Panda Patch Management

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

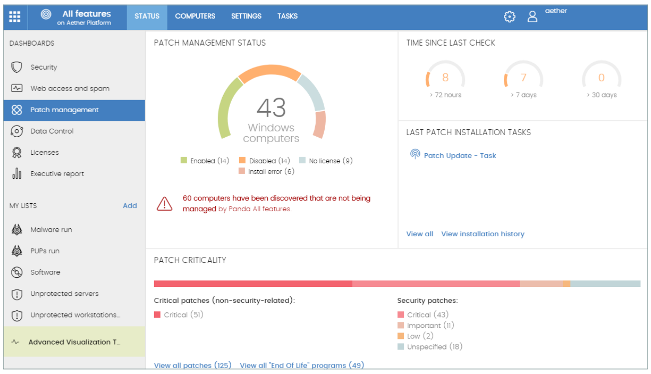
Today, 99.96% of active vulnerabilities in corporate endpoints are related to missing updates which, if installed, would greatly prevent the security risk. Additionally, 86% of vulnerabilities are due to unpatched third-party applications such as Java, Adobe, Mozilla, Firefox, Chrome, Flash, and OpenOffice, among others[1].

If this trend continues, by 2020, 99% of the vulnerabilities causing security incidents will be known exploits that could be easily avoided by being patched before the incident[2].

IT IS TIME TO CHANGE THIS TREND WITH PANDA PATCH MANAGEMENT

Panda Patch Management is a user-friendly solution for managing vulnerabilities of the operating systems and third-party applications on Windows workstations and servers. It reduces risk while strengthening the prevention, containment and attack surface reduction capabilities of your organization.

The solution does not require the deployment of any new endpoint agents or management console as it is fully integrated in all of Panda Security's endpoint solutions. Plus, it provides centralized, 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.



PATCH MANAGEMENT STATUS

43 Windows computers

🟩 Enabled (14) 🟧 Disabled (14) ▨ No license (9) 🟥 Install error (6)

60 computers have been discovered that are not being managed by Panda All features.

TIME SINCE LAST CHECK

8 > 72 hours | 7 > 7 days | 0 > 30 days

LAST PATCH INSTALLATION TASKS

Patch Update - Task

View all   View installation history

PATCH CRITICALITY

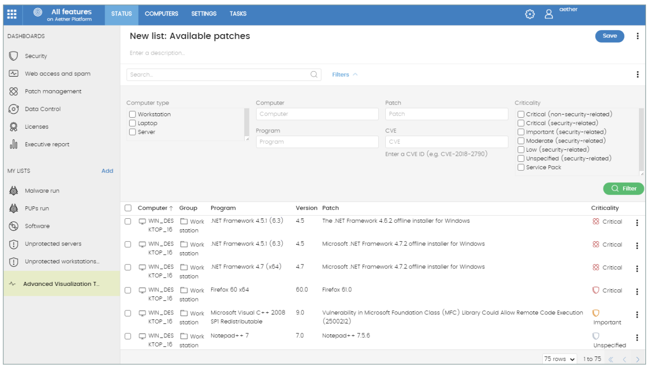
Critical patches (non-security-related):

🟥 Critical (51)

Security patches:

🟥 Critical (43)
🟥 Important (11)
🟧 Low (2)
▨ Unspecified (18)

View all patches (125)   View all "End Of Life" programs (49)



New list: Available patches

Enter a description...

Search...

Computer type
□ Workstation
□ Laptop
□ Server

Computer: Computer

Program: Program

Patch: Patch

CVE: CVE

Enter a CVE ID (e.g. CVE-2018-2790)

Criticality
□ Critical (non-security-related)
□ Critical (security-related)
□ Important (security-related)
□ Moderate (security-related)
□ Low (security-related)
□ Unspecified (security-related)
□ Service Pack

□	Computer ↑	Group	Program	Version	Patch	Criticality
□	WIN_DESKTOP_16	Work station	.NET Framework 4.5.1 (6.3)	4.5	The .NET Framework 4.6.2 offline installer for Windows	Critical
□	WIN_DESKTOP_16	Work station	.NET Framework 4.5.1 (6.3)	4.5	Microsoft .NET Framework 4.7.2 offline installer for Windows	Critical
□	WIN_DESKTOP_16	Work station	.NET Framework 4.7 (x64)	4.7	Microsoft .NET Framework 4.7.2 offline installer for Windows	Critical
□	WIN_DESKTOP_16	Work station	Firefox 60 x64	60.0	Firefox 61.0	Critical
□	WIN_DESKTOP_16	Work station	Microsoft Visual C++ 2008 SP1 Redistributable	9.0	Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)	Important
□	WIN_DESKTOP_16	Work station	Notepad++ 7	7.0	Notepad++ 7.5.6	Unspecified

75 rows   1 to 75

VULNERABILITIES: A LATENT RISK

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

The massive disclosure of information on 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 cybercriminals to launch attacks.

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 requiring updates.

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

- The **vulnerability discovery process is long**. However, in the event of an incident, the response must be immediate.
- **Companies are decentralized**, employees do not connect continuously to the corporate network. **On-premise VM** tools do not cover these scenarios.
- Most VM tools require **another specific agent** on endpoints that are already overloaded.
- Microsoft VM tool does not allow organizations to update **third-party applications** in a centralized and unified way.
- Other security solutions, that offer patch management, **do not correlate detection and vulnerable endpoints** for speeding up the response and the mitigation of the attack.

[1] Gartner, Focus on the Biggest Security Threats, Not the most Publicized. 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] Gartner: How to Respond to the 2018 Threat Landscape. Greg Young. Published: 28 November 2017
[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 Patch Management

BENEFITS

Panda Patch Management allows, within **a single user-friendly solution:**

- **Audit, monitor and prioritize operating systems 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 the 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 mitigate vulnerability exploitation attacks** with immediate updates. Panda Adaptive Defense 360 console, in conjunction with Patch Management, allows organizations to correlate detected threats and exploits with the uncovered vulnerabilities. Response time is minimized, containing and remediating attacks by pushing out patches immediately from the web console. Additionally, affected computers can be isolated from the rest of the network, preventing the attack from spreading.

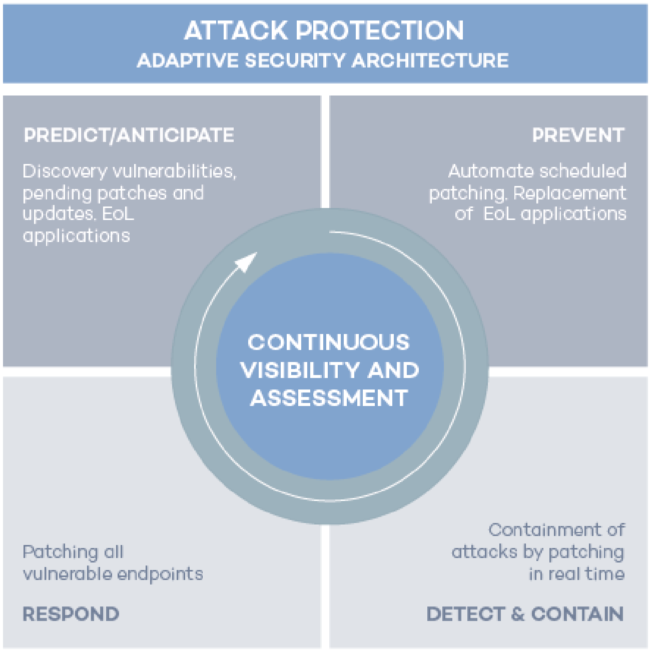
- **Reduce operating costs.**

  - **Panda Patch Management does not require the deployment or update of any new or existing endpoint agents**, simplifying management and avoiding workstation and server overloads.

  - **Minimizes patching efforts as updates are launched remotely** from the cloud-based console. Additionally, installation is optimized to minimize errors.

  - **Provides complete, unattended visibility into all vulnerabilities**, pending updates and EOL[3] applications immediately after activation.

- **Comply with the accountability principle** contemplated in many regulations (GDPR, HIPAA and PCI). It forces organizations to take the appropriate technical and organizational measures to ensure proper protection of the sensitive data under their control.


ATTACK PROTECTION
ADAPTIVE SECURITY ARCHITECTURE
PREDICT/ANTICIPATE
Discovery vulnerabilities, pending patches and updates. EoL applications
PREVENT
Automate scheduled patching. Replacement of EoL applications
CONTINUOUS VISIBILITY AND ASSESSMENT
Patching all vulnerable endpoints
RESPOND
Containment of attacks by patching in real time
DETECT & CONTAIN

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, from a single console, the security and updates of the operating system and third-party applications:

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 patches and pending updates, details of the relevant security bulletin, 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 ID 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).
- In exploit detections, notification of pending patches. Ability to launch installations immediately or scheduled from the console, isolating the computer if required.

Patch and update planning and installation tasks:

- Configurable by criticality.
- Can be performed 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.

Centralized control over updates, patches and software:

- Ability to disable Windows Update and centrally manage operating system updates.
- Ability to exclude patches Windows Update and centrally manage operating system updates.
- Capacity to exclude software (e.g: Java).

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

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

CLOUD BASED MANAGEMENT PLATFORM

Aether Platform

Aether's cloud-based platform and management console, common for all of Panda's endpoint solutions, provide optimized advanced and adaptive security management inside and outside the corporate network. Minimize complexity and maximize flexibility, granularity and scalability.

Achieve more in less time. Easy implementation

- Deploy, install and configure the solution in minutes. Immediate value from day one.
- A single lightweight agent for all products and platforms (Windows, Mac, Linux and Android).
- Automatic discovery of unprotected endpoints. Remote installation.
- Proprietary proxy and repository/cache technologies. Optimized communication even with endpoints without an Internet connection.

Simplified operations. Adapts to your organization

- Intuitive Web console. Flexible, modular management that reduces the total cost of ownership.
- Configures users with total or limited visibility and permissions. Action audit.
- Group and endpoint-based security policies. Predefined and custom roles.
- Hardware and software inventories and change log.

Easy scaling of security and management capabilities over time

- No need for new infrastructure to deploy the modules. No deployment costs.
- Real-time communication with endpoints from a single Web console.
- Dashboards and indicators per module.

Awards and Certifications

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs.

Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.

Panda Security acknowledged as 'Visionary' in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2018.