DATASHEET

WATCHGUARD PATCH MANAGEMENT

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

According to Ponemon Institute,[1] 57% of victims of cyberattacks said that applying a patch would have prevented them from being attacked and 34% said that they knew about the vulnerability before the attack.

Ransomware cyberattacks like Wanny Cry or Petya were the perfect storm against businesses with poor OS patch management policies, but not the only ones. 86% of vulnerabilities are due to unpatched third-party applications such as Java, Adobe, Firefox, Chrome, Flash, and OpenOffice.

VULNERABILITIES: A LATENT RISK

The exploitation of vulnerabilities is currently still the number one cause of most security breaches. Notorious case such as Wanna Cry, Petya and BlueKeep, which caused havoc worldwide, are still fresh in everyone's mind.

Only a small number of attacks occur as a result of true unknown vulnerabilities (zero day attacks), since most are caused by known vulnerabilities.

The digital transformation is making it increasingly difficult to reduce the attack surface, due to the growing number of users, devices, systems and third-party applications that require updates.

At least three common operational issues frustrate vulnerability management (VM) programs:

- Vulnerability discovery is a long process. However, response must be immediate in the event of an incident.
- Companies are decentralized, employees are not continuously connected to the corporate network. On-premises VM tools do not cover these scenarios.
- Other security solutions that offer patch management do not correlate detection with vulnerable endpoints to speed up response and mitigation of the attack.

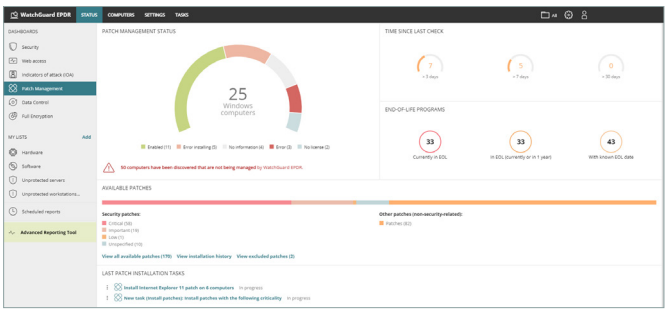


Figure 1: Patch Management organization status - main dashboard

WATCHGUARD PATCH MANAGEMENT

WatchGuard Patch Management is a user-friendly solution for managing vulnerabilities in operating systems and third-party applications on Windows, macOS, Linux workstations and servers. It reduces the attack surface, while at the same time strengthening your organization's prevention and containment capabilities.

The solution does not require any new endpoint agents or management consoles, as it is fully integrated with all of WatchGuard's endpoint solutions.

It also provides centralized, real-time visibility into the security status of software vulnerabilities, missing patches, updates and unsupported (EOL)[2] software, as well as tools for the entire patch management cycle: from discovery and planning to installation and monitoring.

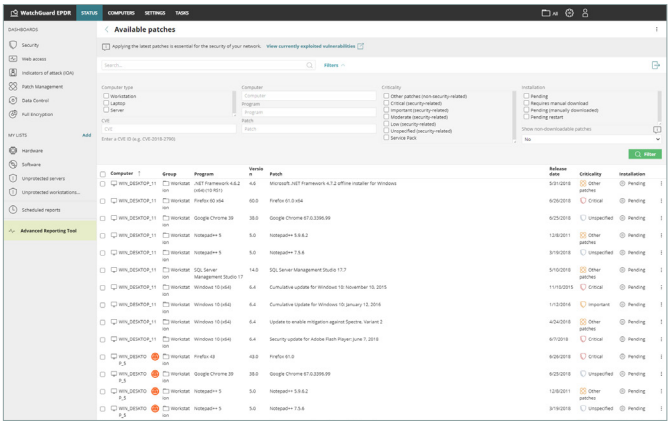


Figure 2: Available patches - Patch Management

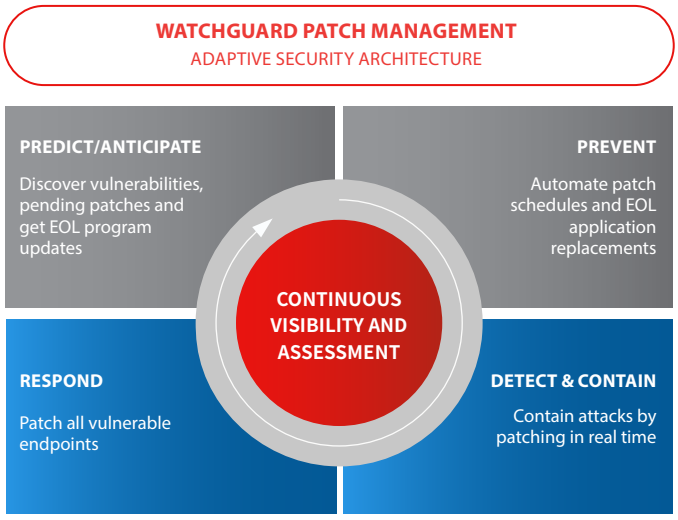
[1] Cost and consequences of gaps in vulnerability response - Ponemon.

[2] EOL (End-of-Life): A product that is at the end of its useful life that no longer receives security updates

BENEFITS

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

- Audit, monitor and prioritize operating system and application updates. The single-panel view offers centralized, up-to-the-minute and aggregated visibility into the security status of the organization with regard to vulnerabilities, patches and pending updates of systems and hundreds of applications.
- Prevent incidents, systematically reducing the attack surface created by software vulnerabilities. Handling patches and updates with easy-to-use, real-time management tools that enable organizations to get ahead of vulnerability exploitation attacks.
- Contain and remediate vulnerability exploitation attacks by immediately pushing out updates or patches from the web console. Affected computers can be isolated from the rest of the network, preventing the attack from spreading.
- Reduce operating cost:
  - Simplifies management, as it does not require you to deploy new endpoint agents or update any existing agents.
  - Minimizes patching efforts as updates are launched remotely from the Cloud-based console.
  - Provides complete, immediate visibility into all vulnerabilities, pending updates and EOL applications immediately after activation.
- Comply with the accountability principle, integral to many regulations. This forces organizations to take the appropriate technical and organizational measures to ensure proper protection of the sensitive data under their control.



"Designing an Adaptive Security Architecture for Protection from Advanced Attacks" - Gartner

KEY FEATURES

Discovery:

- Single-panel view with real-time information of all vulnerable computers, pending patches and unsupported (EOL) software, with their remediation status.
- Detailed information about pending patches and updates, details of relevant security bulletins (CVE).
- Automatic search for available patches in real time or at periodic intervals (3, 6, 12 or 24 hours).
- Notification of pending patches in exploit detections.
- Ability to isolate, patch and deisolate computers and servers.

Patch and update planning and installation tasks:

- Configure criticality and software to patch.
- Schedule for immediate, one-time execution or for repeated execution at regular intervals (date/time).
- Control computer restarts and set exceptions.
- Rollback to uninstall a patch that may cause an unexpected conflict with an existing configuration.

Endpoint and update status monitoring via:

- Dashboard and actionable lists. High-level and detailed reports.
- Lists of updated computers, computers with pending updates with errors.

Granular management based on groups and roles with different permissions:

- Role-based visibility into vulnerable computers, patches and service packs.

Centralized control over updates, patches and software:

- Ability to disable Windows Update and centrally manage operating system updates.
- Ability to exclude specific patches by version and by type.
- Capacity to exclude software (e.g. Java).
- Caching of downloaded patches.

Supported platforms and systems requirements of WatchGuard Patch Management

Compatible with WatchGuard EPDR, WatchGuard Advanced EPDR, WatchGuard EDR and WatchGuard EPP

Supported operating systems: 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