

Panda Security for Business

The best protection for your business assets.

Product
Data Sheet

95% of small and medium-sized businesses nowadays have an antivirus installed on their network endpoints, but 72% are still infected.

Almost all small and medium-sized business organizations have some kind of security solution installed for protection reasons. Most of these organizations feel protected just for having an antivirus installed. However, the reality is that a very high percentage is still infected by malware.

Although it may seem that these infections are not harmful for businesses, according to Gartner almost half of small and medium-sized businesses have to close Internet access due to external malware attacks, causing crippling revenue loss.

This means that traditional protections are not enough for meeting security needs. Malware is now designed specifically to go unnoticed. It is much more complex and varied, and in many cases, it is tailored to achieve specific objectives.

"Almost 50% of SMBs shut down external network access during serious external attacks; for many SMBs, this can cause crippling revenue loss."

- Gartner

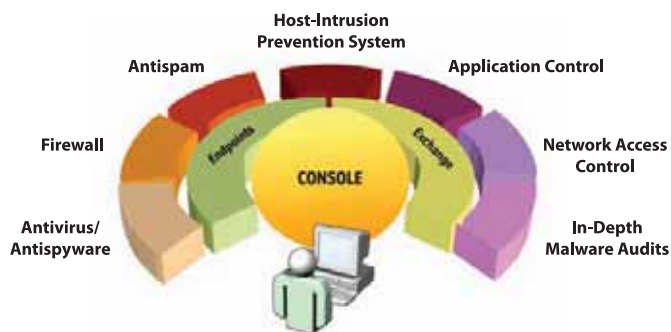


Fig. 1 AdminSecure

THE SOLUTION: PANDA SECURITY FOR BUSINESS

Panda Security for Business provides maximum proactive protection for organizations against today's and tomorrow's threats.

Based on a combination of the most advanced proactive technologies (Truprevent) for endpoints and periodical in-depth audits, Panda Security for Business offers a complete protection against known and unknown threats.

The all-in-one console (Adminsecure) enables administrators to manage all necessary network protections in an extremely easy way, helped by an intuitive wizard for deploying the most adequate protection to endpoints.

Panda Security for Business is the only solution that includes, in a single priced suite, all necessary protections for a medium-sized organization such as host-based intrusion prevention system, in-depth targeted attack audits, application management and network access control.

This solution directly benefits from our Collective Intelligence approach, which increases efficiency against detection, helping maximize your protection against unknown threats.

MAIN BENEFITS

- Protects your critical and sensitive information from data leaks, targeted attacks and unknown malware thanks to its advanced behavioral analysis and proactive protection mechanisms
- 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 with host-based intrusion prevention, access and application control and targeted attack audits
- Increases employee productivity by controlling the use of unproductive or non-allowed applications and eliminating undesired content
- Helps manage risks from advanced threats thanks to a complementary in-depth audit service able to uncover hidden malware not detected by traditional means

"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

KEY FEATURES

- Centralized all-in-one console that enables to manage all protections from one single point
- Most advanced proactive technology composed by 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
- Application control that allows administrators to have complete control over endpoint and network resources
- Wide range of detailed reports about detection activity which can also be customized and configured to be send periodically to administrators
- Anti-spam on desktops and Exchange Servers to eliminate undesired mail
- Centrally-managed Quarantine that allows administrators to control suspected files and determine the actions to take. It includes the possibility to send suspicious files to PandaLabs for analysis
- Real-time incident alerts and monitoring of the security status and performance of the administration and distribution servers

CENTRALIZED ALL IN ONE CONSOLE

Panda AdminSecure is the centralized administration tool for Panda Security for Business. Its ultra-reliable technology 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

Panda Security for Business includes in all its solutions 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.

IN DEPTH MALWARE AUDITS

Panda Malware Radar is an automated audit which locates infection points that traditional security fails 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.

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.

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.

ANTISPAM AT DESKTOP AND EXCHANGE SERVERS

Panda Security for Business 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.

CENTRALLY MANAGED QUARANTINE

If a new threat is detected, the suspicious files will be quarantined to prevent them from causing any damage. They will also be automatically sent to AdminSecure or to PandaLabs for processing.

REAL TIME INCIDENT AND ALERTS MONITORING

Panda Security for Business enables real-time decision-making thanks to its system, for continuously monitoring the network status and the performance of the administration and distribution servers. It also offers a real-time incident warning system via email.

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

PANDA SECURITY CERTIFICATIONS



	Panda Security For Business	Panda Security For Business w/Exchange	Panda Security for Enterprise
AdminSecure	✓	✓	✓
Panda Security for Desktops	✓	✓	✓
Panda Security for File Server	✓	✓	✓
Panda Security for Exchange		✓	✓
Panda Security for ISA Servers			✓
Panda Security for Domino Servers			✓
Panda Security for Sendmail, Qmail y Postfix			✓
Panda Security for Linux Servers			✓
Panda Security for Commandline			✓
Panda Security Management SDK			✓
Panda Security for Linux	✓	✓	✓
Panda Antivirus 2007	✓	✓	✓
Panda Antivirus + Firewall 2007	✓	✓	✓
Panda Internet Security 2007	✓	✓	✓

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 64 bits, Windows NT4 SP6 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64 bits, Windows Vista 32 bits/64 bits, Windows Vista with Service Pack 1. TruPrevent not supported in Windows 95, Windows XP 64 bits and Windows Vista 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;

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, Windows Server 2000, Windows Server 2003 SP2 and 2003 SBS/cluster/R2.

Novell Netware 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: 5.0 Server and Workstation, 4.0 Advanced Server, Enterprise Server and Workstation. SuSE Linux Enterprise: 10 Server and Desktop, 9 Server and desktop. Ubuntu: 7.04 (Feisty), 6.06 LTS. Desktop/Server (Dapper). Debian GNU/Linux 4.0.

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:

Pentium II 500 MHz (or later); 256 MB RAM; Hard Disk: 250 MB

Operating system: 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 system: MS Windows Server 2003 x64 or Windows Server 2003 R2 x64

Applications: Microsoft Exchange Server 2007 and Exchange 2007 with Service Pack.