Alex Verboon

CTO – Principal Security Consultant

Cool Microsoft Security Features introduced in 2021……

That was the title planned for the November 2021 Session that was cancelled, so I let's add some from

2022

About me…

Alex Verboon
Principal Cyber Security Consultant

baseVISION

https://twitter.com/alexverboon

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

https://github.com/alexverboon

https://www.verboon.info/

Microsoft® MVP Most Valuable Professional

MVP Windows Insider MVP

GSEC

MICROSOFT PROFESSIONAL PROGRAM

Workplace Ninja User Group Switzerland

KQL|Cafe

Agenda

New features are announced , go in preview and reach GA almost every week.

Here’s the features I recommend looking at

Microsoft Defender for Endpoint

Evaluation Lab

OS Support
Request new devices
New Simulations

Contoso Electronics | Microsoft 365 Defender | Search

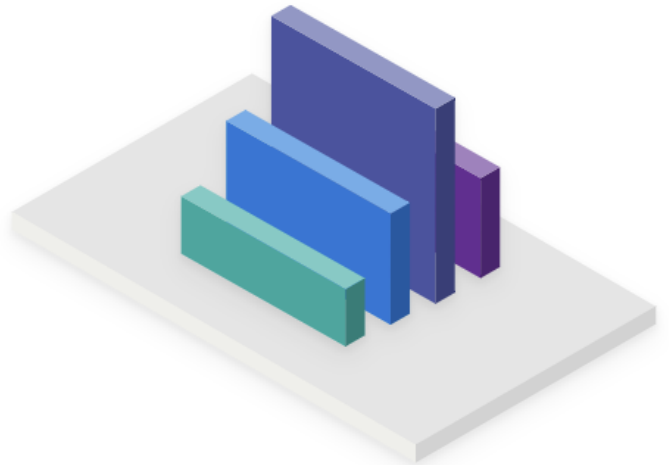
- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Secure score
- Learning hub
- Trials
- Endpoints
  - Device inventory
  - Vulnerability management
  - Partners and APIs
  - Evaluation & tutorials
    - Evaluation lab
    - Tutorials & simulations

Welcome to the Microsoft Defender for Endpoint Evaluation lab

Learn about the Microsoft Defender for Endpoint platform capabilities through a virtual evaluation lab that's ready to go, complete with onboarded test devices. See it in action as it detects and prevents the most sophisticated attacks.

Learn more

Setup lab



Lab configuration

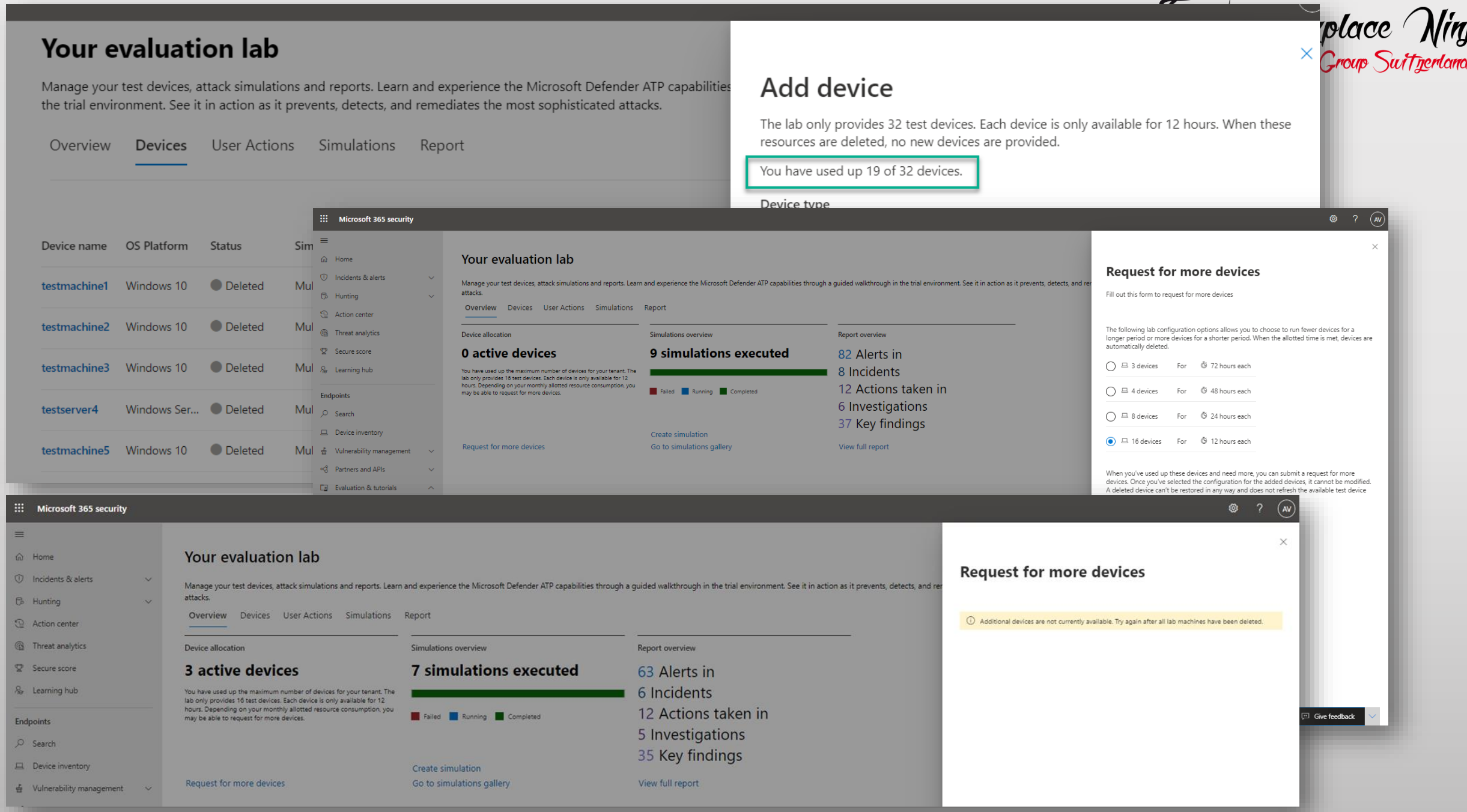
- Select your lab configuration
- Install simulators agent
- Summary

Select your lab configuration

Please note, first set up can not be edited. Learn more

The following lab configuration options allows you to choose to run fewer devices for a longer period or more devices for a shorter period. When the allotted time is met, devices are automatically deleted.

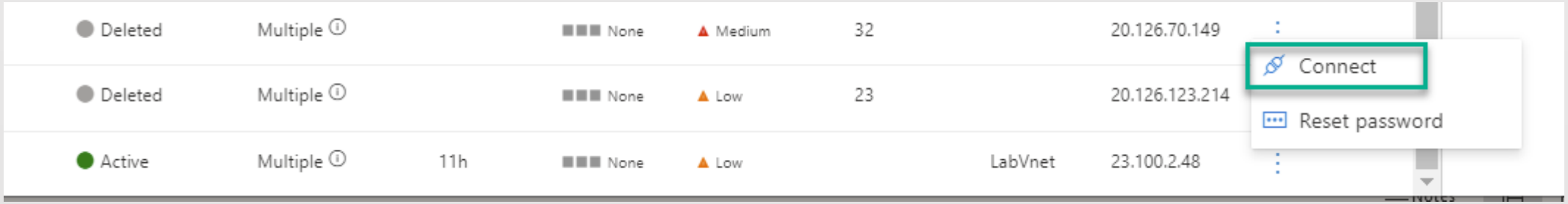
○	3 devices	For	72 hours each
○	4 devices	For	48 hours each
◉	8 devices	For	24 hours each
○	16 devices	For	12 hours each

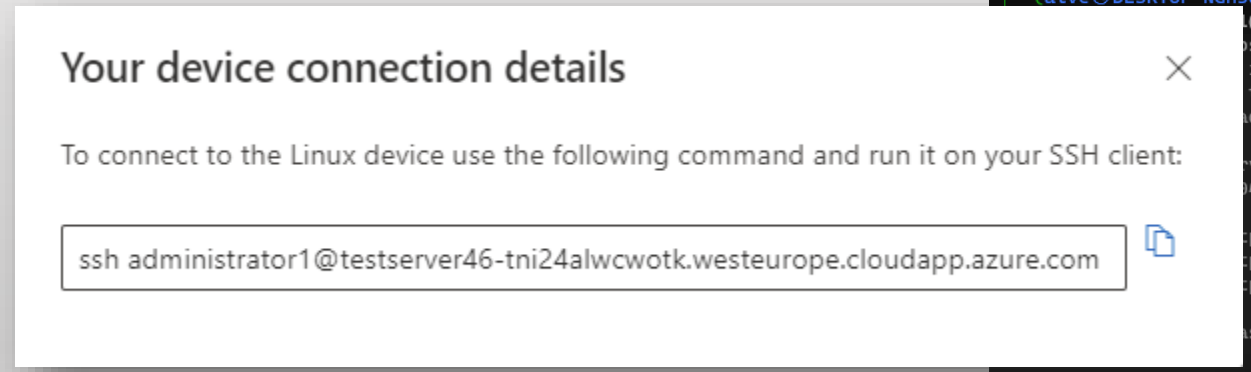

Your evaluation lab
Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities
the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.
Overview
Devices
User Actions
Simulations
Report
Device name
OS Platform
Status
testmachine1
Windows 10
Deleted
testmachine2
Windows 10
Deleted
testmachine3
Windows 10
Deleted
testserver4
Windows Ser...
Deleted
testmachine5
Windows 10
Deleted
Add device
The lab only provides 32 test devices. Each device is only available for 12 hours. When these resources are deleted, no new devices are provided.
You have used up 19 of 32 devices.
Device type
Microsoft 365 security
Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub
Endpoints
Search
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Your evaluation lab
Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and
attacks.
Overview
Devices
User Actions
Simulations
Report
Device allocation
0 active devices
You have used up the maximum number of devices for your tenant. The lab only provides 16 test devices. Each device is only available for 12 hours. Depending on your monthly allotted resource consumption, you may be able to request for more devices.
Request for more devices
Simulations overview
9 simulations executed
Failed
Running
Completed
Create simulation
Go to simulations gallery
Report overview
82 Alerts in
8 Incidents
12 Actions taken in
6 Investigations
37 Key findings
View full report
Request for more devices
Fill out this form to request for more devices
The following lab configuration options allows you to choose to run fewer devices for a longer period or more devices for a shorter period. When the allotted time is met, devices are automatically deleted.
3 devices For 72 hours each
4 devices For 48 hours each
8 devices For 24 hours each
16 devices For 12 hours each
When you've used up these devices and need more, you can submit a request for more devices. Once you've selected the configuration for the added devices, it cannot be modified. A deleted device can't be restored in any way and does not refresh the available test device
Microsoft 365 security
Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub
Endpoints
Search
Device inventory
Vulnerability management
Your evaluation lab
Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender ATP capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and re
attacks.
Overview
Devices
User Actions
Simulations
Report
Device allocation
3 active devices
You have used up the maximum number of devices for your tenant. The lab only provides 16 test devices. Each device is only available for 12 hours. Depending on your monthly allotted resource consumption, you may be able to request for more devices.
Request for more devices
Simulations overview
7 simulations executed
Failed
Running
Completed
Create simulation
Go to simulations gallery
Report overview
63 Alerts in
6 Incidents
12 Actions taken in
5 Investigations
35 Key findings
View full report
Request for more devices
Additional devices are not currently available. Try again after all lab machines have been deleted.
Give feedback

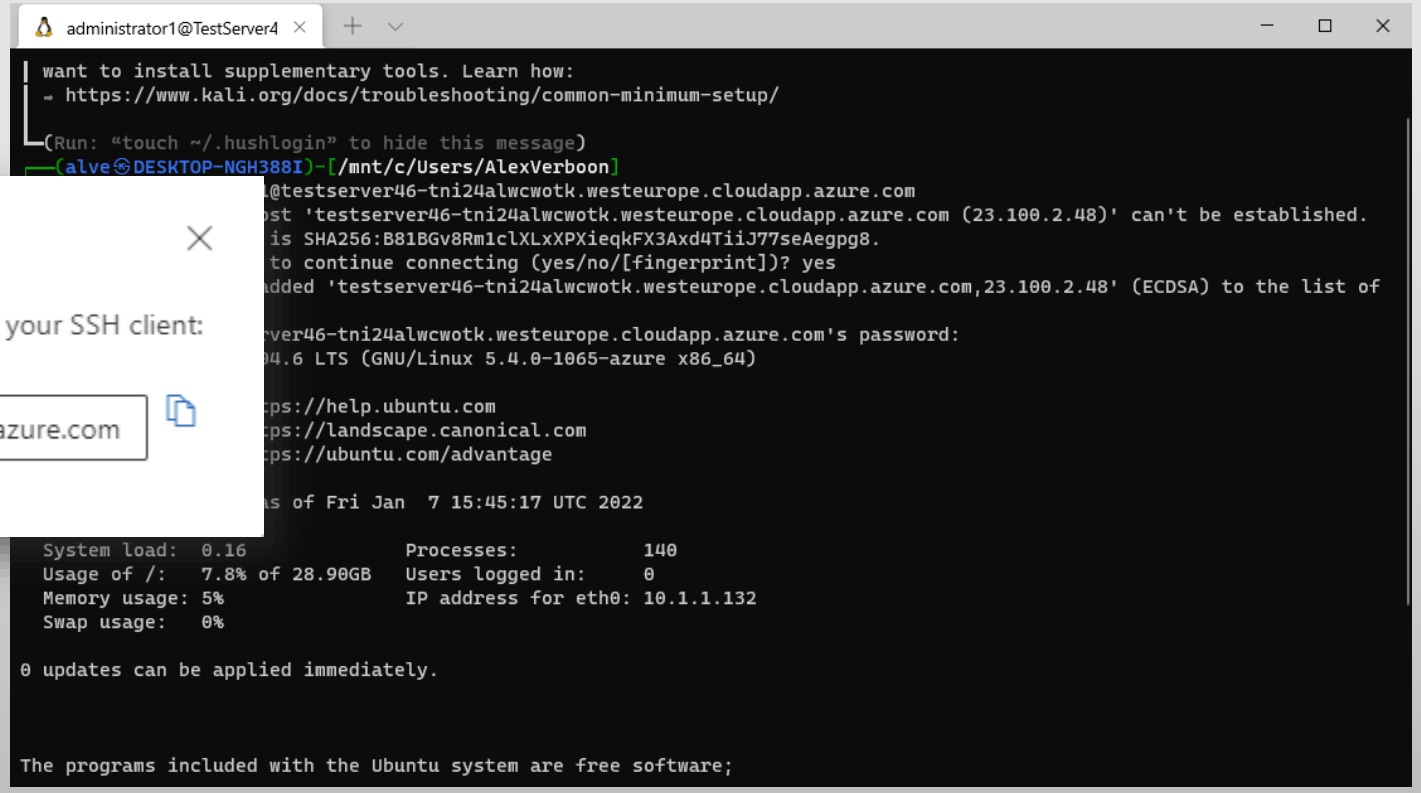
The evaluation lab now supports the following operating systems:

- Windows 10
- Windows 11 (new)
- Windows Server 2019
- Windows Server 2016
- Linux (Ubuntu (new)

Connecting to Ubuntu







New Simulations 1

SolarWinds Campaign simulates attacks for SolarWinds® Orion® Platform software that was compromised with a malware known as SUNBURST. This includes static and behavioral simulations for malware samples and activity.

Initial Access – SUNBURST malware

Initial Access – TEARDROP malware

Initial Access – SUPERNOVA malware

Command and Control – Communication with SUNBURST server

Persistence – WMI event subscription

Collection – Windows system data collection using CMD

New Simulations 2

Carbanak & FIN7 simulates attacks for local host infection and malicious behaviour, performed by Carbanak and FIN7 threat groups. This includes techniques such as malware infection, data collection, and modification of OS configurations.

Initial Access – CARBANAK malware

Defense Evasion – Firewall rule creation using netsh.exe

Defense Evasion – Process hollowing

Defense Evasion – Microsoft Defender Antivirus exclusion creation

Defense Evasion – File masquerading

Discovery – Remote systems discovery

Execution – Code execution using Mshta

Persistence – Scheduled task creation

Defender for Endpoint

Unified Solution for Server 2012-R2 and Server 2016

Server Onboarding

Step 1:
Download package

Windows Server 2012 R2
Windows Server 2016

- Installation package
- Onboarding package

Windows Server 1803
Windows Server 2019

- Onboarding package

Step 2:
Use installation & onboarding tools

- Local script
- Group policy
- Microsoft Configuration Manager
- VDI scripts
- Azure Defender

Supported capabilities for Windows devices

Operating System	Windows 10 & 11	Windows Server 2012 R2 [1]	Windows Server 2016[1]	Windows Server 2019 & 2022	Windows Server 1803+
Prevention					
Attack Surface Reduction rules	Y	Y	Y	Y	Y
Device Control	Y	N	N	N	N
Firewall	Y	Y	Y	Y	Y
Network Protection	Y	Y	Y	Y	Y
Next-generation protection	Y	Y	Y	Y	Y
Tamper Protection	Y	Y	Y	Y	Y
Web Protection	Y	Y	Y	Y	Y

Detection					
Advanced Hunting	Y	Y	Y	Y	Y
Custom file indicators	Y	Y	Y	Y	Y
Custom network indicators	Y	Y	Y	Y	Y
EDR Block & Passive Mode	Y	Y	Y	Y	Y
Sense detection sensor	Y	Y	Y	Y	Y
Endpoint & network device discovery	Y	N	N	N	N

Response					
Automated Investigation & Response (AIR)	Y	Y	Y	Y	Y
Device response capabilities: isolation, collect investigation package, run AV scan	Y	Y	Y	Y	Y
File response capabilities: collect file, deep analysis, block file, stop, and quarantine processes	Y	Y	Y	Y	Y
Live Response	Y	Y	Y	Y	Y

Server version	AV	EDR
Windows Server 2012 R2 SP1	✓	✓
Windows Server 2016	Built-in	✓
Windows Server 2019 or later	Built-in	Built-in

Select operating system to start onboarding process:

Windows 10 and 11

- Windows 7 SP1 and 8.1
- Windows 10 and 11
- Windows Server 2008 R2 SP1, 2012 R2 and 2016 (using Microsoft Monitoring Agent)
- Windows Server 2012 R2 and 2016 (Preview)
- Windows Server 1803, 2019 and 2022
- macOS
- Linux Server
- iOS
- Android

age that matches your prefe

eploy at scale, please see oth
ices, see Configure devices u

section in the Microsoft Defender for Endpoint guide.

Download onboarding package

Add update for EDR Sensor to MEMCM/ WSUS

Microsoft Defender for Endpoint update for EDR Sensor

KB5005292

Upgrade Script

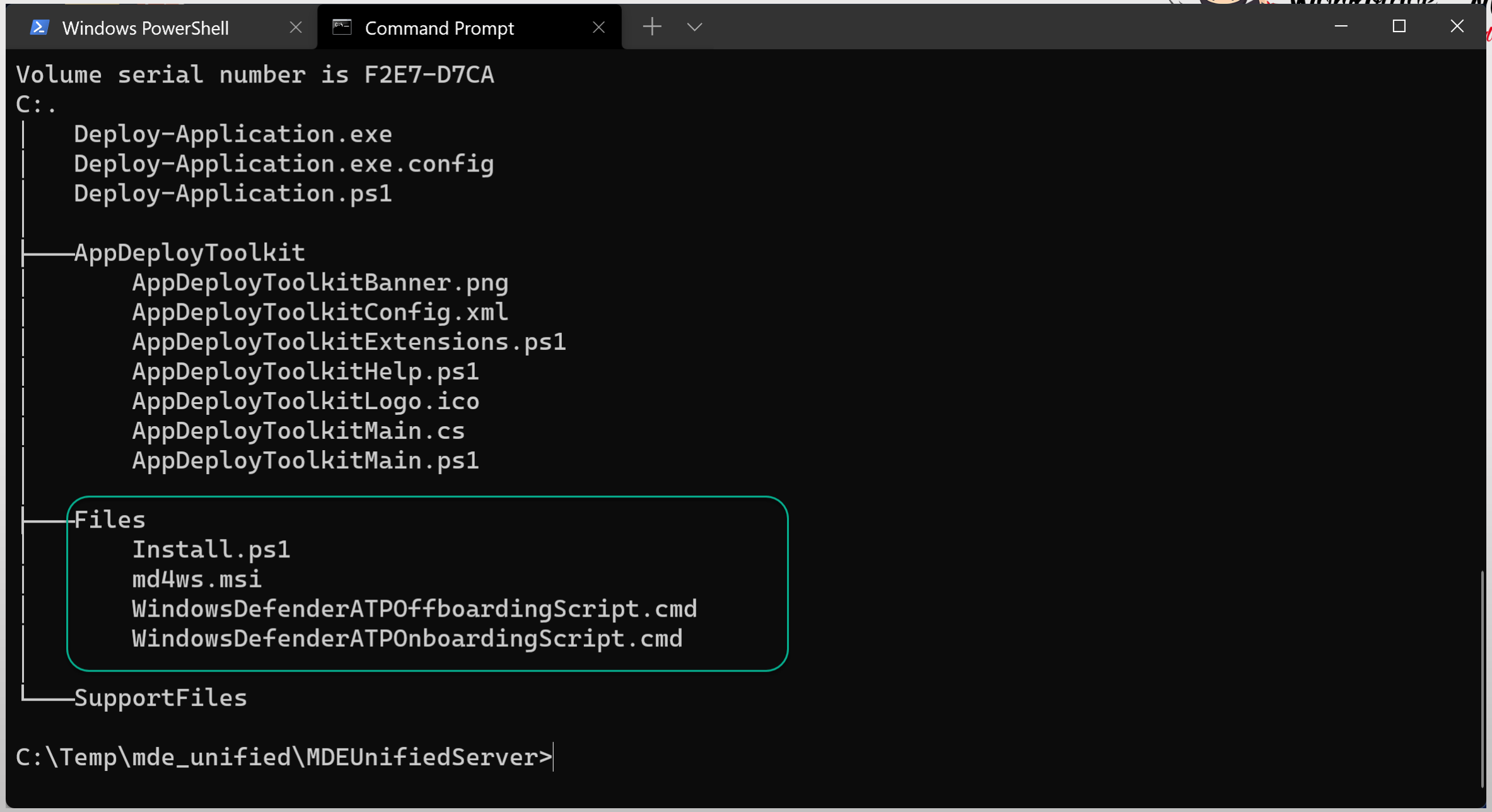
https://github.com/microsoft/mdefordownlevelserver

1. It removes the OMS workspace when the workspace ID is provided with the parameter **RemoveMMA**. **NOTE: this step is for cleanup purposes only. **. ****When installing the new package, the previous sensor will stop running and the workspace is no longer used. You may however still need the MMA for other workspaces/functionality such as OMS, Log Analytics. ****
2. The next step uninstalls SCEP - if it is present, and only on Windows Server 2012 R2 (on Windows Server 2016, SCEP is only a management component and is not required).
3. Then, it checks for prerequisites and downloads and installs two hotfixes on Windows Server 2012 R2 if the prerequisites have not been met, and updates to the latest platform version on Windows Server 2016 if required (NOTE: Defender must be in an upgradeable state, this requires at least one servicing stack and cumulative update to have been applied). Note that on machines that have received recent monthly update rollup packages, the prerequisites will have been met and this step is NOT needed.
4. Next, it installs the Microsoft Defender for Downlevel Servers MSI (md4ws.msi downloaded from the onboarding page for Windows Server 2012 R2 and 2016). If the file is in the same directory as the script, no input is required. If the product was already installed, it will perform a reinstallation with the provided MSI.
5. Finally, it runs the onboarding script, if provided using the parameter **OnboardingScript**. Please use the script for **Group Policy** as it is non-interactive; the local onboarding script will fail.

I need something that I can use with MEMCM or a standalone solution

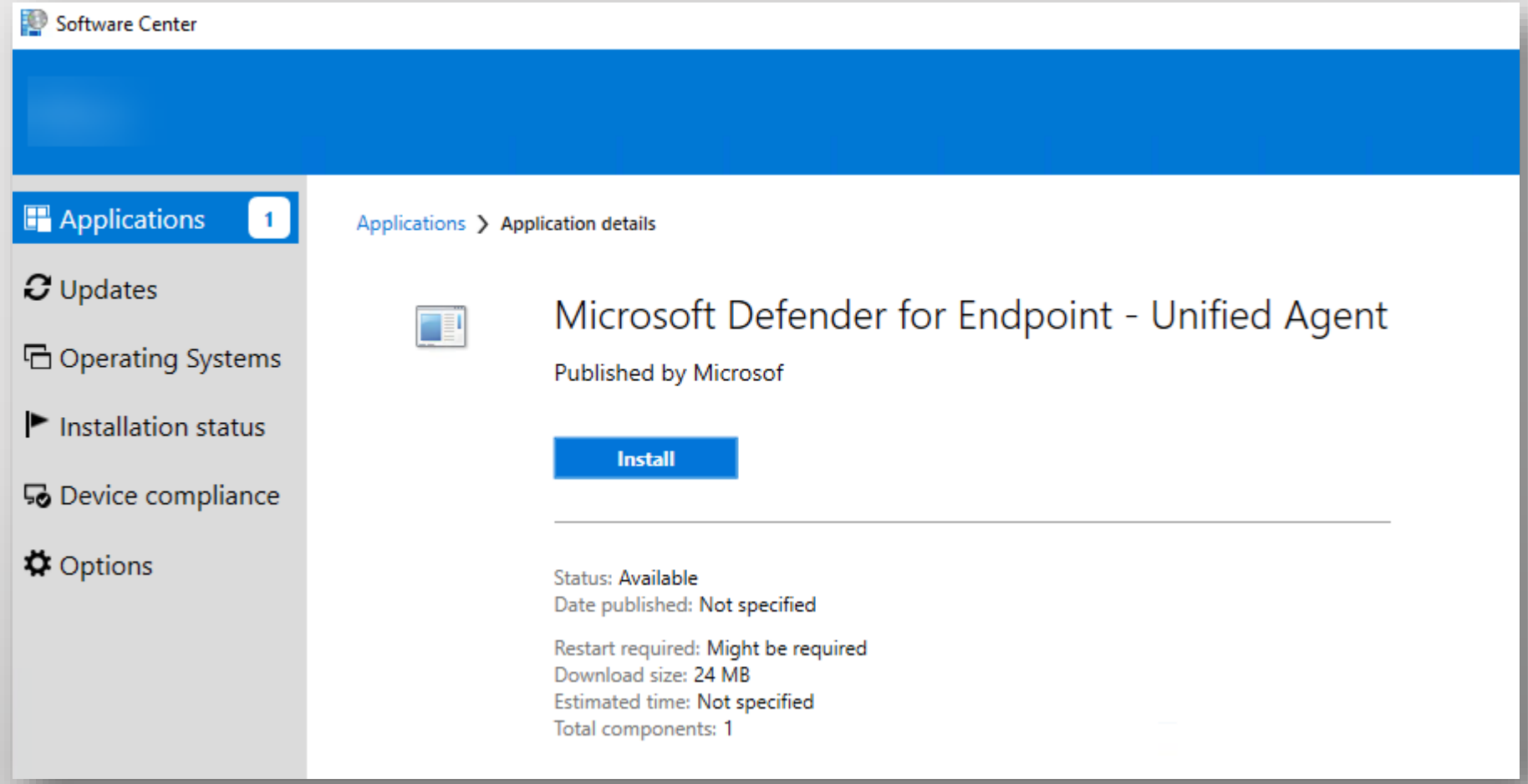
I need an install (onboarding), upgrade and uninstall (offboarding) solution….

So let’s wrap this into a PowerShell App Deployment Toolkit Script


Windows PowerShell
Command Prompt
Volume serial number is F2E7-D7CA
C:.
Deploy-Application.exe
Deploy-Application.exe.config
Deploy-Application.ps1
AppDeployToolkit
AppDeployToolkitBanner.png
AppDeployToolkitConfig.xml
AppDeployToolkitExtensions.ps1
AppDeployToolkitHelp.ps1
AppDeployToolkitLogo.ico
AppDeployToolkitMain.cs
AppDeployToolkitMain.ps1
Files
Install.ps1
md4ws.msi
WindowsDefenderATPOffboardingScript.cmd
WindowsDefenderATPOnboardingScript.cmd
SupportFiles
C:\Temp\mde_unified\MDEUnifiedServer>

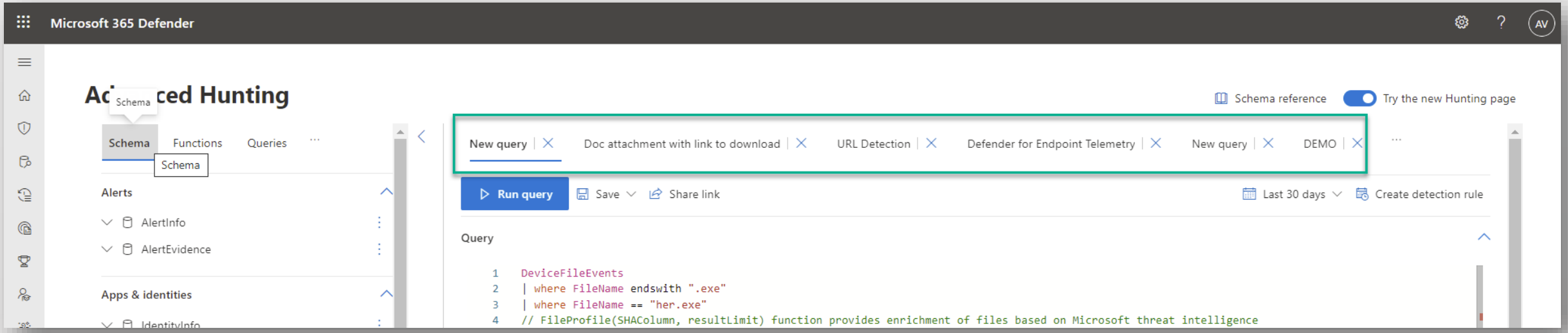
```powershell
## Customer Workspace ID where the MMA Agent was connected to for MDE
[guid]$RemoveMMA = "5
$mma = New-Object -ComObject 'AgentConfigManager.MgmtSvcCfg'
$workspaces = @($mma.GetCloudWorkspaces() | Select-Object -ExpandProperty:workspaceId)
If ($workspaces -contains $RemoveMMA)
{
    $RemoveMMAGuid = $true
}
Else
{
    $RemoveMMAGuid = $false
}


if ($RemoveMMAGuid -eq $true)
{
    $invokeInstallation = & "$($PSScriptRoot)\Files\Install.ps1" -RemoveMMA $RemoveMMA -OnboardingScript "$($PSScr
}
else
{
    $invokeInstallation = & "$($PSScriptRoot)\Files\Install.ps1" -OnboardingScript "$($PSScriptRoot)\Files\WindowsD
}
```

```powershell
# <Perform Uninstallation tasks here>


$invokeUninstallation = & "$($PSScriptRoot)\Files\WindowsDefenderATPOffboardingScript.cmd" -log -Verbose
$invokeUninstallation = & "$($PSScriptRoot)\Files\Install.ps1" -Uninstall -log -Verbose

##*=============================================
##* POST-UNINSTALLATION
```

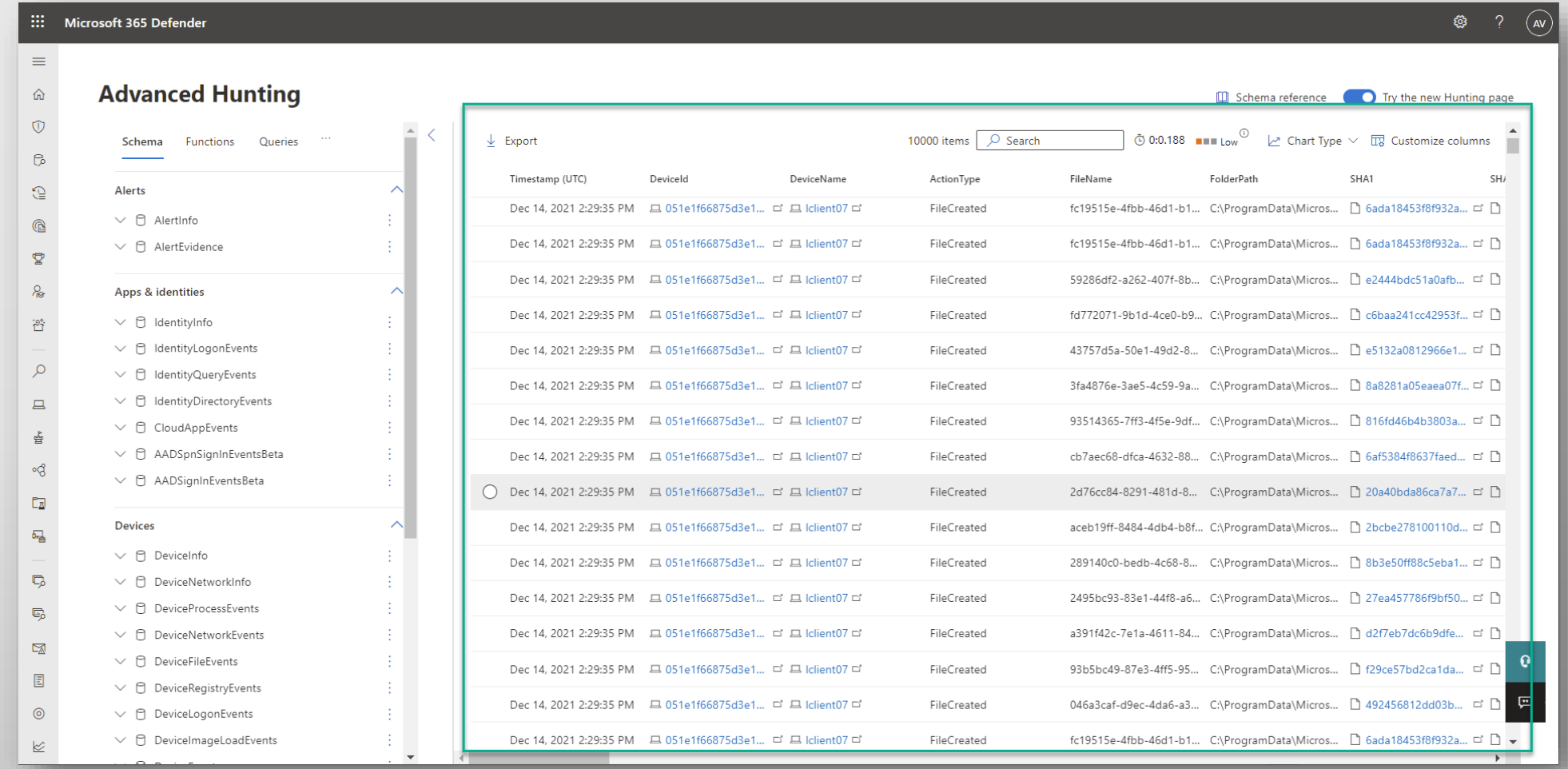


Microsoft Defender for Endpoint

New Advanced Hunting Experience

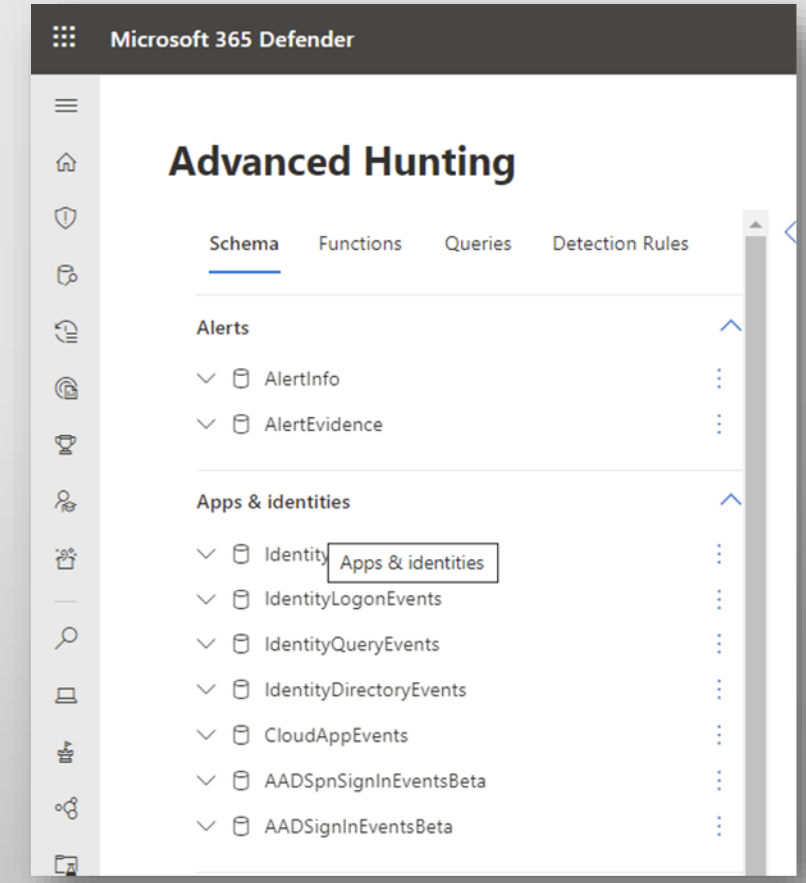


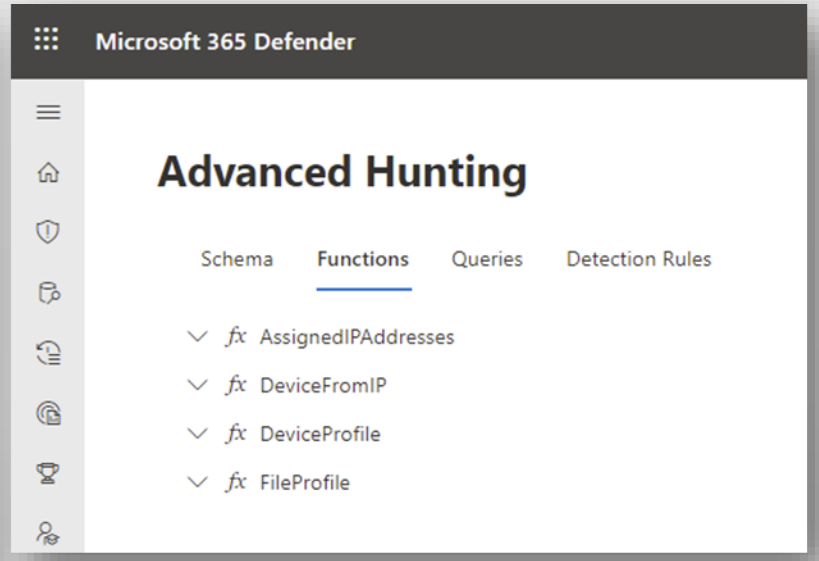
Multi-tab support – You can now use multiple tabs. Every time you create a new query or open a saved query or a custom detection rule, it will launch in a new tab:

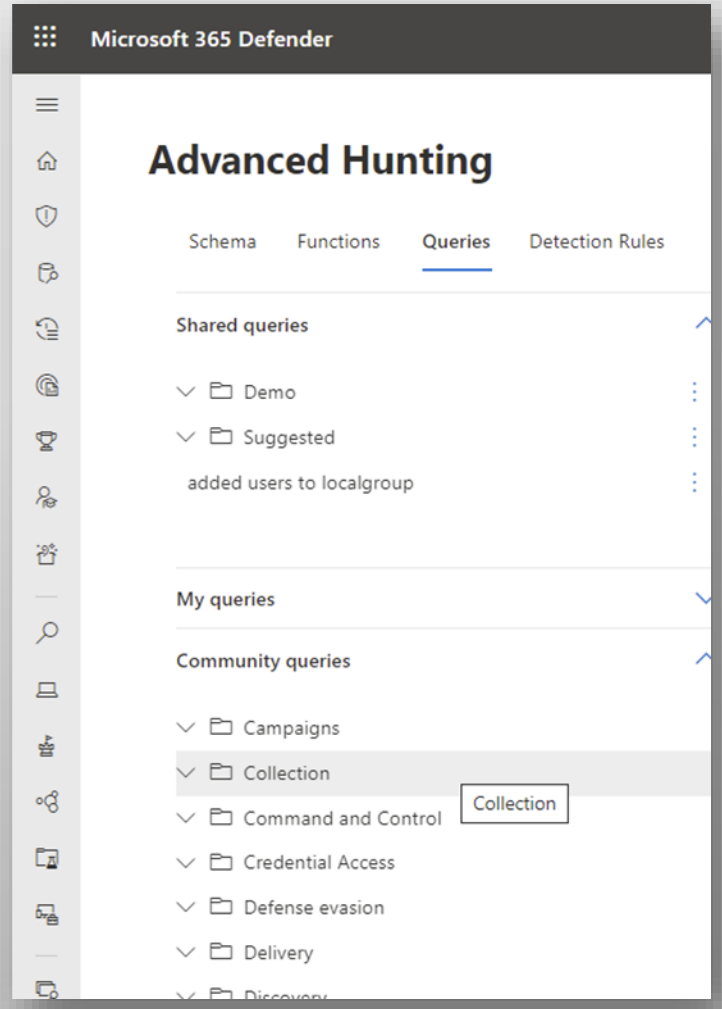


Smart scrolling – Long query results are now rendered in a list that expands automatically as you scroll down, so you can focus on scanning the results.

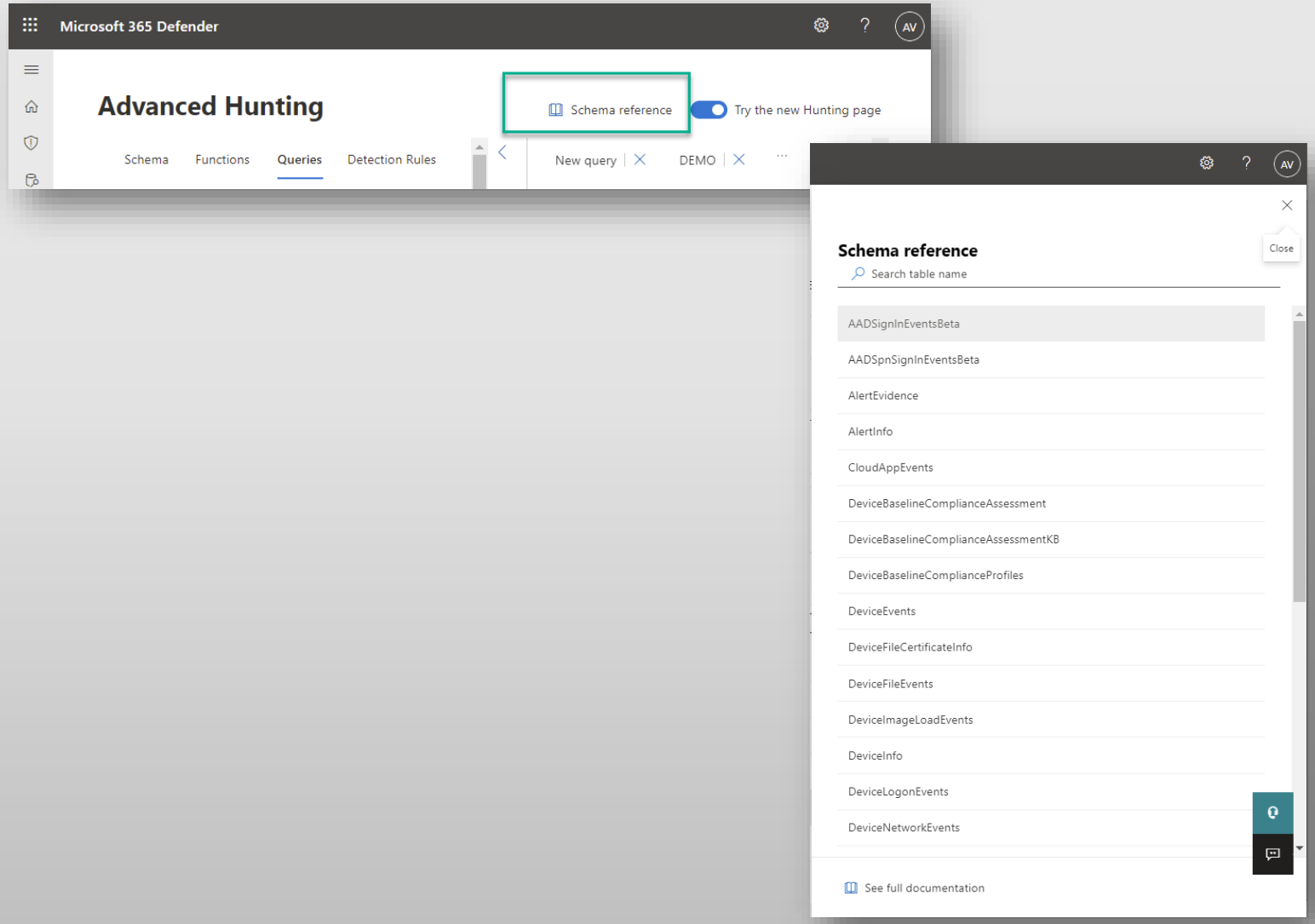
Streamlined schema tabs – Schema, functions, queries, and detection rules are now separate tabs so you can easily pivot between them.

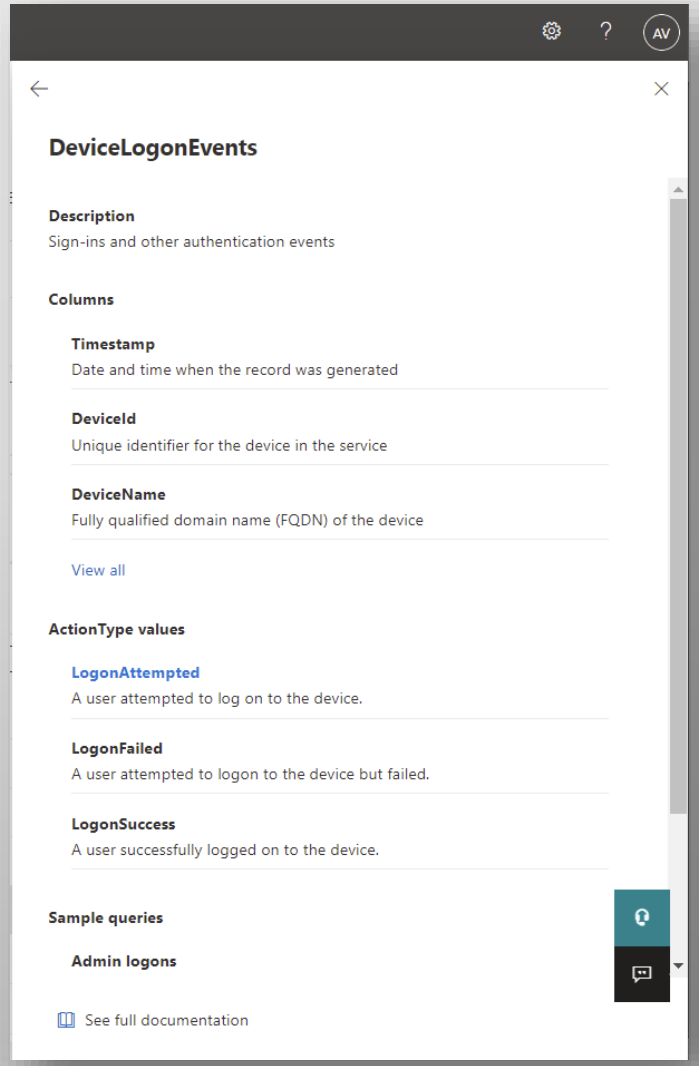




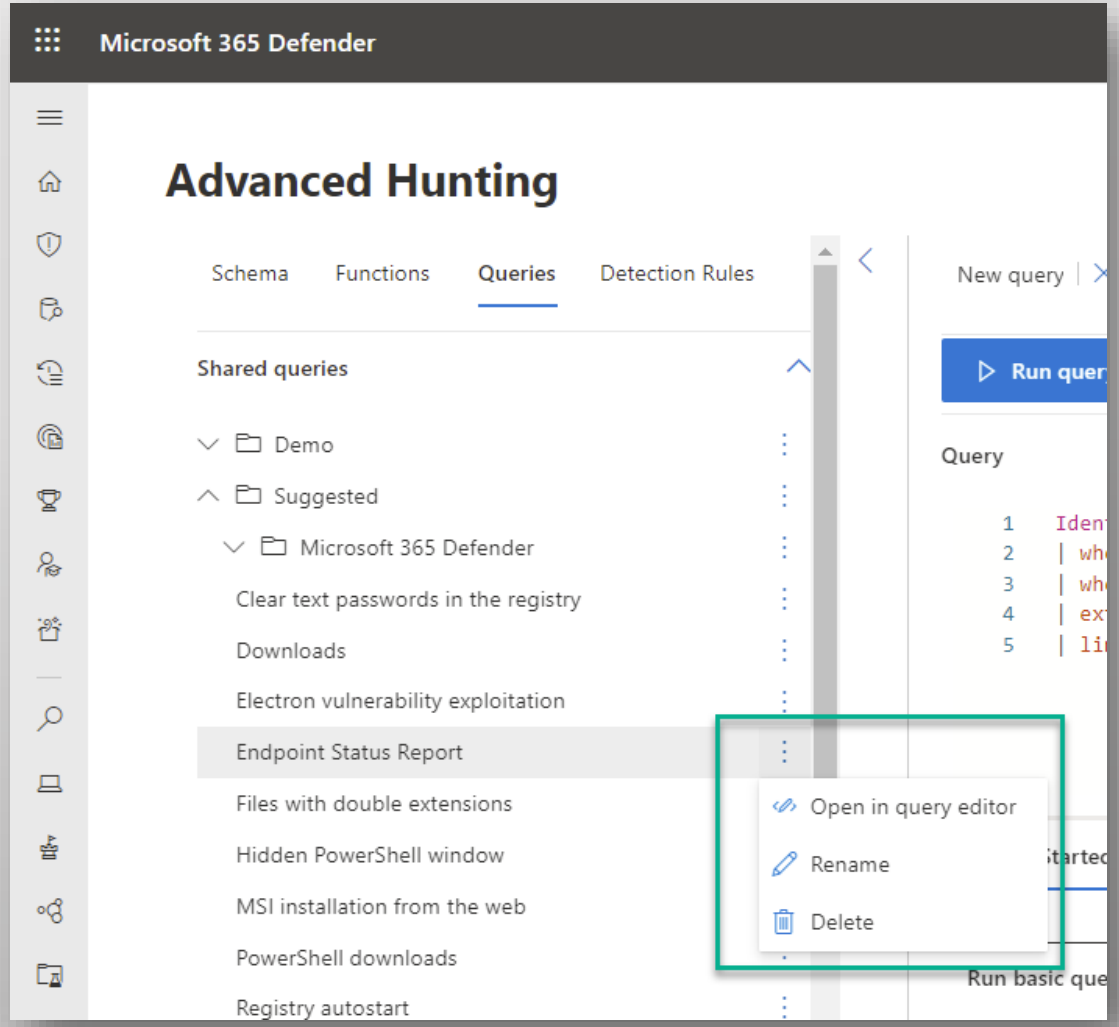


Improved schema reference view so you can easily navigate where you need to.

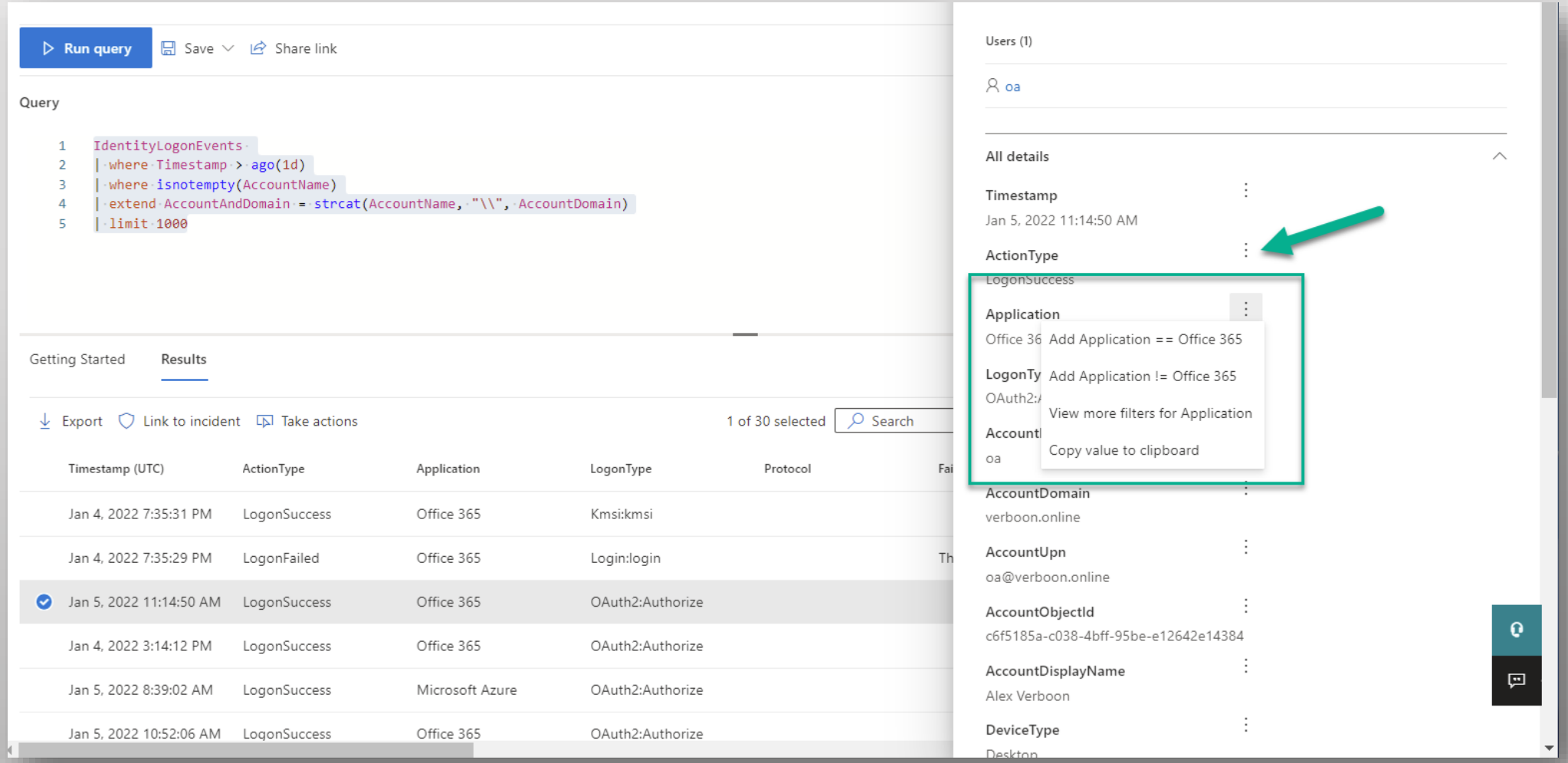




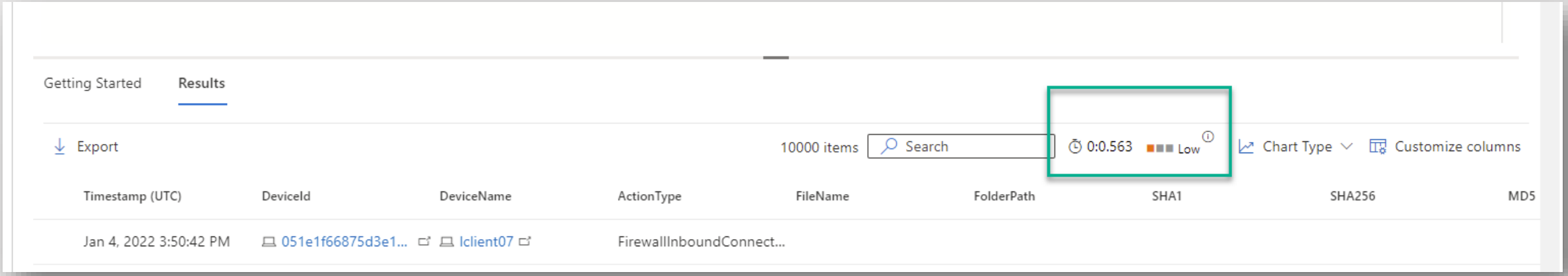
Quick-edit queries – Select or double-click the three dots to the right of the query to open the query in the editor, delete the query, or rename the query.



Refine your query by adding a filter from the results set - From your initial results set, go to the record side pane for one of the results, then select the three dots to the right of a column of interest to add it as a filter in your current query.

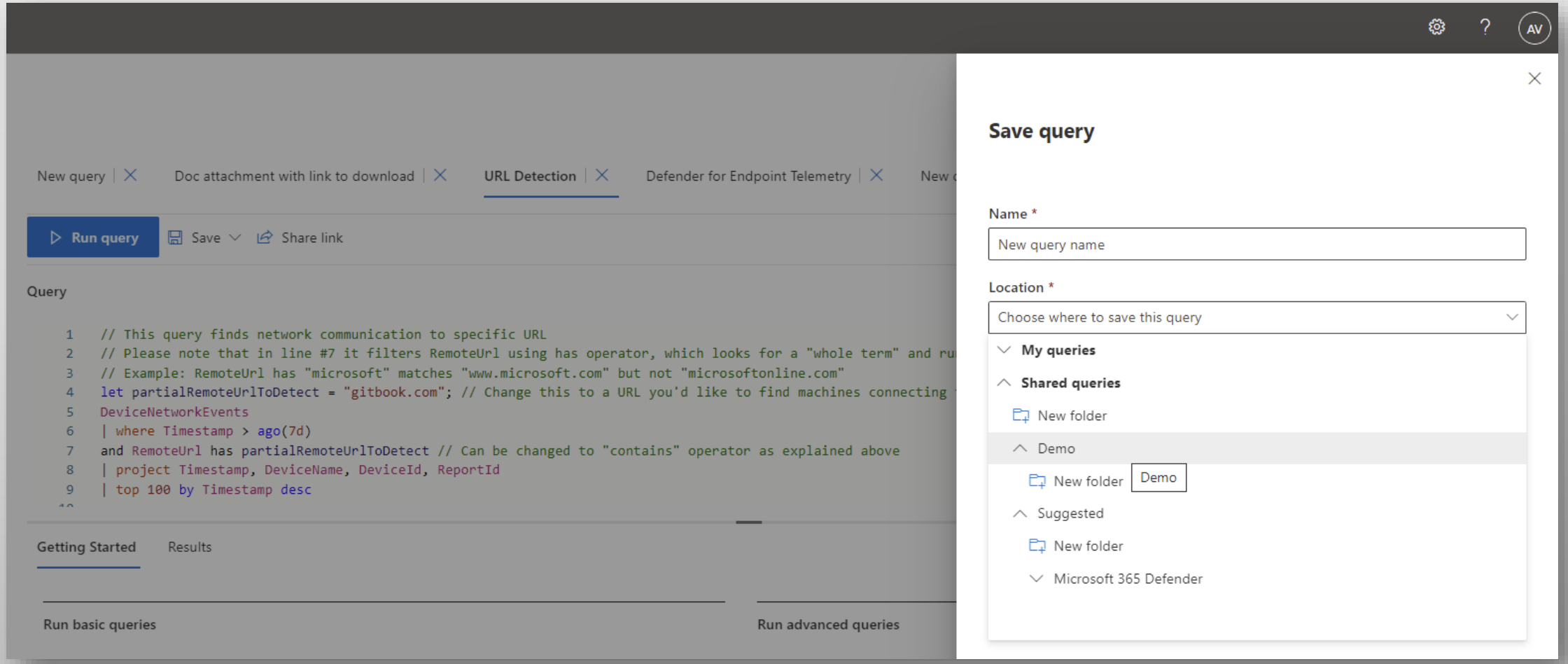


Resource usage indicator - After running your query, you can see the execution time and its resource usage (Low, Medium, High) so you can tweak your query accordingly. High indicates that the query took more resources to run and could be improved to execute more efficiently.

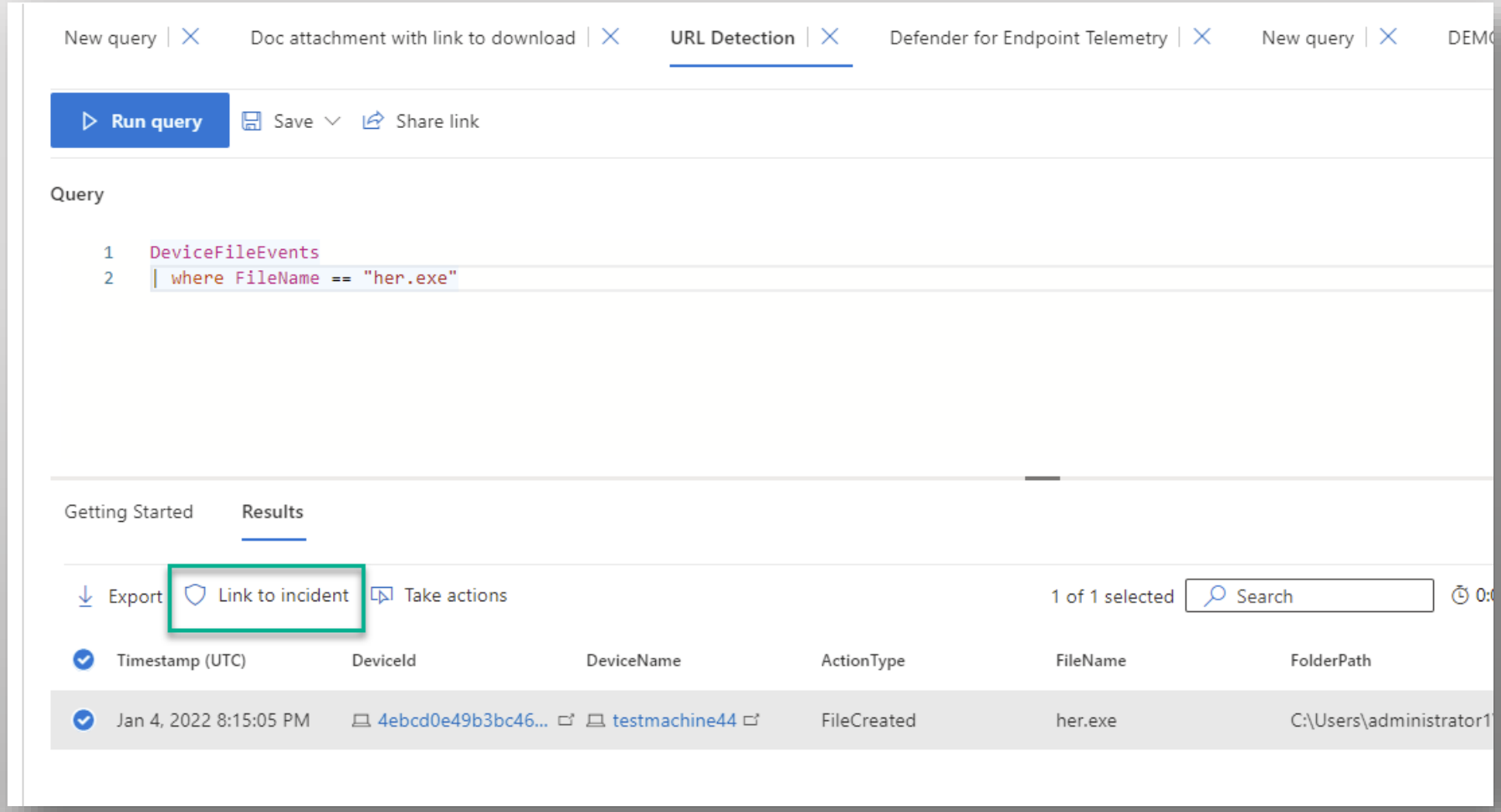


Depending on its size, each tenant has access to a set amount of CPU resources allocated for running advanced hunting queries.

Save query side pane – The Save query option is now located in a side pane for easier viewing.



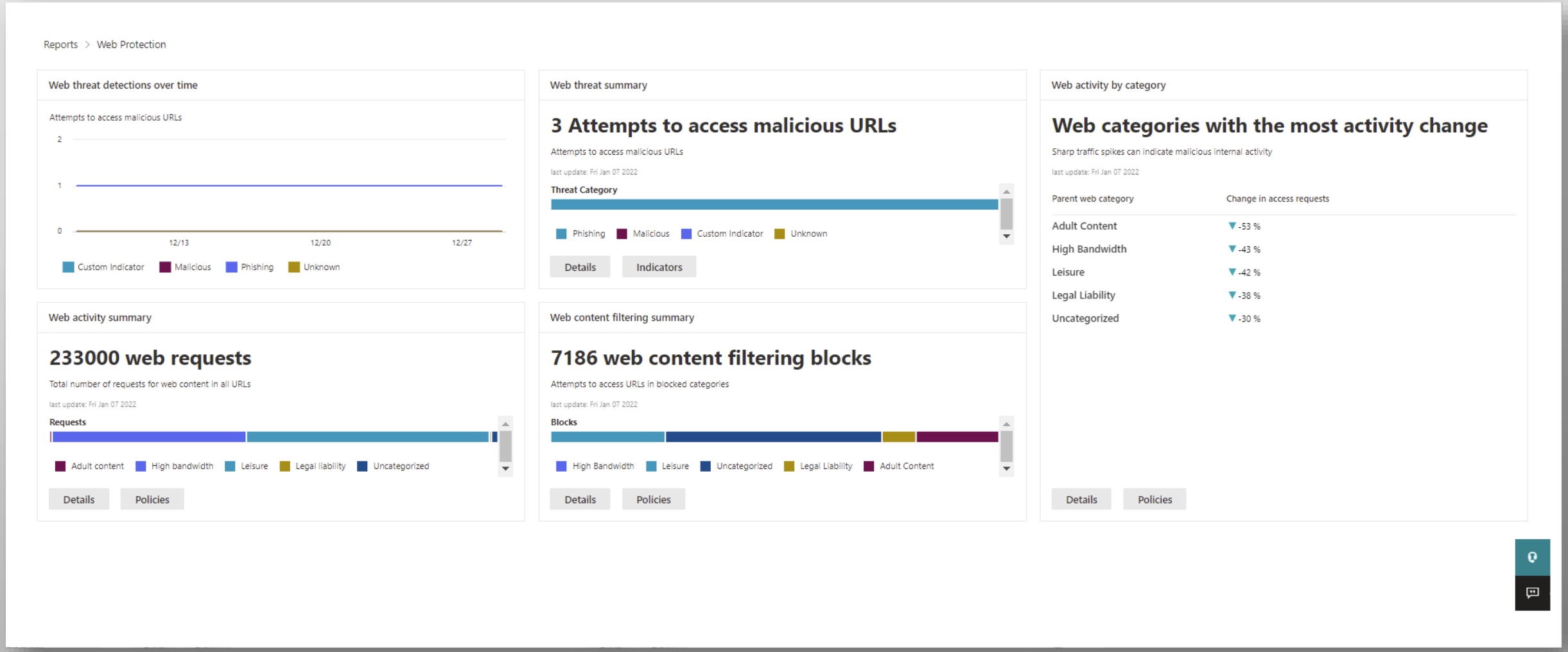
Link query results to an incident - After you run your advanced hunting query, you can select which events are related to the investigation you are working on. The events you select can now be added as an alert to the incident of your choice.



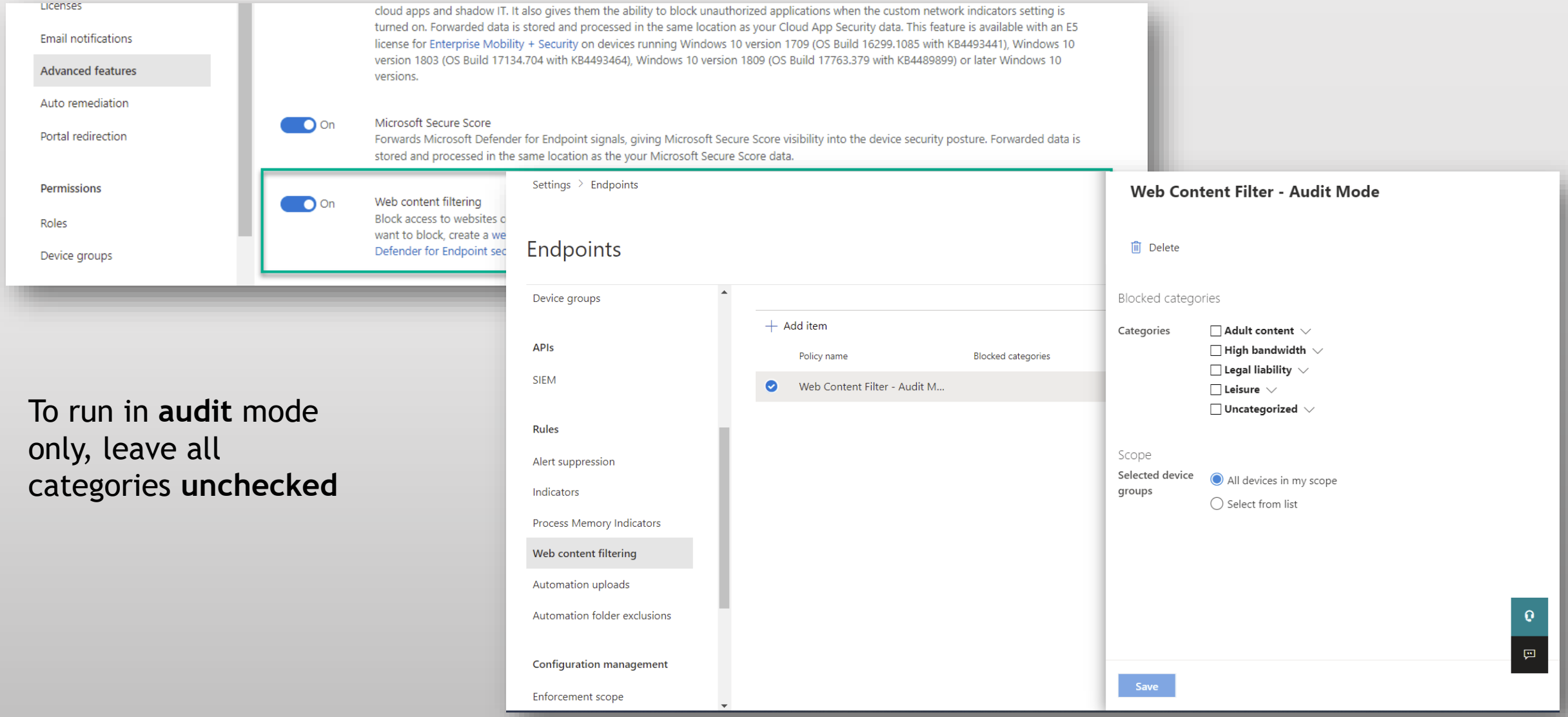
Microsoft Defender for Endpoint

Web Content Filtering

Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.



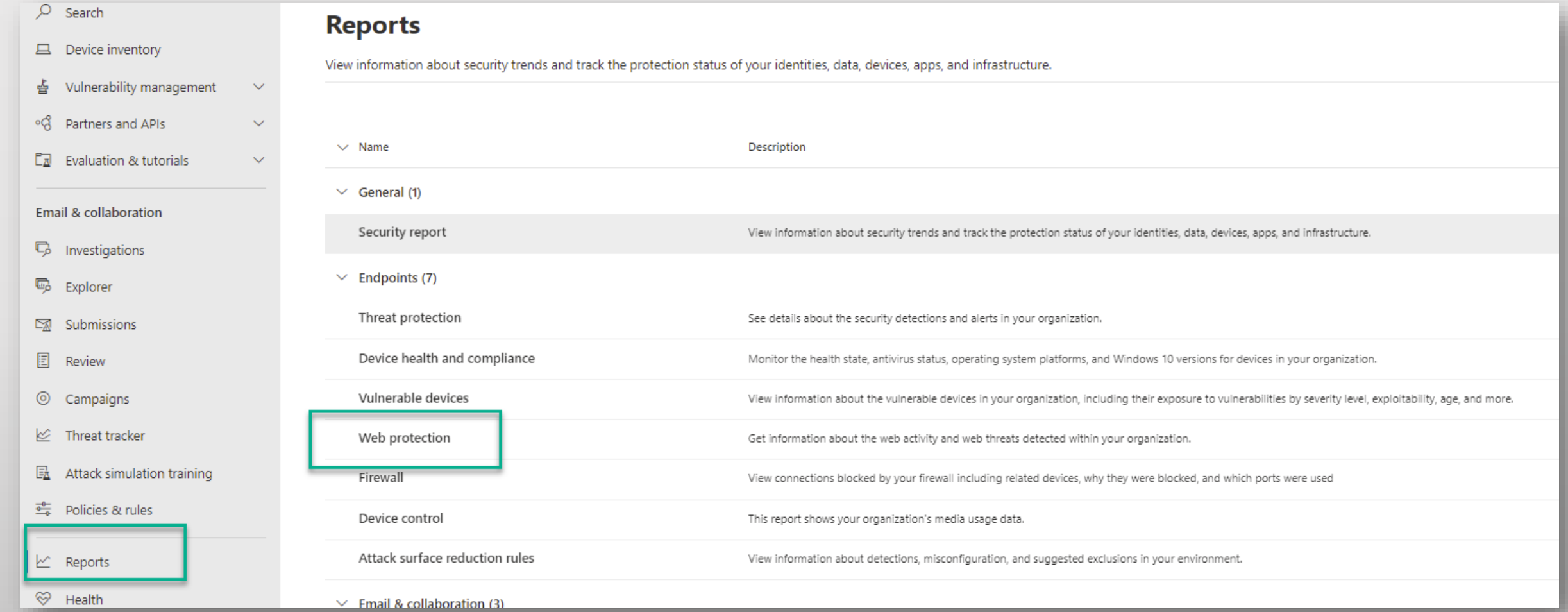
Even if you do not intend to actively block content, we recommend that you enable the feature in audit mode.



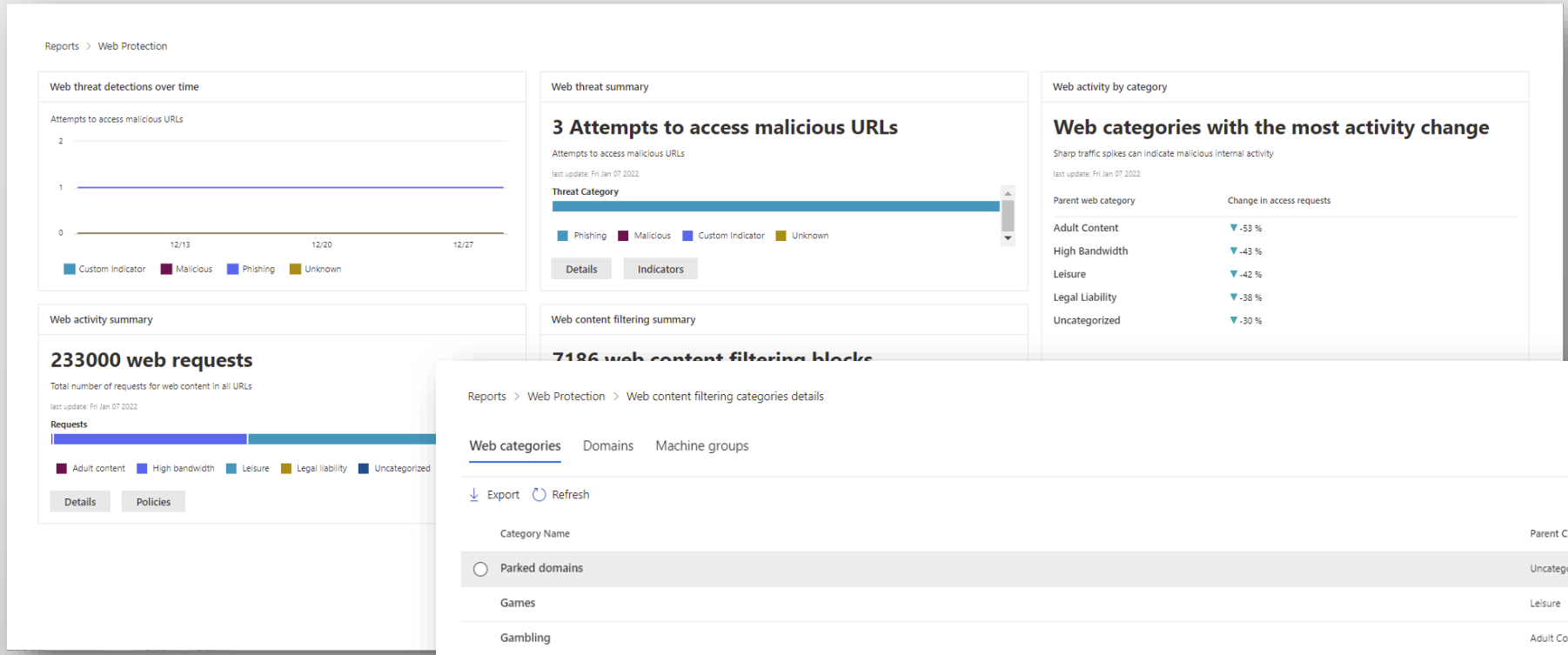
To run in **audit** mode only, leave all categories **unchecked**

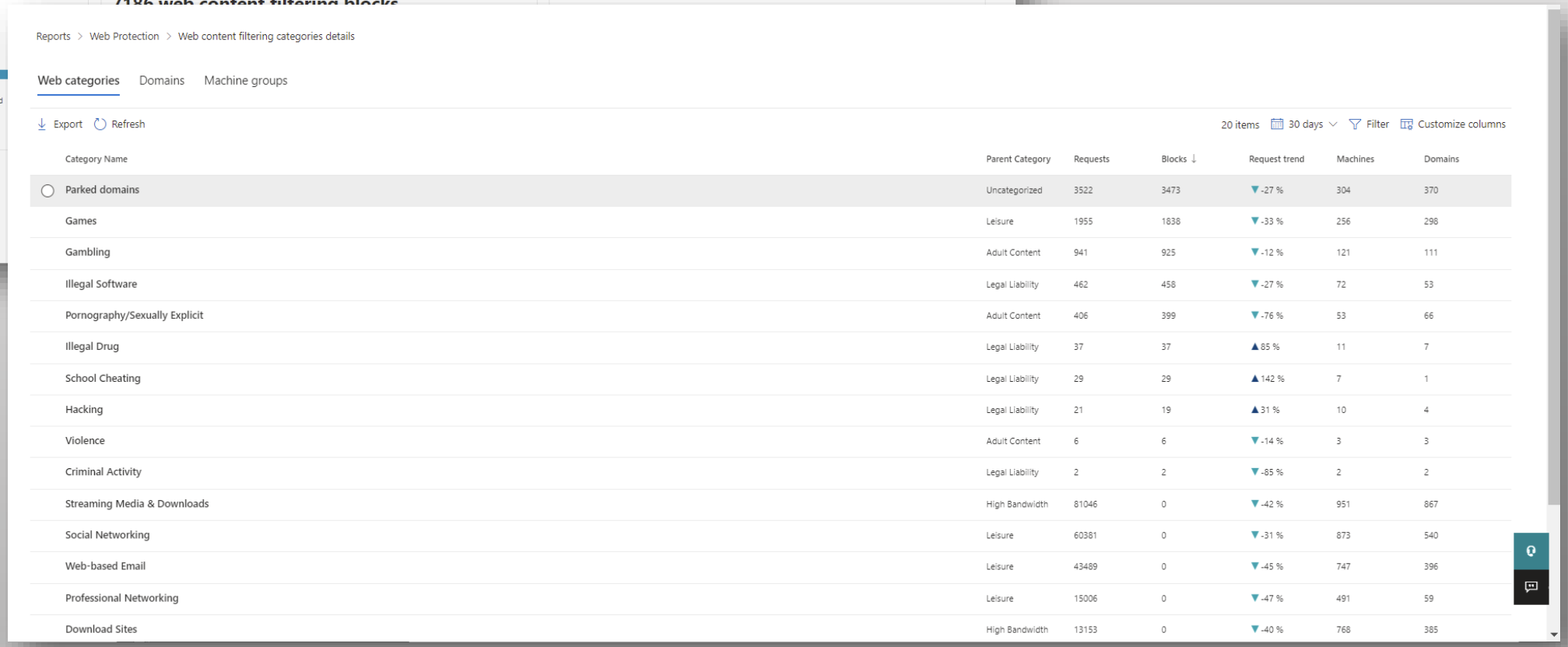
Category	Sub Categories
Adult Content	**Cults**: Sites related to groups or movements whose members demonstrate passion for a belief system that is different from those that are socially accepted. **Gambling**: Online gambling and sites that promote gambling skills and practice. **Nudity**: Sites that provide full-frontal and semi-nude images or videos, typically in artistic form, and might allow the download or sale of such materials. **Pornography** / Sexually explicit: Sites containing sexually explicit content in an image-based or textual form. Any form of sexually oriented material is also listed here. **Sex education**: Sites that discuss sex and sexuality in an informative and non-voyeuristic way, including sites that provide education about human reproduction and contraception, sites that offer advice on preventing infection from sexual diseases, and sites that offer advice on sexual health matters. **Tasteless:** Sites oriented towards content unsuitable for school children to view or that an employer would be uncomfortable with their staff accessing, but not necessarily violent or pornographic.
High Bandwidth	**Download** sites: Sites whose primary function is to allow users to download media content or programs, such as computer programs. **Image sharing**: Sites that are used primarily for searching or sharing photos, including those that have social aspects. **Peer-to-peer**: Sites that host peer-to-peer (P2P) software or facilitate the sharing of files using P2P software. **Streaming media & downloads**: Sites whose primary function is the distribution of streaming media, or sites that
Legal Liability	**Child abuse** images: Sites that include child abuse images or pornography. **Criminal activity:** Sites that give instruction on, advice about or promotion of illegal activities. **Hacking**: Sites that provide resources for illegal or questionable use of computer software or hardware, including sites that distribute copyrighted material that has been cracked. **Hate & intolerance**: Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice. **Illegal drug:** Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia. **Illegal software**: Sites that contain or promote the use of malware, spyware, botnets, phishing scams, or piracy & copyright theft. **School cheating**: Sites related to plagiarism or school cheating. **Self-harm**: Sites that promote self-harm, including cyberbullying sites that contain abusive and/or threatening messages towards users. **Weapons:** Any site that sells weapons or advocates the use of weapons, including but not limited to guns, knives, and ammunition.
Leisure	**Chat:** Sites that are primarily web-based chat rooms. **Games:** Sites relating to video or computer games, including sites that promote gaming through hosting online services or information related to gaming. **Instant messaging:** Sites that can be used to download instant messaging software or client based instant messaging. **Professional network**: Sites that provide professional networking services. **Social networking:** Sites that provide social networking services. **Web-based email**: Sites offering web-based mail services.
Uncategorized	**Newly registered domains**: Sites that have been newly registered in the past 30 days and have not yet been moved to another category. **Parked domains:** Sites that have no content or are parked for later use. NOTE: Uncategorized contains only newly registered domains and parked domains, and does not include all other sites outside of these categories.

The web protection reports are accessible through the Report option within the Microsoft 365 Defender portal

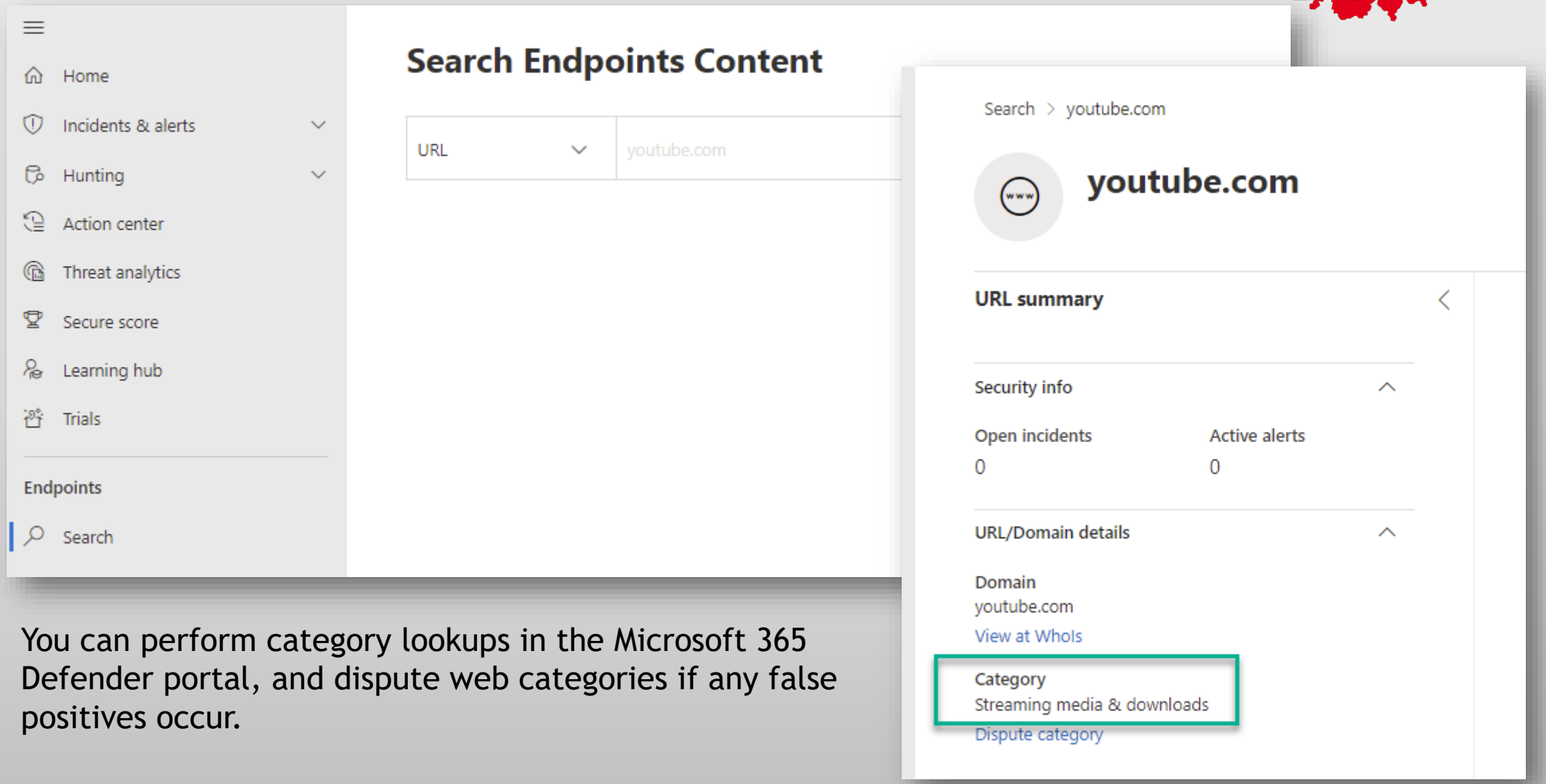


Select the **Details** button underneath each graph to obtain detailed information





Category Name	Parent Category	Requests	Blocks	Request trend	Machines	Domains
Parked domains	Uncategorized	3522	3473	▼-27 %	304	370
Games	Leisure	1955	1838	▼-33 %	256	298
Gambling	Adult Content	941	925	▼-12 %	121	111
Illegal Software	Legal Liability	462	458	▼-27 %	72	53
Pornography/Sexually Explicit	Adult Content	406	399	▼-76 %	53	66
Illegal Drug	Legal Liability	37	37	▲85 %	11	7
School Cheating	Legal Liability	29	29	▲142 %	7	1
Hacking	Legal Liability	21	19	▲31 %	10	4
Violence	Adult Content	6	6	▼-14 %	3	3
Criminal Activity	Legal Liability	2	2	▼-85 %	2	2
Streaming Media & Downloads	High Bandwidth	81046	0	▼-42 %	951	867
Social Networking	Leisure	60381	0	▼-31 %	873	540
Web-based Email	Leisure	43489	0	▼-45 %	747	396
Professional Networking	Leisure	15006	0	▼-47 %	491	59
Download Sites	High Bandwidth	13153	0	▼-40 %	768	385



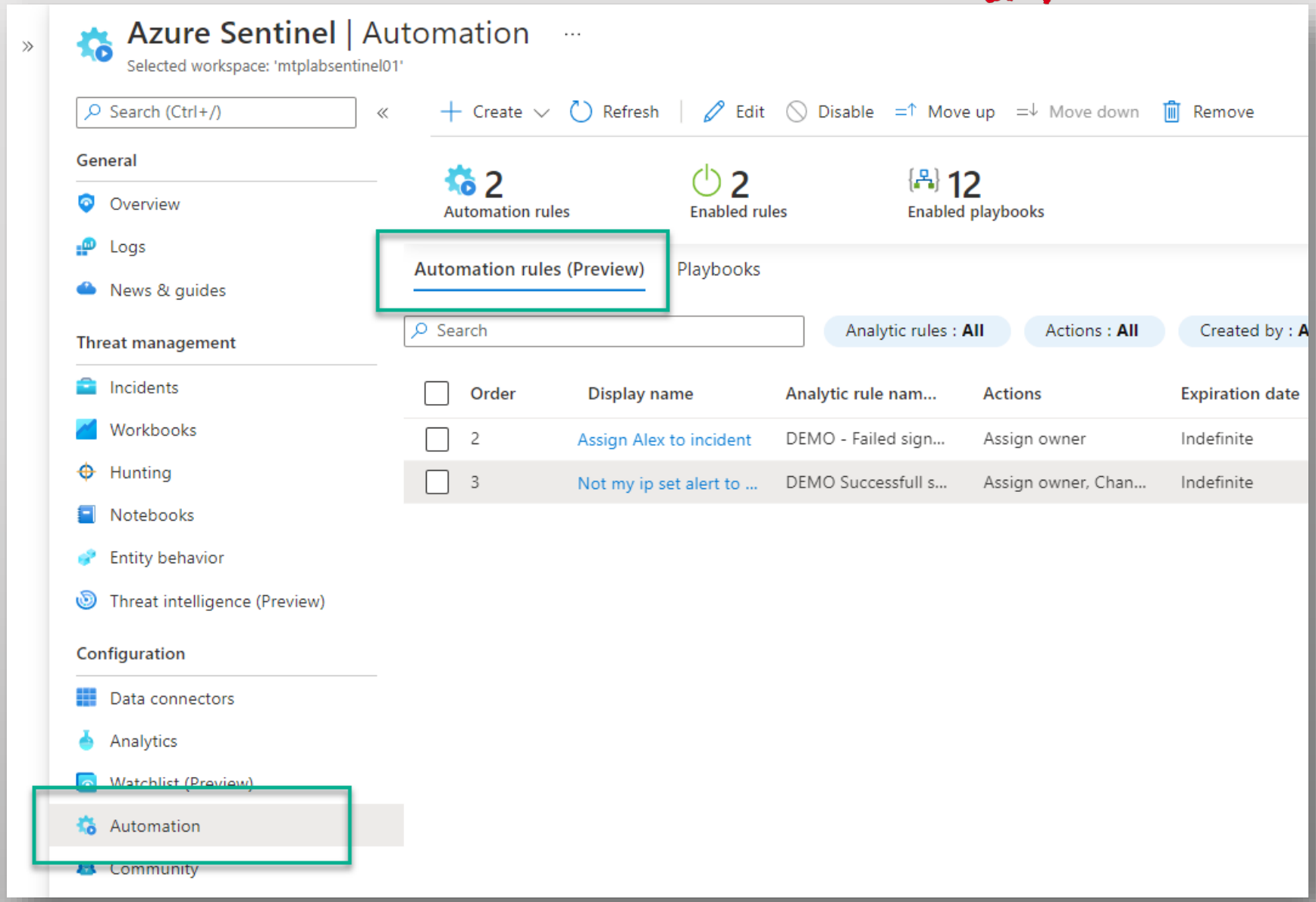
You can perform category lookups in the Microsoft 365 Defender portal, and dispute web categories if any false positives occur.

Microsoft Sentinel

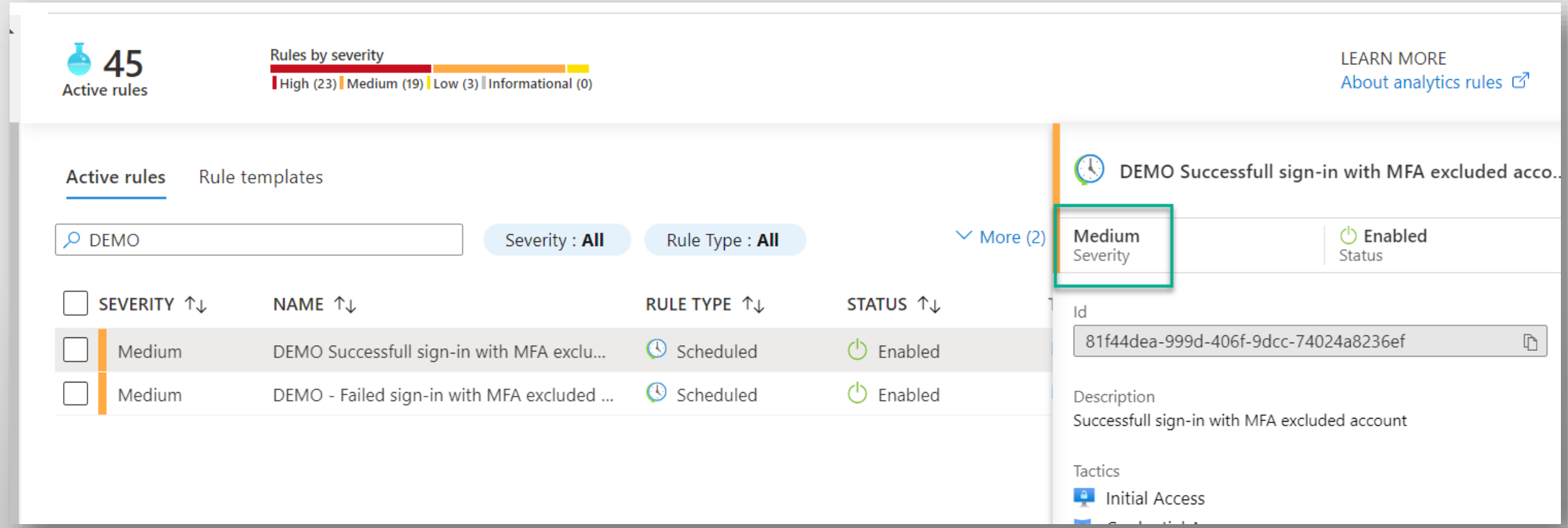
Automation Rules

Azure Sentinel - Automation Rules

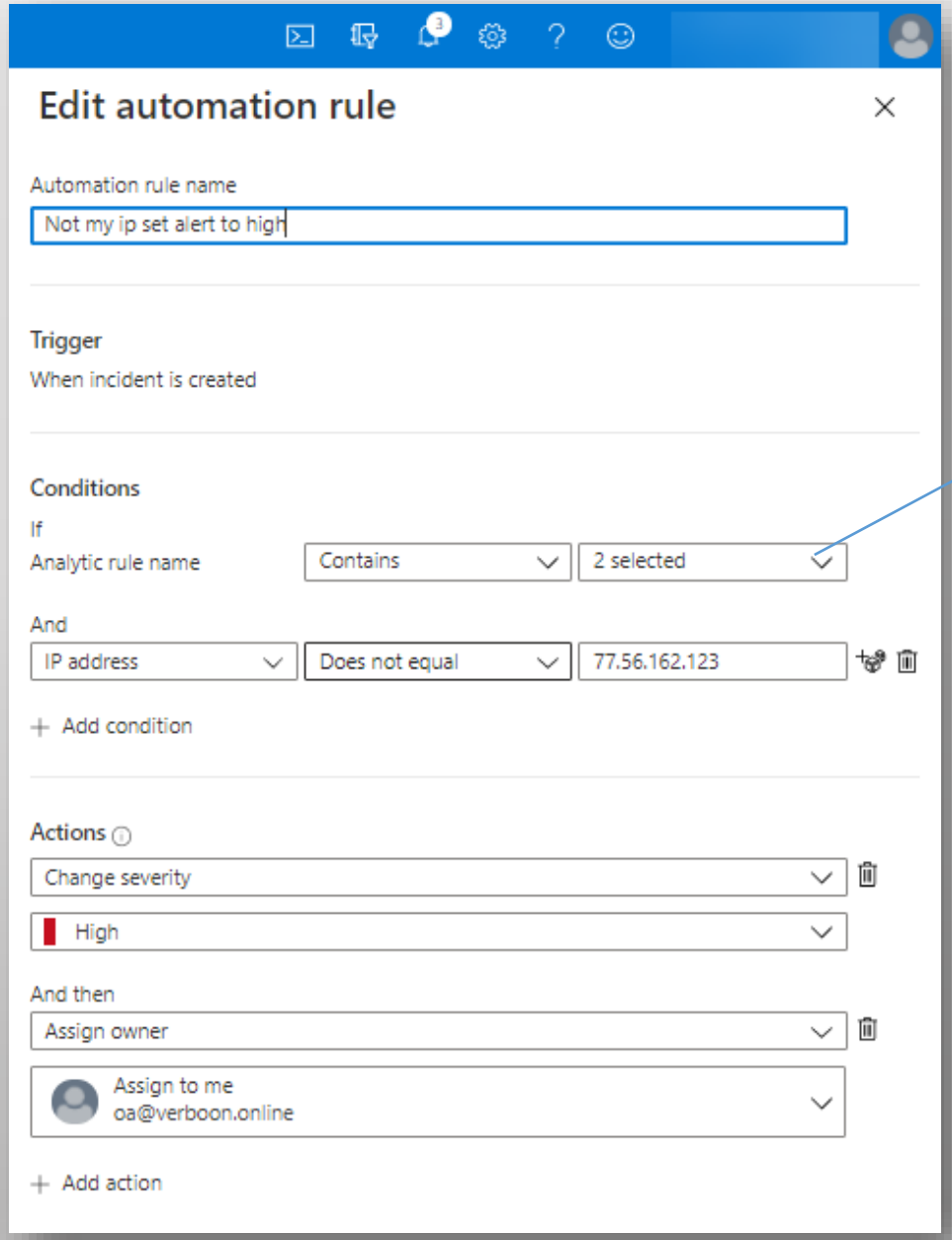
New automation rules make it easy to apply a series of common actions and playbooks to security incidents. You can specify conditions for when the rule will be applied, and select one or more pre-defined actions (e.g. assign to a user, or change severity) and Logic App playbooks to run in sequence. You can also run multiple automation rules in sequence.

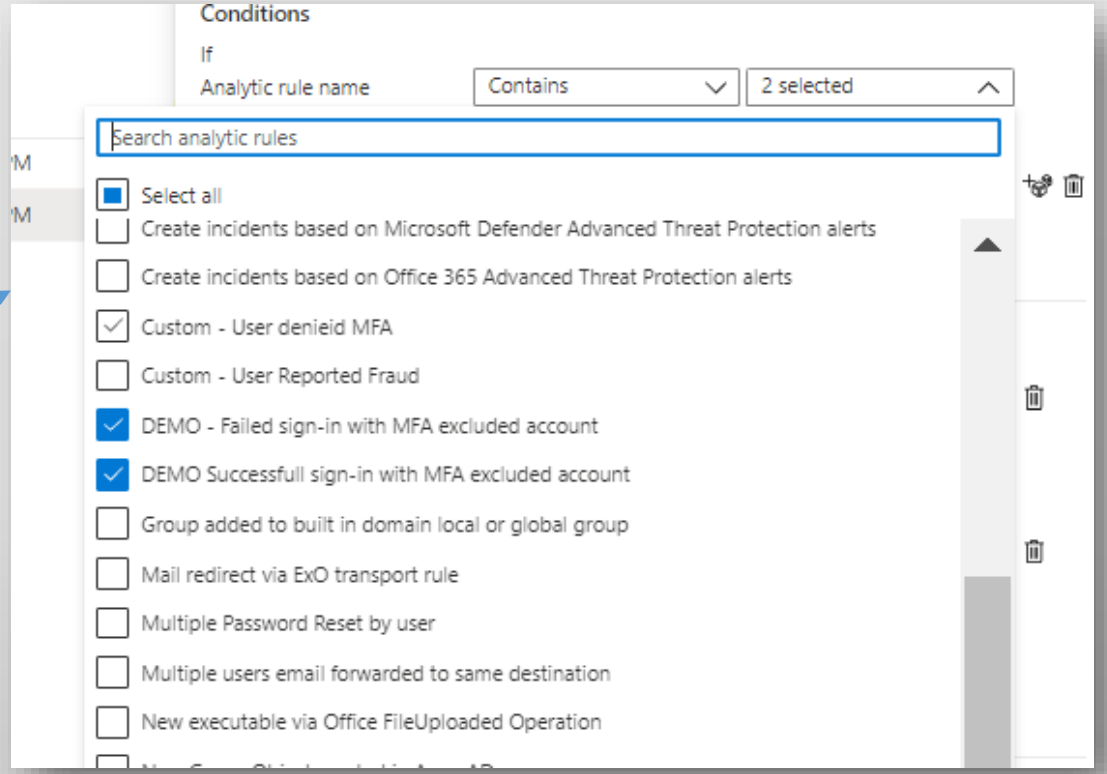


Azure Sentinel - Automation Rules

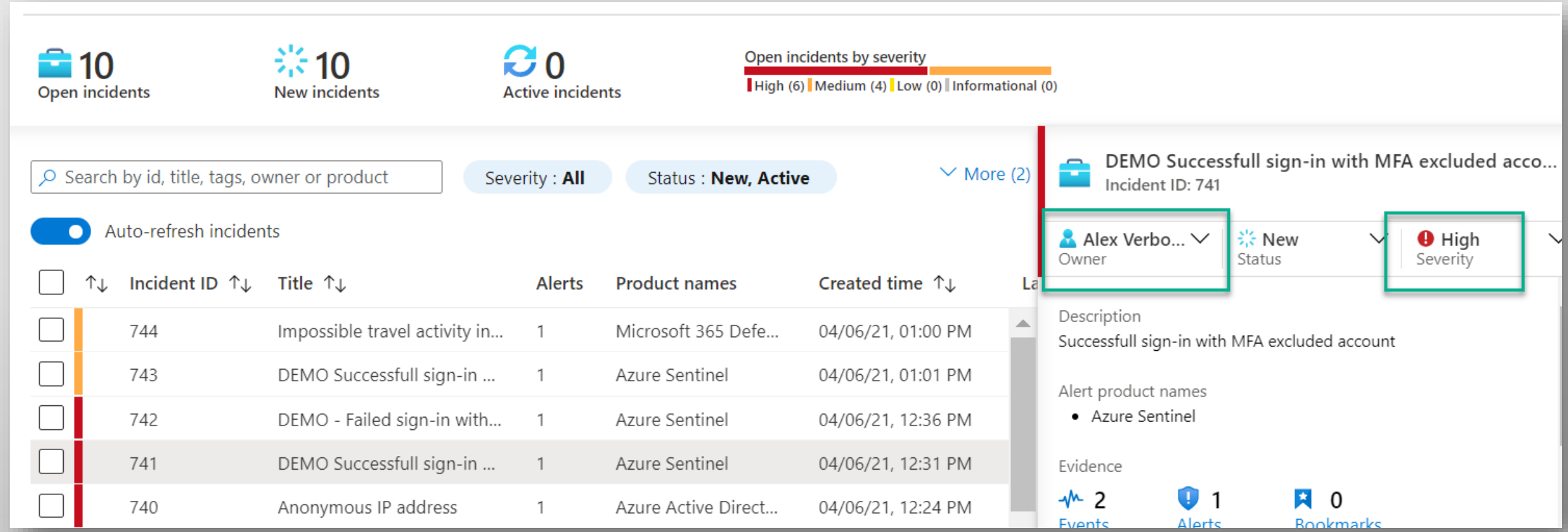


Azure Sentinel - Automation Rules





Azure Sentinel - Automation Rules

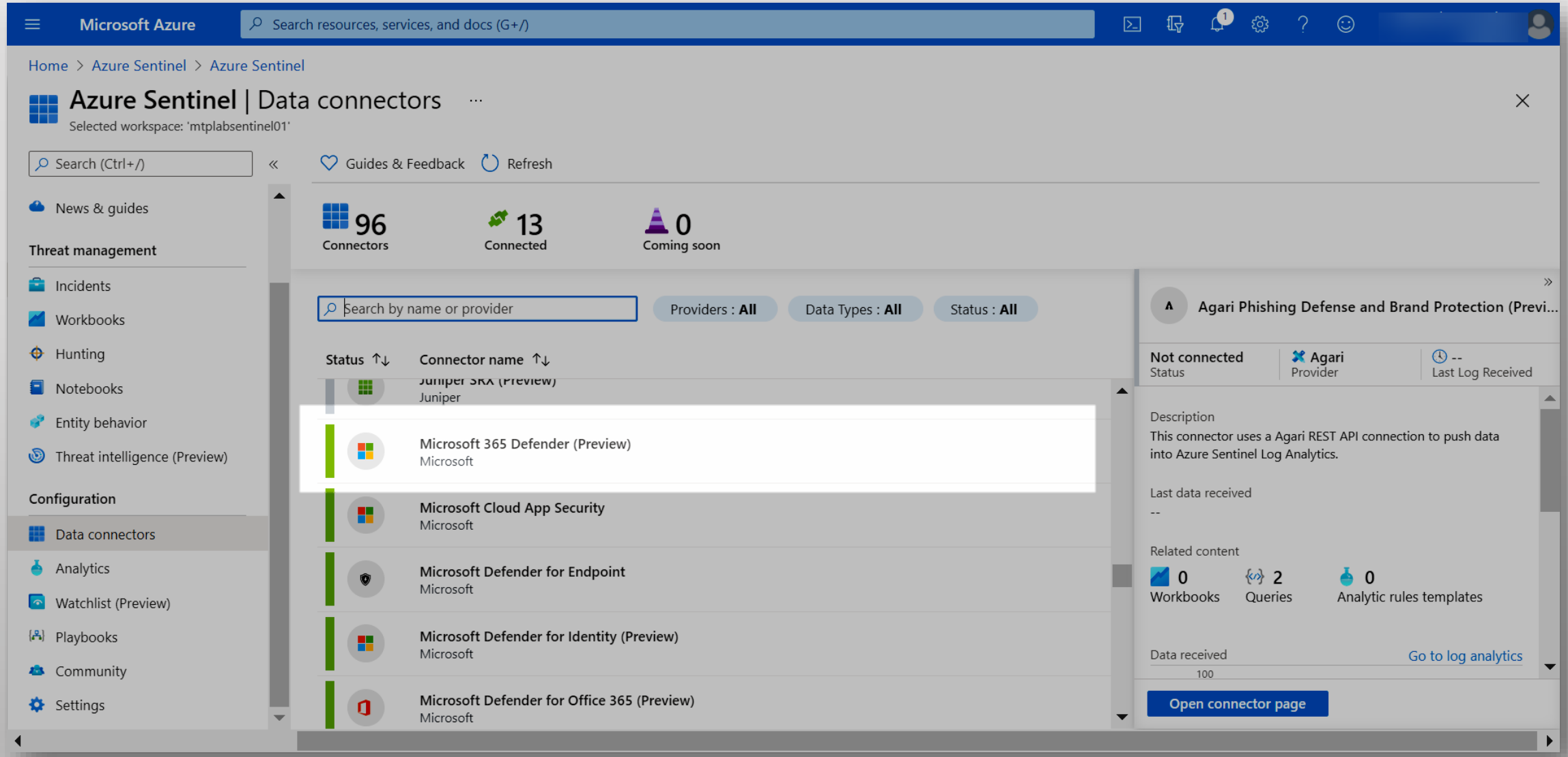


Microsoft Sentinel

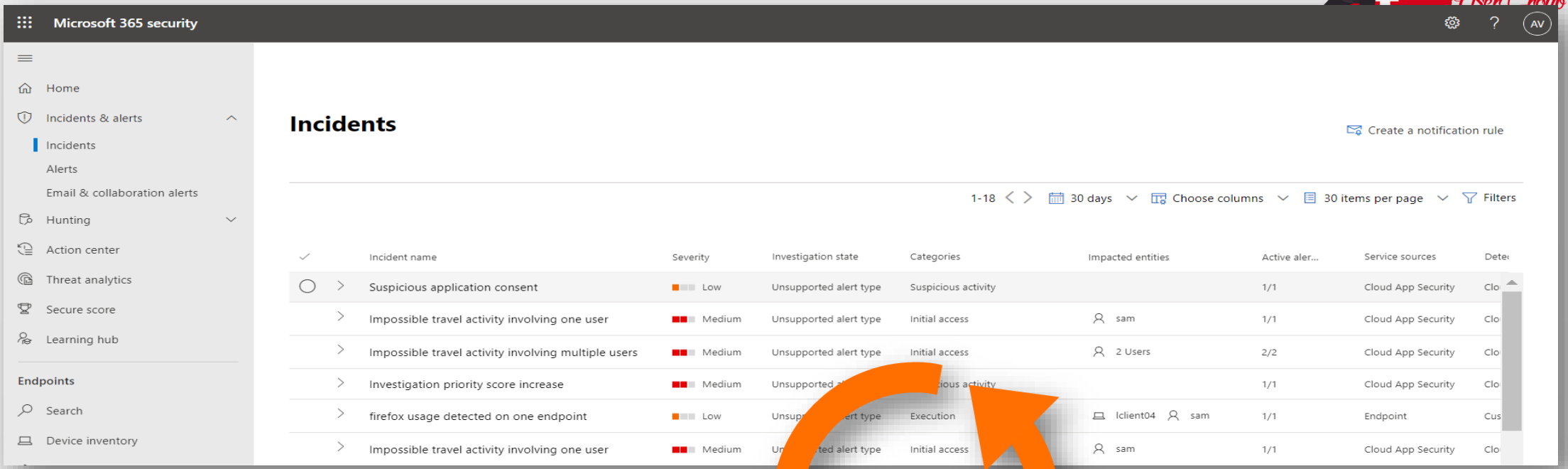
Microsoft 365 Defender Connector

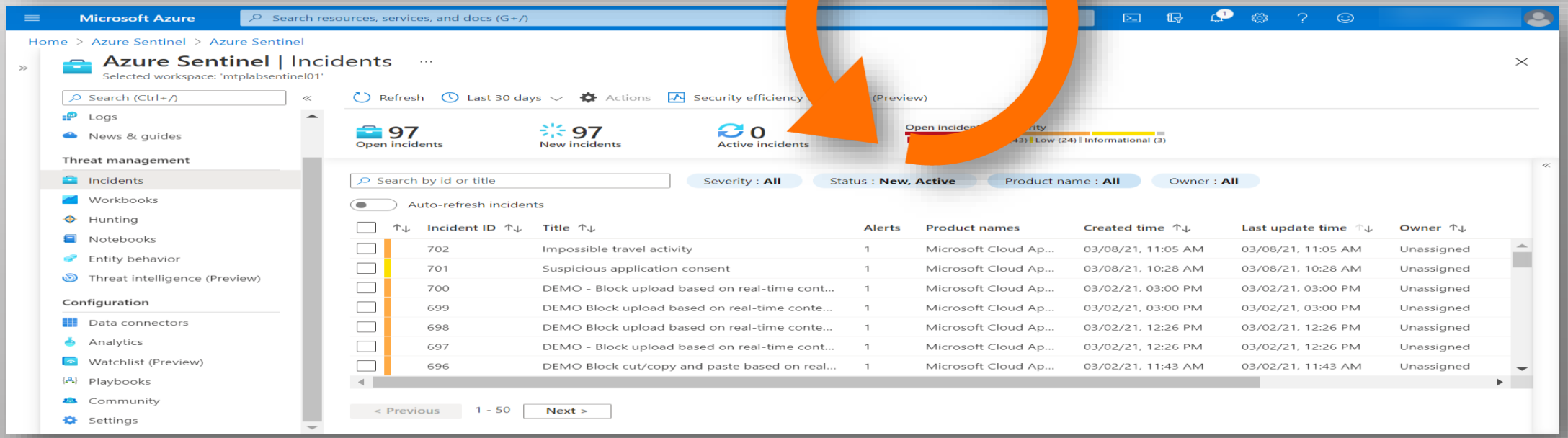
Azure Sentinel - M365 Defender Connector

Azure Sentinel's Microsoft 365 Defender (M365D) incident integration allows you to stream all M365D incidents into Azure Sentinel and keep them synchronized between both portals.



Azure Sentinel - M365 Defender Connector

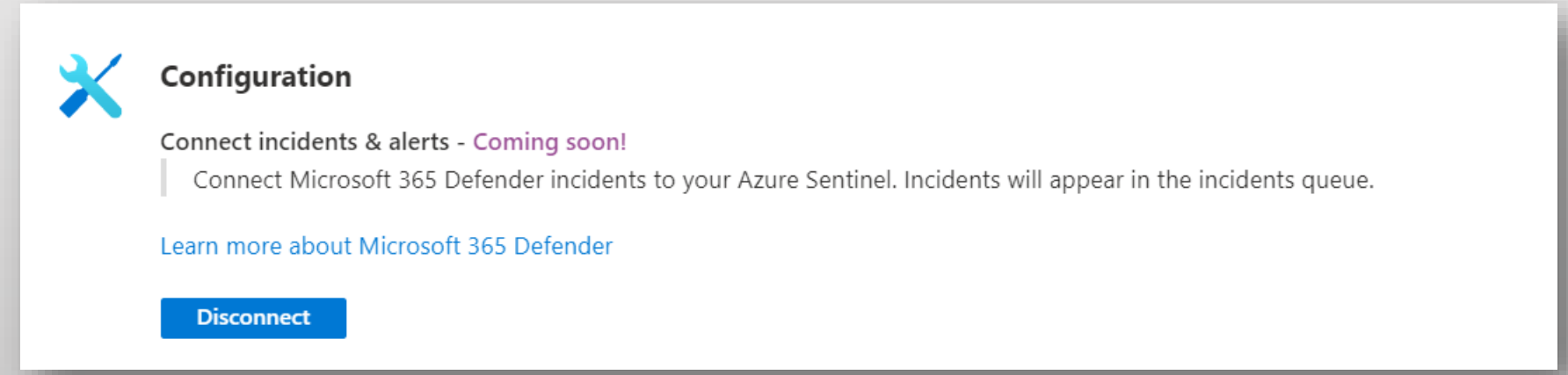




Azure Sentinel - M365 Defender Connector

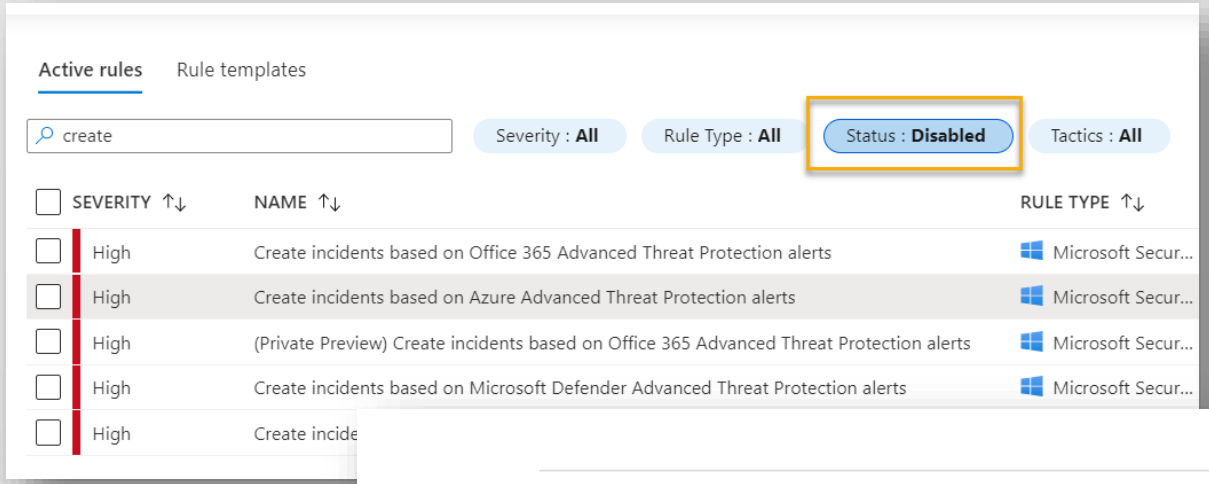
The Microsoft 365 Defender data connector for Azure Sentinel synchronizes alerts and incidents from the following solutions

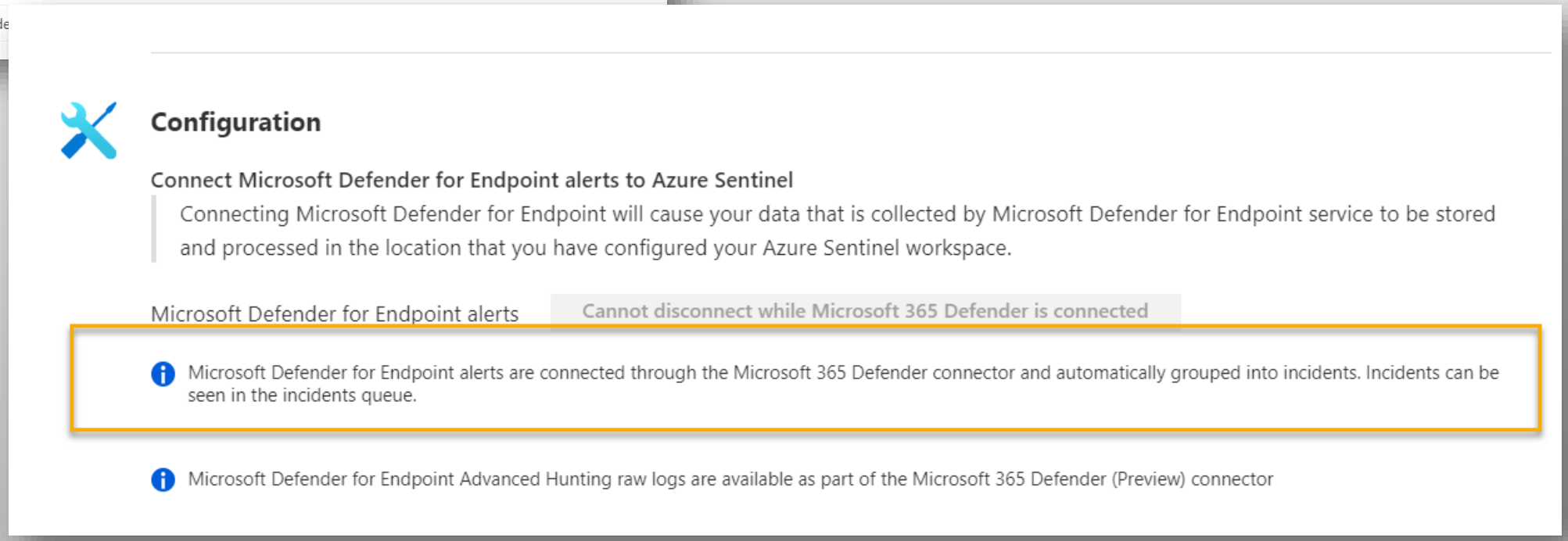
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Cloud App Security
- Microsoft Application Protection (Preview)



Azure Sentinel - M365 Defender Connector

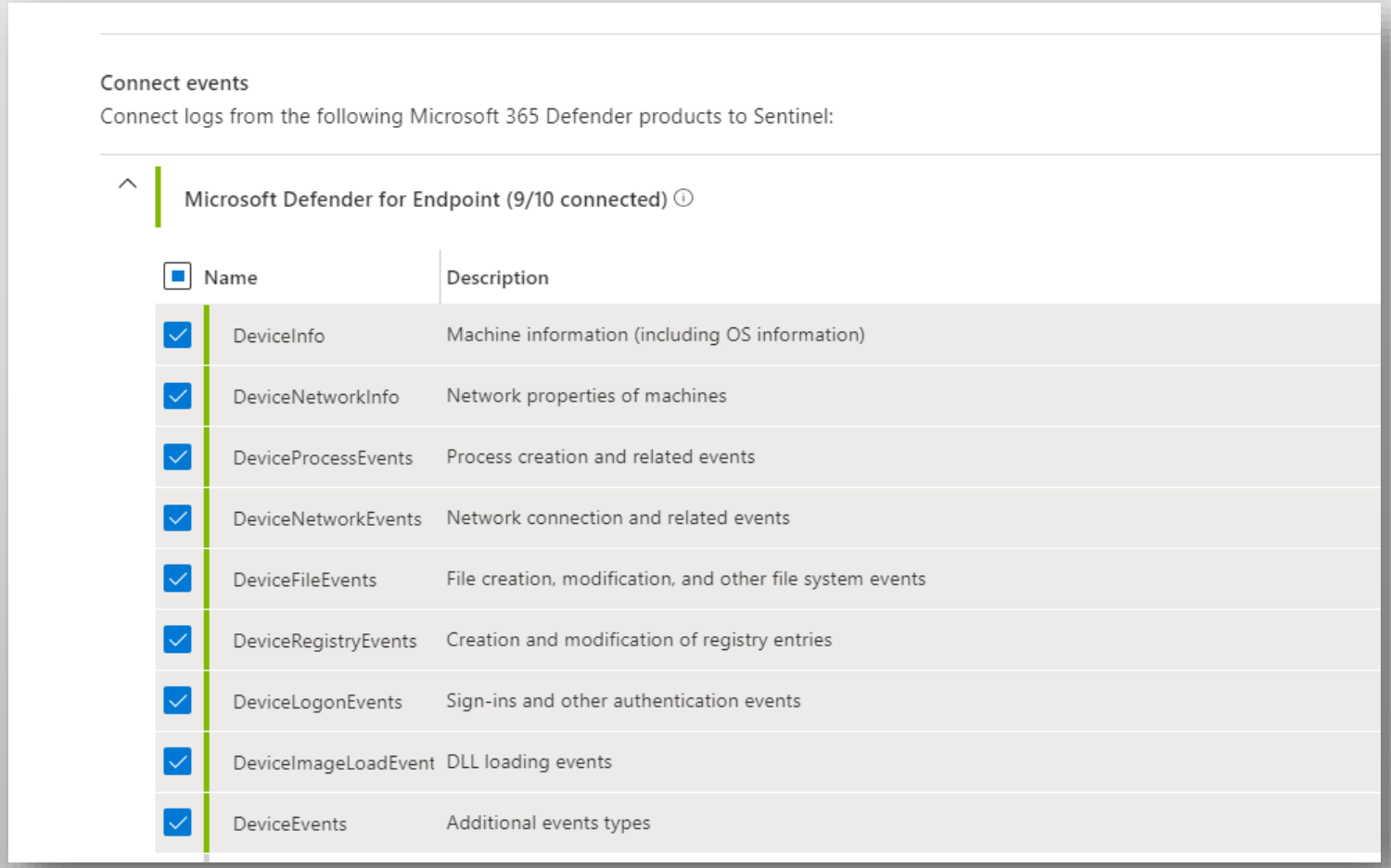
To avoid duplicate incidents, it is recommended to disable incident creation from the previous used connectors provided for the individual connectors.





Azure Sentinel - M365 Defender Connector

In addition to the incidents and alerts, the Microsoft 365 Defender connector also provides the capability to stream the raw logs into Azure Sentinel.



Azure Sentinel - M365 Defender Connector

Streaming the raw logs into Azure Sentinel covers the following use cases:

- You need to keep the logs for longer than 180 days (maximum data retention in Microsoft Defender for Endpoint is 180 days)
- Perform advanced hunting on logs beyond 30 days (maximum advanced hunting in Microsoft Defender for Endpoint is 30 days)
- You have a need to correlate Microsoft Defender for Endpoint data with other data that is ingested into Azure Sentinel for example Threat Intelligence data, DNS or logs from another 3rd party solution.

Important! Ingesting raw logs from Microsoft Defender for Endpoint or other M365 security solutions will result in additional Azure sentinel ingestion and log analytics storage costs.

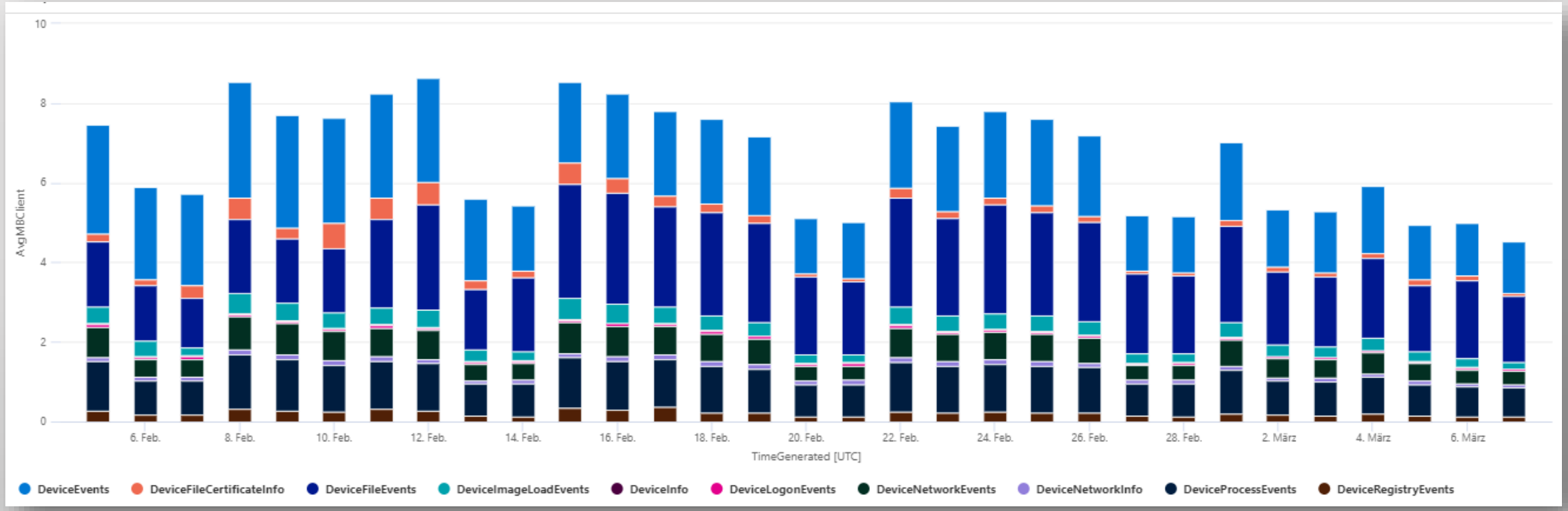
And also check out (**Update 2022**)

Ingest, Archive, Search, and Restore Data in Microsoft Sentinel

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/ingest-archive-search-and-restore-data-in-microsoft-sentinel/ba-p/3195126

Azure Sentinel - M365 Defender Connector

Example: Average volume in MB per client / day



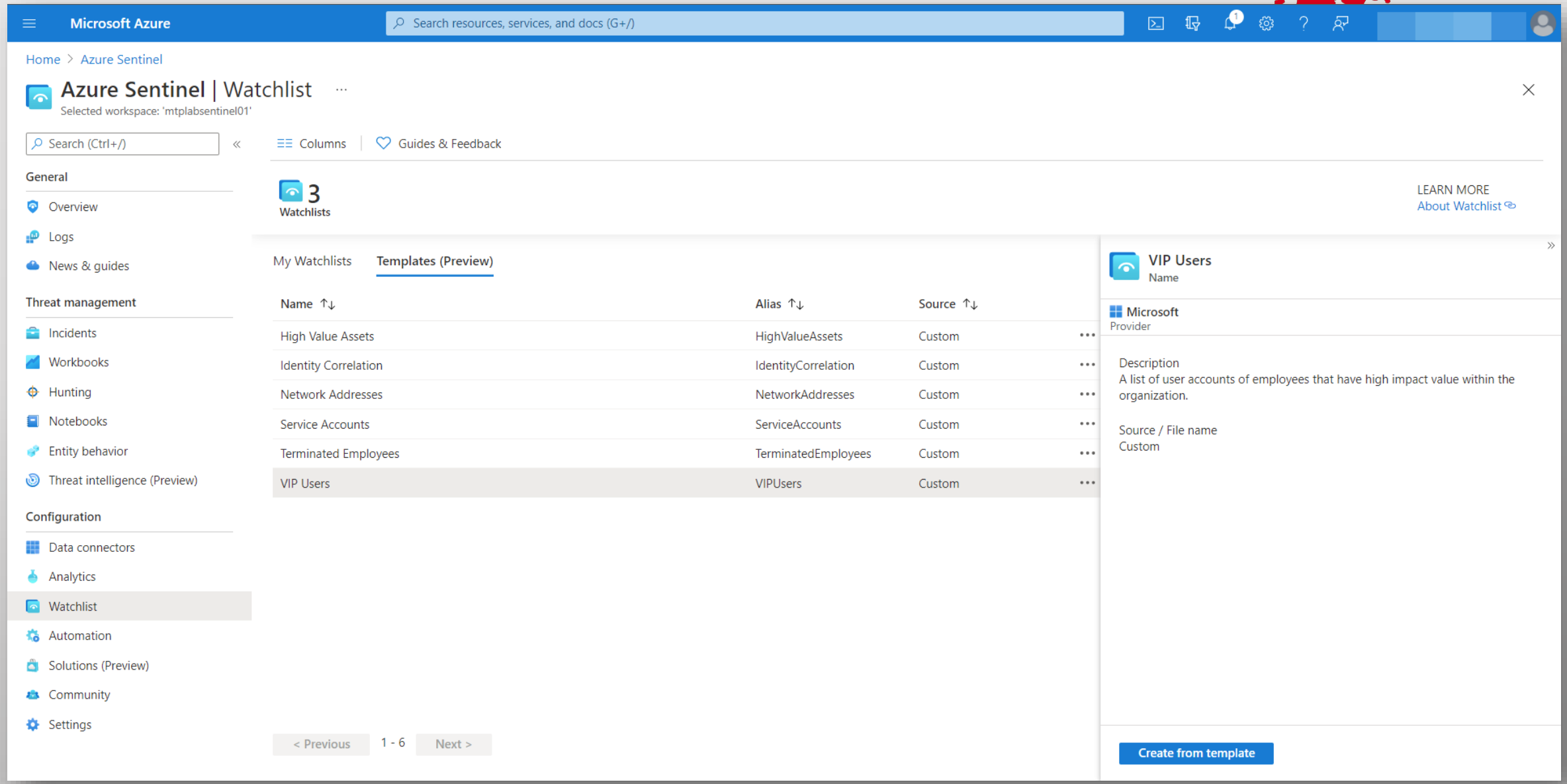
Microsoft Sentinel

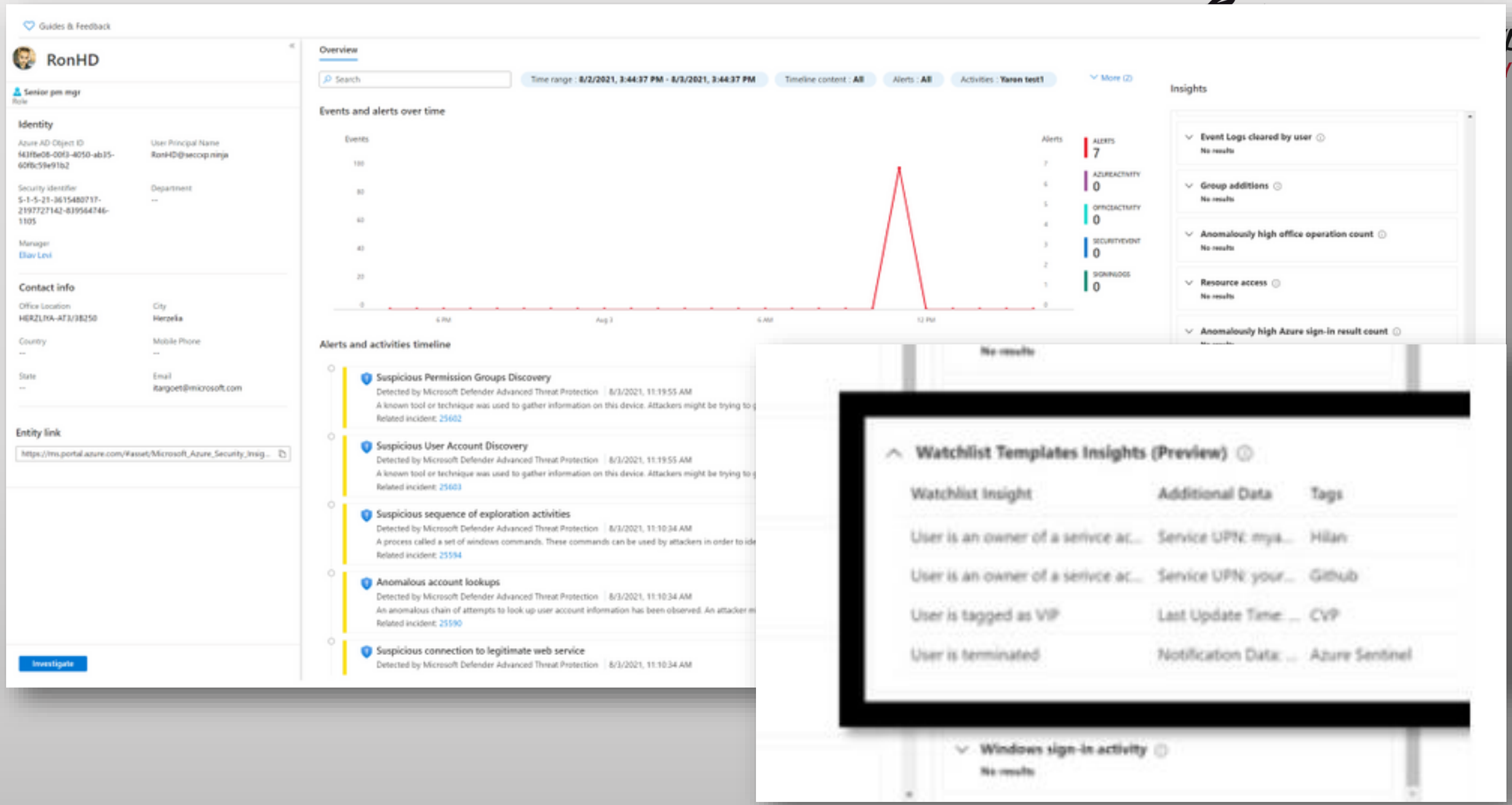
Watchlists

Azure Sentinel now provides built-in watchlist templates, which you can customize for your environment and use during investigations. After those watchlists are populated with data, you can correlate that data with analytics rules, view it in the entity pages and investigation graphs as insights, create custom uses such as to track VIP or sensitive users, and more.

Watchlist templates currently include:

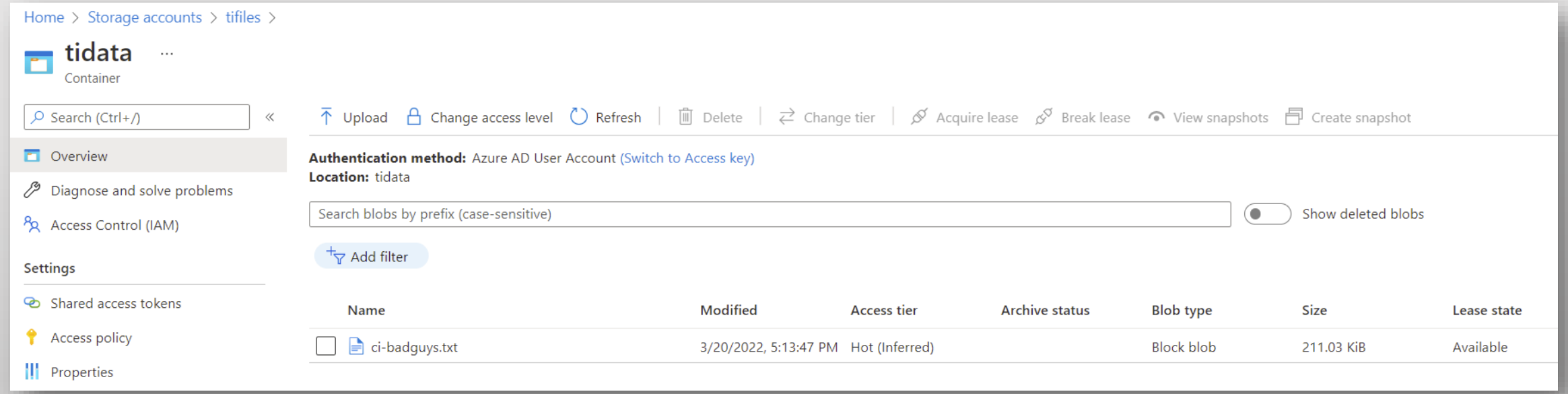
- VIP Users. A list of user accounts of employees that have high impact value in the organization.
- Terminated Employees. A list of user accounts of employees that have been, or are about to be, terminated.
- Service Accounts. A list of service accounts and their owners.
- Identity Correlation. A list of related user accounts that belong to the same person.
- High Value Assets. A list of devices, resources, or other assets that have critical value in the organization.
- Network Mapping. A list of IP subnets and their respective organizational contexts.

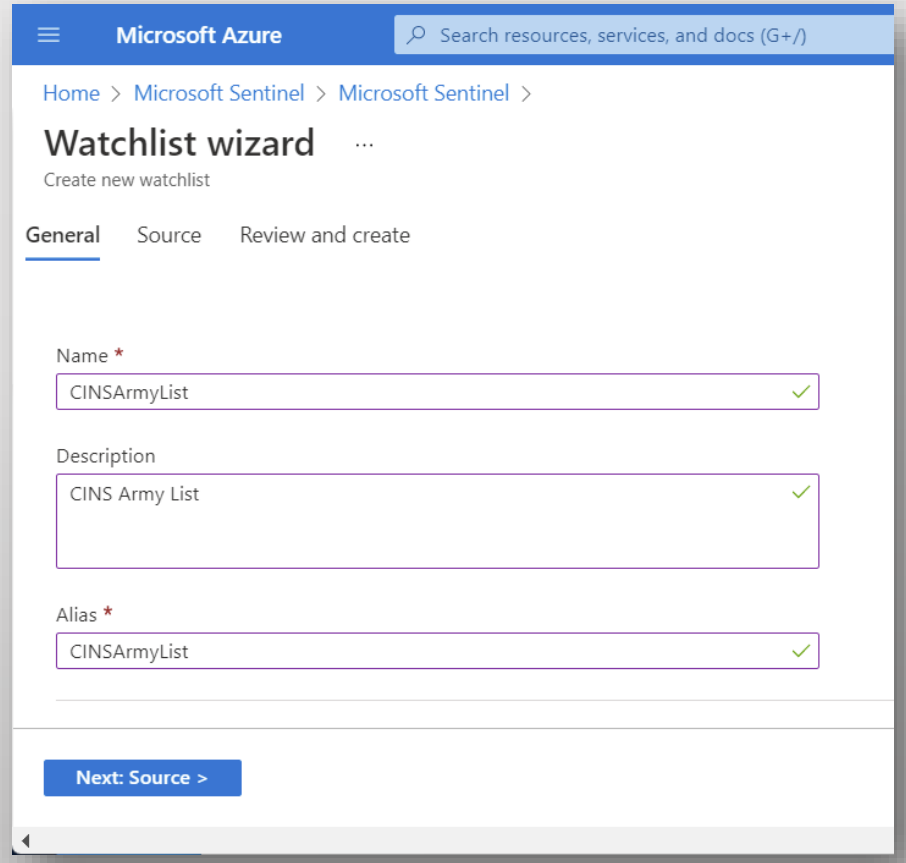

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel
Azure Sentinel | Watchlist
Selected workspace: 'mtplabsentinel01'
Search (Ctrl+/)
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence (Preview)
Configuration
Data connectors
Analytics
Watchlist
Automation
Solutions (Preview)
Community
Settings
3
Watchlists
LEARN MORE
About Watchlist
My Watchlists
Templates (Preview)
Name
Alias
Source
High Value Assets HighValueAssets Custom
Identity Correlation IdentityCorrelation Custom
Network Addresses NetworkAddresses Custom
Service Accounts ServiceAccounts Custom
Terminated Employees TerminatedEmployees Custom
VIP Users VIPUsers Custom
< Previous
1 - 6
Next >
VIP Users
Name
Microsoft
Provider
Description
A list of user accounts of employees that have high impact value within the organization.
Source / File name
Custom
Create from template

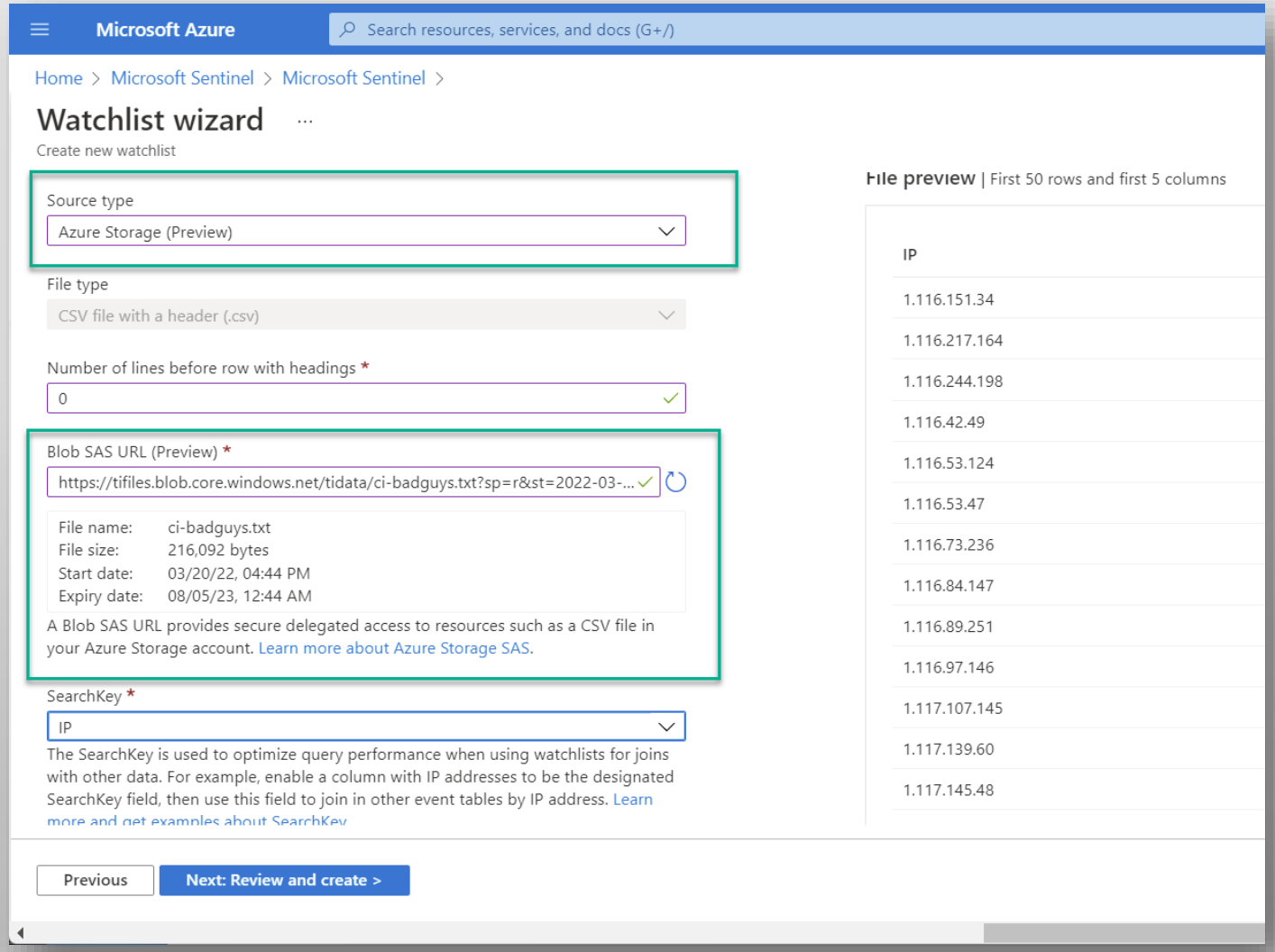

Guides & Feedback
RonHD
Senior pm mgr
Role
Identity
Azure AD Object ID
Security identifier
Department
Manager
Contact info
Office Location
City
Herzelia
Country
Mobile Phone
State
Email
Entity link
Investigate
Overview
Search
Time range : 8/2/2021, 3:44:37 PM - 8/3/2021, 3:44:37 PM
Timeline content : All
Alerts : All
Activities : Yaron test1
More (2)
Events and alerts over time
Events
Alerts
ALERTS 7
AZUREACTIVITY 0
OFFICEACTIVITY 0
SECURITYEVENT 0
SIGNINLOGS 0
Alerts and activities timeline
Suspicious Permission Groups Discovery
Detected by Microsoft Defender Advanced Threat Protection 8/3/2021, 11:19:55 AM
Related incident: 25602
Suspicious User Account Discovery
Detected by Microsoft Defender Advanced Threat Protection 8/3/2021, 11:19:55 AM
Related incident: 25603
Suspicious sequence of exploration activities
Detected by Microsoft Defender Advanced Threat Protection 8/3/2021, 11:10:34 AM
Related incident: 25594
Anomalous account lookups
Detected by Microsoft Defender Advanced Threat Protection 8/3/2021, 11:10:34 AM
Related incident: 25590
Suspicious connection to legitimate web service
Detected by Microsoft Defender Advanced Threat Protection 8/3/2021, 11:10:34 AM
Insights
Event Logs cleared by user
No results
Group additions
No results
Anomalously high office operation count
No results
Resource access
No results
Anomalously high Azure sign-in result count
No results
Watchlist Templates Insights (Preview)
Watchlist Insight
Additional Data
Tags
User is an owner of a serivce ac...
Service UPN: mya...
Hilan
User is an owner of a serivce ac...
Service UPN: your...
GitHub
User is tagged as VIP
Last Update Time: ...
CVP
User is terminated
Notification Data: ...
Azure Sentinel
Windows sign-in activity
No results

Create a large watchlist from file in Azure Storage (public preview)

Create a watchlist from a large file that's up to **500 MB** in size by uploading the file to your Azure Storage account. When you add the watchlist to your workspace, you provide a shared access signature URL. Microsoft Sentinel uses the shared access signature URL to retrieve the watchlist data from Azure Storage.

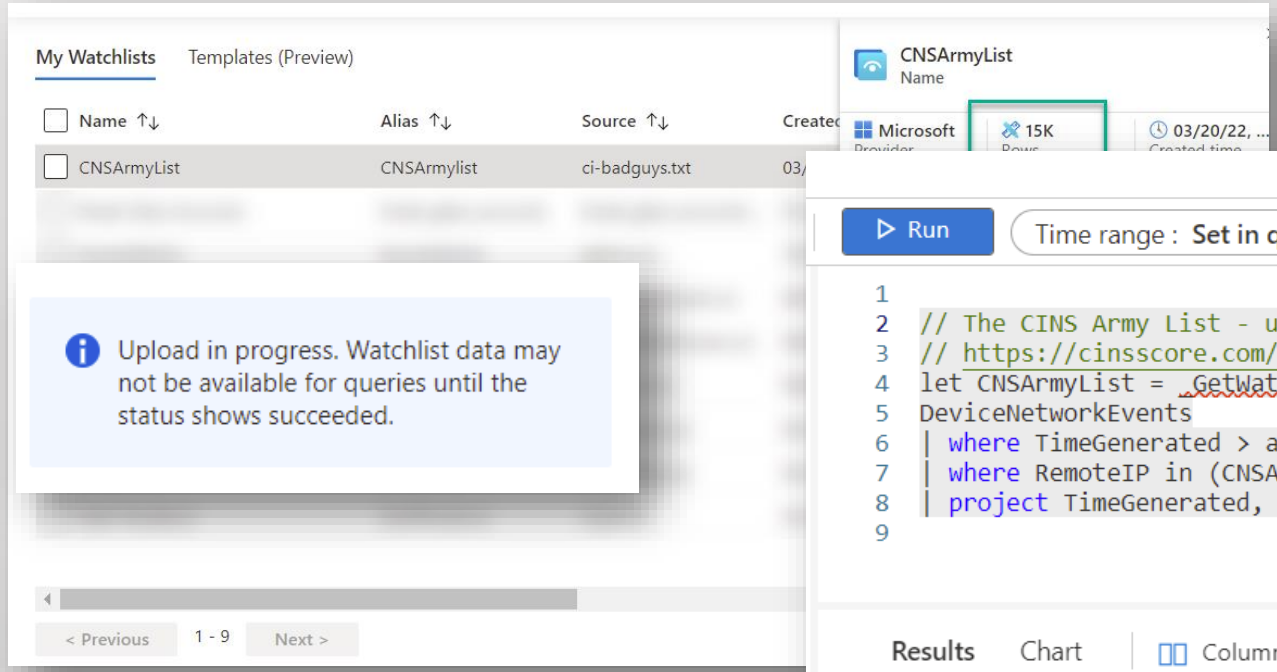


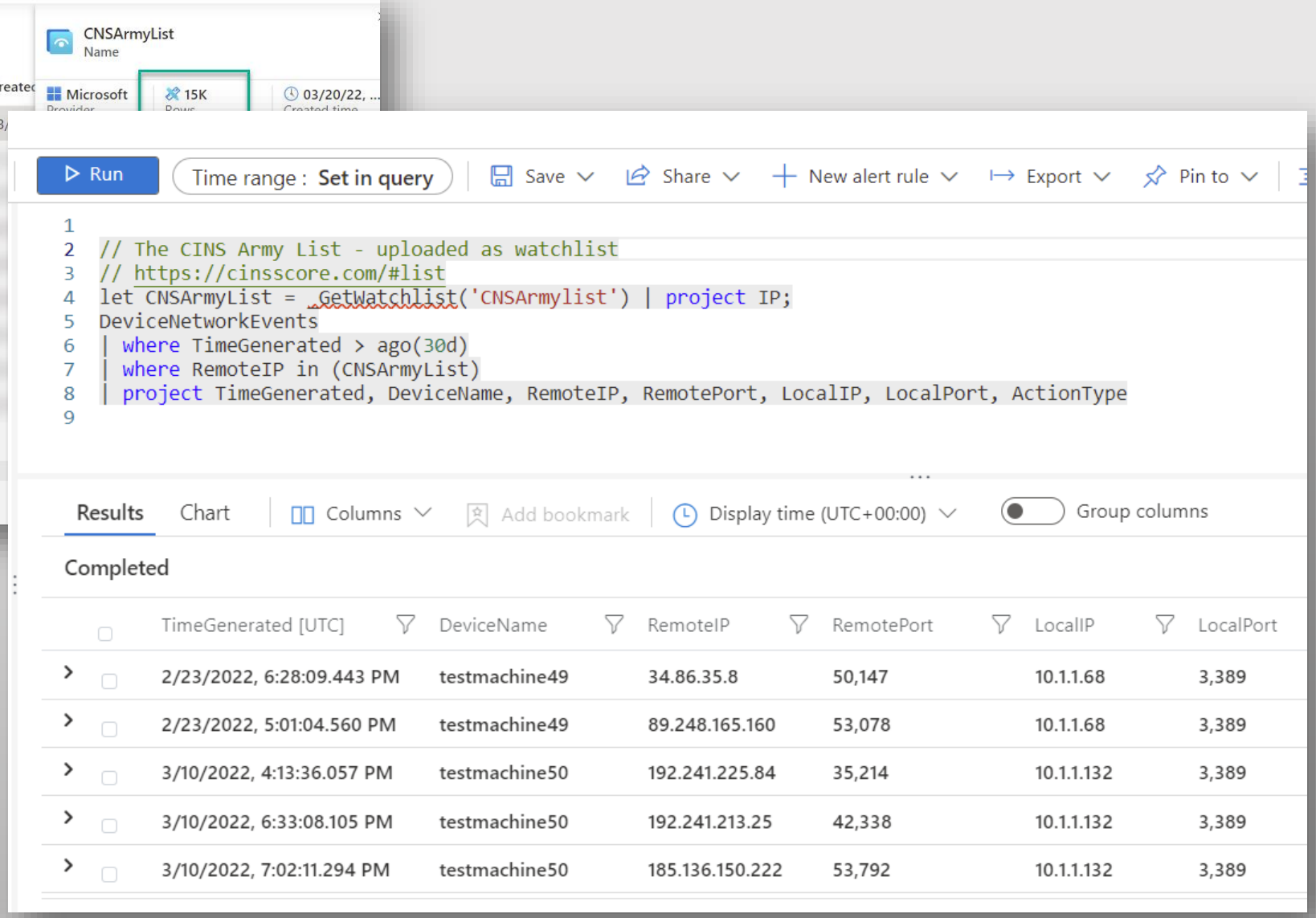

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Watchlist wizard
Create new watchlist
General
Source
Review and create
Name *
CINSArmyList
Description
CINS Army List
Alias *
CINSArmyList
Next: Source >


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Watchlist wizard
Create new watchlist
Source type
Azure Storage (Preview)
File type
CSV file with a header (.csv)
Number of lines before row with headings *
0
Blob SAS URL (Preview) *
https://tifiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-03-...
File name: ci-badguys.txt
File size: 216,092 bytes
Start date: 03/20/22, 04:44 PM
Expiry date: 08/05/23, 12:44 AM
A Blob SAS URL provides secure delegated access to resources such as a CSV file in your Azure Storage account. Learn more about Azure Storage SAS.
SearchKey *
IP
The SearchKey is used to optimize query performance when using watchlists for joins with other data. For example, enable a column with IP addresses to be the designated SearchKey field, then use this field to join in other event tables by IP address. Learn more and get examples about SearchKey
File preview | First 50 rows and first 5 columns
IP
1.116.151.34
1.116.217.164
1.116.244.198
1.116.42.49
1.116.53.124
1.116.53.47
1.116.73.236
1.116.84.147
1.116.89.251
1.116.97.146
1.117.107.145
1.117.139.60
1.117.145.48
Previous
Next: Review and create >

Workplace Ninja User Group Switzerland

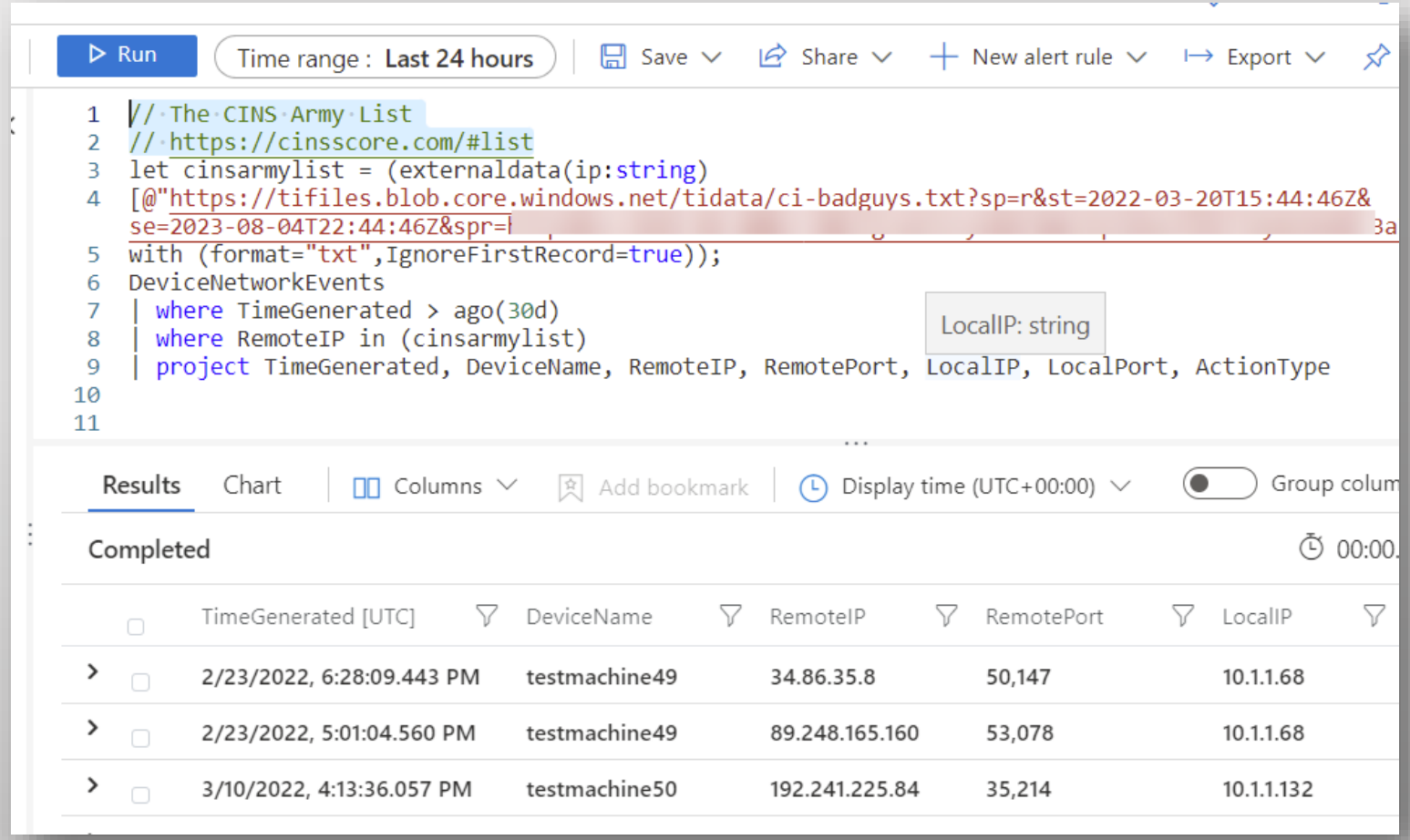
Once we imported the data stored on Azure Storage, we can use the watchlist



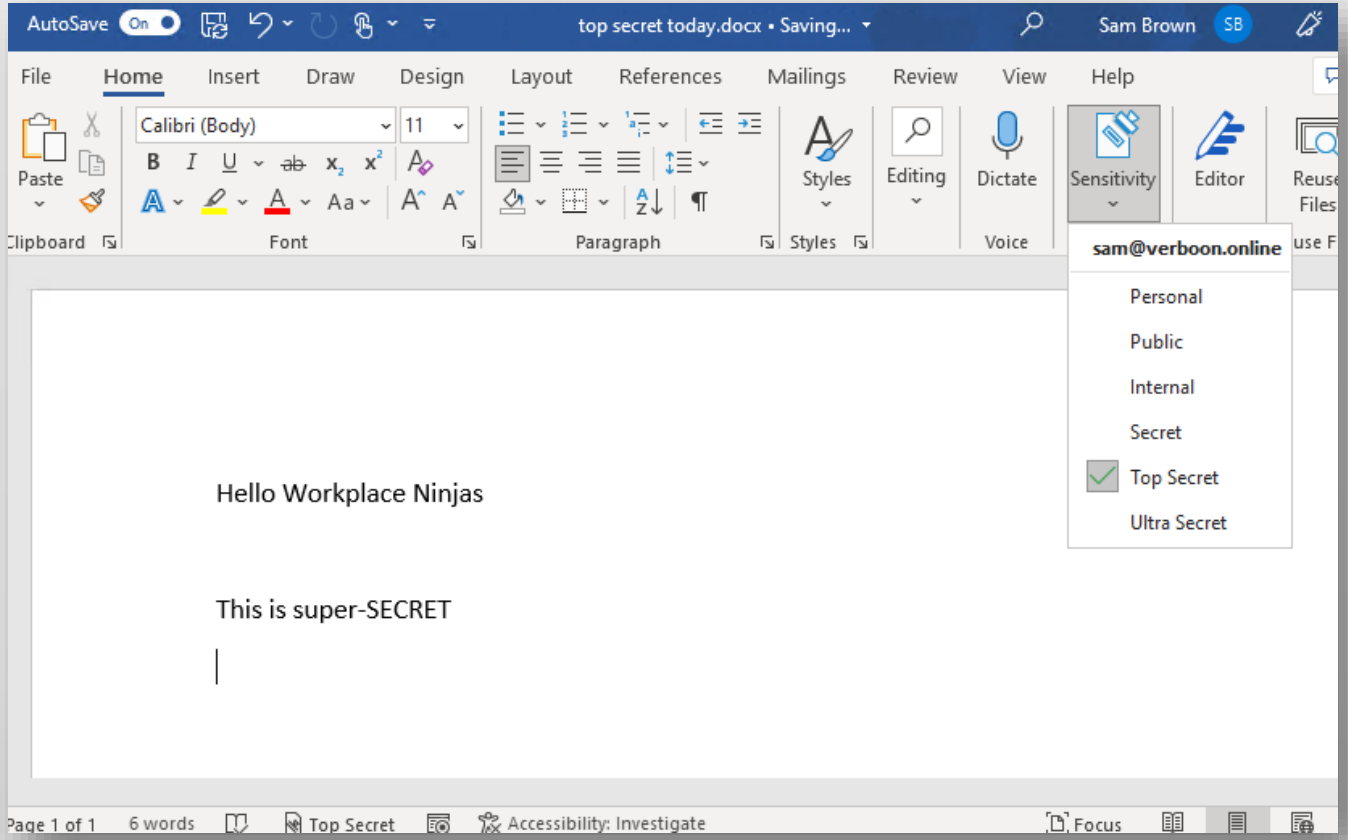


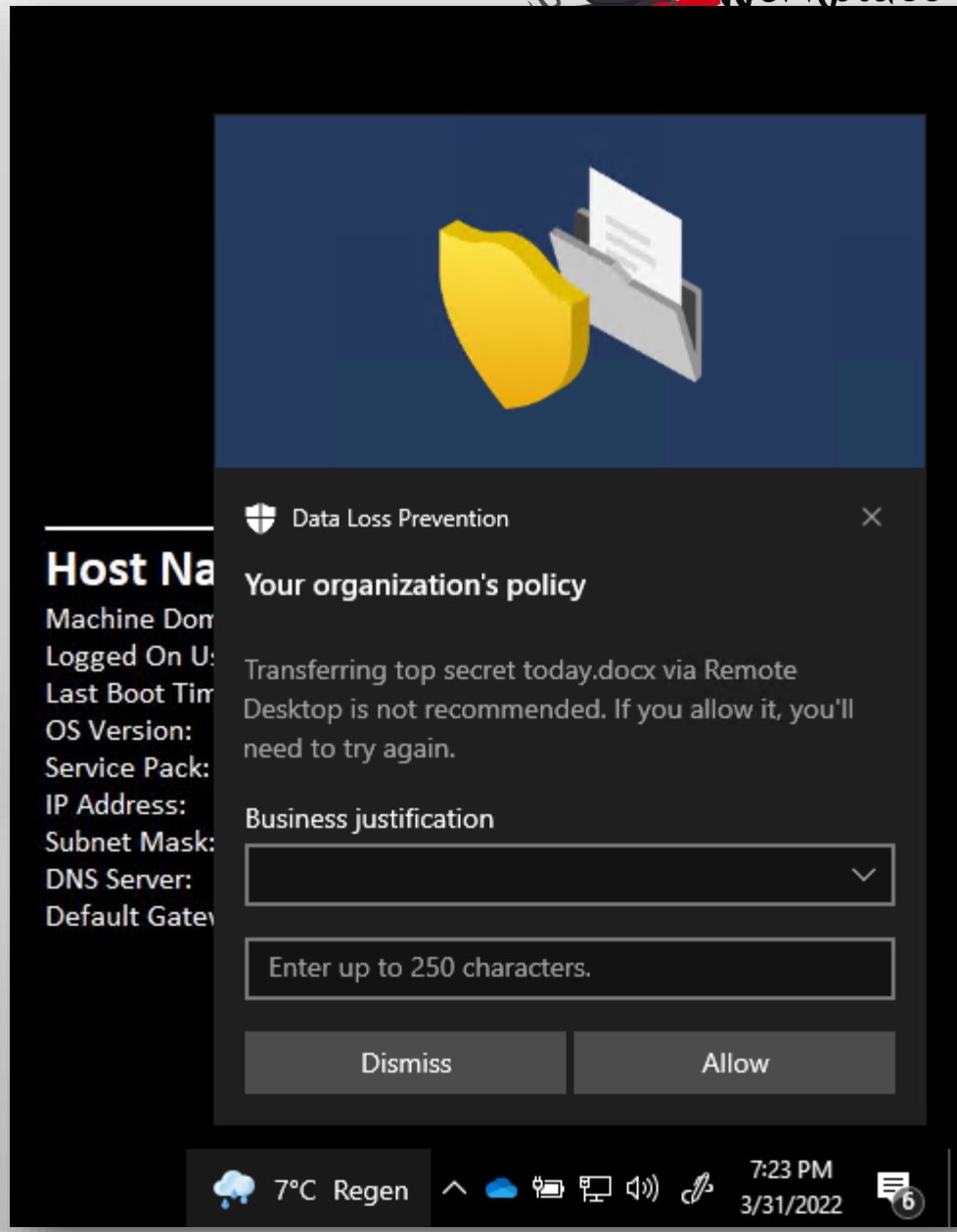

```
AzureActivity
| where CategoryValue == "Administrative"
| where OperationNameValue has "/WATCHLISTS"
```

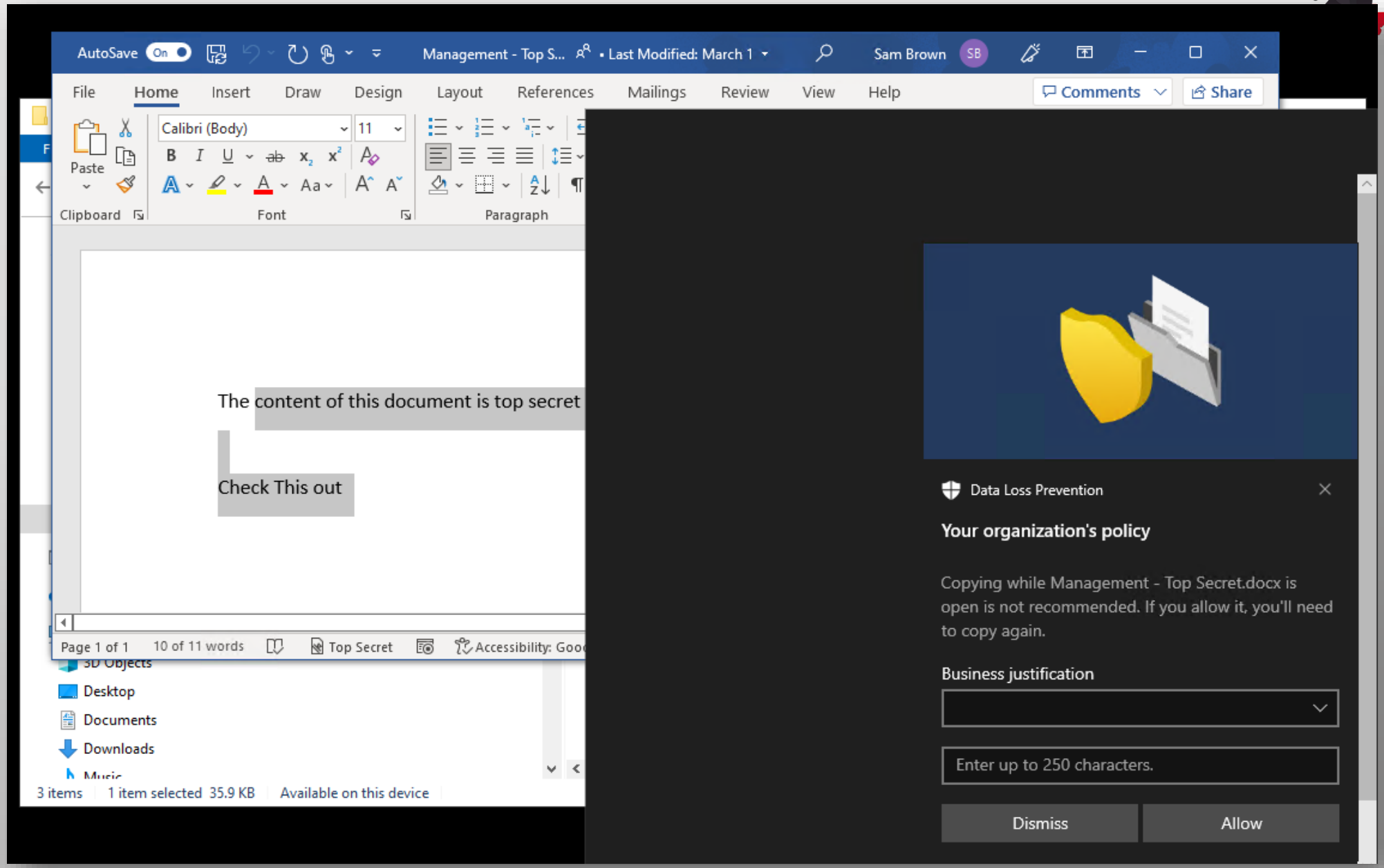
And of course, we can also reference the file directly with externaldata

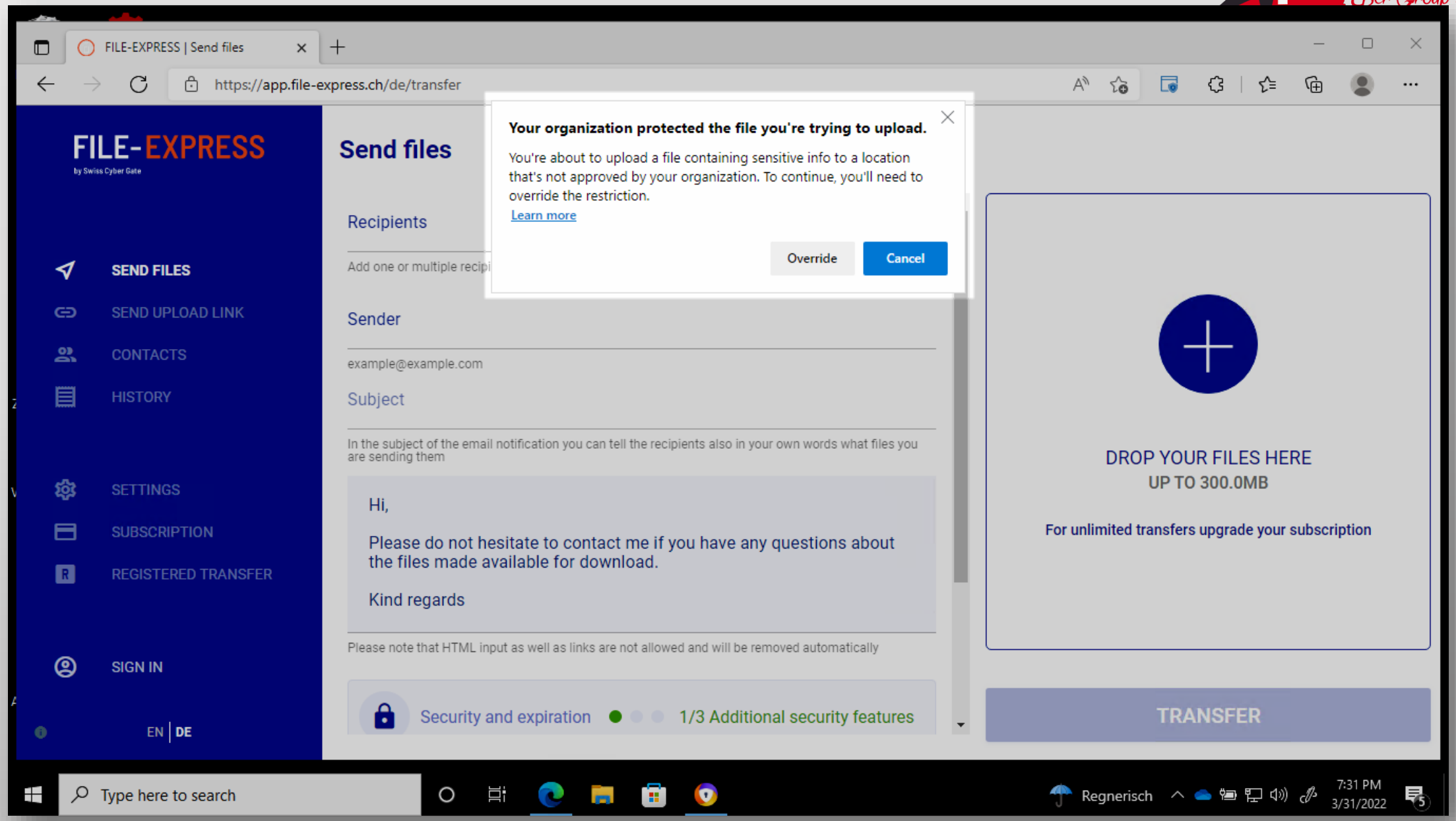


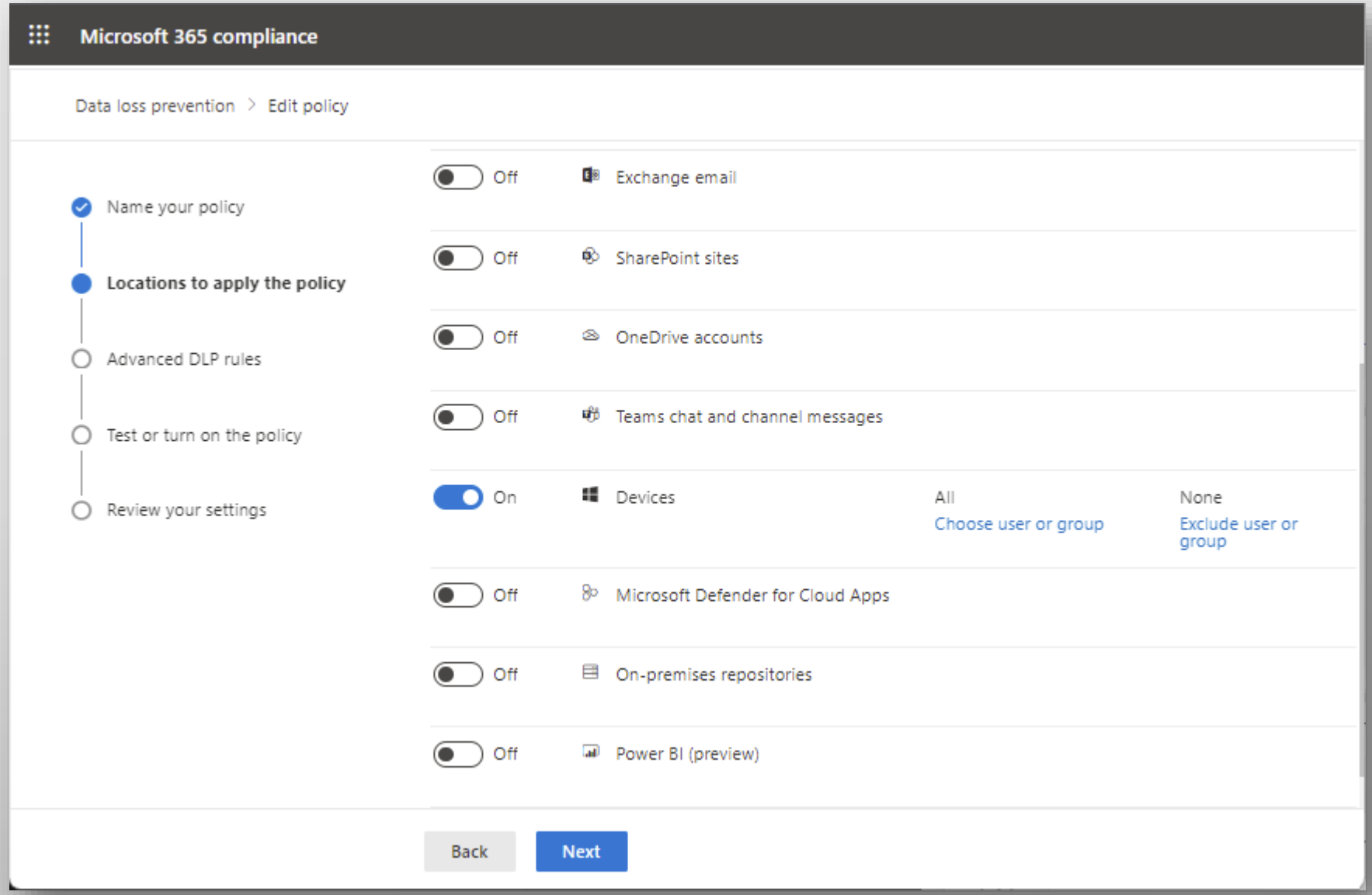
Endpoint DLP

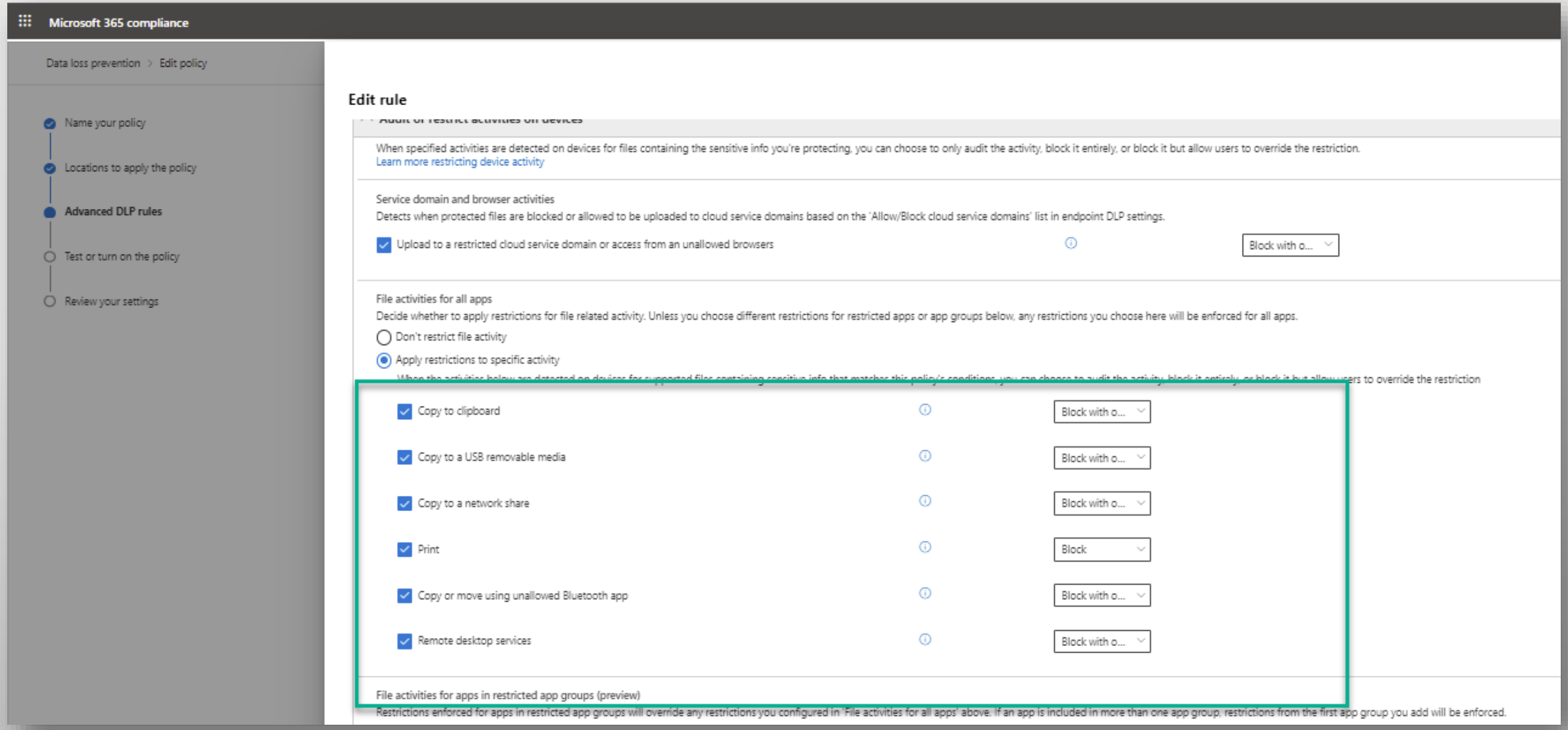







FILE-EXPRESS | Send files
https://app.file-express.ch/de/transfer
FILE-EXPRESS
by Swiss Cyber Gate
SEND FILES
SEND UPLOAD LINK
CONTACTS
HISTORY
SETTINGS
SUBSCRIPTION
REGISTERED TRANSFER
SIGN IN
EN | DE
Send files
Your organization protected the file you're trying to upload.
You're about to upload a file containing sensitive info to a location that's not approved by your organization. To continue, you'll need to override the restriction.
Learn more
Override
Cancel
Recipients
Add one or multiple recipi
Sender
example@example.com
Subject
In the subject of the email notification you can tell the recipients also in your own words what files you are sending them
Hi,
Please do not hesitate to contact me if you have any questions about the files made available for download.
Kind regards
Please note that HTML input as well as links are not allowed and will be removed automatically
Security and expiration
1/3 Additional security features
DROP YOUR FILES HERE
UP TO 300.0MB
For unlimited transfers upgrade your subscription
TRANSFER
Type here to search
Regnerisch
7:31 PM
3/31/2022





Microsoft 365 compliance

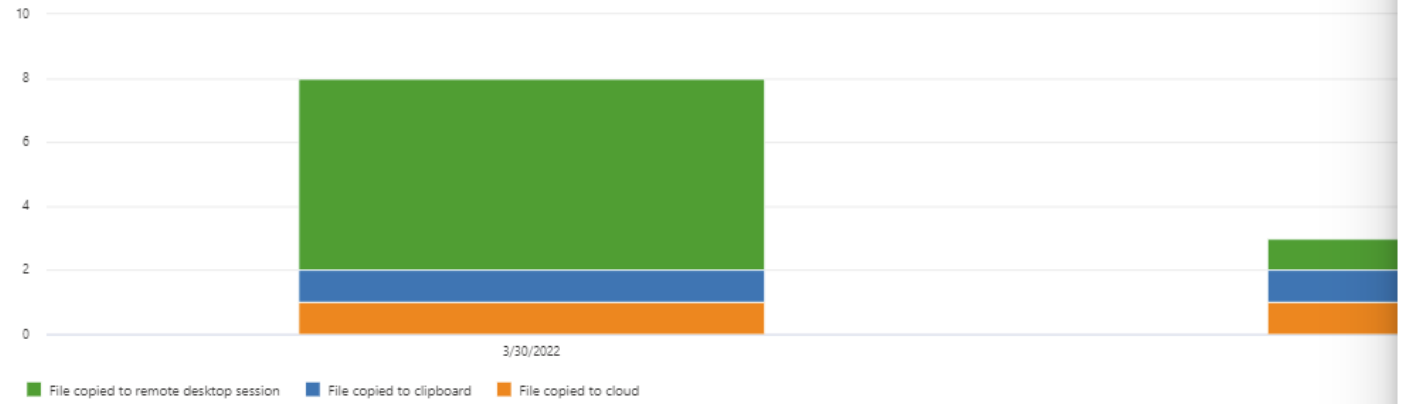
Data classification

Overview | Trainable classifiers | Sensitive info types | Exact data matches | Content explorer | Activity explorer

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, Sha
soon. Learn more

Built-in filters | Reset | Filters

Date: 3/24/2022-3/31/2022 | Activity: FileCopiedToRemoteDesktopSession, +2 | Location: Endpoint | User: Any | Sensitivity label: Any



Export | Refresh

Activity	File	Location	User	Happened
File copied to cloud	C:\Users\sam\avmtplab\DLP - Management\Management - Secret....	Endpoint devices	sam@verboon.online	Mar 31, 2022 7:31 PM
File copied to clipboard	C:\Users\sam\avmtplab\DLP - Management\Management - Top Se...	Endpoint devices	sam@verboon.online	Mar 31, 2022 7:29 PM
File copied to remote desktop session	C:\Users\sam\OneDrive - avmtplab\top secret today.docx	Endpoint devices	sam@verboon.online	Mar 31, 2022 7:23 PM
File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:58 PM
File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:57 PM
File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:54 PM

Next item

File copied to cloud

Activity details

Activity
File copied to cloud

Happened
Mar 31, 2022 7:31 PM

Client IP
83.78.30.236

How applied
None

Label event type
None

Enforcement mode
Warn

Target domain
app.file-express.ch

About this item

File
Management - Secret.docx

User
sam@verboon.online

File extension
docx

File size
64 KB

Sensitivity label
Secret

Sensitive info type

DLP policy
DEMO - Protect Secret - Endpoint

DLP rule
SecretDocumentDevice

Sha1
3a2b763f329116bc667f6b0abadcd6d476d1a088

Sha256
f6a67ead4df17c906fe8b5ded4ab10fc66ac4c59d872a4b55e40fa5a58d12296

Location details

Location
Endpoint devices

Parent
C:\Users\sam\avmtplab\DLP - Management

File path

Microsoft Defender for Endpoint

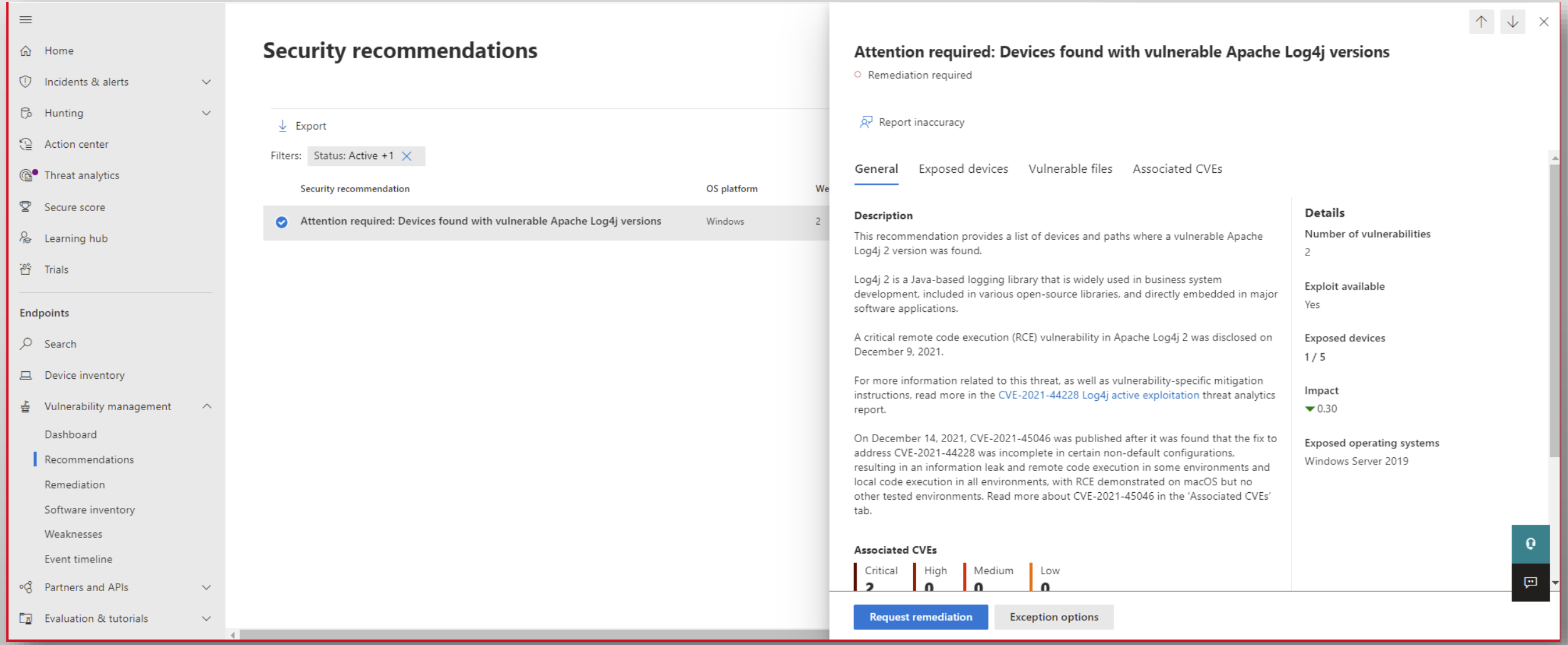
Log4J – Detection & Remediation

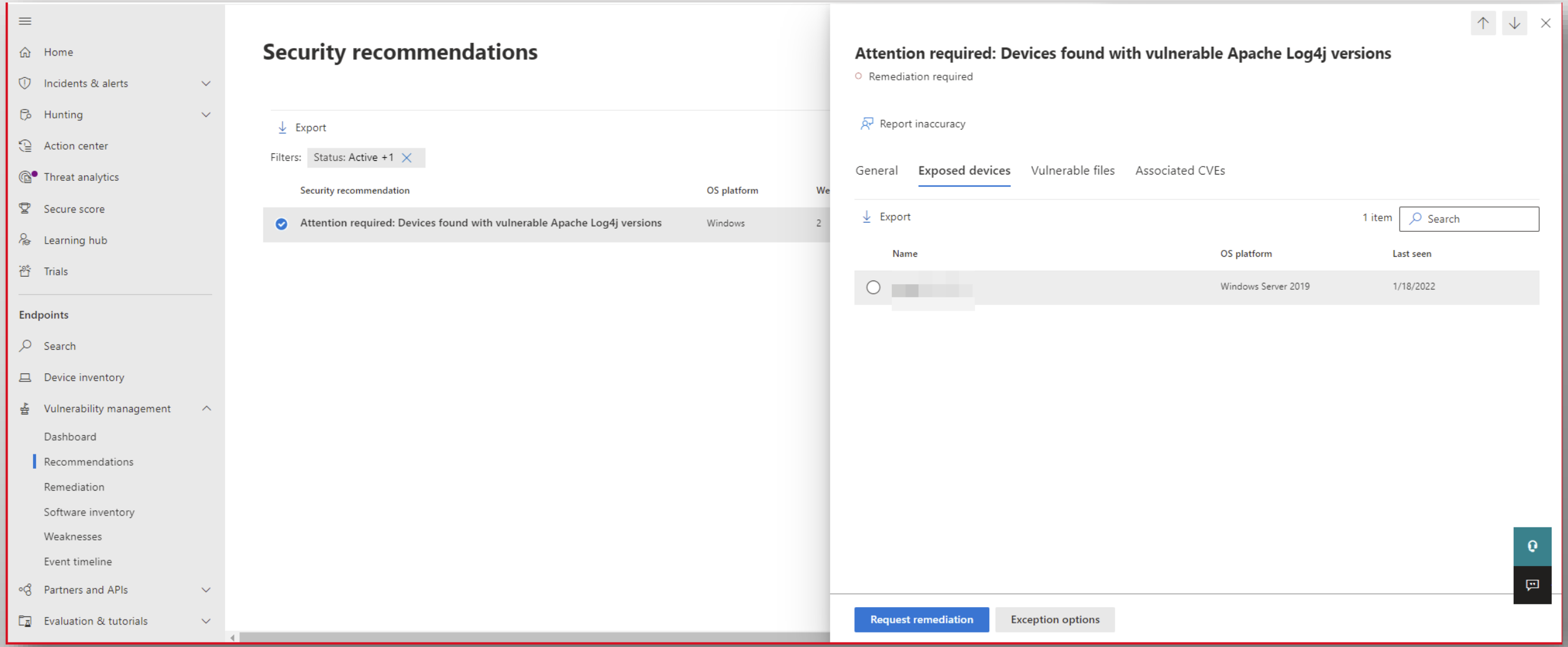
Microsoft Defender for Endpoint Log4J remeidation

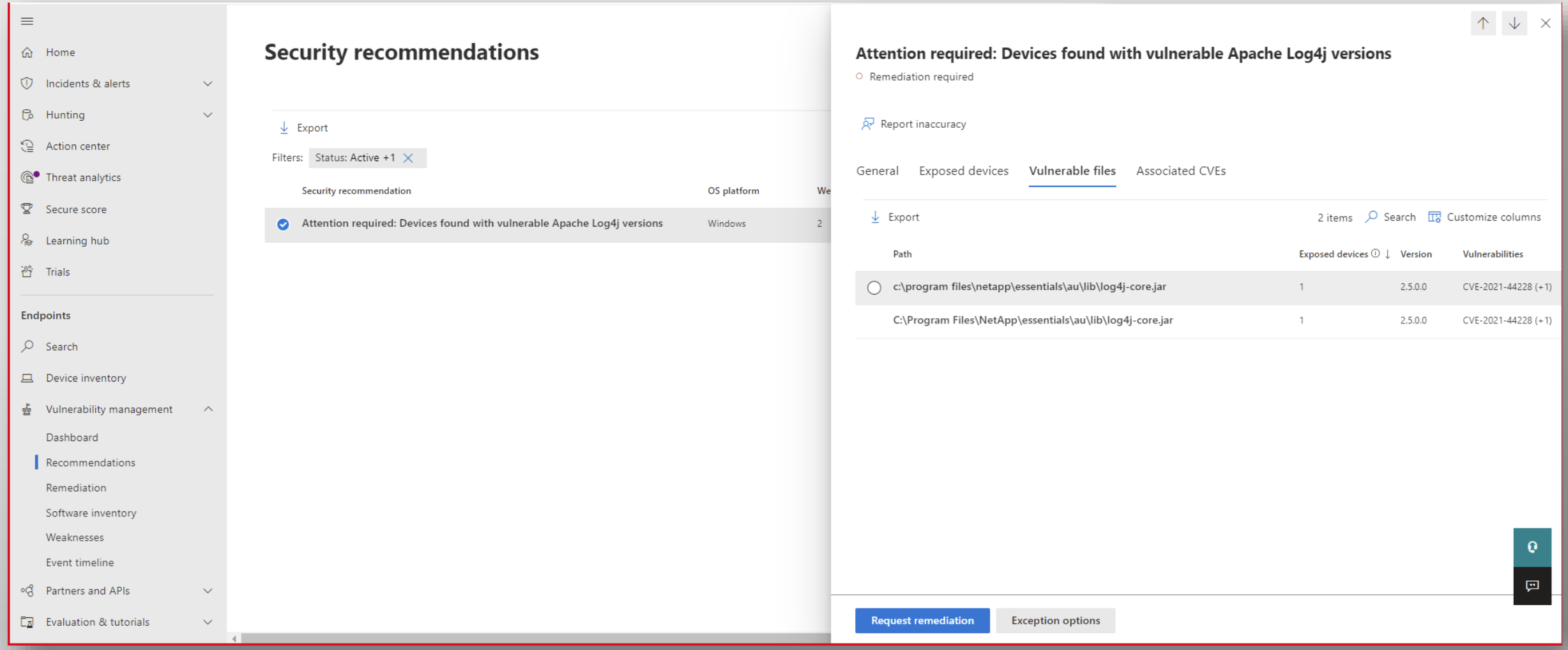
Threat and vulnerability management automatically and seamlessly identifies devices affected by the Log4j vulnerabilities and the associated risk in the environment and significantly reduces time-to-mitigate.

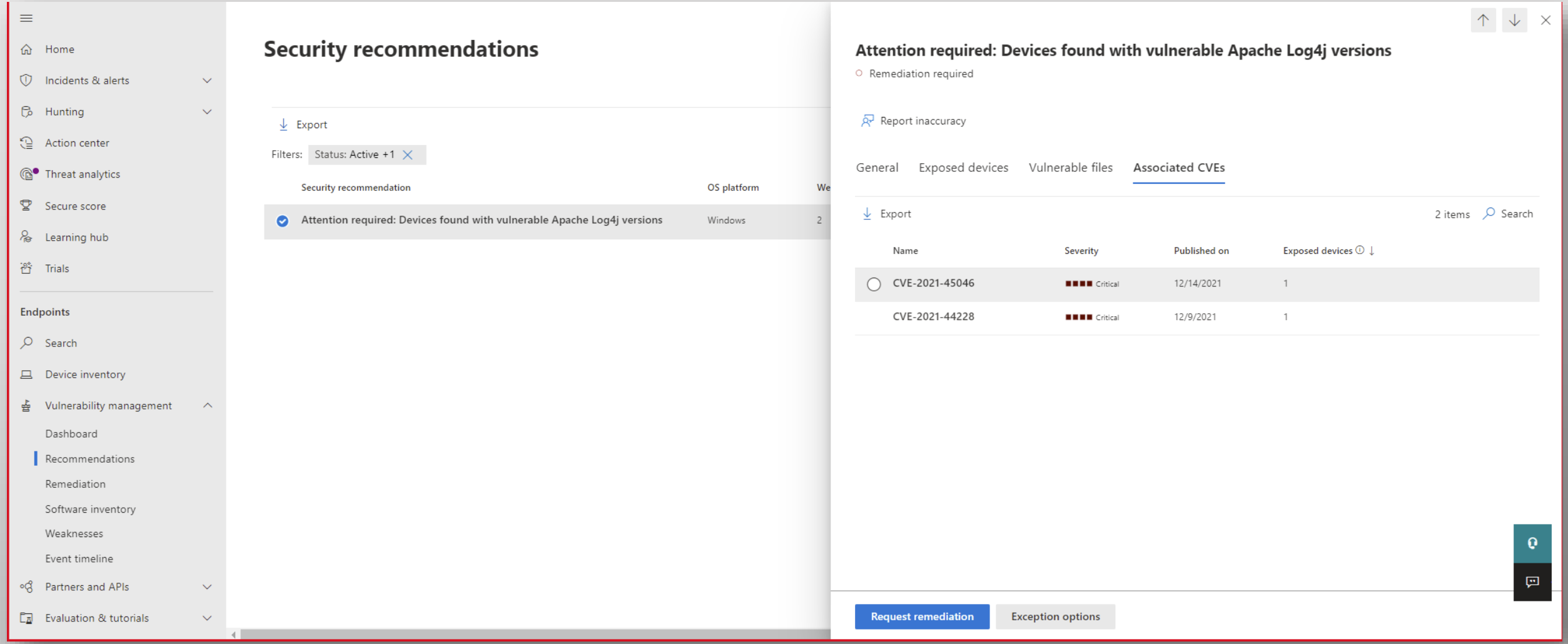
- Discovery of vulnerable Log4j library components (paths) on devices
- Discovery of vulnerable installed applications that contain the Log4j library on devices
- A dedicated Log4j dashboard that provides a consolidated view of various findings across vulnerable devices, vulnerable software, and vulnerable files
- Introduction of a new schema in advanced hunting, DeviceTvmSoftwareEvidenceBeta, which surfaces file-level findings from the disk and provides the ability to correlate them with additional context in advanced hunting.

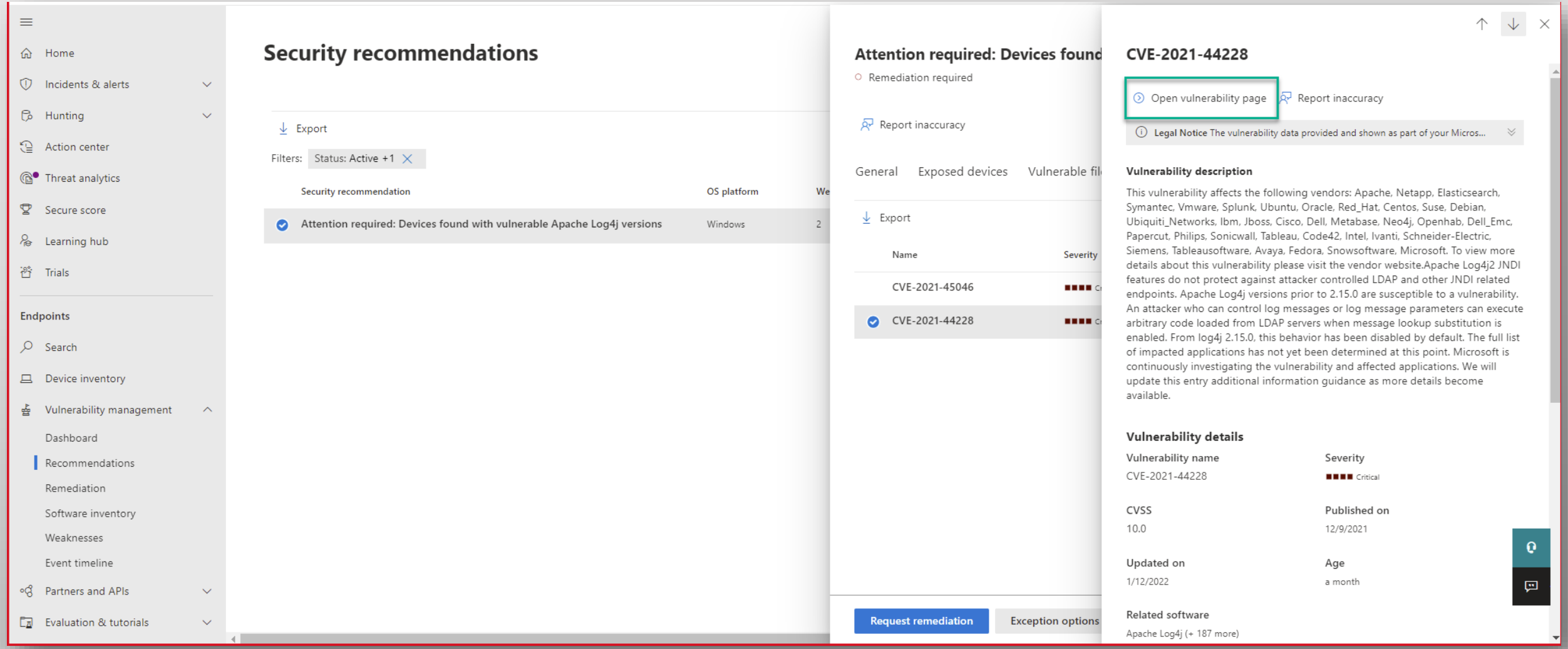
As of January 20, 2022, threat and vulnerability management can discover vulnerable Log4j libraries, including Log4j files and other files containing Log4j, packaged into Uber-JAR files. This capability is supported on Windows 10, Windows 11, Windows Server 2019, and Windows Server 2022. It is also supported on Windows Server 2012 R2 and Windows Server 2016 using the Microsoft Defender for Endpoint solution for earlier Windows server versions.

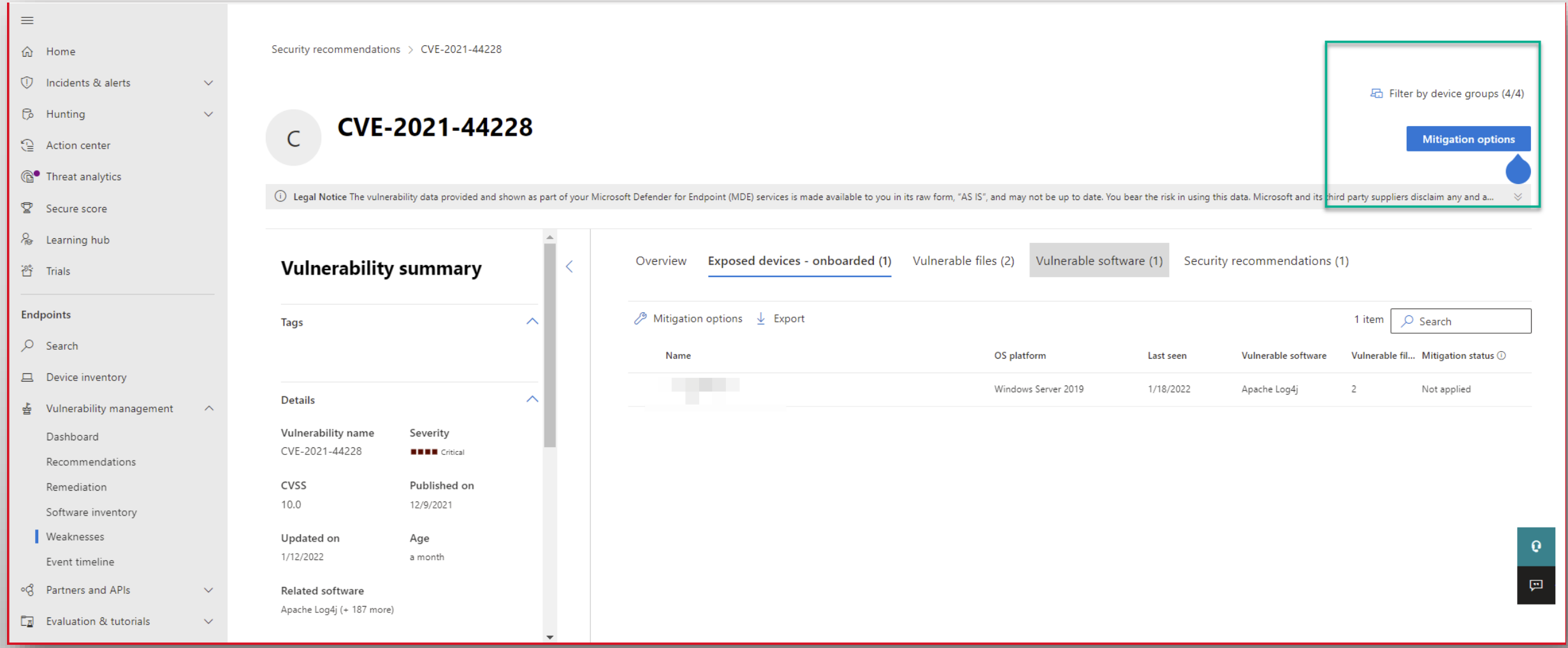


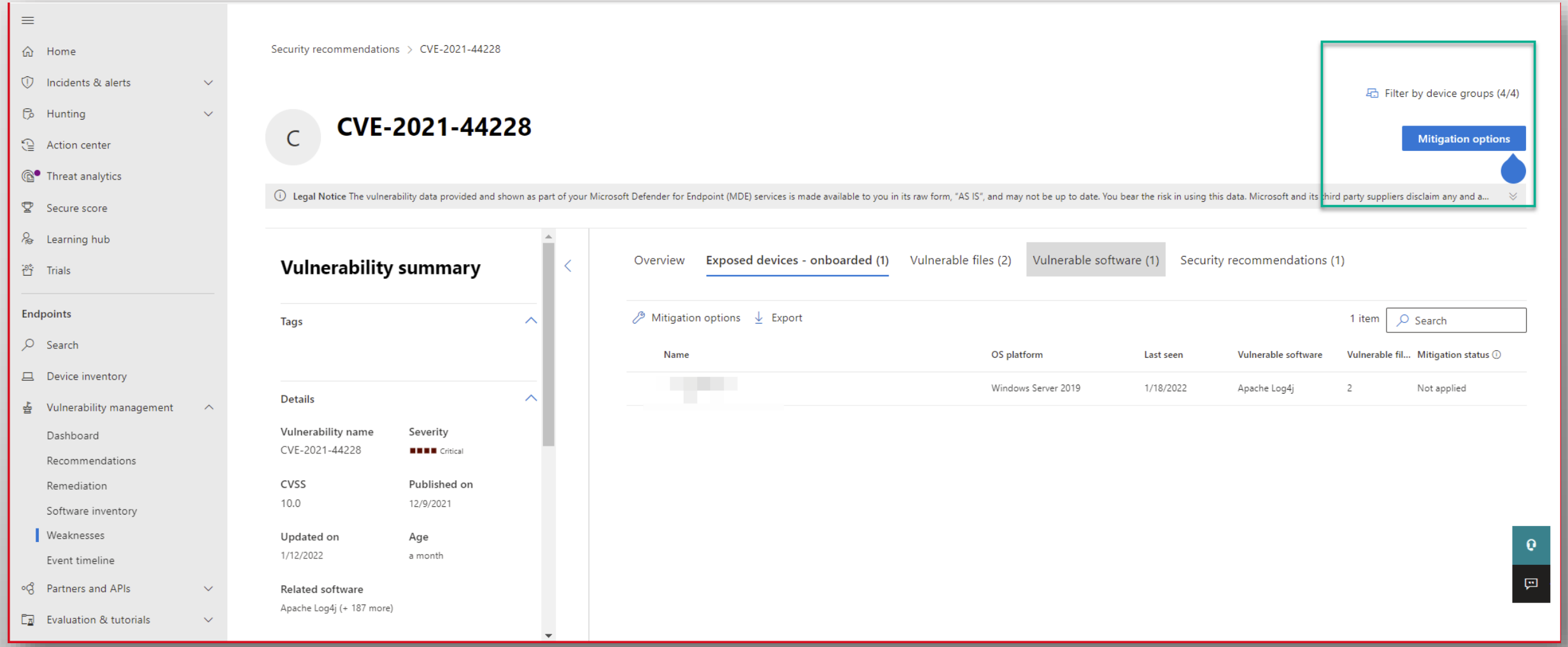


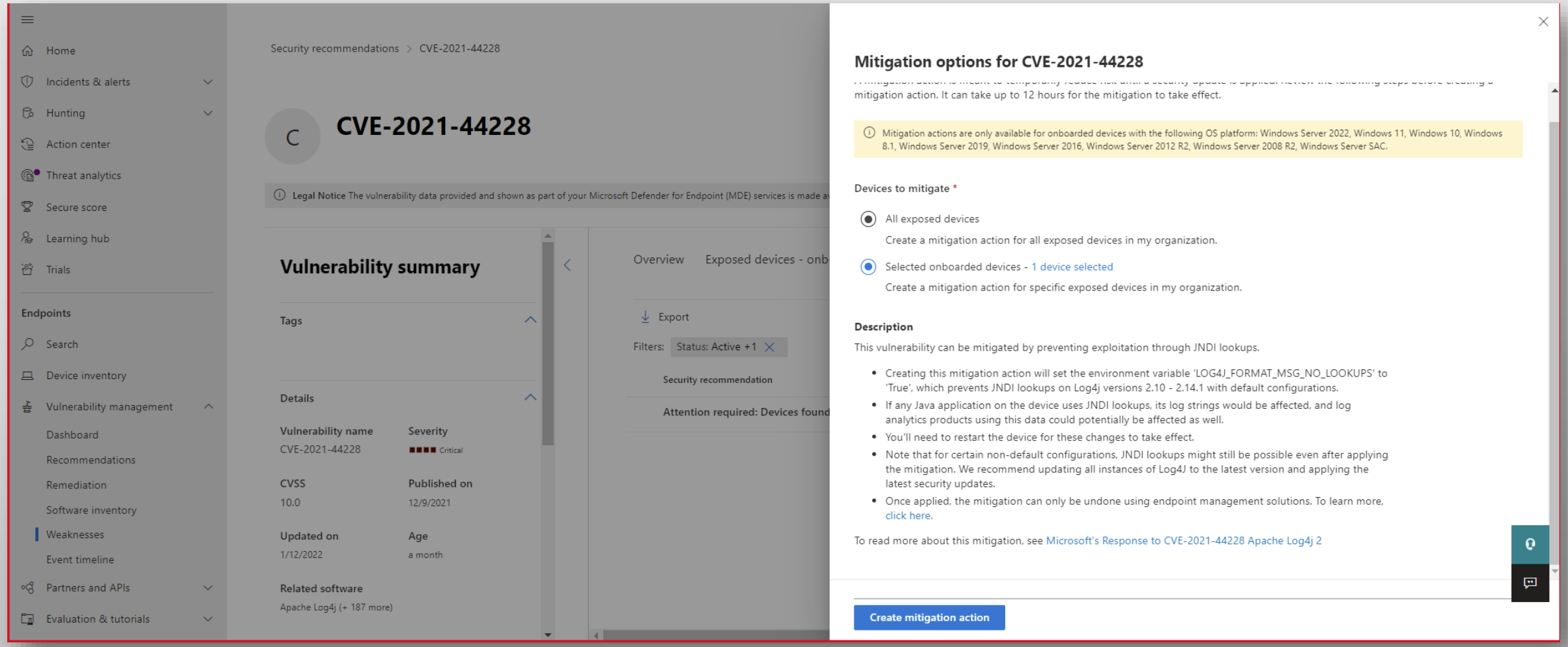


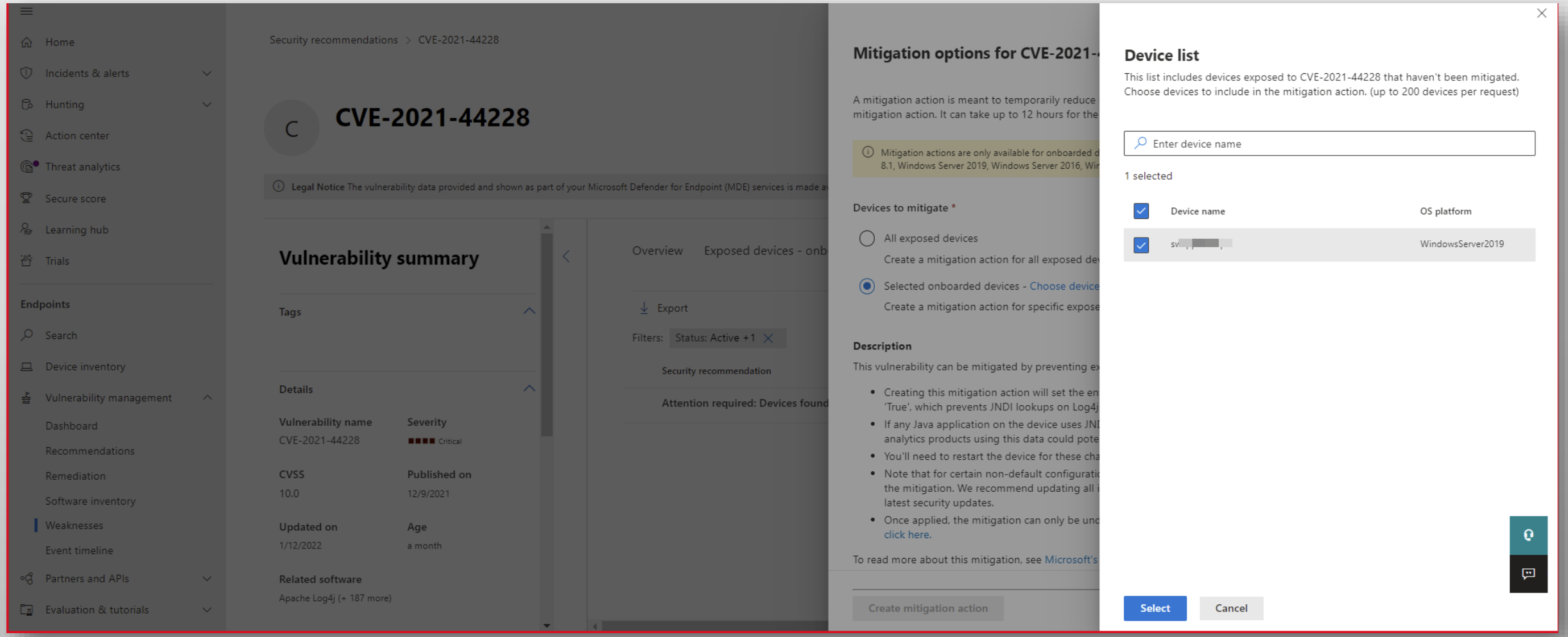


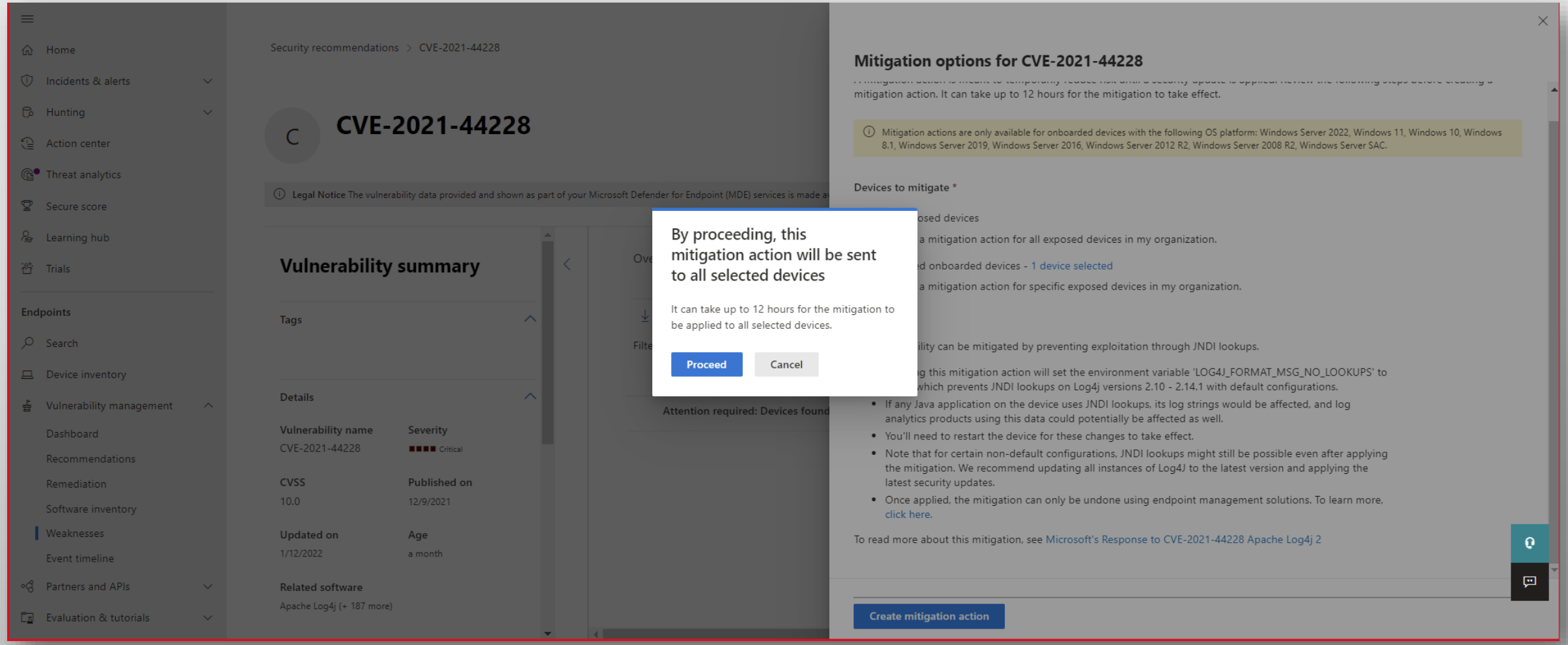




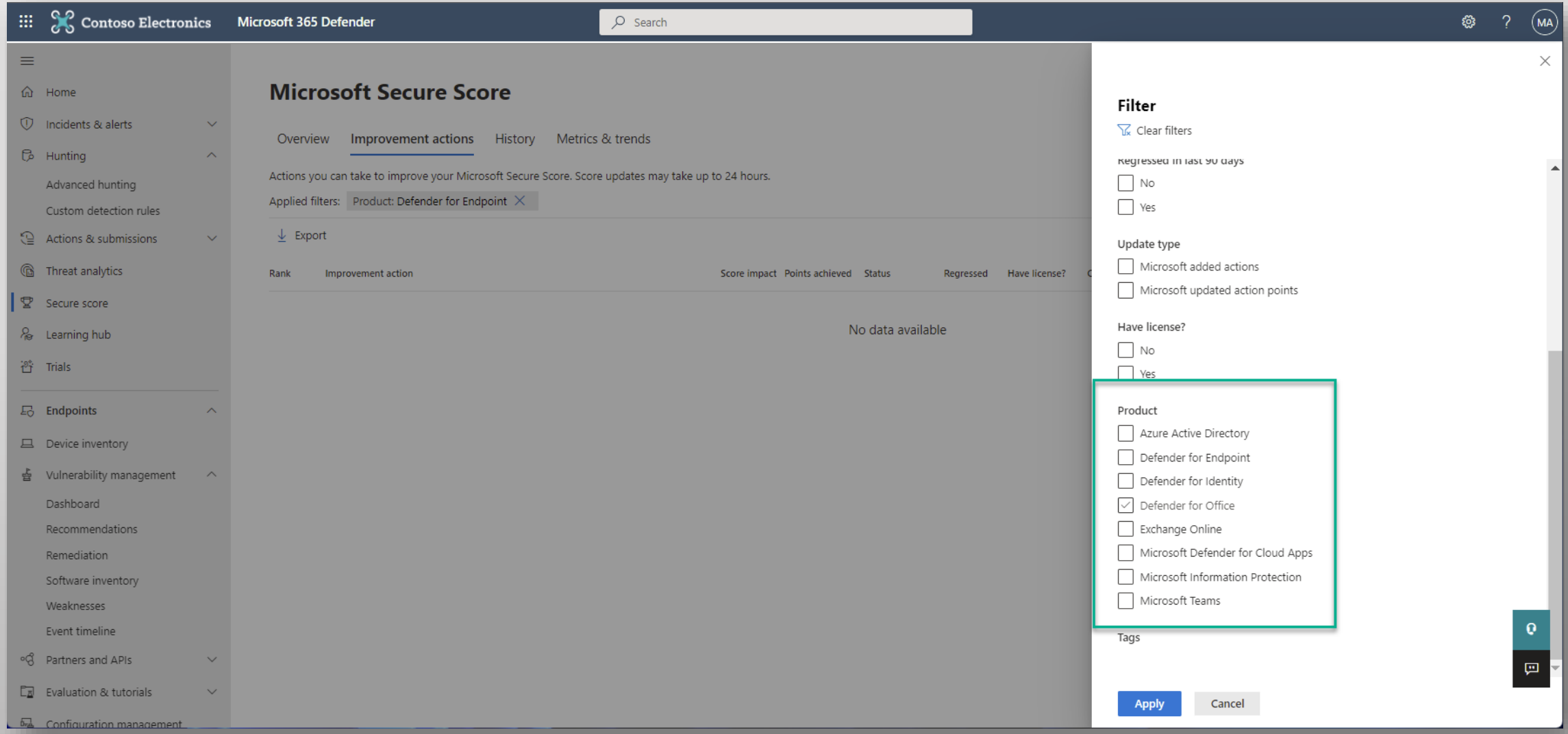





Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub
Trials
Endpoints
Search
Device inventory
Vulnerability management
Dashboard
Recommendations
Remediation
Software inventory
Weaknesses
Event timeline
Partners and APIs
Evaluation & tutorials
Security recommendations > CVE-2021-44228
C
CVE-2021-44228
Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made a
Vulnerability summary
Tags
Details
Vulnerability name
CVE-2021-44228
Severity
Critical
CVSS
10.0
Published on
12/9/2021
Updated on
1/12/2022
Age
a month
Related software
Apache Log4j (+ 187 more)
Overview
Exposed devices - onb
Export
Filters:
Status: Active +1
Security recommendation
Attention required: Devices found
Mitigation options for CVE-2021-
A mitigation action is meant to temporarily reduce
mitigation action. It can take up to 12 hours for the
Mitigation actions are only available for onboarded d
8.1, Windows Server 2019, Windows Server 2016, Wir
Devices to mitigate *
All exposed devices
Create a mitigation action for all exposed dev
Selected onboarded devices - Choose device
Create a mitigation action for specific expose
Description
This vulnerability can be mitigated by preventing ex
Creating this mitigation action will set the en
'True', which prevents JNDI lookups on Log4j
If any Java application on the device uses JN
analytics products using this data could pote
You'll need to restart the device for these cha
Note that for certain non-default configuratio
the mitigation. We recommend updating all i
latest security updates.
Once applied, the mitigation can only be und
click here.
To read more about this mitigation, see Microsoft's
Create mitigation action
Device list
This list includes devices exposed to CVE-2021-44228 that haven't been mitigated.
Choose devices to include in the mitigation action. (up to 200 devices per request)
Enter device name
1 selected
Device name
OS platform
sv
WindowsServer2019
Select
Cancel

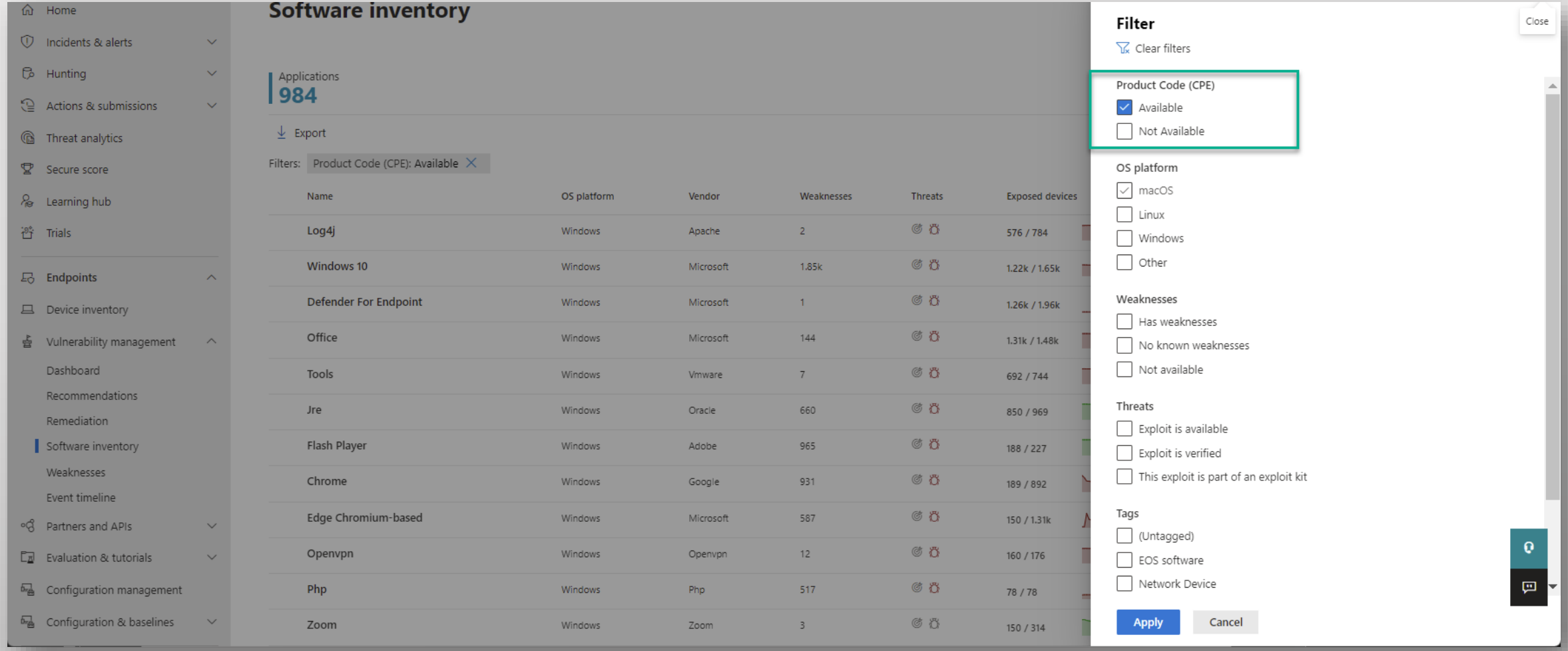


Microsoft Secure Score



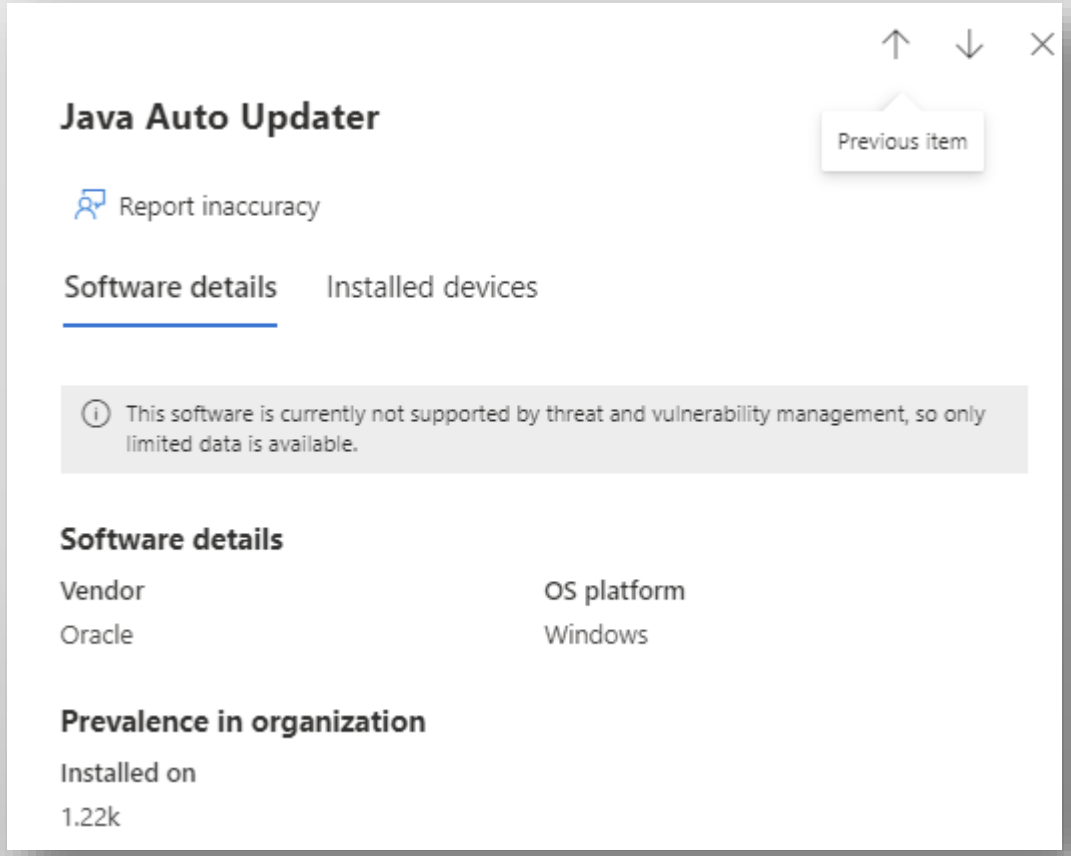
Microsoft Defender for Endpoint

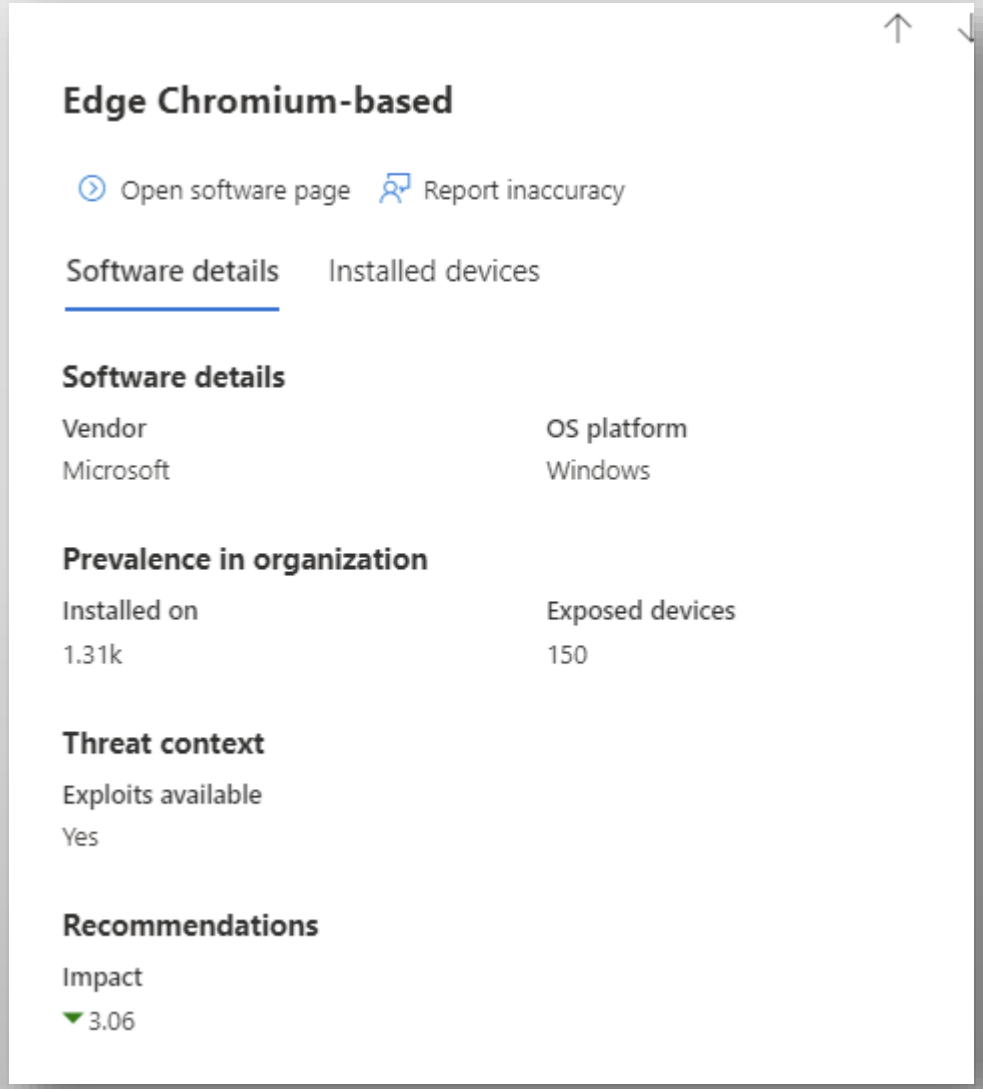
Enhanced Software Inventory



No CPE, no vulnerability Information

CPE





```
1  DeviceTvmSoftwareInventory
2  | distinct SoftwareVendor, SoftwareName, ProductCodeCpe
3  | extend hasCPE = iff(ProductCodeCpe == "Not Available","No","Yes")
4  | project SoftwareName, hasCPE
5  | summarize count() by hasCPE
6
```

Getting Started | Results

Export

hasCPE	count_
No	6369
Yes	3623

Thank you

…oh and if you are interested in KQL, join the KQL Café Community

https://kqlcafe.com