



PANDA CLOUD OFFICE PROTECTION

Simply... Evolution



If you thought that protecting your computers required extensive technical knowledge, think again.

We offer you a cross-platform security solution which is easy to install and manage, and requires no new infrastructure.

Panda Cloud Office Protection is a complete, easy-to-use solution that **provides continuous, real-time protection for Windows, Mac and Linux** as well as the most popular virtualization systems.

Panda Security's Collective Intelligence protects all workstations and servers in real-time **against malware and threats that exploit unknown (zero-day) vulnerabilities**: companies can focus on their business and forget about the costs of operating traditional solutions.

With **Panda Cloud Office Protection** the protection is centrally managed simply and conveniently from **a single Web console, at any time and from anywhere**.



PANDA CLOUD OFFICE PROTECTION is an ultra-light solution: all processes take place in the cloud and clients need no additional resources, minimizing the investment required.



PANDA CLOUD OFFICE PROTECTION offers immediate and effective protection against known and unknown (zero-day) threats and spam, thanks to real-time cloud connectivity.



PANDA CLOUD OFFICE PROTECTION is incredibly easy to use. All the information needed to protect PCs, servers and workstations is available through the solution's Web console.

Main benefits

- Ⓞ **Robust cross-platform protection**
Enjoy proactive, real-time protection from the cloud, with maximum levels of protection against malware and zero-day exploits, personal and managed firewall protection and behavioral detection technologies.

A single solution that provides centralized control from the cloud for Windows, Mac and Linux and is optimized for VMWare, Microsoft and Citrix virtualized environments.
- Ⓞ **Easy to use, easy to maintain**
Panda Cloud Office Protection can be installed and administered at any time, from anywhere transparently to end users. Inform us of any questions or incidents, quickly and easily with the integrated tickets tool.
- Ⓞ **Maximizes security control**
Configure detailed protection settings for each working group, centrally monitoring the precise security status across the entire network through comprehensive and intuitive dashboards.

Launch remedial action remotely and on-demand for any computers with security problems.
- Ⓞ **Minimizes maintenance costs and resource consumption**
Cloud-hosted service leveraging specific technologies to reduce resource and bandwidth consumption. No investment is required in infrastructure or specialized personnel.

*More than **100,000 companies** and **more than 2 million endpoints** stay **protected 24 hours a day** with Panda Cloud Office Protection*

*Every day, our anti-exploit technologies detect more than **100 new malware strains** unknown to our competitors*

*Cloud-based security without interruption: **Server redundancy, 99.9% availability** in 2013*



VB100
Certified 2013.

Simple management through a hosted Web console

Centrally manage the antivirus and firewall protection of your Windows, Mac and Linux workstations, even those in distributed offices or mobile machines, from any Web browser.

Remedial actions

Resolve any security issues remotely by launching **Panda Cloud Cleaner Monitor** on-demand to repair any systems infected by advanced, non-conventional malware.

Remotely reboot servers and workstations to ensure all 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

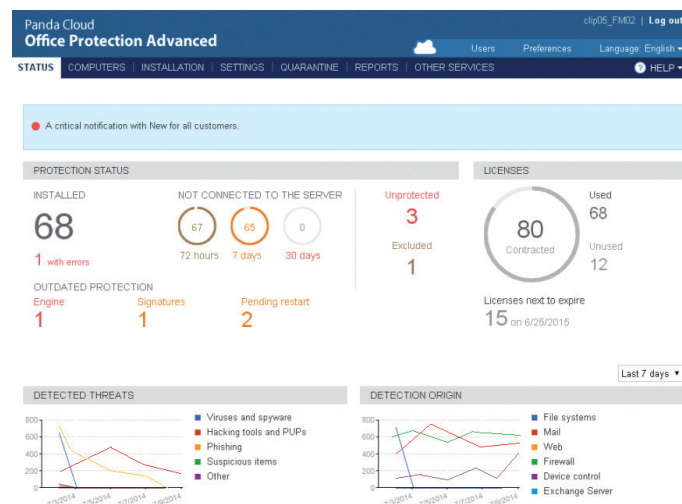
There are several ways to deploy the protection: emails with a download link or transparently to selected endpoints using the solution's own distribution tool. MSI installer compatible with third party tools (Active Directory, Tivoli, SMS, etc.).

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.



The screenshot shows the 'Detected threats' section of the web console. It lists 652 viruses and spyware, 0 suspicious files, and 20 hacking tools and PUPs. Below this, a table shows detected threats in the file system:

Computer	Group	Name	Path	Action	Date
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...OL.zip\Voeb.exe	Quarantined	7/2/2014 3:58:40 PM
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...enamel\TOOL.exe	Quarantined	7/2/2014 3:58:39 PM
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...s\Move\TOOL.exe	Quarantined	7/2/2014 3:58:37 PM
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...OL.zip\Voeb.exe	Quarantined	7/2/2014 3:58:37 PM
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...Ignorant\TOOL.exe	Quarantined	7/2/2014 3:58:34 PM
EXCHSERVERS	\Grupo_S...yuntamiento	Nukes\Voeb-A	D:\cebos\Malw...OL.zip\Voeb.exe	Quarantined	7/2/2014 3:58:34 PM

Technical requirements:

WEB CONSOLE:

- Internet connection
- Internet Explorer
- Firefox
- Google Chrome

FOR WORKSTATIONS / FILE SERVERS:

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

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

FOR LINUX WORKSTATIONS / FILE SERVERS:

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

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



Panda Security Certifications

