Panda Patch Management

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

panda a WatchGuard brand

Today, **99.96% of active vulnerabilities** in corporate endpoints are related to **missing updates**.[1] If these updates were installed, they would greatly contribute to preventing security risks. In fact, according to Ponemon Institute,[2] **57% of victims** of cyber attacks said that applying **a patch would have prevented them** from being attacked and **34%** said that they knew about the vulnerability before the attack.

What's more, **86% of vulnerabilities** are due to unpatched **third-party applications** such as Java, Adobe, Firefox, Chrome, Flash, and OpenOffice, among others.[1]

IT IS TIME TO CHANGE THIS TREND WITH PANDA PATCH MANAGEMENT

Panda Patch Management is a user-friendly **solution for managing vulnerabilities in operating systems and third-party applications** on Windows workstations and servers. It **reduces the attack surface**, while at the same time strengthening your organisation'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 Panda Security's endpoint solutions.

It **provides centralised, real-time visibility** into the security status of **software vulnerabilities**, missing **patches, updates and unsupported (EOL[3]) software**, inside and outside the corporate network, as well as easy-to-use and real-time tools for the entire patch management cycle: from discovery and planning to installation and monitoring.

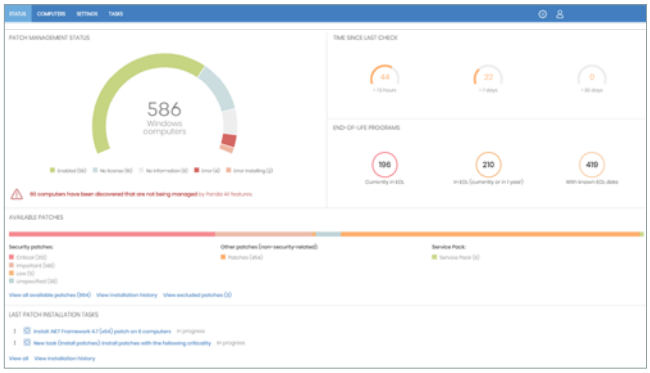


Figure 1: Patch Management organization status - main dashboard

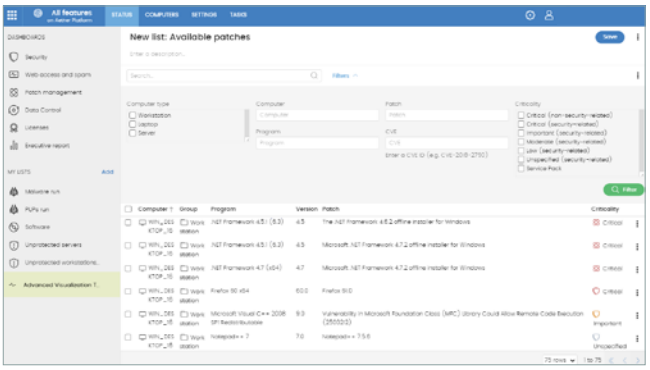


Figure 2: Available patches - Patch Management

VULNERABILITIES: A LATENT RISK

Unpatched **operating systems and third-party software** provide the perfect breeding ground for attackers and exploits. These threats can take advantage of vulnerabilities for which patches have been available weeks or even months before the breach.

The massive disclosure of vulnerabilities, such as those exposed by the Shadow Brokers or WikiLeaks, with detailed instructions on how to compromise systems and applications, enables a growing number of cyber criminals to launch attacks.

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 **five 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 decentralised**, employees are not continuously connected to the corporate network. **On-premises VM tools** do not cover these scenarios.
- Most VM tools require **another specific agent** on endpoints that are already overloaded.
- The Microsoft VM tool does not allow organisations to carry out centralised, unified updates of **third-party applications.**
- Other security solutions that offer patch management **do not correlate detection with vulnerable endpoints** to speed up response and mitigation of the attack.

Compatible solutions within the AETHER PLATFORM:

Panda Endpoint Protection | **Panda Endpoint Protection Plus**

Panda Adaptive Defense | **Panda Adaptive Defense 360**

Installation requirements for Panda Patch Management:
http://go.pandasecurity.com/patch-management/requirements

Supported 3rd-party applications:
www.pandasecurity.com/business/PatchManagementApp

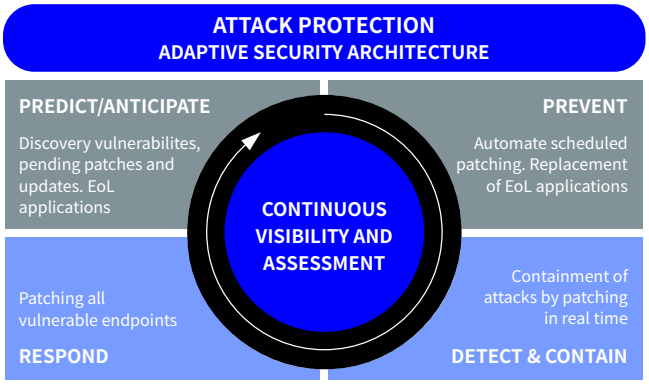
[1] **Gartner, Focus on the Biggest Security Threats, Not the most Publicised.** Published: 2 November 2017. Zero days vulnerabilities are only 0.4%, for the rest of them, 99,96%, there are patches that fix them. National Vulnerability Database. 86% of vulnerabilities are found in 3rd-party applications.
[2] **Cost and consequences of gaps in vulnerability response** – Ponemon
[3] **EOL (End-of-Life): A product that is at the end of its useful life** (from the vendor's point of view), that may no longer receive security updates

panda
a WatchGuard brand

BENEFITS

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

- **Audit, monitor and prioritise operating system and application updates.** The single-panel view offers centralised, up-to-the-minute and aggregated visibility into the security status of the organisation 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 organisations to get ahead of vulnerability exploitation attacks.
- **Contain and mitigate vulnerability exploitation attacks** with immediate updates. The Panda Adaptive Defense 360 console, in conjunction with Patch Management, allows organisations to correlate detected threats and exploits with vulnerabilities. Response time is minimised, containing and remediating attacks by immediately pushing out patches from the web console. Affected computers can be isolated from the rest of the network, preventing the attack from spreading.
- **Reduce operating cost:**
  - **Panda Patch Management does not require you to deploy new endpoint agents or update any existing agents**, simplifying management and avoiding workstation and server overload.
  - **Minimises patching efforts as updates are launched remotely** from the Cloud-based console. Additionally, installation is optimised to minimise errors.
  - **Provides complete, immediate visibility into all vulnerabilities**, pending updates and EOL[3] applications immediately after activation.
- **Comply with the accountability principle**, integral to many regulations (GDPR, HIPAA and PCI). This forces organisations to take the appropriate technical and organisational measures to ensure proper protection of the sensitive data under their control.



Panda Patch Management augments the preventive, detection and response capabilities of Panda Security's endpoint solutions by enabling a robust implementation of the Adaptive Security Architecture.[4]

KEY FEATURES

Panda Patch Management provides all necessary tools to manage the security and updates of the operating system and third-party applications from a single console:

Discovery:

- Single-panel view with real-time information of all vulnerable computers, pending patches and unsupported (EOL[3]) software, with their remediation status.
- Detailed information about pending patches and updates, details of relevant security bulletins (CVE), as well as computer and computer group information, and more. Available actions:
  - Filter and search for patches based on criticality, computer, group, application, patch, CVE and status.
  - Ability to take actions directly on computers: restart, install now or schedule.
- Unattended scanning for pending updates, in real-time or at periodic intervals (3, 6, 12 or 24 hours).
- Notification of pending patches in exploit detections. Ability to launch installations immediately or schedule them from the console, isolating the computer if required.

Patch and update planning and installation tasks:

- Configurable by criticality.
- On specific endpoints and groups.
- Immediate, scheduled for one-time execution or for repeated execution at regular intervals (date/time).
- Ability to 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.

Centralised 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).

[4] **Gartner: "Designing an Adaptive Security Architecture for Protection from Advanced Attacks"**, Neil MacDonald, Peter Firstbrook

WatchGuard
PANDA SECURITY AFRICA 021.683.3899 | sales@za.pandasecurity.com www.watchguard.com | pandasecurity.africa