

## Requerimientos técnicos

### Panda AdminSecure

#### Administration Server:

Pentium III 800 MHz  
RAM: 256MB  
Disco Duro: 25 MB + 120 MB (DDBB) para un red de 1000 ordenadores

#### Repository Server

Pentium III 800 MHz  
RAM: 128MB  
Disco Duro: 520MB

#### Communications Agent

Pentium 133 MHz  
RAM: 64MB  
Disco Duro: 40MB  
Internet Explorer 5.5

#### Consola

Pentium II 266 MHz o superior  
RAM: 140MB  
Disco Duro: 140MB  
Internet Explorer 5.5  
Windows installer 2.0

**Sistemas operativos:** Windows 2000 / XP / Vista (32 y 64bits), Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Server 2008 (32 y 64 bits)

#### Panda Security for Desktops

Pentium 300MHz o superior  
RAM Antivirus: 64MB. Recomendado: 128MB  
RAM Antivirus + TruPrevent: 128MB. Recomendado 512MB  
Disco Duro: 200MB  
Outlook 4 o superior  
Las tecnologías TruPrevent no soportan sistemas de 64 bits  
**Sistemas Operativos:** Windows 2000, XP, Vista SP2, Windows7 (32 y 64 bits), WEPOS 1.1, Tablet PC y WEPOS Ready 2009

#### Panda Security Commandline

Pentium/Athlon o superior  
Minimum RAM: 128MB  
Disco Duro: 120MB  
**Sistemas Operativos:** : Debian 4, Red Hat 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

#### Panda Security for File Servers

Pentium 300 MHz o superior  
RAM Antivirus: 256 MB  
RAM Antivirus + TruPrevent: 256MB. Recomendado: 512MB  
Disco Duro: 160MB  
Las tecnologías TruPrevent no soportan sistemas de 64 bits  
**Sistemas Operativos:** Windows server 2000 Domain Controller, StandAlone, Terminal server, SB server y cluster. Windows Server 2003 (32 y 64 bits) Enterprise Edition, SB server, SP1, SP2 y cluster, Windows server 2003 R2(32 y 64bits), windows server 2008/R2 (32 y 64bits), windows SBS 2008 (32 y 64 bits)

#### Panda Security for Exchange

Exchange Server 2000/2003  
Pentium II 500MHz o superior  
RAM: 512MB for 2000 y 1GB para 2003  
Disco Duro: 200MB

**Sistemas Operativos (2000):** Windows 2000 Server (SP3), 2000 Advanced Server con SP3 o posterior, Windows Server 2003

Standard Edition, Windows Server 2003 Enterprise Edition SP1 Server 2003 R2  
Aplicaciones: Microsoft Exchange server 2000 SP1, including cluster, Exchange server 2003 SP1

#### Exchange Server 2007/2010

Procesor Intel con Intel Extended Memory 64 o AMD con AMD64 platforms  
RAM: 2GB minimo (4GB para 2010).  
Disco Duro: 250MB  
**Sistemas Operativos:** Windows Server 2003 x64 o Windows server 2003 R2 x64, Windows Server 2008 (Exchange 2007 SP1, SP2)  
Aplicaciones: Microsoft Exchange server 2007 SP1/ SP2, Exchange 2010.

#### Panda Security for Domino Servers

Pentium 133 o superior  
RAM: 256MB  
Disco Duro: 200MB  
**Sistemas Operativos:** Microsoft Windows 2000 server SP1, Windows 2003 server, Windows 2003 Server SP1, Windows 2003 Server R2  
Aplicaciones: Lotus Domino 4.5 o superior (8.5 incluido)

#### Panda Security for ISA Servers

**ISA Server 2004 Standard**  
Pentium III 550MHz o superior  
RAM: 1GB  
Particion Local NTFS con 200MB de disco duro mas 60MB para el cache web content

#### ISA Server 2004 Enterprise

Pentium III 550MHz o superior  
RAM 1GB  
Particion Local NTFS con 200MB de disco duro mas 60MB para el cache web content

#### ISA Server 2006 Standard or Enterprise

Pentium III 733MHz  
RAM 1GB  
Particion Local NTFS con 200MB de disco duro mas 60MB para el cache web content  
**Sistemas Operativos:** Windows Server 2003 SP1, Windows Server 2003 R2, ISA Server 2006

#### Panda Security for Qmail, Panda Security for SendMail y Panda Security for PostFix

Pentium III 868MHz  
RAM: 512MB. Recomendado 1GB  
Disco Duro: 5GB

#### Panda Security for Linux

Pentium III o superior 800 MHz (o AMD).  
RAM: 256 MB  
Disco Duro: 200MB

**Distribuciones soportadas:** Debian 3.1, 4, 5, Ubuntu 7.04, 9.10, OpenSUSE 10.1,10.2, 11.2 y Enterprise 10, Fedora Core 6, Red Hat Enterprise 4 (Desktop, Workstation, Server) y 5 (Client), Mandriva 2007.1

#### Panda Security for Linux Servers

Pentium II o AMD 400 MHz (o superior)  
RAM: 128 MB  
Disco Duro: 150MB

**Distribuciones soportadas:** Red Hat Enterprise Linux 5 Server y Workstation 4, Advanced Server, Enterprise Server y Workstation. OpenSUSE 10.1,10.2, 11.2 y Enterprise 10, Ubuntu 7.04, 9.10, Debian 3.1, 4, 5

*\*Las protecciones para Linux no están administradas por Adminsecure.*

Los ataques de malware cuestan el 2,2% de los ingresos anuales de las grandes empresas, a pesar de que tienen instaladas soluciones tradicionales de seguridad.

Todas las grandes empresas tienen instaladas soluciones de seguridad tradicionales para proteger su red. Al disponer de esta protección, probablemente estén protegidas frente a los ataques masivos de malware pero siguen siendo vulnerables frente a las amenazas de malware silenciosos o ataques dirigidos.

De hecho, en 2007 los efectos de los ataques de malware en las grandes empresas alcanzan el 2,2% de sus ingresos anuales. En muchos casos, los ataques de malware toman recursos de la red o apagan ordenadores, causando importantes pérdidas de productividad. Pero en muchos otros casos las empresas pueden enfrentarse a amenazas más silenciosas, como los ataques dirigidos que pasan desapercibidos a las soluciones de seguridad tradicionales basadas en el reconocimiento de firmas. Las empresas de antivirus que continúan protegiendo a sus clientes con modelos tradicionales no pueden ofrecer una protección completa debido al crecimiento exponencial en la creación de malware.

Las grandes empresas necesitan soluciones completas que les permitan gestionar las situaciones de riesgo con métodos proactivos y preventivos. Debido al escenario actual del malware, las empresas necesitan adaptar sus políticas de seguridad para cumplir con las normativas.

Las estrategias de seguridad de la red están convirtiéndose, cada vez más, en parte de la actividad corporativa, ya que ayudan a evitar pérdidas en los beneficios. Una estrategia de seguridad adecuada puede aumentar los beneficios de una actividad reduciendo los riesgos.

**"Las grandes empresas comprueban el malware del cliente a menudo, pero continúan plagados tanto de ataques de DOS como de malware de servidores. En muchos casos, poseen una infraestructura que favorece el rasteo en los momentos de inactividad. Las grandes empresas son también el foco de la mayoría de los ataques dirigidos"**  
*Infonetics: The Cost of Network Security Attacks: Noth America 2007 (Infonetics Research).*

## La solución: Panda Security for Enterprise

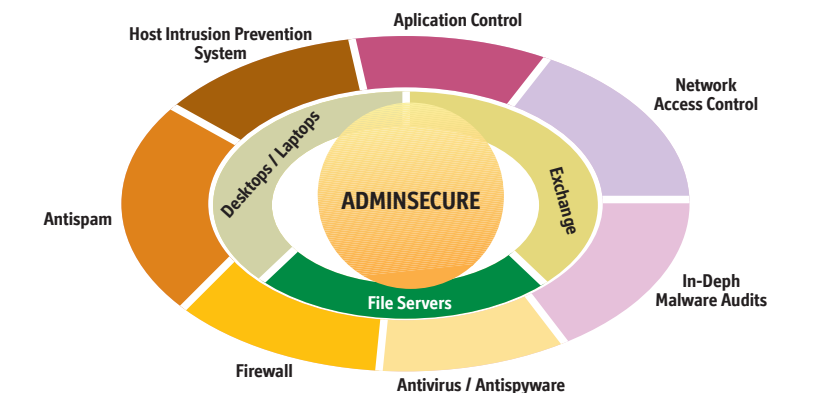
Panda Security for Enterprise proporciona la **protección proactiva** más avanzada con una arquitectura **flexible con múltiples niveles** y en todas las capas de la red. Entre sus funciones se incluyen el acceso a la red y el control de la aplicación.

Panda Security for Enterprise ofrece una solución de prevención completa frente a amenazas conocidas y desconocidas, basada en una combinación de **tecnologías proactivas** (TruPrevent) con múltiples niveles, y **auditorías exhaustivas** y periódicas (Malware Radar).

Panda Security for Enterprise incluye protección para estaciones de trabajo, usuarios en tránsito, servidores de ficheros, servidores de correo electrónico (Exchange, Domino), servidores ISA y MTAs.

La **consola centralizada** (AdminSecure) unifica la información de todas las protecciones y permite a los administradores gestionar el riesgo a través de informes en tiempo real para que estén alerta constantemente frente a las amenazas.

Panda Security for Enterprise es la **única** solución que abarca todos los tipos de protección necesarios en una **única solución; así elimina la necesidad de comprar complementos de seguridad adicionales en el futuro.**



**"El mejor ejemplo de fabricante que haya realizado un avance revolucionario para ofrecer al cliente individual toda una serie de soluciones HIPS es Panda, que tiene el precio de una única solución y abarca ocho de los nueve tipos de protección destacados en nuestro informe sobre HIPS."**  
*Gartner: How to Get Free Anti-spyware (or Antivirus) Protection.*

## Principales beneficios

- **Control completo y centralizado.** La consola de gestión Adminsecure permite al administrador gestionar la seguridad global de su red desde uno o varios puntos, optimizando la productividad de los puestos y permitiendo la aplicación de políticas centralizadas.
- **Solución de seguridad eficiente.** Los diferentes módulos incluidos en cada solución permiten ofrecer a cada empresa, independientemente del tamaño que tenga, el nivel de seguridad adecuado a la estructura de sus sistemas.
- **Favorece el cumplimiento de políticas corporativas y optimiza la productividad de los empleados** Desde la consola central el administrador puede distribuir políticas a los puestos así como bloquear el acceso a aplicaciones o archivos no permitidos.
- **Facilita la gestión de riesgos.** Las soluciones corporativas permiten realizar auditorías automáticas en profundidad para detectar malware escondido.
- **Protege los activos críticos de la compañía.** Las tecnologías proactivas ofrecen una capa complementaria de protección contra todo tipo de malware.
- **Servicios completos.** Nuestras soluciones corporativas incluyen una completa asistencia 24 horas al día, 7 días a la semana y eso durante todo el año.

## Prestaciones fundamentales

- **Consola centralizada unificada** que facilita la gestión de todas las protecciones desde un sólo punto. Un cuadro de mandos ofrece información en tiempo real
- **La tecnología proactiva más avanzada** para la prevención de intrusiones, detección proactiva y análisis de comportamiento.
- **Auditorías de malware exhaustivas** y servicio de desinfección capaz de descubrir avanzadas amenazas ocultas que pasan desapercibidas.
- **Control de acceso a la red** para evitar que estaciones infectadas, inseguras o peligrosas se conecten a la red y contaminen los ficheros y la información.
- **Anti-spam en estaciones de trabajo servidores de correo y MTAs** para eliminar el correo no deseado.
- **Bloqueo exhaustivo de contenidos** exhaustivo filtrado de contenidos para el bloqueo preventivo de virus y spam, tanto en el correo electrónico de entrada como en el de salida.
- **Control de la aplicación** con el que los administradores controlan totalmente los estaciones y los recursos de la red.
- **Ámplio abanico de informes detallados** sobre la actividad de detección que pueden personalizarse y configurarse.
- **Protección antimulware y filtrado de contenidos para servidores Microsoft ISA.** Compruebe la consistencia de las políticas de seguridad. Impida la propagación de infecciones en la red local.

## Consola centralizada unificada

**Panda AdminSecure** es la herramienta de administración centralizada de las soluciones corporativas de Panda Security for Enterprise. Su cuadro de mandos ofrece la posibilidad de monitorizar y controlar en tiempo real la seguridad y el nivel de riesgo de todos los elementos de la red: estaciones, portátiles, servidores de ficheros, servidores de correo y pasarelas, cortafuegos, etc.

**AdminSecure** se adapta a la estructura organizativa de su empresa, permitiéndole instalar, gestionar, mantener y supervisar, con toda comodidad y sencillez, el sistema de protección instalado en toda la red, cualquiera que sea el idioma o el número de equipos y plataformas que deben protegerse.

## La tecnología proactiva más avanzada

Todas las soluciones de Panda Security for Enterprise incorporan las tecnologías proactivas más avanzadas y mejor valoradas que utilizan procesos automáticos sin la intervención del usuario. Esta tecnología incluye un motor de análisis heurístico genético, el bloqueo por comportamiento y el análisis de comportamiento de malware conocido y desconocido: **Tecnologías TruPrevent**.

## Auditorias de malware exhaustivas

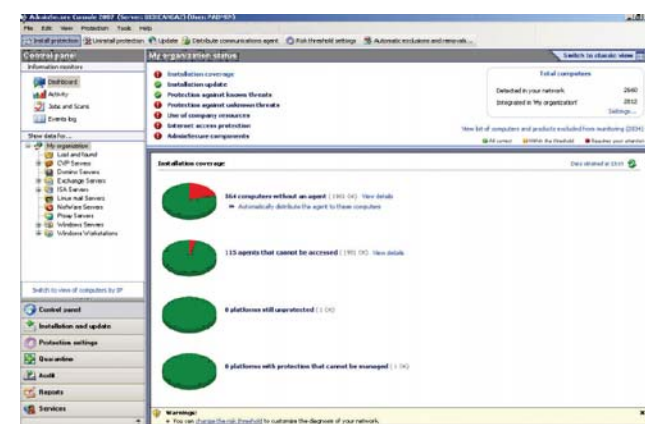
**Panda Malware Radar** es una auditoría automatizada que localiza los puntos de infección que las herramientas de seguridad tradicionales no detectan.

Se basa en el enfoque de la **Inteligencia Colectiva** y complementa y ayuda a optimizar su protección contra amenazas ocultas sin necesidad de componentes o infraestructura adicional.

**Malware Radar** le permite auditar automáticamente su red y le facilita informes detallados con los resultados y las recomendaciones, además le ofrece la opción de automatizar rutinas de desinfección de malware.

## Control de acceso a la red

Panda es el único fabricante de seguridad que incluye la opción del control de acceso a la red por defecto (NetworkSecure). Esta característica garantiza que no accedan usuarios peligrosos a la red. Analiza cualquier ordenador que intente acceder a la red para determinar si su antivirus (cualquiera que sea) está debidamente actualizado. Si la respuesta es negativa, no dejará a ese ordenador acceder a la red.



## Anti-spam en estaciones de trabajo

Panda Security for Enterprise es la única solución que incluye una opción anti-spam para estaciones de trabajo, servidores de correo (Exchange y Domino) y MTAs (Qmail, Sendmail y Postfix) lo que permite a las empresas aumentar la productividad y la capacidad del ancho de banda.

Los motores anti-spam incluidos en Panda security for Business ofrecen ratios de detección superiores al 95%.

## Control de la aplicación

La utilización de determinadas aplicaciones podría plantear amenazas de seguridad o causar pérdidas de productividad para las empresas. Gracias al Control de aplicación los administradores pueden bloquear las aplicaciones que no se pueden utilizar.

## Bloqueo exhaustivo de contenidos

Exhaustivo filtrado de contenidos en Exchange para el bloqueo preventivo de virus y spam, tanto en el correo electrónico de entrada como en el de salida. El filtro de contenido actúa tanto en el contenido, como en la información del cuerpo del correo, así como en su cabecera (ej. "Asunto") para clasificar, aceptar o rechazar el mensaje.

## Informes detallados

Los administradores pueden obtener informes completos que muestran la actividad de seguridad de las redes, en diferentes formatos y muy fáciles de utilizar. A pesar de que existe una larga lista de informes predefinidos, el administrador puede personalizar sus informes.

Los informes pueden configurarse para que sean enviados periódicamente, por correo electrónico, a direcciones de e-mail concretas.

## Protección antimalware y filtrado de contenidos para servidores Microsoft ISA

Compruebe la consistencia de las políticas de seguridad. Impida la propagación de infecciones en la red local. Maximice el retorno de la inversión. Panda Security for Enterprise analiza y desinfecta todos los formatos de ficheros enviados y recibidos. Para esto, se usa un filtro web (ISAPI) y un filtro de aplicación a través de los protocolos HTTP, SMTP y FTP (sobre HTTP).



## TruPrevent: Protección inteligente basada en comportamiento

Panda Security ofrece la protección proactiva más avanzada con la incorporación de las Tecnologías TruPrevent en todas sus soluciones.

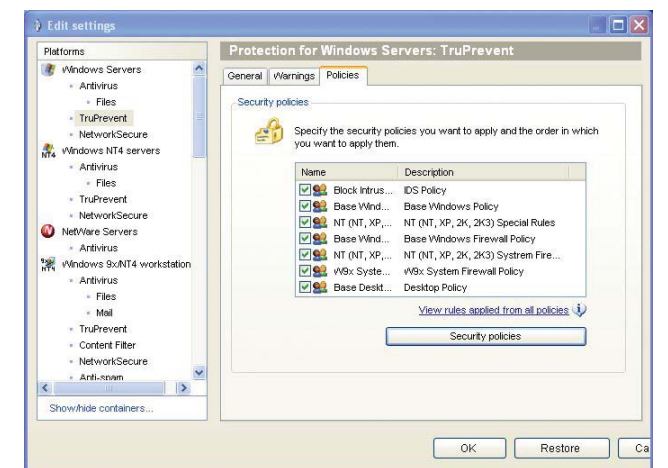
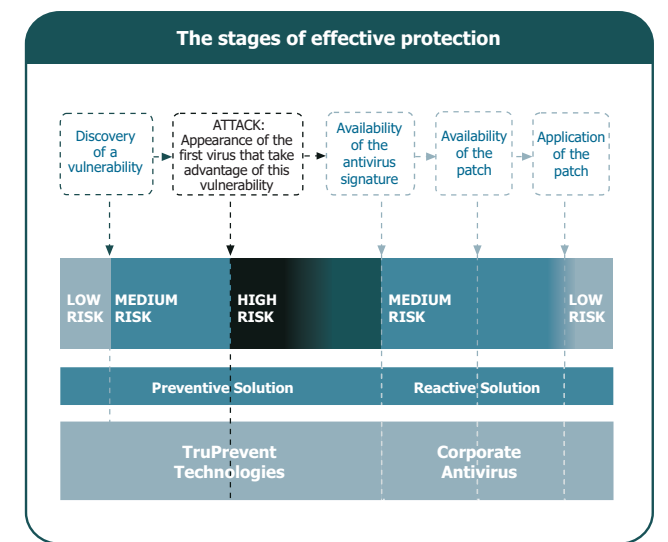
Gracias a su capacidad de detectar anomalías de comportamiento, las Tecnologías TruPrevent son las primeras de su tipo capaces de prevenir de forma efectiva las interrupciones de servicio causadas por intrusiones y cualquier tipo de malware desconocido. Estas tecnologías innovadoras y de alto rendimiento reducen el riesgo de sufrir infecciones y los costes asociados a las mismas.

Las Tecnologías TruPrevent son la solución ideal para estaciones y servidores, ya que identifican y bloquean de forma precisa y automática gusanos, virus de red, spyware y cualquier otro tipo de malware desconocido que haya conseguido burlar otras protecciones, ya sea porque no estén completamente actualizadas o porque, en lugar de actuar sobre el malware, se limiten a informar al administrador sobre los posibles ataques.

Con las Tecnologías TruPrevent, las organizaciones se benefician de:

- Reducción de la ventana de riesgo abierta por las vulnerabilidades, al prevenir las infecciones que explotan agujeros de seguridad antes de la aplicación de los parches correspondientes.
- Mantenimiento del nivel de seguridad de la red mediante el bloqueo de ataques de hackers, robo de información confidencial y las infecciones generadas por ordenadores no gestionados de forma interna: accesos Wi-Fi y consultores externos.
- Gestión flexible de políticas de seguridad para personalizar y reforzar las reglas de seguridad por toda la red, impidiendo el robo de información confidencial por parte de empleados desleales.

Las Tecnologías TruPrevent resultan el complemento perfecto para el antivirus, ya que proporcionan una capa de protección inteligente que maximiza la capacidad de detectar cualquier tipo de nuevo virus o intruso.



		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	✓	✓	✓