



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

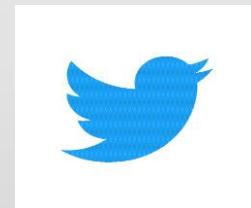




About me...

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/>



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

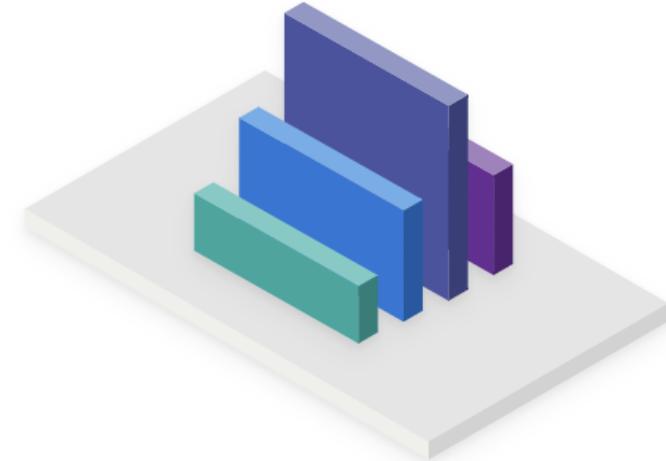
Tutorials & simulations

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

i 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 in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview Devices User Actions Simulations Report

Microsoft 365 security

Device name	OS Platform	Status	Sim
testmachine1	Windows 10	Deleted	Mul
testmachine2	Windows 10	Deleted	Mul
testmachine3	Windows 10	Deleted	Mul
testserver4	Windows Ser...	Deleted	Mul
testmachine5	Windows 10	Deleted	Mul

Device allocation

Simulations overview

Report overview

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 remediates the most sophisticated attacks.

Overview Devices User Actions Simulations Report

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

Create simulation Go to simulations gallery View full report

Microsoft 365 security

Home

Incidents & alerts

Hunting

Action center

Threat analytics

Secure score

Learning hub

Endpoints

Search

Device inventory

Vulnerability management

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 remediates the most sophisticated attacks.

Overview Devices User Actions Simulations Report

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

Create simulation Go to simulations gallery View full report

Simulations overview

7 simulations executed

Failed Running Completed

Report overview

63 Alerts in 6 Incidents 12 Actions taken in 5 Investigations 35 Key findings

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

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.

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

Deleted	Multiple ⓘ	None	Medium	32	20.126.70.149	⋮	
Deleted	Multiple ⓘ	None	Low	23	20.126.123.214	⋮	
Active	Multiple ⓘ	11h	None	Low	LabVnet	23.100.2.48	⋮

Connect

Reset password

administrator1@TestServer4 ~ +

```
I want to install supplementary tools. Learn how:
 - https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
[alve@DESKTOP-NGH388I]~[/mnt/c/Users/AlexVerboon]
@testserver46-tni24alwcwotk.westeurope.cloudapp.azure.com
post 'testserver46-tni24alwcwotk.westeurope.cloudapp.azure.com (23.100.2.48)' can't be established.
is SHA256:B81BGv8Rm1clXLxXPXieqkFX3Axd4TiiJ77seAegpg8.
to continue connecting (yes/no/[fingerprint])? yes
added 'testserver46-tni24alwcwotk.westeurope.cloudapp.azure.com,23.100.2.48' (ECDSA) to the list of
server46-tni24alwcwotk.westeurope.cloudapp.azure.com's password:
Ubuntu 14.04.6 LTS (GNU/Linux 5.4.0-1065-azure x86_64)

https://help.ubuntu.com
https://landscape.canonical.com
https://ubuntu.com/advantage

as of Fri Jan 7 15:45:17 UTC 2022

System load: 0.16          Processes:      140
Usage of /: 7.8% of 28.90GB  Users logged in:   0
Memory usage: 5%
Swap usage:  0%
```

0 updates can be applied immediately.

The programs included with the Ubuntu system are free software;

Your device connection details

To connect to the Linux device use the following command and run it on your SSH client:

ssh administrator1@testserver46-tni24alwcwotk.westeurope.cloudapp.azure.com

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	Y	Y	Y	Y	Y
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

section in the [Microsoft Defender for Endpoint guide](#).

age that matches your prefe

ploy at scale, please see other
ices, see [Configure devices u](#)

↓ 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>

```
## 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 $RemoveMMA -OnboardingScript "$($PSScriptRoot)\Files\windowsDefenderATPoffboardingscript.cmd" -log -Verbose
}
else
{
    $invokeInstallation = & "$($PSScriptRoot)\Files\Install.ps1" -OnboardingScript "$($PSScriptRoot)\Files\windowsDefenderATPoffboardingscript.cmd" -log -Verbose
}

# <Perform Uninstallation tasks here>

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

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

Software Center

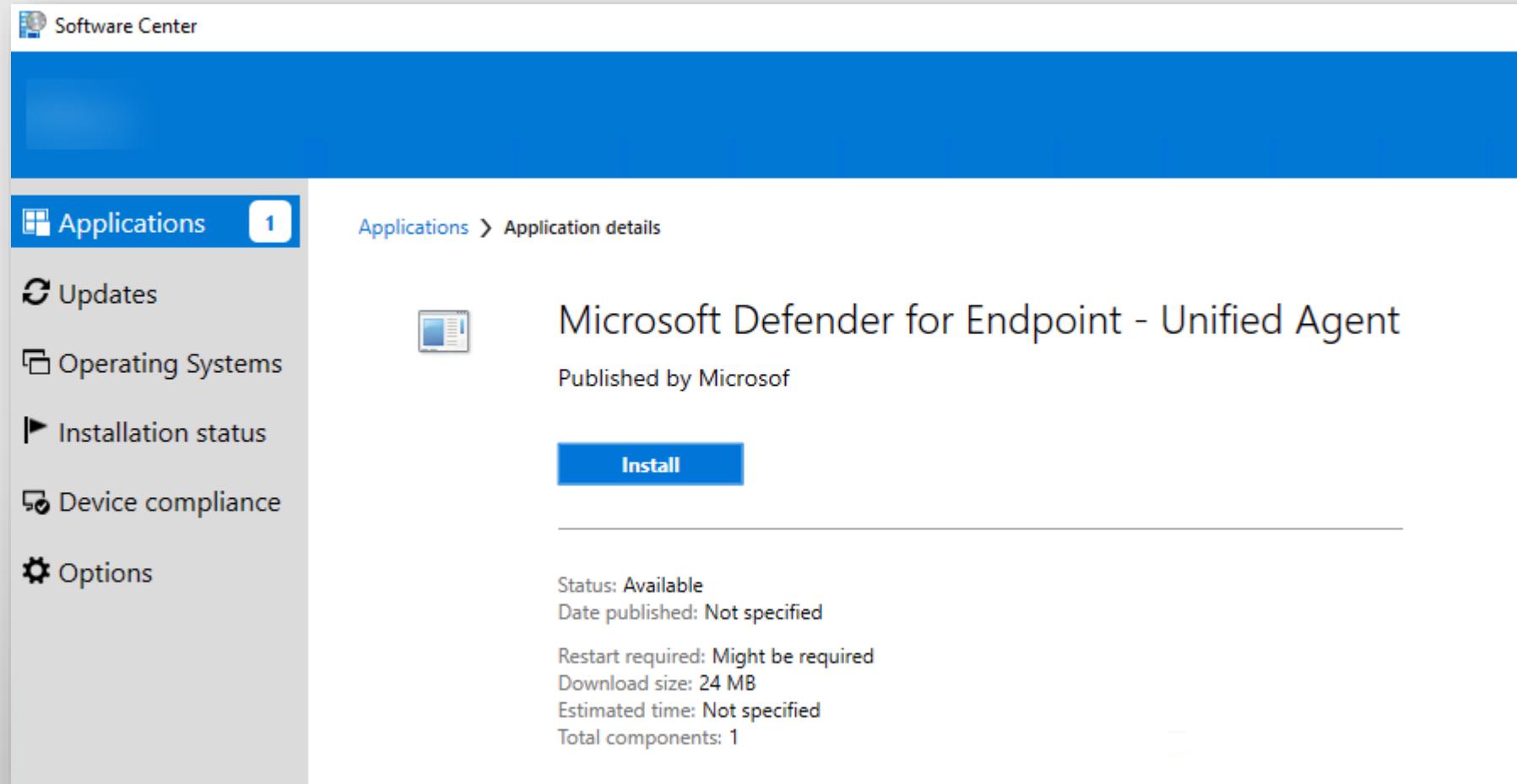
Applications > Application details

Microsoft Defender for Endpoint - Unified Agent

Published by Microsoft

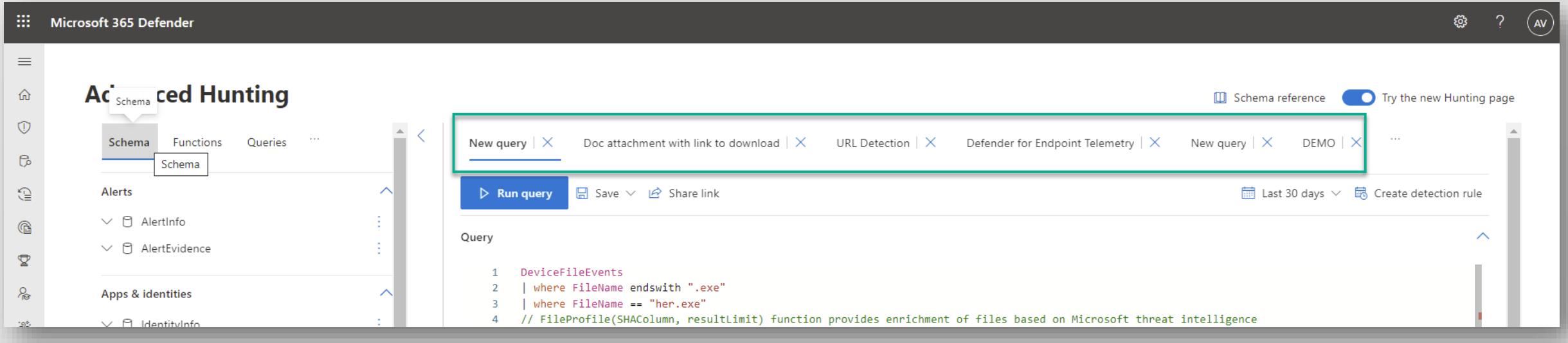
Install

Status: Available
Date published: Not specified
Restart required: Might be required
Download size: 24 MB
Estimated time: Not specified
Total components: 1



Microsoft Defender for Endpoint

New Advanced Hunting Experience



The screenshot shows the Microsoft 365 Defender Advanced Hunting interface. On the left, there's a navigation sidebar with icons for Home, Alerts, Apps & identities, and IdentityInfo. The main area is titled "Advanced Hunting" and has tabs for Schema, Functions, Queries, and more. A search bar at the top right includes "Schema reference" and a toggle for "Try the new Hunting page". Below the search bar, several tabs are open: "New query" (highlighted with a green border), "Doc attachment with link to download", "URL Detection", "Defender for Endpoint Telemetry", "New query", and "DEMO". There are also buttons for "Run query", "Save", "Share link", and "Create detection rule". The "Last 30 days" filter is selected. The bottom section shows a query editor with the following code:

```
1 DeviceFileEvents  
2 | where FileName endswith ".exe"  
3 | where FileName == "her.exe"  
4 // FileProfile(SHAColumn, resultLimit) function provides enrichment of files based on Microsoft threat intelligence
```

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:



Microsoft 365 Defender

Advanced Hunting

Schema Functions Queries ...

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

Devices

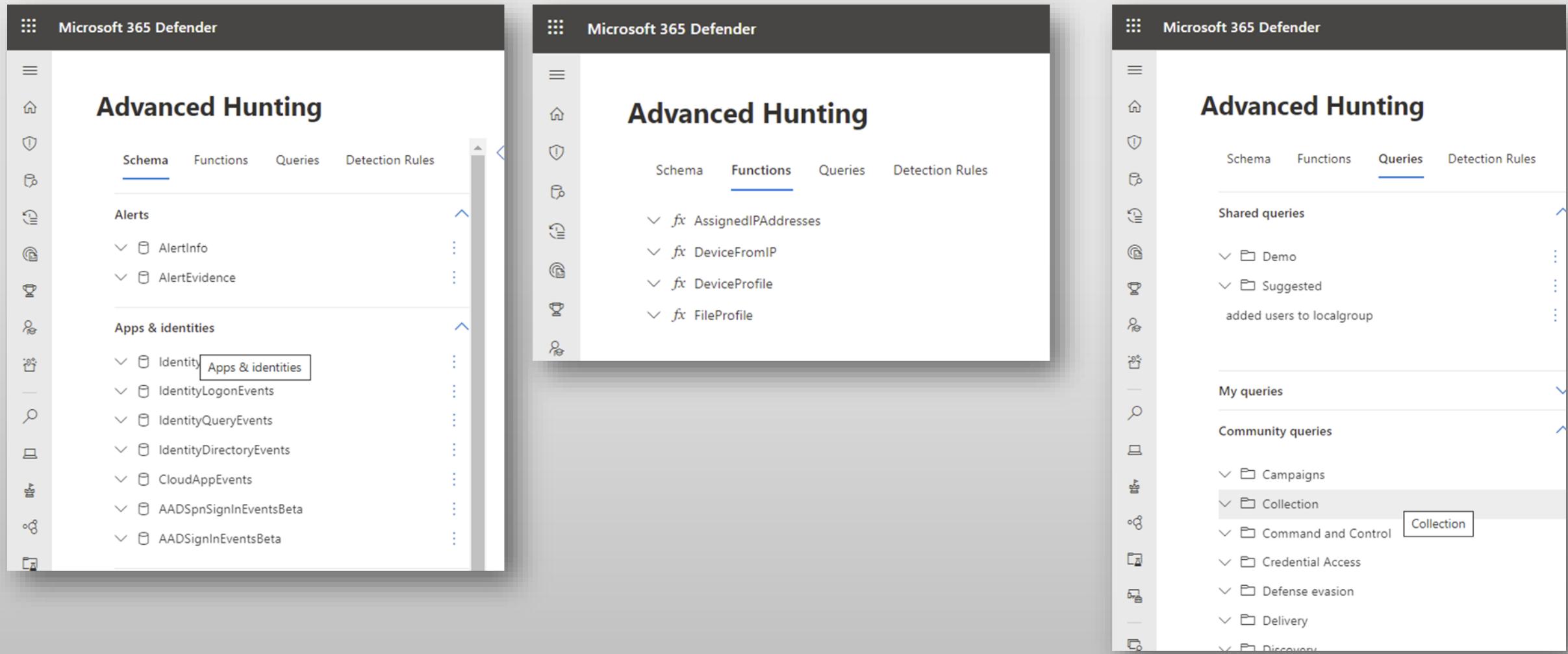
- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents
- DeviceImageLoadEvents

Export 10000 items Search 0:0.188 Low Schema reference Try the new Hunting page

Timestamp (UTC)	DeviceId	DeviceName	ActionType	FileName	FolderPath	SHA1	SH/
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	fc19515e-4fb... b1...	C:\ProgramData\Micros...	Gada18453f8f932a...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	fc19515e-4fb... b1...	C:\ProgramData\Micros...	Gada18453f8f932a...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	59286df2-a262-407f-8b...	C:\ProgramData\Micros...	e2444bdc51a0afb...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	fd772071-9b1d-4ce0-b9...	C:\ProgramData\Micros...	c6baa241cc42953f...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	43757d5a-50e1-49d2-8...	C:\ProgramData\Micros...	e5132a0812966e1...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	3fa4876e-3ae5-4c59-9a...	C:\ProgramData\Micros...	8a8281a05eaea07f...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	93514365-7ff3-4f5e-9df...	C:\ProgramData\Micros...	816fd46b4b3803a...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	cb7aec68-dfca-4632-88...	C:\ProgramData\Micros...	6af5384f8637faed...	...
() Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	2d76cc84-8291-481d-8...	C:\ProgramData\Micros...	20a40bda86ca7a7...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	aceb19ff-8484-4db4-b8f...	C:\ProgramData\Micros...	2bcbe278100110d...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	289140c0-bedb-4c68-8...	C:\ProgramData\Micros...	8b3e50ff88c5eba1...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	2495bc93-83e1-44f8-a6...	C:\ProgramData\Micros...	27ea457786f9bf50...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	a391f42c-7e1a-4611-84...	C:\ProgramData\Micros...	d2f7eb7dc6b9dfe...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	93b5bc49-87e3-4ff5-95...	C:\ProgramData\Micros...	f29ce57bd2ca1da...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	046a3caf-d9ec-4da6-a3...	C:\ProgramData\Micros...	492456812dd03b...	...
Dec 14, 2021 2:29:35 PM	051e1f66875d3e1...	Iclient07	FileCreated	fc19515e-4fb... b1...	C:\ProgramData\Micros...	Gada18453f8f932a...	...

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.

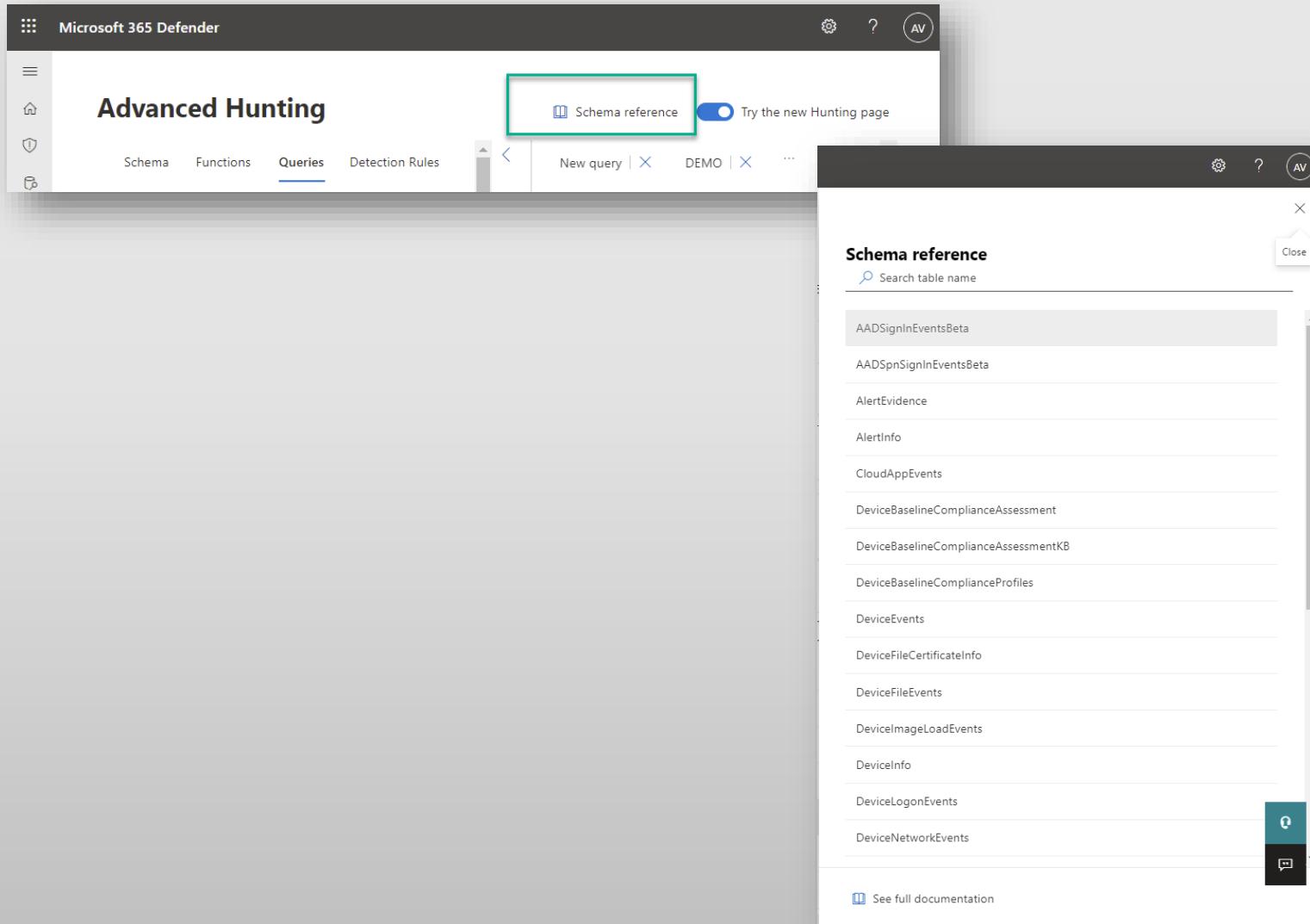
Streamlined schema tabs - Schema, functions, queries, and detection rules are now separate tabs so you can easily pivot between them.



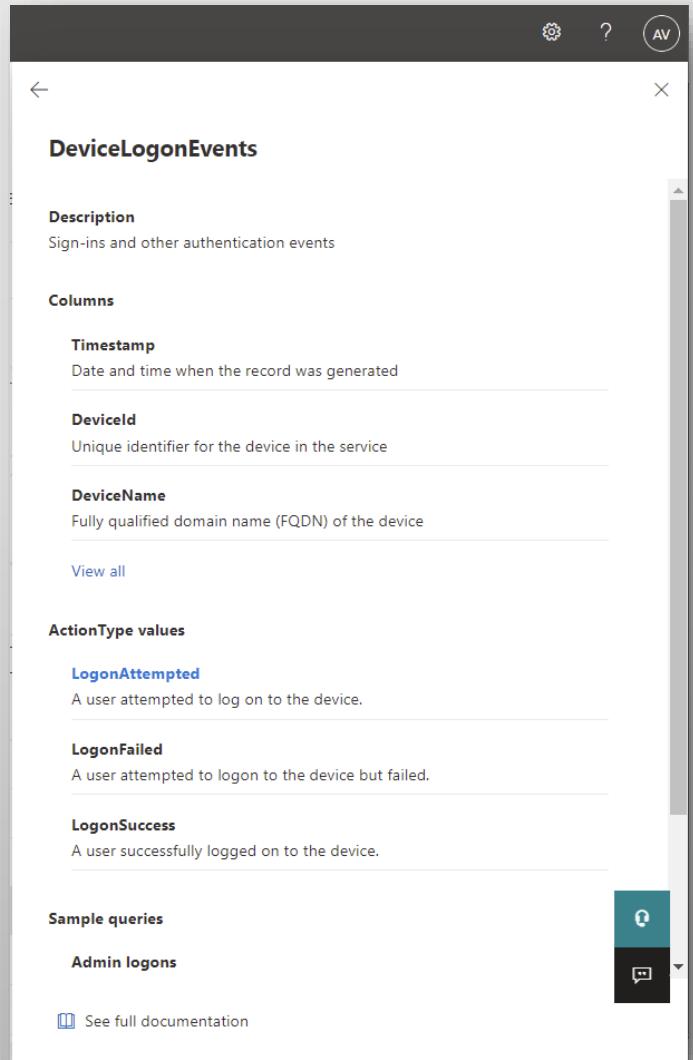
The image displays three side-by-side screenshots of the Microsoft 365 Defender Advanced Hunting interface, illustrating the evolution of schema navigation:

- Left Screenshot (Schema Tab):** Shows the "Advanced Hunting" page with a sidebar of icons. The "Schema" tab is selected at the top. Under "Alerts", "Identity", and "CloudAppEvents", there are expandable sections like "AlertInfo", "AlertEvidence", etc. A tooltip highlights the "Identity" section under "Apps & identities".
- Middle Screenshot (Functions Tab):** Shows the same interface, but the "Functions" tab is selected. Under "Identity", it lists expanded functions: "AssignedIPAddresses", "DeviceFromIP", "DeviceProfile", and "FileProfile".
- Right Screenshot (Queries Tab):** Shows the same interface, but the "Queries" tab is selected. It displays a list of shared queries: "Shared queries" (Demo, Suggested), "added users to localgroup", "My queries", and "Community queries". Under "Community queries", the "Collection" folder is expanded, with its sub-folders: "Campaigns", "Command and Control", "Credential Access", "Defense evasion", "Delivery", and "Discovery". A tooltip highlights the "Collection" folder.

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

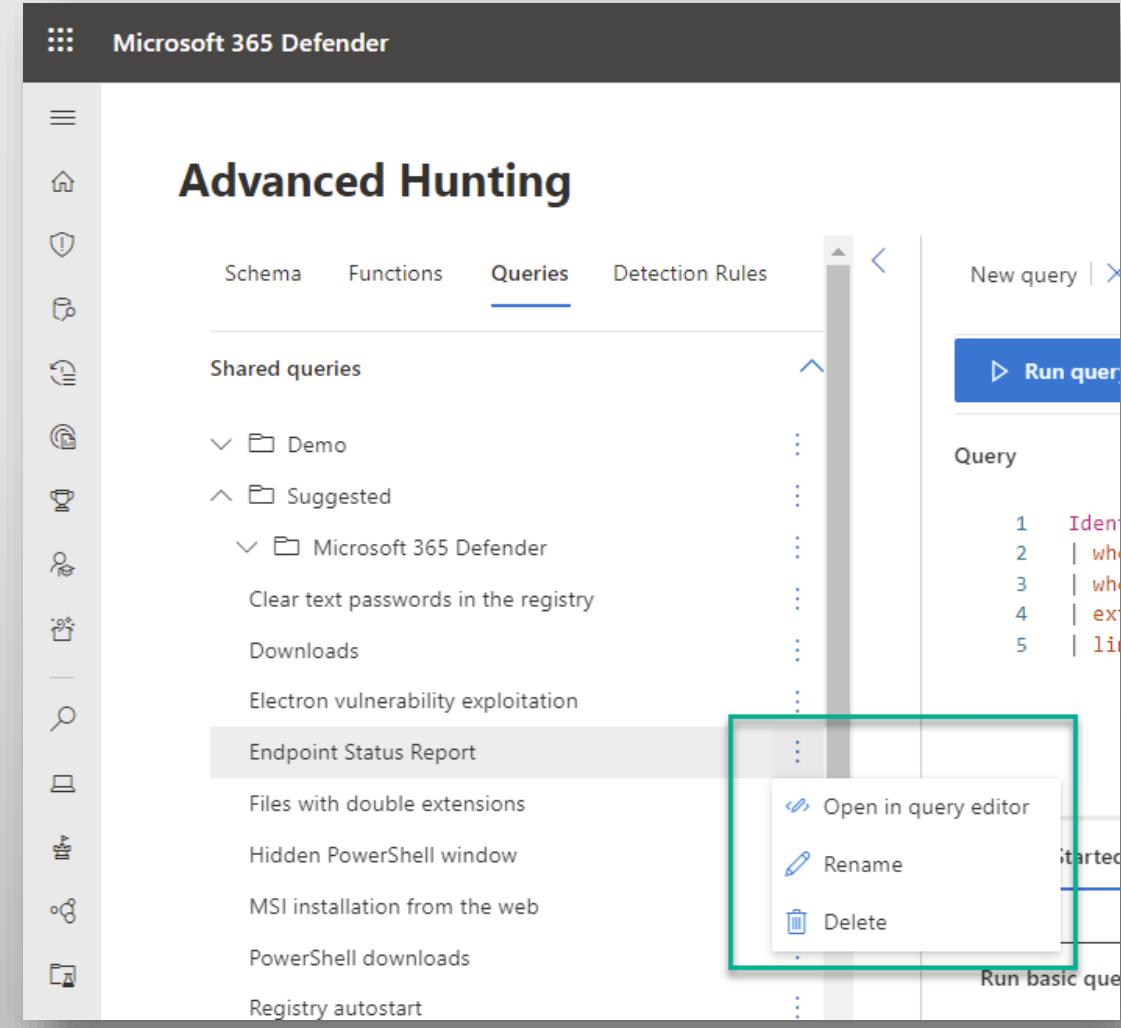


The screenshot shows the Microsoft 365 Defender Advanced Hunting interface. In the top navigation bar, there is a button labeled "Schema reference" with a teal border, which is highlighted with a green rectangular box. Below the navigation bar, there are tabs for "Schema", "Functions", "Queries" (which is underlined), and "Detection Rules". A modal window titled "Schema reference" is open, displaying a list of tables. The tables listed are: AADSignInEventsBeta, AADSpnSignInEventsBeta, AlertEvidence, AlertInfo, CloudAppEvents, DeviceBaselineComplianceAssessment, DeviceBaselineComplianceAssessmentKB, DeviceBaselineComplianceProfiles, DeviceEvents, DeviceFileCertificateInfo, DeviceFileEvents, DeviceImageLoadEvents, DeviceInfo, DeviceLogonEvents, and DeviceNetworkEvents. At the bottom of the modal, there is a link "See full documentation".



The screenshot shows the "DeviceLogonEvents" schema reference page. At the top, there is a back arrow, a title "DeviceLogonEvents", and a close button. Below the title, there is a "Description" section with the text "Sign-ins and other authentication events". Under the "Columns" section, there are three entries: "Timestamp" (Date and time when the record was generated), "DeviceId" (Unique identifier for the device in the service), and "DeviceName" (Fully qualified domain name (FQDN) of the device). There is also a "View all" link. The "ActionType values" section lists three items: "LogonAttempted" (A user attempted to log on to the device), "LogonFailed" (A user attempted to logon to the device but failed), and "LogonSuccess" (A user successfully logged on to the device). At the bottom, there is a "Sample queries" section with a "Admin logons" entry and a "See full documentation" link.

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.



The screenshot shows the Microsoft 365 Defender Advanced Hunting interface. The top navigation bar includes icons for Home, Protection, Functions, Queries (which is the active tab), and Detection Rules. Below the navigation is a sidebar with various icons and sections: Shared queries, Demo (expanded), Suggested (expanded), Microsoft 365 Defender (expanded), Clear text passwords in the registry, Downloads, Electron vulnerability exploitation, Endpoint Status Report (selected and highlighted with a green box), Files with double extensions, Hidden PowerShell window, MSI installation from the web, PowerShell downloads, and Registry autostart. To the right of the sidebar is a main content area with a "Run basic query" button and a "Query" section containing five numbered lines of code. A context menu is open over the "Endpoint Status Report" query, with options: "Open in query editor", "Rename", and "Delete".

```
1 Identity | whoami
2 | where ...
3 | where ...
4 | exec ...
5 | limit ...
```



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.

Run query Save Share link

Query

```
1 IdentityLogonEvents
2 | where Timestamp > ago(1d)
3 | where isnotempty(AccountName)
4 | extend AccountAndDomain = strcat(AccountName, "\\", AccountDomain)
5 | limit 1000
```

Getting Started Results

Export Link to incident Take actions 1 of 30 selected Search

Timestamp (UTC)	ActionType	Application	LogonType	Protocol	Fai
Jan 4, 2022 7:35:31 PM	LogonSuccess	Office 365	Kmsi:kmsi		
Jan 4, 2022 7:35:29 PM	LogonFailed	Office 365	Login:login		
Jan 5, 2022 11:14:50 AM	LogonSuccess	Office 365	OAuth2:Authorize		
Jan 4, 2022 3:14:12 PM	LogonSuccess	Office 365	OAuth2:Authorize		
Jan 5, 2022 8:39:02 AM	LogonSuccess	Microsoft Azure	OAuth2:Authorize		
Jan 5, 2022 10:52:06 AM	LogonSuccess	Office 365	OAuth2:Authorize		

Users (1)

oa

All details

Timestamp Jan 5, 2022 11:14:50 AM

ActionType

LogonSuccess

Application Office 365 Add Application == Office 365

LogonTy Add Application != Office 365

OAuth2: Authorize View more filters for Application

Account oa Copy value to clipboard

AccountDomain verboon.online

AccountUpn oa@verboon.online

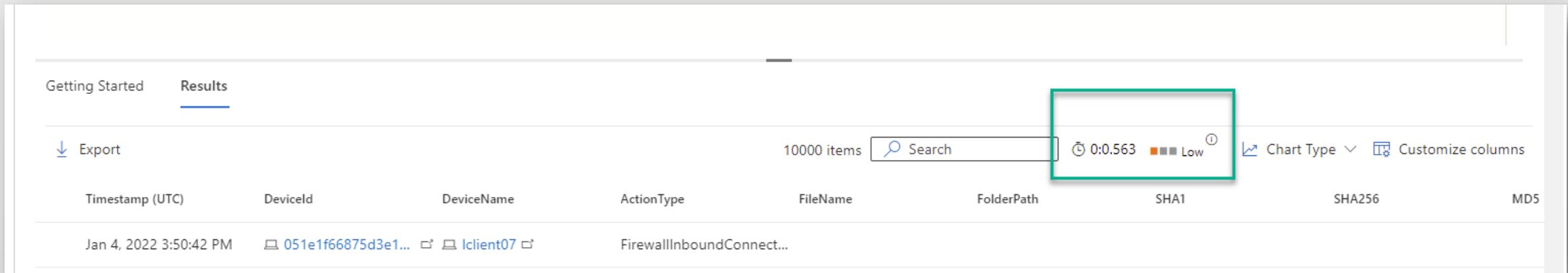
AccountObjectId c6f5185a-c038-4bff-95be-e12642e14384

AccountDisplayName Alex Verboon

DeviceType Desktop

A red arrow points from the 'LogonSuccess' entry in the context menu back to the 'LogonType' column in the main table, indicating how to apply a filter.

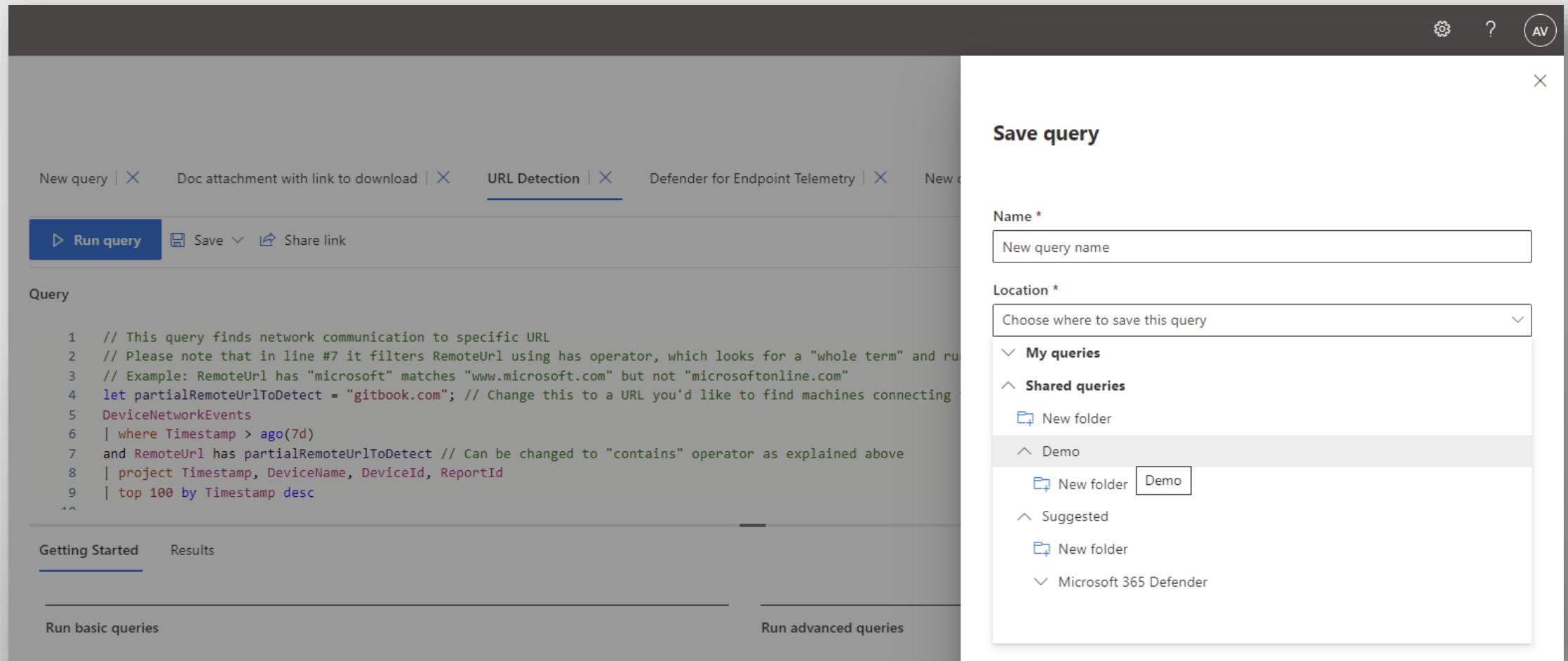
Resource usage indicator - After running your query, you can see the execution time and its resource usage (Low, Medium, High) so you can tweak your query accordingly. High indicates that the query took more resources to run and could be improved to execute more efficiently.



The screenshot shows the Microsoft Sentinel interface with the "Results" tab selected. At the top, there are buttons for "Getting Started" and "Results", and a "Export" button. To the right of the search bar, there is a "0:0.563" execution time indicator with a "Low" resource usage level, which is highlighted with a green box. Below the search bar are buttons for "Chart Type" and "Customize columns". The main table has columns for Timestamp (UTC), DeviceId, DeviceName, ActionType, FileName, FolderPath, SHA1, SHA256, and MD5. A single row of data is shown: Jan 4, 2022 3:50:42 PM, 051e1f66875d3e1..., lclient07, FirewallInboundConnect..., and some truncated file information.

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.

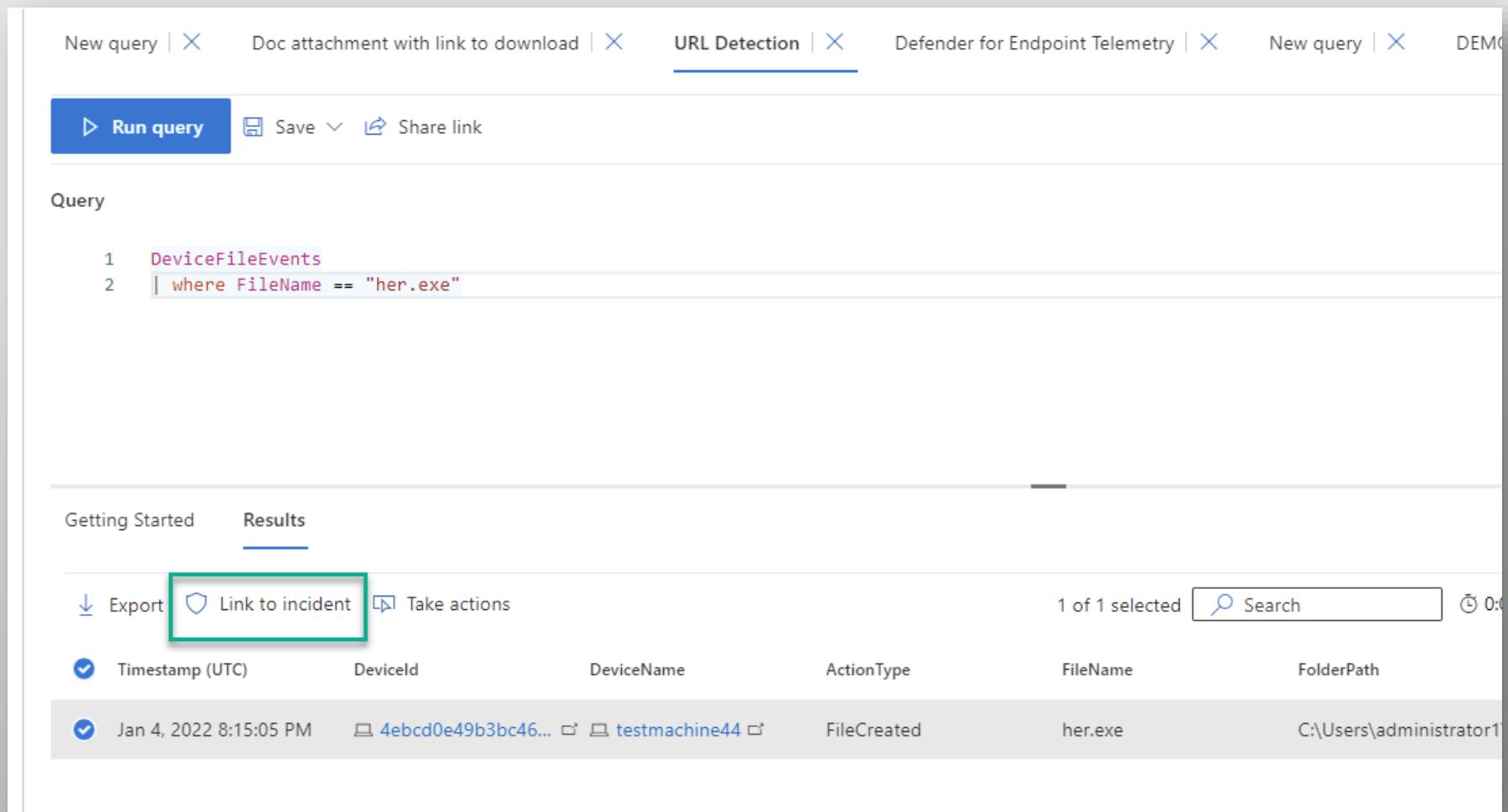


The screenshot shows the Microsoft Defender for Endpoint Query Editor interface. On the left, there's a main workspace with tabs like "New query", "Doc attachment with link to download", "URL Detection" (which is active), and "Defender for Endpoint Telemetry". Below the tabs is a toolbar with "Run query", "Save", and "Share link". The main area is titled "Query" and contains the following PowerShell-like query:

```
1 // This query finds network communication to specific URL
2 // Please note that in line #7 it filters RemoteUrl using has operator, which looks for a "whole term" and runs
3 // Example: RemoteUrl has "microsoft" matches "www.microsoft.com" but not "microsoftonline.com"
4 let partialRemoteUrlToDetect = "gitbook.com"; // Change this to a URL you'd like to find machines connecting to
5 DeviceNetworkEvents
6 | where Timestamp > ago(7d)
7 and RemoteUrl has partialRemoteUrlToDetect // Can be changed to "contains" operator as explained above
8 | project Timestamp, DeviceName, DeviceId, ReportId
9 | top 100 by Timestamp desc
10
```

Below the query editor are "Getting Started" and "Results" buttons. At the bottom are "Run basic queries" and "Run advanced queries" buttons. A "Save query" side pane is open on the right, titled "Save query". It has fields for "Name" (containing "New query name") and "Location" (a dropdown menu showing "Choose where to save this query" with options like "My queries", "Shared queries", "Demo", and "Suggested").

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.



The screenshot shows the Microsoft Defender for Endpoint Telemetry search interface. At the top, there are several tabs: "New query" (with an "X"), "Doc attachment with link to download" (with an "X"), "URL Detection" (which is selected, indicated by a blue underline), "Defender for Endpoint Telemetry" (with an "X"), "New query" (with an "X"), and "DEMO". Below the tabs are buttons for "Run query" (highlighted with a blue border), "Save", and "Share link".

The "Query" section contains the following Advanced Hunt query:

```
1 DeviceFileEvents  
2 | where FileName == "her.exe"
```

Below the query, there are two tabs: "Getting Started" and "Results" (which is selected, indicated by a blue underline). Under "Results", there are buttons for "Export", "Link to incident" (which is highlighted with a green box), and "Take actions". There is also a search bar with "1 of 1 selected" and a timestamp of "0:00".

The results table has columns: "Timestamp (UTC)", "DeviceId", "DeviceName", "ActionType", "FileName", and "FolderPath". One row is visible in the table:

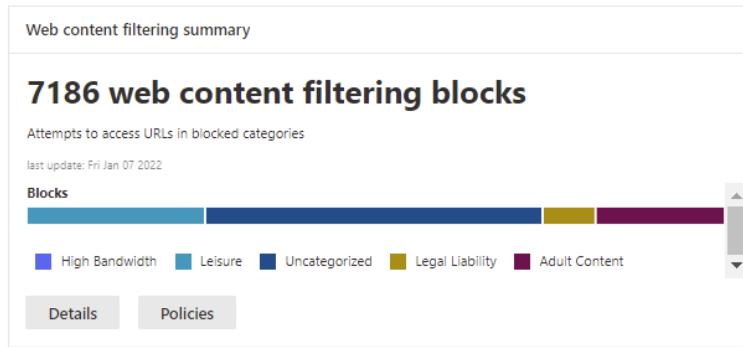
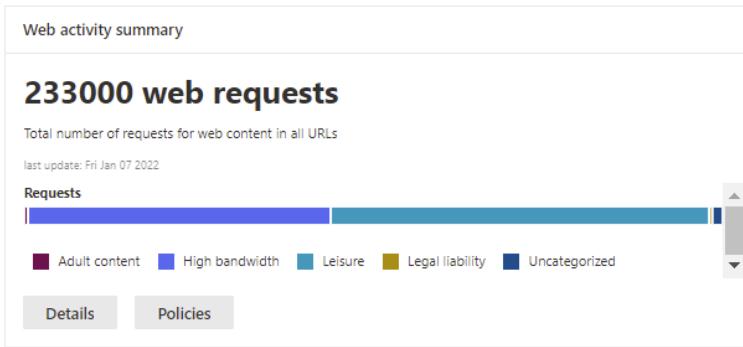
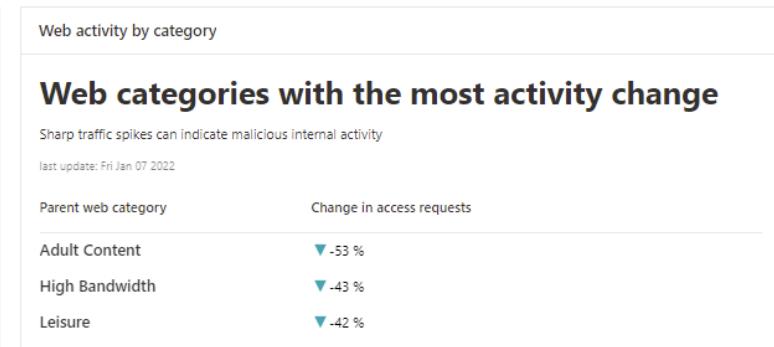
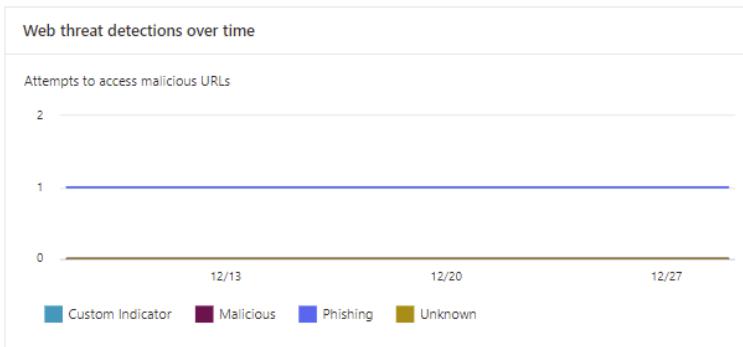
Timestamp (UTC)	DeviceId	DeviceName	ActionType	FileName	FolderPath
Jan 4, 2022 8:15:05 PM	4ebcd0e49b3bc46...	testmachine44	FileCreated	her.exe	C:\Users\administrator1

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.

Reports > Web Protection





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

The screenshot illustrates the configuration of a Web Content Filter policy in Audit Mode. On the left, a navigation pane lists various features: Licenses, Email notifications, Advanced features (selected), Auto remediation, Portal redirection, Permissions, Roles, and Device groups. The 'Advanced features' section contains two toggle switches: 'Microsoft Secure Score' (On) and 'Web content filtering' (On). The 'Web content filtering' switch is highlighted with a green box. The main content area shows the 'Endpoints' settings page. A policy named 'Web Content Filter - Audit M...' is listed under 'Blocked categories'. The 'Categories' section shows several checkboxes for content types: Adult content, High bandwidth, Legal liability, Leisure, and Uncategorized. The 'Scope' section indicates that the policy applies to 'All devices in my scope'. A 'Save' button is at the bottom right. The overall title of the interface is 'Web Content Filter - Audit Mode'.

To run in audit mode only, leave all categories unchecked

Licenses
Email notifications
Advanced features
Auto remediation
Portal redirection
Permissions
Roles
Device groups

Microsoft Secure Score
On

Web content filtering
On

Settings > Endpoints

Endpoints

Device groups
APIs
SIEM
Rules
Alert suppression
Indicators
Process Memory Indicators
Web content filtering
Automation uploads
Automation folder exclusions
Configuration management
Enforcement scope

Add item

Policy name: Web Content Filter - Audit M...
Blocked categories: Adult content High bandwidth Legal liability Leisure Uncategorized

Categories: Adult content High bandwidth Legal liability Leisure Uncategorized

Scope:
Selected device groups: All devices in my scope Select from list

Save

Category	Sub Categories
Adult Content	<p>Cults: Sites related to groups or movements whose members demonstrate passion for a belief system that is different from those that are socially accepted.</p> <p>Gambling: Online gambling and sites that promote gambling skills and practice.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
High Bandwidth	<p>Download sites: Sites whose primary function is to allow users to download media content or programs, such as computer programs.</p> <p>Image sharing: Sites that are used primarily for searching or sharing photos, including those that have social aspects.</p> <p>Peer-to-peer: Sites that host peer-to-peer (P2P) software or facilitate the sharing of files using P2P software.</p> <p>Streaming media & downloads: Sites whose primary function is the distribution of streaming media, or sites that</p>
Legal Liability	<p>Child abuse images: Sites that include child abuse images or pornography.</p> <p>Criminal activity: Sites that give instruction on, advice about or promotion of illegal activities.</p> <p>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.</p> <p>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.</p> <p>Illegal drug: Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia.</p> <p>Illegal software: Sites that contain or promote the use of malware, spyware, botnets, phishing scams, or piracy & copyright theft.</p> <p>School cheating: Sites related to plagiarism or school cheating.</p> <p>Self-harm: Sites that promote self-harm, including cyberbullying sites that contain abusive and/or threatening messages towards users.</p> <p>Weapons: Any site that sells weapons or advocates the use of weapons, including but not limited to guns, knives, and ammunition.</p>
Leisure	<p>Chat: Sites that are primarily web-based chat rooms.</p> <p>Games: Sites relating to video or computer games, including sites that promote gaming through hosting online services or information related to gaming.</p> <p>Instant messaging: Sites that can be used to download instant messaging software or client based instant messaging.</p> <p>Professional network: Sites that provide professional networking services.</p> <p>Social networking: Sites that provide social networking services.</p> <p>Web-based email: Sites offering web-based mail services.</p>
Uncategorized	<p>Newly registered domains: Sites that have been newly registered in the past 30 days and have not yet been moved to another category.</p> <p>Parked domains: Sites that have no content or are parked for later use.</p> <p>NOTE: Uncategorized contains only newly registered domains and parked domains, and does not include all other sites outside of these categories.</p>



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

Search

Device inventory

Vulnerability management

Partners and APIs

Evaluation & tutorials

Email & collaboration

Investigations

Explorer

Submissions

Review

Campaigns

Threat tracker

Attack simulation training

Policies & rules

Reports

Health

Reports

View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.

Name	Description
General (1)	
Security report	View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.
Endpoints (7)	
Threat protection	See details about the security detections and alerts in your organization.
Device health and compliance	Monitor the health state, antivirus status, operating system platforms, and Windows 10 versions for devices in your organization.
Vulnerable devices	View information about the vulnerable devices in your organization, including their exposure to vulnerabilities by severity level, exploitability, age, and more.
Web protection	Get information about the web activity and web threats detected within your organization.
Firewall	View connections blocked by your firewall including related devices, why they were blocked, and which ports were used.
Device control	This report shows your organization's media usage data.
Attack surface reduction rules	View information about detections, misconfiguration, and suggested exclusions in your environment.
Email & collaboration (3)	



Select the Details button underneath each graph to obtain detailed information

Reports > Web Protection

Web threat detections over time

Attempts to access malicious URLs

2

1

0

12/13 12/20 12/27

Custom Indicator Malicious Phishing Unknown

Web threat summary

3 Attempts to access malicious URLs

Attempts to access malicious URLs

last update: Fri Jan 07 2022

Threat Category
Phishing
Malicious
Custom Indicator
Unknown

Details Indicators

Web activity by category

Web categories with the most activity change

Sharp traffic spikes can indicate malicious internal activity

last update: Fri Jan 07 2022

Parent web category	Change in access requests
Adult Content	-53 %
High Bandwidth	-43 %
Leisure	-42 %
Legal Liability	-36 %
Uncategorized	-30 %

Web activity summary

233000 web requests

Total number of requests for web content in all URLs

last update: Fri Jan 07 2022

Requests

Adult content High bandwidth Leisure Legal liability Uncategorized

Details Policies

Web content filtering summary

7186 web content filtering blocks

Reports > Web Protection > Web content filtering categories details

Web categories Domains Machine groups

Export Refresh

Category Name Parent Category Requests Blocks ↓ Request trend Machines Domains

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

- ≡
- [!\[\]\(9c6dc213295b620389617389f15c94f0_img.jpg\) Home](#)
- [!\[\]\(86e76716e719e1794580a2abb382bc2a_img.jpg\) Incidents & alerts](#)
- [!\[\]\(44298d4d999c16adc91d7accd5867a90_img.jpg\) Hunting](#)
- [!\[\]\(c125d0e073c4c95481eaf1167609e50d_img.jpg\) Action center](#)
- [!\[\]\(f4b6bfc94c487034ab80a8f35dff40ea_img.jpg\) Threat analytics](#)
- [!\[\]\(e3ecde01aaec6249a571582d49974e02_img.jpg\) Secure score](#)
- [!\[\]\(e593f23585c6cb3e0d680f2ca582ca4c_img.jpg\) Learning hub](#)
- [!\[\]\(591fa5eb68a8d5d25935ef7c36eaa6bb_img.jpg\) Trials](#)
- [!\[\]\(afe4702a571a7a8abf238c322e6d563d_img.jpg\) Endpoints](#)
- [!\[\]\(e81ce8f4ca3d917ac296bb4509183934_img.jpg\) Search](#)

Search Endpoints Content

URL

Search > youtube.com

 youtube.com

URL summary

Security info

Open incidents	Active alerts
0	0

URL/Domain details

Domain
youtube.com
[View at Whois](#)

Category
Streaming media & downloads
[Dispute category](#)

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** Selected workspace: 'mtplabsentinel01'

Search (Ctrl+ /) Create Refresh Edit Disable Move up Move down Remove

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Automation**
- Community

Automation rules (Preview)

Automation rules (Preview) Search Analytic rules : All Actions : All Created by : A

<input type="checkbox"/> Order	Display name	Analytic rule nam...	Actions	Expiration date
<input type="checkbox"/> 2	Assign Alex to incident	DEMO - Failed sign...	Assign owner	Indefinite
<input type="checkbox"/> 3	Not my ip set alert to ...	DEMO Successfull s...	Assign owner, Chan...	Indefinite

Enabled rules 2

Enabled playbooks 12

Playbooks

Azure Sentinel - Automation Rules

 **45**
Active rules

Rules by severity
High (23) Medium (19) Low (3) Informational (0)

[LEARN MORE](#)
[About analytics rules](#)

[Active rules](#) [Rule templates](#)

Severity : All Rule Type : All

SEVERITY ↑↓ NAME ↑↓ RULE TYPE ↑↓ STATUS ↑↓

<input type="checkbox"/>	Medium	DEMO Successfull sign-in with MFA exclu...	 Scheduled	 Enabled
<input type="checkbox"/>	Medium	DEMO - Failed sign-in with MFA excluded ...	 Scheduled	 Enabled

[More \(2\)](#)

 DEMO Successfull sign-in with MFA excluded account

Medium Severity  Enabled Status

Id: 81f44dea-999d-406f-9dcc-74024a8236ef 

Description: Successfull sign-in with MFA excluded account

Tactics:  Initial Access  Privilege Escalation

Azure Sentinel - Automation Rules



Edit automation rule

Automation rule name
Not my ip set alert to high

Trigger
When incident is created

Conditions
If
Analytic rule name Contains 2 selected

And
IP address Does not equal 77.56.162.123

+ Add condition

Actions
Change severity High

And then
Assign owner Assign to me oa@verboon.online

+ Add action

Conditions
If
Analytic rule name Contains 2 selected

Search analytic rules

- Select all
- Create incidents based on Microsoft Defender Advanced Threat Protection alerts
- Create incidents based on Office 365 Advanced Threat Protection alerts
- Custom - User denied MFA
- Custom - User Reported Fraud
- DEMO - Failed sign-in with MFA excluded account
- DEMO Successfull sign-in with MFA excluded account
- Group added to built in domain local or global group
- Mail redirect via ExO transport rule
- Multiple Password Reset by user
- Multiple users email forwarded to same destination
- New executable via Office FileUploaded Operation
- New File Shared via OneDrive API

Azure Sentinel - Automation Rules

Open incidents: 10 | New incidents: 10 | Active incidents: 0 | Open incidents by severity: High (6) Medium (4) Low (0) Informational (0)

Search by id, title, tags, owner or product | Severity: All | Status: New, Active | More (2)

Auto-refresh incidents

Incident ID	Title	Alerts	Product names	Created time
744	Impossible travel activity in...	1	Microsoft 365 Defe...	04/06/21, 01:00 PM
743	DEMO Successfull sign-in ...	1	Azure Sentinel	04/06/21, 01:01 PM
742	DEMO - Failed sign-in with...	1	Azure Sentinel	04/06/21, 12:36 PM
741	DEMO Successfull sign-in ...	1	Azure Sentinel	04/06/21, 12:31 PM
740	Anonymous IP address	1	Azure Active Direct...	04/06/21, 12:24 PM

DEMO Successfull sign-in with MFA excluded account
Incident ID: 741

Alex Verbo... Owner | New Status | **High Severity**

Description: Successfull sign-in with MFA excluded account

Alert product names: Azure Sentinel

Evidence: 2 Events, 1 Alerts, 0 Bookmarks



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.

The screenshot shows the Azure Sentinel Data connectors page. The left sidebar includes Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (Preview)) and Configuration (Data connectors, Analytics, Watchlist (Preview), Playbooks, Community, Settings). The main area displays 96 connectors, with 13 connected and 0 coming soon. A search bar and filters for Providers (All), Data Types (All), and Status (All) are present. The Microsoft 365 Defender (Preview) connector is highlighted. On the right, detailed information for the Agari Phishing Defense and Brand Protection connector is shown, including its status (Not connected), provider (Agari), last log received (--), description (uses Agari REST API to push data to Log Analytics), last data received (--), related content (0 workbooks, 2 queries, 0 analytic rules templates), and data received (100). A blue "Open connector page" button is at the bottom.

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Azure Sentinel > Azure Sentinel

Azure Sentinel | Data connectors

Selected workspace: 'mplabsentinel01'

Search (Ctrl+/)

Guides & Feedback Refresh

News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

96 Connectors

13 Connected

0 Coming soon

Search by name or provider

Providers : All Data Types : All Status : All

Status	Connector name	Provider	Last Log Received
Connected	Juniper SRA (Preview)	Juniper	--
Connected	Microsoft 365 Defender (Preview)	Microsoft	--
Connected	Microsoft Cloud App Security	Microsoft	--
Connected	Microsoft Defender for Endpoint	Microsoft	--
Connected	Microsoft Defender for Identity (Preview)	Microsoft	--
Connected	Microsoft Defender for Office 365 (Preview)	Microsoft	--

Agari Phishing Defense and Brand Protection (Preview)

Not connected

Agari Provider

Last Log Received

Description

This connector uses a Agari REST API connection to push data into Azure Sentinel Log Analytics.

Last data received

Related content

0 Workbooks 2 Queries 0 Analytic rules templates

Data received

100 Go to log analytics

Open connector page

Azure Sentinel - M365 Defender Connector



Microsoft 365 security

Incidents & alerts

Incidents

Alerts

Email & collaboration alerts

Hunting

Action center

Threat analytics

Secure score

Learning hub

Endpoints

Search

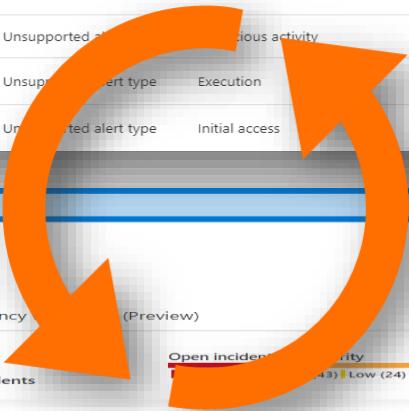
Device inventory

Incidents

Create a notification rule

1-18 < > 30 days Choose columns 30 items per page Filters

Incident name	Severity	Investigation state	Categories	Impacted entities	Active aler...	Service sources	Dete...
Suspicious application consent	Low	Unsupported alert type	Suspicious activity	1/1	Cloud App Security	Clo...	
Impossible travel activity involving one user	Medium	Unsupported alert type	Initial access	1/1	Cloud App Security	Clo...	
Impossible travel activity involving multiple users	Medium	Unsupported alert type	Initial access	2 Users	2/2	Cloud App Security	Clo...
Investigation priority score increase	Medium	Unsupported alert type	Suspicious activity	1/1	Cloud App Security	Clo...	
firefox usage detected on one endpoint	Low	Unsupported alert type	Execution	Iclient04 1/1	Endpoint	Cus...	
Impossible travel activity involving one user	Medium	Unsupported alert type	Initial access	1/1	Cloud App Security	Clo...	



Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Azure Sentinel > Azure Sentinel

Azure Sentinel | Incidents

Selected workspace: 'mtplabsentinel01'

97 Open Incidents 97 New incidents 0 Active incidents

(Preview) Open Incident Severity: 43 Low (24) Informational (3)

Logs News & guides Threat management Configuration

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

Auto-refresh incidents

Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
702	Impossible travel activity	1	Microsoft Cloud Ap...	03/08/21, 11:05 AM	03/08/21, 11:05 AM	Unassigned
701	Suspicious application consent	1	Microsoft Cloud Ap...	03/08/21, 10:28 AM	03/08/21, 10:28 AM	Unassigned
700	DEMO - Block upload based on real-time conte...	1	Microsoft Cloud Ap...	03/02/21, 03:00 PM	03/02/21, 03:00 PM	Unassigned
699	DEMO Block upload based on real-time conte...	1	Microsoft Cloud Ap...	03/02/21, 03:00 PM	03/02/21, 03:00 PM	Unassigned
698	DEMO Block upload based on real-time conte...	1	Microsoft Cloud Ap...	03/02/21, 12:26 PM	03/02/21, 12:26 PM	Unassigned
697	DEMO - Block upload based on real-time conte...	1	Microsoft Cloud Ap...	03/02/21, 12:26 PM	03/02/21, 12:26 PM	Unassigned
696	DEMO Block cut/copy and paste based on real...	1	Microsoft Cloud Ap...	03/02/21, 11:43 AM	03/02/21, 11:43 AM	Unassigned

< Previous 1 - 50 Next >

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)

 **Configuration**

Connect incidents & alerts - **Coming soon!**

Connect Microsoft 365 Defender incidents to your Azure Sentinel. Incidents will appear in the incidents queue.

[Learn more about Microsoft 365 Defender](#)

[Disconnect](#)

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.

Active rules Rule templates

create Severity : All Rule Type : All Status : **Disabled** Tactics : All

SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓
<input type="checkbox"/>	High Create incidents based on Office 365 Advanced Threat Protection alerts	Microsoft Secur...
<input type="checkbox"/>	High Create incidents based on Azure Advanced Threat Protection alerts	Microsoft Secur...
<input type="checkbox"/>	High (Private Preview) Create incidents based on Office 365 Advanced Threat Protection alerts	Microsoft Secur...
<input type="checkbox"/>	High Create incidents based on Microsoft Defender Advanced Threat Protection alerts	Microsoft Secur...
<input type="checkbox"/>	High Create incide	

Configuration

Connect Microsoft Defender for Endpoint alerts to Azure Sentinel

Connecting Microsoft Defender for Endpoint will cause your data that is collected by Microsoft Defender for Endpoint service to be stored and processed in the location that you have configured your Azure Sentinel workspace.

Microsoft Defender for Endpoint alerts Cannot disconnect while Microsoft 365 Defender is connected

Info: Microsoft Defender for Endpoint alerts are connected through the Microsoft 365 Defender connector and automatically grouped into incidents. Incidents can be seen in the incidents queue.

Info: Microsoft Defender for Endpoint Advanced Hunting raw logs are available as part of the Microsoft 365 Defender (Preview) connector

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.

Connect events

Connect logs from the following Microsoft 365 Defender products to Sentinel:

^ Microsoft Defender for Endpoint (9/10 connected) ⓘ

<input type="checkbox"/> Name	Description
<input checked="" type="checkbox"/> DeviceInfo	Machine information (including OS information)
<input checked="" type="checkbox"/> DeviceNetworkInfo	Network properties of machines
<input checked="" type="checkbox"/> DeviceProcessEvents	Process creation and related events
<input checked="" type="checkbox"/> DeviceNetworkEvents	Network connection and related events
<input checked="" type="checkbox"/> DeviceFileEvents	File creation, modification, and other file system events
<input checked="" type="checkbox"/> DeviceRegistryEvents	Creation and modification of registry entries
<input checked="" type="checkbox"/> DeviceLogonEvents	Sign-ins and other authentication events
<input checked="" type="checkbox"/> DeviceImageLoadEvent	DLL loading events
<input checked="" type="checkbox"/> DeviceEvents	Additional events types

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](#))

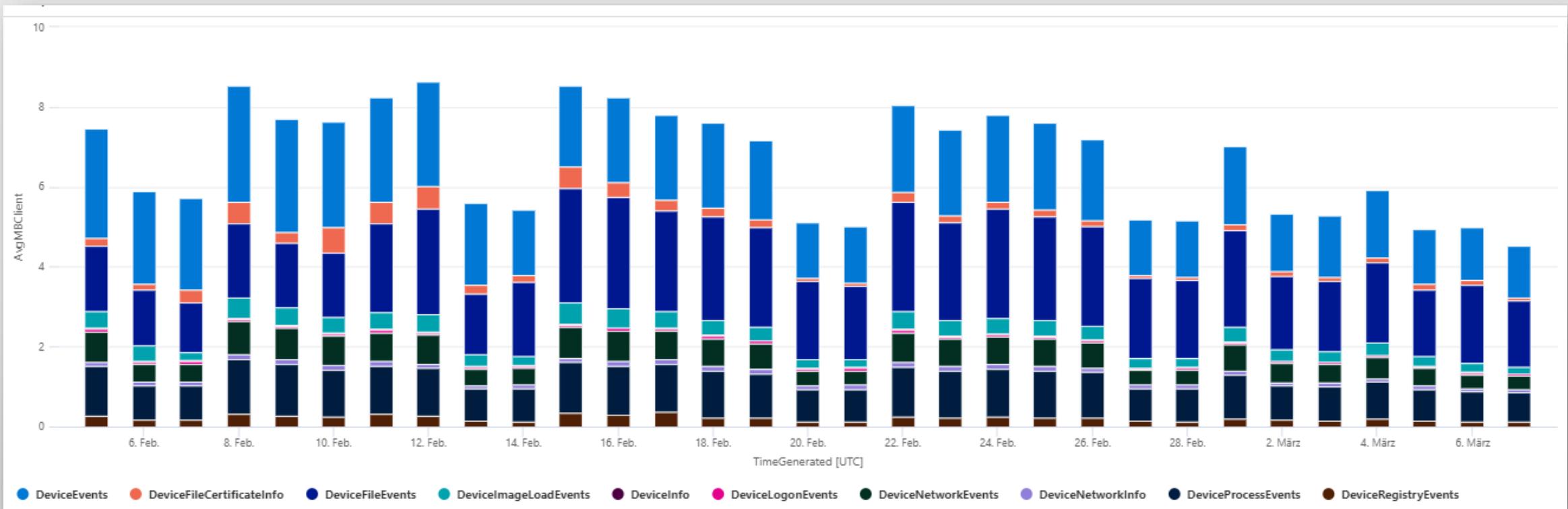
[Ingest, Archive, Search, and Restore Data in Microsoft Sentinel](#)

<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

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	...

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

< Previous 1 - 6 Next >

Create from template



RonHD

Senior pm mgr

Role

Identity

Azure AD Object ID: 541fb08-0083-4050-ab15-60fc59491b2
User Principal Name: RonHD@secop.ninja

Security Identifier: S-1-5-21-361548717-2197727142-839544746-1105
Department: --

Manager:

[Elay Levi](#)

Contact info

Office Location: HERZLIAH-AFL/3B250
City: Herzlia

Country: --

State: --
Email: itangoet@microsoft.com

Entity link

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/InsightsBlade/Overview[Investigate](#)

Overview

[Search](#)

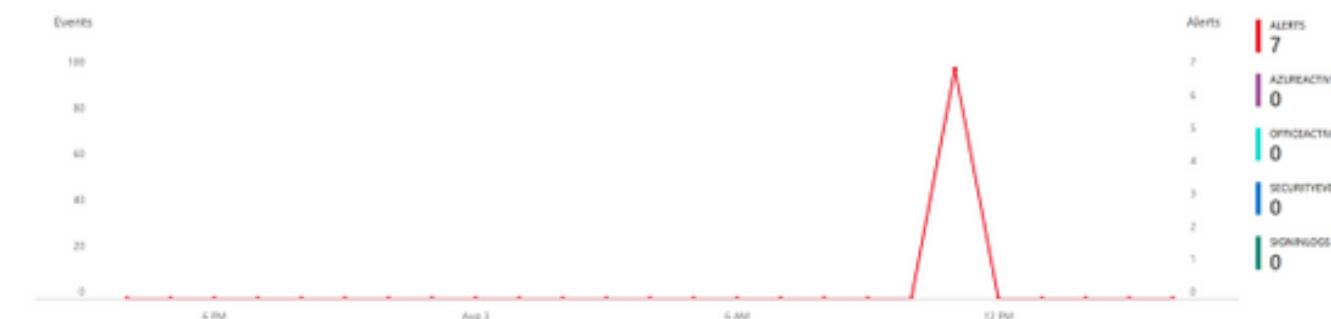
Time range: 8/2/2021, 3:44:37 PM - 8/3/2021, 3:44:37 PM

Timeline content: All

Alerts: All

Activities: [Karen test1](#)[More \(2\)](#)

Events and alerts over time



Alerts and activities timeline

- ! Suspicious Permission Groups Discovery
Detected by Microsoft Defender Advanced Threat Protection | 8/3/2021, 11:19:55 AM
A known tool or technique was used to gather information on this device. Attackers might be trying to gain access.
Related incident: [25602](#)
- ! Suspicious User Account Discovery
Detected by Microsoft Defender Advanced Threat Protection | 8/3/2021, 11:19:55 AM
A known tool or technique was used to gather information on this device. Attackers might be trying to gain access.
Related incident: [25603](#)
- ! Suspicious sequence of exploration activities
Detected by Microsoft Defender Advanced Threat Protection | 8/3/2021, 11:10:34 AM
A process called a set of windows commands. These commands can be used by attackers in order to identify the system.
Related incident: [25594](#)
- ! Anomalous account lockups
Detected by Microsoft Defender Advanced Threat Protection | 8/3/2021, 11:10:34 AM
An anomalous chain of attempts to look up user account information has been observed. An attacker might be trying to gain access.
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

No results

^ Watchlist Templates Insights (Preview)

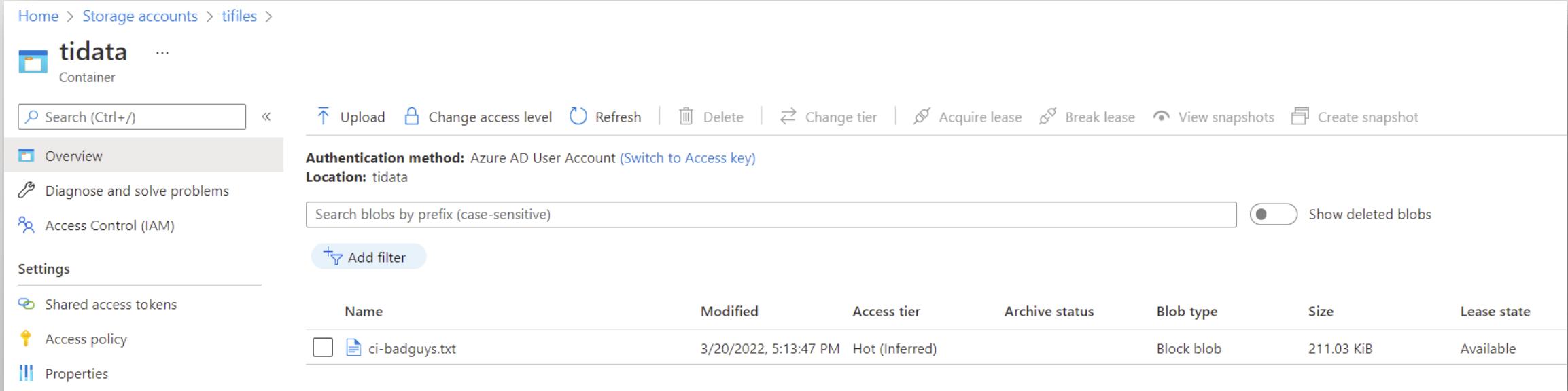
Watchlist insight	Additional Data	Tags
User is an owner of a service ac...	Service UPN: my4...	Hilary...
User is an owner of a service ac...	Service UPN: your...	Github...
User is tagged as VIP	Last Update Time: ...	CVP
User is terminated	Notification Data: ...	Azure Sentinel

✓ 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.



The screenshot shows the Azure Storage account interface for the container 'tidata'. The left sidebar includes links for Home, Storage accounts, tifiles, Overview, Diagnose and solve problems, Access Control (IAM), Shared access tokens, Access policy, and Properties. The main area displays a single blob named 'ci-badguys.txt' with the following details:

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
ci-badguys.txt	3/20/2022, 5:13:47 PM	Hot (Inferred)		Block blob	211.03 KiB	Available

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Microsoft Sentinel > Microsoft Sentinel >

Watchlist wizard

Create new watchlist

General Source Review and create

Name * ✓

Description ✓

Alias * ✓

Next: Source >

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Microsoft Sentinel > Microsoft Sentinel >

Watchlist wizard

Create new watchlist

Source type

File type

Number of lines before row with headings * ✓

Blob SAS URL (Preview) * ✓

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 *

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.](#)

Previous **Next: Review and create >**

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

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

My Watchlists				Templates (Preview)	
<input type="checkbox"/> Name ↑↓	<input type="checkbox"/> Alias ↑↓	<input type="checkbox"/> Source ↑↓	<input type="checkbox"/> Created ↑↓		
<input type="checkbox"/> CNSArmyList	CNSArmyList	ci-badguys.txt	03/20/22, ...		

Upload in progress. Watchlist data may not be available for queries until the status shows succeeded.

▶ Run Time range : Set in query Save Share New alert rule Export Pin to

```

1 // The CINS Army List - uploaded as watchlist
2 // https://cinsscore.com/#list
3 let CNSArmyList = GetWatchlist('CNSArmyList') | project IP;
4 DeviceNetworkEvents
5 | where TimeGenerated > ago(30d)
6 | where RemoteIP in (CNSArmyList)
7 | project TimeGenerated, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort, ActionType
8
9

```

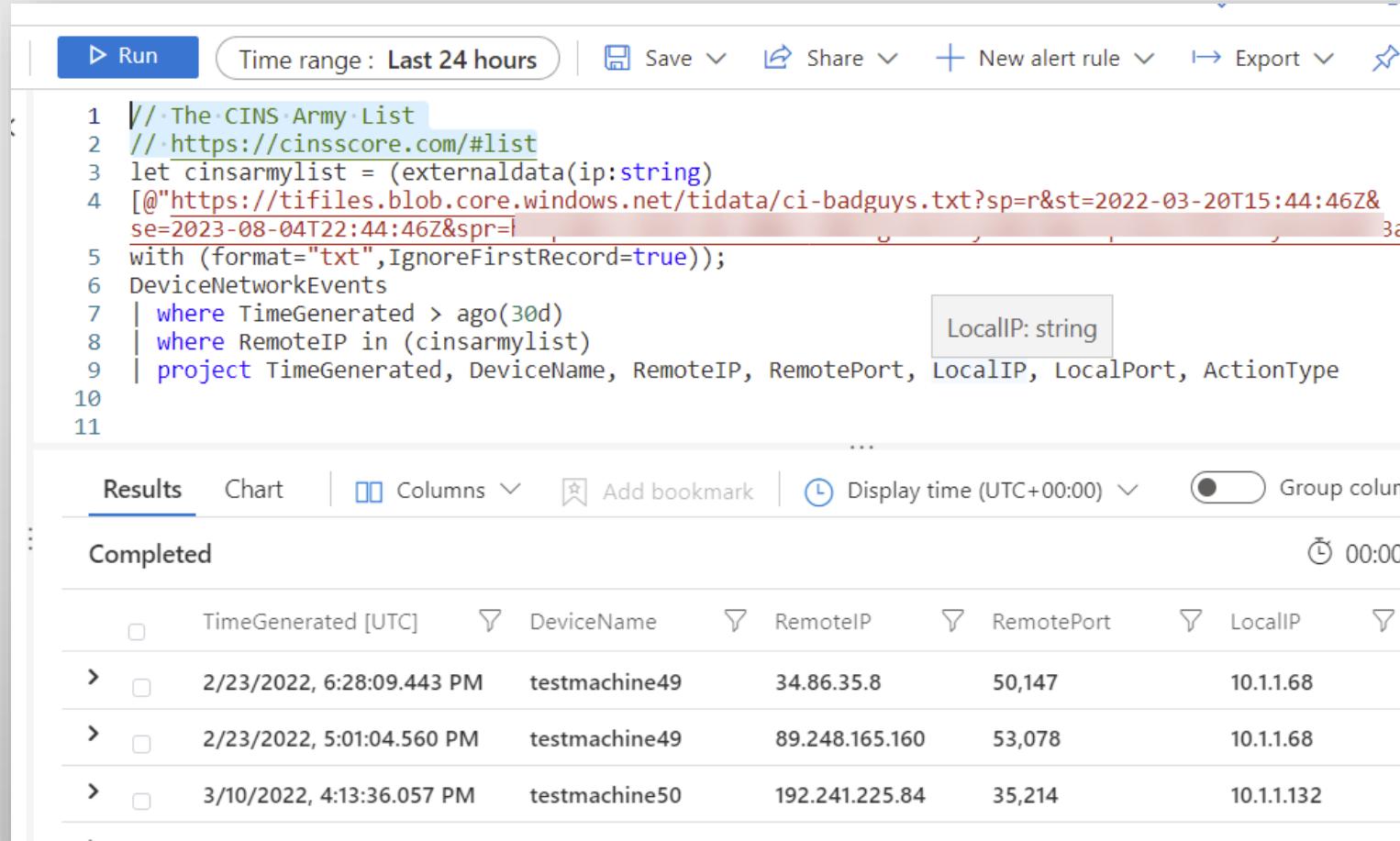
Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed

	TimeGenerated [UTC]	DeviceName	RemoteIP	RemotePort	LocalIP	LocalPort
>	2/23/2022, 6:28:09.443 PM	testmachine49	34.86.35.8	50,147	10.1.1.68	3,389
>	2/23/2022, 5:01:04.560 PM	testmachine49	89.248.165.160	53,078	10.1.1.68	3,389
>	3/10/2022, 4:13:36.057 PM	testmachine50	192.241.225.84	35,214	10.1.1.132	3,389
>	3/10/2022, 6:33:08.105 PM	testmachine50	192.241.213.25	42,338	10.1.1.132	3,389
>	3/10/2022, 7:02:11.294 PM	testmachine50	185.136.150.222	53,792	10.1.1.132	3,389

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

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



The screenshot shows a Power BI Data Studio interface with the following details:

- Top Bar:** Includes "Run" button, "Time range: Last 24 hours", "Save", "Share", "New alert rule", "Export", and a gear icon.
- Query Editor:** Displays the following Kusto Query Language (KQL) code:

```
1 // The CINS Army List
2 // https://cinsscore.com/#list
3 let cinsarmylist = (externaldata(ip:string)
4 [@"https://tfiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-03-20T15:44:46Z&
se=2023-08-04T22:44:46Z&spr=l
5 with (format="txt",IgnoreFirstRecord=true));
6 DeviceNetworkEvents
7 | where TimeGenerated > ago(30d)
8 | where RemoteIP in (cinsarmylist)
9 | project TimeGenerated, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort, ActionType
10
11
```
- Results Tab:** Selected tab, showing the results of the query.
- Results View:** A table with the following columns and data:

TimeGenerated [UTC]	DeviceName	RemoteIP	RemotePort	LocalIP
2/23/2022, 6:28:09.443 PM	testmachine49	34.86.35.8	50,147	10.1.1.68
2/23/2022, 5:01:04.560 PM	testmachine49	89.248.165.160	53,078	10.1.1.68
3/10/2022, 4:13:36.057 PM	testmachine50	192.241.225.84	35,214	10.1.1.132



Endpoint DLP



AutoSave On

top secret today.docx • Saving...

Sam Brown SB

File Home Insert Draw Design Layout References Mailings Review View Help

Clipboard Paste Calibri (Body) 11
Font B I U ab x² A² A² A² A²

Paragraph Styles Editing Dictate Voice

Sensitivity sam@verboon.online
Personal Public Internal Secret
 Top Secret Ultra Secret

Hello Workplace Ninjas

This is super-SECRET

Page 1 of 1 6 words Top Secret Accessibility: Investigate Focus

Data Loss Prevention

Host Name Your organization's policy

Machine Domains
Logged On User
Last Boot Time
OS Version:
Service Pack:
IP Address:
Subnet Mask:
DNS Server:
Default Gateway

Transferring top secret today.docx via Remote Desktop is not recommended. If you allow it, you'll need to try again.

Business justification

Enter up to 250 characters.

Dismiss Allow

7°C Regen 7:23 PM 3/31/2022 6

The content of this document is top secret

Check This out

Page 1 of 1 10 of 11 words Top Secret Accessibility: Good

3D Objects

- Desktop
- Documents
- Downloads
- Music

3 items | 1 item selected 35.9 KB | Available on this device

Management - Top S... Last Modified: March 1

Sam Brown SB

Comments Share

Font

Paragraph

Data Loss Prevention

Your organization's policy

Copying while Management - Top Secret.docx is open is not recommended. If you allow it, you'll need to copy again.

Business justification

Enter up to 250 characters.

Dismiss Allow

FILE-EXPRESS | Send files https://app.file-express.ch/de/transfer

Send files

Recipients

Add one or multiple recipients

Override Cancel

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](#)

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

Regnerisch 7:31 PM 3/31/2022

Microsoft 365 compliance

Data loss prevention > Edit policy

Name your policy

Locations to apply the policy

- Advanced DLP rules
- Test or turn on the policy
- Review your settings

Exchange email Off

SharePoint sites Off

OneDrive accounts Off

Teams chat and channel messages Off

Devices On

All	Choose user or group	None	Exclude user or group
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Microsoft Defender for Cloud Apps Off

On-premises repositories Off

Power BI (preview) Off

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

Microsoft 365 compliance

Data loss prevention > Edit policy

Name your policy

Locations to apply the policy

Advanced DLP rules

Test or turn on the policy

Review your settings

Edit rule

Cloud or hybrid activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.

[Learn more restricting device activity](#)

Service domain and browser activities

Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

Upload to a restricted cloud service domain or access from an unallowed browsers Block with o... ▾

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

Don't restrict file activity

Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

<input checked="" type="checkbox"/> Copy to clipboard	Block with o... ▾
<input checked="" type="checkbox"/> Copy to a USB removable media	Block with o... ▾
<input checked="" type="checkbox"/> Copy to a network share	Block with o... ▾
<input checked="" type="checkbox"/> Print	Block ▾
<input checked="" type="checkbox"/> Copy or move using unallowed Bluetooth app	Block with o... ▾
<input checked="" type="checkbox"/> Remote desktop services	Block with o... ▾

File activities for apps in restricted app groups (preview)

Restrictions enforced for apps in restricted app groups will override any restrictions you configured in 'File activities for all apps' above. If an app is included in more than one app group, restrictions from the first app group you add will be enforced.

Microsoft 365 compliance

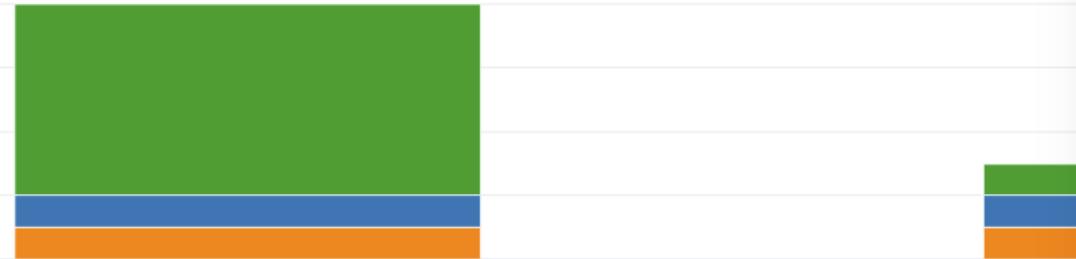
Data classification

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, SharePoint, and OneDrive. Learn more

Built-in filters Reset Filters

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



Activity details

Activity	Happened
File copied to cloud	Mar 31, 2022 7:31 PM
Client IP	How applied
83.78.30.236	None
Label event type	Enforcement mode
None	Warn
Target domain	
app.file-express.ch	

About this item

File	User
Management - Secret.docx	sam@verboon.online
File extension	File size
docx	64 KB
Sensitivity label	Sensitive info type
Secret	
DLP policy	DLP rule
DEMO - Protect Secret - Endpoint	SecretDocumentDevice
Sha1	
3a2b763f329116bc667f6b0abacd6d476d1a088	
Sha256	
f6a67ead4df17c906fe8b5ded4ab10fc66ac4c59d872a4b55e40fa5a58d12296	

Location details

Location	Endpoint devices
Parent	C:\Users\sam\avmtpLab\DLP - Management
File path	

Export Refresh

Activity	File	Location	User	Happened
<input checked="" type="checkbox"/> File copied to cloud	C:\Users\sam\avmtpLab\DLP - Management\Management - Secret....	Endpoint devices	sam@verboon.online	Mar 31, 2022 7:31 PM
<input type="checkbox"/> File copied to clipboard	C:\Users\sam\avmtpLab\DLP - Management\Management - Top Se... Endpoint devices	Endpoint devices	sam@verboon.online	Mar 31, 2022 7:29 PM
<input type="checkbox"/> 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
<input type="checkbox"/> File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:58 PM
<input type="checkbox"/> File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:57 PM
<input type="checkbox"/> File copied to remote desktop session	C:\Users\sam\Documents\topsecret special.docx	Endpoint devices	sam@verboon.online	Mar 30, 2022 7:54 PM

Microsoft Defender for Endpoint

Log4J - Detection & Remediation



Microsoft Defender for Endpoint Log4J remediation

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

[Export](#)

Filters: Status: Active +1 [X](#)

Security recommendation	OS platform	Weight
<input checked="" type="checkbox"/> Attention required: Devices found with vulnerable Apache Log4j versions	Windows	2

Attention required: Devices found with vulnerable Apache Log4j versions

[Remediation required](#)

[Report inaccuracy](#)

General Exposed devices Vulnerable files Associated CVEs

Description

This recommendation provides a list of devices and paths where a vulnerable Apache Log4j 2 version was found.

Log4j 2 is a Java-based logging library that is widely used in business system development, included in various open-source libraries, and directly embedded in major software applications.

A critical remote code execution (RCE) vulnerability in Apache Log4j 2 was disclosed on December 9, 2021.

For more information related to this threat, as well as vulnerability-specific mitigation instructions, read more in the [CVE-2021-44228 Log4j active exploitation](#) threat analytics report.

On December 14, 2021, CVE-2021-45046 was published after it was found that the fix to address CVE-2021-44228 was incomplete in certain non-default configurations, resulting in an information leak and remote code execution in some environments and local code execution in all environments, with RCE demonstrated on macOS but no other tested environments. Read more about CVE-2021-45046 in the 'Associated CVEs' tab.

Associated CVEs



[Request remediation](#)

[Exception options](#)

Details

Number of vulnerabilities
2

Exploit available
Yes

Exposed devices
1 / 5

Impact
▼ 0.30

Exposed operating systems
Windows Server 2019

- ≡
- [*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

[Export](#)

 Filters: Status: Active +1 [X](#)

Security recommendation

OS platform

We

 Attention required: Devices found with vulnerable Apache Log4j versions

Windows

2

Attention required: Devices found with vulnerable Apache Log4j versions

[Remediation required](#)
[Report inaccuracy](#)
[General](#)
[Exposed devices](#)
[Vulnerable files](#)
[Associated CVEs](#)
[Export](#)

1 item

[Search](#)

Name	OS platform	Last seen
[Redacted]	Windows Server 2019	1/18/2022

[Request remediation](#)
[Exception options](#)


Security recommendations

Export

Filters: Status: Active +1 X

Security recommendation	OS platform	W...
Attention required: Devices found with vulnerable Apache Log4j versions	Windows	2

Attention required: Devices found with vulnerable Apache Log4j versions

Remediation required

Report inaccuracy

General Exposed devices Vulnerable files Associated CVEs

Export 2 items Search Customize columns

Path	Exposed devices	Version	Vulnerabilities
c:\program files\netapp\essentials\au\lib\log4j-core.jar	1	2.5.0.0	CVE-2021-44228 (+1)
C:\Program Files\NetApp\essentials\au\lib\log4j-core.jar	1	2.5.0.0	CVE-2021-44228 (+1)

Request remediation Exception options

- ≡
- 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

Export

Filters: Status: Active +1 X

Security recommendation	OS platform	W...
Attention required: Devices found with vulnerable Apache Log4j versions	Windows	2

Attention required: Devices found with vulnerable Apache Log4j versions

Remediation required

Report inaccuracy

General Exposed devices Vulnerable files Associated CVEs

Export 2 items Search

Name	Severity	Published on	Exposed devices
CVE-2021-45046	■■■■ Critical	12/14/2021	1
CVE-2021-44228	■■■■ Critical	12/9/2021	1

Request remediation Exception options

Security recommendations

Export

Filters: Status: Active +1 X

Security recommendation	OS platform	Weight
Attention required: Devices found with vulnerable Apache Log4j versions	Windows	2

Request remediation Exception options

Attention required: Devices found with vulnerable Apache Log4j versions

Remediation required

Report inaccuracy

General	Exposed devices	Vulnerable files
Export	Name	Severity
CVE-2021-45046	■■■■ Critical	
CVE-2021-44228	■■■■ Critical	

Request remediation Exception options

CVE-2021-44228

Open vulnerability page Report inaccuracy

Legal Notice The vulnerability data provided and shown as part of your Microsoft 365 security information is for informational purposes only.

Vulnerability description

This vulnerability affects the following vendors: Apache, Netapp, Elasticsearch, Symantec, Vmware, Splunk, Ubuntu, Oracle, Red_Hat, Centos, Suse, Debian, Ubiquiti_Networks, Ibm, Jboss, Cisco, Dell, Metabase, Neo4j, Openhab, Dell_Emc, Papercut, Philips, Sonicwall, Tableau, Code42, Intel, Ivanti, Schneider-Electric, Siemens, Tableausoftware, Avaya, Fedora, Snowsoftware, Microsoft. To view more details about this vulnerability please visit the vendor website. Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. Apache Log4j versions prior to 2.15.0 are susceptible to a vulnerability. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. The full list of impacted applications has not yet been determined at this point. Microsoft is continuously investigating the vulnerability and affected applications. We will update this entry additional information guidance as more details become available.

Vulnerability details

Vulnerability name	Severity
CVE-2021-44228	■■■■ Critical
CVSS	Published on
10.0	12/9/2021
Updated on	Age
1/12/2022	a month
Related software	
Apache Log4j (+ 187 more)	



Security recommendations > CVE-2021-44228

CVE-2021-44228

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available to you in its raw form, "AS IS", and may not be up to date. You bear the risk in using this data. Microsoft and its third party suppliers disclaim any and all liability.

Vulnerability summary

Tags

Details

Name	OS platform	Last seen	Vulnerable software	Vulnerable fil...	Mitigation status
[REDACTED]	Windows Server 2019	1/18/2022	Apache Log4j	2	Not applied

Mitigation options Export

1 item Search

Overview Exposed devices - onboarded (1) Vulnerable files (2) Vulnerable software (1) Security recommendations (1)

Weaknesses

Event timeline

Partners and APIs

Evaluation & tutorials

Security recommendations > CVE-2021-44228

CVE-2021-44228

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available to you in its raw form, "AS IS", and may not be up to date. You bear the risk in using this data. Microsoft and its third party suppliers disclaim any and all liability in respect of such data.

Vulnerability summary

Tags

Details

Vulnerability name	Severity
CVE-2021-44228	■■■■ Critical

CVSS	Published on
10.0	12/9/2021

Updated on	Age
1/12/2022	a month

Related software

Apache Log4j (+ 187 more)

Overview Exposed devices - onboarded (1) Vulnerable files (2) Vulnerable software (1) Security recommendations (1)

Mitigation options Export

Name	OS platform	Last seen	Vulnerable software	Vulnerable fil... Mitigation status
[REDACTED]	Windows Server 2019	1/18/2022	Apache Log4j	2 Not applied

1 item Search

Q Feedback

评价 & tutorials

Security recommendations > CVE-2021-44228

CVE-2021-44228

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available by Microsoft under the Microsoft Privacy Statement.

Vulnerability summary

Tags	Overview	Exposed devices - onboarded
	Export	
	Filters: Status: Active +1 X	
	Security recommendation	
	Attention required: Devices found	

Details

Vulnerability name	Severity
CVE-2021-44228	■■■■ Critical
CVSS	Published on
10.0	12/9/2021
Updated on	Age
1/12/2022	a month
Related software	
Apache Log4j (+ 187 more)	

Mitigation options for CVE-2021-44228

This mitigation action is meant to temporarily reduce how often a security update is applied. Review the following steps before creating a mitigation action. It can take up to 12 hours for the mitigation to take effect.

(i) Mitigation actions are only available for onboarded devices with the following OS platform: Windows Server 2022, Windows 11, Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server SAC.

Devices to mitigate *

All exposed devices
Create a mitigation action for all exposed devices in my organization.

Selected onboarded devices - 1 device selected
Create a mitigation action for specific exposed devices in my organization.

Description

This vulnerability can be mitigated by preventing exploitation through JNDI lookups.

- Creating this mitigation action will set the environment variable 'LOG4J_FORMAT_MSG_NO_LOOKUPS' to 'True', which prevents JNDI lookups on Log4j versions 2.10 - 2.14.1 with default configurations.
- If any Java application on the device uses JNDI lookups, its log strings would be affected, and log analytics products using this data could potentially be affected as well.
- You'll need to restart the device for these changes to take effect.
- Note that for certain non-default configurations, JNDI lookups might still be possible even after applying the mitigation. We recommend updating all instances of Log4j to the latest version and applying the latest security updates.
- Once applied, the mitigation can only be undone using endpoint management solutions. To learn more, [click here](#).

To read more about this mitigation, see [Microsoft's Response to CVE-2021-44228 Apache Log4j 2](#)

[Create mitigation action](#)



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

CVE-2021-44228

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available by Microsoft under the terms of the Microsoft Software License Terms.

Vulnerability summary

Tags

Details
<p>Vulnerability name: CVE-2021-44228 (Severity: Critical)</p> <p>CVSS: 10.0 (Published on: 12/9/2021)</p> <p>Updated on: 1/12/2022 (Age: a month)</p> <p>Related software: Apache Log4j (+ 187 more)</p>

Overview Exposed devices - onboarded

Export

Filters: Status: Active +1

Security recommendation

Attention required: Devices found

Mitigation options for CVE-2021-44228

A mitigation action is meant to temporarily reduce the impact of a vulnerability. It can take up to 12 hours for the mitigation to be applied.

Mitigation actions are only available for onboarded devices running Windows 10, Windows 11, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012.

Devices to mitigate *

All exposed devices

Selected onboarded devices - Choose device

1 selected

Device name	OS platform
sv-1-1-1	WindowsServer2019

Description

This vulnerability can be mitigated by preventing external JNDI lookups.

- Creating this mitigation action will set the environment variable `JNDI_BLOCKED` to `'True'`, which prevents JNDI lookups on Log4j.
- If any Java application on the device uses JNDI, this mitigation action could potentially affect other Java-based analytics products using this data.
- You'll need to restart the device for these changes to take effect.
- Note that for certain non-default configurations, this mitigation may not fully prevent the vulnerability. We recommend updating all Java applications to the latest security updates.
- Once applied, the mitigation can only be undone by removing the mitigation or clicking here.

To read more about this mitigation, see Microsoft's documentation.

Create mitigation action

Select Cancel

Security recommendations > CVE-2021-44228

CVE-2021-44228

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available by Microsoft under the terms of the Microsoft Software License Terms.

Vulnerability summary

Tags	Details
	<p>Vulnerability name CVE-2021-44228 ■■■■ Critical</p> <p>CVSS 10.0 Published on 12/9/2021</p> <p>Updated on 1/12/2022 Age a month</p> <p>Related software Apache Log4j (+ 187 more)</p>

Mitigation options for CVE-2021-44228

This mitigation action is meant to temporarily reduce risk until a security update is applied. Review the following steps before applying a mitigation action. It can take up to 12 hours for the mitigation to take effect.

Mitigation actions are only available for onboarded devices with the following OS platform: Windows Server 2022, Windows 11, Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server SAC.

Devices to mitigate *

All exposed devices
Apply a mitigation action for all exposed devices in my organization.

Selected onboarded devices - 1 device selected
Apply a mitigation action for specific exposed devices in my organization.

By proceeding, this mitigation action will be sent to all selected devices

It can take up to 12 hours for the mitigation to be applied to all selected devices.

Attention required: Devices found

Proceed **Cancel**

Attention required: Devices found

- If any Java application on the device uses JNDI lookups, its log strings would be affected, and log analytics products using this data could potentially be affected as well.
- You'll need to restart the device for these changes to take effect.
- Note that for certain non-default configurations, JNDI lookups might still be possible even after applying the mitigation. We recommend updating all instances of Log4j to the latest version and applying the latest security updates.
- Once applied, the mitigation can only be undone using endpoint management solutions. To learn more, [click here](#).

To read more about this mitigation, see [Microsoft's Response to CVE-2021-44228 Apache Log4j 2](#)

Create mitigation action



Microsoft Secure Score

Contoso Electronics Microsoft 365 Defender ⚙️ ? MA X

Home Incidents & alerts Hunting Advanced hunting Custom detection rules Actions & submissions Threat analytics Secure score Learning hub Trials Endpoints Device inventory Vulnerability management Dashboard Recommendations Remediation Software inventory Weaknesses Event timeline Partners and APIs Evaluation & tutorials Configuration management

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

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

Applied filters: Product: Defender for Endpoint

Export

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Other
No data available							

Filter

Regressed in last 90 days No Yes

Update type Microsoft added actions Microsoft updated action points

Have license? No Yes

Product

Azure Active Directory Defender for Endpoint Defender for Identity Defender for Office Exchange Online Microsoft Defender for Cloud Apps Microsoft Information Protection Microsoft Teams

Tags



Microsoft Defender for Endpoint

Enhanced Software Inventory



Home

Incidents & alerts

Hunting

Actions & submissions

Threat analytics

Secure score

Learning hub

Trials

Endpoints

Device inventory

Vulnerability management

Dashboard

Recommendations

Remediation

Software inventory

Weaknesses

Event timeline

Partners and APIs

Evaluation & tutorials

Configuration management

Configuration & baselines

Software inventory

Applications **984**

Export

Filters: Product Code (CPE): Available X

Name	OS platform	Vendor	Weaknesses	Threats	Exposed devices
Log4j	Windows	Apache	2	ⓘ ⓘ	576 / 784
Windows 10	Windows	Microsoft	1.85k	ⓘ ⓘ	1.22k / 1.65k
Defender For Endpoint	Windows	Microsoft	1	ⓘ ⓘ	1.26k / 1.96k
Office	Windows	Microsoft	144	ⓘ ⓘ	1.31k / 1.48k
Tools	Windows	Vmware	7	ⓘ ⓘ	692 / 744
Jre	Windows	Oracle	660	ⓘ ⓘ	850 / 969
Flash Player	Windows	Adobe	965	ⓘ ⓘ	188 / 227
Chrome	Windows	Google	931	ⓘ ⓘ	189 / 892
Edge Chromium-based	Windows	Microsoft	587	ⓘ ⓘ	150 / 1.31k
Openvpn	Windows	Openvpn	12	ⓘ ⓘ	160 / 176
Php	Windows	Php	517	ⓘ ⓘ	78 / 78
Zoom	Windows	Zoom	3	ⓘ ⓘ	150 / 314

Filter

X Clear filters

Product Code (CPE)

Available

Not Available

OS platform

macOS

Linux

Windows

Other

Weaknesses

Has weaknesses

No known weaknesses

Not available

Threats

Exploit is available

Exploit is verified

This exploit is part of an exploit kit

Tags

(Untagged)

EOS software

Network Device

Apply **Cancel**

No CPE, no vulnerability information

CPE



↑ ↓ ×

Previous item

Java Auto Updater

Report inaccuracy

Software details Installed devices

This software is currently not supported by threat and vulnerability management, so only limited data is available.

Software details

Vendor	OS platform
Oracle	Windows

Prevalence in organization

Installed on	Exposed devices
1.22k	150

Edge Chromium-based

Open software page Report inaccuracy

Software details Installed devices

Software details

Vendor	OS platform
Microsoft	Windows

Prevalence in organization

Installed on	Exposed devices
1.31k	150

Threat context

Exploits available	
Yes	

Recommendations

Impact	
▼ 3.06	

```
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>

