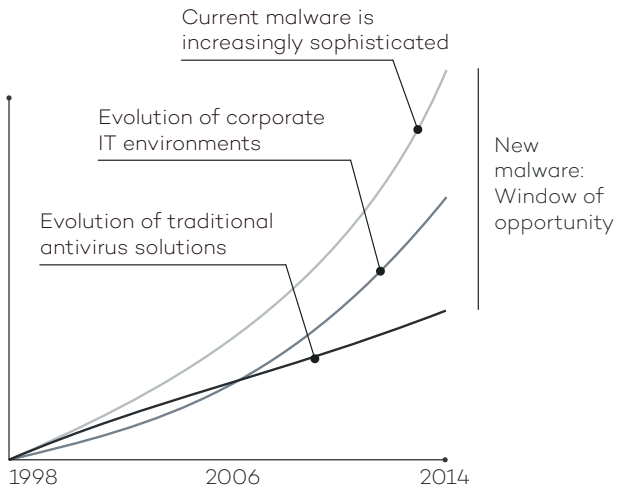
Adaptive Defense 360

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.

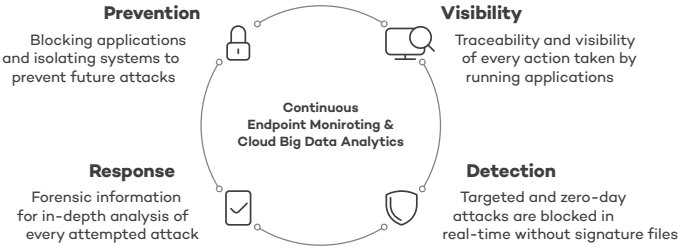
Adaptive Defense 360 is the first and only offering to combine Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities into a single solution. Adaptive Defense 360 also automates capabilities reducing the burden on IT. Adaptive Defense 360 starts with Panda's best-of-breed EPP 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