

Technical requirements

AdminSecure Administration Server:

Pentium III 800 MHz (or faster); 256 MB RAM; Hard disk: 25 MB + 120 MB (Database).

Operating systems: Windows NT4 SP6, and Terminal Server, Windows 2000 and 2000 Server SBS, Windows XP/XP 64 bits, Windows Server 2003 Enterprise Edition / SBS / R2, Windows Server 64 bits, Windows Vista 32 bits/64 bits.

AdminSecure Repository Server:

Pentium III 800 MHz (or faster); 128 MB RAM; Hard disk: 250 MB.

Operating systems: Windows NT4 SP6, and Terminal Server, Windows 2000 and 2000 Server SBS, Windows XP/XP 64 bits, Windows Server 2003 Enterprise Edition / SBS / R2, Windows Server 64 bits, Windows Vista 32 bits/64 bits.

AdminSecure Console:

Pentium II 266 MHz; 64 MB RAM; Hard disk: 140 MB.

Operating systems: Windows 2000 / XP / XP 64 bits, Windows NT4 SP6 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 32 bits/64 bits.

Panda Security for Desktops:

Pentium III 300 MHz (or faster). 64 MB RAM (128 MB if TruPrevent Technologies are enabled); Hard disk: 200 MB.

Operating systems: Windows 9x/2000/ME/XP/XP (SP3) 64 bits, Windows NT4 (SP6) Windows Vista 32 bits/64 bits, Windows Vista (SP1). TruPrevent not supported in Windows 95 and 64 bits.

Panda Security for Linux:

Pentium III or higher 800+ MHz (or AMD). RAM: 256 MB. Hard Disk: 200 MB.

Supported Distributions: Ubuntu: 6.06, 6.10, 7.04; OpenSuse: 10.1 and 10.2; Fedora Core: 6; Debian: 3.1 (Sarge) and 4.0 (Etch); Red Hat Enterprise: 4 (Desktop, Workstation, Server) and 5 (Client); SUSE Enterprise: 10; Mandriva: 2007, 2007.1.

Panda Security for File Servers:

Windows Servers:

Pentium 300 MHz (or higher); 256 MB RAM. Hard disk: 85 MB

Operating systems: Windows NT 4.0 SP6 Domain Controller, Small Business Server, Terminal Server and Cluster. Windows Server 2000 Domain Controller, Stand Alone, Terminal Server, Small Business Server and Cluster. Windows Server 2003 SP1 and SP2 (32bits and 64 bits) Enterprise Edition, Small Business Server and Cluster. Windows Server 2003 R2 (32 bits and 64 bits). Windows Server 2008, Server Core 2008, Small Business Server 2008. TruPrevent not supported in 64 bits.

Novell Network Servers: 486 Processor or later.; 32 MB RAM; Hard disk: 12 MB.

Operating systems: Novell Netware 4.11, 5.0, 5.1, 6.0 ó 6.5.

Panda Security for Linux Servers:

Pentium II or AMD 400 MHz (or later); RAM: 128 MB; Hard Disk: 150 MB.

Supported Distributions: Red Hat Enterprise Linux: 4.0 (Desktop, Workstation, Enterprise Server and Advanced Server) and 5.0 (Desktop and Server). SuSE Linux Enterprise Desktop: 10. SuSE Linux Enterprise Server: 9 and 10. Ubuntu: 7.04 (Feisty), 6.06 LTS. Debian: 3.1 (sarge) and 4.0 (etch).

Panda Security for Exchange:

For Exchange Server 5.5: Pentium II 500 MHz (or later); 256 MB RAM; Hard Disk: 250 MB.

Operating systems: Windows NT Server 4.0 (or later) with Service Pack 5 (or later) and Windows 2000.

Applications: Microsoft Exchange Server 5.5 with Service Pack 3. Exchange cluster.

For Exchange Server 2000/2003:

For Exchange Server 5.5: Pentium II 500 MHz (or later); 256 MB RAM; Hard Disk: 250 MB.

Operating systems: Microsoft Windows 2000 Advanced Server SP3 or later, Windows Server 2003/R2.

Applications: Microsoft Exchange Server 2000 with SP 1 (or later) or Exchange 2003, including cluster.

For Exchange Server 2007:

Intel EM64T or AMD64 platforms at least 2 GB of RAM, at least 250 MB hard disk space apart from Exchange 2007.

Operating systems: MS Windows Server 2003 x64 or Windows Server 2003 R2 x64, Windows Server 2008 (only for Exchange 2007 SP1).

Applications: Microsoft Exchange Server 2007 and Exchange 2007 SP1.

Panda Security for Domino Servers:

Pentium 133 MHz (or later); 128 MB RAM; Hard Disk: 55 MB Domino cluster.

Operating systems: Windows NT Server 4.0 SP6a (or higher), Windows 2000, Windows 2000 Advanced Server and Windows Server 2003.

Applications: Lotus Domino 4.5.x (or later). Domino Server 8 (32 bits).

Panda Security for ISA Servers:

For Microsoft ISA Server 2000:

Pentium II 300 Mhz o higher; RAM: 256 MB; Hard disk: 90 MB.

Operating systems: Windows 2000 Server, Advanced Server SP 1 (o higher) or Windows Server 2003/R2.

Microsoft ISA Server 2004 (Standard and Enterprise Edition) and Microsoft ISA Server 2006 (Standard and Enterprise Edition): Pentium III a 550 MHz o higher (up to 4 CPUs on one server). RAM: 256 MB; Hard Disk: 180 Mb with NTFS.

Operating systems: Windows 2000 Server, Advanced Server SP 4 (or higher) or Windows Server 2003/R2.

Panda Security for Qmail, Panda Security for SendMail and Panda Security for PostFix:

Pentium II 200 MHz (or higher); 64 MB RAM; Hard Disk: 80 MB, 90MB for PostFix.

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 loss 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..."
Infonetics: The Cost of Network Security Attacks: North America 2007 (Infonetics Research).

The solution: Panda Security for Enterprise

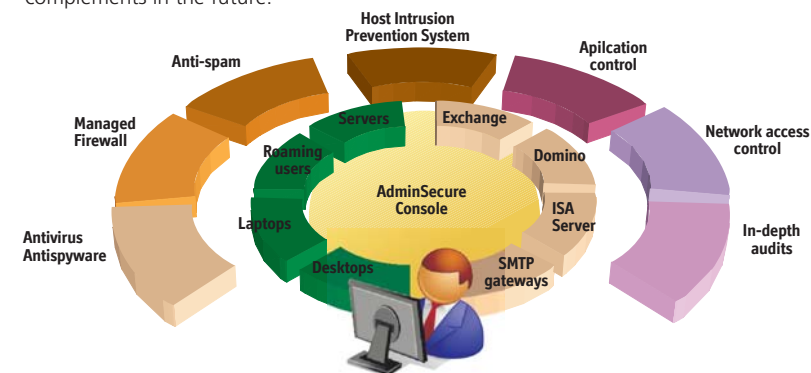
Panda Security for Enterprise provides the most advanced **proactive protection** in a **multi-tier flexible** architecture covering all layers of the network. Its functionalities include network access and application control.

Based on a combination of a **multi-tier proactive protection** (TruPrevent) 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 complements 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 Software, with its ClientShield product, which is priced as a single solution and provides protection across eight of the nine protection styles outlined in our HIPS research"
Gartner: How to Get Free Anti-spyware (or Antivirus) Protection.

Main benefits

- Protects critical and sensitive information from data leaks, targeted attacks and unknown malware thanks to its advanced behavioral analysis and proactive protection mechanisms.
- Helps implement enterprise regulation compliance by managing security policies with a rule-based application control and network access control.
- Reduces operation complexity thanks to an easy-to-use centralized management console that controls all endpoints from a single point.
- Maximizes return of investment by providing a converged, single-priced solution complemented with host-based intrusion prevention, access and application control and targeted attack audits.
- Increases employee productivity by drastically reducing spam and controlling the use of unproductive or non-allowed applications with undesired content.
- Helps manage risks from advanced threats thanks to a complementary in-depth audit service capable of uncovering hidden malware not detected by traditional means.

Key features

- Centralized all-in-one console to manage all protections from a single point. **Dashboard** provides real-time information.
- 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-spam for desktops and Exchange Servers to eliminate undesired mail.
- Application control that allows administrators to have complete control over endpoint and network resources.
- Multi-tier and flexible architecture for heterogeneous networks, servers and gateway exchange servers platforms.
- Wide range of detailed detection activity reports which can be customized and configured to be sent periodically to administrators.

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 genetic heuristic engine, behavioral blocking and behavioral scanning of known and unknown malware (TruPrevent Technologies).

In-depth malware audits included

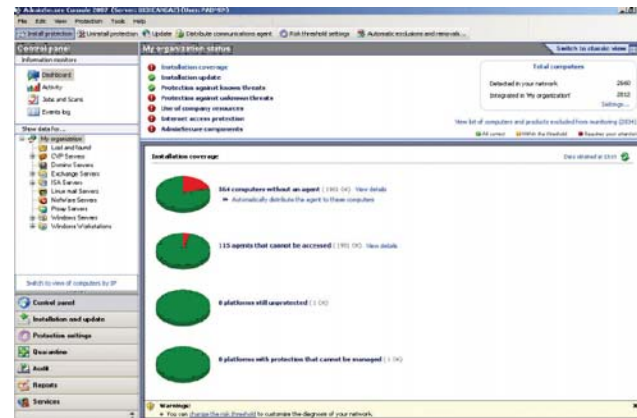
Panda Malware Radar is an automated audit which locates infection points that traditional security tools fail to detect.

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

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.



Antispam at desktop and Exchange servers

Panda Security for Enterprise is the only solution that includes an anti-spam feature for desktops and Exchange servers allowing organizations to increase their productivity and increasing 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.

Multi-tier and flexible architecture

Panda Security for Enterprise offers protection for heterogeneous networks, servers and gateway exchange server platforms. It allows security management integration within third-party tools (release versions or proprietary developments) for deploying pure and mixed solutions, through the Software Development Kit included in the box.

Panda Security for Enterprise includes **CommandlineSecure**, the ideal security solution for expert administrators to protect feature-rich heterogeneous environments without Windows interface.

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.

Panda Collective Intelligence:

It is a matter of survival for AV vendors, who increasingly are looking for ways to reinvent themselves as their product struggle to thwart new type of infections. Cloud-based, collective intelligence services are the next big thing for anti-malware. I expect that every AV vendor will need to embrace an approach like this if they expect to survive "

Yankee Group: Andrew Jaquith



TruPrevent: Intelligent protection based in behavior

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

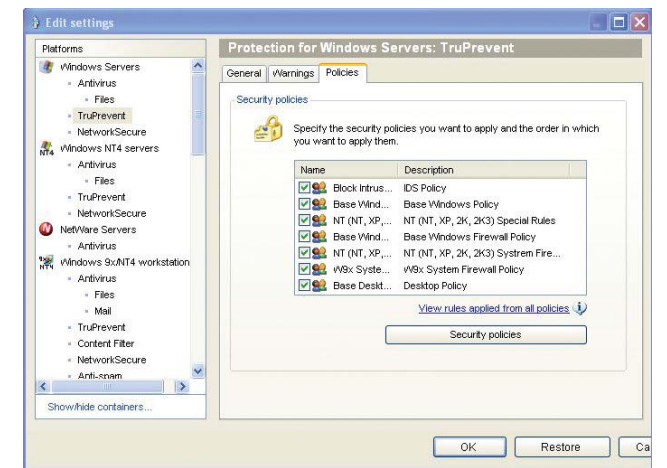
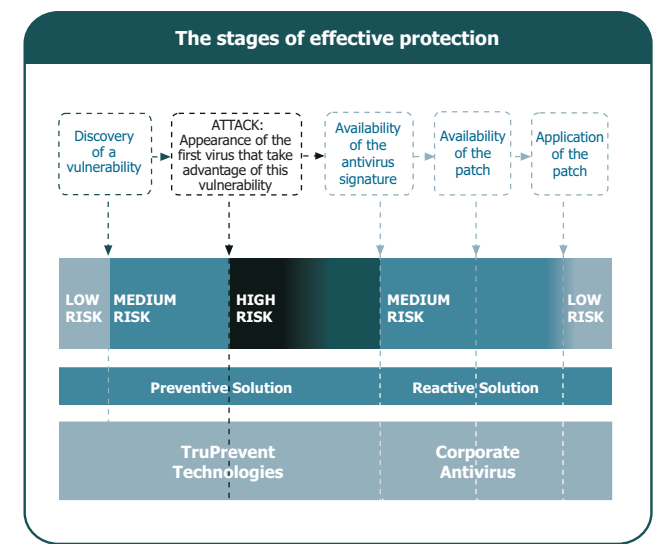
Thanks to its capacity to detect behavioral anomalies, TruPrevent Technologies are the first of their kind capable of effectively preventing service downtime due to intruders and all types of unknown malware. These innovative, high performance technologies reduce the risk of infection and associated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



| | Panda Security For Business | Panda Security For Business with Exchange | Panda Security For Enterprise |
|--|-----------------------------|---|-------------------------------|
| AdminSecure | ✓ | ✓ | ✓ |
| Panda Security for Desktop | ✓ | ✓ | ✓ |
| Panda Security for File Server | ✓ | ✓ | ✓ |
| Panda Security for Exchange | | ✓ | ✓ |
| Panda Security for ISAServers | | | ✓ |
| Panda Security for Domino Servers | | | ✓ |
| Panda Security for Sendmail, Qmail y Postfix | | | ✓ |
| PandaSecurity for Linux Servers | | | ✓ |
| Panda Security for Commandline | | | ✓ |
| Panda Security for Management SDK | | | ✓ |
| Panda Security For Linux | ✓ | ✓ | ✓ |
| Panda Antivirus 2008 | ✓ | ✓ | ✓ |
| Panda Antivirus+Firewall 2008 | ✓ | ✓ | ✓ |
| Panda Internet Security 2008 | ✓ | ✓ | ✓ |