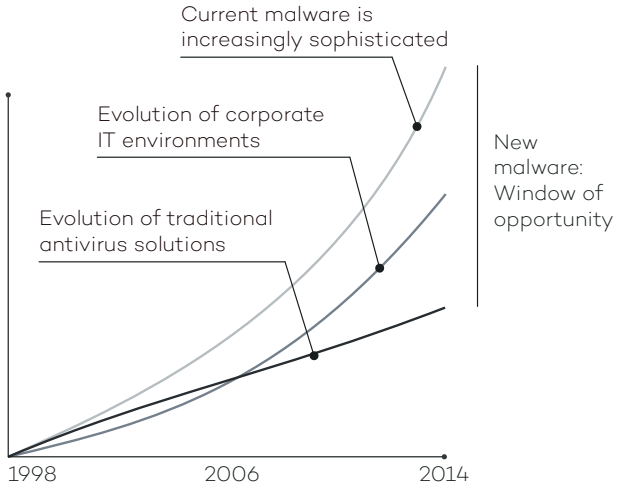
Adaptive Defense 360

Find the answers, solve the problem

COMPLETE ENDPOINT DEFENSE INTEGRATING PROTECTION, DETECTION, RESPONSE AND REMEDIATION IN A SINGLE SOLUTION

Defending your customers' endpoints 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, you needed to provide 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 your burden when managing customers' 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.



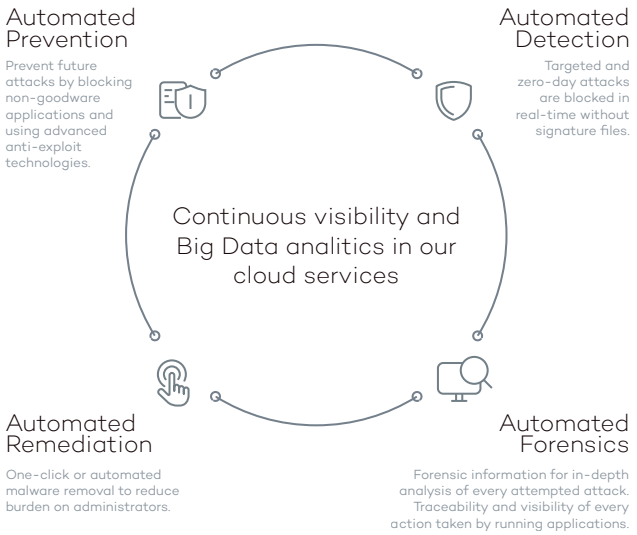
However, that is only the beginning. The malware and IT security environment has undergone major changes in terms of volume and sophistication. With over 250,000 new viruses appearing every day, and the sophistication of techniques for penetrating defenses and hiding malware, corporate networks are more 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 against zero-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** rely 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.**



CONQUER A NEW MARKET AND EXPAND YOUR BUSINESS WITH THE MOST POWERFUL SOLUTION

Benefits for you

ENHANCE YOUR VALUE ADDED SERVICES PORTFOLIO

Provide value added security services easily with minimum impact to your technical staff and maximum customer satisfaction.

Make the most of our solution to offer your customers more services like:

- Advanced forensic analysis.
- Repair against advanced threats.
- Early warning against direct attacks in the same industry or geographical area.
- Protection against information leaks.

COMPLEMENT YOUR CUSTOMERS' SECURITY WITH BEST-OF-BREED EDR SOLUTION

Take the opportunity to complement your product offering with Endpoint Detection and Response (EDR) "as a service", one of the categories with higher growth potential over the next 5 years.

Be one of the first to offer EDR services and take part of a market with an estimated growth of 250% in the coming years and 80% of penetration, up from less than 5% in 2013.

PROMOTE CUSTOMER LOYALTY AND INCREASE RENEWALS

- Proactive non-intrusive service avoids interruptions to customers' daily activities.
- Increase your customers' security and productivity and promote loyalty to service providers.
- Demonstrate the value of the service with activity reports.
- Personalize the service, adopting it to your brand image.

Benefits for your customers

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...

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.

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.

Benefits for both

SIEM INTEGRATION

Adaptive Defense 360 integrates with SIEM solutions to provide detailed data on the activity of all applications run on your customers' systems.

For clients without SIEM solution, Adaptive Defense 360 optionally includes its own system for storing and managing security events to analyze all the information collected in real time.

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 customers' network.

CONTINUOUS STATUS INFORMATION ON ALL ENDPOINTS IN THE NETWORK

Get immediate alerts the moment that malware is identified on your customers' 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.

TECHNICAL REQUIREMENTS

Web Console (only monitoring):
- Internet connection.
- Internet Explorer 7.0 or later.
- Firefox 3.0 or later.
- Google Chrome 2.0 or later.

Agent:
- Operating systems (workstations): Windows XP SP2 and later, Vista, Windows 7, 8, 8.1 & 10.
- Operating systems (servers): Windows 2003 Server, Windows 2008, Windows Server 2012.
- Internet connection (direct or through a proxy)

Partially supported (only EPP):
- Linux, MAC OS X and Android.