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 multicloud and hybrid environments against ever-evolving threats.

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 and monitoring

Proactively prevent breaches with built-in and agentless scanners for continuous discovery and assessment.

» Asset discovery with one less agent
Leverage Defender for Endpoint agent 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.

» Agentless scanning
Frictionless full visibility on posture issues across VMs, containers, and endpoints even when not connected to the corporate network.

Uncover risks and prioritize what matters
Vast assessments are available to uncover vulnerabilities and misconfigurations across endpoints and multicloud workloads. 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.

» 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.

» 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.

» Hardware and firmware assessment
Full visibility into device manufacturer, processors and BIOS information to assess vulnerabilities and firmware risk.

» Cloud security posture management
Remediate your most critical risk with advanced vulnerability management capabilities for multicloud servers and containers in Defender Cloud Security Posture Management.

» 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.

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.

» 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.
## Vulnerability Management for Endpoints and Cloud Workloads

<table>
<thead>
<tr>
<th>Feature</th>
<th>Defender Vulnerability Management Standalone</th>
<th>Defender for Endpoint P2 or Defender for Servers P1</th>
<th>Defender for Endpoint P2 + Defender Vulnerability Management Add On or Defender for Servers P2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core capabilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device inventory</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk based prioritization</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remediation tracking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Continuous monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Software inventory</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Software usages insights</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Premium capabilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security baselines assessment</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Block vulnerable applications</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Browser extensions assessment</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Digital certificate assessment</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Network share analysis</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Hardware and firmware assessment</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Authenticated scan for Windows</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Vulnerability Management capabilities for multicloud servers and containers included in Defender Cloud Security Posture Management** in Microsoft Defender for Cloud at no additional cost:

- Vulnerability management is integral part of both VMs and servers, but also end-to-end cloud security posture management
- Use built-in and agentless scanners to discover vulnerabilities and misconfigurations in near real time
- Reduce cyber risk with vulnerability and misconfiguration assessments, software inventories, and usage insights
- Quickly prioritize your biggest risks in a single view with integrated CVE details
- Seamlessly remediate your biggest vulnerabilities with built-in workflows and remediation tracking

**Ready to learn more?**

- Defender Vulnerability Management
  - Learn more and get started >>
  - Implementation and technical guidance >>
- Defender for Servers
  - Learn more >>