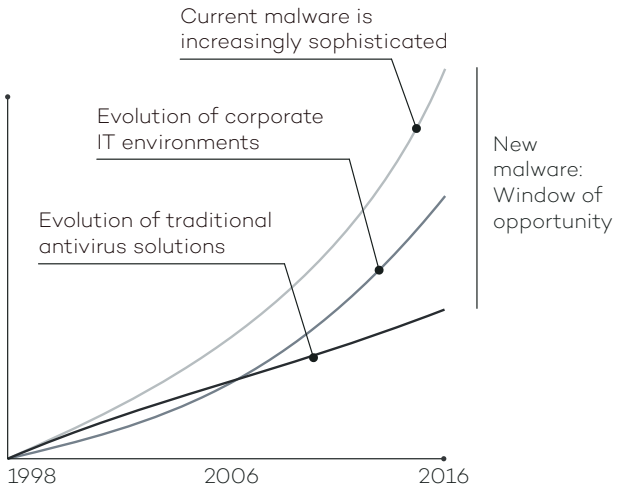
Adaptive Defense

Shut the window of opportunity to advanced threats

panda

DO YOU THINK YOUR ORGANIZATION IS PROTECTED AGAINST ZERO-DAY AND TARGETED ATTACKS?

The malware and IT security panorama has undergone a major change in terms of volume and sophistication. There has been an exponential increase in the number of viruses in circulation (around 200,000 new viruses appear every day), and new techniques for penetrating defenses and hiding malware are allowing threats to remain on corporate networks for long periods.



At the same time, IT environments have become increasingly complex, making management more difficult and systems more vulnerable.

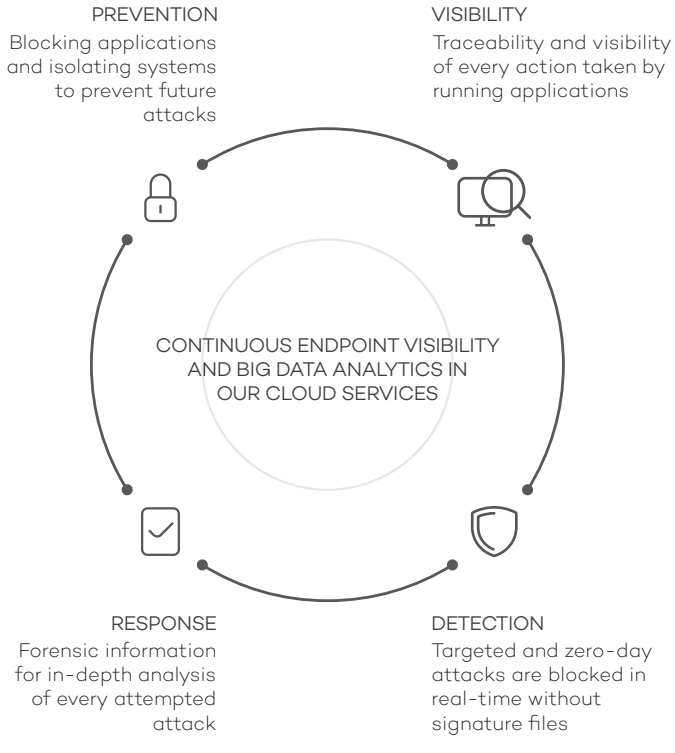
Yet traditional antivirus solutions are out of step with the reality. Their linear evolution continues to use outdated detection techniques based on signature files and heuristic algorithms. This means that the results are inaccurate, i.e., that malware can go undetected and false positives are generated.

This discrepancy has led to what has been dubbed the '**window of opportunity for malware**': the time lapse between the appearance of a new virus 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.

Governments, banks and other large companies are bearing the brunt of attacks that traditional antivirus solutions are simply not detecting in time. Our Research Department has analyzed millions of virus samples and the best antivirus products on the market to reveal that 18 percent of malware is undetected in the first 24 hours after it is released, and even after three months, these traditional solutions are still unable to detect 2 percent of malware.

The solution to this situation is **Adaptive Defense**: a Panda Security service which can accurately classify every application running in your organization, only allowing legitimate programs to run.

To achieve this, we have been working for five years on a **new 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.



THE ONLY SOLUTION TO GUARANTEE THE SECURITY OF ALL RUNNING APPLICATIONS

COMPLETE AND ROBUST PROTECTION GUARANTEED

Panda Adaptive Defense offers two operational modes:

- **Standard mode allows** all applications cataloged as goodware to be run, along with the applications that are yet to be cataloged 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 'zerorisk' approach to security.

FORENSIC INFORMATION

- **Execution event graphs** give a clear view 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.

COMPATIBLE WITH TRADITIONAL ANTIVIRUS SOLUTIONS

Adaptive Defense can coexist with traditional antivirus solutions, and take the role of a **corporate tool capable of blocking all types of malware, including targeted and zero-day attacks** that such traditional solutions are unable to detect.

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% of malware.

The vulnerability protection module in **Adaptive Defense** uses contextual and behavioral rules to ensure companies can work in a secure environment even if they have systems that are not updated.

CONTINUOUS INFORMATION ON NETWORK STATUS

- 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 integrates with SIEM solutions to provide detailed data on the activity of all applications run on your systems.

For clients without SIEM, **Adaptive Defense** includes 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** 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 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 and 10)
- Operating systems (servers): Windows 2003 Server, Windows 2008, Windows Server 2012
- Internet connection (direct or through a proxy)