Endpoint Protection Plus

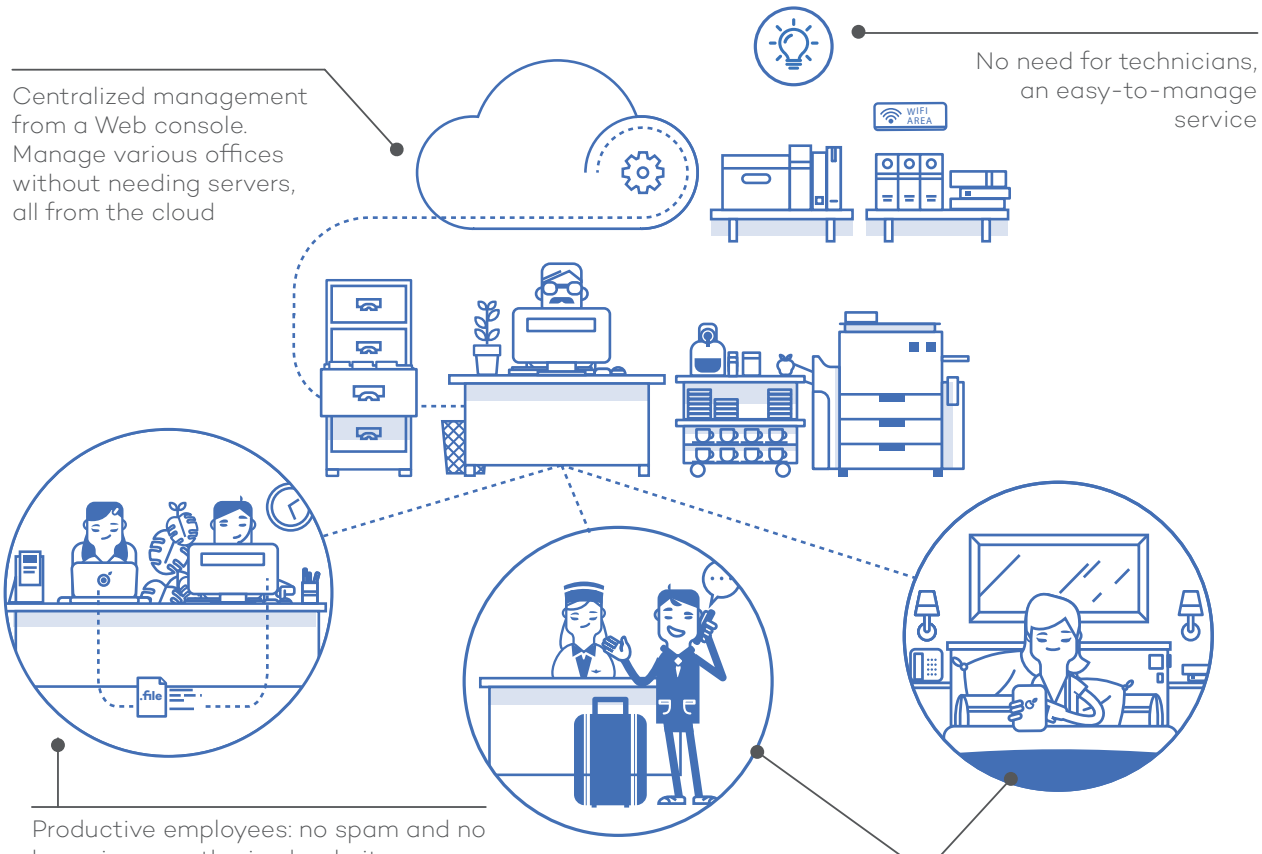
Simple and light endpoint security and productivity solution

MANAGE THE SECURITY OF ALL THE COMPUTERS IN YOUR NETWORK AND CONTROL USER PRODUCTIVITY AT THE LOWEST POSSIBLE COST OF OWNERSHIP

Panda Security presents its simple and light endpoint security and productivity solution. **Endpoint Protection Plus** provides centralized and uninterrupted protection for all of your Windows, Mac and Linux workstations, including laptops, servers and Exchange, in addition to the leading virtualization systems and Android devices.

Panda Security's Collective Intelligence technology protects all workstations and servers against threats and exploits that use unknown zero-day vulnerabilities in real time, without needing to install additional servers or IT infrastructures. It also monitors and filters Web traffic and spam, allowing the company to focus on its business and forget about unproductive employee behavior.

With **Endpoint Protection**, the protection is managed conveniently and easily from a single Web console, permitting centralized administration anytime and anywhere, without needing technical knowledge.



Simple and centralized security for all devices

Centralized management of security and product upgrades through a simple Web browser for all network workstations and servers. Manage your Windows, Linux, Exchange Server, Mac OS X or Android protection from a single administration console.

Android Anti-Theft

Secure organisation information on Android with Remote Locate, Lock and Wipe functions for mislaid or misappropriated devices.

Remedial actions

Run Cleaner Monitor remotely and repair workstations infected with advanced or non-conventional malware.

Remotely reboot servers and workstations to ensure the latest product updates are installed.

Real-time monitoring and reports

Detailed monitoring of your IT infrastructure in real-time thanks to comprehensive and intuitive dashboards.

Reports can be generated and sent automatically, detailing the protection status, detections and inappropriate use of resources.

Profile-based protection

Assign profile-based protection policies, ensuring the most appropriate policies are applied to each group of users.

Centralized device control

Prevent malware entry and data loss by blocking device types (USB keys and modems, webcams, DVD/CD drives, etc.), whitelisting specific devices and preventing dangerous actions (access, read, write)..

Web monitoring and Filtering

Increase user productivity by preventing and/or monitoring access to content belonging to categories considered dangerous or unproductive during working hours, regardless of the type of browser used.

No more saturated mailboxes

Reduce the risk of attacks on your Exchange servers with the content filter feature. Improve end-user productivity and protection by filtering unwanted and malicious messages with the anti-malware and anti-spam engines.

Malware Freezer

Do not get burnt by false positives again. Malware Freezer freezes detected malware for seven days just in case there is a false positive, in which case the file is automatically restored to the system.

ISO 27001 and SAS 70 compliant. Guaranteed 24x7 availability

The solution is hosted on Microsoft Azure with complete data protection guaranteed. Our data centers are ISO 27001 and SAS 70 certified.

TECHNICAL REQUIREMENTS

Web Console

- Internet connection.
- Internet Explorer.
- Firefox 3.0.
- Google Chrome.

For workstations / file servers

- At least one with an Internet connection.
- Operating systems (workstations): Windows 2000 Professional, XP SP0, SP1 SP2 and later, Vista, 7, 8 & 8.1.
- Operating systems (servers): Windows 2000 Server, Home Server, 2003 (32, 64 bits and R2) SP1 and greater, 2008 (32 and 64 bits), 2008 R2 (64 bits), Small Business Server 2011, Server 2012 (64 bit and R2).

For Exchange server

- Microsoft Exchange Server 2003, 2007, 2010 y 2013

For MAC workstations / file servers

- Mac OS X 10.6 Snow leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite

For Linux workstations / file servers

- Ubuntu 12 32/64 bits and later
- Red Hat Enterprise Linux 6.0 64 bits and later
- CentOS 6.0 64 bits and later
- Debian 6.9 Squeeze and later
- OpenSuse 12 32/64 bits and later
- Suse Enterprise Server 11SP2 64 bits and later

For Android devices

- Android (from 2.3)

Virtual engine certified

- VMWare ESX 3.x,4.x, 5,x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x y 9.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008 R2 y 2012 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer and XenApp 5.x & 6.x

Compatible with:

Certifications: