# The Threat Landscape Is Constantly Evolving

In order to be truly efficient, an endpoint protection solution should offer prevention, detection, visibility, and adaptive intelligence — before, during, and after an attack takes place.

**Adaptive Defense 360** integrates all of these elements into a lightweight protection package for endpoints, supported by a large and scalable processing capacity in the cloud.

panda
a WatchGuard brand

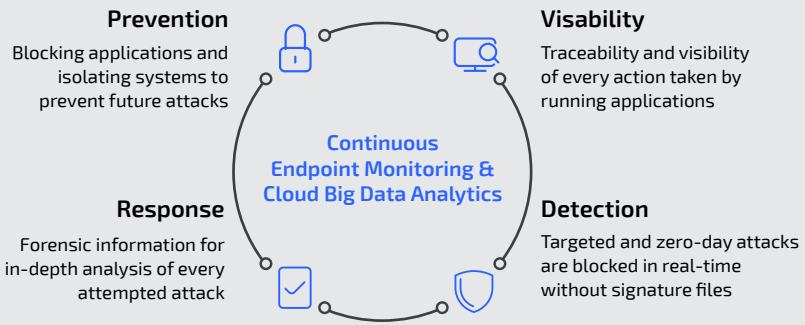
pandasecurity.com/business
watchguard.com

# Adaptive Defense 360

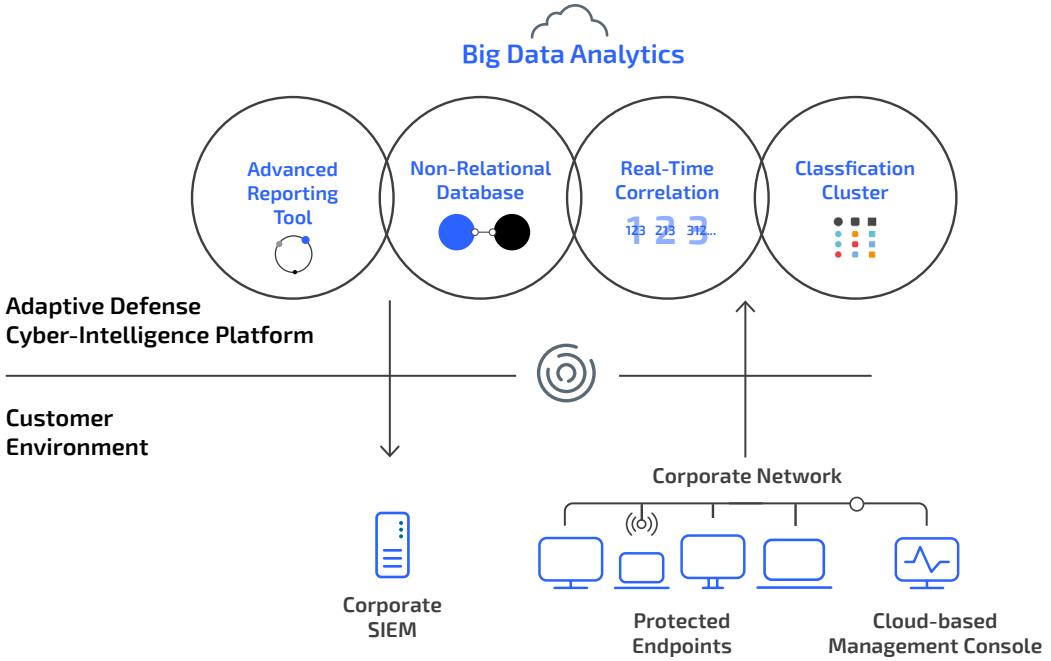
Traditional antivirus solutions are effective in blocking known malware using detection techniques based on signature indexes and heuristic algorithms. However, they are not effective against zero-day attacks and targeted attacks, which are designed to take advantage of malware's "window of opportunity" through tools, tactics, techniques, and malicious procedures (TTPs).
The window of opportunity is getting wider, and this widening is being exploited by hackers to infect networks with viruses, ransomware, Trojans and other types of advanced malware and targeted attacks.

## Guarantee the Security of All Running Applications

The Adaptive Defense family of products and services is Panda Security's solution to these types of attacks. Adaptive Defense offers an endpoint detection and response service capable of accurately classifying every application running in the organization, allowing only trusted actions to be executed.




Panda Adaptive Defense is built on a security model based on three principles: continuous monitoring of all applications on servers and workstations, automatic classification of endpoint processes using big data and machine learning techniques in a cloud-based platform, and the possibility, should a process not be automatically classified, of an expert technician analyzing the behavior.




True security solutions should combine advanced technologies with human and computational intelligence. In other words, machine learning with experts at the helm. For a security solution to be considered a next gen technology, it should offer prevention, detection, visibility, and intelligence that can uninterruptedly detain any kind of cyberattack.

Decision-makers should look for the following key elements when it comes to choosing an endpoint security solution:

- **Continuous monitoring** by recording and monitoring all activity of running processes in order to stop untrusted software in its tracks at the time of execution, detect advanced threats in real time, respond in a matter of seconds, and recover instantaneously.
- **Detect the execution of untrusted files** which allows for a reduction in the attack surface. Ensuring that the security solution classifies all applications running on devices as either trusted or malicious is vital to protecting the network from threats.
- **Intelligent threat detection,** because human intervention is not always possible to manage the monitoring and response of an attack. Effective security solutions must be able to operate autonomously and automatically to adapt to the operating environment, which is unique to every organization.
- **Quick and automated response.** Organizations are saturated with the volume of events and alerts generated by their systems, but once the cybercriminal has infiltrated, the theft of information can happen in a matter of seconds. Therefore, the chosen security solution must be able to quickly identify an ongoing attack, establish measures to avoid damage and relieve the workload placed on systems. An automated response can cut costs and complete tasks that previously took days to finish.

# Next-Gen Protection Capabilities

| | Adaptive Defense 360 | AV | Anti Exploit | Anti Ransom | Sand Boxing |
|---|---|---|---|---|---|
| **PROTECTION AGAINST THE DYNAMICS OF ATTACKS, SUCH AS:** | | | | | |
| Known malware, unknown malware, and zero day attacks, including any new ransomware or variant | ● | ◒ | | | ◒ |
| Advanced Persistent Threats (APTs), Targeted attacks and Cyberspionage | ● | | | | |
| Known and unknown exploit attacks including malwareless attacks | ● | | ● | | |
| Botnet attacks that turn computers into controlled by Command and Control (C&C) servers | ● | | | | ◒ |
| **NEXT-GENERATION ENDPOINT PROTECTION (NGEP)** | | | | | |
| Prevents malicious software, detects attacks while they're taking place, and prevents repeat attempts | ● | ◒ | ◒ | ◒ | |
| Continuously monitors running processes, classifies all applications stopping their execution if they are not trusted | ● | | | | |
| Continuously adapts to new threat dynamics using machine learning techniques in a big data environment | ● | ◒ | | | ◒ |
| Long-term focus on the attack, detecting and dynamically blocking tools, tactics, techniques, and malicious procedures (TPPs) | ● | | | | |
| **DETECTION, CONTAINMENT, AND RESOLUTION** | | | | | |
| If something is not looking right or some suspicious behavior is blocked, you will be alerted in real time | ● | | | | |
| Provides information in real time about the activities of an attacker: origin, cause, impacted assets, and actions taken | ● | | | | |
| Automatic resolution, deleting malicious files, repairing changes, and killing compromised processes | ● | ◒ | ◒ | ● | ◒ |
| Offers operative information on tasks carried out after the fact, and measures taken against future attacks | ● | | | | |
| **MANAGED SECURITY SERVICE** | | | | | |
| Automation with machine learning and big data, minimizing the workload of security teams and the time between detection and response | ● | | | | |
| Experts in the field of discovering new attacks ("threat hunters") reinforce the service | ● | ◒ | | | |
| Surveillance and monitoring of attackers' activity 24/7, 365 days a year | ● | ◒ | | | ◒ |
| **INCIDENT INVESTIGATION TOOLS** | | | | | |
| Provides timelines of an attack (files, records, drivers, etc.) and its impact on the business (e.g., affected assets, zombie machines or devices) | ● | | | | |
| Access to granular, user-based information to preserve confidentiality | ● | | | | |
| Full integration with other investigation tools, and SIEMs in particular | ● | | | | |
| **RISK MANAGEMENT INTELLIGENCE** | | | | | |
| Complete visibility on all systems: software running, vulnerable applications, user behavior, traffic, etc. | ● | | | | |
| Search tools for anomalies caused by external attacks, insiders, or improper use of company resources | ● | | | | |
| Tools based in a big data, cloud-based platform, which minimizes operating costs and response time | ● | | | | |
| **EASY TO DEPLOY AND MANAGE** | | | | | |
| Easy to deploy, update and manage from the cloud, which allows remote systems to be protected as if they were on the network | ● | ● | ● | ● | ◒ |
| Large-scale deployment, without interruption of service, with self-learning and adaptation to the company in a transparent way (up & running in hours) | ● | | | | |
| Multiple technologies perfectly integrated, avoiding undue consumption and enhancing synergies between them | ● | ● | | | |
| Minimum impact on the network and on protected devices, with a maximum impact of 5% on system performance | ● | ◒ | ◒ | ◒ | |
| Minimal inconvenience for end-users. It avoids work overload on Operations Teams that can focus on incidents investigation | ● | ◒ | ◒ | ◒ | |
| **REAL TIME PROCESSING CAPABILITY** | | | | | |
| Machine learning technology in big data environments as the exclusive method for classifying processes in real time | ● | | | | |
| Cloud and big data processing enable the spread, sharing and exponential growth of knowledge, in real time | ● | ◒ | | | |
| Cloud use and data mining without computational limitation reduce the complexity of systems and promote efficient risk management | ● | ◒ | | | |

Get started protecting your endpoints with Adaptive Defense 360
visit **pandasecurity.com/business** and **watchguard.com** to learn more.

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