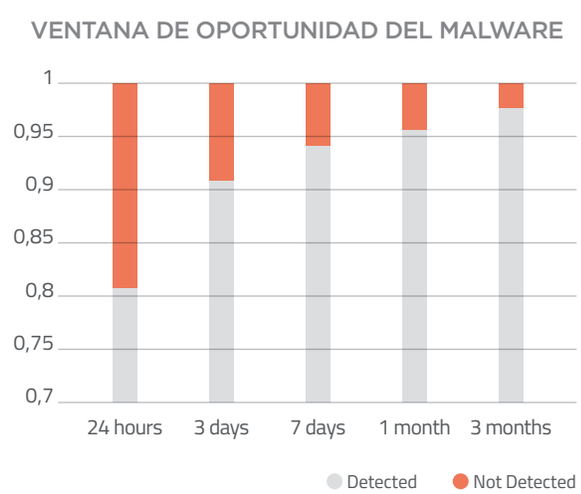
PANDA**ADVANCED**PROTECTION**SERVICE**

CLOSING THE GAP IN MALWARE DETECTION

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

Over 200,000 new malware strains are detected every day, including **a new breed of highly sophisticated targeted attacks** aimed at corporate networks and capable of staying under the radar of traditional antivirus and firewall solutions.

This next-generation malware known as **APT (Advanced Persistent Threat)** uses multiple infection vectors simultaneously over large spans of time, remaining hidden for months thanks to its polymorphic nature. This way, once they infect a network, these threats can carry out continued data theft and industrial espionage activities for long periods.

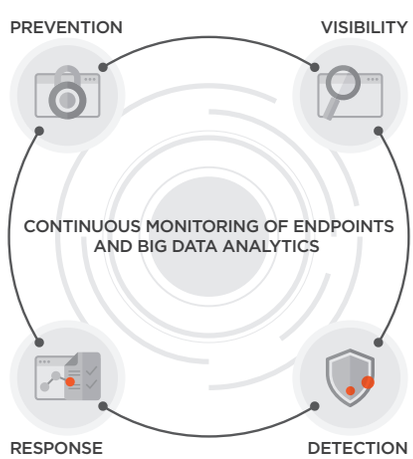


Source: Panda Research. January-June 2014 with over 10 mill. samples.

Traditional antivirus solutions are unable to detect 18% of new malware within the first 24 hours, and after three months about 2% is still not blocked.

Panda Advanced Protection Service is a new security model which ensures complete network protection by monitoring, controlling and classifying the behavior of each application running on every computer throughout the organization. This solution leverages innovative technologies to determine the precise nature of every file, **enabling the execution of legitimate applications only (goodware).**

The ability to integrate with the customer's existing infrastructure, coexisting with traditional antivirus and **SIEM** solutions, plus its virus disinfection capabilities **make Panda Advanced Protection Service the ultimate, most complete tool for protecting companies against all types of malware, including zero-day and targeted attacks.**



VISIBILITY

Provides real-time visibility into each action taken by the applications running on a system.

DETECTION

Classifies each file and process running on the network, **applying cutting-edge machine learning techniques and Big Data analytics.**

RESPONSE

Rids systems of latest-generation malware and provides forensic information to analyze each attempted attack in detail.

PREVENTION

Blocks applications and isolates systems to prevent future attacks.

PANDA**ADVANCED**PROTECTION**SERVICE**

CLOSING THE GAP IN MALWARE DETECTION

PANDA**ADVANCED**PROTECTION**SERVICE**

THE ONLY SOLUTION TO ENSURE THE SECURITY OF ALL RUNNING APPLICATIONS

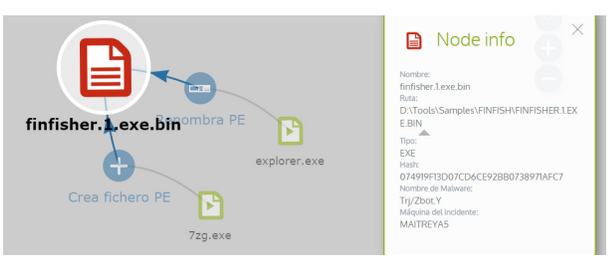
ENSURE COMPLETE NETWORK PROTECTION

In **Basic Blocking mode,** Panda Advanced Protection Service allows the execution of goodware applications as well as those applications not yet categorized by Panda Security's malware experts and automated systems. In **Extended Blocking mode,** Panda Advanced Protection Service only allows applications classified as goodware to run. The Extended Blocking feature is the perfect solution for companies looking for **zero risk** in information systems.

FORENSIC REPORTS

View **Execution graphs** on the events triggered by malware. Consult **Heat maps** with visual information about the destination of malware communications, the files created and much more. Identify software with critical vulnerabilities.

Heat maps with visual information about the destination of communitacions.



Execution gragh on the events triggered by malware.

MALWARE DISINFECTION

Remove hidden malware that traditional security solutions cannot detect

PROTECTION OF VULNERABLE SYSTEMS

Where systems are no longer supported by the manufacturer (e.g. Windows XP), and consequently no longer updated, they become a surefire target for latest generation and zero-day attacks that exploit system vulnerabilities. Protect them with our light and highly robust security solution.

CONTINUOUS MONITORING OF NETWORK STATUS

Panda Advanced Protection Service alerts you immediately if threats are detected on the network, generating a complete report with the location, the devices infected and the action taken by the malware. Receive daily reports by email detailing the service activity.

FULLY MANAGED SERVICE

Panda Advanced Protection Service requires no investment in specialized personnel to manage quarantines, suspicious files, disinfect and reinstall infected computers, etc. Panda Advanced Protection Service classifies all applications automatically by **using machine learning techniques and Big Data analytics** under constant supervision and control from specialized **PandaLabs** technicians.

SIEM MODULE

Panda Advanced Protection Service integrates with **SIEM** products (QRadar, ArcSight...), providing detailed information about the activities of all the applications running on the network.

Customers who don't have a SIEM solution can also benefit from **Panda Advanced Protection Service's** own security event storage and management system. This tool collects and analyzes network data in real time, allowing organizations to obtain graphical representations of **behavior patterns and trends** on the corporate network.

PANDA SECURITY CERTIFICATIONS

TECHNICAL REQUIREMENTS

WEB CONSOLE (for monitoring only)
- Internet connection.
- Internet Explorer 7.0 or later.
- Firefox 3.0 or later.
- Google Chrome 2.0 or later.

FOR ENDPOINTS (including file servers)
- Operating systems (workstations): Windows XP SP2 and greater (Vista, Windows 7, 8 & 8.1).
- Operating systems (servers): Windows Server 2003, Windows Server 2008, Windows Server 2012.
- Internet connection (direct or via proxy)