

Requisiti tecnici

**Panda AdminSecure**

**Server di Amministrazione**

Pentium III 800 MHz  
256 MB RAM  
Hard disk 25 MB + 120 MB (Database) per una rete con 1000 macchine

**Server di Repository AdminSecure**

Pentium III 800 MHz  
128 MB RAM  
Hard disk: 520 MB

**Communication Agent**

Pentium III 133 MHz  
64 MB RAM  
Hard disk: 40 MB  
Internet Explorer 5.5

**Console**

Pentium II 266 MHz  
140 MB RAM  
Hard disk: 140 MB  
Internet Explorer 5.5  
Windows Installer 2.0

**Sistemi operativi**

Windows 2000/XP/Vista (32 bit/64 bit), Terminal Server,  
Windows 2000 Server SBS, Windows Server 2003 Enterprise  
Edition/SBS/R2, Windows Server 64 bit, Windows Server 2008 (32 bit/64 bit).

**Panda Security for Desktops**

Pentium 300 MHz (o superiore)  
64 MB RAM per le funzionalità antivirus. Consigliato 128 MB  
128 MB RAM per le funzionalità antivirus + tecnologie TruPrevent.  
Consigliato 512 MB  
Hard disk: 200 MB  
Outlook 4 o superioreLe tecnologie TruPrevent non sono supportate da sistemi a 64 bit

**Sistemi operativi**

Windows 2000, XP, Vista SP2, Windows 7 32. WEPOS 1.1, tablet PC e WEPOS Ready 2009

**Panda Security for Commandline**

Pentium/Athlon o superiore  
Minimo 128 MB RAM  
Hard disk: 120 MB

**Sistemi operativi**

Debian 4, Red Hat Enterprise 4, mandrake 10.1/Mandriva 2006, Ubuntu 6.06, Fedora Core 5, CentOS 4.6 o Windows 2000/XP/Windows Server 2003 (Enterprise Edition) /Vista

**Panda Security for File Server**

**Windows Server**

Pentium 300 MHz o superiore  
256 MB RAM per le funzionalità antivirus  
256 MB RAM per le funzionalità antivirus + tecnologie TruPrevent.  
Consigliato 512 MB  
Hard disk: 160 MB  
Le tecnologie TruPrevent non sono supportate da sistemi a 64 bit

**Sistemi operativi**

Windows Server 2000 Domain Controller, Stand Alone, Terminal Server, SB Server e Cluster. Windows Server 2003 (32 bit e 64 bit) Enterprise Edition, SB Server, SP1, SP2 e Cluster, Windows Server 2003 R2 (32 bit e 64 bit), Windows Server 2008 (32 bit e 64 bit), Windows 2008/R2 (32 bit e 64 bit).

**Panda Security for Exchange**

**For Exchange Server 2000/2003**

Pentium II 500 MHz o superior  
512 MB RAM per la versione 2000 e 1 GB per il 2003  
Hard Disk: 200 MB

**Sistemi operativi**

Windows 2000 server (SP3), 2000 Advanced Server e Windows Server 2003 Enterprise Edition SP1, Server 2003 R2

**Applicazioni**

Microsoft Exchange Server 2000 SP1, compreso il Cluster, Exchange Server 2003 SP1

**For Exchange Server 2007**

Processore Intel con Intel Extended Memory 64 o AMD con piattaforme AMD64  
Minimo 2 GB RAM (4 GB per la versione 2010)  
Hard Disk: 250 MB

**Sistemi operativi**

Windows Server 2000 x64 o Windows Server 2003 R2 x64, Windows Server 2008 (Exchange, 2007 SP1, SP2)  
Applicazioni: Microsoft Exchange Server 2007 SP1/SP2, Exchange 2010

**Applicazioni**

Microsoft Exchange Server 2007 e Exchange 2007 SP1

**Panda Security for Domino Server**

Pentium 133 o superiore  
256 MB RAM  
Hard Disk: 200 MB  
Sistemi operativi: Microsoft Windows Server 2000 SP1 o superiore, Windows Server 2003 SP1, Windows Server 2003 R2  
Applicazioni: Lotus Domino 4.5 o superiore (compreso 8.5)

**Panda Security for ISA Server**

**ISA Server 2004 standard**

Pentium III 550 MHz o superiore  
RAM: 1 GB  
Partizione locale NFTS di 200 MB di spazio libero sull'hard disk più 60 MB per la cache Web

**ISA Server 2004 Enterprise**

Pentium III 550 MHz o superiore  
RAM: 1 GB  
Partizione locale NFTS di 200 MB di spazio libero sull'hard disk più 60 MB per la cache Web

**ISA Server 2006 Standard e Enterprise**

Pentium III 733 MHz  
RAM: 1 GB  
Partizione locale NFTS di 200 MB di spazio libero sull'hard disk più 60 MB per la cache Web

**Sistemi operativi:** Windows Server 2003 SP1, Windows Server 2003 R2, ISA Server 2006

**Panda Security for Qmail, Panda Security for SendMail e Panda Security for PostFix**

Pentium III 868 MHz  
RAM: 512 MB. Consigliato 1 GB  
Hard Disk: 5 GB

**Panda Security for Linux**

Pentium III o superiore 800 MHz (o AMD)  
RAM: 256 MB  
Hard Disk: 200 MB

**Distribuzioni supportate:** Debian 3.1,4, 5, Ubuntu 7.04, 9, 10, OpenSuse 10.1, 10.2, 11.2 e Enterprise 10, Fedora Core 6, Red Hat Enterprise 4 (Desktop, Workstation e Server) e 5 (Client), Mandriva 2007.1.

**Panda Security for Linux Servers**

Pentium II o AMD 400 MHz (o superiore)  
RAM: 128 MB  
Hard Disk libero: 150 MB

**Distribuzioni supportate:** Red Hat Enterprise Linux 5 Server e Workstation 4, Advanced Server, Enterprise Server e Workstation. OpenSUSE 10.1, 10.2, 11.2 ed Enterprise 10, Ubuntu 7.04, 9, 10, Debian 3.1, 4, 5.

\*Le protezioni per Linux non sono gestite da AdminSecure

Gli attacchi del malware costano alle grandi aziende il 2,2% dei loro utili di un anno, pur avendo una soluzione di sicurezza tradizionale installata

Tutte le aziende di grandi dimensioni hanno installato una soluzione di sicurezza tradizionale per proteggere la propria rete. Di conseguenza possono essere protette da attacchi massivi, ma restano ancora vulnerabili agli attacchi "zero-day" o agli attacchi mirati.

In realtà, gli effetti del malware nelle aziende di grandi dimensioni hanno raggiunto il 2,2% dei loro utili nel 2007. In molti casi, gli attacchi si impadroniscono delle risorse di rete o spengono autonomamente i computer, causando grandi perdite di produttività. Purtroppo in molti altri casi le aziende sono vittime di minacce silenziose e di attacchi mirati che possono eludere le soluzioni di sicurezza tradizionali. I produttori di antivirus che continuano a proteggere i loro clienti con un modello tradizionale non sono in grado di offrire una protezione completa a causa della produzione esponenziale di malware.

Le grandi realtà necessitano di soluzioni complete che gli consentano di gestire questi rischi con metodi preventivi e quindi in maniera proattiva. Dato lo scenario attuale del malware, esse devono adeguare le loro politiche di sicurezza per rispettare le norme imposte e per essere realmente sicure.

Le strategie della sicurezza diventano sempre più parte del business aziendale dato che contribuiscono a evitare perdite di denaro. Una strategia di sicurezza corretta e appropriata può aumentare i profitti riducendo al contempo i rischi.

"Le aziende sono costantemente attente alla presenza del malware al loro interno, ma sono spesso vittime di infezioni di grande impatto (attacchi DOS o direttamente sui loro server). Hanno la migliore infrastruttura ma spesso resa inoperante per questi motivi. In particolare le grandi aziende sono vittime di attacchi mirati (costruiti ad hoc per loro)...". *Infonetics: Il Costo degli Attacchi alla Sicurezza della Rete: America del Nord 2007 (Infonetics Research).*

La soluzione: Panda Security for Enterprise

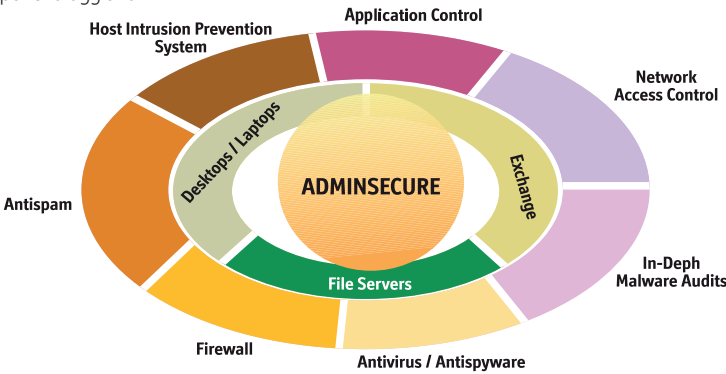
Panda Security for Enterprise fornisce la protezione preventiva più avanzata con un'architettura flessibile e multi-livello, per tutelare ogni livello della rete IT. Le sue funzionalità si estendono fino agli accessi alla rete e al controllo delle applicazioni.

Basata sulla combinazione di una protezione preventiva multi-livello (TruPrevent) e di analisi approfondite periodiche (Malware Radar), Panda Security for Enterprise offre realmente una soluzione preventiva completa contro le minacce note e sconosciute.

Panda Security for Enterprise dispone di moduli di protezione per desktop, utenti mobili, file server, email server (Exchange, Domino), ISA server e MTA generici.

La console centralizzata (AdminSecure) è in grado di raccogliere le informazioni di tutti i moduli di protezione al fine di garantire all'amministratore la gestione completa del rischio, attraverso una serie completa di informazioni in tempo reale, con il vantaggio di essere sempre e costantemente informato sullo stato della protezione e la presenza di minacce all'interno della rete aziendale.

Panda Security for Enterprise è l'unica soluzione in grado di fornire tutte le tipologie di protezione necessarie al mercato in una soluzione "all-in-one", evitando di dover acquistare in futuro componenti aggiuntivi.



"L'esempio migliore di vendor che ha scelto in anticipo di fornire in un solo client una soluzione completa di tecnologie HIPS è Panda, che al costo di una soluzione unica garantisce una protezione in grado di coprire 8 dei 9 moduli che devono far parte, a nostro parere, di una soluzione HIPS completa". *Gartner: How to Get Free Anti-Spyware (or Antivirus) Protection*

Principali benefici

- **Monitoraggio centralizzato e completo di tutti i computer presenti nella rete aziendale.** La console di amministrazione AdminSecure consente agli amministratori di gestire la sicurezza della rete nella sua interezza da uno o più postazioni, ottimizzando la produttività dei computer e centralizzando le politiche di sicurezza.
- **Soluzione di sicurezza efficiente.** I diversi moduli presenti in ciascuna soluzione offrono alle aziende (qualunque sia la loro dimensione), il livello di sicurezza più adeguato per la loro infrastruttura IT.
- **Garantisce il rispetto completo delle politiche e ottimizza la produttività degli impiegati.** L'amministratore può distribuire le politiche su ogni PC, e bloccare l'uso di specifiche applicazioni o file direttamente dalla console.
- **Semplifica la gestione del rischio.** Le soluzioni Corporate dispongono di analisi approfondite automatiche in grado di rilevare il malware invisibile alle analisi ordinarie.
- **Protegge i beni aziendali più critici.** Le tecnologie preventive garantiscono un livello di protezione ulteriore contro ogni tipologia di malware sconosciuto, minacce provenienti da Internet e contro attacchi mirati.

Funzionalità chiave

- **Console centralizzata** per gestire tutti i moduli di protezione da un singolo PC. **Un cruscotto per i dati** fornisce informazioni in tempo reale.
- **La tecnologia preventiva più avanzata** composta da prevenzione delle intrusioni, rilevazione preventiva e analisi comportamentale.
- **Analisi approfondite del malware** e servizio di **disinfezione** anche nei confronti di minacce nascoste e di nuova generazione.
- **Controllo degli accessi alla rete** per impedire il collegamento alla rete aziendale di PC infetti, non sicuri o potenzialmente pericolosi rispetto alle politiche di sicurezza dell'azienda, evitando la contaminazione dei file e dei dati presenti.
- **Anti-Spam per desktop, e-mail server e MTA generici**, per eliminare la posta indesiderata.
- **Filtro dei Contenuti completo.** Una barriera contro virus e spam, sia per la posta in ingresso che in uscita.
- **Controllo delle applicazioni** che consente all'amministratore di gestire in maniera totale le risorse di rete e dei singoli endpoint.
- **Ampia gamma di report dettagliati delle attività** che possono essere personalizzati e configurati per un invio periodico di dati e report all'amministratore.
- **Protezione Anti-Malware e filtro dei contenuti per Microsoft ISA Server.** Assicura la robustezza delle vostre politiche di sicurezza. Impedisce la diffusione di infezioni all'interno delle reti aziendali.

Console centralizzata all-in-one

**Panda AdminSecure** è lo strumento di amministrazione centralizzata per Panda Security for Enterprise. Il suo cruscotto di controllo (Dashboard) garantisce un monitoraggio e un controllo della sicurezza e del livello di rischio di tutti i sistemi in rete, in tempo reale: workstation, portatili, file server, mail server, gateway, firewall, etc..

**AdminSecure** si adegua alla struttura della vostra azienda, permettendo una semplice e veloce installazione, gestione, manutenzione e supervisione dei moduli di protezione installati nella vostra rete, a prescindere dalla lingua o dal numero di computer e piattaforme protette.

La più avanzata tecnologia preventiva

Tutte le soluzioni disponibili in Panda Security for Enterprise adottano le tecnologie preventive più avanzate e premiate che si basano su processi automatici e che non richiedono l'intervento dell'utente. La suite comprende un motore genetico euristico (GHE) e la capacità di analizzare e bloccare comportamenti anomali del malware noto o sconosciuto: **Tecnologie TruPrevent.**

Basata sul nostro modello dell'**Intelligenza Collettiva**, si completa e rafforza la vostra protezione contro minacce nascoste senza infrastrutture o componenti aggiuntivi.

**Panda Malware Radar** consente di effettuare audit automatici della vostra rete e di ottenere report dettagliati con risultati e suggerimenti, offrendo la possibilità di automatizzare la disinfezione.

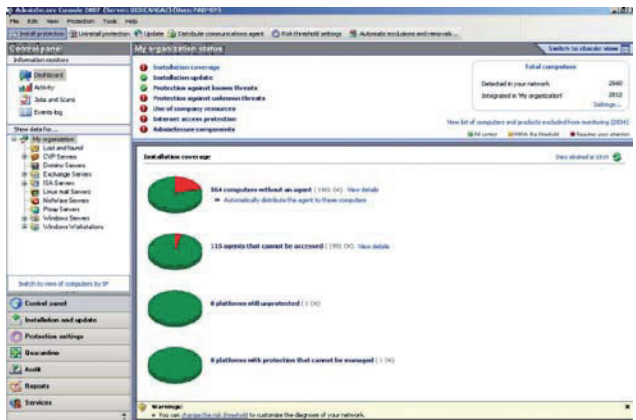
Controllo degli accessi alla rete

Panda è l'unico vendor di sicurezza che include un controllo degli accessi in rete di default. Questo modulo consente di non compromettere lo stato della rete quando utenti esterni vi si collegano. Esso analizza ogni computer che tenta/richiede di collegarsi alla rete per determinare se il suo antivirus (qualsiasi antivirus) è adeguatamente aggiornato o meno. Se l'esito è "no", il computer non potrà collegarsi alla rete.

Anti-Spam per desktop, email server e MTA

Panda Security for Enterprise è l'unica soluzione dotata di un modulo Anti-Spam per desktop, email server (Exchange e Domino) e MTA (Qmail, SendMail e Postfix) che contribuiscono a incrementare la produttività e la disponibilità di banda di rete.

I motori Anti-Spam inclusi in Panda Security for Enterprise offrono una velocità di rilevazione sempre superiore al 95%.



Controllo delle applicazioni

L'uso di alcune applicazioni potrebbe essere una minaccia per la sicurezza o causare perdite di produttività per le aziende. Grazie al controllo delle applicazioni, gli amministratori potranno decidere quali applicazioni autorizzare e quali escludere dall'uso all'interno della rete aziendale.

Filtro dei contenuti completo

Blocco preventivo di virus e spam su server Exchange sia per l'email in uscita che in ingresso. I filtri dei contenuti agiscono sia sul contenuto, sulle informazioni presenti nel corpo dei messaggi, sia sulla Header del messaggio (es.: l'oggetto); inoltre classifica, accetta o rifiuta un messaggio.

Report dettagliati

Gli amministratori possono ricevere report completi che riportino le attività di protezione svolte nelle reti gestite in un formato molto semplice e intuitivo. Inoltre è disponibile un lungo elenco di report predefiniti, da cui l'amministratore può realizzare dei report ulteriormente personalizzati.

È possibile configurare l'invio regolare di report via email a indirizzi specifici.

Protezione Anti-Malware e filtro dei contenuti per Microsoft ISA Server

Assicura la robustezza e l'efficacia delle vostre politiche di sicurezza. Impedisce o limita la diffusione di infezioni all'interno della rete. Analizza file di qualsiasi formato, inviato e ricevuto. Si basa sul filtro Web (ISAPI) e su un filtro per applicazioni su protocolli http, SMTP e FTP (via HTTP).



TruPrevent: Protezione intelligente basata sul comportamento

Come parte della protezione preventiva più avanzata Panda Security utilizza in tutte le sue soluzioni le Tecnologie TruPrevent.

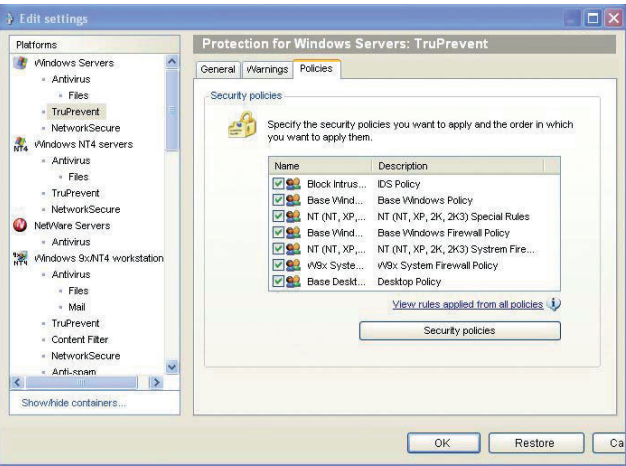
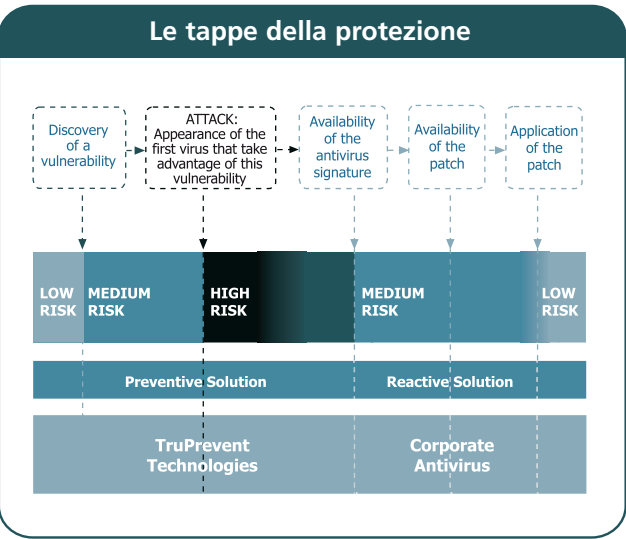
Grazie alla loro capacità di rilevare anomalie nei comportamenti, le Tecnologie TruPrevent sono le prime della loro categoria capaci di prevenire effettivamente interruzioni di servizio a causa di intrusioni o malware sconosciuto. Queste tecnologie innovative e altamente performanti riducono il rischio di infezione e i costi ad esso associati.

Le Tecnologie TruPrevent sono la soluzione per workstation e server che bloccano e identificano automaticamente: worm, virus, spyware e il nuovo malware che ha eluso gli altri sistemi di protezione, perché non completamente aggiornati o perché hanno semplicemente notificato all'amministratore possibili attacchi in corso anziché agire direttamente.

Attivare le Tecnologie TruPrevent porta alle aziende i seguenti benefici:

- Riduzione del rischio causato dalle vulnerabilità attraverso la prevenzione da nuove infezioni che spesso usano falle di sicurezza dei sistemi prima che sia disponibile una patch.
- Tutela del livello di sicurezza della vostra rete bloccando gli attacchi di hacker, il furto di dati sensibili e le infezioni causate da computer non gestiti internamente: accessi WiFi e consulenti esterni.
- Gestione flessibile delle politiche di sicurezza per personalizzare e rafforzare le regole aziendali nei confronti di tutta la rete, prevenzione dal furto intenzionale di dati sensibili o informazioni confidenziali a opera di dipendenti.

Le Tecnologie TruPrevent sono il complemento perfetto per arricchire un antivirus di un livello di protezione intelligente che massimizzi la capacità di rilevazione di qualsiasi nuovo virus o intrusione.



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