

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  
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 64bits, Windows Server 2008 (32 y 64bits)

**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 NT/2000/XP/Windows Server 2003 (Enterprise Edition) / Vista, Suse 10.0

**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 (32 y 64 bits), windows SBS 2008 (32 y 64 bits), Windows Server 2008 R2 (64bits)

**Panda Security for Exchange**

**Exchange Server 2000/2003**

Pentium II 500MHz o superior  
RAM: Al menos 256 MB  
Disco Duro: 200MB

**Sistemas Operativos (2000):** Windows 2000 Server (SP3 o superior), 2000 Advanced server, Windows Server 2003 Enterprise Edition RC2 Server 2003 R2, Windows Server 2003 Standard Edition, Windows Server 2003 Datacenter Edition  
Aplicaciones: Microsoft Server 2000 SP1 o superior, Microsoft Server 2003 SP1 o superior

**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 64 bits SP1 o superior, Windows server 2008 64 bits, Windows Server 2008 64 bits SP2  
Aplicaciones: Microsoft Exchange server 2007 y Microsoft Exchange Server 2007 SP1/SP2, Exchange 2010.

**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 de Linux no están administradas desde Adminsecure.

El 95% de las empresas tienen, a día de hoy, un antivirus y un antispam instalado en sus estaciones, pero el 72% siguen infectadas.

Prácticamente todas las empresas tienen algún tipo de solución de seguridad instalada para su protección. La mayoría de estas empresas se sienten protegidas sólo por tener un antivirus instalado. Sin embargo, la realidad es que un porcentaje bastante alto siguen infectadas por malware.

A pesar de que estas infecciones pueden parecer inofensivas para las empresas, según Gartner, casi la mitad de las pequeñas y medianas empresas se ven obligadas a cerrar el acceso a internet debido a ataques externos de malware que causan enormes pérdidas de beneficios. Por otro lado, el spam es uno de los principales problemas que pueden producir importantes pérdidas de productividad y consumo de recursos en las empresas.

Lo que quiere decir que las protecciones tradicionales no son suficientes para reunir las necesidades de seguridad. Hoy en día, el malware está específicamente diseñado para pasar desapercibido. Es mucho más complejo y variado, e incluso, en ocasiones, está diseñado para alcanzar objetivos específicos.

**"Casi el 50% de las pequeñas y medianas empresas han tenido que cerrar su acceso externo a la red debido a los ataques recibidos; para muchas PYMEs esto puede causar importantes pérdidas en los beneficios"**  
Gartner: *User Survey Analysis: IT Security Opportunities in the SMB Market, North America, 2007.*

La solución: Panda Security for Business with Exchange

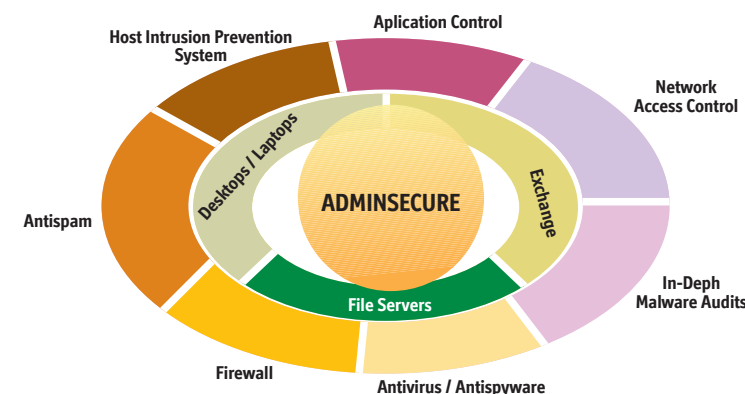
Panda Security for Business with Exchange proporciona a las empresas la **mejor protección para su principal activo** frente a amenazas presentes y futuras.

Panda Security for Business with Exchange ofrece una protección completa frente a amenazas conocidas y desconocidas, basada en una combinación de las **tecnologías proactivas** más avanzadas para estaciones (TruPrevent), y **auditorías exhaustivas** y periódicas (Malware Radar). Los motores anti-spam incluidos ofrecen ratios de detección superiores al 95%.

La **interfaz de usuario unificada** (Adminsecure) permite a los empresarios gestionar todas las protecciones de redes necesarias de una **forma realmente sencilla**, con la ayuda de un **asistente** que le ayudará a desplegar la protección más adecuada para estaciones.

Panda Security for Business with Exchange es la única solución que incluye, en un paquete de **precio único**, todas las protecciones que necesita una pequeña o mediana empresa, como el sistema de prevención de intrusiones basado en host, las auditorías exhaustivas de ataques dirigidos, la gestión de la aplicación y el control de acceso a la red.

Esta solución se beneficia de nuestra estrategia de **Inteligencia Colectiva** que aumenta la eficacia de la detección, ayudando a optimizar su protección contra amenazas desconocidas.



**"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 contra 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.
- **Control de aplicación** con el que los administradores controlan totalmente las estaciones y los recursos de la red.
- **Amplio abanico de informes detallados** sobre la actividad de detección, que pueden personalizarse y configurarse para que los administradores los reciban periódicamente.
- **Anti-spam en estaciones de trabajo y servidores Exchange** para eliminar el correo no deseado. (Incluye nueva compatibilidad con Exchange 2010).
- **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.
- **Cuarentena centralizada** que permite a los administradores controlar ficheros sospechosos y determinar las medidas que se tomarán. Incluye la posibilidad de enviar los archivos sospechosos a PandaLabs para ser analizados.
- **Supervisión y alertas de incidencias, en tiempo real,** del estado de seguridad y del rendimiento de los servidores de administración y distribución.

## Interfaz centralizada unificada

**Panda AdminSecure** es la herramienta de administración centralizada de las soluciones corporativas de Panda Security for Business with Exchange. Su cuadro de mandos ofrece la posibilidad de monitorizar y controlar, en tiempo real, los niveles de seguridad y de riesgo de todos los sistemas de redes: estaciones, portátiles, servidores de ficheros, y servidores Exchange.

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

## La tecnología proactiva más avanzada

Panda Security for Business with Exchange incluye en todas sus soluciones las tecnologías más avanzadas y mejor valoradas que utilizan procesos automáticos sin la intervención del usuario. Incluye un motor de análisis heurístico genético, el bloqueo por comportamiento y el análisis de comportamiento de malware conocido y desconocido: **Tecnologías TruPrevent**.

## Auditorías de malware exhaustivas

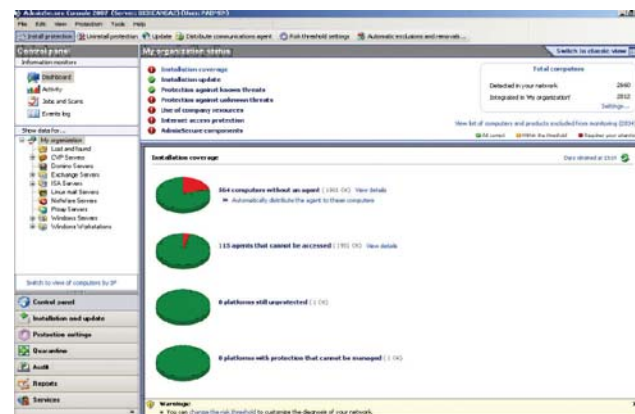
**Panda Malware Radar** es una auditoría automatizada que localiza los puntos de infección que la seguridad tradicional no detecta.

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

**Malware Radar** le permite auditar automáticamente la 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.



## 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.

## 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.

## Anti-spam en estaciones de trabajo

Panda Security for Business with Exchange es la única solución que incluye una opción anti-spam para estaciones de trabajo y servidores Exchange 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 with Exchange ofrecen ratios de detección superiores al 95%.

## Cuarentena centralizada

Si se detecta una nueva amenaza, los ficheros sospechosos pasan al estado de cuarentena para impedir que se originen daños. Además, existe la posibilidad de enviar estos ficheros sospechosos a PandaLabs para su tratamiento.

## Supervisión y alertas de incidencias en tiempo real

Panda Security for Business with Exchange facilita la toma de decisiones, en tiempo real, a través de su sistema de supervisión continua del estado de la red y del rendimiento de los servidores de administración y distribución. Además, cabe la posibilidad de enviar, en tiempo real, al administrador una alerta de incidencia a través del correo electrónico.

## 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. 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.



## 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.

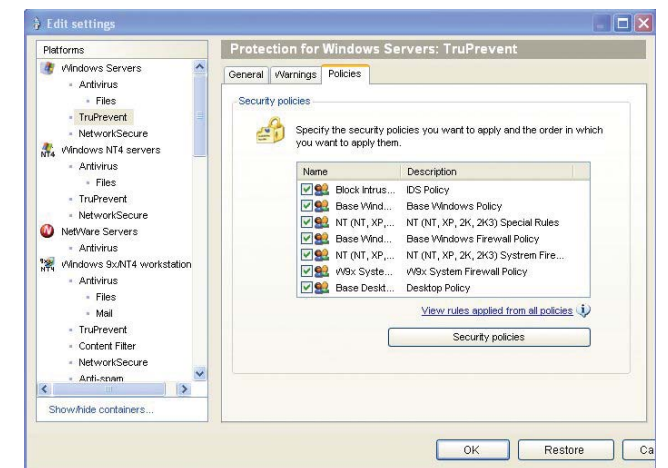
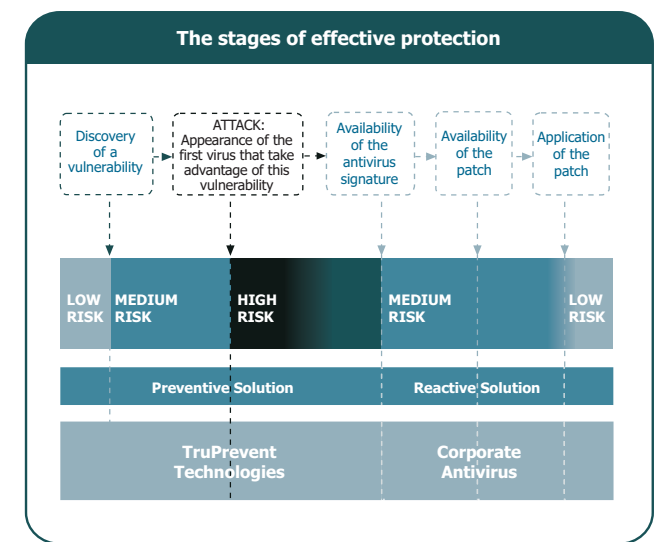
Gracias a su capacidad de detectar anomalías de comportamiento, las Tecnologías TruPrevent son las primeras de su tipo capaces de prevenir de forma efectiva las interrupciones de servicio causadas por intrusiones y cualquier tipo de malware desconocido. Estas tecnologías innovadoras y de alto rendimiento 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
<b>Console</b>	<b>AdminSecure</b>	✓	✓	✓
<b>Endpoint</b>	<b>Panda Security for Desktops</b>	✓	✓	✓
	<b>Panda Security for File Servers</b>	✓	✓	✓
	<b>Panda Security for Linux</b>	✓	✓	✓
	<b>Panda Security for Linux servers</b>	✓	✓	✓
<b>Mail</b>	<b>Panda Security for Exchange Servers</b>		✓	✓
	<b>Panda Security for Postfix</b>			✓
	<b>Panda Security for Qmail</b>			✓
	<b>Panda Security for Sendmail</b>			✓
	<b>Panda Security for Domino Servers</b>			✓
<b>Gateway</b>	<b>Panda Security for ISA Servers</b>			✓
<b>TechTools</b>	<b>Panda Security Commandline</b>	✓	✓	✓