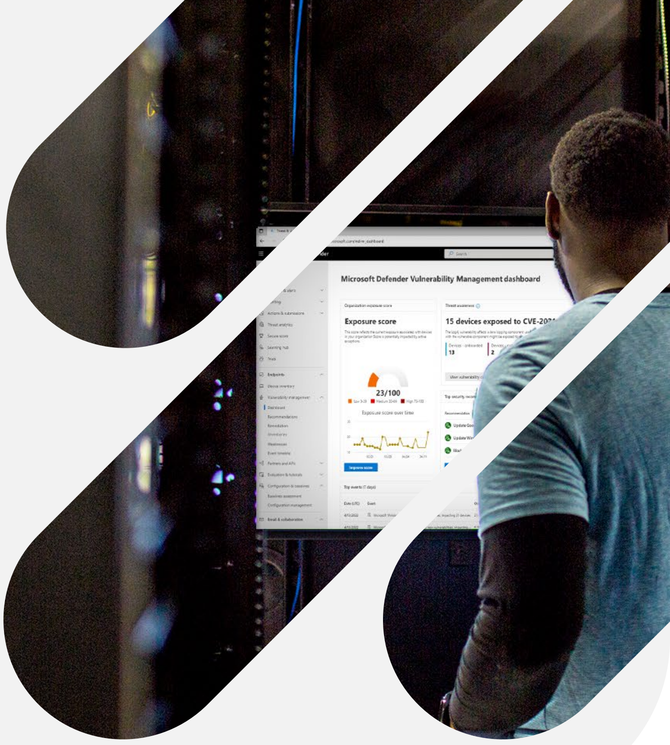
Microsoft Security

Microsoft Defender Vulnerability Management



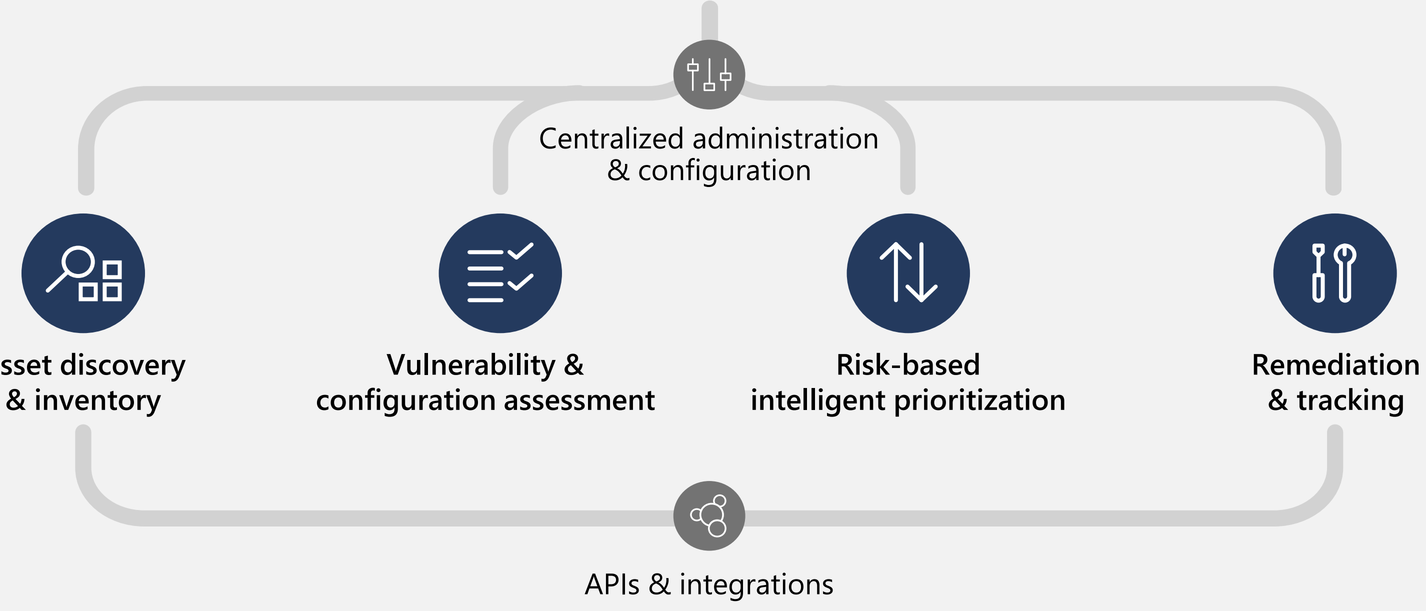
Reduce cyber risk with continuous vulnerability discovery and assessment, risk-based prioritization, and remediation.

Assess and remediate vulnerabilities across your assets

As organizations accelerate adoption of digital transformation and hybrid work models, CISOs are tasked with securing their environments against ever-evolving threats. Last year alone saw 21,957 published vulnerabilities, the highest number to date and 3x higher than in 2016 (NIST).

Proactively reducing your organization's exposure requires a comprehensive risk-based vulnerability management solution so you can identify, assess, remediate, and track all your biggest vulnerabilities and misconfigurations across your most critical assets.

Microsoft Defender Vulnerability Management



Centralized administration & configuration

Asset discovery & inventory

Vulnerability & configuration assessment

Risk-based intelligent prioritization

Remediation & tracking

APIs & integrations

Microsoft Defender Vulnerability Management provides continuous asset discovery and inventory in a consolidated view, intelligent assessments leveraging Microsoft threat intelligence, risk-based prioritization, and built-in remediation and mitigation flows.

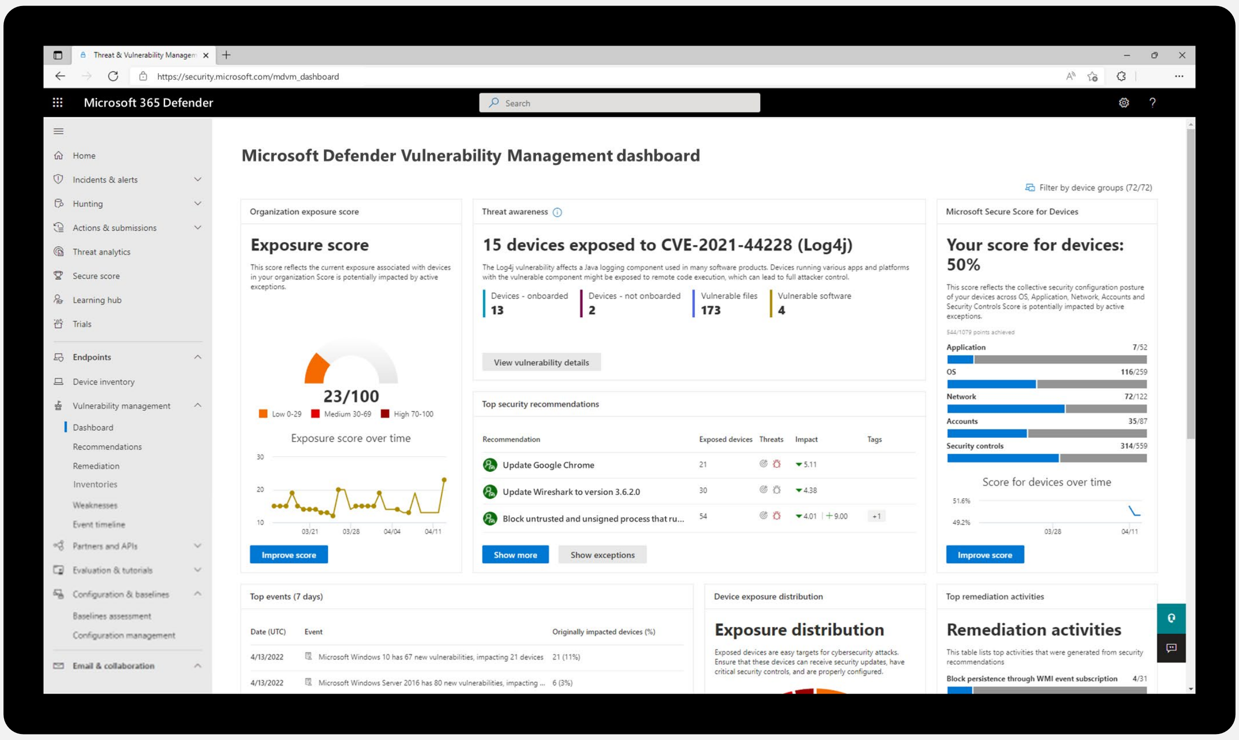
Key capabilities include:

- **Security baselines assessment:** continuously monitor posture against customizable benchmarks and industry standards (CIS, NIST, MS)
- Intelligent **vulnerability assessment tools** across devices, software applications, browser extensions, digital certificates, and network shares
- Mitigate risk during remediation planning with **blocking vulnerable applications** and warning users with custom messages
- And more

Microsoft Defender Vulnerability Management

Learn how our discovery tools, asset inventories, threat intelligence, and built-in workflows to help security teams reduce risk.

Defender Vulnerability Management dashboard



Microsoft Defender Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization Score is potentially impacted by active exceptions.

23/100

Threat awareness

15 devices exposed to CVE-2021-44228 (Log4j)

The Log4j vulnerability affects a Java logging component used in many software products. Devices running various apps and platforms with the vulnerable component might be exposed to remote code execution, which can lead to full attacker control.

Devices - onboarded	Devices - not onboarded	Vulnerable files	Vulnerable software
13	2	173	4

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update Google Chrome	21		5.11	
Update Wireshark to version 3.6.2.0	30		4.38	
Block untrusted and unsigned process that ru...	54		4.01 | + 9.00	+1

Microsoft Secure Score for Devices

Your score for devices: 50%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

544/1079 points achieved

Application	7/52
OS	116/259
Network	72/122
Accounts	35/87
Security controls	314/559

Top events (7 days)

Date (UTC)	Event	Originally impacted devices (%)
4/13/2022	Microsoft Windows 10 has 67 new vulnerabilities, impacting 21 devices	21 (11%)
4/13/2022	Microsoft Windows Server 2016 has 80 new vulnerabilities, impacting ...	6 (3%)

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

Top remediation activities

Remediation activities

This table lists top activities that were generated from security recommendations

Block persistence through WMI event subscription 4/31

Proactively reduce risk to your organization

Know what to protect in a single view

Built-in and agentless scanners continuously monitor and detect risk even when devices aren't connected to the corporate network. Expanded asset coverage consolidates software applications, digital certificates, network shares, and browser extensions into a single inventory view.

Remediate and track progress across teams

Seamlessly plan remediations with built-in workflows and mitigate risk with blocking vulnerable applications for specific device groups. Bridge the gap between teams with real-time remediation tracking and posture measurement.

Get advanced vulnerability assessment tools

Understand your risk exposure with the relevant threat and business contexts. Create customizable baseline profiles to measure risk compliance against established benchmarks (CIS, STIG, MS).

Focus on what's important

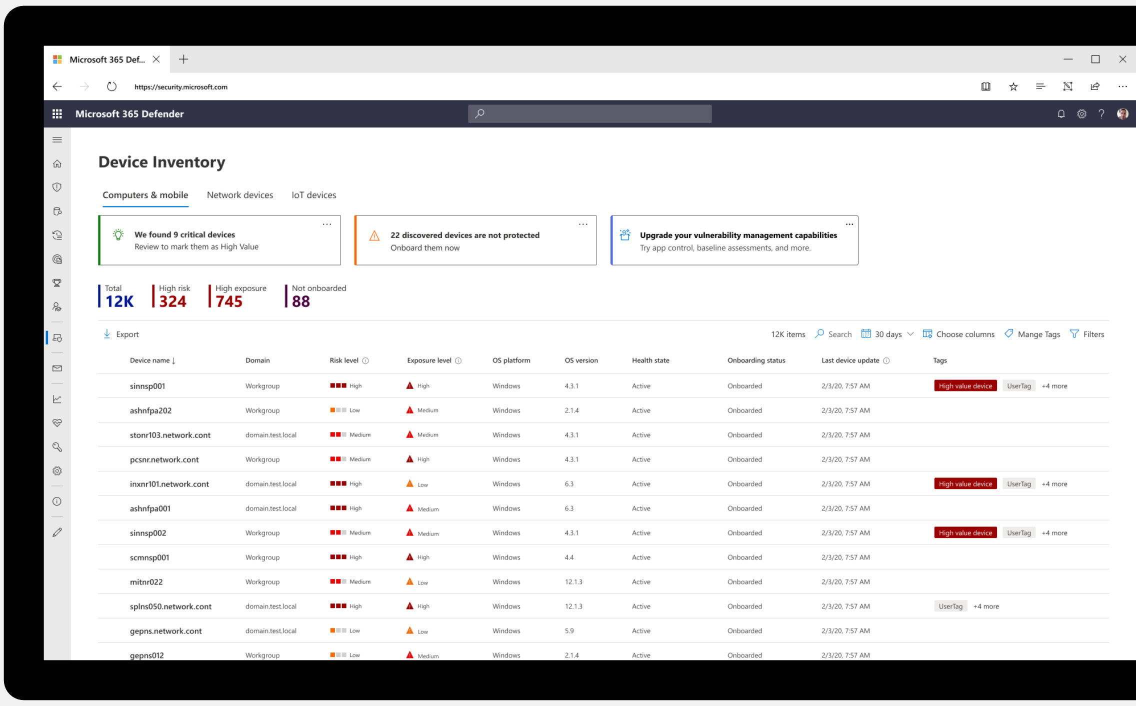
View risk-based, prioritized recommendations in a single view. Use threat intelligence insights including breach likelihood predictions, event timelines, and vulnerable device reports to prioritize the biggest vulnerabilities and misconfigurations across your most critical assets.

Know what to protect in a single view

Discover and assess all your organization's assets in a single view. Eliminate periodic scans with continuous monitoring and alerts. Detect risk even when devices are not connected to the corporate network.

Asset discovery and inventory

Continuously detect risk across managed and unmanaged endpoints with built-in modules and agentless scanners, even when devices aren't connected to the corporate network. View entity-level risk assessment data to focus on your most critical assets.



Device Inventory

Computers & mobile | Network devices | IoT devices

We found 9 critical devices
Review to mark them as High Value

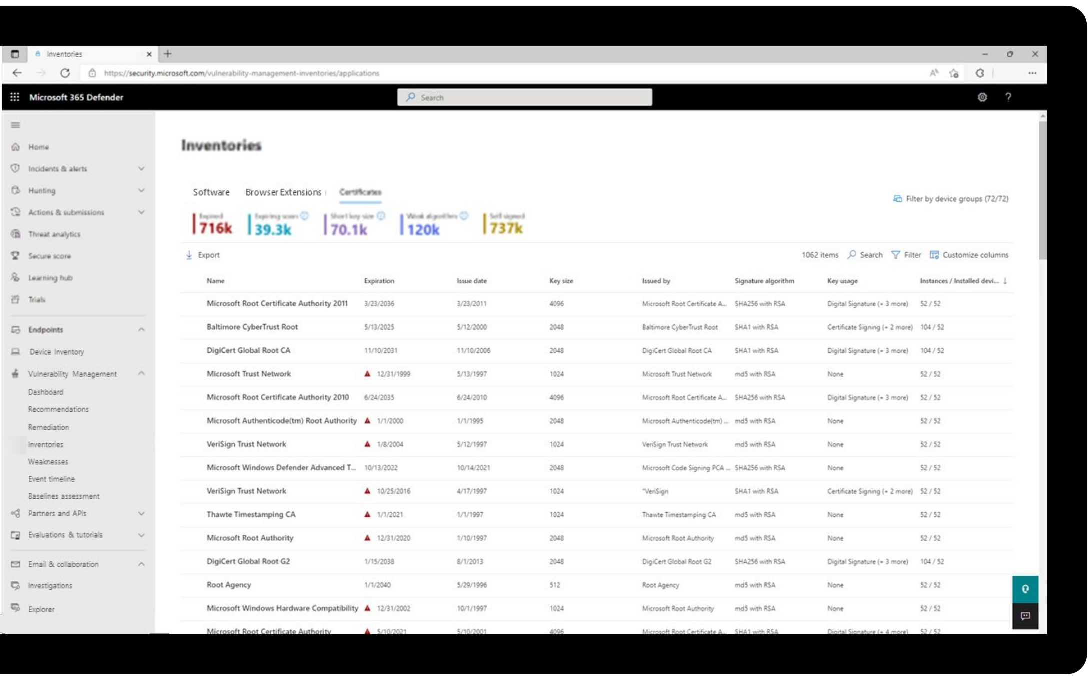
22 discovered devices are not protected
Onboard them now

Upgrade your vulnerability management capabilities
Try app control, baseline assessments, and more.

Total 12K | High risk 324 | High exposure 745 | Not onboarded 88

Export — 12K items — Search — 30 days — Choose columns — Mange Tags — Filters

Device name ↓	Domain	Risk level	Exposure level	OS platform	OS version	Health state	Onboarding status	Last device update	Tags
sinnsp001	Workgroup	High	High	Windows	4.3.1	Active	Onboarded	2/3/20, 7:57 AM	High value device UserTag +4 more
ashnfpa202	Workgroup	Low	Medium	Windows	2.1.4	Active	Onboarded	2/3/20, 7:57 AM	
stonr103.network.cont	domain.test.local	Medium	Medium	Windows	4.3.1	Active	Onboarded	2/3/20, 7:57 AM	
pcsnr.network.cont	Workgroup	Medium	High	Windows	4.3.1	Active	Onboarded	2/3/20, 7:57 AM	
inxnr101.network.cont	domain.test.local	High	Low	Windows	6.3	Active	Onboarded	2/3/20, 7:57 AM	High value device UserTag +4 more
ashnfpa001	domain.test.local	High	Medium	Windows	6.3	Active	Onboarded	2/3/20, 7:57 AM	
sinnsp002	Workgroup	Medium	Medium	Windows	4.3.1	Active	Onboarded	2/3/20, 7:57 AM	High value device UserTag +4 more
scmnsp001	Workgroup	High	High	Windows	4.4	Active	Onboarded	2/3/20, 7:57 AM	
mitnr022	Workgroup	Medium	Low	Windows	12.1.3	Active	Onboarded	2/3/20, 7:57 AM	
splns050.network.cont	domain.test.local	High	High	Windows	12.1.3	Active	Onboarded	2/3/20, 7:57 AM	UserTag +4 more
gepns.network.cont	domain.test.local	Low	Low	Windows	5.9	Active	Onboarded	2/3/20, 7:57 AM	
gepns012	Workgroup	Low	Medium	Windows	2.1.4	Active	Onboarded	2/3/20, 7:57 AM	



Inventories

Software | Browser Extensions | Certificates

Filter by device groups (72/72)

Expired 716k | Expiring soon 39.3k | Short key size 70.1k | Weak algorithm 120k | Self signed 737k

Export — 1062 items — Search — Filter — Customize columns

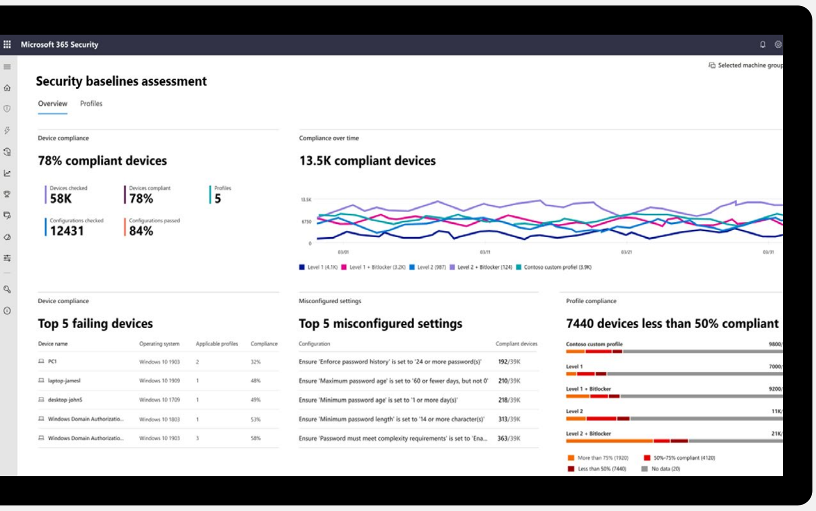
Name	Expiration	Issue date	Key size	Issued by	Signature algorithm	Key usage	Instances / Installed devi... ↓
Microsoft Root Certificate Authority 2011	3/23/2036	3/23/2011	4096	Microsoft Root Certificate A...	SHA256 with RSA	Digital Signature (+ 3 more)	52 / 52
Baltimore CyberTrust Root	5/13/2025	5/12/2000	2048	Baltimore CyberTrust Root	SHA1 with RSA	Certificate Signing (+ 2 more)	104 / 52
DigiCert Global Root CA	11/10/2031	11/10/2006	2048	DigiCert Global Root CA	SHA1 with RSA	Digital Signature (+ 3 more)	104 / 52
Microsoft Trust Network	▲ 12/31/1999	5/13/1997	1024	Microsoft Trust Network	md5 with RSA	None	52 / 52
Microsoft Root Certificate Authority 2010	6/24/2035	6/24/2010	4096	Microsoft Root Certificate A...	SHA256 with RSA	Digital Signature (+ 3 more)	52 / 52
Microsoft Authenticode(tm) Root Authority	▲ 1/1/2000	1/1/1995	2048	Microsoft Authenticode(tm) ...	md5 with RSA	None	52 / 52
VeriSign Trust Network	▲ 1/8/2004	5/12/1997	1024	VeriSign Trust Network	md5 with RSA	None	52 / 52
Microsoft Windows Defender Advanced T...	10/13/2022	10/14/2021	2048	Microsoft Code Signing PCA ...	SHA256 with RSA	None	52 / 52
VeriSign Trust Network	▲ 10/25/2016	4/17/1997	1024	"VeriSign	SHA1 with RSA	Certificate Signing (+ 2 more)	52 / 52
Thawte Timestamping CA	▲ 1/1/2021	1/1/1997	1024	Thawte Timestamping CA	md5 with RSA	None	52 / 52
Microsoft Root Authority	▲ 12/31/2020	1/10/1997	2048	Microsoft Root Authority	md5 with RSA	None	52 / 52
DigiCert Global Root G2	1/15/2038	8/1/2013	2048	DigiCert Global Root G2	SHA256 with RSA	Digital Signature (+ 3 more)	104 / 52
Root Agency	1/1/2040	5/29/1996	512	Root Agency	md5 with RSA	None	52 / 52
Microsoft Windows Hardware Compatibility	▲ 12/31/2002	10/1/1997	1024	Microsoft Root Authority	md5 with RSA	None	52 / 52
Microsoft Root Certificate Authority	▲ 5/10/2021	5/10/2001	4096	Microsoft Root Certificate A...	SHA1 with RSA	Digital Signature (+ 4 more)	52 / 52

Continuous vulnerability and misconfiguration assessments

Access consolidated inventories across software applications, digital certificates, browser extensions, and network shares. View information on extension permissions and associated risk levels, identify certificates before they expire, detect potential vulnerabilities due to weak signature algorithms, and assess misconfigurations in internal network shares.

Get advanced vulnerability assessment tools

Understand your cyberexposure and relevant threat and business contexts in one place. Proactively prevent breaches with risk assessments leveraging industry standards, including CIS and STIG.



Microsoft 365 Security

Selected machine group

Security baselines assessment

Overview | Profiles

Device compliance

78% compliant devices

Devices checked 58K | Devices compliant 78% | Profiles 5

Configurations checked 12431 | Configurations passed 84%

Compliance over time

13.5K compliant devices

13.5K
6750
0
03/01
03/11
03/21
03/31
Level 1 (4.1K)
Level 1 + Bitlocker (3.2K)
Level 2 (987)
Level 2 + Bitlocker (124)
Contoso custom profiel (3.9K)

Device compliance

Top 5 failing devices

Device name	Operating system	Applicable profiles	Compliance
PC1	Windows 10 1903	2	32%
laptop-jamesl	Windows 10 1909	1	48%
desktop-johnS	Windows 10 1709	1	49%
Windows Domain Authorizatio...	Windows 10 1803	1	53%
Windows Domain Authorizatio...	Windows 10 1903	3	58%

Misconfigured settings

Top 5 misconfigured settings

Configuration	Compliant devices
Ensure 'Enforce password history' is set to '24 or more password(s)'	192/39K
Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	210/39K
Ensure 'Minimum password age' is set to '1 or more day(s)'	218/39K
Ensure 'Minimum password length' is set to '14 or more character(s)'	313/39K
Ensure 'Password must meet complexity requirements' is set to 'Ena...	363/39K

Profile compliance

7440 devices less than 50% compliant

Security baselines assessments

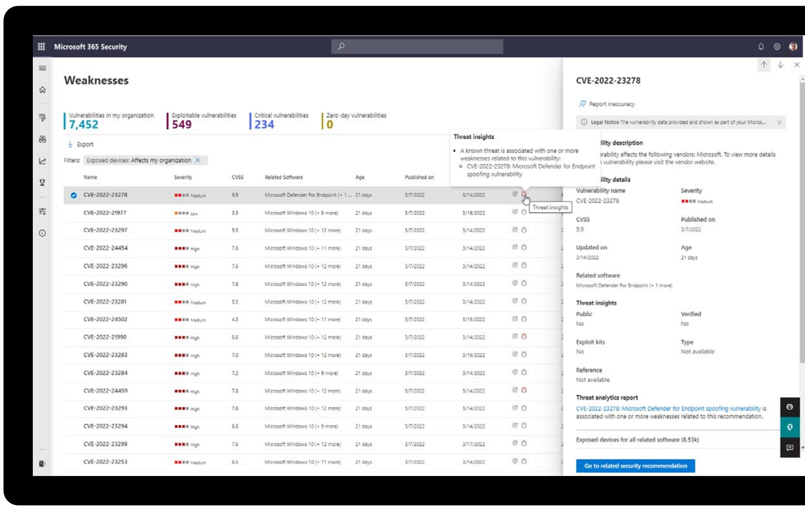
Instead of relying on compliance scans, continuously monitor security baseline compliance and identify changes in real-time. Set up customizable profiles and leverage Center for Internet Security (CIS), Security Technical Implementation Guides (STIG), and Microsoft security benchmarks.

Prioritize what's important

Quickly remediate the biggest vulnerabilities on your most critical assets. Prioritize risks using Microsoft threat intelligence, likelihood predictions, event timelines, and device reports.

Expert-level threat monitoring and analysis

Use Microsoft threat intelligence, breach likelihood analysis, event timelines, and entity-level vulnerability assessments to understand and prioritize vulnerabilities.



Microsoft 365 Security

Weaknesses

Vulnerabilities in my organization 7,452 | Exploitable vulnerabilities 549 | Critical vulnerabilities 234 | Zero-day vulnerabilities 0

Export

Filters: Exposed devices: Affects my organization ✕

Name	Severity	CVSS	Related Software	Age	Published on	
CVE-2022-23278	Medium	5.9	Microsoft Defender For Endpoint (+ 1 ...	21 days	3/7/2022	3/14/2022
CVE-2022-21977	Low	3.3	Microsoft Windows 10 (+ 8 more)	21 days	3/7/2022	3/16/2022
CVE-2022-23297	Medium	5.5	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-24454	High	7.8	Microsoft Windows 10 (+ 11 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23296	High	7.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23290	High	7.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23281	Medium	5.5	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-24502	Medium	4.3	Microsoft Windows 10 (+ 11 more)	21 days	3/7/2022	3/15/2022
CVE-2022-21990	High	8.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23283	High	7.0	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/16/2022
CVE-2022-23284	High	7.2	Microsoft Windows 10 (+ 9 more)	21 days	3/7/2022	3/14/2022
CVE-2022-24459	High	7.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23293	High	7.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23294	High	8.8	Microsoft Windows 10 (+ 9 more)	21 days	3/7/2022	3/14/2022
CVE-2022-23299	High	7.8	Microsoft Windows 10 (+ 12 more)	21 days	3/7/2022	3/17/2022
CVE-2022-23253	Medium	6.5	Microsoft Windows 10 (+ 11 more)	21 days	3/7/2022	3/14/2022

Threat insights

- A known threat is associated with one or more weaknesses related to this vulnerability:
  - CVE-2022-23278: Microsoft Defender for Endpoint spoofing vulnerability

CVE-2022-23278

Report inaccuracy

Legal Notice The vulnerability data provided and shown as part of your Micros...

...lity description

...erability affects the following vendors: Microsoft. To view more details ... vulnerability please visit the vendor website.

...lity details

Vulnerability name: CVE-2022-23278 | Severity: Medium

CVSS: 5.9 | Published on: 3/7/2022

Updated on: 3/14/2022 | Age: 21 days

Related software: Microsoft Defender For Endpoint (+ 1 more)

Threat insights

Public: No | Verified: No

Exploit kits: No | Type: Not available

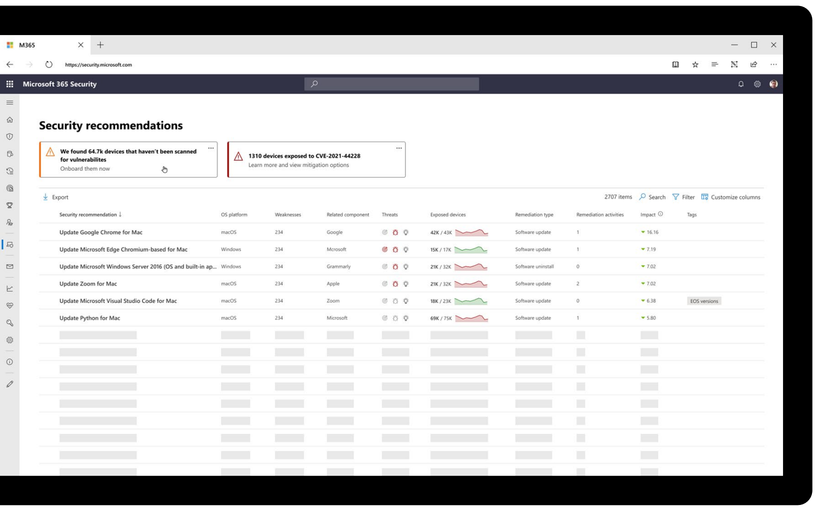
Reference: Not available

Threat analytics report

CVE-2022-23278: Microsoft Defender for Endpoint spoofing vulnerability is associated with one or more weaknesses related to this recommendation.

Exposed devices for all related software (8.53k)

Go to related security recommendation



M365
https://security.microsoft.com
Microsoft 365 Security

Security recommendations

We found 64.7k devices that haven't been scanned for vulnerabilites
Onboard them now

1310 devices exposed to CVE-2021-44228
Learn more and view mitigation options

Export | 2707 items | Search | Filter | Customize columns

Security recommendation ↓	OS platform	Weaknesses	Related component	Threats	Exposed devices	Remediation type	Remediation activities	Impact	Tags
Update Google Chrome for Mac	macOS	234	Google		42K / 43K	Software update	1	16.16	
Update Microsoft Edge Chromium-based for Mac	Windows	234	Microsoft		15K / 17K	Software update	1	7.19	
Update Microsoft Windows Server 2016 (OS and built-in ap...	Windows	234	Grammarly		21K / 32K	Software uninstall	0	7.02	
Update Zoom for Mac	macOS	234	Apple		21K / 32K	Software update	2	7.02	
Update Microsoft Visual Studio Code for Mac	macOS	234	Zoom		18K / 23K	Software update	0	6.38	EOS versions
Update Python for Mac	macOS	234	Microsoft		69K / 75K	Software update	1	5.80	

Prioritized security recommendations

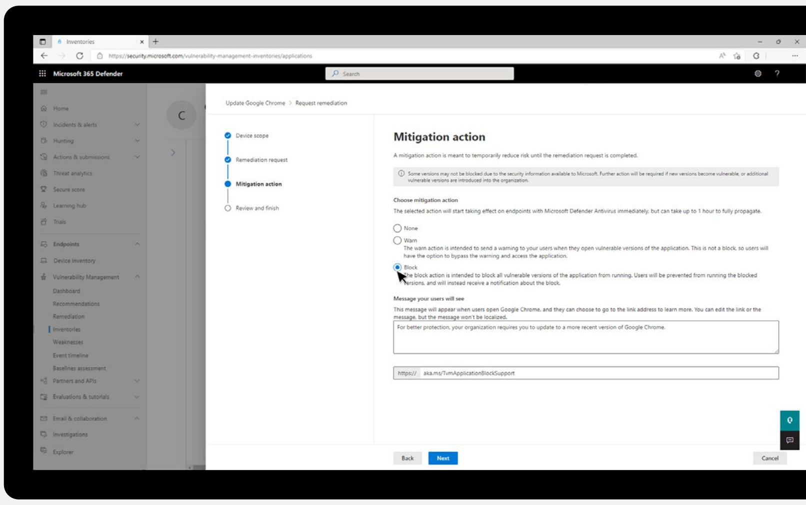
Focus on threats that pose the highest risk with a single view of prioritized recommendations from multiple security feeds. Access critical details including related CVEs, exposed devices, and more.

Remediate and track progress across teams

Bridge the gap between security and IT teams. Help reduce risk with automated vulnerability remediation tools, built-in workflows, integrations, and real-time measurements to seamlessly track progress across the organization.

Block vulnerable applications

While remediating vulnerabilities, reduce cyber exposure and mitigate risk by taking immediate action to block all currently known vulnerable versions of apps for specific device groups. Block app versions through file indicators of compromise (IoCs), provide customer warning messages to users, and surface links to learn more on how to upgrade to approved versions.



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.

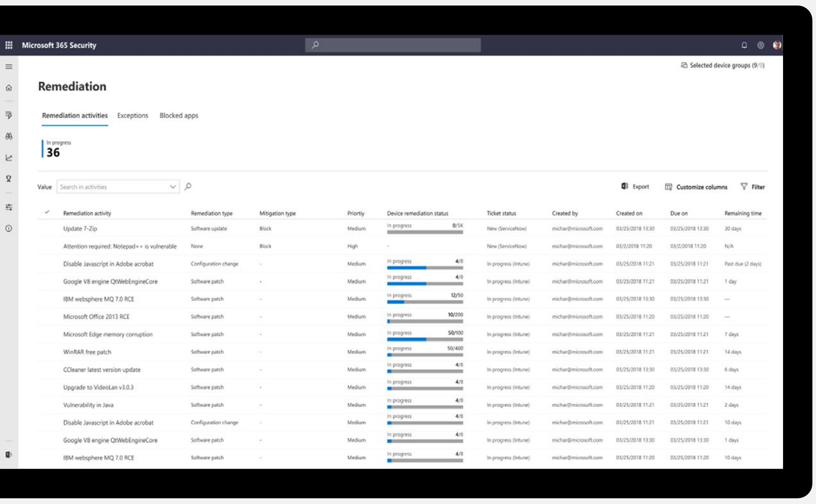
● Block
The block action is intended to block all vulnerable versions of the application from running. Users will be prevented from running the blocked versions, and will instead receive a notification about the block.

Message your users will see

This message will appear when users open Google Chrome, and they can choose to go to the link address to learn more. You can edit the link or the message, but the message won't be localized.

For better protection, your organization requires you to update to a more recent version of Google Chrome.

https:// aka.ms/TvmApplicationBlockSupport



Remediation

In progress
36

Remediation activity	Remediation type	Mitigation type	Priortiy	Device remediation status	Ticket status	Created by	Created on	Due on	Remaining time
Update 7-Zip	Software update	Block	Medium	In progress 0/5K	New (ServiceNow)	michar@microsoft.com	03/25/2018 13:30	03/25/2018 13:30	30 days
Attention required: Notepad++ is vulnerable	None	Block	High	-	New (ServiceNow)	michar@microsoft.com	03/2/2018 11:20	03/2/2018 11:20	N/A
Disable Javascript in Adobe acrobat	Configuration change	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	Past due (2 days)
Google V8 engine QtWebEngineCore	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	1 day
IBM websphere MQ 7.0 RCE	Software patch	-	Medium	In progress 12/50	In progress (Intune)	michar@microsoft.com	03/25/2018 13:30	03/25/2018 13:30	—
Microsoft Office 2013 RCE	Software patch	-	Medium	In progress 10/200	In progress (Intune)	michar@microsoft.com	03/25/2018 11:20	03/25/2018 11:20	—
Microsoft Edge memory corruption	Software patch	-	Medium	In progress 50/100	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	7 days
WinRAR free patch	Software patch	-	Medium	In progress 50/400	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	14 days
CCleaner latest version update	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 13:30	03/25/2018 13:30	6 days
Upgrade to VideoLan v3.0.3	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:20	03/25/2018 11:20	14 days
Vulnerability in Java	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	2 days
Disable Javascript in Adobe acrobat	Configuration change	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:21	03/25/2018 11:21	10 days
Google V8 engine QtWebEngineCore	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 13:30	03/25/2018 13:30	1 days
IBM websphere MQ 7.0 RCE	Software patch	-	Medium	In progress 4/8	In progress (Intune)	michar@microsoft.com	03/25/2018 11:20	03/25/2018 11:20	10 days

Seamlessly remediate and track progress

Connect teams with built-in workflows and integrations. Track progress and trends in real time with remediation tracking and device reports. Leverage integrations with partners including ServiceNow, Kenna Security, and Vulcan Cyber.

Compare flexible purchasing options

Microsoft Defender Vulnerability Management add-on

For Defender for Endpoint Plan 2 customers, get consolidated inventories, expanded asset coverage, and enhanced assessment and mitigation tools.

Defender Vulnerability Management add-on features:

- ✓ Security baseline assessments (CIS, STIG, MS)
- ✓ New risk-based vulnerability assessments of browser extensions and digital certificates
- ✓ Network shares analysis
- ✓ Blocking vulnerable applications
- ✓ Authenticated scans for Windows devices
- ✓ Consolidated asset inventories

Microsoft Defender Vulnerability Management

For customers looking to complement their EDR solution, efficiently discover, assess, and remediate vulnerabilities and misconfigurations all in one place. Get the full set of vulnerability management capabilities in Defender for Endpoint Plan 2, and advanced assessment and mitigation tools.

All Defender Vulnerability Management add-on features, plus:

- ✓ Device discovery and inventory
- ✓ Continuous monitoring
- ✓ Vulnerability assessments
- ✓ Configuration assessments
- ✓ Threat analytics and threat intelligence
- ✓ Risk-based prioritization
- ✓ Remediation tracking

Microsoft Defender Vulnerability Management and Defender for Endpoint

Feature	MDVM Standalone	MDE P2 + MDVM Add-On
Endpoint detection and response		
Unified security tools & centralized management		●
Next generation antimalware		●
Attack surface reduction rules		●
Device control		●
Endpoint firewall		●
Network protection		●
Web control URL blocking		●
Device-based conditional access		●
Controlled folder access		●
APIs, SIEM connector		●
App control		●
Endpoint detection & response		●
Auto investigation & remediation		●
Sandbox (deep analysis)		●
Microsoft Threat Experts		●
Threat analytics / Threat intelligence		●
Vulnerability management		
Device discovery (unmanaged)	●	●
Device inventory (managed)	●	●
Device inventory (network devices)	●	●
Vulnerability assessment	●	●
Configuration assessment	●	●
Risk-based prioritization	●	●
Remediation tracking	●	●
Continuous monitoring	●	●
Software applications assessment	●	●
Browser plugin assessment	●	●
Digital certificates assessment	●	●
Security baselines assessment	●	●
Vulnerability assessment for unmanaged endpoints	●	●
Block vulnerable applications	●	●
Network share analysis	●	●

Resources

Sign up for Public Preview:
aka.ms/MDVM

Learn more:
aka.ms/DefenderVulnerabilityManagementDocs