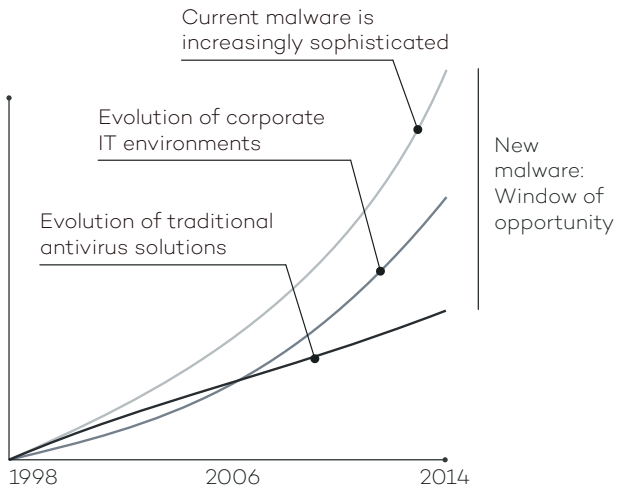
Adaptive Defense 360

Limitless Visibility, Absolute Control

COMPLETE ENDPOINT DEFENSE INTEGRATING PROTECTION, DETECTION, RESPONSE AND REMEDIATION IN A SINGLE SOLUTION

Defending the endpoint against attack is hard. Protection must include a wide range of defenses including traditional antivirus/anti-malware, personal firewall, Web & email filtering and device control. And, any defense must provide additional safeguards against difficult-to-detect zero-day and targeted attacks. Up to now, IT has needed to acquire and maintain a number of different products from different vendors to defend the endpoint.

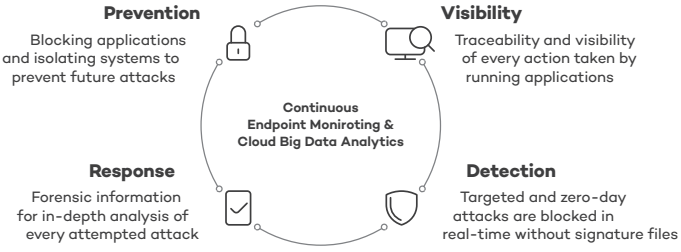
Adaptive Defense 360 is the first and only offering to combine Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities into a single solution. Adaptive Defense 360 also automates capabilities reducing the burden on IT. Adaptive Defense 360 starts with Panda's best-of-breed EPP solution which includes Simple and centralized security, Remedial actions, Real-time monitoring and reports, Profile-based protection, Centralized device control, and Web monitoring and Filtering.



However, that is only the beginning. The malware and IT security environment has undergone major changes in terms of volume and sophistication. With over 200,000 new viruses appearing every day, and the sophistication of techniques for penetrating defenses and hiding malware, corporate networks are more vulnerable than ever to zero-day and targeted attacks.

Traditional Endpoint Protection solutions are efficient at blocking known malware by using detection techniques based on signature files and heuristic algorithms. However, they are no defense againstzero-day and targeted attacks that take advantage of the 'window of opportunity for malware,' the time lapse between the appearance of new malware and the release of the antidote by security companies. An increasing gap that is exploited by hackers to get viruses, ransomware, Trojans and other types of malware into corporate networks. Such increasingly common threats can encrypt confidential documents and demand a ransom, or simply collect sensitive data for industrial espionage.

Adaptive Defense is Panda's solution to these types of attacks. Adaptive Defense provides an EDR service that can accurately classify every application running in an organization, only allowing legitimate programs to run. The EDR capabilities of Panda Adaptive Defense 360 relies on a security model based on three principles: continuous monitoring of applications on a company's computers and servers, automatic classification using machine learning on our Big Data platform in the cloud, and finally, as an option, our technical experts analyze those applications that haven't been classified automatically to be certain of the behavior of everything that is run on the company's systems.



These capabilities are now combined with the best-of-breed EPP solution from Panda, closing the cycle of the adaptive malware protection, which now includes automated prevention, detection, forensics and remediation.

The only solution to guarantee the security of all running applications

COMPLETE AND ROBUST PROTECTION GUARANTEED

Panda Adaptive Defense 360 offers two operational modes:

- Standard mode allows all applications catalogued as goodware to be run, along with the applications that are yet to be catalogued by Panda Security and the automated systems.
- Extended mode only allows the running of goodware. This is the ideal form of protection for companies with a 'zero risk' approach to security.

FORENSIC INFORMATION

- View execution event graphs to gain a clear understanding of all events caused by malware.
- Get visual information through heat maps on the geographical source of malware connections, files created and much more.
- Locate software with known vulnerabilities installed on your network.

PROTECTION FOR VULNERABLE OPERATING SYSTEMS AND APPLICATIONS

Systems such as Windows XP, which are no longer supported by the developer and are therefore unpatched and vulnerable, become easy prey for zero-day and new generation attacks.

Moreover, vulnerabilities in applications such as Java, Adobe, Microsoft Office and browsers are exploited by 90 percent of malware.

The vulnerability protection module in Adaptive Defense 360 uses contextual and behavioral rules to ensure companies can work in a secure environment even if they have systems that are not updated.

FULL EPP CAPABILITIES

Adaptive Defense 360 integrates Panda Endpoint Protection Plus, the most sophisticated EPP solution from Panda, thus providing full EPP capabilities, including:

- Remedial actions
- Centralized device control: Prevent malware entry and data loss by blocking device types
- Web monitoring and filtering
- Exchange server antivirus and anti-spam
- Endpoint Firewall, and many others...

CONTINUOUS STATUS INFORMATION ON ALL ENDPOINTS IN THE NETWORK

Get immediate alerts the moment that malware is identified on the network, with a comprehensive report detailing the location, the computers infected, and the action taken by the malware.

Receive reports via email on the daily activity of the service.

SIEM AVAILABLE

Adaptive Defense 360 integrates with SIEM solutions to provide detailed data on the activity of all applications run on your systems.

For clients without SIEM solution, Adaptive Defense 360 can include its own system for storing and managing security events to analyze all the information collected in real time.

100% MANAGED SERVICE

Forget about having to invest in technical personnel to deal with quarantine or suspicious files or disinfect and restore infected computers. Adaptive Defense 360 classifies all applications automatically thanks to machine learning in our Big Data environments under the continuous supervision of PandaLabs' experts.

TECHNICAL REQUIREMENTS

Web Console

- Internet connection
- Internet Explorer 10
- Microsoft Edge
- Firefox (latest version)
- Google Chrome (latest version)

Agent

- Operating systems (workstations): Windows XP SP2 or higher, Vista, Windows 7, 8, 8.1 and 10.
- Operating systems (servers): Windows Server 2003 SP1 or higher, 2008, 2008 R2, 2012, 2012 R2, 2016 and Server Core 2008, 2008 R2, 2012, 2012 R2 and 2016.
- Internet connection (direct or through a proxy)

Partially supported (only EPP):

- Linux, MAC OS X and Android

Advanced Reporting Tool

From Data to Actionable IT and Security Insight

The increase in the security data volumes handled by organizations prevents IT departments from adequately focusing on important details

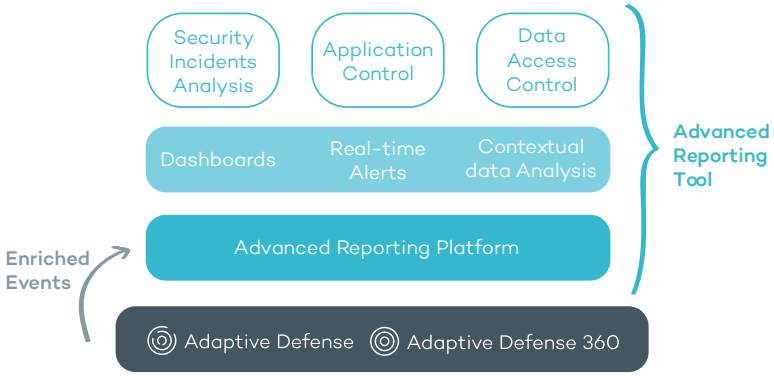
This information can be used to detect security issues and breaches caused by both external factors and company insiders.

IT departments are overwhelmed: The large volumes of information handled and the appearance of next-generation malware causes many details to be **overlooked or simply not registered at all**, compromising the security of the entire system.

The solution: Adaptive Defense and Advanced Reporting Tool

Advanced Reporting Platform automates the storage and correlation of the information related to process execution and its context extracted by **Adaptive Defense** from endpoints.

This information enables **Advanced Reporting Tool** to automatically generate security intelligence and provide tools that allow organizations to **pinpoint attacks and unusual behaviors**, regardless of their origin, as well as **detecting internal misuse of the corporate systems and network**.



Advanced Reporting Tool provides the necessary data to draw informed conclusions about corporate IT and security management. These conclusions can then be used to define the basis of an action plan aimed at:

› **Determining the origin of security threats** and applying security measures to prevent future attacks.

› Implementing **more restrictive policies to access critical business information**.

› Monitoring and controlling **misuse of corporate resources** that may have an impact on business and employee performance.

› **Correcting employee behavior** that is not in line with the usage policies defined.

Key Benefits

1. Find relevant information

Maximize visibility into everything that occurs on every device and increase IT department efficiency and productivity.

Access historical data to analyze corporate resource security and usage indicators.

Get in-depth information to identify security risks and insider misuse of the IT infrastructure.

2. Diagnose network issues

Reduce the number of tools and data sources required to fully understand what happens on devices and its relation to the security and use of corporate assets.

Extract resource usage and user behavior patterns to demonstrate their potential business impact.

3. Alert and be alerted

Transform anomaly detection into real-time alerts and reports.

Build business confidence, flagging security anomalies and employee misuse of IT resources in real time.

4. Create horizontal and vertical insight

Generate configurable detailed reports to perform methodical analyses of your company's security posture, identify misuse of corporate assets and find behavioral anomalies.

Show the status of key security indicators and track their evolution over time as a consequence of the corrective actions taken.

FLEXIBLE ANALYSES ADAPTED TO YOUR COMPANY'S NEEDS

Advanced Reporting Tool incorporates dashboards with key indicators, search options and default alerts for three specific areas:

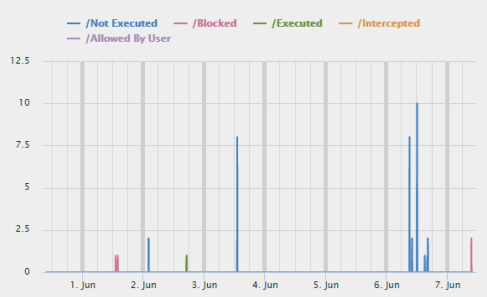
- Security incidents.
- Access to critical information.
- Application and network resource usage.

Adapt searches and key information alerts to your business needs.

SECURITY INCIDENT INFORMATION

Generate security intelligence, processing and correlating the events generated during intrusion attempts.

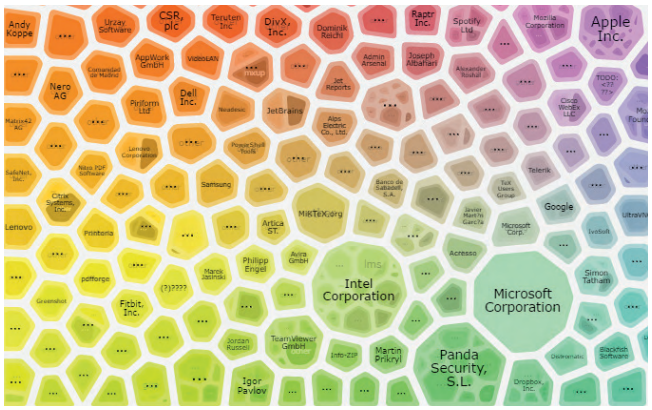
- Calendar charts showing the malware and PUPs detected over the last year.
- Computers with most infection attempts and malware specimens detected.
- Malware execution status on network computers.
- Pinpoint computers with vulnerable applications.



COST REDUCTION

Discover IT resource usage patterns to define and enforce cost reduction policies.

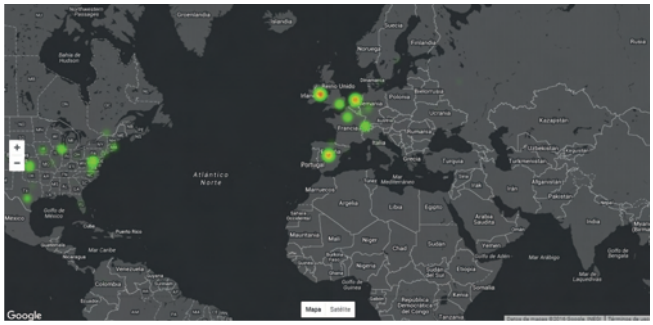
- Find the corporate and non-corporate applications run on your network.
- Office licenses used vs purchased.
- Applications with most bandwidth consumption.
- Vulnerable applications run or installed on the network that may lead to infections, have an impact on business performance or involve remediation costs.



CONTROL ACCESS TO BUSINESS DATA

Shows access to confidential data files and data leaks across the network.

- Countries that receive most connections from your network.
- Files most accessed and run by network users.
- Find out which users have accessed certain computers on the network.
- Calendar charts showing the data sent over the last year.



REAL-TIME ALERTS

Configure alerts based on events that can reveal a security breach or the infringement of a corporate data management policy:

- Default alerts indicating risk situations.
- Define custom alerts based on user-created queries.
- Seven delivery methods (on-screen and via email, JSON, Service Desk, Jira, Pushovery, and PagerDuty).

FLEXIBLE, CONFIGURABLE, CLOUD-HOSTED BIG DATA SERVICE

- Adapted to the needs of network administrators, both regarding storage space as well as the ability to perform searches on historical data.
- Immediate startup. Doesn't require changes to the customer's network or installing additional infrastructures.
- Configurable environment, perfectly suited to the needs of the IT department.

TECHNICAL REQUIREMENTS

Supported browsers (others may also work):

- Mozilla Firefox.
- Google Chrome.

Internet connection and secure communication through port 443.

Minimum screen resolution 1280x1024 (1920x1080 recommended).

Compatible with:

- Adaptive Defense
- Adaptive Defense 360

Data Control

Monitor sensitive data across endpoints and servers

Panda Data Control: Real-time data security, visibility and control in one product.

Uncontrolled access to **your company's personal and sensitive data** is an everyday security threat that may lead to **serious financial loss and reputational damage**. **Are you willing to take that risk?**

WHY DO YOU NEED TO PROTECT YOUR ORGANIZATION'S PERSONAL AND SENSITIVE DATA?

Companies are forced to strengthen or adopt new measures to protect personal or sensitive data for the organization. The most important factors that motivate this transformation are:

- **Exponential increase in exfiltration cases.** The number of cases where poorly managed and secured data is exfiltrated from computing systems is increasing every day. Often the affected organization is not even aware that this is happening.
  These data thefts are usually due to external attacks, malicious insiders driven by lucrative objectives or revenge, or simply negligence.

- **Proliferation of unstructured data.** Unstructured data held on servers as well as on employees' and collaborators' (partners, consultants, etc.) devices and laptops makes up roughly 80 percent of all business-related data. And just as the volume of unstructured data doubles every year, so does the risk posed to businesses[1].

- **Regulatory compliance with laws such as the GDPR** whose violation can lead to 'dissuasive' fines of up to 20 million euros or 4 percent of a company's global turnover, whichever is greater. Not to mention the reputational damage caused by a data leak, and its effects on the confidence of employees as well as current and potential customers.

THE SOLUTION: PANDA DATA CONTROL

Data Control is a data security module fully integrated into the Panda Adaptive Defense platform. Data Control is designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data, both in real time and throughout its lifecycle on endpoints and servers.

Panda Data Control discovers, audits and monitors **unstructured[2] personal data** on endpoints and servers: from data at rest to data in use and data in motion.

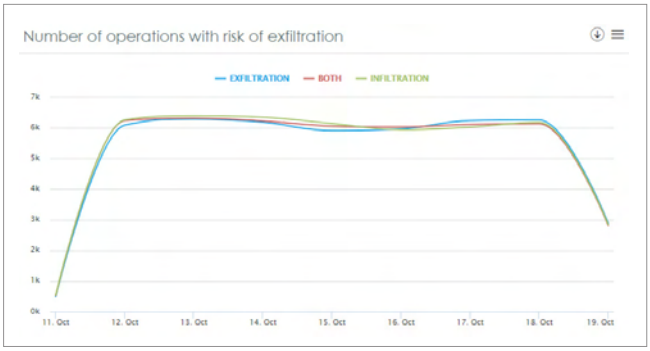


Figure 1 - This information enables organizations to monitor and determine the usual number of exfiltration operations, detecting deviations caused by security incidents.

KEY BENEFITS

Discover and audit

Identify files with Personally Identifiable Information (PII) as well as users, employees, collaborators, endpoints and servers in your organization that are accessing this personal data.

Monitor and detect

Implement proactive measures to prevent access to PII with the help of reports and real-time alerts on the unauthorized and suspicious use, transmission and exfiltration of personal data files.

Simplify management

The Panda Data Control module is native in Panda Adaptive Defense and Panda Adaptive Defense 360. It doesn't require organizations to deploy any additional software or hardware, and can be easily and immediately activated without cumbersome configurations. The Data Control module is enabled and managed from the cloud platform.

Demonstrate compliance with relevant regulations to senior management, the DPO[3], all other employees in your organization, and the Supervisory Authorities. Show the strict security measures in place to protect PII at rest, in use and in transit between endpoints and servers.

[1] Carla Arend. IDC Opinion - March 2017.
[2] Unstructured data refers to data that does not reside in a database or any other data structure. Unstructured data can be textual or non-textual. Panda Data Control focuses on the textual unstructured data held on endpoints and servers.
[3] DPO (Data Protection Officer): The person responsible for overseeing the data protection strategy in an organization.

PII SECURITY AND GOVERNANCE

Organizations protected by **Panda Adaptive Defense** can rest assured that their endpoints and servers won't be compromised by malicious programs coming from external sources, and therefore won't fall victim to external data exfiltration attacks.

Panda Adaptive Defense's **classification service categorizes 100 percent of all applications** running on the protected endpoints and servers, returning a verdict on their trustability or malicious nature, using **machine learning** techniques supervised by Panda Security's malware specialists. This system ensures that **only those applications classified as goodware** are allowed to run.

The **Data Control module** leverages the solution's Endpoint Detection and Response (EDR) capabilities to continuously monitor the protected endpoints in the organization, discovering and tracking the unstructured personal data held and transmitted across the network.

Finally, the Data Control **alerts and reports** can be customized and adapted to the specific needs of each company.

BUSINESS DATA GOVERNANCE

Strong data governance allows organizations to answer any questions related to the personal and sensitive data handled by employees: What data is held on employees' endpoints? Who accesses that data and what actions are taken on it? Are those actions aligned with your corporate policies?

Ensuring data governance is a continuous improvement process, and Panda Data Control provides the necessary tools to increase efficiency and reduce costs at every stage of that process:

- **Discover and understand** the unstructured personal and sensitive data stored across your network. Data Control allows tagging, grouping and classifying this data according to its criticality.
- **Establish security and access policies** to control data access and use by 'authorized users'.
- **Educate your employees and company** collaborators in order to ensure that they handle data in accordance with external regulations and internal policies.
- **Monitor and Demonstrate.** Use Panda Data Control's dashboard, reports and custom and predefined alerts to demonstrate data governance and compliance to the rest of the organization.
- **Analyze causes of any personal data breach and adjust corporate policies:** Panda Data Control lets you establish the sequence of actions performed by an external attacker or an insider in a breach of personal or sensitive information. This analysis allows organizations to identify and apply improvements to the data access policies in place in a continuous improvement process, as well as to provide the information required by regulations in the event of a security incident.

KEY FEATURES

Data Discovery:

Creates an indexed inventory of all files that store unstructured personal data (data at rest), with the number of occurrences of each type of data. It classifies all information automatically.

The classification process uses a combination of rules, regular expressions, and machine learning techniques, among others, optimizing classification results while reducing false positives and resource consumption on devices.

Data Monitoring:

Monitors the various types of operations performed on unstructured files (data in use), while keeping the personal data file inventory fully up to date. Any attempt to copy or move any of these files out of the network via, email, Web browsers, FTP or removable storage (data in motion) is recorded by the module.

Data Visualization:

The results of the data monitoring and discovery tasks are continuously synced on the Adaptive Defense platform and in its module Advanced Visualization Tool. This module provides tools for investigating all events affecting data at rest, in use and in motion, both in real time and retrospectively throughout its lifecycle on devices.

Data Control's dashboards and predefined reports and alerts help to cover use cases and ensure security governance of the unstructured personal data held on the organization's protected devices.

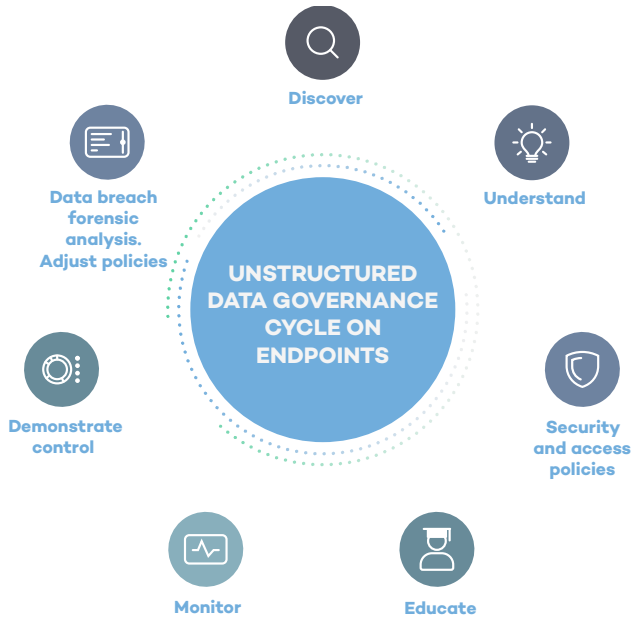


Figure 2 - Phases of the continuous improvement process to ensure data governance, and Panda Data Control's contribution to reduce costs and efforts.

Panda Data Control is an add-on for Panda Adaptive Defense or Panda Adaptive Defense 360. Available in the following countries: Spain, Germany, UK, France, and Sweden.

Panda Patch Management

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

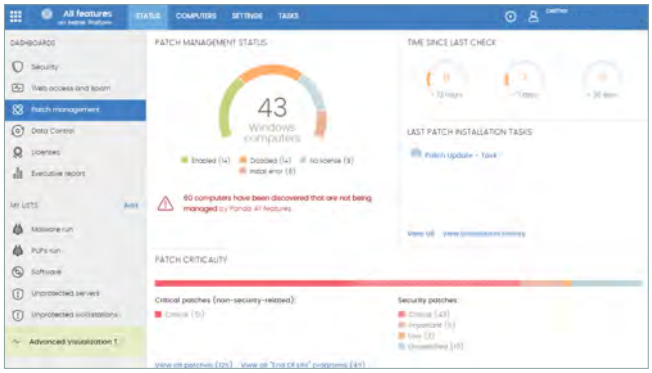
Today, 99.96% of active vulnerabilities in corporate endpoints are related to missing updates which, if installed, would greatly prevent the security risk. Additionally, 86% of corporate endpoints are missing critical patches for third-party applications such as Java, Adobe, Mozilla, Firefox, Chrome,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

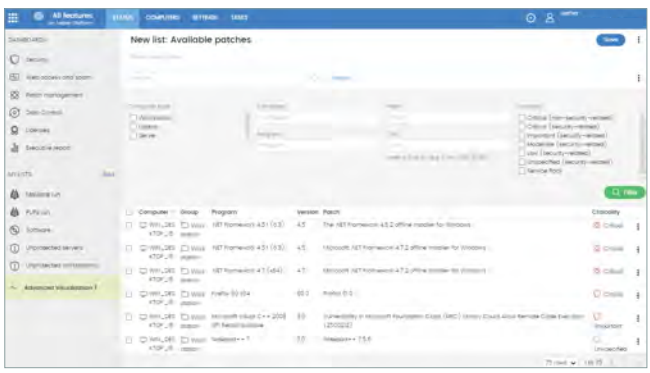
If this trend continues, by 2020, 99% of the vulnerabilities causing security incidents will be known exploits that could be easily avoided by being patched before the incident[2].

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.





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 professional 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.

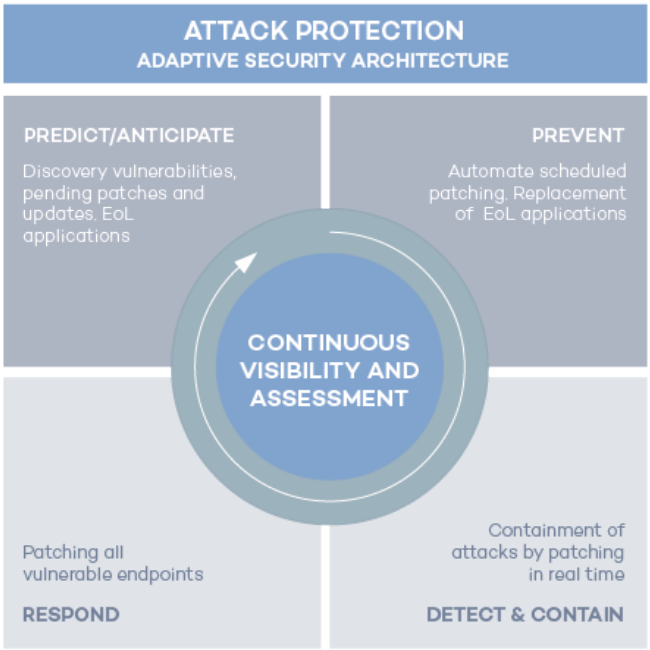
[1] National Vulnerability Database. Critical updates of 3rd-party applications are applied only in 14% of corporate endpoints and servers
[2] Gartner: How to Respond to the 2018 Threat Landscape. Greg Young. Published: 28 November 2017
[3] EOL (End-of-Life): A product that is at the end of its useful life (from the vendor's point of view). They may not 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.



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.
- Configurable alerts upon finding vulnerable workstations or servers.
- 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 and application.
- Can be performed on specific endpoints and groups.
- Immediate, or scheduled for one-time execution or for repeated execution at regular intervals (date/time).
- Ability to control computer restarts and set exceptions.

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.

Compatible with the following solutions within Aether Platform:

Panda Endpoint Protection | Panda Endpoint Protection Plus
Panda Adaptive Defense | Panda Adaptive Defense 360

Supported Operating Systems: Windows XP SP3+. Windows Server 2003 (32/64 bits and R2) SP2+

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

Certifications and awards:

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.

"Gartner Named Panda Security as a Visionary in Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) in 2018"
https://www.pandasecurity.com/gartner-magic-quadrant/

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