

Requisiti tecnici

Panda AdminSecure

Server di Amministrazione

Pentium III 800 MHz
256 MB RAM
Hard disk: 25 MB + 120 MB (Database) per una rete di 1000 PC

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

Panda Security for Desktops

Pentium 300 MHz (o superiore)
64 MB RAM per le funzionalità antivirus. Raccomandati 128 MB
128 MB RAM per le funzionalità antivirus + Tecnologie TruPrevent.
Raccomandati 512 MB
Hard disk: 200 MB.
Outlook 4 o superiore
Tecnologie TruPrevent non supportate su sistemi a 64 bit

Sistemi operativi

Windows 2000, XP, Vista SP2, Windows 7 (32 e 64 bit). WEPOS 1.1, Tablet PC e WEPOS Ready 2009

Panda Security for Commandline

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

Sistemi operativi

Debian4 o superiore, RedHat Enterprise 4, Mandrake 10.1/Mandriva 2006,
Ubuntu 6.06, Fedora Core 5, CentOS 4.6, Windows 2000/XP/Windows Server 2003 (Enterprise Edition)/Vista, Suse 10.0

Panda Security for File Server

Windows Server
Pentium 300 MHz o superiore
RAM AV 256 MB
RAM AV + TP: 256 MB. Raccomandati 512 MB
Hard disk: 160 MB
TruPrevent non supportate su 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 SBS 2008 (32 e 64 bit), Windows Server 2008 R2 (64 bit)

Panda Security for Exchange

For Exchange Server 2000/2003

Pentium II 500 MHz o superiore
Almeno 256 MB RAM
Hard Disk: 200 MB

Sistemi operativi

Windows 2000 Server (SP3 o superiore), 2000 Advanced Server, Windows Server 2003 Enterprise Edition, Server 2003 R2, Windows Server 2003 Standard Edition, Windows Server 2003 Datacenter Edition

Applicazioni

Microsoft Exchange Server 2000 SP1 o successivi, compreso il cluster, Exchange Server 2003 SP1 o superiore

Exchange Server 2007/2010

Processore Intel con EM64 o AMD con piattaforme AMD64
Minimo 2 GB RAM (4 GB per il 2010)
Hard disk: 250 MB

Sistemi operativi

Windows Server 2003 64 bit SP1 o superiore, Windows Server 2008 64 bit, Windows Server 2008 64 bit SP2

Applicazioni

Microsoft Exchange Server 2007 e Exchange 2007 SP1/SP2 e Exchange 2010

Panda Security for Linux

Pentium III o superiore 800 MHz (o AMD)
256 MB RAM
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 Server

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

Oggi il 95% delle aziende ha installato un antivirus sui propri endpoint in rete, ma il 72% di questi è comunque infetto

Tutte le aziende hanno installato una soluzione di sicurezza con modulo antispam per proteggere la propria rete. Di conseguenza molte di loro si ritengono adeguatamente protette. Purtroppo la realtà è ben diversa, una percentuale molto elevata tra queste risulta comunque infetta dal malware.

Al contrario di quanto possa sembrare, queste infezioni sono particolarmente pericolose per le aziende e le loro finanze, Gartner sostiene che circa la metà delle aziende ha dovuto chiudere gli accessi a Internet per la quantità e la gravità degli attacchi subiti causando sensibili perdite di utili. Inoltre, lo spam è una delle principali cause di perdita di produttività e consumo di risorse di sistemi aziendali.

Ciò significa che le protezioni tradizionali non sono più sufficienti per le attuali esigenze di sicurezza.

“Circa il 50% delle PMI è costretto a bloccare gli accessi esterni alla rete a causa degli attacchi; per molte imprese, questa situazione causa significative perdite di denaro”. Gartner: User Survey Analysis: IT Security Opportunities in the SMB Market, North America, 2007.

La soluzione: Panda Security for Business with Exchange

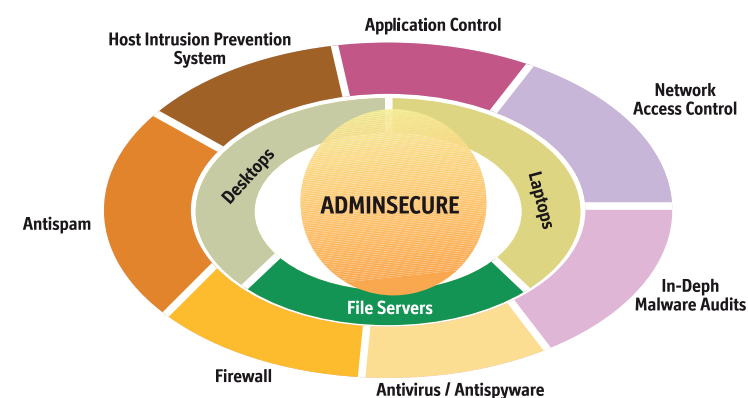
Panda Security for Business with Exchange fornisce la **protezione migliore per i tuoi asset aziendali** contro le minacce attuali e future.

Basata sulla combinazione di una **protezione preventiva** (TruPrevent) per endpoint e di **analisi approfondite** periodiche (Malware Radar), Panda Security for Business offre realmente una soluzione preventiva completa contro le minacce note e sconosciute.

La **console centralizzata** (AdminSecure) consente agli amministratori di gestire al meglio il livello di protezione per la rete aziendale in maniera **molto semplice**, supportati da una wizard (utilità di configurazione guidata) per attivare la protezione più aderente alle esigenze di ogni computer.

Panda Security for Business with Exchange è l'unica soluzione che include, **al prezzo di una singola suite**, tutte le tipologie di protezione per aziende come il sistema di prevenzione delle intrusioni (HIPS), l'audit approfondito contro gli attacchi mirati, la gestione delle applicazioni e il controllo degli accessi alla rete aziendale.

Questa soluzione si avvale del nostro modello dell'**Intelligenza Collettiva**, in grado di incrementare l'efficienza di rilevazione, elevando il livello di protezione nei confronti delle minacce sconosciute.



“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 del 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, dalle minacce provenienti da Internet agli 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 di PC infetti, non sicuri o potenzialmente pericolosi rispetto alle politiche di sicurezza dell'azienda, evitando la contaminazione dei file e dei dati presenti.
- **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.
- **Anti-Spam per desktop ed Exchange Server**, per eliminare la posta indesiderata.
- **Filtro dei contenuti completo**, Una barriera contro virus e spam, sia per la posta in ingresso che in uscita.
- **Quarantena gestita centralmente** che gli amministratori possono gestire, controllando file sospetti e definire le azioni da svolgere. E' possibile inoltre inviare i file sospetti ai PandaLabs per la loro analisi.
- **Monitoraggio e notifiche di anomalie in tempo reale** circa lo stato della sicurezza e delle performance dei server di amministrazione e distribuzione.

Console centralizzata all-in-one

Panda AdminSecure è lo strumento di amministrazione centralizzata per Panda Security for Business. 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 e Exchange Server.

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

Panda Security for Business with Exchange adotta le tecnologie preventive più avanzate e premiate che si basano su processi automatici e 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.**

Audit approfonditi del malware

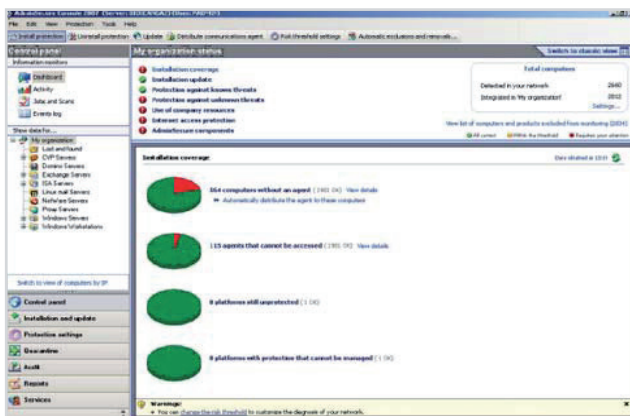
Panda Malware Radar è un'analisi automatizzata in grado di identificare le infezioni che le soluzioni tradizionali non rilevano.

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

Malware Radar fornisce un audit automatico della vostra rete e report dettagliati con dati e raccomandazioni, con l'opzione di automatizzare anche il processo di disinfezione del malware rilevato.

Controllo degli accessi in 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.



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.

Report dettagliati

Gli amministratori possono ricevere report completi che riportano 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 report ulteriormente personalizzati.

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

Anti-Spam per desktop

Panda Security for Business è l'unica soluzione dotata di un modulo Anti-Spam per desktop che contribuisce a incrementare la produttività e la disponibilità di banda di rete.

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

Quarantena gestita centralmente

Se viene rilevata una nuova minaccia, i file sospetti vengono posti in quarantena per evitare eventuali danni. Essi vengono anche inviati automaticamente ad AdminSecure o ai PandaLabs per verifica.

Monitoraggio di notifiche e malfunzionamenti in tempo reale

Panda Security for Business with Exchange permette di operare in automatico per monitorare con continuità lo stato della rete e le performance dei server di amministrazione e di distribuzione. Inoltre consente di inviare via email in tempo reale, per notifica, eventuali malfunzionamenti.

Filtro dei contenuti completo

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



TruPrevent: Protezione intelligente basata sul comportamento

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

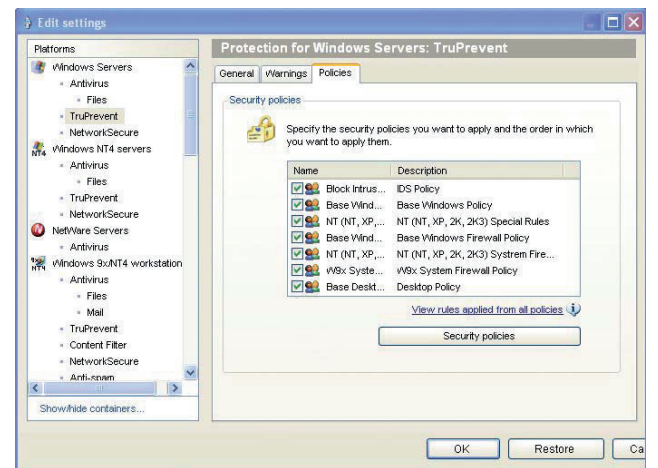
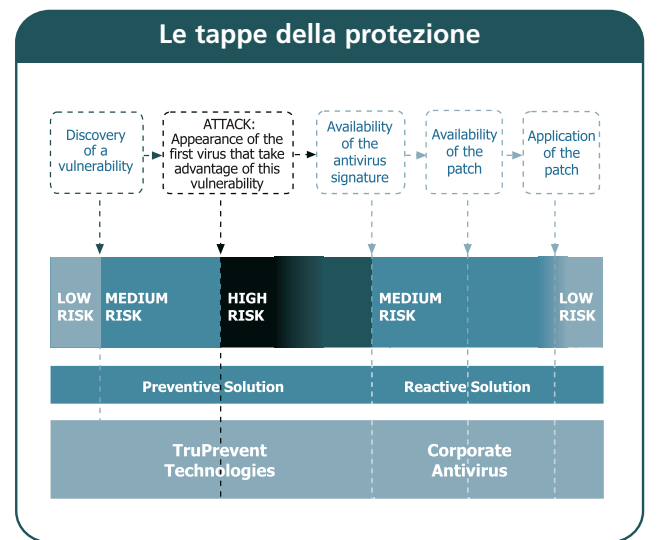
Grazie alla loro capacità di rilevare anomalie nei comportamenti, le Tecnologie TruPrevent sono le prime, della loro categoria, capaci di prevenire effettivamente interruzioni di servizio a causa di intrusioni o malware sconosciuto. Queste tecnologie innovative e altamente performanti riducono il rischio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