DATASHEET

WatchGuard Patch Management

Reduce the risk and complexity of managing vulnerabilities in OS and third-party applications

Exploitation of known vulnerabilities remains one of the most common attack methods. Industry reports continue to highlight that attackers increasingly target vulnerabilities that already have available patches, often within days of disclosure.

For MSPs who manage lots of different environments, patching has shifted from a routine maintenance task to an operational challenge. They must act quickly to reduce exposure while ensuring updates do not disrupt business operations.

Vulnerabilities: A Latent Risk

Today's patch management challenge isn't just identifying missing updates but applying them safely at scale. With so many different customer environments, patching needs to be executed in a way that limits instability, downtime, or inconsistency across them.

Many organizations struggle with traditional vulnerability management tools because:

- Vulnerability discovery is a long process. Teams must deploy critical patches quickly to reduce exposure, and if an incident occurs, the response must be immediate.
- Remote work and decentralized infrastructure make it difficult for on-premises, network-dependent tools to ensure full coverage.
- Managing separate test and production workflows and inconsistent patch sets increases the likelihood of human error and patch variability.

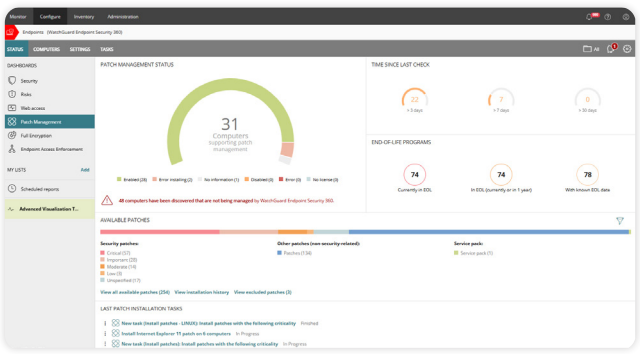

Figure 1: Patch Management organization status - main dashboard

WatchGuard Patch Management

WatchGuard Patch Management simplifies and modernizes how organizations manage vulnerabilities across Windows, macOS, and Linux, as well as third-party applications.

Fully integrated with WatchGuard Cloud and leveraging existing endpoint agents, the solution delivers centralized visibility and control across the entire patch lifecycle, from discovery and prioritization to deployment and validation.

Built for MSPs and the SMBs they protect, Patch Management enables teams to transform patching from a manual, risk-prone task into a controlled, automated process for a more predictable, scalable, and secure patching process.

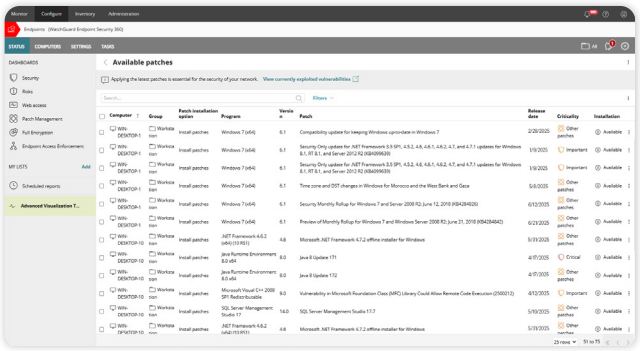

Figure 2: Available patches - Patch Management

Key Features

Discovery and Visibility

- Real-time, multi-tenant visibility into vulnerable endpoints, missing patches, and unsupported (EOL) software, with remediation status
- Detailed patch intelligence, including CVE references of associated security bulletins
- Continuous or scheduled patch discovery with configurable scan intervals
- Notification of pending patches in exploit detection
- Correlation of exploit detections with missing patches to accelerate remediation
- Remote isolation, patching, and re-connection of endpoints from a single console

Planning and Deployment

- Define patch policies by severity, software, and environment
- Schedule patching for immediate, one-time, or recurring execution
- Automate staged deployments by testing patches on designated endpoints before promoting to production
- Ensure consistency by deploying the exact same validated patches across environments
- Configure restart behavior and exceptions to minimize user disruption
- Rollback to quickly resolve compatibility issues

Monitoring and Reporting

- Centralized dashboards with real-time visibility into patch status across all endpoints
- Actionable views of update status, including pending or unsuccessful patches
- High-level summaries and detailed reporting for operational tracking and compliance

Access Control and Administration

- Role-based access control with granular permissions by user, group, or tenant
- Scoped visibility into vulnerabilities, patches, and update status based on assigned roles

Centralized Patch Control

- Full control over operating system updates, including the ability to disable native update services (e.g., Windows Update)
- Exclude specific patches by version, type, or known conflicts
- Exclude specific applications from patching as needed
- Local caching of downloaded patches to optimize bandwidth and deployment performance

Benefits

Within a single user-friendly solution, WatchGuard Patch Management allows you to:

Shrink the Attack Surface
Stay ahead of threats by creating automatic patching rollouts, including critical patches, to reduce entry points for attackers

Prioritize Response to Vulnerabilities
Quickly identify, prioritize, and remediate exposures across OS and third-party applications.

Reduce Risk With Validated Patching
Test patches before deployment and ensure only proven updates reach production systems.

Gain Visibility Across Environments
Get an aggregated view of vulnerabilities, patch status, and pending updates to quickly visualize customers' security status.

Improve Patching Efficiency
Reduce lag time with automated sequencing, centralized control, and real-time visibility.

Uniquely Control Multi-Tenant Environments
Apply subscriber-aware policies and success criteria tailored to each customer environment.

Supported platforms and systems requirements of WatchGuard Patch Management

Compatible with WatchGuard EDR, Endpoint Security Basic, Prime, 360, and Elite.

Supported operating systems: Windows, macOS (Catalina or higher) and Linux (RedHat, CentOS and SUSE).Windows, macOS (Catalina or higher) and Linux (RedHat, CentOS and SUSE).

List of compatible browsers: Google Chrome, Mozilla Firefox, Microsoft Edge and Safari.

Patch Management for Vulnerabilities:
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Supported 3rd-party applications:
https://www.watchguard.com/wgrd-resource-center/patch-management

About WatchGuard

WatchGuard Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers (MSPs). For more than 30 years, WatchGuard has defined how MSPs deliver security at scale, continuously innovating to stay ahead of every major shift in the threat landscape. WatchGuard's AI-powered Unified Security Platform® delivers zero trust-aligned network, endpoint, and identity protection in a single, integrated platform, enabling MSPs to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by more than 25,000 MSPs protecting over 1.5 million customers worldwide, WatchGuard enables partners to deliver strong, measurable security outcomes for customers across the globe. Learn more at WatchGuard.com.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.