The Data Fueled Intelligence You Need to Be Breach Proof

PANDA ADAPTIVE DEFENSE 360

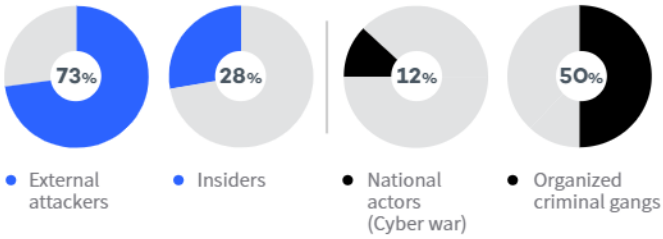
Panda Adaptive Defense 360 combines traditional antivirus technology with the advanced protection model of endpoint detection and response into a single solution to defend against both known and unknown threats.

panda
a WatchGuard brand

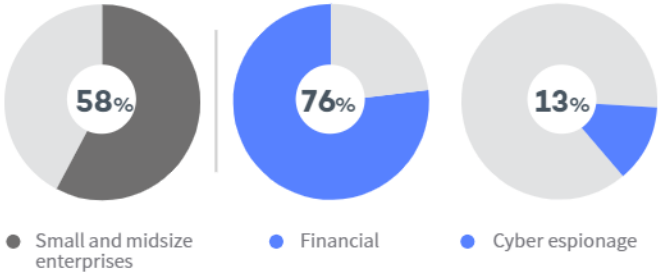
panda
a WatchGuard brand

THE THREAT LANDSCAPE

Where are attacks coming from?[1]



Who are the victims? What are the motives?[1]



What is the cost to companies?

- Global cost: $600,000 M[2]
- Cost of a Data Breach: $3.86 M[3]

THE EVOLUTION OF HACKERS

Hackers are increasingly sophisticated and growing in number as a result of their professionalization, the sharing of technologies, and the continuous leaks of cyber intelligence.

ELIMINATING THE ATTACK SURFACE

Next-generation cyber threats they manufacture are designed to slip past **traditional solutions** completely undetected, leaving networks everywhere vulnerable without the proper defenses in place.

Traditional protection platforms are insufficient against advanced 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. EDR capabilities include continuous monitoring and data analytics of network activity, giving IT departments the data and detection they need to combat advanced threats.

MANAGING THE IT WORKLOAD

With the number of machines deployed in the corporate infrastructure increasing every year, security teams face difficulties managing and defending devices that reside both on and off the network. And while EDR solutions are a vital part of protection for advanced threats, most add to the difficulty of managing the IT environment. This is mostly due to lack of automation when it comes to management of the platform, because they require the team to manage alerts being generated and manually classify threats.

ENDPOINT DETECTION AND RESPONSE SOLUTIONS (EDR)

What Is the Primary Functionality of EDR Solutions?

EDR solutions monitor, log and store the details of endpoint activity, such as user events, processes, changes to the registry, memory and network usage. This visibility uncovers threats that would otherwise go unnoticed.

What Are the Hidden Problems with EDR Solutions?

Multiple techniques and tools are used to search for security anomalies in events and confirm or reject alerts. All of this requires human intervention.

EDR solutions require 24/7 supervision and rapid response from highly qualified personnel.

These resources are expensive and hard to find. Short-staffed organizations with low budgets are unprepared to take advantage of the benefits of EDR solutions on their own. Personnel find themselves with greater workloads deriving from the implementation and operation of these solutions, instead of the solutions supporting them in what matters: improving the security posture of their organizations.

The Answer to This Problem?

Panda's Adaptive Defense 360.

[1] "2018 Data Breach Investigation report". Verizon
[2] "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
[3] "2018 Cost of a Data Breach Study: Global Overview". Ponemon Institute/IBM Security

panda
a WatchGuard brand

PANDA ADAPTIVE DEFENSE 360

Panda Adaptive Defense 360 is an innovative cyber-security solution for desktops, laptops and servers, delivered from the Cloud. It automates the prevention, detection, containment and response against any present or future advanced attacks, zero day malware, ransomware, phishing, memory exploits and malware-less attacks, inside and outside the corporate network.

Thanks to its Cloud architecture, the agent is light and does not impact the performance of endpoints, which are managed through a single Cloud console, even when not connected to the Internet.

Panda Adaptive Defense 360 integrates Cloud Protection and Management Platforms (Aether), which maximize prevention, detection and automated response, minimizing the effort required.

It differs from other solutions in that it combines the widest range of protection technologies (EPP) with automated EDR capabilities, thanks to one service managed by Panda Security experts, and delivered as feature of the solution: Zero-Trust Application Service, which automates the management of alerts and the decision-making around them.

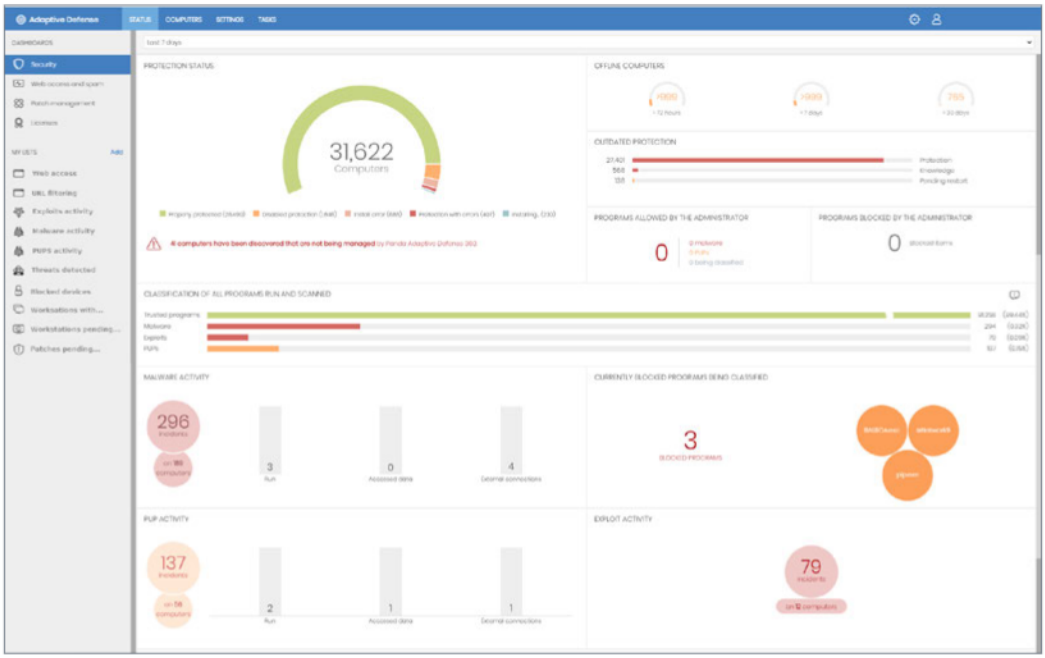


Figure 1: Main Panda Adaptive Defense Dashboard.

BENEFITS: PANDA ADAPTIVE DEFENSE 360

Simplifies and Minimizes the Cost of Advanced and Adaptive Security

- Its managed services reduce the cost of expert personnel by eliminating the responsibility of managing alerts and the decision-making around what to do with them
- 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
- There is no management infrastructure to install, configure or maintain
- Endpoint performance is not impacted as it is based on a lightweight agent and Cloud architecture

Automates and Reduces Detection and Exposure Time (Dwell Time)

- Prevents the running of threats, zero day malware, ransomware and phishing
- Detects and blocks malicious activity in memory (exploits), before it can cause damage
- Detects malicious processes that slip past preventive measures
- Detects and blocks hacking techniques and procedures

Automates and Reduces Response and Investigation Time

- Automatic and transparent remediation
- Recovery of endpoint activity and the immediate recovery of normal activity
- Actionable insights into attackers and their activity, speeding up forensic investigation
- Reduction of the attack surface, instantly improving the security posture

REDUCING THE IT WORKLOAD: ZERO-TRUST APPLICATION SERVICE

The Zero-Trust Application Service monitors and prevents the execution of malicious applications and processes on endpoints. For each execution, a real-time classification is automatically issued of either malicious or legitimate, eliminating the need for human intervention. All this is possible thanks to the speed, capacity, flexibility and scalability of AI and Cloud processing.

The service combines big data and multi-level machine learning, including deep learning, and is fueled by the continuous supervision and automation of the experience, intelligence and accumulated knowledge of experts in security and threats at Panda Security's Intelligence Center.

The Zero-Trust Application Service is able, like no other solution on the market, to free IT Departments from the risk of running malware on endpoints inside and outside the corporate network.

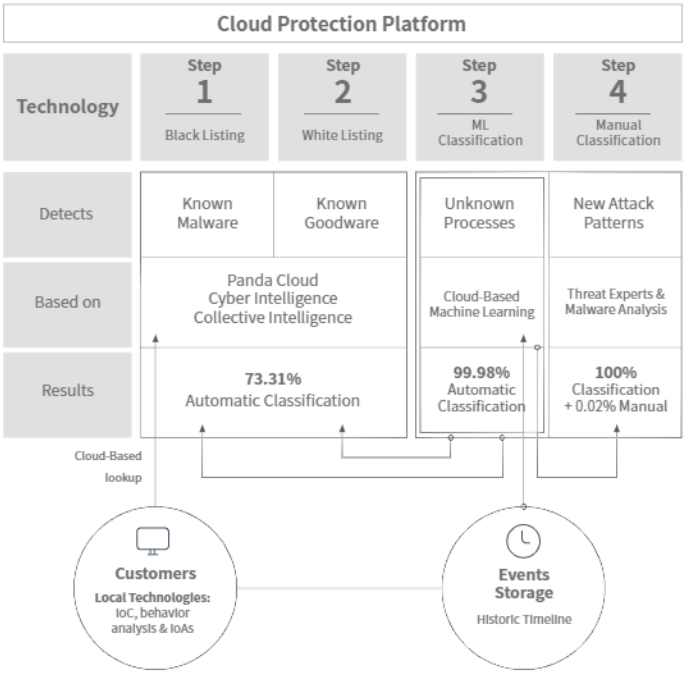


Figure 2: Workflow of the managed Cloud Zero-Trust Application service.

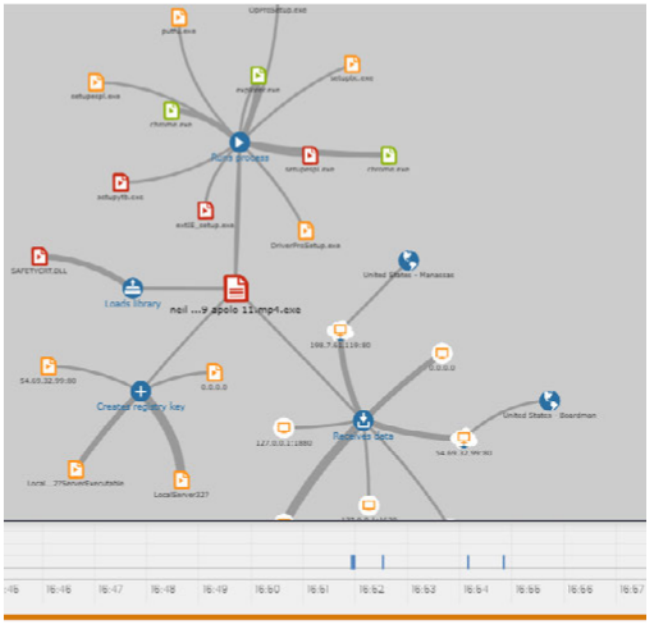


Figure 3: The Panda Adaptive Defense 360 console incident timeline enables forensic investigation: the date it was first seen on the network, names and number of endpoints affected, settings changes and with whom it has communicated.

ADVANCED AUTOMATED SECURITY ON ENDPOINTS

Panda Adaptive Defense 360 integrates, in a single solution, traditional preventive technologies with next-gen capabilities for prevention, detection and automated response against advanced cyber threats.

Traditional Preventive Technologies

- Personal or managed firewall. IDS
- Device control
- Multi-vector permanent anti-malware and on-demand scan
- Managed blacklisting/whitelisting. Collective intelligence
- Pre-execution heuristics
- Web access control
- Anti-spam & Anti-phishing
- Anti-tampering
- Mail content filter
- Remediation and rollback

Advanced Security Technologies

- EDR: continuous monitoring on endpoints activity
- Prevention of the execution of unknown processes
- Cloud-based machine learns to classify 100% of processes (APTs, ransomware, rootkits, etc)
- Cloud-based sandboxing in real environments
- Behavioral analysis and IoA detection (scripts, macros, etc)
- Automatic detection and response to memory exploits

CLOUD MANAGEMENT PLATFORM: AETHER

Next-generation security, visibility and control. Comprehensive and scalable from the Cloud, to deliver value immediately.

The Aether platform and its Cloud console optimize the management of advanced and adaptive security inside and outside the network.

Designed so that security teams focus solely on managing the cybersecurity posture of the organization, it minimizes complexity and maximizes flexibility, granularity and scalability.

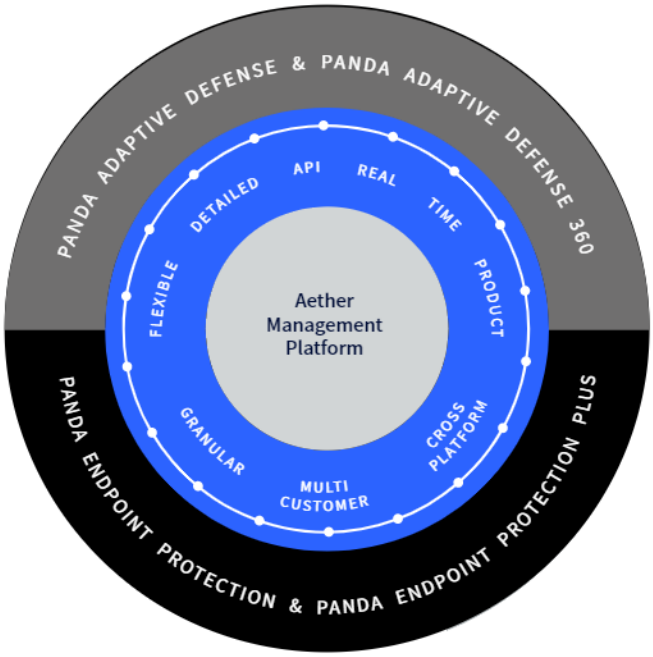


Figure 3: Unified Cloud management platform: Aether

BENEFITS OF THE AETHER PLATFORM

Achieve Greater Value in Less Time with Simple Implementation That Provides Immediate Visibility

- Deployment, installation and configuration in minutes providing value from day one
- Lightweight multi-product and multi-module agent deployable on all common platforms (Windows, Mac, Linux, Android)
- Automatic discovery of unprotected endpoints and remote installation
- Proprietary proxy technology, even on computers with no web connection
- Traffic optimization, with proprietary repository/cache technology

Easy to Use, Adapting to Your Organization

- Intuitive Cloud-based console that provides flexible and modular management
- Predefined and custom roles
- Detailed audit of actions in the console
- Users with total or restricted permissions and visibility
- Security policies for groups and endpoints
- Hardware and software inventories and changelog

Facilitates Monitoring That Accelerates Response

- Prioritized key indicators and dashboards
- Prioritized and confirmed alerts in your workflow
- Complete and actionable history of incidents: processes involved, source, dwell time, prevalence, etc.
- Act on endpoints with a single click: restart, isolate, patch and scan, accelerating response time

AWARDS AND CERTIFICATIONS

WatchGuard and Panda are committed to consistently subjecting their solutions to independent third-party testing and validation. We are proud of the recognition we receive from leading testing organizations including Virus Bulletin, AV-Comparatives, AV-Test and NSS Labs.

AV-Comparatives endorses Adaptive Defense 360 "As this solution classifies all executed processes, it cannot fail to record any malware"

Supported Platforms And System Requirements of PANDA ADAPTIVE DEFENSE 360

The supported platforms are continually evolving in order to provide the maximum possible coverage to the newest operating systems. Access the online support of each of our products using the following links:

Windows Servers & Workstations: http://go.pandasecurity.com/endpoint-windows/requirements
Mac OS Devices: http://go.pandasecurity.com/endpoint-macos/requirements
Linux Servers & Workstations: http://go.pandasecurity.com/endpoint-linux/requirements
Android Mobile & Devices: http://go.pandasecurity.com/endpoint-android/requirements
Panda Patch Management: http://go.pandasecurity.com/patch-management/requirements
Panda Cloud Systems Management: http://go.pandasecurity.com/systems-management/requirements
SIEM Feeder: http://go.pandasecurity.com/siem-feeder/requirements
Advanced Reporting Tool: http://go.pandasecurity.com/reporting-tool/requirements
Panda Full Encryption: http://go.pandasecurity.com/full-encryption/requirements

WatchGuard

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