Adaptive Defense 360

Next-Gen Security That Puts An End To Cyberthreats

panda a WatchGuard brand

Cybersecurity Built To Provide Optimal Protection With Minimal Management

Mobility, processing, and cloud storage have all revolutionized the corporate network structure. But with all of the advancements made, hackers are still able to find their way in. IT departments receive thousands of malware alerts every week, of which only 19% are considered trustworthy and only 4% are ever investigated. It's no wonder that two-thirds of a typical cybersecurity administrators' time is dedicated to managing alerts alone.

Endpoint security solutions need to address not only the threats from a cyberattack, but also the lack of resources to manage the process of combatting those attacks. Prevention and detection are key, but so is ensuring that the IT department gains valuable time back to focus on other critical areas by automating the activities associated with the management of the solution deployed.

The Problem With Advanced Cyberdefense Solutions

State-of-the-art cyberattacks are designed to get around the protection provided by traditional security solutions. These types of 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**.

Traditional protection platforms (EPPs) are insufficient against these kinds of attacks because they do not provide enough visibility and detail into the processes and applications running on corporate networks. To address this issue, IT departments are adding additional protection in the form of Endpoint Defense and Response (EDR) solutions. The problem with most EDR platforms is the management falls entirely on the security admin, increasing their workload tenfold by requiring them to manage alerts and manually classify threats.

The Solution To Advanced Cyberdefense: Adaptive Defense 360

Panda Adaptive Defense 360 (AD360) 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. This level of protection ensures that both present and future threats are eliminated regardless of if they reside inside or outside of the corporate network.

Unlike other solutions that focus solely on EDR capabilities, AD360 combines traditional endpoint protection (EPP) with next-gen automated EDR capabilities providing a full protection model to address both known and unknown threats. Another market differentiator are two key features that AD360 delivers as a service, unlike competitors that leave the management of both to the IT department:

- **100% Classification Service**
- **Threat Hunting and Investigation Service**

Thanks to its cloud architecture, the 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

- Managed services means there are no tasks to delegate and no false alerts to manage which reduces the costs of expert personnel needed
- The managed services automatically learn from threats so no time is wasted on manual settings
- Maximum prevention on the endpoint reduces operating costs 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 bypassed preventive measures
- Detects and blocks hacking techniques, tactics and procedures

Automates and Reduces Response and Investigation Time

- Resolution and response via forensic information to investigate each attack attempt and tools to mitigate its effects (disinfection)
- Ability to trace each action of the attacker and their activity, facilitating forensic investigation
- Improvement and adjustments to security policies thanks to the conclusions of the forensic analysis

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com/business

Adaptive Defense 360

panda a WatchGuard brand

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 putting an end to cyberthreats forces a shift away from traditional prevention to a model of continuous prevention, detection and response, assuming at all times that the network has been compromised, and that all endpoints are constantly under attack.

Panda Adaptive Defense 360 allows IT departments to achieve this security posture by integrating traditional EPP technologies with EDR capabilities under a single solution making the network impenetrable against both known and unknown threats.

Traditional Preventive Technologies

- Personal or managed firewall. IDS
- Device control
- Permanent multivector antimalware & on-demand scan
- Managed blacklisting/whitelisting
- Collective Intelligence
- Pre-execution heuristics
- URL filtering - web browsing
- Antispam & Antiphishing
- Anti-tampering
- Email content filtering
- Remediation and rollback

Advanced Security Technologies

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

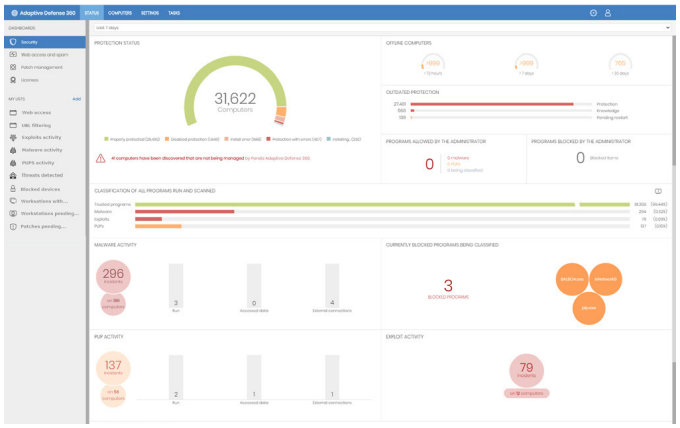

Figure 1: Main Panda Adaptive Defense 360 Dashboard

Zero-Trust Model

AD360 operates on a "Zero Trust Model" which is the principle belief that organizations should not trust any entity inside or outside of their perimeter at any time. This methodology is achieved through the managed service that classifies 100% of processes, monitors endpoint activity, and blocks the execution of applications and malicious processes. For each execution, a real time classification verdict is sent of either malicious or legitimate, with no uncertainty, and without intervention by the IT staff. 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**, which is the result of continuous supervision and automation of the experience and knowledge accumulated by Panda's internal security team.

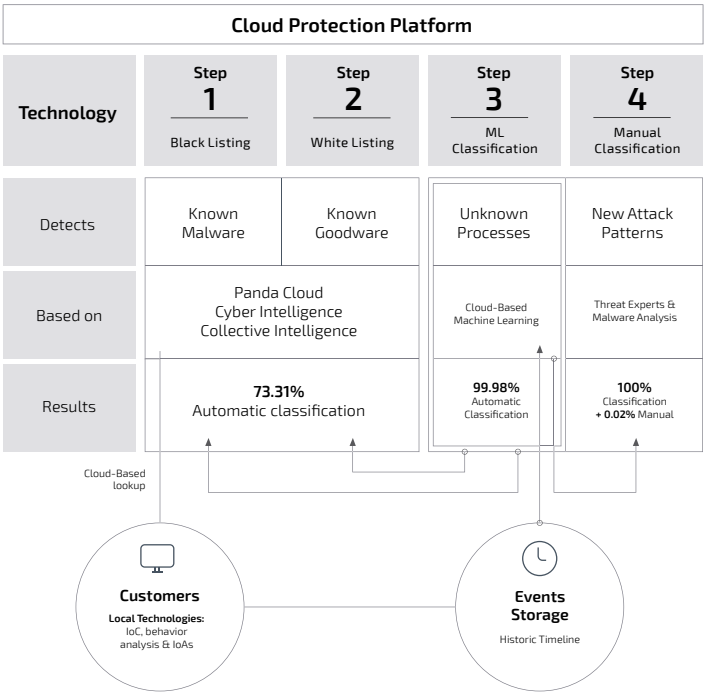

Figure 2: Sequence of cloud classification service.

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

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

AWARDS AND CERTIFICATIONS

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, and NSSLabs. Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.