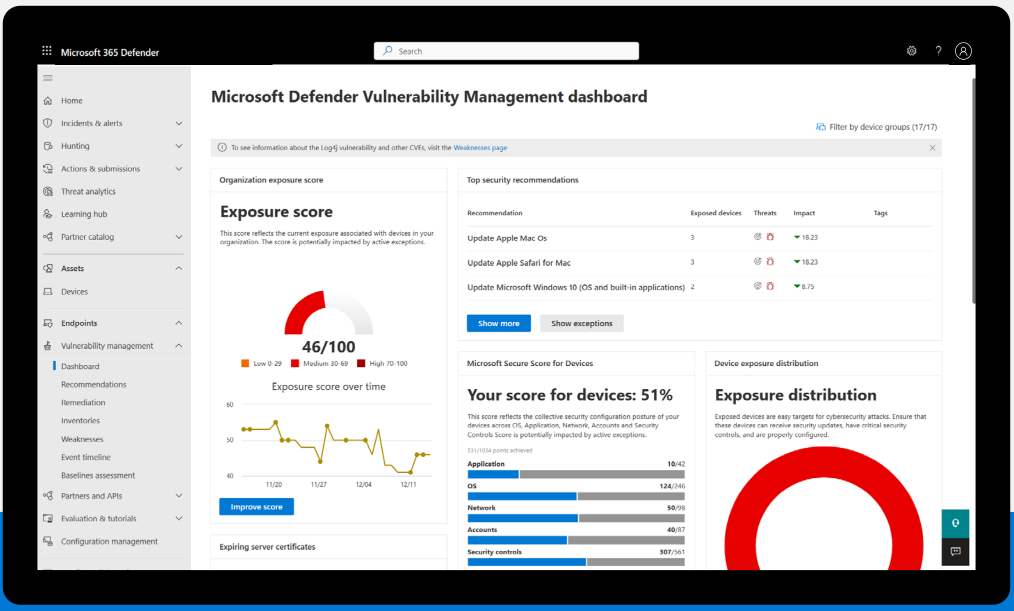
Microsoft Security

Microsoft Defender Vulnerability Management

Reduce cyber risk with continuous asset visibility, risk-based prioritization, and built-in remediation tools to address the most critical vulnerabilities.

Assess and remediate vulnerabilities across your assets

Over 25k CVEs (common vulnerabilities and exposures) were published by CISA in 2022. As organizations accelerate adoption of digital transformation and hybrid work models, CISOs are tasked with securing their environments against ever-evolving threats.



Microsoft Defender Vulnerability Management dashboard

To see information about the Log4j vulnerability and other CVEs, visit the Weaknesses page

Organization exposure score

Exposure score

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

46/100

Low 0-29 Medium 30-69 High 70-100

Exposure score over time

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update Apple Mac Os	3		▼18.23	
Update Apple Safari for Mac	3		▼18.23	
Update Microsoft Windows 10 (OS and built-in applications)	2		▼8.75	

Microsoft Secure Score for Devices

Your score for devices: 51%

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.

531/1034 points achieved

Application	10/42
OS	124/246
Network	50/98
Accounts	40/87
Security controls	307/561

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.

Expiring server certificates

Risk-based approach to vulnerability management

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.

Continuous asset discovery & monitoring

Proactively prevent breaches with continuous discovery and assessment. Detect risk even when devices are not connected to the corporate network with agentless scanning capabilities.

Asset discovery with one less agent

Leverage Defender for Endpoint agent and devices without the need to install additional dedicated scanners.

Real-time visibility

Identify and protect high value assets with business-critical applications, confidential data, or high-value users.

Exposure score

See the current state of your organization's exposure to threats and vulnerabilities, factoring weaknesses discovered, breach likelihood, device values, and relevant alerts.

Uncover risks and prioritize what matters

Vast assessments are available to uncover vulnerabilities and misconfigurations. Prioritize the biggest vulnerabilities on your most critical assets using Microsoft's threat intelligence, breach likelihood predictions and business contexts.

Security baselines assessment

Get customized baseline assessments against industry security benchmarks and Microsoft benchmarks.

Digital certificate assessment

Identify certificates about to expire, detect potential vulnerabilities, and ensure compliance with regulatory guidelines and policy.

Hardware and Firmware assessment

Full visibility into device manufacturer, processors and BIOs information to assess vulnerabilities and firmware risk.

Browser extensions assessment

Expand your asset coverage beyond devices and gain entity-level visibility into the various browser extensions installed across assets, permissions requested, and associated risks.

Authenticated scans for vulnerability assessment

Run scans on unmanaged devices by remotely targeting by IP ranges or hostnames to remotely access the devices.

Network shares assessment

Protect against misconfigurations used in the wild by attackers for lateral movement, reconnaissance, data exfiltration, and more with configuration assessments related to common weaknesses with Windows Shares.

Leverage Microsoft threat intelligence to prioritize vulnerabilities

See the list of common vulnerabilities and exposures (CVEs) in your organization and in the broader landscape, and view events that may impact your cyber risk.

Read more about these assessments and more here »

Track and mitigate risks with ease

Bridge the gap between security and IT teams to seamlessly remediate vulnerabilities with robust contextual recommendations, built-in workflows, and application block capabilities to enable protection faster.

Comprehensive remediation information at your fingertips

Take the action-oriented recommendations and vulnerability context to initiate remediation.

Block vulnerable applications

Proactively reduce risks when taking remediation steps by blocking vulnerable versions of applications.

Seamlessly request remediations across workflows

Create a remediation task from a specific security recommendation and leverage one-click remediation requests via Intune/SCCM.

Track and report on vulnerability management progress

Get a view that shows current statistics and vulnerable device trends over time. Access APIs with rich data for custom reporting on vulnerability management progress.

Ready to learn more?

Learn more and get started »

Implementation & technical guidance »