

Every day, over 350,000 new malicious programs (malware) and potentially unwanted applications (PUA) are registered.¹ Hackers are targeting vulnerable endpoints, where enterprises store their most valuable assets. The reason? As is so often the case, **for economic gain**.

Enterprises are increasingly dependent of new technologies, and are thus **exposed** to new kinds of malware that **endanger** their security. This, of course, requires security approaches that **reduce the attack surface**.

EVOLUTION OF ENTERPRISE IT ENVIRONMENTS

Over the last few years, the evolution of technology, along with the widespread use of the Internet, mobile devices, and Cloud-based storage and apps, have all led to a real revolution in the corporate environment. This revolution, however, isn't without risks. While these advantages are a boost for enterprises, these same advantages are also leveraged by cyber criminals.

The increase in the number of cyber attacks is down to the increased value of the digital assets stored by companies. This also means that cyber criminals see a potential for themselves to increase their economic returns. Malware and ransomware have become some of the most prevalent threats, although paradoxically, the direct costs are not the main problem — rather, it is the downtime they cause. This is forcing enterprises to adopt measures to improve their security posture.

PROTECT YOUR COMPANY AGAINST MALWARE AND RANSOMWARE

Panda Endpoint Protection Plus is a complete, advanced security solution for desktops, laptops and servers. It centrally manages the security of endpoints both inside and outside the corporate network.

This service provides a set of EPP technologies to control malware, ransomware and threats that leverage unknown (zero day) vulnerabilities. There is no need to install or maintain new hardware resources on the enterprise's infrastructure.

Moreover, the lightweight agent has no impact on endpoint performance and is accessible via a single web console, simplifying security management and increasing operational efficiency.

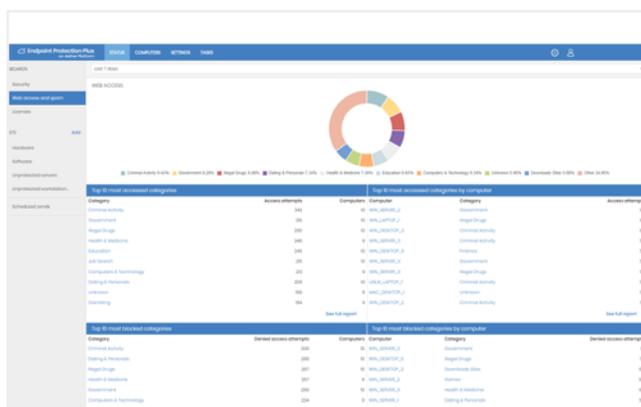


Figure 1: Web access and Spam dashboard.

BENEFITS

Multi-Platform Security

- Security against unknown advanced threats: detects and blocks malware, trojans, phishing and ransomware.
- Security for all attack vectors: browsers, email, file systems, and external devices connected to endpoints.
- Automatic analysis and disinfection of computers. Behavioral analysis to detect known and unknown malware.
- Security for Windows systems, Linux, macOS, Android and virtual environments (VMware, Virtual PC, MS Hyper-V, Citrix) — as well as for both persistent and non-persistent virtualization infrastructure (VDI).

Increased Productivity

- Panda Endpoint Protection Plus provides anti-spam protection for Exchange servers in order to improve user productivity and increase the security of all computers on the network.
- It monitors and filters web traffic, preventing employees from engaging in unproductive behaviors or falling victim to security threats such as bots or phishing.
- No specific infrastructure or maintenance is required; the IT department can focus on more important tasks.

Simplify Management

- Easy to maintain: no specific infrastructure required to host the solution; the IT department can focus on more important tasks.
- Easy to protect remote users: each computer protected with Panda Endpoint Protection Plus communicates with the Cloud; remote users and offices are protected quickly and easily, with no additional installations.
- Easy to deploy: multiple deployment methods, with automatic uninstallers for competitors' products to facilitate rapid migration from third-party solutions.

CENTRALIZED ENDPOINT SECURITY

Includes centralized management of security and product updates for all workstations and servers on the corporate network. Manage the protection of Windows, Linux, macOS and Android devices from a single web-based administration console.

¹ AV-Test: <https://www.av-test.org/en/statistics/malware/>

MALWARE AND RANSOMWARE PROTECTION

Panda Endpoint Protection Plus analyzes behaviors and hacking techniques to detect and block both known and unknown malware, as well as ransomware, trojans and phishing. Moreover, Malware Freezer freezes detected malware for seven days and, in the event of a false positive, automatically restores the affected file to the system.

ADVANCED DISINFECTION

In the event of a security breach, Panda Endpoint Protection Plus allows enterprises to quickly restore affected computers to the state they were in before the infection with advanced disinfection tools and quarantine, which stores suspicious and deleted items. It also allows administrators to remotely restart workstations and servers to ensure they have the latest product updates installed.

MONITORING AND WEB FILTERING

Detailed, real-time network security monitoring via comprehensive dashboards and easy-to-interpret graphs.

Web filtering increases productivity in the company, and monitors activity to prevent access to dangerous or unproductive URLs.

SPAM, VIRUS AND CONTENT FILTERING

Panda Endpoint Protection Plus scans Exchange servers for viruses, hacking tools, and potentially unwanted programs. It increases user productivity and security, blocking spam, and malicious emails and scams.

CENTRALIZED DEVICE CONTROL

Stop malware and information leaks by blocking entire device categories (flash drives, USB modems, webcams, DVD/CD, etc), whitelisting devices or configuring read-only, write-only, and read-and-write access permissions, and blocking any activities that could be considered a risk.

FAST, FLEXIBLE INSTALLATION

Deploy the protection via email with a download URL, or silently to selected endpoints via the solution's distribution tool. MSI installer compatible with third-party tools (Active Directory, Tivoli, SMS, etc).

ISO 27001 AND SAS 70 COMPLIANT GUARANTEED 24/7 AVAILABILITY

Solution is hosted on Aether, the platform with complete data protection guaranteed. Our data centers are ISO 27001 and SAS 70 certified, allowing customers to avoid costly service outages and malware infections.

CLOUD MANAGEMENT PLATFORM

Aether Platform

The Cloud platform Aether and its management console, shared by all of Panda Security's endpoint solutions, optimize the management of advanced, adaptive security, both inside and outside the network. Designed for minimum complexity and maximum flexibility, granularity and scalability.

Achieve More In Less Time. Easy Implementation

- Deployment, installation and configuration in minutes. Maximum value from day one.
- Single lightweight agent for all products and all systems (Windows, macOS, Linux and Android).
- Automatic discovery of unprotected endpoints. Remote installation.
- Proprietary proxy and repository/cache technologies. Optimized communication, even with endpoints with no Internet connection.

Simplified Operations Adapts To Your Organization

- Intuitive web console. Flexible, modular management that reduces total cost of ownership.
- Users with full or restricted permissions and visibility. Activity audits.
- Security policies by endpoints and by groups. Predefined or custom roles.
- Hardware and software inventory, and changelog.

Easy Implementation of Security and Management Capacities Over Time

- No new infrastructure needed to deploy modules. No deployment costs.
- Communication with endpoints in real time from single web management console.
- Detailed reports, dashboards and indicators for each module.

Compatible solutions on Aether platform:

 Panda Endpoint Protection  Panda Endpoint Protection

Windows workstations and servers:
<http://go.pandasecurity.com/endpoint-windows/requirements>

macOS devices:
<http://go.pandasecurity.com/endpoint-macos/requirements>

Linux workstations and servers:
<http://go.pandasecurity.com/endpoint-linux/requirements>

Android mobile devices:
<http://go.pandasecurity.com/endpoint-android/requirements>