

ORGANIZATIONAL CYBERSECURITY

Mobility, processing, and Cloud storage have all revolutionized the business environment. **Endpoints are the primary target for most cyber attacks.** This is why endpoint security solutions need to be **advanced, adaptive, and automatic**, with the highest possible levels of **prevention and detection.**

Organizations receive thousands of weekly malware alerts, of which only 19 percent are considered trustworthy, and only 4 percent of which are ever investigated. **Two-thirds of cybersecurity administrators' time is dedicated to managing malware alerts.**

SOPHISTICATION OF CYBER ATTACKS

Cyber Defense Against Advanced Threats

State-of-the-art **cyber attacks** are designed to get around the protection provided by traditional security solutions. These attacks are becoming **more frequent** and **more sophisticated** as hackers become more professionalized. It is also a result of a lack of focus on correcting **security vulnerabilities in systems.**

In light of this scenario, **traditional protection platforms (EPPs) are insufficient.** This is because they **do not provide detailed enough visibility** into the processes and applications running on corporate networks. What's more, **some EDR solutions**, far from solving anything, **create greater stress** and increase security administrators' workloads **by delegating the responsibility for managing alerts and forcing them to manually classify threats.**

PANDA ADAPTIVE DEFENSE 360

The EDR Solution - Endpoint Detection & Response

Panda Adaptive Defense 360 is an innovative cybersecurity solution for computers, laptops and servers, delivered from the Cloud. **It automates the prevention, detection, containment and response** to any advanced threat, zero-day malware, ransomware, phishing, in-memory exploits, and malwareless attacks, both present and future, inside and outside the corporate network.

Unlike other solutions, it **combines** the widest range of **protection technologies (EPP) with automated EDR capabilities.** It also has **two services, managed by Panda Security experts**, which are delivered as a feature of the solution:

- **Zero-Trust Application Service**
- **Threat Hunting Service**

Thanks to its Cloud architecture, its agent is lightweight and has little impact on endpoints, which are managed via a single Cloud architecture, even when they are isolated.

Panda Adaptive Defense 360 is accessible from a single web console. It **integrates Cloud Protection and Management platforms (Aether)**, which maximize prevention, detection and automated response, minimizing the effort required.

BENEFITS

Simplifies and Minimizes Security Costs

- Its managed services reduce the costs of expert personnel. There are no false alerts to manage and no responsibility is delegated.
- The managed services automatically learn from threats. No time wasted on manual settings.
- Maximum prevention on the endpoint. Operating costs reduced to almost zero.
- No management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted, since it is based on a lightweight agent and Cloud-native architecture.

Automates and Reduces Detection Time

- Applications that pose a security risk are blocked (by hash or process name).
- Blocks the execution of threats, zero day malware, fileless/malwareless attacks, ransomware and phishing.
- Detects and blocks malicious in-memory activity (exploits) before it can cause damage.
- Detects malicious processes that have gotten around preventive measures.
- Detects and blocks hacking techniques, tactics and procedures.

Automates and Reduces Response and Investigation Time

- Resolution and response: forensic information to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each action; actionable visibility of the attacker and their activity, facilitating forensic investigation.
- Improvement and adjustments to security policies thanks to the conclusions of the forensic analysis.

Supported platforms and systems requirements of PANDA ADAPTIVE DEFENSE 360

Supported operating systems: [Windows](#), [macOS](#) and [Linux](#). EDR capabilities are available on Windows, macOS, and Linux, with Windows being the platform that provides all the capabilities in its entirety.

List of compatible browsers: [Google Chrome](#), [Mozilla Firefox](#), [Internet Explorer](#), [Microsoft Edge](#) and [Opera](#).

ADVANCED AND AUTOMATED ENDPOINT SECURITY

Traditional protection technologies (EPPs) focused on prevention are low-cost measures, valid for known threats and malicious behaviors, but they are insufficient. Successfully defending an organization and putting an end to cyber threats forces a shift away from traditional prevention to continuous prevention, detection and response, assuming at all times that the organization has been compromised, and that all endpoints are continually being threatened by attackers.

Panda Adaptive Defense 360 integrates traditional preventive technologies with innovative, adaptive prevention, detection and response technologies in a single solution, to deal with advanced cyber threats, both present and future:

Traditional Preventive Technologies

- Personal or managed firewall. IDS
- Device control
- Permanent multi-vector anti-malware & on-demand scan
- Managed blacklisting/whitelisting.
- Collective Intelligence
- Pre-execution heuristics
- URL filtering - web browsing
- Anti-spam and anti-phishing
- Anti-tampering
- Email content filtering
- Remediation and rollback

Advanced Security Technologies

- EDR: continuous endpoint monitoring
- Prevention of execution of unknown processes
- Cloud-based machine learns to classify 100% of processes (APTs, ransomware, rootkits, etc.)
- Sandboxing in real environments



Figure 1: Main Panda Adaptive Defense Dashboard.

- Behavioral analysis and detection of IoAs (indicators of attack) such as scripts, macros, etc.
- Automatic detection and response for targeted attacks and in-memory exploits
- Threat hunting and forensic analysis

ZERO-TRUST MODEL

This is the managed service that classifies 100% of processes, monitors endpoint activity, and blocks the execution of applications and malicious processes. For each execution, it sends out a real-time classification verdict, malicious or legitimate, with no uncertainty and without delegating to the client. All of this is possible thanks to the capacity, speed, adaptability and scalability of AI and Cloud processing.

The service unifies **big data** technologies and multi-level **machine learning** techniques, including **deep learning**, the results of continuous supervision and the automation of the experience and knowledge accumulated by Panda Security's security and threat team.

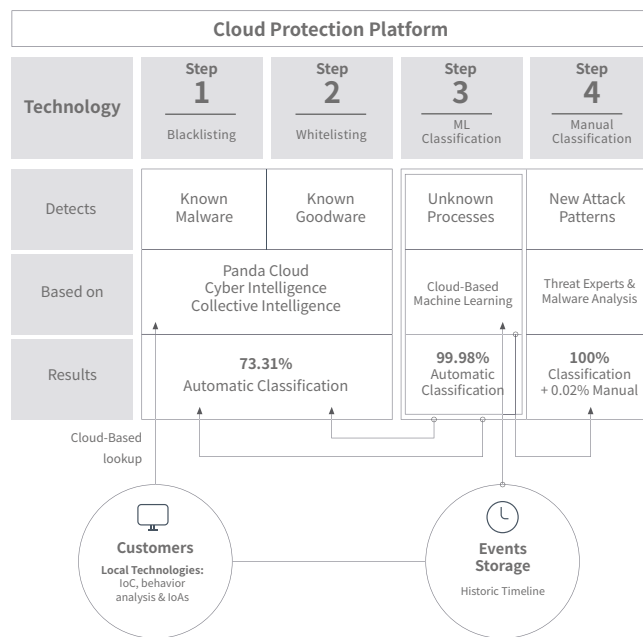


Figure 2: Sequence of Cloud classification service.

The managed Threat Hunting and Forensic Analysis Service is operated by a team of experts who use profiling analysis and event correlation tools to proactively discover new hacking and evasion techniques.

The hunters at the Panda Intelligence Center work on the premise that organizations are constantly being compromised.