

Put an end to cyberthreats

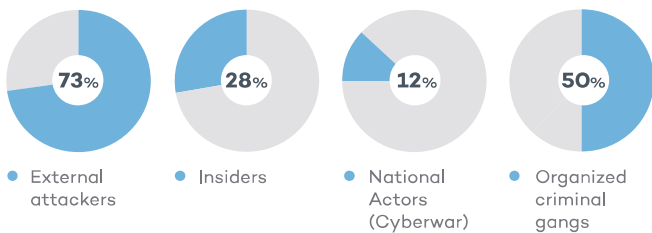
An abstract graphic on a dark blue background. It features several circular nodes connected by thin lines. One node at the top right contains an orange 'X' and has a horizontal orange line extending to the right. Another node on the left contains a green '+' and has a horizontal green line extending to the right. A third node at the bottom left contains an orange 'I' and has a horizontal orange line extending to the left. A fourth node at the bottom center contains a blue '-' and has a horizontal blue line extending to the left. A fifth node at the top center contains a white '-' and has a horizontal white line extending to the left. The lines connecting the nodes are thin and light-colored.

Panda Adaptive Defense 360

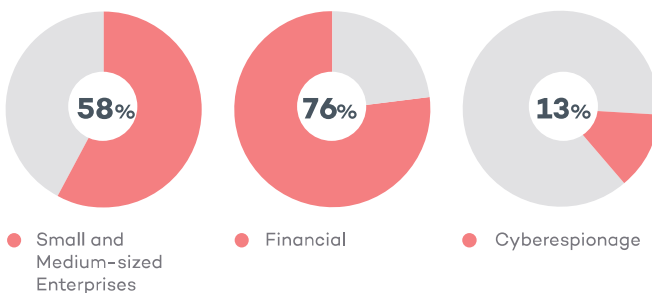
Automated and centralized *Advanced Security*

CORPORATE CYBERSECURITY

Who is behind cyberthreats?¹



Who are the victims? What are the motives?¹



Endpoints are the new perimeter

Mobility, processing and cloud storage have revolutionized corporate environments. **Endpoints are the new perimeter.** Security solutions on endpoints must be **advanced, adaptive and automatic**, with the highest levels of prevention and detection of attackers, who will sooner or later manage to evade preventive measures. Such solutions must also offer agile tools to respond quickly, minimizing damage and reducing the attack surface.

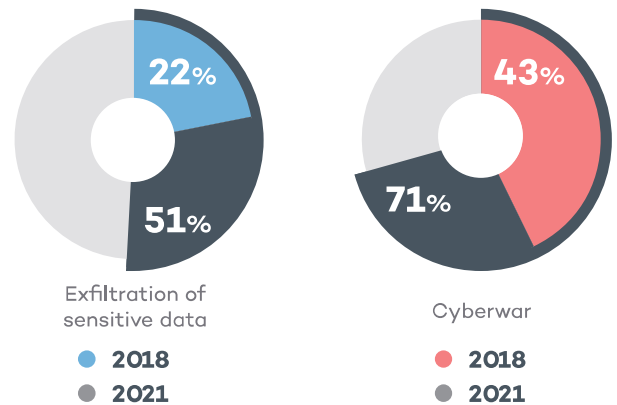
Professionalization of hackers

Enemies are increasingly sophisticated and growing in number, the result of their professionalization, the democratization of technologies and the continuous leaks of cyberintelligence.

What is the cost to companies?

- **Global cost:** \$600,000 M³
- **Cost of a Data Breach:** \$3.86 M⁴

Companies and perception of high risk⁴



In 60% of cases, national attacks lead to **cyberwar**.

Next-generation cyberthreats are designed to slip past **traditional solutions** completely undetected.

Cyberdefense in organizations

Hackers are targeting computers and servers, where the most valuable assets of organizations reside, and **security teams have great difficulties in defending them.** EDR (Endpoint Detection and Response) applications, far from being the solution, **increase workloads**, as there is no automation of threat prevention, detection, containment and response. **Improving the security posture** of your company, **without increasing operating costs** inevitably means **automating the prevention, detection and response capabilities** in endpoints.

ENDPOINT DETECTION AND RESPONSE SOLUTIONS (EDR)

EDR solutions monitor, log and store the details of endpoint activity, such as user events, processes, changes to the registry, memory and network usage. This visibility uncovers threats that would otherwise go unnoticed.

What are the hidden problems with EDR solutions?

Multiple techniques and tools are used to search for security anomalies in events and confirm or reject alerts. All of this requires human intervention.

EDR solutions require 24/7 supervision, and rapid response from highly qualified personnel.

However, such resources are expensive and hard to find. Short-staffed organizations with low budgets are unprepared to take advantage of the benefits of EDR solutions on their own. Personnel find themselves with greater workloads deriving from the implementation and operation of these solutions, instead of supporting them in what matters: improving the security posture of their organizations.

¹ "2018 Data Breach Investigation report", Verizon

² "2018 Economic Impact of Cybercrime — No Slowing Down", CSIC/McAfee

³ "2018 Cost of Data Breach Study: Global Overview", Ponemon Institute/IBM Security

⁴ "2018 study on global megatrends in cybersecurity", Ponemon Institute

🎯 Panda Adaptive Defense 360

Panda Adaptive Defense 360 is an innovative cybersecurity solution for desktops, laptops and servers, delivered from the cloud. It **automates the prevention, detection, containment and response** against any present or future advanced attacks, zero-day malware, ransomware, phishing, memory exploits and malwareless attacks, inside and outside the corporate network.

It differs from other solutions in that it combines the widest range of **protection technologies (EPP) with automated EDR capabilities**, thanks to two services **managed by Panda Security experts**, and delivered as features of the solution:

- **100% attestation Service.**
- **Threat Hunting and Investigation Service (THIS).**

Thanks to its cloud architecture, the **agent is light** and does not impact the performance of endpoints, which are managed through a **single cloud console**, even when not connected to the Internet.

Panda Adaptive Defense 360 integrates **Cloud Protection and Management Platforms (Aether)**, which maximize prevention, detection and automated response, minimizing the effort required.

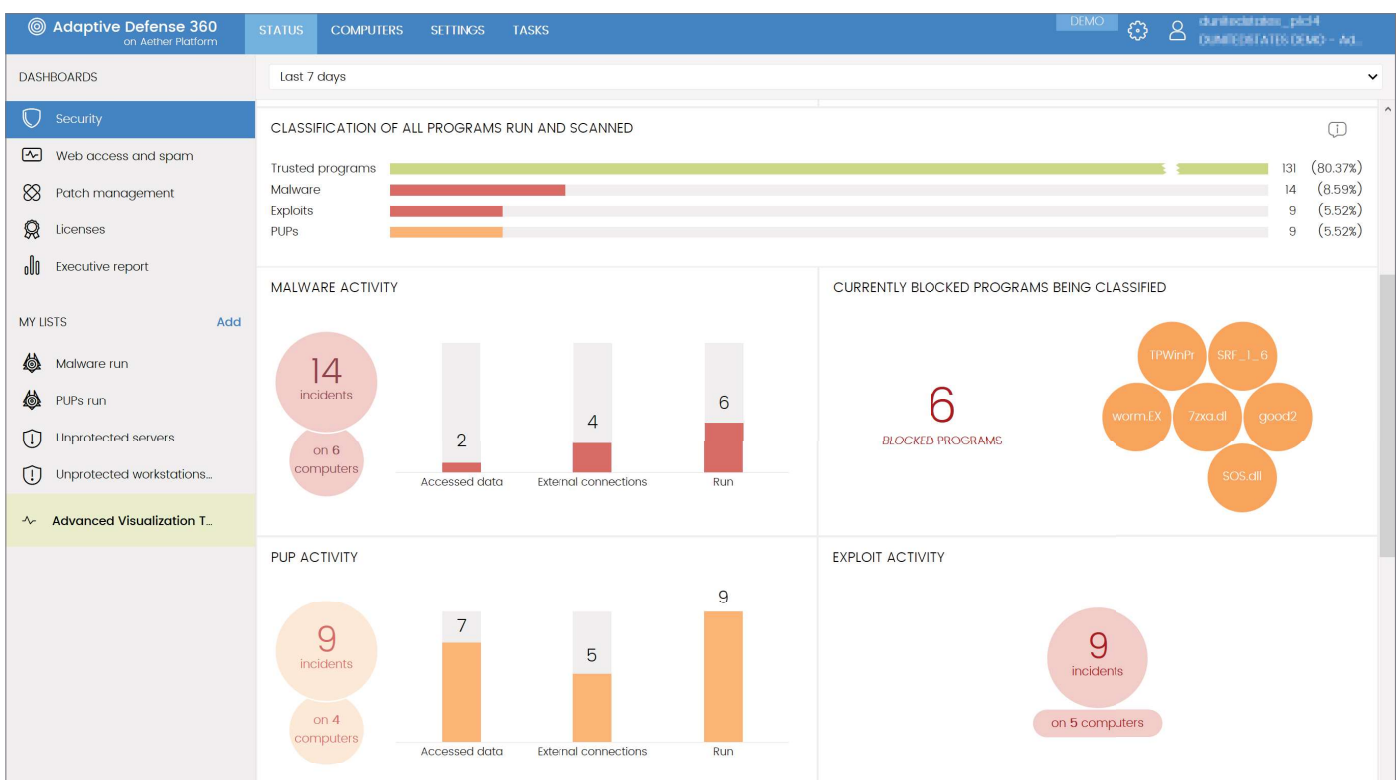


Figure 1: A single dashboard provides a global vision and consolidated management prioritizing detected threats

BENEFITS

🎯 Panda Adaptive Defense 360

Simplifies and minimizes the cost of advanced and adaptive security

- Its managed services reduce the cost of expert personnel. There are no false alarms, no responsibility is delegated.
- The managed services learn automatically from the threats. No time is wasted with manual settings.
- Maximum prevention on endpoints. Operating costs are reduced practically to zero.
- There is no management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted as it is based on a lightweight agent and cloud architecture.

Automates and reduces detection and exposure time (Dwell Time)

- Prevents the running of threats, zero-day malware, ransomware and phishing.
- Detects and blocks malicious activity in memory (exploits), before it can cause damage.
- Detects malicious processes that slip past preventive measures.
- Detects and blocks hacking techniques and procedures.

Automates and reduces response and investigation time

- Automatic and transparent remediation.
- Recovery of endpoint activity – immediate recovery of normal activity.
- Actionable insights into attackers and their activity, speeding up forensic investigation.
- Helps reduce the attack surface. Supports improvement to security posture and maturity.

CLOUD ADAPTIVE PROTECTION PLATFORM

Humans and Machines Leading Advanced and Adaptive Security.

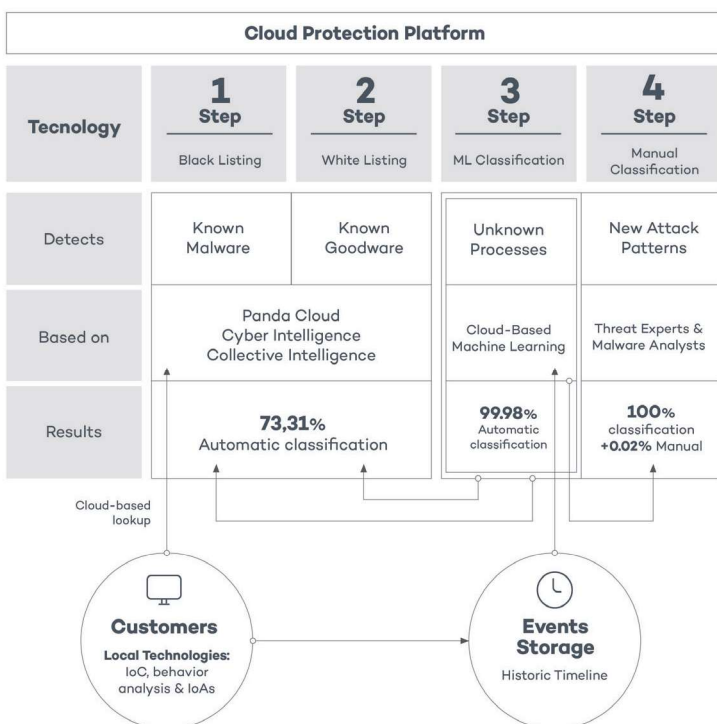
100% ATTESTATION SERVICE

The **100% Attestation Service** monitors and prevents the execution of malicious applications and processes on endpoints. For each execution, it issues a real-time **classification, malicious or legitimate, with no uncertainty**, and without delegating to the client. All this is possible thanks to the speed, capacity, flexibility and scalability of AI and cloud processing.

The service combines **Big Data** and multi-level **Machine Learning**, including **Deep Learning**, the result of the continuous supervision and automation of **the experience, intelligence and accumulated knowledge of experts** in security and threats at Panda Security's Intelligence center.

The 100% Attestation Service is able, like no other solution on the market, to free companies from the risk of running malware on endpoints inside and outside the corporate network.

Figure 2: Workflow of the managed cloud classification service



THREAT HUNTING & INVESTIGATION MANAGED SERVICE

There will be always threats that bypass the deployed security controls

Threat Hunting is the process to discover new, advanced threats and their TTPs*, beyond what the current Threat Detection systems can do before they cause serious damage to the organization.

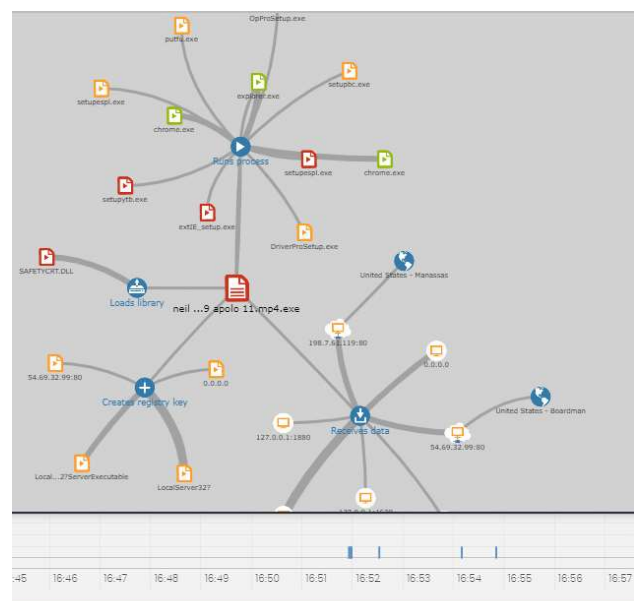
Threat hunters operate on the premise that organizations are in a **continuous state of compromise**.

Among others, its **benefits** are:

- Create new Threat Detections.
- Improve the Incident Response.
- Reduce the Attack surface.

Panda Security **Threat Hunting and Investigation** managed service is operated by highly skilled cyber-security experts, armed with profiling, analysis and events correlation in real-time and retrospectively tools, discover new hacking and evasion techniques.

Figure 3: The Panda Adaptive Defense 360 console incident timeline enables forensic investigation: the date it was first seen on the network, names and number of endpoints affected, settings changes and with whom it has communicated.



* TTPs: Tactics, techniques and procedures used by hackers

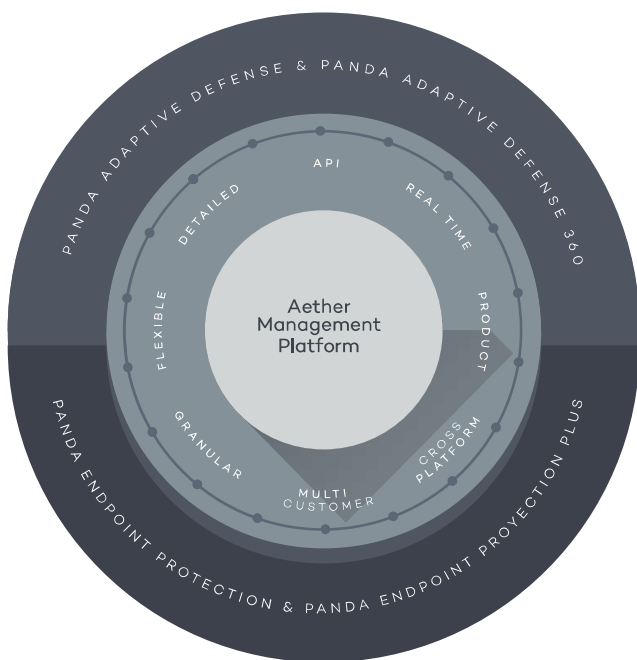
CLOUD MANAGEMENT PLATFORM: AETHER

Next-generation security, visibility and control. Comprehensive and scalable from the cloud, to deliver value immediately

The Aether platform and its cloud console, common to all Panda Security endpoint solutions, optimize the management of advanced and adaptive security inside and outside the network.

Designed so that security teams focus solely on managing the cybersecurity posture of the organization, it minimizes complexity and maximizes flexibility, granularity and scalability.

Figure 3: Unified cloud management platform: Aether



BENEFITS OF AETHER IN

🎯 Panda Adaptive Defense 360

Generates greater value in less time. Simple to implement – immediate visibility

- Deployment, installation and configuration in minutes. See the value from day one.
- Lightweight multi-product and multi-module Panda agent. Cross-platform (Windows, Mac, Linux, Android).
- Automatic discovery of unprotected endpoints. Remote installation.
- Proprietary proxy technology, even on computers with no Web connection.
- Traffic optimization, with proprietary repository/ cache technology.

Easy to use, adapting to your organization

- Intuitive Web console. Flexible and modular management.
- Predefined and custom roles.
- Detailed audit of actions in the console.
- Users with total or restricted permissions and visibility.
- Security policies for groups and endpoints.
- Hardware and software inventories and change log.

Facilitates monitoring. Accelerates response

- Prioritized key indicators and dashboards.
- Prioritized and confirmed alerts in your workflow.
- Complete and actionable history of incidents: processes involved, source, dwell time, prevalence, etc.
- Act on endpoints with a single click: restart, isolate, patch and scan, accelerating the response.

ADVANCED AUTOMATED SECURITY ON ENDPOINTS

Panda Adaptive Defense 360 integrates, in a single solution, traditional preventive technologies with innovative technologies for prevention, detection and automated response against advanced cyberthreats.

Traditional preventive technologies

- Personal or managed firewall. IDS.
- Device control.
- multivector permanent antimalware and on-demand scan.
- Managed blacklisting/whitelisting. Collective intelligence.
- Pre-execution Heuristics.
- Web access control.
- Antispam & Antiphishing.
- Anti-tampering.
- Mail content filter.
- Remediation and rollback.

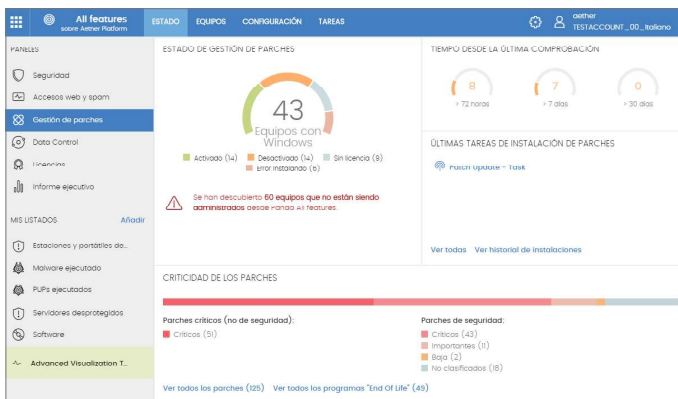
Advanced security technologies

- EDR: continuous monitoring on endpoints activity.
- Prevention of execution of unknown processes.
- Cloud-based Machine Learning of behavior to classify 100% unknown processes (APTs, ransomware, Rootkits, etc.)
- Cloud-based Sandboxing in real environments.
- Behavioral analysis and IoA detection (scripts, macros, etc.).
- Automatic detection and response to memory exploits.
- Managed Threat Hunting for malwareless attacks.

OPTIONAL MODULES

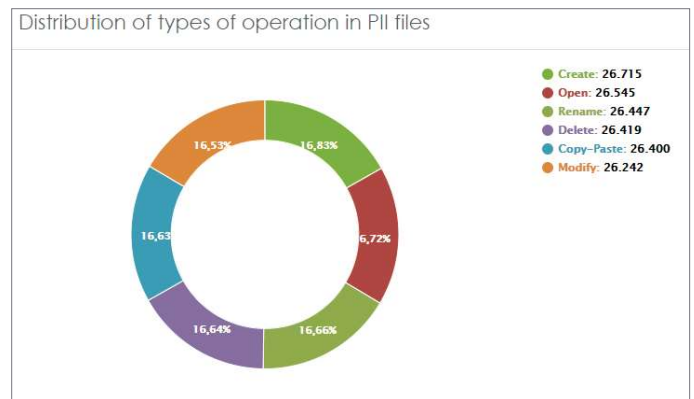
Panda Patch Management

Panda Patch Management is an intuitive solution for managing vulnerabilities in operating systems and third-party applications on Windows endpoints and servers. The result is a reduced attack surface, strengthening preventive capabilities and incident containment.



Panda Data Control

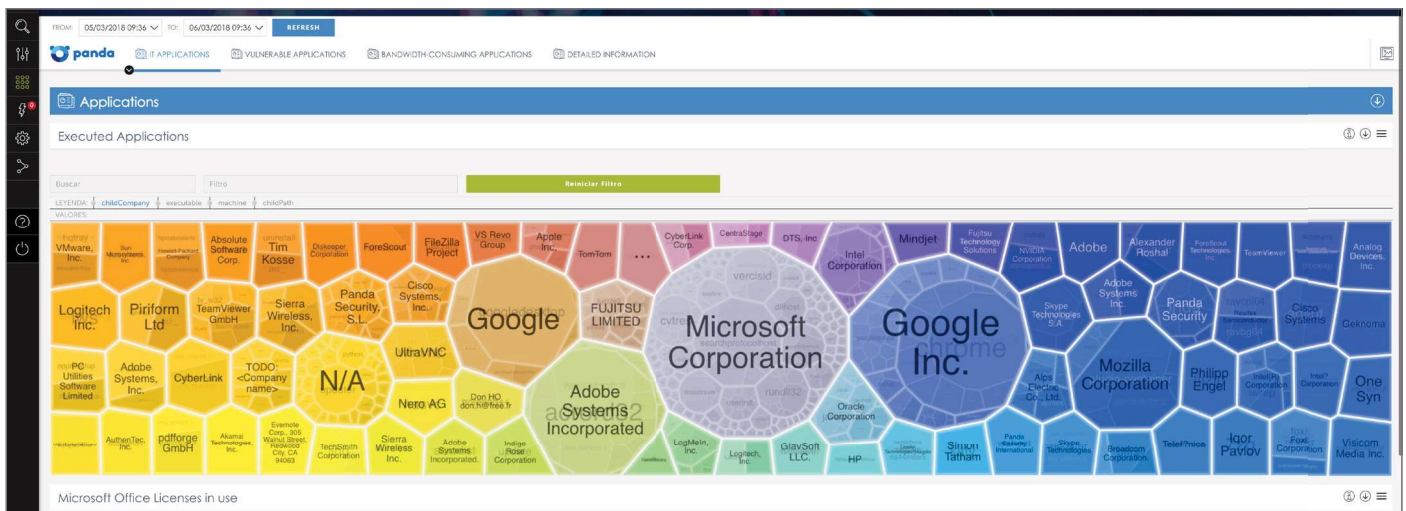
Panda Data Control discovers, audits and monitors unstructured sensitive or personal data on endpoints: from data at rest to data in use and data in motion.



Panda Advanced Reporting Tool

Reporting platform automates the correlation of the information generated by the execution of processes and applications on protected endpoints and their context, which Panda Adaptive Defense 360 collects and enriches in the Cloud Protection Platform.

Panda Advanced Reporting Tool automatically generates intelligence on organization activity and enables the searching, correlation and configuration of alerts regarding events.



The **SIEMFeeder** module sends to organizations, in real time, the events collected on endpoints and enriched with security intelligence in the Cloud Protection Platform so it can be integrated in the corporate SIEM.

Find out more at: www.pandasecurity.com/business/solutions

AWARDS AND CERTIFICATIONS

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, NSS Labs.

Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.

Panda Security acknowledged as 'Visionary' in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2018. <https://www.pandasecurity.com/gartner-magic-quadrant/>



Gartner



ITPRO
IT ANALYSIS. BUSINESS INSIGHT.



AV-Comparatives endorses Adaptive Defense 360
“As this solution classifies all executed processes, it cannot fail to record any malware”



“Foresight is our greatest ally when it comes to defining our future needs and preventing risks. Adaptive Defense 360 gives us the visibility we need to achieve this foresight.”

Jean-Yves Andreoletti

Systems and Networks Integration,
Validation and Maintenance Platform
Engineer

Operating systems supported on endpoints

Windows workstations: XP SP3 or later

Windows servers: Server 2003 (32/64-bit and R2) SP2 or later

MacOS workstations and servers: macOS 10.10 Yosemite or later

Linux workstations and servers: Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS and 16.10. Fedora 23, 24 and 25.

Contact your Panda Security sales representative or partner for details of other supported distributions.

Android: Version 4 or later

Platform certifications: ISO27001, SAS 70

