Panda AdminSecure | Centralized management of your corporate network security

Simplify your corporate security management

Corporate IT systems are increasingly complex and heterogeneous: new operating systems to manage, applications that require constant maintenance, employees accessing data from different locations, increased integration with international partners and suppliers. Worse still, all these factors, along with security holes in software applications, are exploited by new threats such as spyware or rootkits.

In this dynamic environment, **it is difficult to ensure appropriate preventive action** and correctly monitor security levels, especially when physical access is needed to keep track of the status of each computer or if several administration consoles are needed to administer the different types of protection: antivirus, antispam, antispyware, etc.

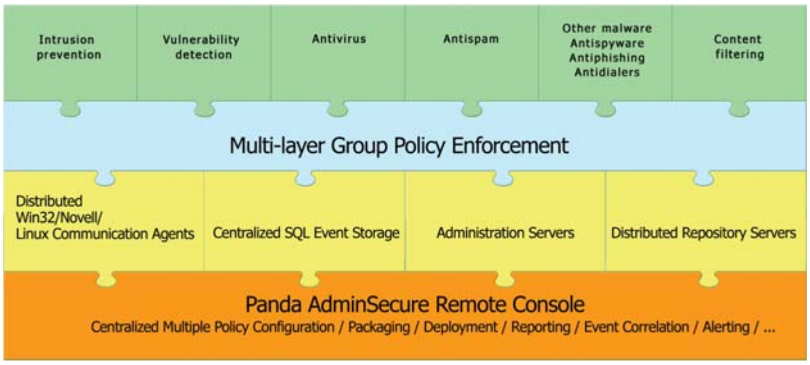
It's essential to reduce the number of routine tasks that take up most of an administrator's time. It is also important to have a console to cover the entire protection cycle: identifying vulnerabilities, detecting and removing threats… and to avoid the time-consuming task of consolidating reports and integrating multiple products.

Administer your protection through a single, centralized console

Panda AdminSecure is the centralized administration tool for the **Panda Security for Business** and **Panda Security for Enterprise** corporate solutions.

Its ultra-reliable technology provides real-time monitoring and control of the security and risk levels of all network systems: workstations, laptops, files 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 language or the number of computers and platforms to protect.


Intrusion prevention
Vulnerability detection
Antivirus
Antispam
Other malware Antispyware Antiphishing Antidialers
Content filtering
Multi-layer Group Policy Enforcement
Distributed Win32/Novell/ Linux Communication Agents
Centralized SQL Event Storage
Administration Servers
Distributed Repository Servers
Panda AdminSecure Remote Console
Centralized Multiple Policy Configuration / Packaging / Deployment / Reporting / Event Correlation / Alerting / ...

Main benefits

- Enables **real-time decision making**.
- **Simple to use**. No need to contract specialized security staff.
- Fully-automated system **reduces** maintenance time and **operating costs**.
- Customizable security policies help protect **corporate image**, avoid fines for failure to comply with regulations, prevent industrial espionage, data theft, etc.
- Boosts administrator and end-user **productivity.**

Key features

- **Flexible architecture.** Enables deployment, installation and configuration of the protection modules with TruPrevent Technologies (HIPS) in multiple platforms, versions and network layers.
- **Centralized quarantine**, incremental updates and *SmartClean2* for automatically disinfecting new unknown threats and repairing the damage they cause.
- **Identification of vulnerabilities** through TruPrevent Technologies to reduce the risk of viruses, rootkits, adware, spyware, intruders etc.
- **Adapts to your network structure**, letting you customize the console to your precise needs.
- 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.
- **Real-time incident alerts and monitoring** of the security status and of the performance of the administration and distribution servers. Compatible with other administration tools including HP OpenView, Tivoli, etc.

Flexible architecture

AdminSecure comprises a user interface (AdminSecure Console), a business logic module (Administration Server), a transport layer (AdminSecure Communications Agent) and data modules (Repository Server and Event Storage Database).

The agents and the protection can be pushed out from the repositories to network computers in several ways: directly from the console using the machine name or IP address; with scripts, using tools like Tivoli; from shared folders, via email or Active Directory.

The versatility of **AdminSecure** eases installation and control of the protection for Windows, Linux and NetWare systems from a single location. The same administration console can also be used to configure the antivirus unit, email and web traffic filtering, the anti-spam protection, the **TruPrevent Technologies**, and even complement the protection with an SDK.

Deployment of the protection through **AdminSecure** is quick and simple, with minimal use of network hardware and software resources.

Centralized 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** and to PandaLabs for processing.

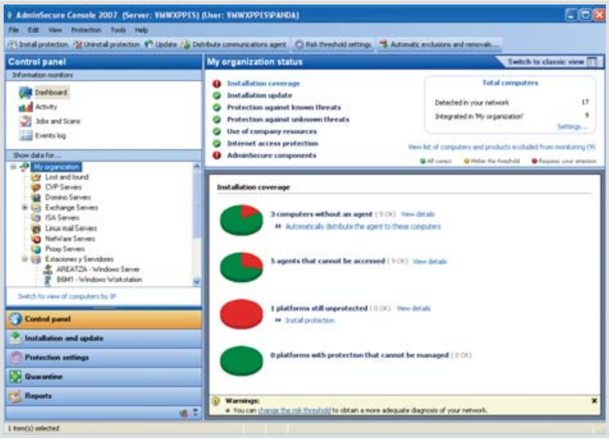
Incremental updates are available for the protection, downloading the new signature file as soon as it is released. Its *SmartClean2* technology lets administrators disinfect and repair remote computers, without needing to deploy additional tools.

Security management

To reduce the risk of infection, **AdminSecure** identifies vulnerabilities. At any time, the administrator can check the security status, both inside and outside the organization in the self-diagnosis and graphic reports. This allows them to evaluate the risks, while **TruPrevent Technologies** can guarantee security until patches have been deployed.

Adapts to your company's structure

The organizational views can be customized from the **AdminSecure** console, through integration with Microsoft's Active Directory, and allow Panda's corporate solutions to be adapted to the real structure of the organization. Even employees that use laptops can keep their computers automatically protected by updating the malware signature file from the Extranet every day.



Detected in your network 17

Integrated in 'My organization' 9

View list of computers and products excluded from monitoring (9)

3 computers without an agent (9 OK) View details

Automatically distribute the agent to these computers

5 agents that cannot be accessed (9 OK) View details

1 platforms still unprotected (0 OK) View details

Install protection

0 platforms with protection that cannot be managed (0 OK)

Warnings:

You can change the risk threshold to obtain a more adequate diagnosis of your network.

1 item(s) selected

AdminSecure allows administrators to track the development of security indicators and pinpoint violations of corporate security policies, guaranteeing consistency in each network layer, even in computers belonging to external staff.

Administrator profiles and secure, simple access to **AdminSecure** from multiple consoles in order to share the administration tasks by responsibility or roles allow a rapid response to any attack.

Real-time monitoring and incident alerts

AdminSecure 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. This integrates perfectly via SNMP with other network management systems such as HP OpenView.

Technical requirements

AdminSecure Administration Server: Pentium III 800 MHz. RAM: 256 MB. Hard disk: 25 MB + 120 MB (Database). Operating system: 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-bit, Windows Vista 32/64 bit.

AdminSecure Repository Server: Pentium III 800 MHz, RAM: 128 MB, Hard disk: 250 MB. Operating system: Windows NT4 SP6 y Terminal Server, Windows 2000 and 2000 Server SBS, Windows XP/XP 64 bit, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64 bit, Windows Vista 34/64 bit.

AdminSecure Communications Agent: Pentium 133 MHz. RAM: 64 MB. Hard disk: 40 MB. Operating system: Windows 9x/2000/ME/XP/XP 64 bit, Windows NT4 SP5 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 34/64 bit. Novell Netware 4.X/5.0/6.5 and Linux distributions: Red Hat, SUSE, Mandriva, Debian and Best Linux 2000.

AdminSecure Console: Pentium II 266 MHz, RAM: 64 MB, Hard disk: 55 MB. Operating systems: Windows 2000/XP/XP 64 bit, Windows NT4 SP6 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 32/64 Bit.

> *"The installation of …the protection on the workstations is a simple and intuitive process that does not require login scripts or intervention in-situ."*
> **Pedro Rebollo. EADS CASA ESPACIO. SPAIN.**

Panda Security Certifications

Remember **AdminSecure** is a tool integrated in **Panda Security for Business** or **Panda Security for Enterprise**. It cannot be bought separately.

Get your evaluation version of Panda AdminSecure.
www.pandasecurity.com