Endpoint Protection

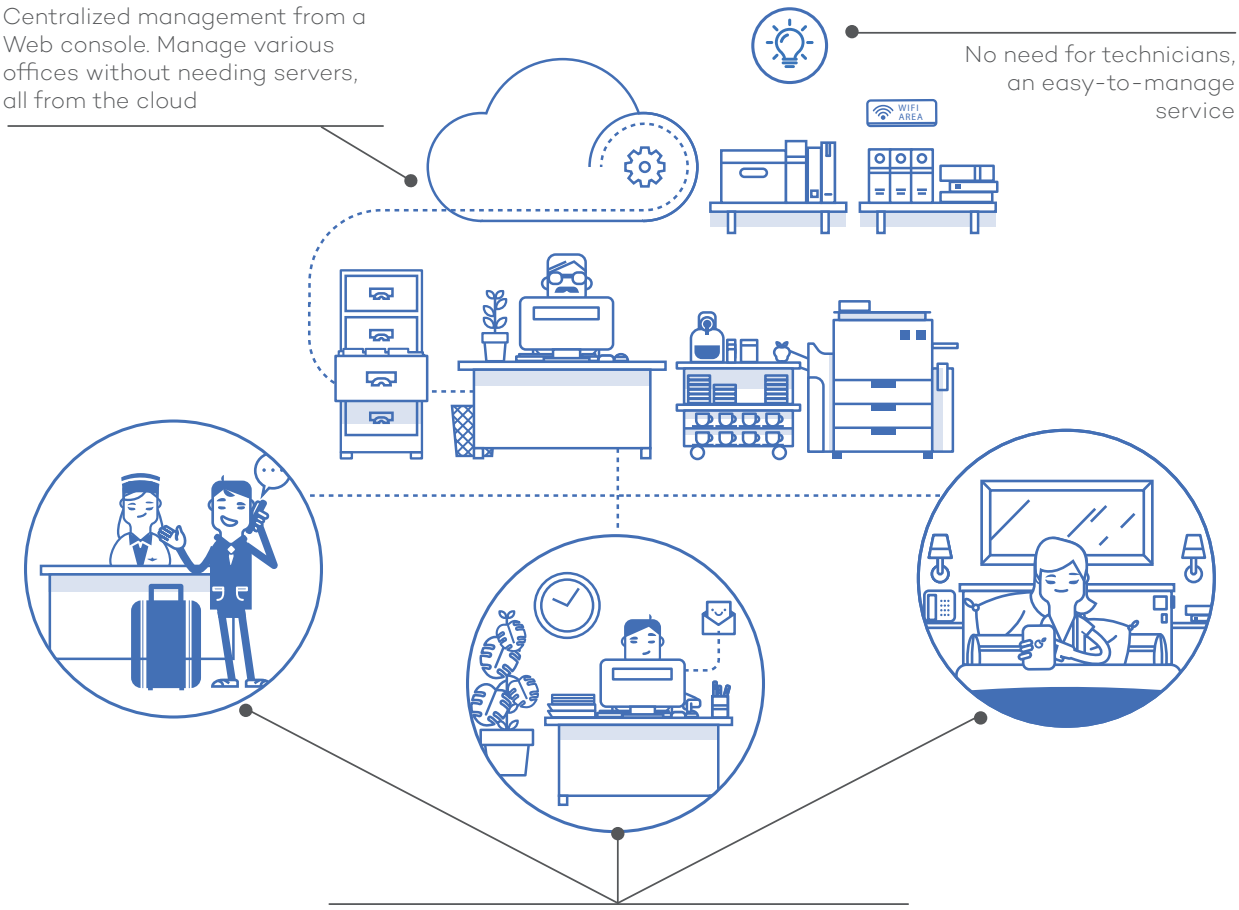
Simple and light endpoint security solution

MANAGE THE SECURITY OF ALL THE COMPUTERS IN YOUR NETWORK WITHOUT AFFECTING PERFORMANCE AND AT THE LOWEST POSSIBLE COST OF OWNERSHIP

Panda Security presents its simple and light endpoint security solution. **Endpoint Protection** provides centralized and uninterrupted protection for all of your Windows, Mac and Linux workstations, including laptops and servers, 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.

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, Mac OS X or Android protection from a single administration console.

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

Block devices (USB drives and modems, webcams, DVD/CD, etc.) or establish the actions allowed (access, blocking, read, write) to prevent malware from entering or data leakages.

Flexible, rapid installation

There are several ways to deploy the protection: emails with a download link or transparently to selected endpoints using the solution's own distribution tool. MSI installer compatible with third party tools (Active Directory, Tivoli, SMS, etc.).

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 10
- Microsoft Edge
- Firefox (latest version)
- Google Chrome (latest version)

For workstations / file servers

- At least one with an Internet connection.
- Workstation operating systems supported: XP SP2 and later, Windows Vista, Windows 7, Windows 8 (32 and 64-bit), Windows 8.1 (32 and 64-bit) and Windows 10 (32 and 64-bit).
- Server operating systems supported: Windows 2003 (32, 64-bit and R2) SP1 and greater, Windows 2008 (32 and 64-bit), Windows 2008 R2, Windows Small Business Server 2011, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

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
- Mac OS X 10.11 El Capitan
- macOS Sierra

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 4.0)

Virtual engine certified

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

Compatible with: