Panda Security for Desktops

Surefire protection for workstations against viruses, intruders and dangerous content

How to avoid interruptions at work and the damage caused by infections

IT threats are constantly growing in number and becoming increasingly varied. The time needed to detect new threats and repair the damage is vital to preventing productivity losses when malware renders systems partially or wholly inoperative.

Most attacks target computers of inexperienced users who download all types of software, including malicious software such as adware, and who unwittingly open spam or messages with worms.

As a result, administrators constantly have to intervene. The only way to preempt these problems is with an automatic integrated protection system.

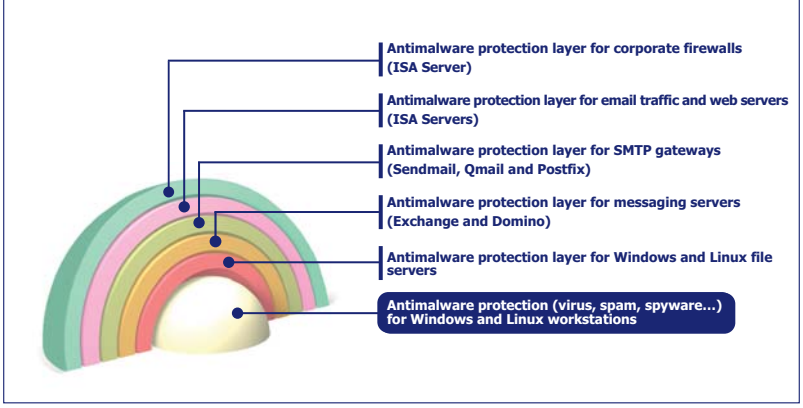
Get complete protection without sacrificing the performance of your workstations

Panda Security for Desktops is the ideal solution for protecting workstations against the widespread and instant propagation of viruses and other threats: spam, spyware, rootkits, dangerous or time-wasting content and phishing, hacker and intruder attacks.

In addition to its unrivalled threat detection and elimination capacity, **Panda for Desktops** also stands out for its high performance, ultra-low resource consumption and minimal maintenance requirements. Its administration console, Panda AdminSecure, minimizes the risk of infection for all the desktops, terminals and laptops across an organization by heading off attacks that exploit vulnerabilities and quarantining files and email messages carrying new threats.

Layered preventive protection strategy

Panda for Desktops protects workstations against viruses and intruders.



Main benefits

- Allows simple and centralized management, deployment, monitoring and definition of security policies.
- Allows **real-time decision making**.
- **Protects workstations** at all levels.
- **Controls user** behavior that could lead to network infections.
- **Boosts** administrator and end-user **productivity**.

Key features

- **Maximum protection and minimum risk of infection** from viruses, intruders, rootkits and other threats thanks to its effective detection of vulnerabilities.
- **Immediate response** to new threats through network-wide **global quarantine**, completely automatic **hourly updates** and proactive bulletins.
- New **TruPrevent Technologies** (HIPS) preempt unknown malware by blocking suspicious processes and preventing denial of service (DoS) and buffer overflow attacks.
- **Content filtering and antispam protection** to detect and eliminate potentially dangerous or time-wasting content.
- Includes **Panda Malware Radar**, the first automated malware audit, which performs online in-depth scans of your IT resources to provide maximum security against targeted attacks, botnets and other threats.
- **Complete control** of internal and external computers, when accessing from within the corporate network or from the outside (mobile computers).
- Rapid and simple **deployment and maintenance** system.

Maximum protection and minimum risk of infection

Panda for Desktops protects against intruder attacks that exploit new vulnerabilities, worms that spread using social engineering techniques, confidential information stolen by disloyal employees or spyware. It also offers complete protection against any attack and malware that could enter through different protocols (http, etc.), messaging applications such as MSN Messenger, Yahoo Messenger or AOL Messenger, email, etc. It also lets you monitor the applications used by employees and prevent them from running dangerous software.

Hourly updates and global quarantine for suspicious files

Panda for Desktops is an effective and stable solution that incorporates a centralized quarantine area and hourly incremental updates of the malware signature file in record time to head off new threats.

TruPrevent Technologies against unknown viruses and intruders

TruPrevent Technologies (HIPS) monitor running processes on the lookout for malicious behavior. They not only detect unknown malware, but also block their communications, preventing them from running, and request the vaccine from Panda to disinfect and repair the computer with *SmartClean2* technology.

Panda for Desktops provides an intelligent answer through its Genetic Heuristic Engine, which assesses the threat of processes before they are run; an automatic deep packet inspection firewall, to analyze the data packets transferred for malware and a buffer overflow detection module, which supervises memory access.

Antispam protection and content filtering

In addition to protecting MAPI, POP3, SMTP and NNTP mail, **Panda for Desktops** incorporates an effective antispam mechanism that uses rules, Bayesian patterns, lists and remote learning to classify junk mail allowing the user to reclassify email through Microsoft Outlook or Outlook Express.

Nevertheless, the spam filter on its own cannot block all types of dangerous content. For this reason, **Panda for Desktops** also incorporates protection against phishing attacks, as well as a set of options to filter mail by its extension or MIME type.

Reinforcement of protection technologies

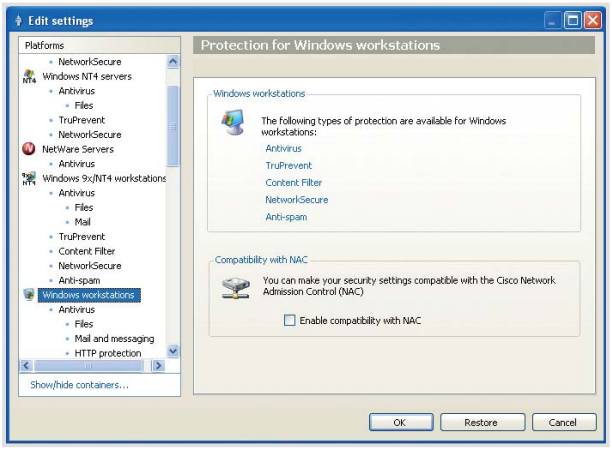
As well as integrating with security programs like CISCO NAC, the NetworkSecure unit incorporated in Panda for Desktops guarantees control of access through MAC addresses, limiting the risk of theft of confidential information and ensuring that external staff connecting to the local network comply with security rules.

Through its roaming system, **Panda for Desktops** accompanies you wherever you go, even if you need to update the protection from home, a hotel or a client's offices, through the corporate Extranet.

Quick and simple deploymen and maintenance

With Panda AdminSecure, the management tool for **Panda for Desktops**, implementing a consistent security policy couldn't be easier. The solution can be installed in two ways: either directly from the console using the IP address or machine name or manually with tools like SMS or Tivoli.

Once set up, administrators have a centralized and global view of the entire network in real-time. What's more, they can generate remote on-demands scans and define the distribution server providing fault tolerance. Overall, **Panda for Desktops** is designed to optimize the performance of computers and bandwidth consumption.



Technical requirements

Panda AdminSecure Console
Pentium II 266 MHz or above.
RAM: 140MB.
Hard disk free space: 140MB.
Internet Explorer 5.5.
Windows installer 2.0.
AdminSecure operating systems: Windows 2000/XP/Vista (32 and 64bits), Vista, Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64bits, Windows Server 2008 (32 and 64bits)

Panda Security for Desktops
Pentium 300MHz or above
RAM Antivirus: 64MB. Recommended: 128MB
RAM Antivirus + TruPrevent: 128MB. Recommended 512MB
Hard disk free space: 200MB
Outlook 4 or above
TruPrevent not supported on 64-bit systems
Operating systems: Windows 2000/ME, XP, Vista SP2, Windows7 (32 and 64 bits). WEPOS 1.1, Tablet PC and WEPOS Ready 2009.

Panda Security for Linux
Supported Distributions: Debian 3.1, 4, 5, Ubuntu 7.04, 9.10, OpenSUSE 10.1,10.2, 11.2 and Enterprise 10, Fedora Core 6, Red Hat Enterprise 4 (Desktop, Workstation, Server) and 5 (Client), Mandriva 2007.1

"All of our 1,000 workstations are well protected with Panda Security."
Luis Valmiki. Systems Manager. Portucel. PORTUGAL.

Panda Security Certifications

Powered by: mailshell™

Remember **Panda for Desktops** can be bought separately or as part of **Panda Security for Business** or **Panda Security for Enterprise**.