Panda Endpoint Protection

Endpoint security is evolving

panda
a WatchGuard brand

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.

In fact, in 2020 **over 350,000 new malicious programs** are being registered[1] every day. Hackers are targeting vulnerable endpoints, where enterprises store their **most valuable assets**. The reason? As is so often the case, for economic gain. **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

The increasing exposure of companies to new types of malware and threats endangers their security posture, requiring new approaches to help reduce the impact of possible attacks.

Panda Endpoint Protection is an effective Cloud-native security solution for desktops, laptops and servers. It centrally manages the security of endpoints, both inside and outside the corporate network.

It includes a set of EPP technologies to prevent malware, ransomware and the latest threats. One of these technologies checks in real time the Panda Threat Intelligence, a huge repository being fed by the latest machine-learning algorithms, to detect malicious attacks faster.

Moreover, there is no need to maintain hardware and software. Its lightweight agent has no impact on endpoint performance, simplifying security management and increasing operational efficiency.

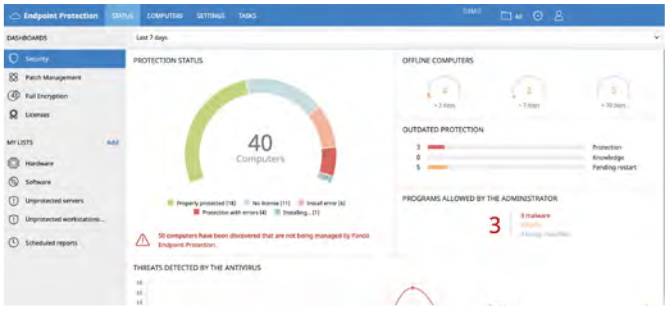

Figure 1: Network protection status dashboard.

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.
- Cross-platform security: Windows systems, Linux, macOS, iOS, Android and virtual environments (VMware, Virtual PC. MS Hyper-V, Citrix). Management of licenses belonging to both persistent and non-persistent virtualization infrastructure (VDI).

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 communicates with the Cloud; remote offices and users 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.
- Smooth learning curve: intuitive, simple web-based management interface, with most-frequent options one click away.

Lower Impact On Performance

- The agent has minimal network, memory and CPU usage, since all operations are performed in the Cloud.
- Panda Endpoint Protection requires no installation, management or maintenance of new hardware resources in the organization's infrastructure.

[1] **AV-Test**: https://www.av-test.org/en/statistics/malware/

panda
a WatchGuard brand

CENTRALIZED DEVICE SECURITY

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

MALWARE AND RANSOMWARE PROTECTION

Panda Endpoint Protection analyzes behaviors and hacking techniques to detect and blocks both known and unknown malware, as well as ransomware, trojans and phishing.

ADVANCED DISINFECTION

In the event of a security breach, Panda Endpoint Protection allows enterprises to quickly restore affected computers to the state they were in before the infection with advanced disinfection tools and quarantine, which store suspicious and deleted items.

It also allows administrators to remotely restart workstations and servers to ensure they have the latest product updates installed.

REAL-TIME MONITORING AND REPORTS

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

Reports are automatically generated and delivered on protection status, detections and improper use of devices.

GRANULAR CONFIGURATION OF PROFILES

Assign specific protection policies by user profiles, guaranteeing the application of the most appropriate policy for every group of users.

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.

FAST, FLEXIBLE INSTALLATION

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

MALWARE FREEZER

Malware Freezer quarantines detected malware for seven days and, in the event of a false positive, automatically restores the affected file to the system.

ISO 27001 AND SAS 70 COMPLIANT GUARANTEED 24/7 AVAILABILITY

Solution is hosted on Aether 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.

RANSOMWARE REMEDIATION & RECOVERY

To prevent the recovery of a corrupted system, apart from encrypting files, adversaries try to delete backup and VSS files created by admins and turn off services designed to help recovery.

The shadow copies feature leverages the operating system technology, and it will protect these files using our anti-tampering technology so users will be able to recover the information after a ransomware attack.

IT professionals use shadow copies to recover files from critical system failures, but it is also an excellent technology for recovering files encrypted by ransomware.

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

iOS devices:
https://www.pandasecurity.com/support/card?id=700123

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com