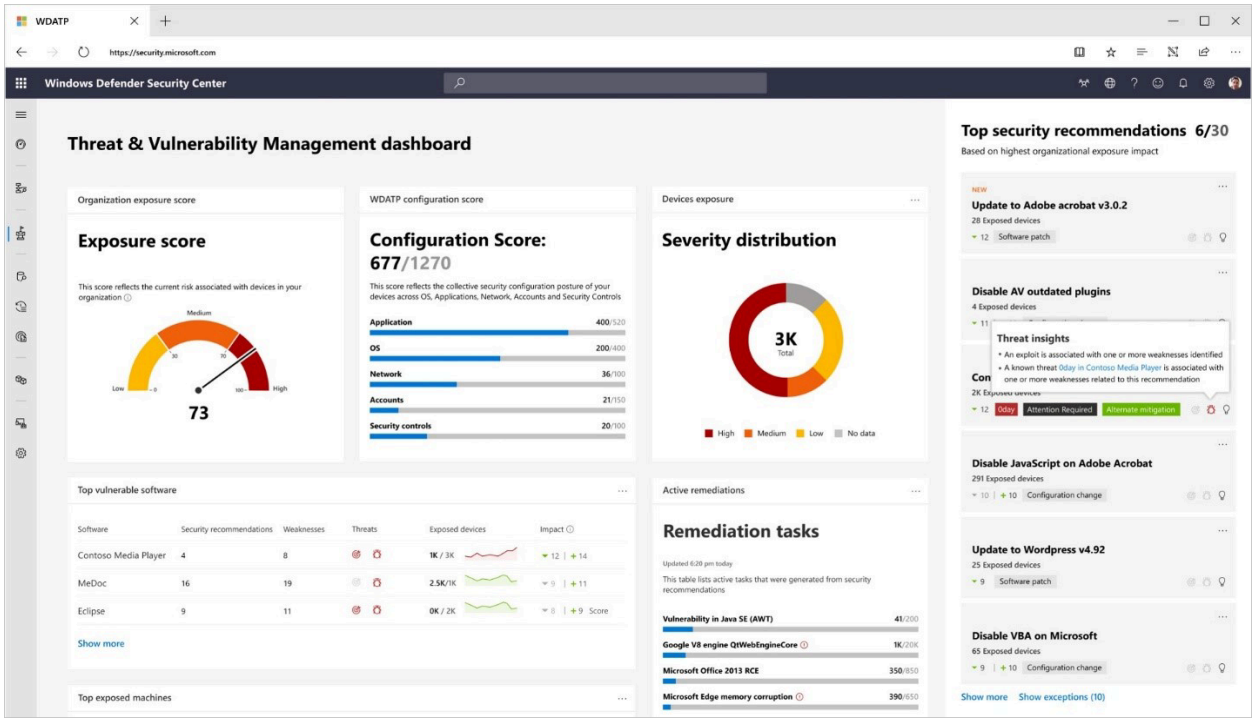
Practice security administration

By: Ryan Stewart



“Threat and vulnerability management”

Effectively identifying, assessing, and remediating endpoint weaknesses is pivotal to running a healthy security program and reducing organizational risk. Threat and vulnerability management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.

This infrastructure helps organizations discover vulnerabilities and misconfigurations in real time, based on sensors, without the need of agents or periodic scans. It prioritizes issues based on many factors. Those factors include the threat landscape, detections in your organization, sensitive information on vulnerable devices, and business context.

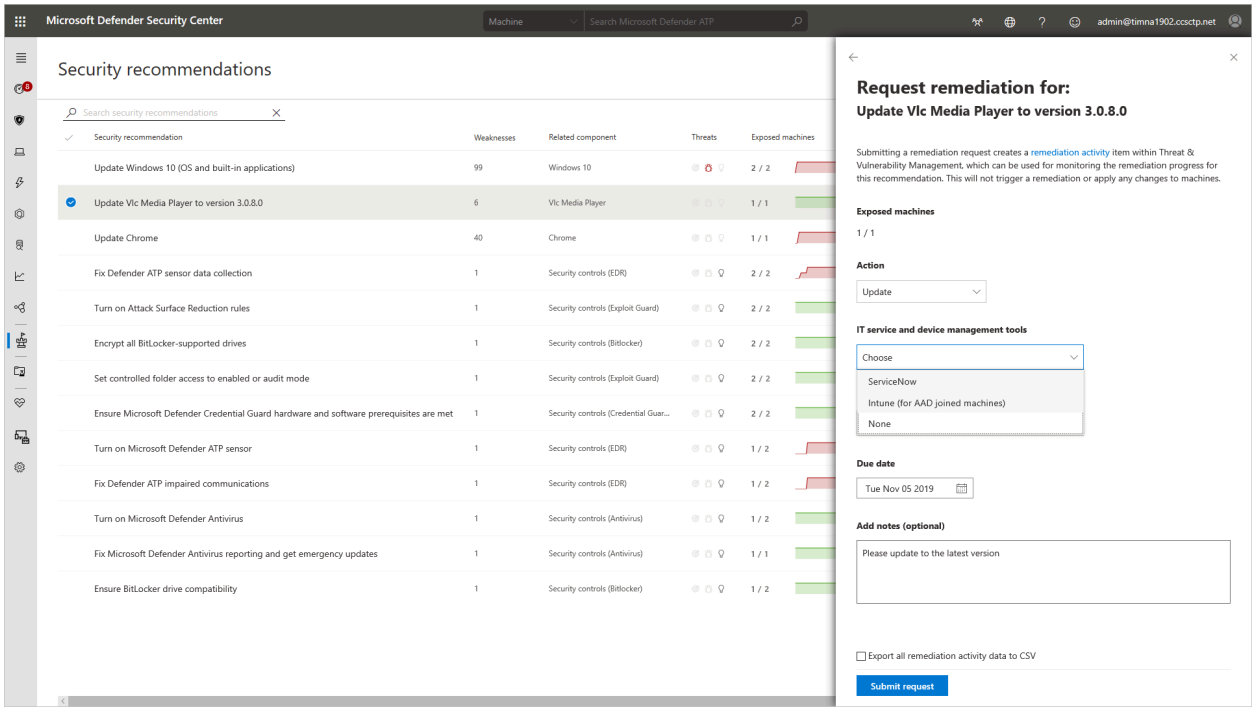
Threat and vulnerability management is built in, real-time, cloud-powered, fully integrated with the Microsoft endpoint security stack, the Microsoft Intelligent Security Graph, and the application analytics knowledge base. It can create a security task or ticket through integration with **Microsoft Intune** and **Microsoft Endpoint Manager**.

It provides the following solutions to **gaps** across security operations, security administration, and IT administration:

- Real-time endpoint detection and response (**EDR**) insights correlated with endpoint vulnerabilities
- Linked machine vulnerability and security configuration assessment data in the context of exposure discovery

- Built-in remediation processes through Microsoft Intune and Microsoft Endpoint Manager

For example, using the security recommendations present in the portal, an administrator could request an application update, which would then notify the Intune team to remediate the request.



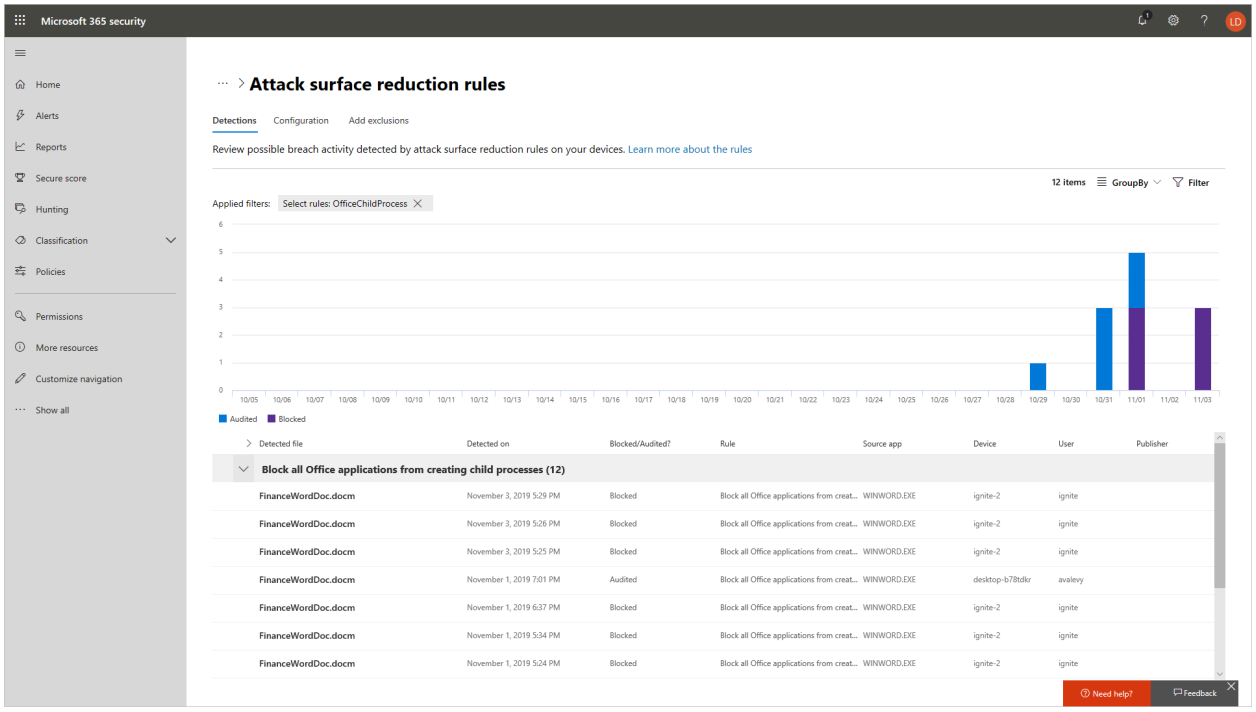
Attack surface reduction

The attack surface reduction set of capabilities provides the first line of defense in the stack by ensuring configuration settings are properly set and exploit mitigation techniques are applied.

- **Hardware-based isolation** protects and maintains the integrity of the system as it starts and while it's running, and validates system integrity through local and remote attestation. Container isolation for Microsoft Edge helps protect the host operating system from malicious websites.
- **Application control** moves away from the traditional application trust model where all applications are assumed trustworthy by default to one where applications must earn trust in order to run.
- **Exploit protection** applies mitigation techniques to apps your organization uses, both individually and organization-wide.
- **Network protection** extends the malware and social engineering protection offered by Microsoft Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices.

- **Controlled folder access** helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware.
- **Attack surface reduction** reduces the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script-, and mail-based malware.
- **Network firewall** uses host-based, two-way network traffic filtering that blocks unauthorized network traffic flowing into or out of the local device.

The below screenshot shows a chart of detections against an attack surface reduction rule that is protecting office applications:



Next generation protection

Microsoft Defender Antivirus is a **built-in** antimalware solution that provides next generation protection for desktops, portable computers, and servers. Microsoft Defender Antivirus includes:

- **Cloud-delivered protection** for near-instant detection and blocking of new and emerging threats. Along with machine learning and the Intelligent Security Graph, cloud-delivered protection is part of the next-gen technologies that power Microsoft Defender Antivirus.
- **Always-on scanning**, using advanced file and process behavior monitoring and other heuristics (also known as "real-time protection").
- Dedicated protection updates based on **machine-learning**, human and automated big-data analysis, and in-depth threat resistance research.

The following proxy and network settings should be considered:

- The **Microsoft Defender for Endpoint sensor** requires **Microsoft Windows HTTP** (WinHTTP) to report sensor data and communicate with the Microsoft Defender for Endpoint service.
- The embedded Microsoft Defender for Endpoint sensor runs in system context using the LocalSystem account. The sensor uses Microsoft Windows HTTP Services (WinHTTP) to enable communication with the Microsoft Defender for Endpoint cloud service.
- The WinHTTP configuration setting is independent of the Windows Internet (WinINet) internet browsing proxy settings and can only discover a proxy server by using the following auto discovery methods:
    - Transparent proxy
    - Web Proxy Autodiscovery Protocol (WPAD)

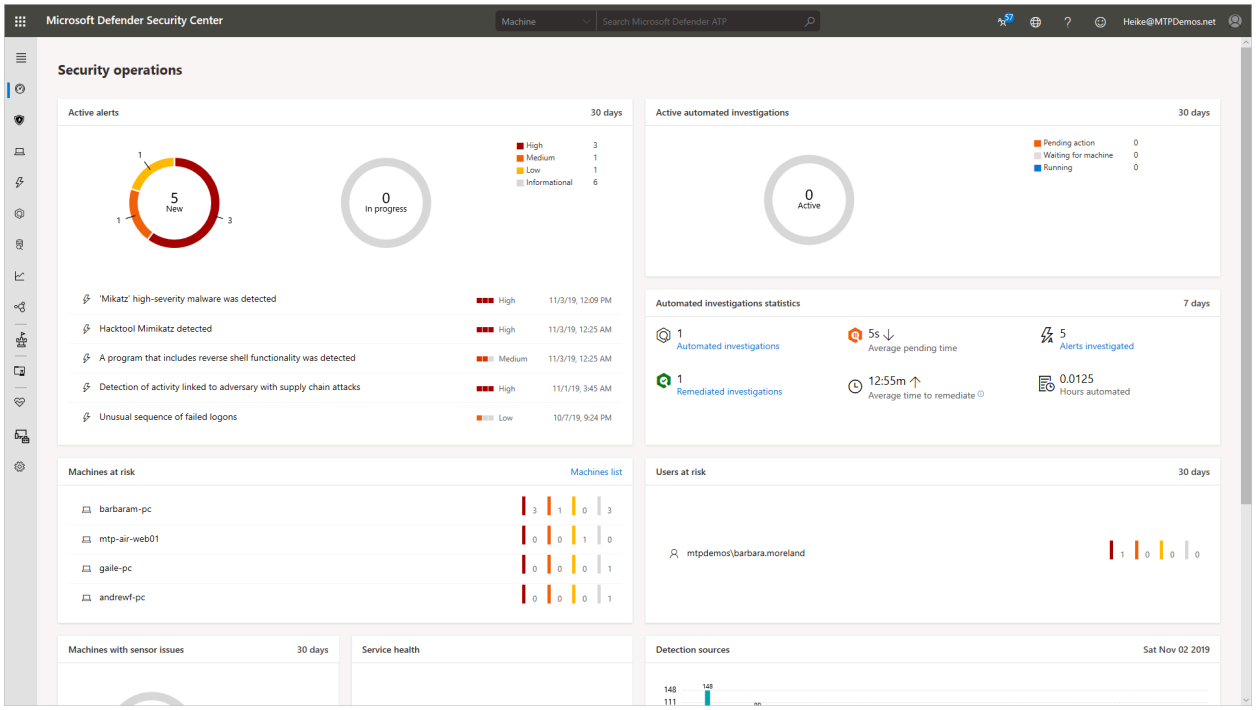
Endpoint detection and response

Microsoft Defender for Endpoint endpoint detection and response capabilities provides advanced attack detections that are **near real-time and actionable**. Security analysts can **prioritize** alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

When a threat is detected, alerts are created in the system for an analyst to investigate. Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an **incident**. Aggregating alerts in this manner makes it easy for analysts to collectively investigate and respond to threats.

Inspired by the "assume breach" mindset, Microsoft Defender for Endpoint continuously collects behavioral cyber telemetry. Which includes process information, network activities, deep optics into the kernel and memory manager, **user sign-in activities**, **registry and file system changes**, and others. The information is stored for six months, enabling an analyst to travel back in time to the start of an attack. The analyst can then pivot using various views and approach an investigation through multiple vectors.

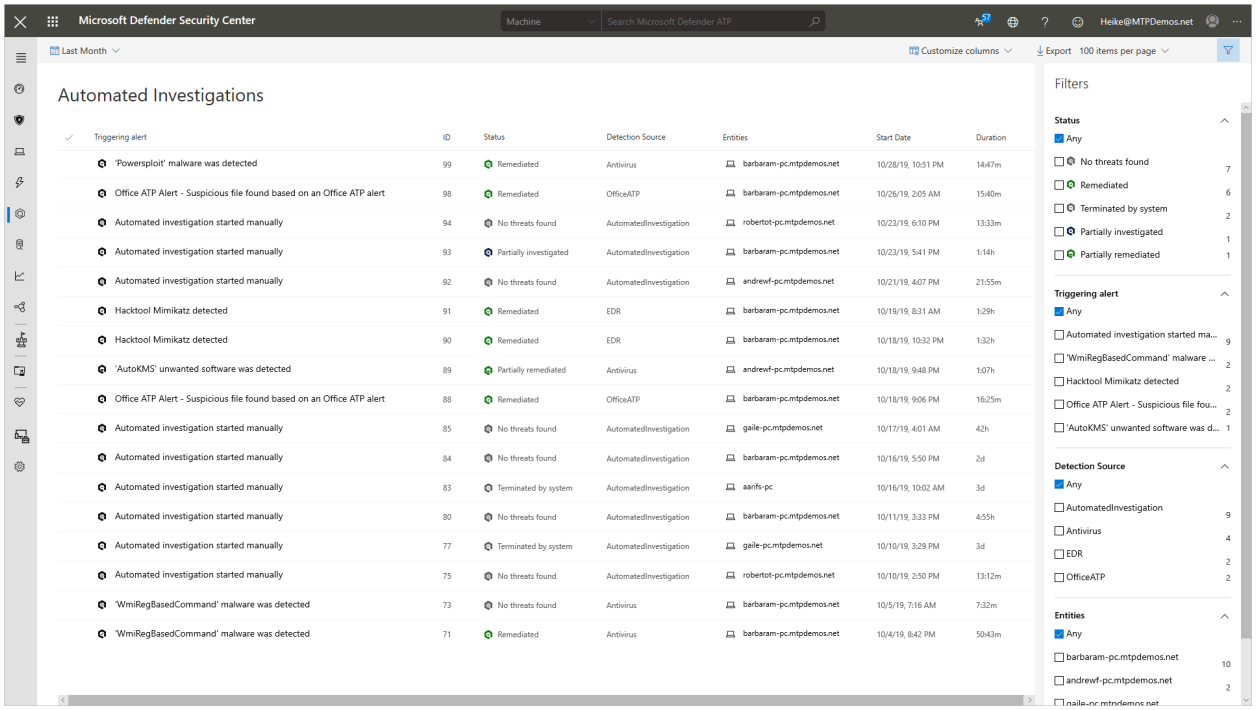
The Security operations dashboard (shown in the screenshot) is where the endpoint detection and response capabilities are surfaced. It provides a **high-level overview** of where detections were seen and highlights where response actions are needed.

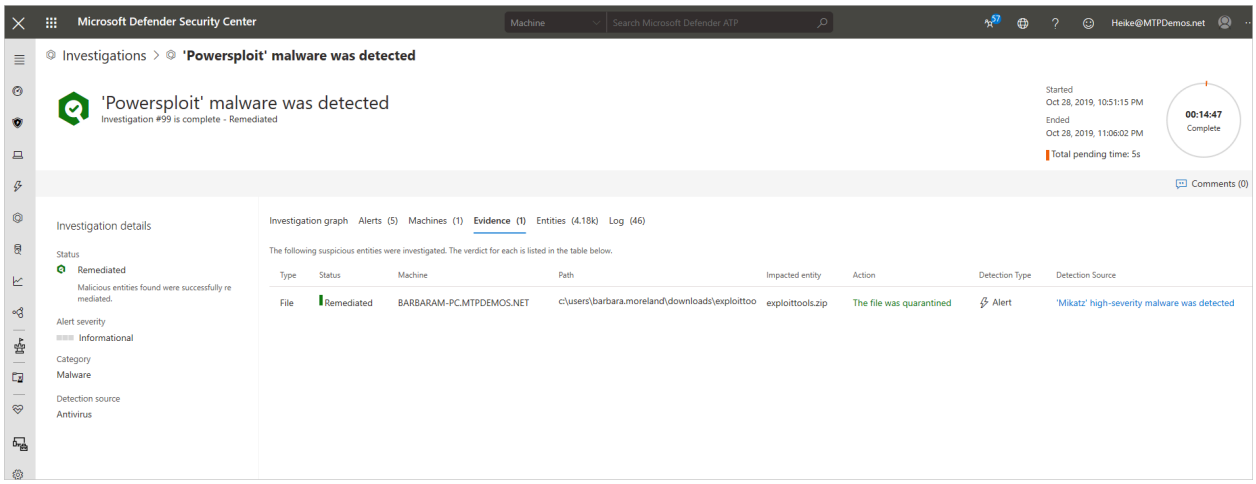


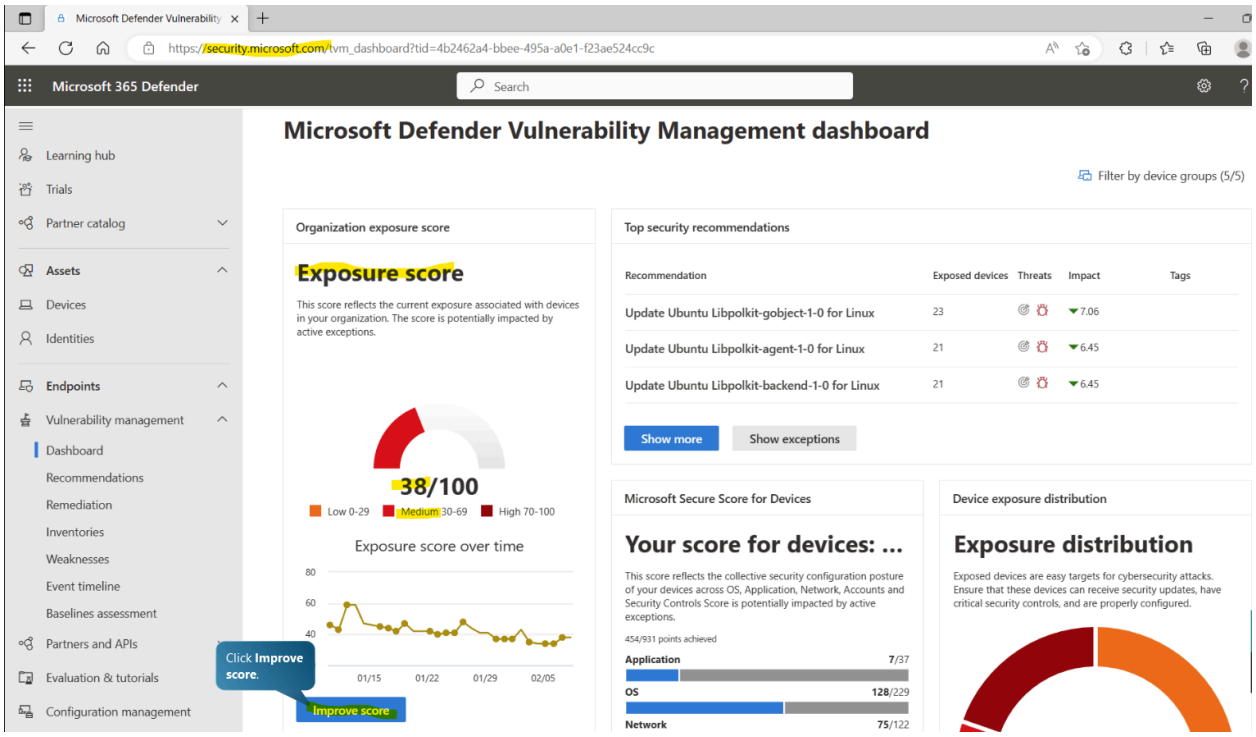
Automated investigation and remediation

Microsoft Defender for Endpoint offers a wide breadth of visibility on multiple machines. With this kind of optics, the service generates a multitude of alerts. The volume of alerts generated can be challenging for a typical security operations team to individually address. To address this challenge, Microsoft Defender for Endpoint uses automated investigation and remediation capabilities to significantly reduce the volume of alerts that must be investigated individually.

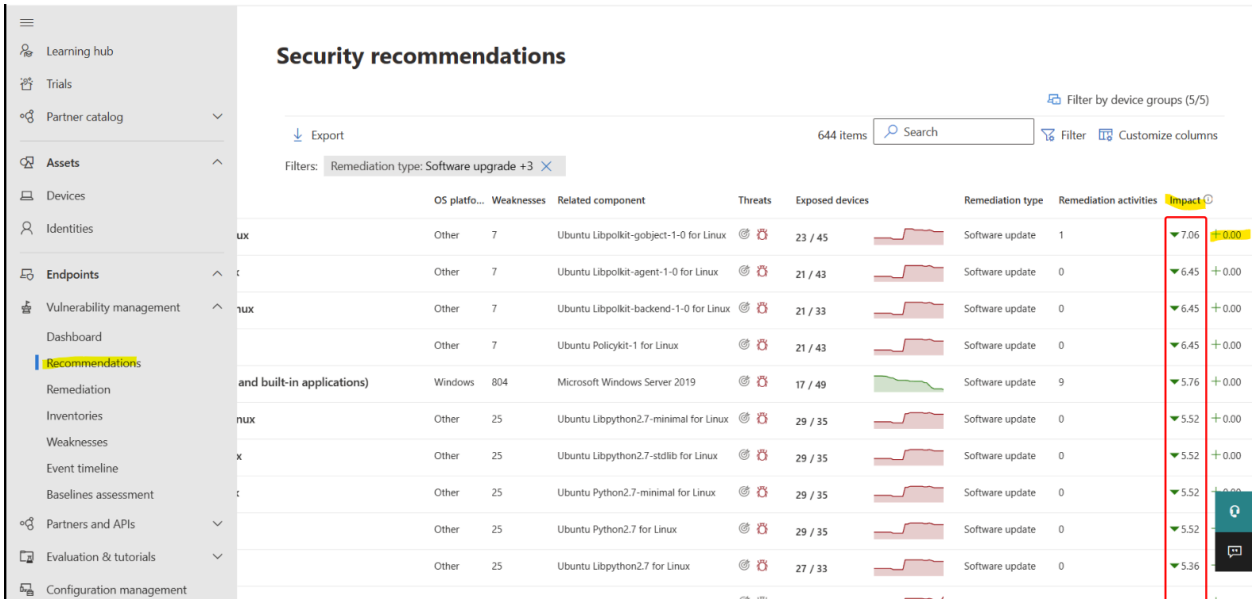
The automated investigation feature uses various inspection algorithms, and processes used by analysts (such as playbooks) to examine alerts and take immediate remediation action to resolve breaches. This significantly reduces alert volume, allowing security operations experts to focus on more sophisticated threats and other high value initiatives. In the following investigation screenshot, we can see that malware was detected, and automatically remediated:


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
Heike@MTPDemos.net
Last Month
Customize columns
Export
100 items per page
Automated Investigations
Triggering alert
ID
Status
Detection Source
Entities
Start Date
Duration
'Powersploit' malware was detected 99 Remediated Antivirus barbaram-pc.mtpdemos.net 10/28/19, 10:51 PM 14:47m
Office ATP Alert - Suspicious file found based on an Office ATP alert 98 Remediated OfficeATP barbaram-pc.mtpdemos.net 10/26/19, 2:05 AM 15:40m
Automated investigation started manually 94 No threats found AutomatedInvestigation robertot-pc.mtpdemos.net 10/23/19, 6:10 PM 13:33m
Automated investigation started manually 93 Partially investigated AutomatedInvestigation barbaram-pc.mtpdemos.net 10/23/19, 5:41 PM 1:14h
Automated investigation started manually 92 No threats found AutomatedInvestigation andrewf-pc.mtpdemos.net 10/21/19, 4:07 PM 21:55m
Hacktool Mimikatz detected 91 Remediated EDR barbaram-pc.mtpdemos.net 10/19/19, 8:31 AM 1:29h
Hacktool Mimikatz detected 90 Remediated EDR barbaram-pc.mtpdemos.net 10/18/19, 10:32 PM 1:32h
'AutoKMS' unwanted software was detected 89 Partially remediated Antivirus andrewf-pc.mtpdemos.net 10/18/19, 9:48 PM 1:07h
Office ATP Alert - Suspicious file found based on an Office ATP alert 88 Remediated OfficeATP barbaram-pc.mtpdemos.net 10/18/19, 9:06 PM 16:25m
Automated investigation started manually 85 No threats found AutomatedInvestigation gaile-pc.mtpdemos.net 10/17/19, 4:01 AM 42h
Automated investigation started manually 84 No threats found AutomatedInvestigation barbaram-pc.mtpdemos.net 10/16/19, 5:50 PM 2d
Automated investigation started manually 83 Terminated by system AutomatedInvestigation aarifs-pc 10/16/19, 10:02 AM 3d
Automated investigation started manually 80 No threats found AutomatedInvestigation barbaram-pc.mtpdemos.net 10/11/19, 3:33 PM 4:55h
Automated investigation started manually 77 Terminated by system AutomatedInvestigation gaile-pc.mtpdemos.net 10/10/19, 3:29 PM 3d
Automated investigation started manually 75 No threats found AutomatedInvestigation robertot-pc.mtpdemos.net 10/10/19, 2:50 PM 13:12m
'WmiRegBasedCommand' malware was detected 73 No threats found Antivirus barbaram-pc.mtpdemos.net 10/5/19, 7:16 AM 7:32m
'WmiRegBasedCommand' malware was detected 71 Remediated Antivirus barbaram-pc.mtpdemos.net 10/4/19, 8:42 PM 50:43m
Filters
Status
Any
No threats found 7
Remediated 6
Terminated by system 2
Partially investigated 1
Partially remediated 1
Triggering alert
Any
Automated investigation started ma... 9
'WmiRegBasedCommand' malware ... 2
Hacktool Mimikatz detected 2
Office ATP Alert - Suspicious file fou... 2
'AutoKMS' unwanted software was d... 1
Detection Source
Any
AutomatedInvestigation 9
Antivirus 4
EDR 2
OfficeATP 2
Entities
Any
barbaram-pc.mtpdemos.net 10
andrewf-pc.mtpdemos.net 2

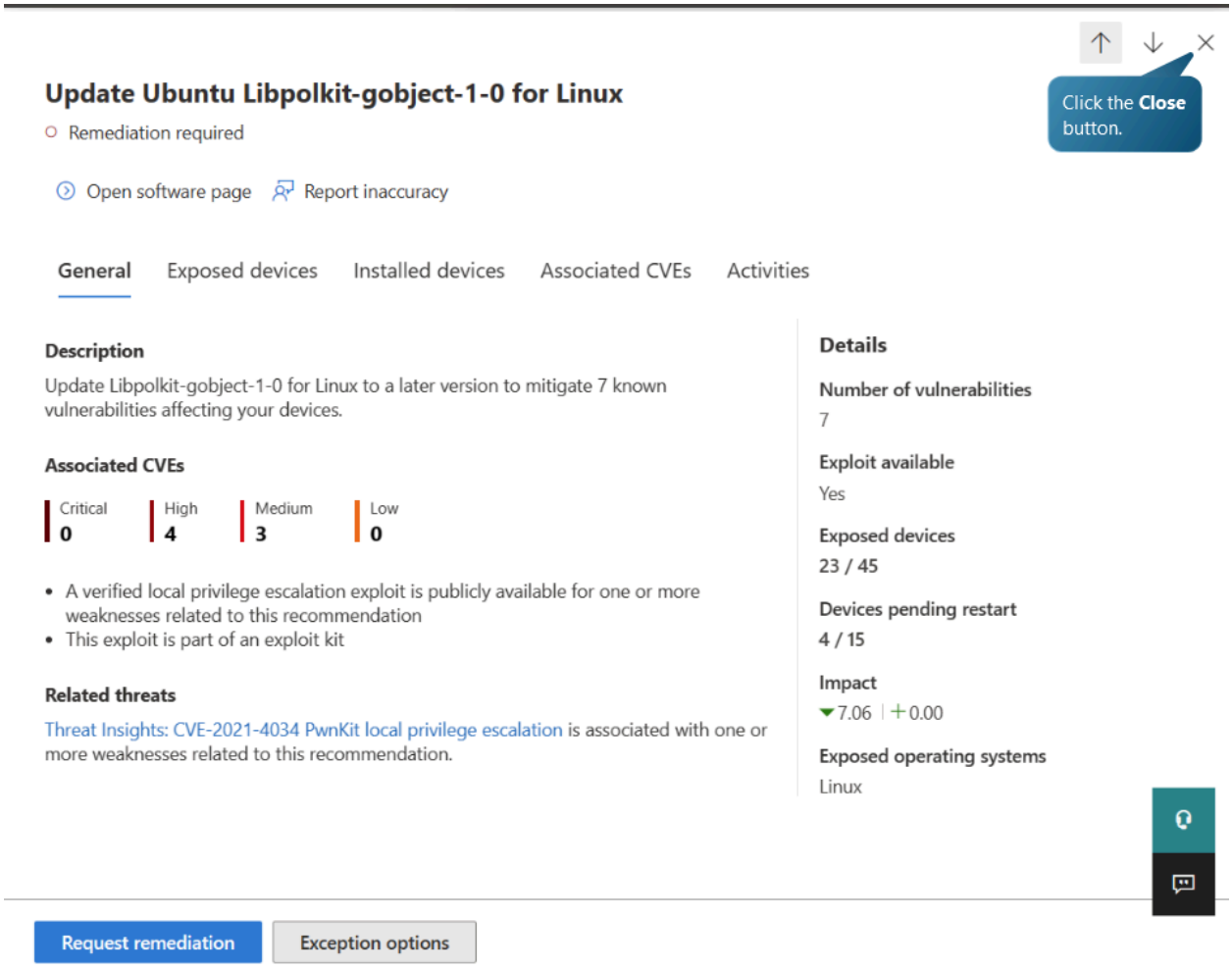

Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
Heike@MTPDemos.net
Investigations > 'Powersploit' malware was detected
'Powersploit' malware was detected
Investigation #99 is complete - Remediated
Started
Oct 28, 2019, 10:51:15 PM
Ended
Oct 28, 2019, 11:06:02 PM
Total pending time: 5s
00:14:47
Complete
Comments (0)
Investigation details
Status
Remediated
Malicious entities found were successfully re mediated.
Alert severity
Informational
Category
Malware
Detection source
Antivirus
Investigation graph
Alerts (5)
Machines (1)
Evidence (1)
Entities (4.18k)
Log (46)
The following suspicious entities were investigated. The verdict for each is listed in the table below.
Type
Status
Machine
Path
Impacted entity
Action
Detection Type
Detection Source
File
Remediated
BARBARAM-PC.MTPDEMOS.NET
c:\users\barbara.moreland\downloads\exploittoo
exploittools.zip
The file was quarantined
Alert
'Mikatz' high-severity malware was detected

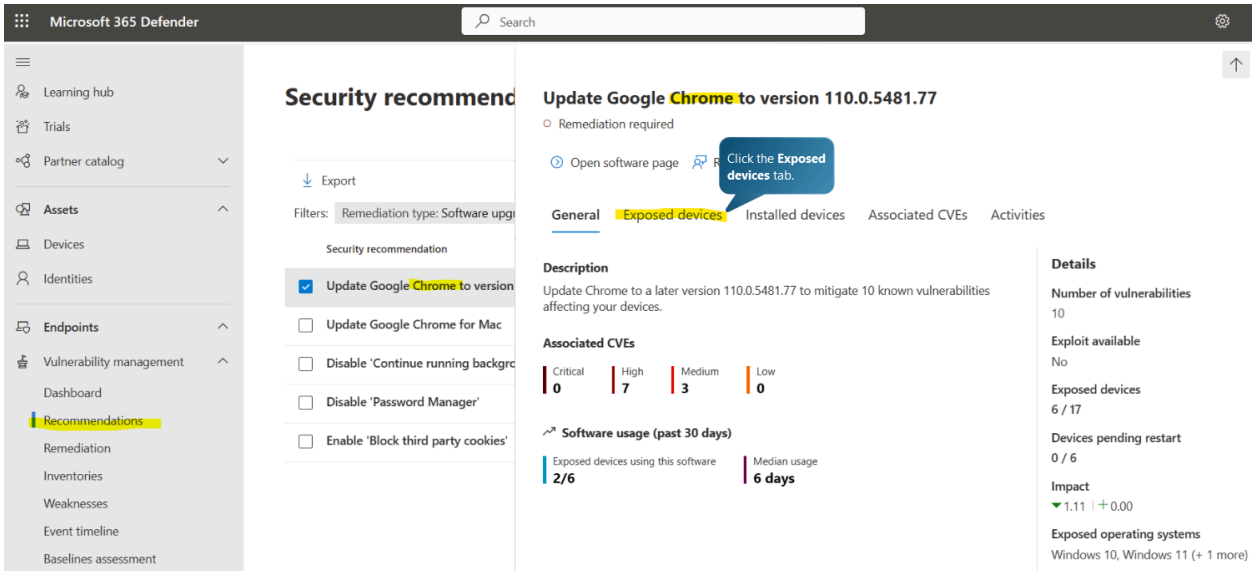


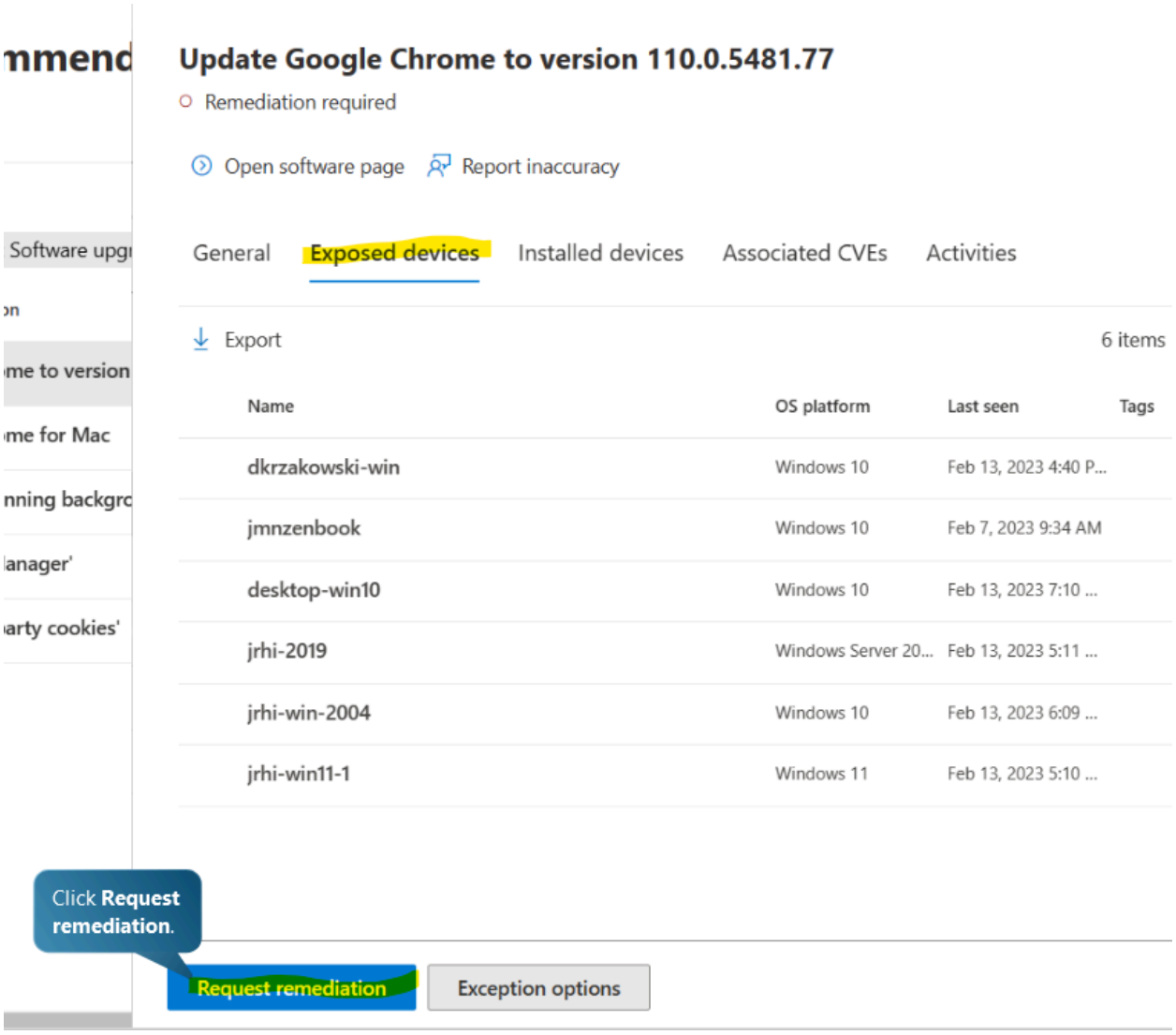
- Your exposure score reflects how vulnerable your organization is to cybersecurity threats. A low exposure score means your devices are less vulnerable to exploitation.

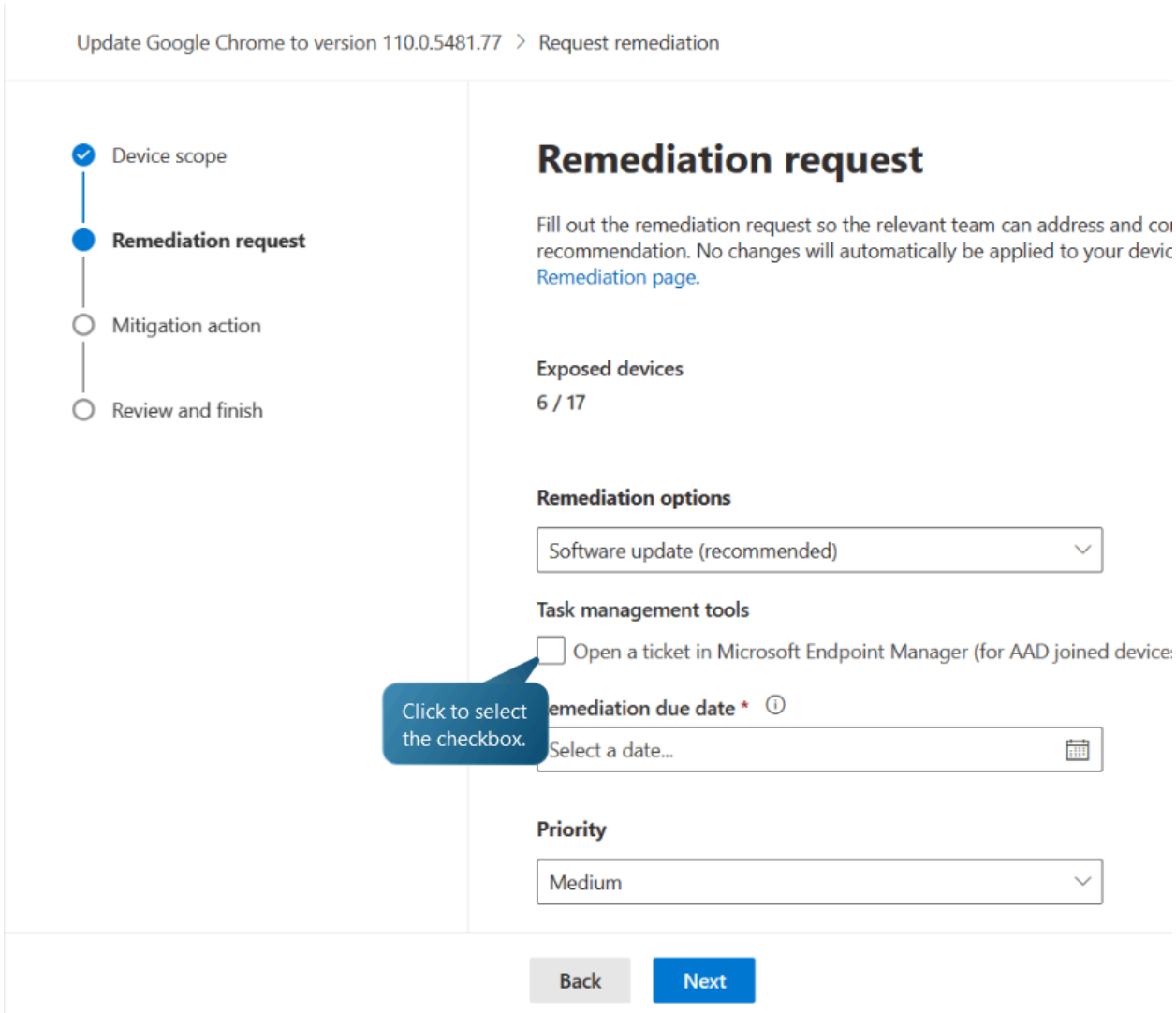


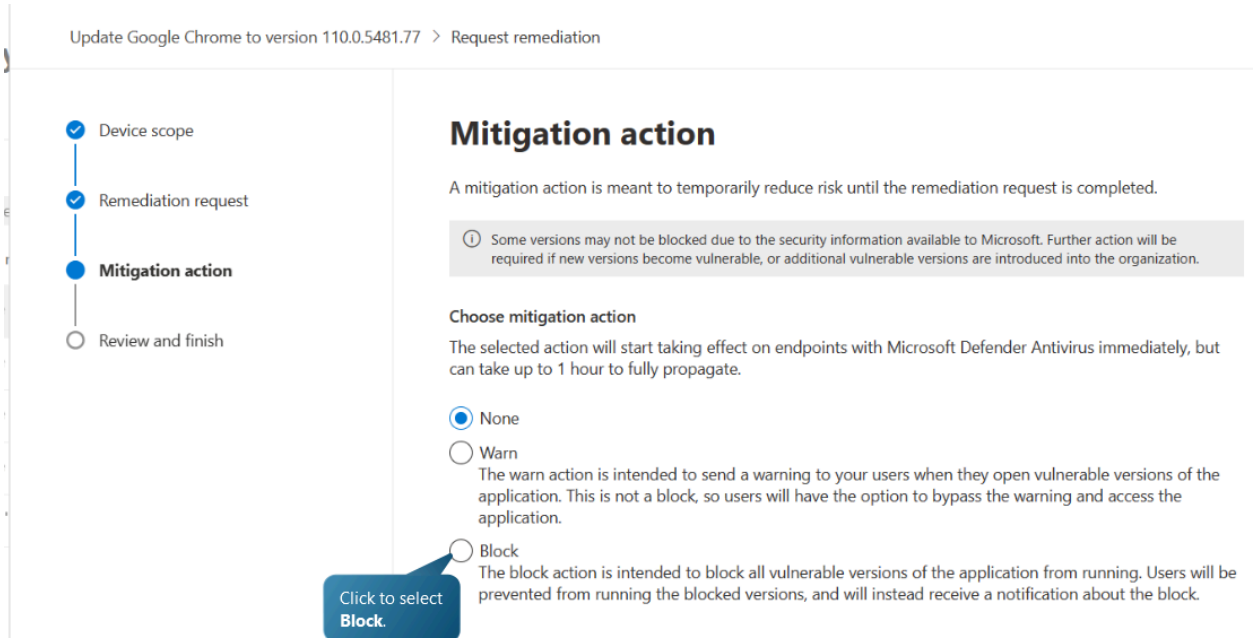
- The impact column displays the potential reduction in your exposure score and the projected increase to your secure score for devices once a recommendation is implemented. A higher secure score for devices means your endpoints are more resilient against cybersecurity attacks.

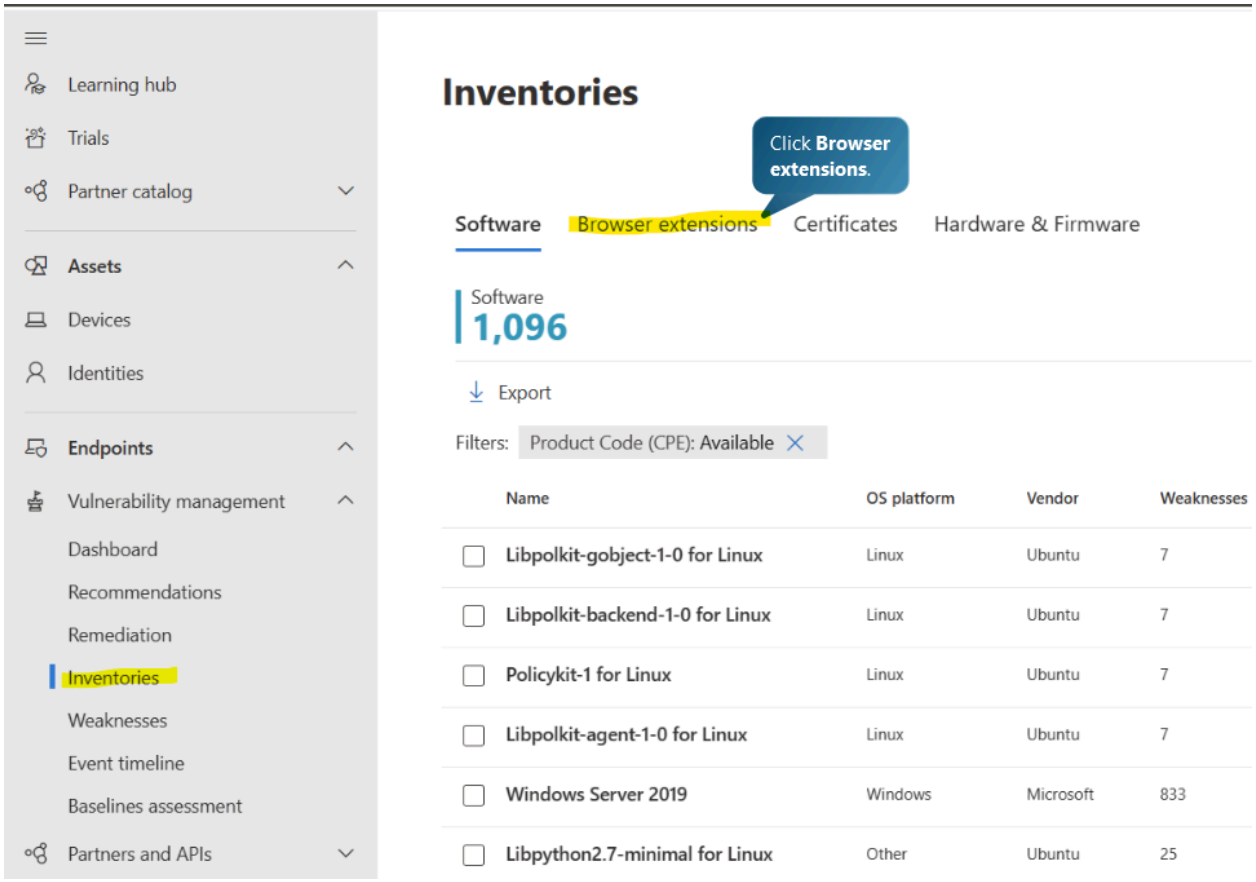

Update Ubuntu Libpolkit-gobject-1-0 for Linux
Remediation required
Click the Close button.
Open software page
Report inaccuracy
General
Exposed devices
Installed devices
Associated CVEs
Activities
Description
Update Libpolkit-gobject-1-0 for Linux to a later version to mitigate 7 known vulnerabilities affecting your devices.
Associated CVEs
Critical 0
High 4
Medium 3
Low 0
A verified local privilege escalation exploit is publicly available for one or more weaknesses related to this recommendation
This exploit is part of an exploit kit
Related threats
Threat Insights: CVE-2021-4034 PwnKit local privilege escalation is associated with one or more weaknesses related to this recommendation.
Details
Number of vulnerabilities
7
Exploit available
Yes
Exposed devices
23 / 45
Devices pending restart
4 / 15
Impact
7.06 | +0.00
Exposed operating systems
Linux
Request remediation
Exception options


Microsoft 365 Defender
Search
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Security recommend
Export
Filters:
Remediation type: Software upgr
Security recommendation
Update Google Chrome to version
Update Google Chrome for Mac
Disable 'Continue running backgrc
Disable 'Password Manager'
Enable 'Block third party cookies'
Update Google Chrome to version 110.0.5481.77
Remediation required
Open software page
Click the Exposed devices tab.
General
Exposed devices
Installed devices
Associated CVEs
Activities
Description
Update Chrome to a later version 110.0.5481.77 to mitigate 10 known vulnerabilities affecting your devices.
Associated CVEs
Critical 0
High 7
Medium 3
Low 0
Software usage (past 30 days)
Exposed devices using this software 2/6
Median usage 6 days
Details
Number of vulnerabilities
10
Exploit available
No
Exposed devices
6 / 17
Devices pending restart
0 / 6
Impact
1.11 | +0.00
Exposed operating systems
Windows 10, Windows 11 (+ 1 more)


nmend
Update Google Chrome to version 110.0.5481.77
Remediation required
Open software page
Report inaccuracy
Software upgr
on
me to version
me for Mac
nning backgrc
anager'
arty cookies'
General
Exposed devices
Installed devices
Associated CVEs
Activities
Export
6 items
Name
OS platform
Last seen
Tags
dkrzakowski-win
Windows 10
Feb 13, 2023 4:40 P...
jmnzenbook
Windows 10
Feb 7, 2023 9:34 AM
desktop-win10
Windows 10
Feb 13, 2023 7:10 ...
jrhi-2019
Windows Server 20...
Feb 13, 2023 5:11 ...
jrhi-win-2004
Windows 10
Feb 13, 2023 6:09 ...
jrhi-win11-1
Windows 11
Feb 13, 2023 5:10 ...
Click Request remediation.
Request remediation
Exception options


Update Google Chrome to version 110.0.5481.77 > Request remediation
Device scope
Remediation request
Mitigation action
Review and finish
Remediation request
Fill out the remediation request so the relevant team can address and co
recommendation. No changes will automatically be applied to your devic
Remediation page.
Exposed devices
6 / 17
Remediation options
Software update (recommended)
Task management tools
Open a ticket in Microsoft Endpoint Manager (for AAD joined device
Click to select the checkbox.
emediation due date *
Select a date...
Priority
Medium
Back
Next


Update Google Chrome to version 110.0.5481.77 > Request remediation
Device scope
Remediation request
Mitigation action
Review and finish
Mitigation action
A mitigation action is meant to temporarily reduce risk until the remediation request is completed.
Some versions may not be blocked due to the security information available to Microsoft. Further action will be required if new versions become vulnerable, or additional vulnerable versions are introduced into the organization.
Choose mitigation action
The selected action will start taking effect on endpoints with Microsoft Defender Antivirus immediately, but can take up to 1 hour to fully propagate.
None
Warn
The warn action is intended to send a warning to your users when they open vulnerable versions of the application. This is not a block, so users will have the option to bypass the warning and access the application.
Block
The block action is intended to block all vulnerable versions of the application from running. Users will be prevented from running the blocked versions, and will instead receive a notification about the block.
Click to select Block.


Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Partners and APIs
Inventories
Click Browser extensions.
Software
Browser extensions
Certificates
Hardware & Firmware
Software
1,096
Export
Filters: Product Code (CPE): Available
Name
OS platform
Vendor
Weaknesses
Libpolkit-gobject-1-0 for Linux
Linux
Ubuntu
7
Libpolkit-backend-1-0 for Linux
Linux
Ubuntu
7
Policykit-1 for Linux
Linux
Ubuntu
7
Libpolkit-agent-1-0 for Linux
Linux
Ubuntu
7
Windows Server 2019
Windows
Microsoft
833
Libpython2.7-minimal for Linux
Other
Ubuntu
25

Inventories

Click **Hardware & Firmware.**

Software | Browser extensions | Certificates | Hardware & Firmware

Gain insights into potentially vulnerable certificates by viewing the number of certificates that have been identified as potentially less secure and intr organization. Show more

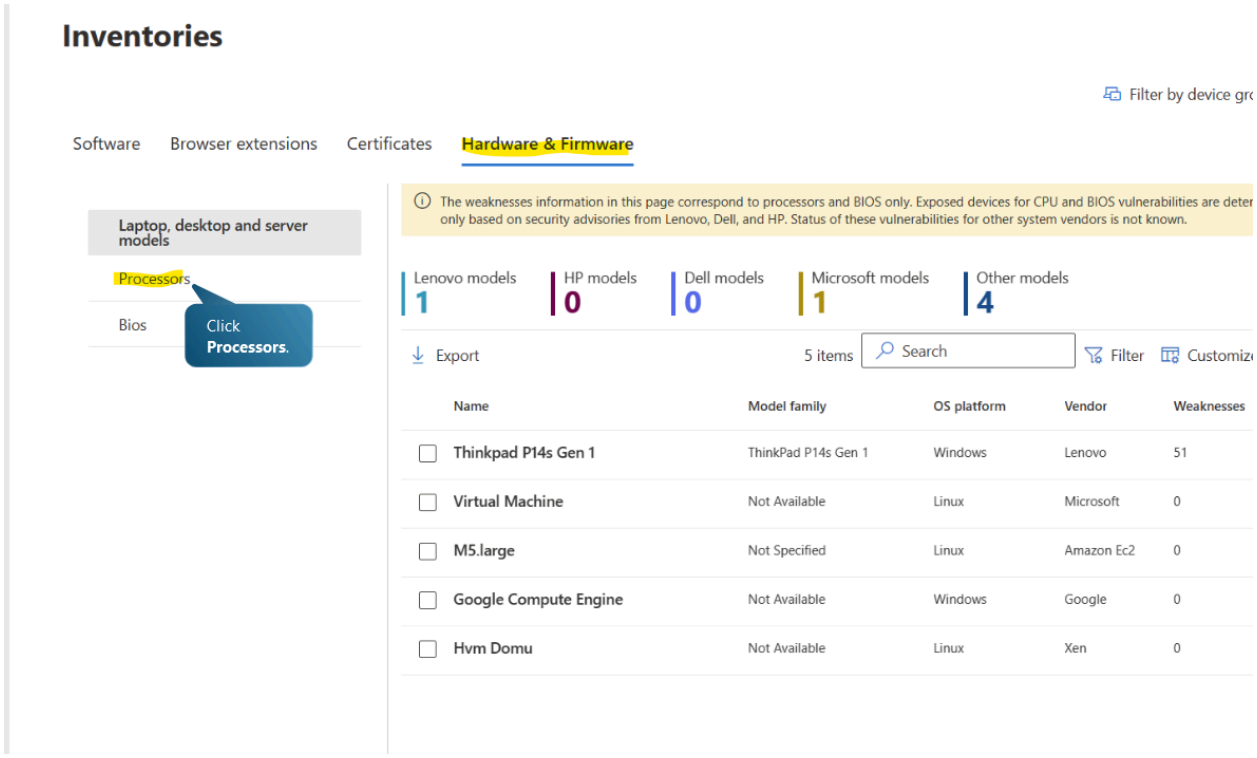
Expired	Expiring soon	Short key size	Weak algorithm	Self-signed
40	62	20	189	480

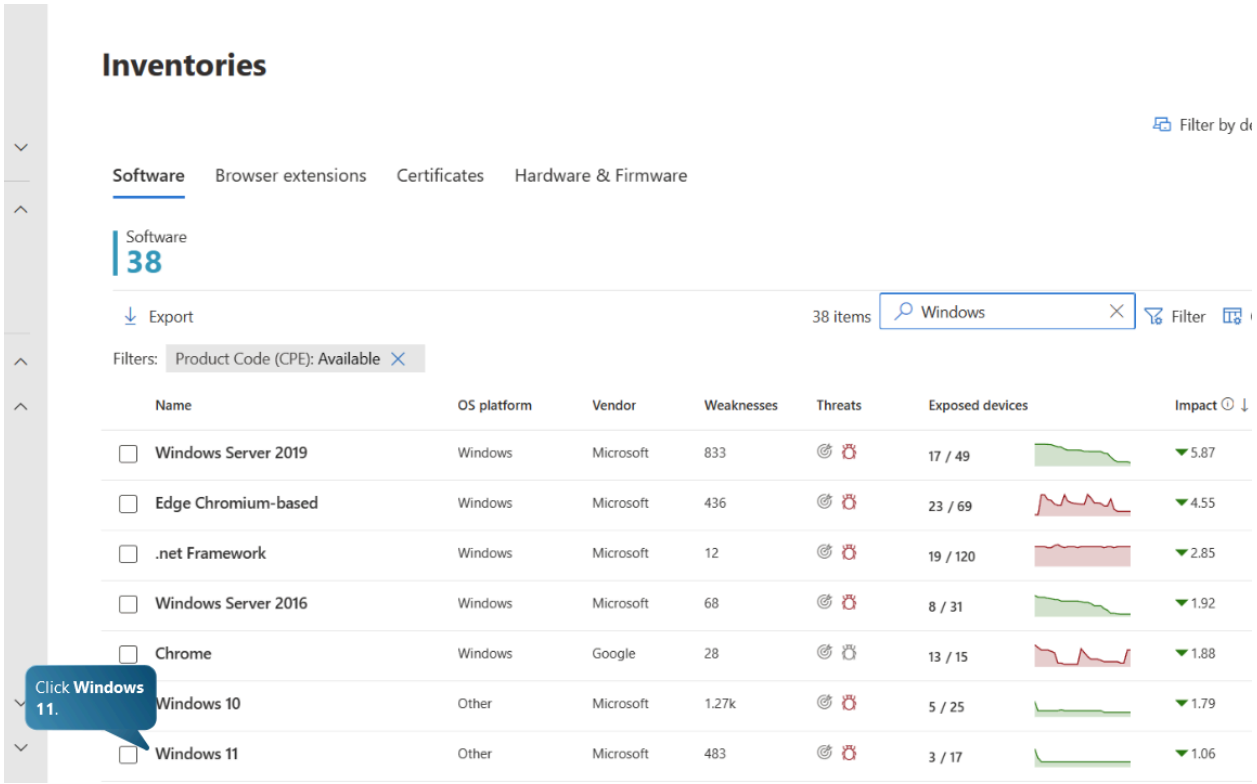
Export

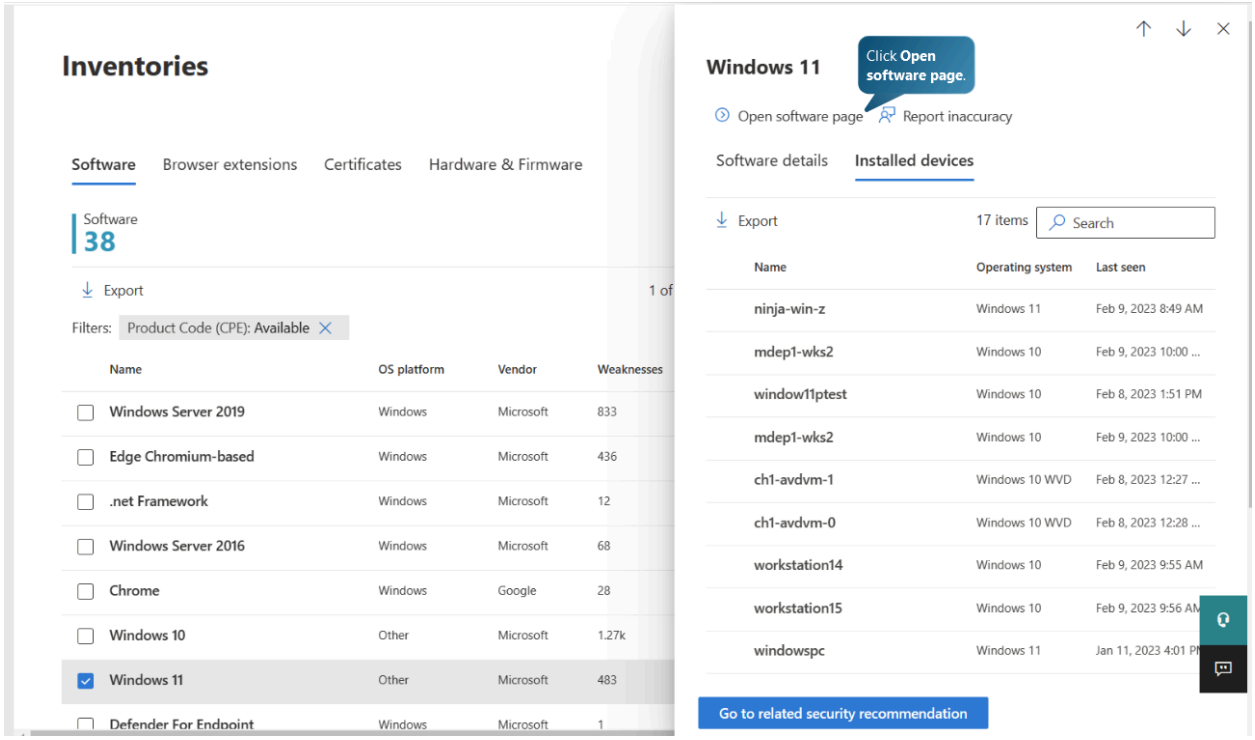
561 items

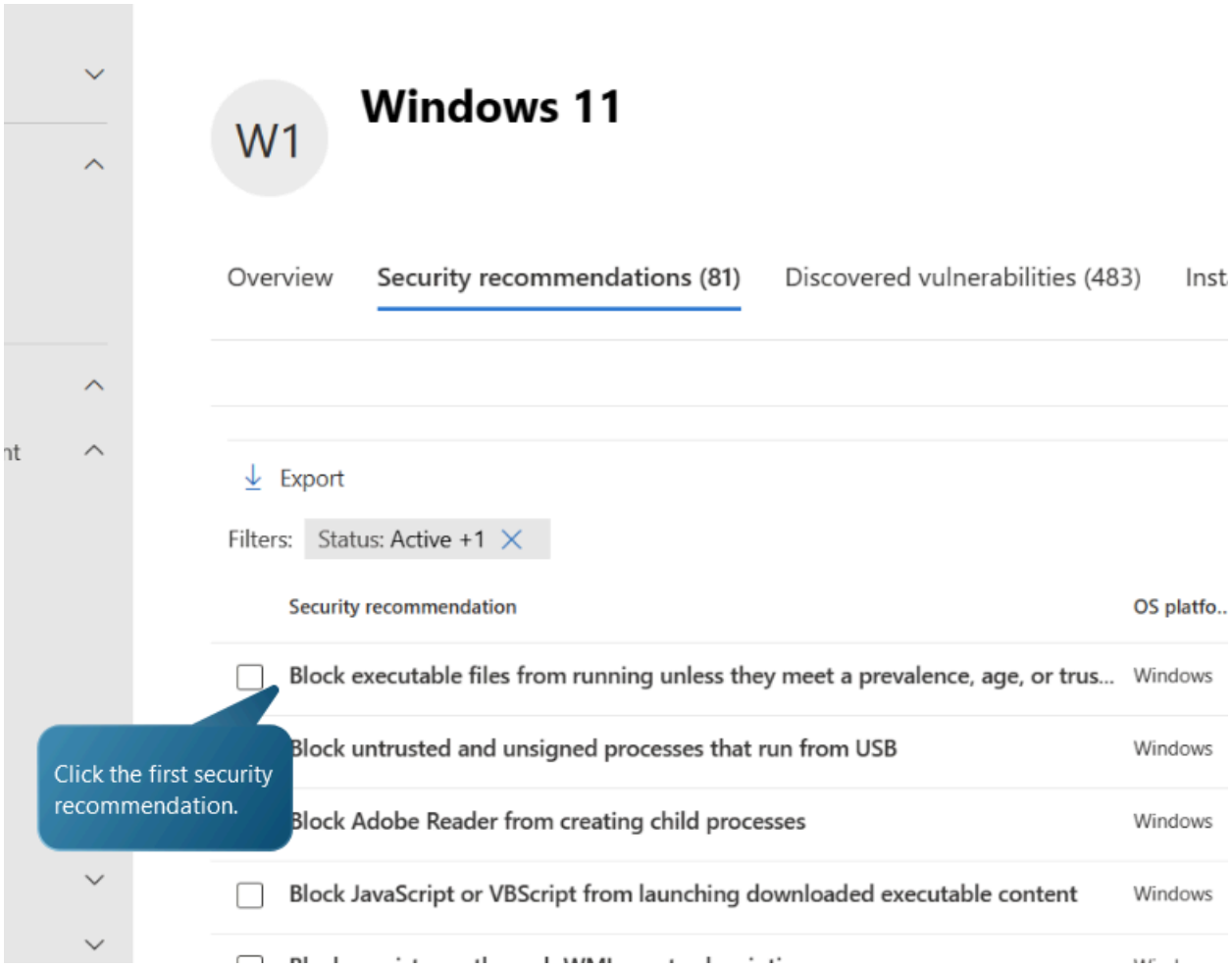
Search

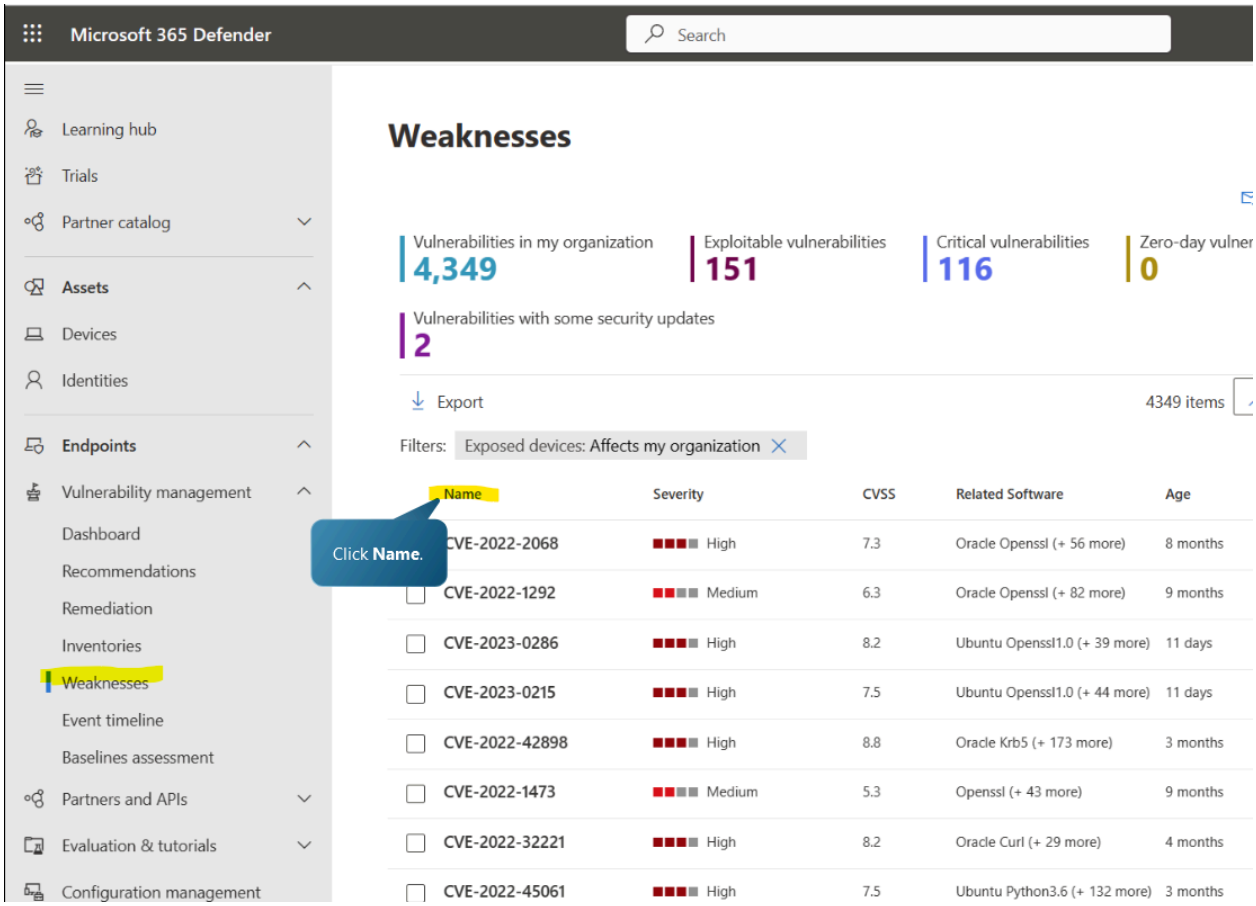
Name	Issued by	Type	Validation status	Scope
95a65f9d-3894-4f7e-bc6b-9de253a7c1c7	95a65f9d-3894-4f7e-bc6b-9...	Other	Self-signed	N/A
226b617e-7513-4d71-b6e1-bfc50bbd1db7	226b617e-7513-4d71-b6e1-...	Root CA	Weak signature (+ 1 more)	Private
8a553601-ccca-4b2d-b923-04a7200dc2b2	8a553601-ccca-4b2d-b923-...	Root CA	Weak signature (+ 1 more)	Private
SimulandWAP.seccxp.ninja	SimulandWAP.seccxp.ninja	Server	Self-signed	N/A
6cff374c-b8ff-4495-9470-930d981b217a	6cff374c-b8ff-4495-9470-93...	Other	Self-signed	N/A
d95d1214-2fa1-4667-a92a-2ca22a5cd4e1	d95d1214-2fa1-4667-a92a-2...	Root CA	Weak signature (+ 1 more)	Private
e2c104ab-7dde-4a09-ac76-28ee5066a28c	e2c104ab-7dde-4a09-ac76-...	Root CA	Weak signature (+ 1 more)	Private
Microsoft Test Root Authority	Microsoft Test Root Authority	Other	Expired (+ 3 more)	N/A

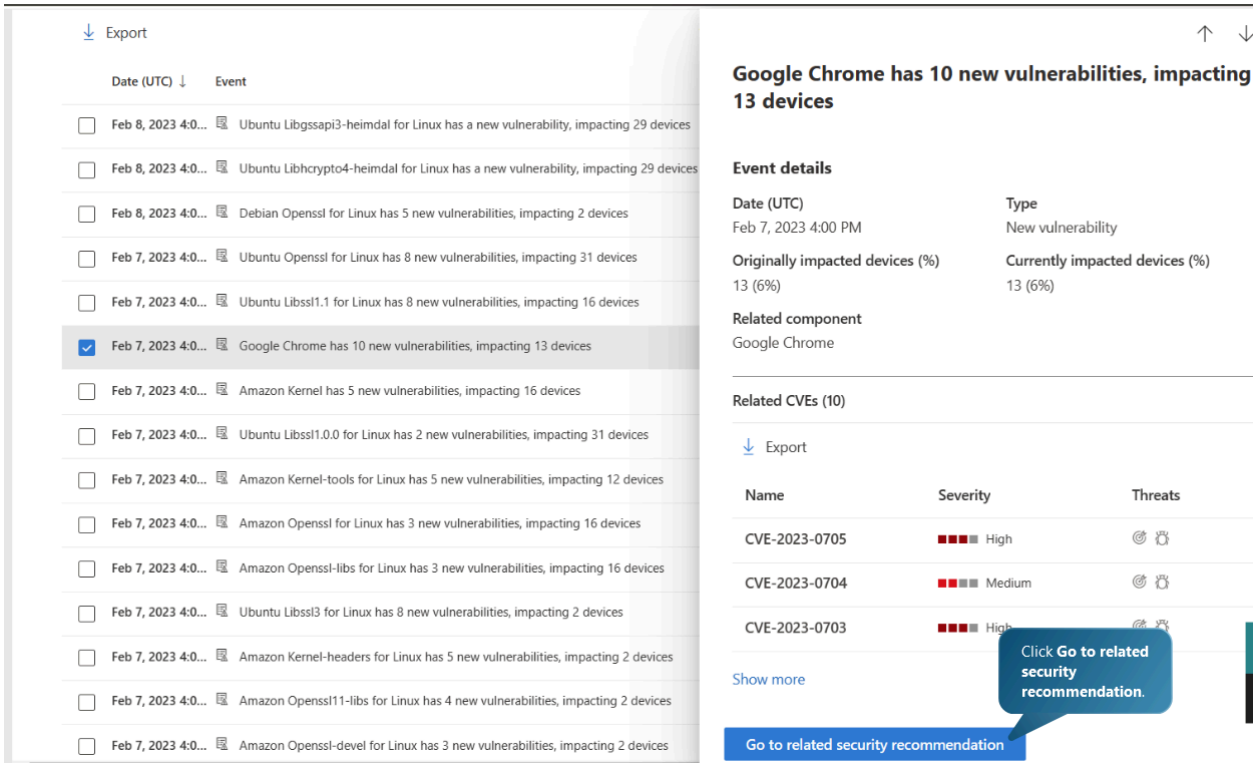

Inventories
Filter by device gr
Software
Browser extensions
Certificates
Hardware & Firmware
Laptop, desktop and server models
Processors
Bios
Click Processors.
The weaknesses information in this page correspond to processors and BIOS only. Exposed devices for CPU and BIOS vulnerabilities are deter
only based on security advisories from Lenovo, Dell, and HP. Status of these vulnerabilities for other system vendors is not known.
Lenovo models 1
HP models 0
Dell models 0
Microsoft models 1
Other models 4
Export
5 items
Search
Filter
Customiz
Name
Model family
OS platform
Vendor
Weaknesses
Thinkpad P14s Gen 1
ThinkPad P14s Gen 1
Windows
Lenovo
51
Virtual Machine
Not Available
Linux
Microsoft
0
M5.large
Not Specified
Linux
Amazon Ec2
0
Google Compute Engine
Not Available
Windows
Google
0
Hvm Domu
Not Available
Linux
Xen
0

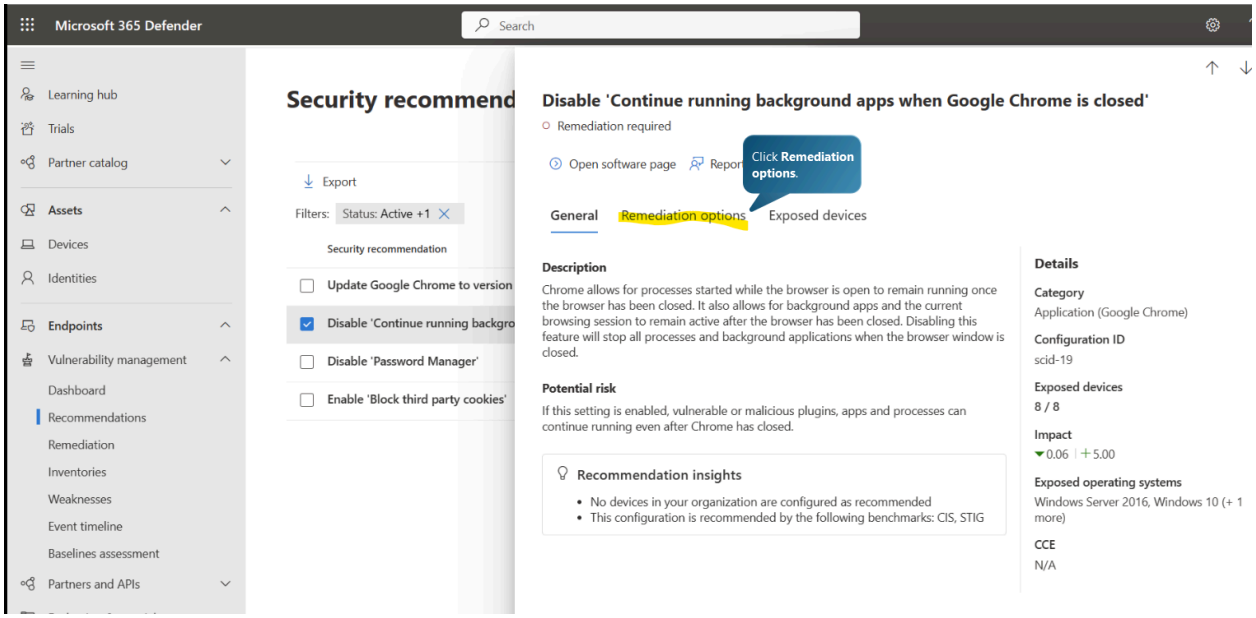

Inventories
Filter by d
Software
Browser extensions
Certificates
Hardware & Firmware
Software 38
Export
38 items
Windows
Filter
Filters:
Product Code (CPE): Available
Name
OS platform
Vendor
Weaknesses
Threats
Exposed devices
Impact
Windows Server 2019
Windows
Microsoft
833
17 / 49
5.87
Edge Chromium-based
Windows
Microsoft
436
23 / 69
4.55
.net Framework
Windows
Microsoft
12
19 / 120
2.85
Windows Server 2016
Windows
Microsoft
68
8 / 31
1.92
Chrome
Windows
Google
28
13 / 15
1.88
Windows 10
Other
Microsoft
1.27k
5 / 25
1.79
Windows 11
Other
Microsoft
483
3 / 17
1.06
Click Windows 11.

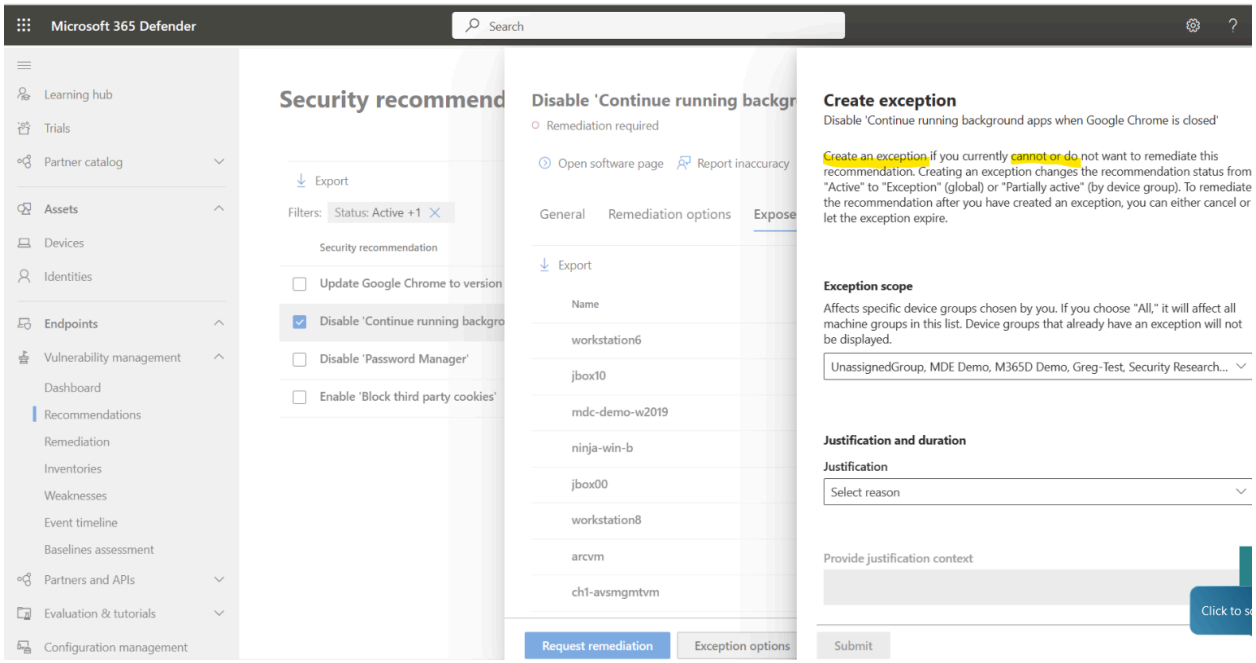

Inventories
Software
Browser extensions
Certificates
Hardware & Firmware
Software
38
Export
1 of
Filters:
Product Code (CPE): Available
Name
OS platform
Vendor
Weaknesses
Windows Server 2019
Windows
Microsoft
833
Edge Chromium-based
Windows
Microsoft
436
.net Framework
Windows
Microsoft
12
Windows Server 2016
Windows
Microsoft
68
Chrome
Windows
Google
28
Windows 10
Other
Microsoft
1.27k
Windows 11
Other
Microsoft
483
Defender For Endpoint
Windows
Microsoft
1
Windows 11
Click Open software page.
Open software page
Report inaccuracy
Software details
Installed devices
Export
17 items
Search
Name
Operating system
Last seen
ninja-win-z
Windows 11
Feb 9, 2023 8:49 AM
mdep1-wks2
Windows 10
Feb 9, 2023 10:00 ...
window11ptest
Windows 10
Feb 8, 2023 1:51 PM
mdep1-wks2
Windows 10
Feb 9, 2023 10:00 ...
ch1-avdvm-1
Windows 10 WVD
Feb 8, 2023 12:27 ...
ch1-avdvm-0
Windows 10 WVD
Feb 8, 2023 12:28 ...
workstation14
Windows 10
Feb 9, 2023 9:55 AM
workstation15
Windows 10
Feb 9, 2023 9:56 AM
windowspc
Windows 11
Jan 11, 2023 4:01 PM
Go to related security recommendation


W1
Windows 11
Overview
Security recommendations (81)
Discovered vulnerabilities (483)
Inst
Export
Filters:
Status: Active +1
Security recommendation
OS platfo..
Block executable files from running unless they meet a prevalence, age, or trus...
Windows
Block untrusted and unsigned processes that run from USB
Windows
Block Adobe Reader from creating child processes
Windows
Block JavaScript or VBScript from launching downloaded executable content
Windows
Click the first security recommendation.


Microsoft 365 Defender
Search
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Partners and APIs
Evaluation & tutorials
Configuration management
Weaknesses
Vulnerabilities in my organization 4,349
Exploitable vulnerabilities 151
Critical vulnerabilities 116
Zero-day vulner 0
Vulnerabilities with some security updates 2
Export
4349 items
Filters: Exposed devices: Affects my organization
Click Name.
Name
Severity
CVSS
Related Software
Age
CVE-2022-2068 High 7.3 Oracle Openssl (+ 56 more) 8 months
CVE-2022-1292 Medium 6.3 Oracle Openssl (+ 82 more) 9 months
CVE-2023-0286 High 8.2 Ubuntu Openssl1.0 (+ 39 more) 11 days
CVE-2023-0215 High 7.5 Ubuntu Openssl1.0 (+ 44 more) 11 days
CVE-2022-42898 High 8.8 Oracle Krb5 (+ 173 more) 3 months
CVE-2022-1473 Medium 5.3 Openssl (+ 43 more) 9 months
CVE-2022-32221 High 8.2 Oracle Curl (+ 29 more) 4 months
CVE-2022-45061 High 7.5 Ubuntu Python3.6 (+ 132 more) 3 months


Export
Date (UTC)
Event
Feb 8, 2023 4:0... Ubuntu Libgssapi3-heimdal for Linux has a new vulnerability, impacting 29 devices
Feb 8, 2023 4:0... Ubuntu Libhcrypto4-heimdal for Linux has a new vulnerability, impacting 29 devices
Feb 8, 2023 4:0... Debian Openssl for Linux has 5 new vulnerabilities, impacting 2 devices
Feb 7, 2023 4:0... Ubuntu Openssl for Linux has 8 new vulnerabilities, impacting 31 devices
Feb 7, 2023 4:0... Ubuntu Libssl1.1 for Linux has 8 new vulnerabilities, impacting 16 devices
Feb 7, 2023 4:0... Google Chrome has 10 new vulnerabilities, impacting 13 devices
Feb 7, 2023 4:0... Amazon Kernel has 5 new vulnerabilities, impacting 16 devices
Feb 7, 2023 4:0... Ubuntu Libssl1.0.0 for Linux has 2 new vulnerabilities, impacting 31 devices
Feb 7, 2023 4:0... Amazon Kernel-tools for Linux has 5 new vulnerabilities, impacting 12 devices
Feb 7, 2023 4:0... Amazon Openssl for Linux has 3 new vulnerabilities, impacting 16 devices
Feb 7, 2023 4:0... Amazon Openssl-libs for Linux has 3 new vulnerabilities, impacting 16 devices
Feb 7, 2023 4:0... Ubuntu Libssl3 for Linux has 8 new vulnerabilities, impacting 2 devices
Feb 7, 2023 4:0... Amazon Kernel-headers for Linux has 5 new vulnerabilities, impacting 2 devices
Feb 7, 2023 4:0... Amazon Openssl11-libs for Linux has 4 new vulnerabilities, impacting 2 devices
Feb 7, 2023 4:0... Amazon Openssl-devel for Linux has 3 new vulnerabilities, impacting 2 devices
Google Chrome has 10 new vulnerabilities, impacting 13 devices
Event details
Date (UTC)
Feb 7, 2023 4:00 PM
Type
New vulnerability
Originally impacted devices (%)
13 (6%)
Currently impacted devices (%)
13 (6%)
Related component
Google Chrome
Related CVEs (10)
Export
Name
Severity
Threats
CVE-2023-0705 High
CVE-2023-0704 Medium
CVE-2023-0703 High
Show more
Click Go to related security recommendation.
Go to related security recommendation


Microsoft 365 Defender
Search
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Partners and APIs
Security recommend
Export
Filters: Status: Active +1
Security recommendation
Update Google Chrome to version
Disable 'Continue running backgro
Disable 'Password Manager'
Enable 'Block third party cookies'
Disable 'Continue running background apps when Google Chrome is closed'
Remediation required
Open software page
Report
Click Remediation options.
General
Remediation options
Exposed devices
Description
Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed. Disabling this feature will stop all processes and background applications when the browser window is closed.
Potential risk
If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.
Recommendation insights
No devices in your organization are configured as recommended
This configuration is recommended by the following benchmarks: CIS, STIG
Details
Category
Application (Google Chrome)
Configuration ID
scid-19
Exposed devices
8 / 8
Impact
0.06 5.00
Exposed operating systems
Windows Server 2016, Windows 10 (+ 1 more)
CCE
N/A


Microsoft 365 Defender
Search
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Partners and APIs
Evaluation & tutorials
Configuration management
Security recommend
Export
Filters: Status: Active +1
Security recommendation
Update Google Chrome to version
Disable 'Continue running backgro
Disable 'Password Manager'
Enable 'Block third party cookies'
Disable 'Continue running backgr
Remediation required
Open software page
Report inaccuracy
General
Remediation options
Expose
Export
Name
workstation6
jbox10
mdc-demo-w2019
ninja-win-b
jbox00
workstation8
arcvm
ch1-avsmgmtvm
Request remediation
Exception options
Create exception
Disable 'Continue running background apps when Google Chrome is closed'
Create an exception if you currently cannot or do not want to remediate this recommendation. Creating an exception changes the recommendation status from "Active" to "Exception" (global) or "Partially active" (by device group). To remediate the recommendation after you have created an exception, you can either cancel or let the exception expire.
Exception scope
Affects specific device groups chosen by you. If you choose "All," it will affect all machine groups in this list. Device groups that already have an exception will not be displayed.
UnassignedGroup, MDE Demo, M365D Demo, Greg-Test, Security Research...
Justification and duration
Justification
Select reason
Provide justification context
Submit

Create exception

Disable 'Continue running background apps when Google Chrome is closed'

Exception scope

Affects specific device groups chosen by you. If you choose "All," it will affect all machine groups in this list. Device groups that already have an exception will not be displayed.

UnassignedGroup, MDE Demo, M365D Demo, Greg-Test, Security Research...

Justification and duration

Justification

Risk accepted

Provide justification context

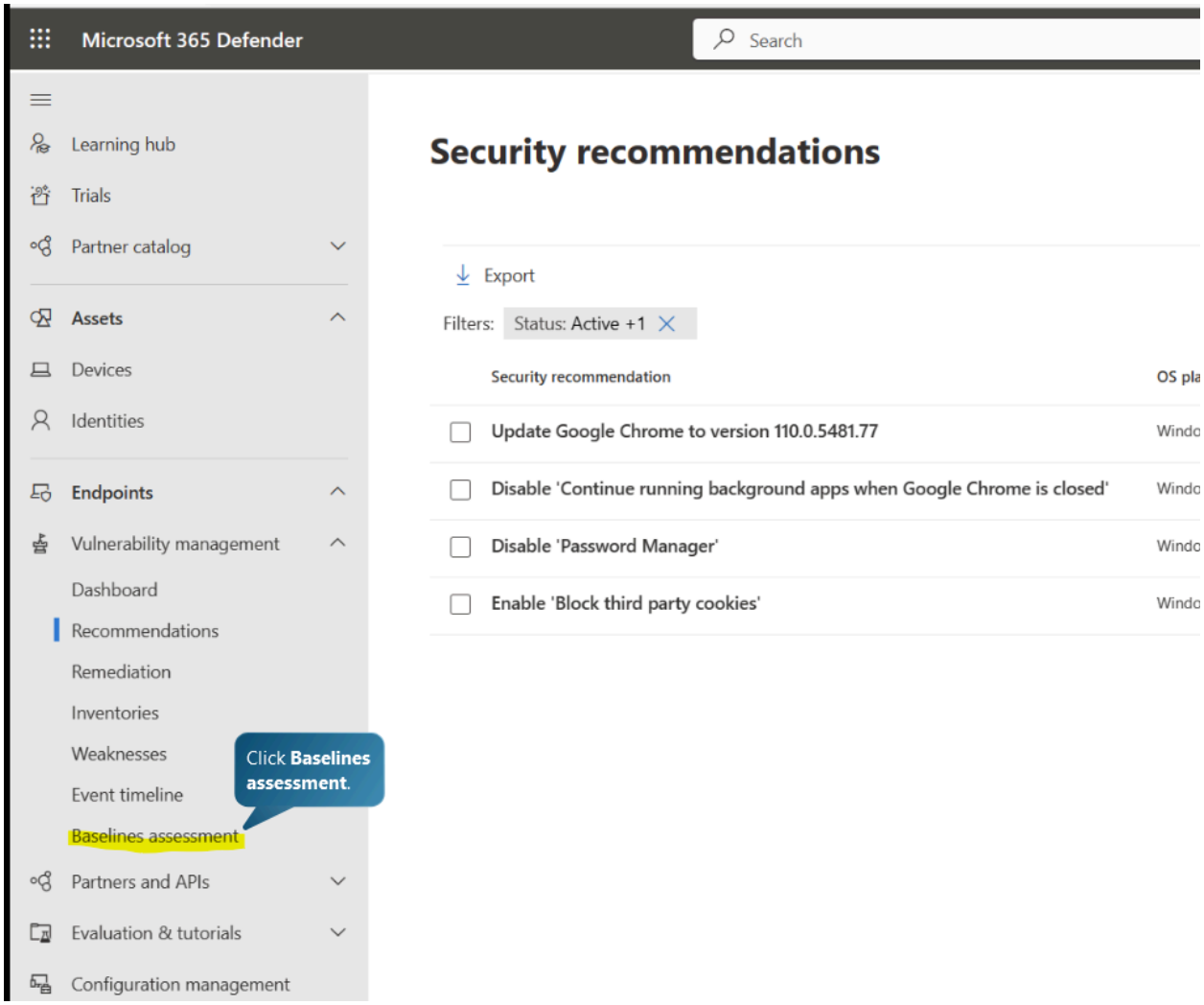
The organization accepts the risk associated with this recommendation due to the low organizational risk posed by this process.

Exception duration

Set date

Click the **Exception duration** dropdown.

Submit


Microsoft 365 Defender
Search
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Event timeline
Baselines assessment
Click Baselines assessment.
Partners and APIs
Evaluation & tutorials
Configuration management
Security recommendations
Export
Filters:
Status: Active +1
Security recommendation
OS pla
Update Google Chrome to version 110.0.5481.77
Windo
Disable 'Continue running background apps when Google Chrome is closed'
Windo
Disable 'Password Manager'
Windo
Enable 'Block third party cookies'
Windo

Security baselines assessment

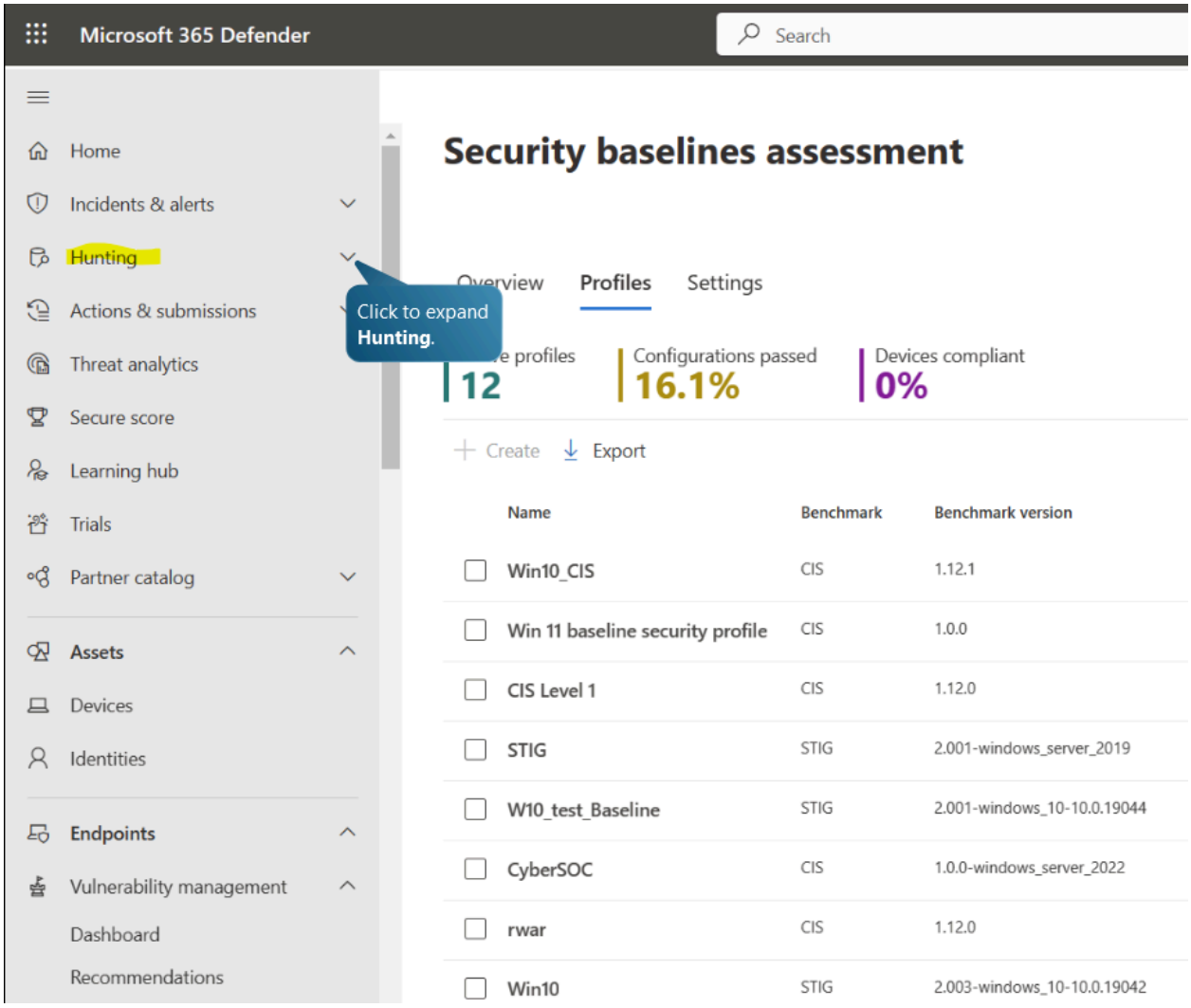
Overview **Profiles** Settings

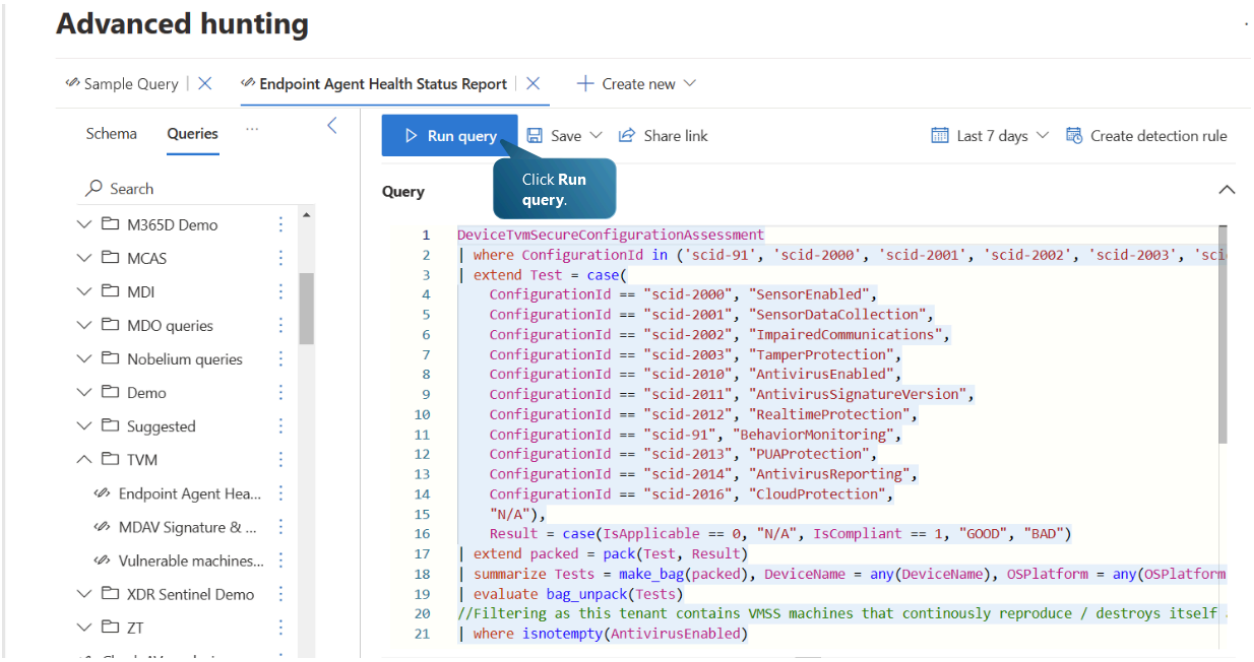
Active profiles	Configurations passed	Devices compliant
12	16.1%	0%

+ Create ↓ Export

	Name	Benchmark	Benchmark version
☐	CIS Benchmark Level 2 - Windo...	CIS	1.3.0-windows_server_2019
☐	Win 11 baseline security profile	CIS	1.0.0
☐	CIS Level 1	CIS	1.12.0
☐	STIG	STIG	2.001-windows_server_2019
☐	W10_test_Baseline	STIG	2.001-windows_10-10.0.19044
☐	CyberSOC	CIS	1.0.0-windows_server_2022
☐	rwar	CIS	1.12.0
☐	Win10	STIG	2.003-windows_10-10.0.19042

Click the first profile.


Microsoft 365 Defender
Search
Home
Incidents & alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Click to expand Hunting.
Security baselines assessment
Overview
Profiles
Settings
e profiles
12
Configurations passed
16.1%
Devices compliant
0%
Create
Export
Name
Benchmark
Benchmark version
Win10_CIS
CIS
1.12.1
Win 11 baseline security profile
CIS
1.0.0
CIS Level 1
CIS
1.12.0
STIG
STIG
2.001-windows_server_2019
W10_test_Baseline
STIG
2.001-windows_10-10.0.19044
CyberSOC
CIS
1.0.0-windows_server_2022
rwar
CIS
1.12.0
Win10
STIG
2.003-windows_10-10.0.19042


Advanced hunting
Sample Query
Endpoint Agent Health Status Report
Create new
Schema
Queries
Search
M365D Demo
MCAS
MDI
MDO queries
Nobelium queries
Demo
Suggested
TVM
Endpoint Agent Hea...
MDAV Signature & ...
Vulnerable machines...
XDR Sentinel Demo
ZT
Run query
Save
Share link
Last 7 days
Create detection rule
Click Run query.
Query
DeviceTvmSecureConfigurationAssessment
| where ConfigurationId in ('scid-91', 'scid-2000', 'scid-2001', 'scid-2002', 'scid-2003', 'sci
| extend Test = case(
ConfigurationId == "scid-2000", "SensorEnabled",
ConfigurationId == "scid-2001", "SensorDataCollection",
ConfigurationId == "scid-2002", "ImpairedCommunications",
ConfigurationId == "scid-2003", "TamperProtection",
ConfigurationId == "scid-2010", "AntivirusEnabled",
ConfigurationId == "scid-2011", "AntivirusSignatureVersion",
ConfigurationId == "scid-2012", "RealtimeProtection",
ConfigurationId == "scid-91", "BehaviorMonitoring",
ConfigurationId == "scid-2013", "PUAProtection",
ConfigurationId == "scid-2014", "AntivirusReporting",
ConfigurationId == "scid-2016", "CloudProtection",
"N/A"),
Result = case(IsApplicable == 0, "N/A", IsCompliant == 1, "GOOD", "BAD")
| extend packed = pack(Test, Result)
| summarize Tests = make_bag(packed), DeviceName = any(DeviceName), OSPlatform = any(OSPlatform
| evaluate bag_unpack(Tests)
//Filtering as this tenant contains VMSS machines that continously reproduce / destroys itself
| where isnotempty(AntivirusEnabled)