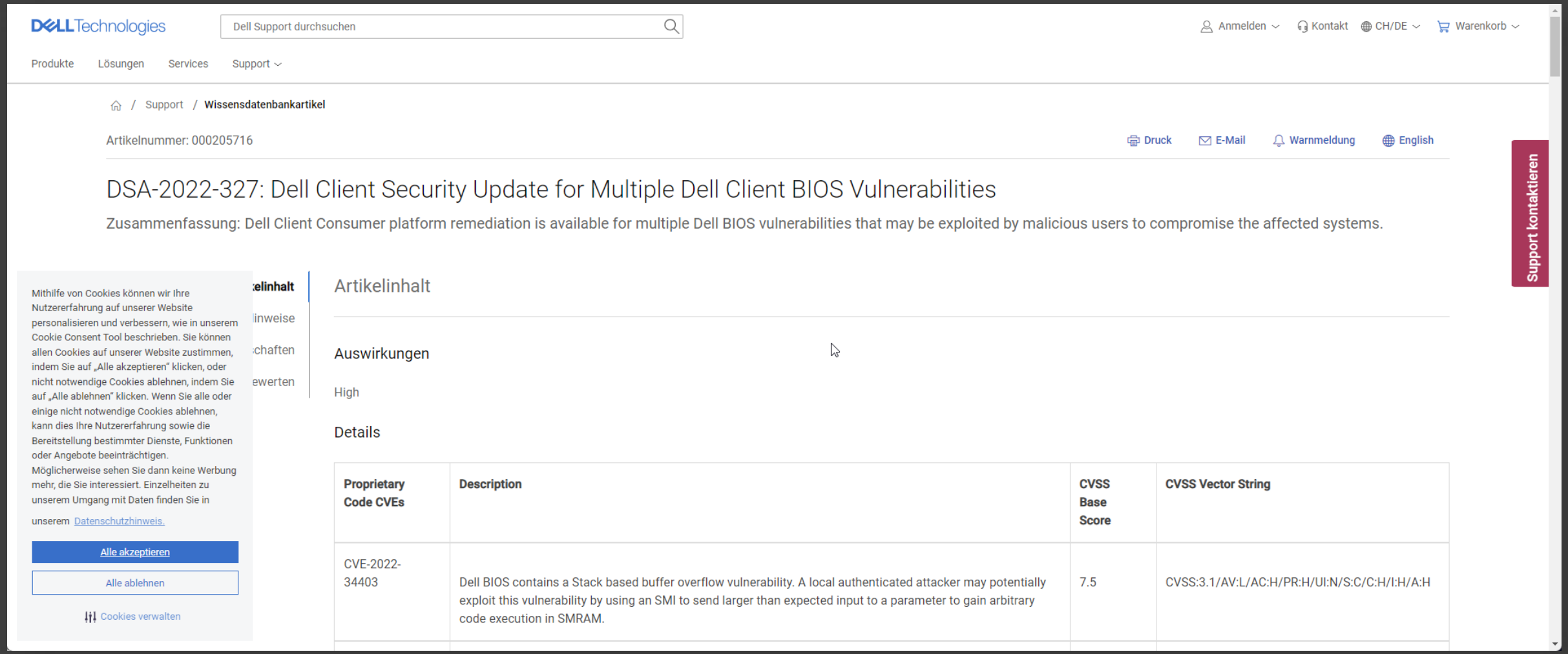
geekmania

Missing updates & Vulnerabilities

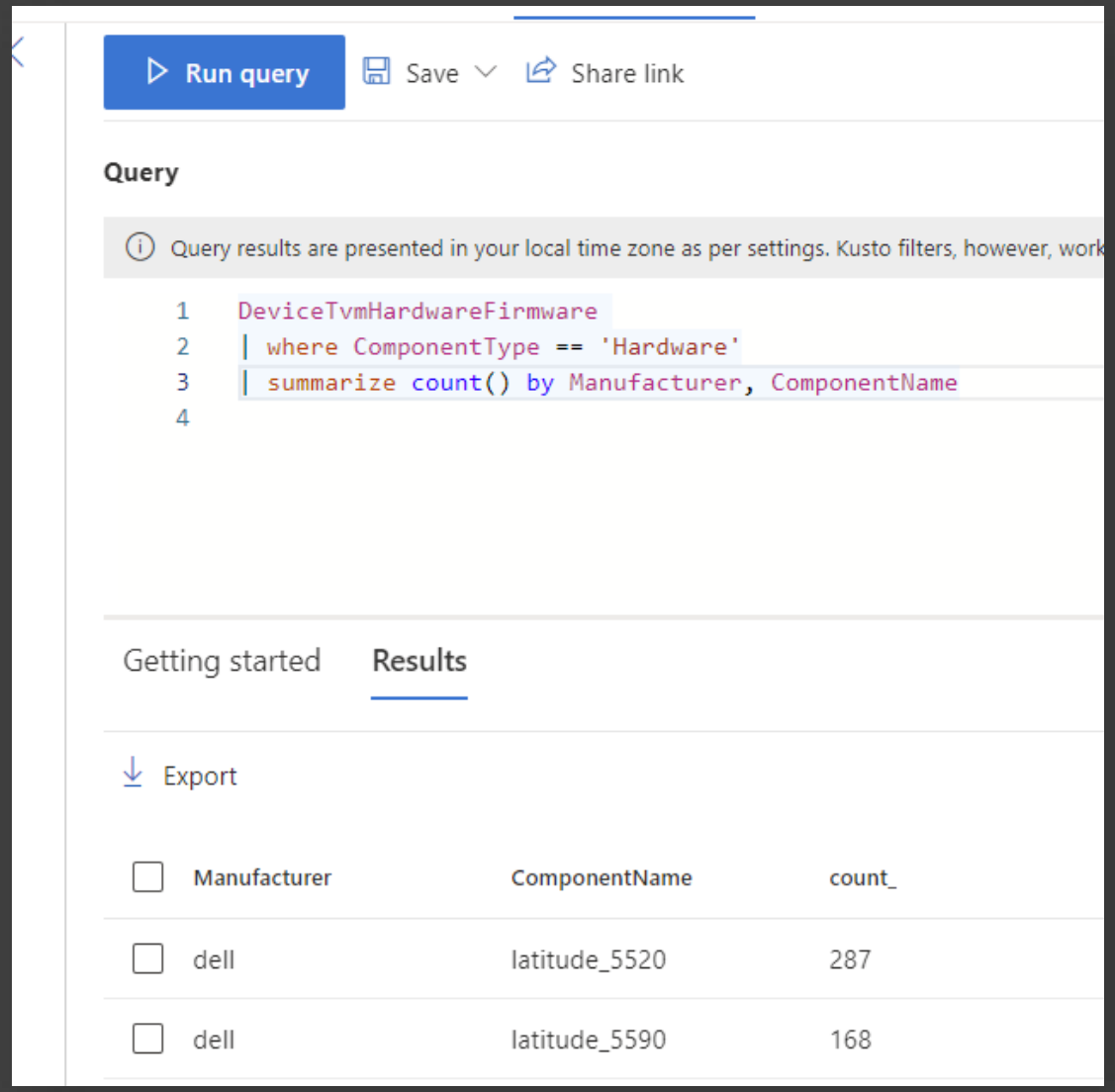


geekmania

Direct Links to Vendor support



geekmania



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

geekmania

Microsoft Defender XDR

New file analysis and pivoting capabilities

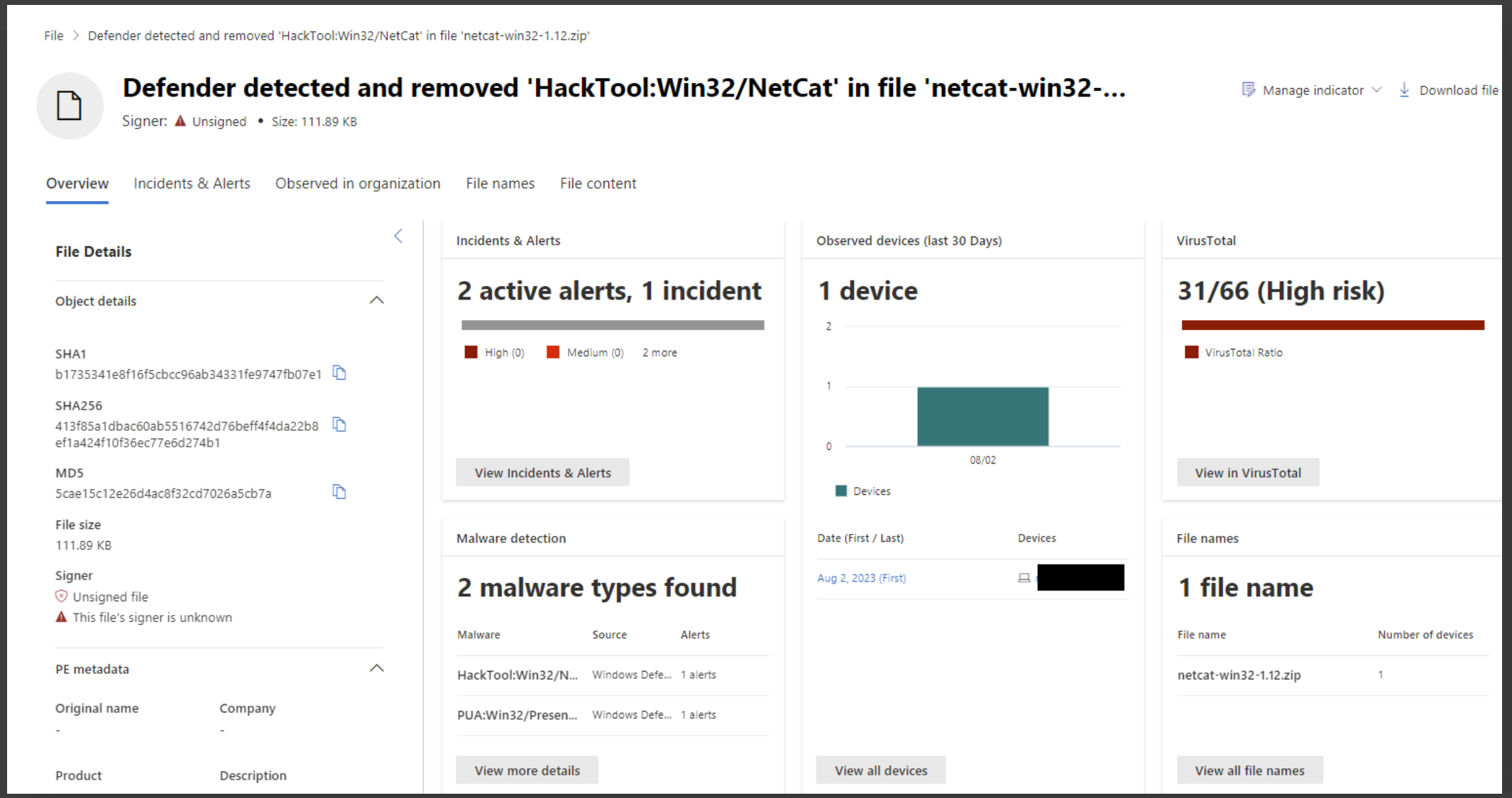
geekmania

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

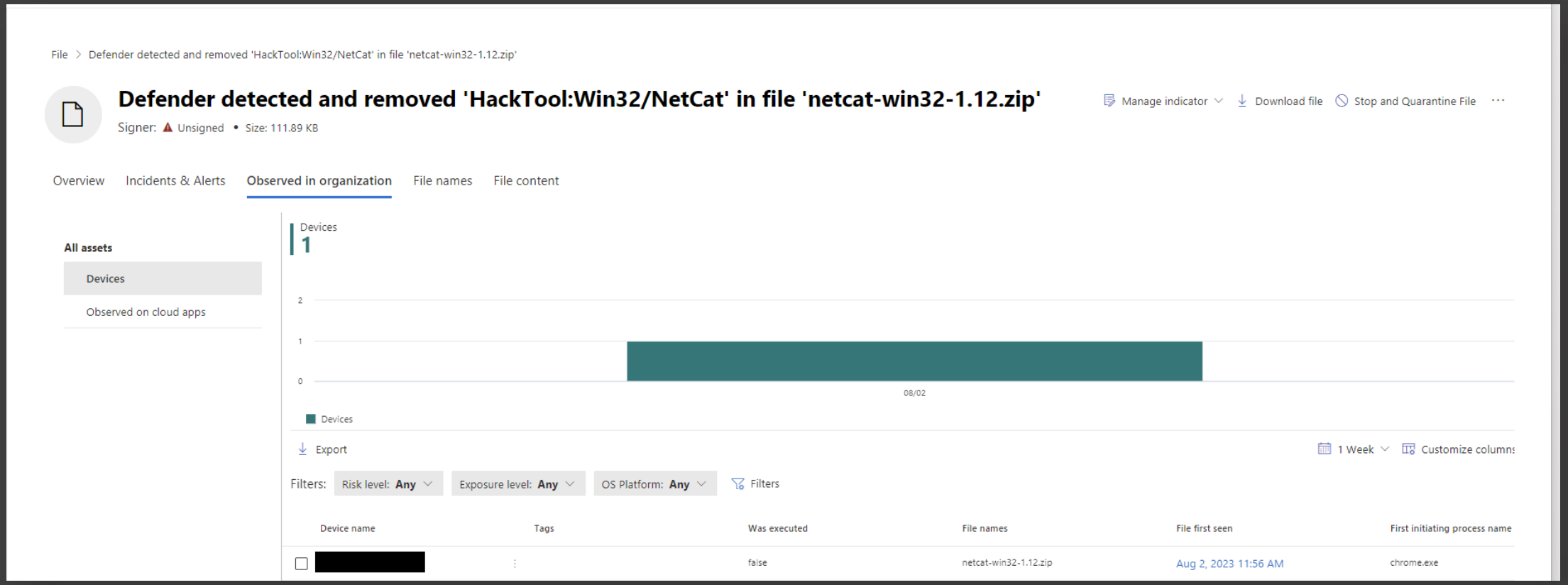
geekmania

New Interface



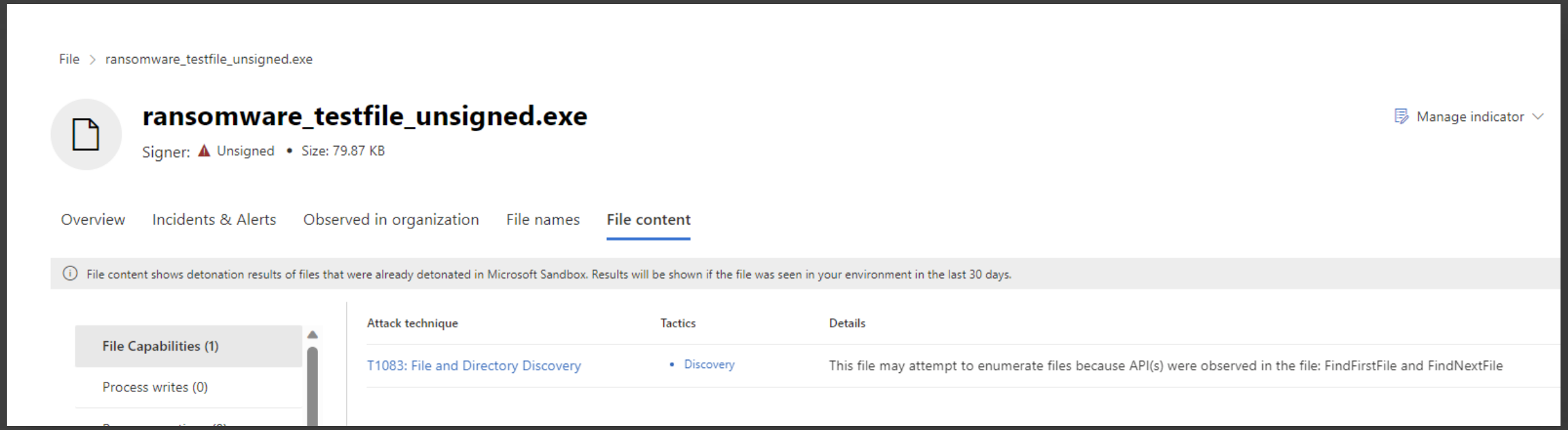
geekmania

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.



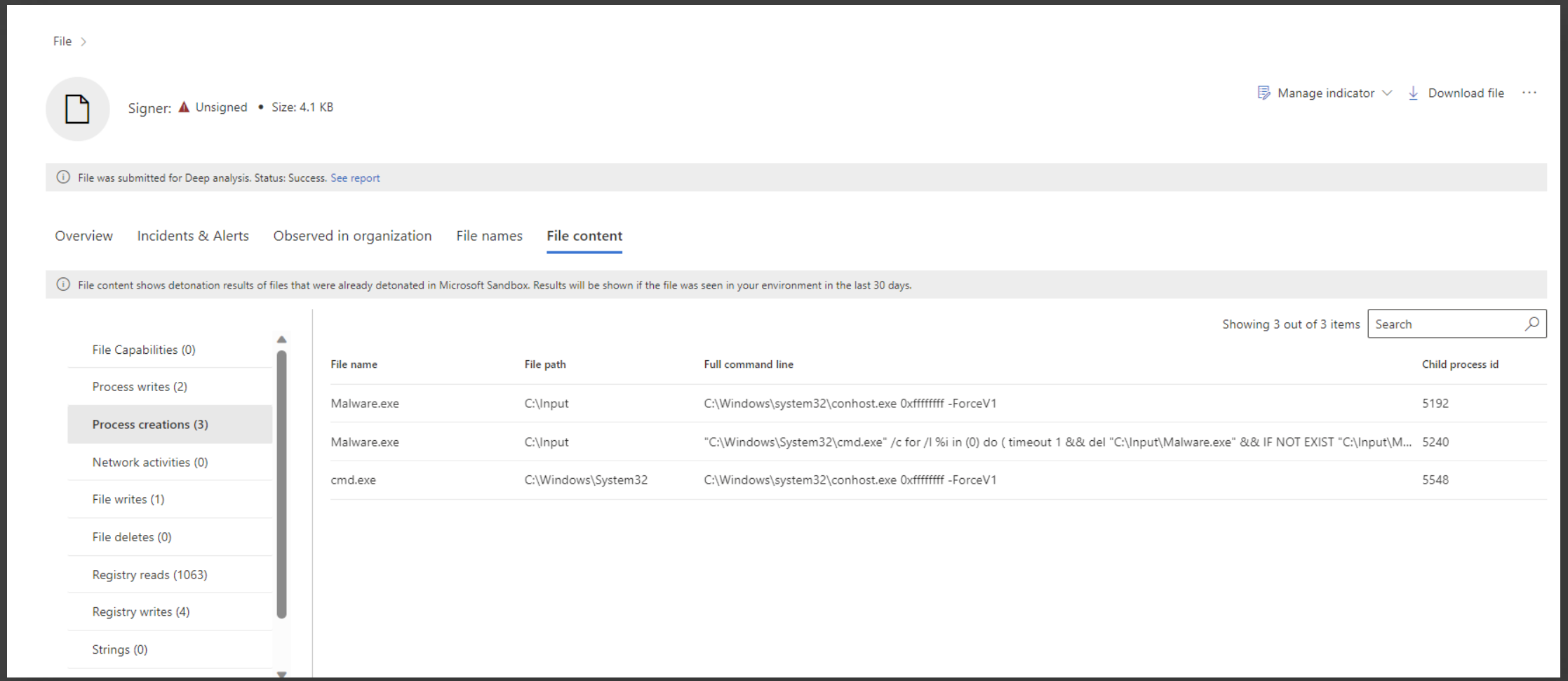
geekmania

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.



geekmania

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.



geekmania

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

C: > Temp > 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  }
19
```

Showing 3 out of 3 items Search

Process writes (2)

Process creations (3)

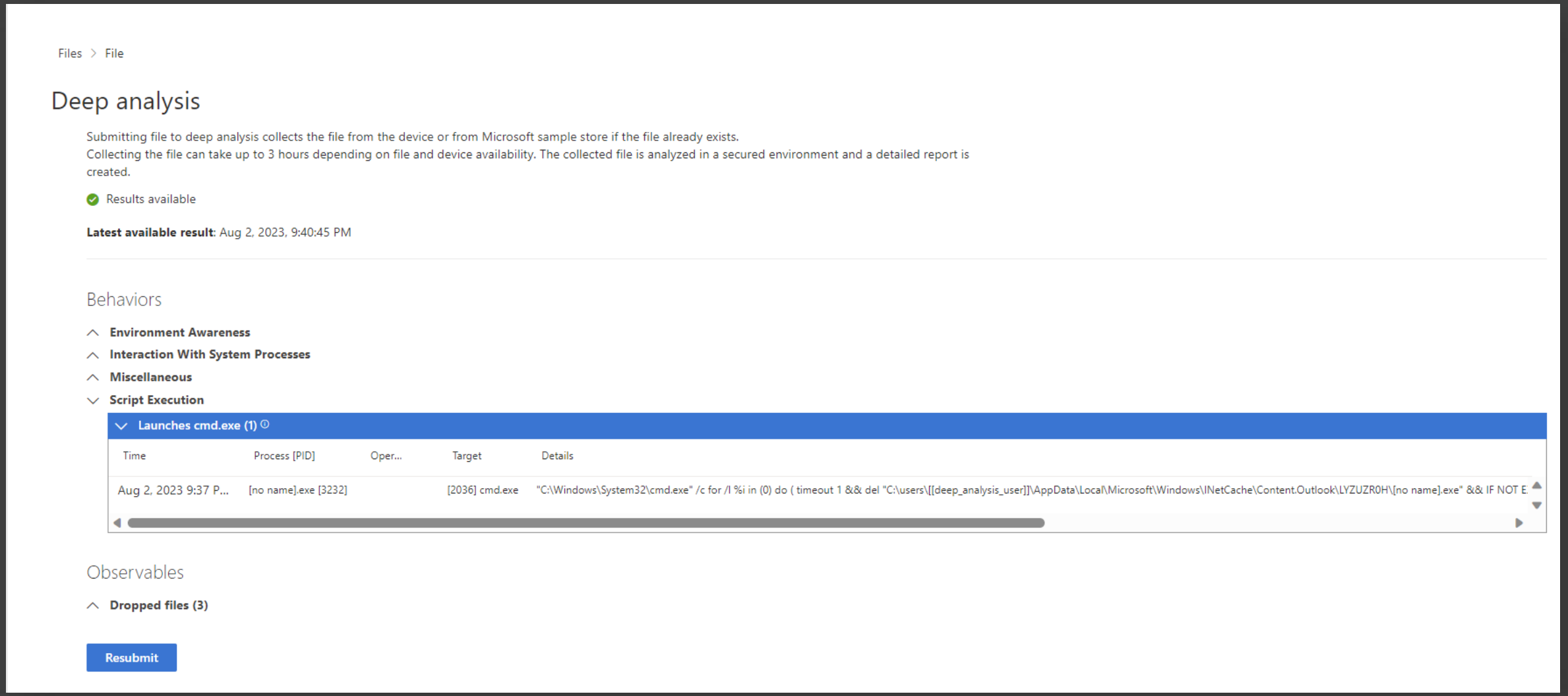
Network activities (0)

File writes (1)

			Child process
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

geekmania

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.



geekmania

Microsoft Defender XDR

RBAC

geekmania

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

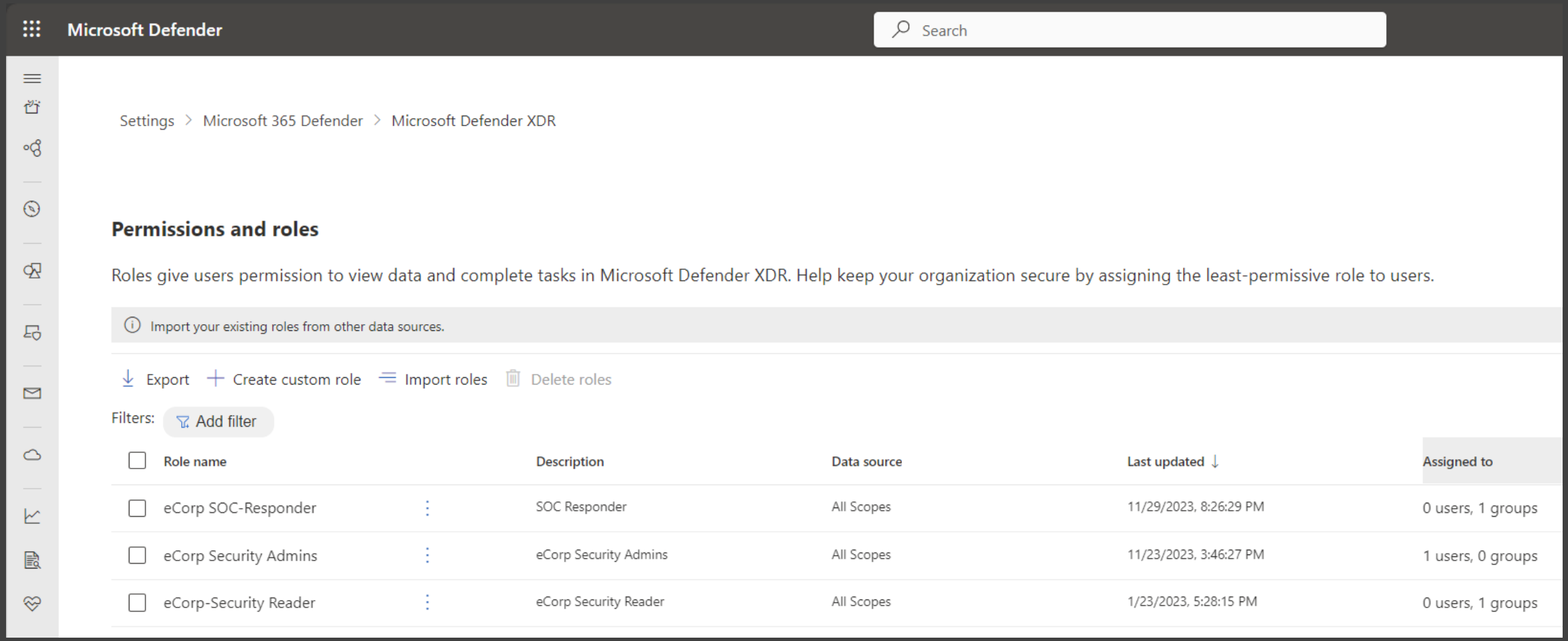
Secure Score

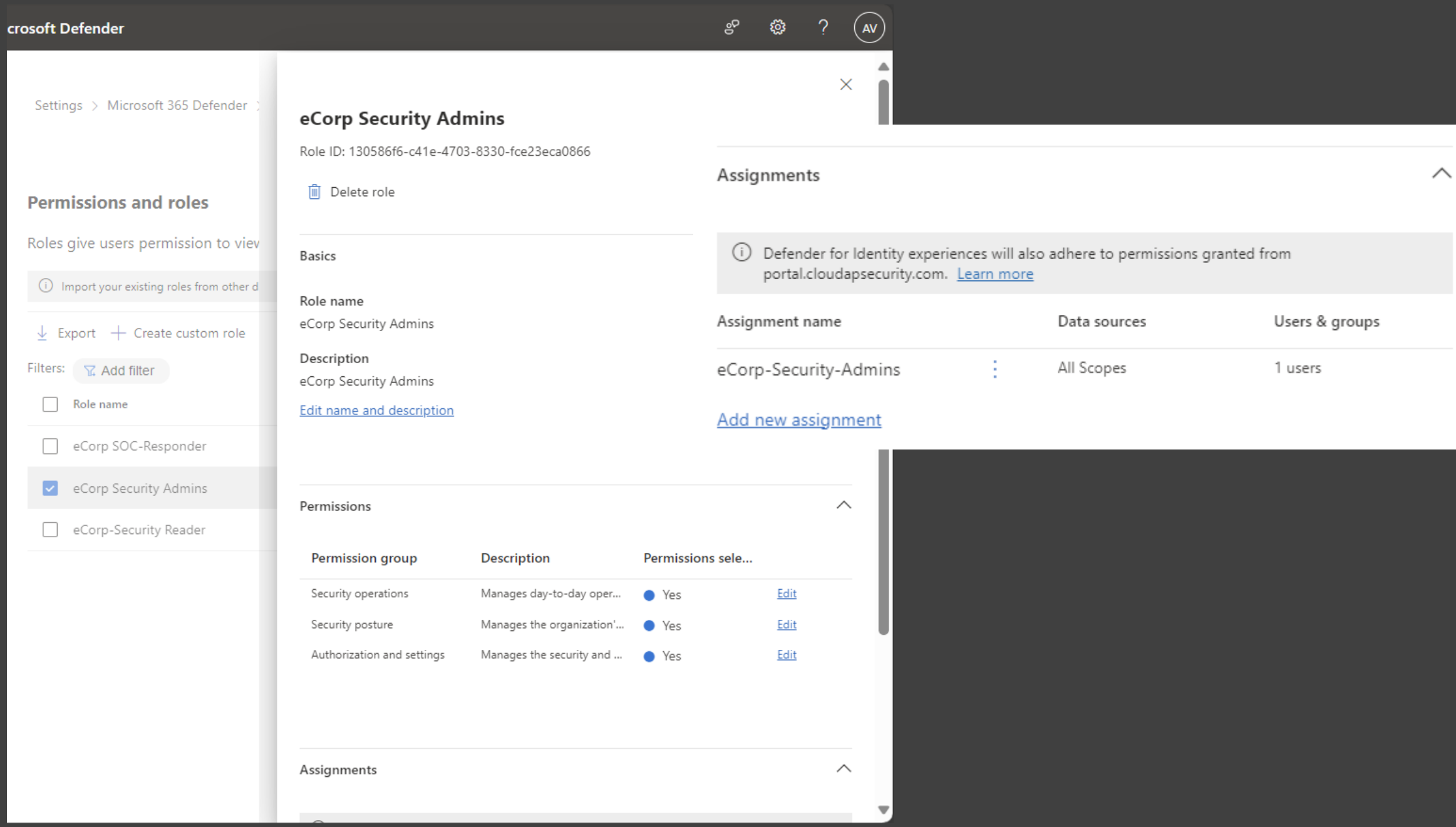
Enabling this setting will stream additional 'non-workload' sources for Secure Score. Learn more about data sources in Secure Score.

Active

Go to Permissions and roles

geekmania


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
Filters:
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


crosoft Defender
AV
Settings > Microsoft 365 Defender
Permissions and roles
Roles give users permission to viev
Import your existing roles from other d
Export
Create custom role
Filters:
Add filter
Role name
eCorp SOC-Responder
eCorp Security Admins
eCorp-Security Reader
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
Permissions
Permission group
Description
Permissions sele...
Security operations
Manages day-to-day oper...
Yes
Edit
Security posture
Manages the organization'...
Yes
Edit
Authorization and settings
Manages the security and ...
Yes
Edit
Assignments
Assignments
Defender for Identity experiences will also adhere to permissions granted from portal.cloudapsecurity.com. Learn more
Assignment name
Data sources
Users & groups
eCorp-Security-Admins
All Scopes
1 users
Add new assignment

geekmania

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)

Apply Cancel

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)

Apply Cancel

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 ⓘ

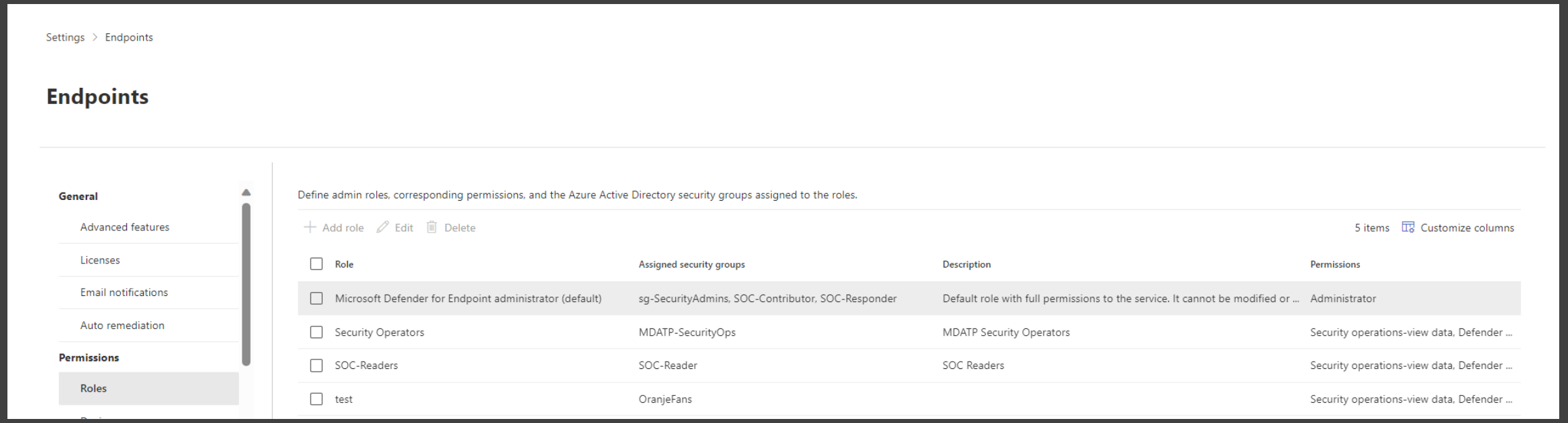
- ○ Read-only
- ○ Select all permissions
- ○ Select custom permissions
  - ☐ Detection tuning (manage)
  - ☐ Core security settings (read)
  - ☐ Core security settings (manage)

System settings ⓘ

Apply Cancel

geekmania

Tip: Don’t forget the Role permissions in MDE



geekmania