tenable | Data Sheet

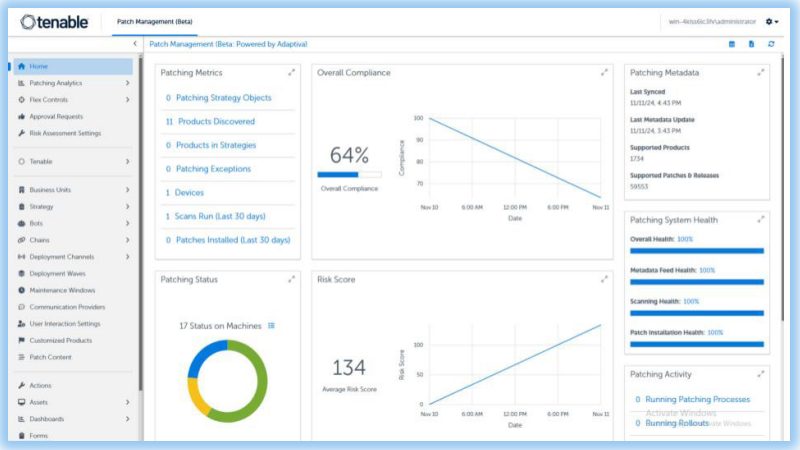
Vulnerability Exposure

Tenable Patch Management

Tenable Patch Management streamlines the time from vulnerability discovery to remediation

Companies face thousands of vulnerabilities each month and spend hours conducting research to address them. IT teams might even be wasting time applying a patch for a vulnerability that has a low chance of being exploited. With both teams working long hours only to be stuck in a reactive state, a new tactic is required to get ahead of threat actors and transition to a proactive program.

Tenable's leading vulnerability and exposure management solutions pair built-in prioritization, threat intelligence and real-time insight with enterprise level patching to shorten mean time to remediation (MTTR). With Tenable Patch Management your teams can collaborate efficiently with automatically synced vulnerabilities and their security context to the best superseded patch, helping to eliminate the bottleneck effect between prioritization and remediation. IT teams then have the power to decide when, where, and how to deploy remediation actions. Whether your organization requires approval workflows, different policies per user group or device type, version control and more, Tenable Patch Management gives your teams full control. Move your organization forward with customizable autonomous patching to help IT teams scale and move away from firefighting.



Tenable Patch Management shortens the time from discovery to remediation with automated correlation between vulnerabilities and patches.

Key benefits

- **Know your exposure**

  Tenable's leading exposure management capabilities provide full visibility into impactful vulnerabilities.

- **Expose remediation blockers**

  Gain the context you need to strategically mobilize teams against critical vulnerabilities.

- **Close vulnerability exposure**

  With a proactive patching strategy, easily align SLAs with company policies and get ahead of threat actors.

- **Mobilize IT teams**

  Automatically sync vulnerability data to the best superseded patch so IT isn't waiting for the next findings export.

- **Increase efficiency**

  Track remediation improvement via analytics dashboards when using customizable controls to deploy autonomous patching within your organization's requirements.

- **Maximize ROI**

  Leverage automation where possible allowing your teams to spend their hours tackling higher priority tasks.

Key capabilities

Automatically correlate vulnerabilities to the best superseding patch

With our integrated solution, get the combined power of Tenable, the world's #1 vulnerability management solution, and patch management for seamless risk-based vulnerability remediation. Automated correlation between vulnerabilities and the correct remediation action ensures Security and IT teams are working off the same information, rather than IT teams waiting for the latest exported spreadsheet. IT teams also get security context from Tenable's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) in their console to make informed patching decisions.

Automate patching

Teams are constantly firefighting to keep up with new patches. With Tenable Patch Management your IT team can set up automation with guardrails in place to prevent problematic updates from going out, such as customizable controls that give real-time control of deployment actions (e.g. pausing, canceling or rolling back patches), and applying precise controls like version management, product exceptions, and targeted or global pauses.

Flexible deployment

Autonomous patching works when settings are highly customizable to meet organization policies. Tenable Patch Management gives administrators the power to create phased deployment schedules for different user groups or system types, leverage criticality ratings to prioritize critical patches when they're available, create exceptions for patches based on attributes (e.g. expiration, installation requirements, and versions), define and edit approval settings and workflows to align with your policies, and block patches based on a number of factors such as specific groups of devices, system type and more.

Off-network delivery

Endpoints receive content from a geographically optimal source, with peer delivery when available ensuring off-network devices receive content wherever they are. Unique peer to peer technology scales distribution from a single server, without additional infrastructure or incremental cost. This is key for securing remote and mobile locations without compromising network performance.

Comprehensive Patch Library backed by research

Each patch is processed and tested before publishing to minimize manual packaging. Patches for Windows, MAC, Linux, 1700+ third party applications, drivers, and BIOS are automatically available when a new patch is released. Problematic updates are automatically added to a Block List until a new fix is published. Organizations also have the power to create their own Block List manually or dynamically via rules.

Track and visualize remediation success with patch analytics

While security teams have dashboards and reports from Tenable, IT teams get their own console with real-time visibility into remediation metrics, trends and exposure in Tenable Patch Management. With both teams using a Tenable solution, organizations can unify KPIs and encourage collaboration for more effective and efficient remediation. IT teams can also monitor patching progress and compliance status in real-time via analytics dashboards along with CVEs by exploit type, vulnerability age and more along with Tenable's VPR and ACR.

Powered by Adaptiva

Tenable and Adaptiva have collaborated to bring Tenable Patch Management to market, bringing Adaptiva's expertise and leading technology to our leading vulnerability management solutions. Adaptiva's game-changing automation capabilities empower our customers to move from reactive firefighting to proactive programs.

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.