

Panda SecurityforEnterprise

Technical requirements

Panda AdminSecure

Administration Server:

Pentium III 800 Mhz
RAM: 256MB
Hard Disk free space: 25MB + 120MB (DDBB) for a network with 1000 machines

Repository Server

Pentium III 800 Mhz
RAM: 128MB
Hard Disk free space: 520MB

Communications Agent

Pentium III 133 Mhz
RAM: 64MB
Hard Disk free space: 40MB
Internet Explorer 5.5

Console

Pentium III 266 Mhz
RAM: 140MB
Hard Disk free space: 140MB
Internet Explorer 5.5
Windows installer 2.0

Operating Systems: Windows 2000/XP/Vista (32 and 64bits), 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 + TruePrevent: 128MB, Recommended 512MB
Hard disk free space: 200MB

Outlook 4 or above

TruePrevent not supported on 64-bit systems

Operating Systems: Windows 2000, XP, Vista SP2, Windows7 (32 and 64 bits), WEPOS 1.1, Tablet PC and WEPOS Ready 2009

Panda Security Commandline

Pentium/athlon or above
Minimum RAM: 128MB
Hard Disk: 120MB

Operating Systems: Debian 4, Red Hat Enterprise 4, Mandrake 10.1,Mandriva 2006, Ubuntu 6.06, Fedora Core 5, CentOS 4.6 or, Windows 2000/XP/Windows Server 2003 (Enterprise Edition)/Vista

Panda Security for File Servers

Pentium 300 MHz or above
RAM Antivirus: 256 MB
RAM Antivirus + TruePrevent: 256MB, Recommended: 512MB
Hard Disk: 160MB

TruePrevent not supported on 64-bit systems

Operating Systems: Windows server 2000 Domain Controller, StandAlone, Terminal server, SB server and cluster, Windows Server 2003 (32 and 64 bits) Enterprise Edition, SB server, SP1, SP2 and cluster, Windows server 2003 R2(32 and 64bits), windows server 2008 (32 and 64 bits), windows 2008/R2 (32 and 64 bits)

Panda Security for Exchange

Exchange Server 2000/2003
Pentium II 500MHz or above
RAM: 512MB for 2000 and 1 GB for 2003
Hard Disk: 200MB

Operating Systems (2000): Windows 2000 Server (SP3), 2000 Advanced server, Windows Server 2003 Enterprise Edition SP1

Server 2003 R2
Applications: Microsoft Exchange server 2000 SP1, including cluster, Exchange server 2003 SP1

Exchange Server 2007/2010

Intel processor with Intel Extended Memory 64 or AMD with AMD64 platform.
RAM: 2GB minimum (4GB in 2010).
Hard Disk: 250MB

Operating Systems: Windows Server 2003 R2/Windows server2003 R2 x64, Windows Server 2008 (Exchange 2007 SP1, SP2)

Applications: Microsoft Exchange server 2007 SP1/SP2, Exchange 2010.

Panda Security for Domino Servers

Pentium 133 or above
RAM: 256KB
Disco Duro: 200MB

Operating Systems: Microsoft Windows 2000 server SP1 or higher, Windows 2003 server, Windows 2003 Server SP1, Windows 2003 Server R2
Applications: Lotus Domino 4.5 or higher (8.5 included)

Panda Security for ISA Servers

ISA Server 2004 Standard
Pentium III 550MHz or above
RAM: 1GB

Local NTFS partition with 200MB of free hard disk space plus 60MB for the Web content cache

ISA Server 2004 Enterprise

Pentium III 550MHz or above
RAM/ 1GB

Local NTFS partition with 200MB of free hard disk space plus 60MB for the Web content cache

ISA Server 2006 Standard or Enterprise

Pentium III 330MHz
RAM/ 1GB

Local NTFS partition with 200MB of free hard disk space plus 60MB for the Web content cache

Operating Systems: Windows Server 2003 SP1
Windows Server 2003 R2, ISA Server 2006

Panda Security for Gmail, Panda Security for SendMail and Panda Security for Postfix

Pentium III 668MHz
RAM: 512MB, Recommended 1GB
Hard Disk: 5GB

Panda Security for Linux

Pentium III or higher 800 MHz (or AMD).
RAM: 256 MB
Hard disk free space: 200MB

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

Panda Security for Linux Servers

Pentium II or AMD 400 MHz (or higher)
RAM: 128 MB
Hard disk free space: 150MB

Supported Distributions: Red Hat Enterprise Linux 5 Server and Workstation 4, Advanced Server, Enterprise Server and Workstation, OpenSUSE 10.1, 10.2, 11.2 and Enterprise 10, Ubuntu 7.04, 9, 10, Debian 3.1, 4, 5

* Linux protections are not managed by AdminSecure.

Panda SecurityforEnterprise

Proactive Multi-tier Protection

Malware attacks cost large organizations 2.2% of their annual revenues even though they have traditional security solution installed.

All large organizations have traditional security solutions installed for protecting their network. By having so, they may be protected from massive malware attacks but they can still be vulnerable to zero-day malware threats or targeted attacks.

In fact, the effects of malware attacks in large organizations have risen to 2.2% of their annual revenues in 2007. In many cases, malware attacks take up network resources or shut down computers, causing an important lost of productivity. But in many other cases organizations can face more silent threats such as targeted attacks that can go unnoticed by signature-based traditional security solutions. Antivirus companies that continue to protect their clients with the traditional model are unable to offer complete protection due to the exponential growth in malware creation.

Large organizations need complete solutions that allow them to manage risk situations with proactive and preventive methods. Due to the existing malware scenario, organizations need to adapt their security policies to comply with regulation requirements and become trusted.

Network security strategies are increasingly becoming a part of the business as they may prevent it from losing revenue. A correct security strategy can increase business profits by reducing risks.

"Large organizations have client malware largely in check, but are plagued roughly evenly by DOS attacks and server malware. In most cases, they have best infrastructure in place to track downtime. Large organizations are also the focus of the most targeted attacks..."
(Infortics - The Cost of Network Security Attacks, North America 2007 (Infortics Research))

The solution: Panda Security for Enterprise

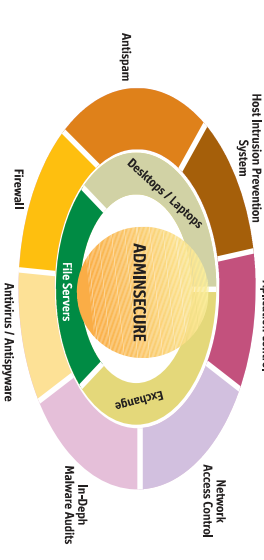
Panda Security for Enterprise provides the most advanced **proactive protection** in a **multi-tier flexible** architecture covering all layers of the network. Its functionalities include network access and application control.

Based on a combination of a **multi-tier proactive protection** (TruePrevent) and periodical **in-depth audits** (Malware Radar), Panda Security for Enterprise offers a complete preventive solution against known and unknown threats.

Panda Security for Enterprise includes protection for desktops, roaming users, file servers, e-mail servers (Exchange, Domino), ISA servers and MTAs.

The **centralized console** (AdminSecure) unifies the information of all protections and allows administrators to manage risks by offering real-time information to keep them constantly alert to threats.

Panda Security for Enterprise is the **only** solution that covers all necessary types of protection as an **all-in-one** solution, eliminating the need to purchase additional security components in the future.



"The best example of a vendor that has taken the visionary step of delivering a single client with a full complement of host-based intrusion prevention technologies is Panda, with its ClientShield product, which is priced as a single solution and provides protection across eight of the nine protection styles outlined in our file's research."
(Gartner - How to Get Free Anti-Spyware (for Antivirus) Protection)



Main benefits

- Complete centralized monitoring of all the corporate network computers. The AdminSecure management console allows the administrator to manage the whole of the network from one or more points, optimizing computer productivity and allowing centralized policies.
- Efficient security solution. The different modules included in the solution offer each company the freedom of selecting the right security level for its system structure.
- Ensures corporate policy fulfillment and optimizes employer productivity. The administrator can distribute policies to the computers and block access to restricted applications or files from the central console.
- Simplifies risk management. Corporate protection is centralized in a single console to detect hidden malware that could have gone unnoticed during other scans.
- Protects the company's critical assets. Proactive technologies provide an additional protection layer against all types of unknown malware, targeted attacks and Internet threats.

Key features

- Centralized all-in-one console to manage all the protection layers. AdminSecure provides real-time information. Dashboard
- Most advanced proactive technology composed of intrusion prevention, proactive detection and behavioral analysis.
- In-depth malware audits and disinfection service capable of uncovering advanced hidden threats.
- Network access control to prevent infected, insecure or compromised PCs from connecting to your network and contaminating your files and data.
- Anti-spy for desktops, e-mails servers and MTAs to eliminate undesired mail.
- Exhaustive Content Filtering. Preventive blocking of viruses and spam, in both inbound and outbound email.
- Application control that allows administrators to have complete control over endpoint and network wide scope of detailed detection activity reports which can be optimized and configured to be sent periodically to administrators.
- Anti-malware protection and content filtering for Microsoft ISA servers. Ensures the robustness of your security policies. Stops the spread of infections on local networks.

Check it now at www.pandasecurity.com
Get your evaluation version of Panda Security for Enterprise.

www.pandasecurity.com

PANDA
SECURITY

PANDA | 20th Anniversary
SECURITY 1990-2010

www.pandasecurity.com

Centralized all in one console

Panda AdminSecure is the centralized administration tool for Panda Security for Enterprise. Its dashboard provides real-time monitoring and control of the security and risk levels of all network systems: workstations, laptops, file servers, mail servers and gateways, firewalls, etc.

AdminSecure adapts to the structure of your company, allowing you to install, manage, maintain and supervise the protection installed across your network quickly and simply, regardless of the language or the number of computers and platforms to protect.

Most advanced proactive technology

All the solutions included in Panda Security for Enterprise incorporate the most advanced and most recognized proactive technologies that use automatic processes without user intervention. It includes a generic heuristic engine, behavioral blocking and behavioral scanning of known and unknown malware: **TruPrevent Technologies**.

In-depth malware audits included

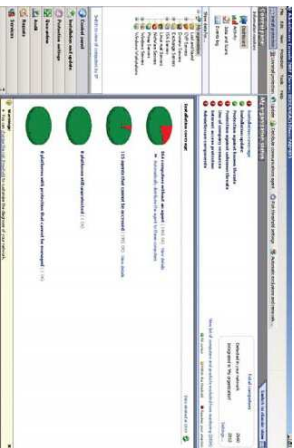
Panda Malware Radar is an automated audit which locates infection points that traditional security tools fail to detect.

Based on our **Collective Intelligence** approach, it complements and helps maximize your protection against hidden threats without additional components or infrastructure.

Panda Malware Radar provides automatic audits of your network and detailed reports with results and recommendations offering the option to automate malware disinfection routines.

Network Access Control

Panda is the only security vendor that includes a Network Access Control feature by default. This feature ensures that there are not compromised users entering your network. It will scan any computer that tries to enter the network to determine if its antivirus (any antivirus) is properly updated or not. If the answer is "no", it will not let this computer enter the network.



Anti-spam at desktop, e-mail servers and MTAs

Panda Security for Enterprise is the only solution that includes an anti-spam feature for desktops, e-mail servers (Exchange and Domino) and MTAs (Gmail, Sendmail and Postfix) allowing organizations to increase productivity and bandwidth capacity.

The anti-spam engines included in Panda Security for Enterprise offer ratios of detection higher than 95%.

Application Control

The use of some applications could pose security threats or could cause loss of productivity to organizations. Thanks to the application control feature, administrators will be capable of controlling the applications that can or cannot be used.

Exhaustive content filtering

Preventive blocking in Exchange of viruses and spam in both inbound and outbound email. Content filters act either on the content, the information contained in the mail body, or on the mail headers (like "Subject:") to either classify, accept or reject a message.

Detailed Reports

Administrators can have complete reports that show the security activity of their networks in a very user friendly format. Although there is an extensive list of predefined reports, administrator have the possibility to customize their own reports.

Reports can be configured to be regularly sent by email to certain email addresses.

Anti-malware protection and content filtering for Microsoft ISA servers

Ensures the robustness of your security policies. Stops the spread of infections on local networks. It scans all the formats sent and received. It does this using a Web filter (ISAP) and an application filter through HTTP, SMTP and FTP (over HTTP).



TruPrevent: Intelligent protection based in behavior

As part of the most advanced proactive protection Panda Security includes in all its solutions TruPrevent technologies.

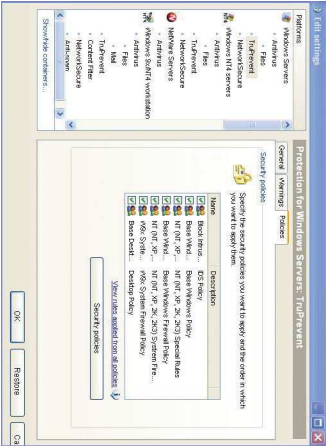
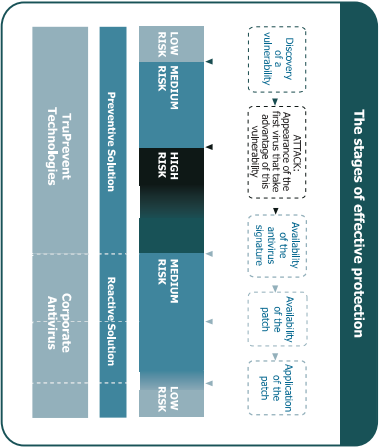
Thanks to its capacity to detect behavioral anomalies, TruPrevent Technologies are the first of their kind capable of effectively preventing service downtime due to intruders and all types of unknown malware. These innovative, high performance technologies reduce the risk of infection and associated costs.

TruPrevent Technologies are the solution for workstations and servers capable of automatically and accurately identifying and blocking: worms, network viruses, spyware and other new malware that has slipped past other protection, either because it is not completely updated or because instead of taking action, it has simply notified the administrator about the possible attack.

By having TruPrevent Technologies running, organizations benefit from:

- Reducing the risk window opened by vulnerabilities by preventing new infections that exploit these security holes from spreading before the patch has been applied.
- Maintains your network security level by blocking hacker attacks confidential data theft and infection generated by computers that are not managed internally. Wi-Fi access and external consultants.
- Flexible security policy management to customize and reinforce security rules across the entire network, preventing theft of confidential information by disloyal employees.

TruPrevent Technologies are the perfect complement for the antivirus providing an intelligent layer of protection that maximizes the capacity to detect any type of new virus or intruder.



Console	AdminSecure	Panda Security For Business	Panda Security For Exchange	Panda Security For Enterprise
Endpoint	Panda Security for Desktops	✓	✓	✓
	Panda Security for File Servers	✓	✓	✓
	Panda Security for Linux servers	✓	✓	✓
	Panda Security for Exchange Servers	✓	✓	✓
Mail	Panda Security for Postfix	✓	✓	✓
	Panda Security for Gmail	✓	✓	✓
	Panda Security for Sendmail	✓	✓	✓
	Panda Security for Domino Servers	✓	✓	✓
Gateway	Panda Security for ISA Servers	✓	✓	✓
TechTools	Panda Security Commandline	✓	✓	✓