

# Panda Software

## *Prevención de Virus e Intrusos*






# Objetivos de la reunión



- ☒ Acerca de Panda Software
- ☒ Soluciones para Grandes Empresas
- ☒ Soluciones para Application Service Providers (ASP)
- ☒ Nuevas tecnologías
- ☒ Posibles áreas de colaboración



# Acerca de Panda Software

- 
- ☒ Establecido en 1990.
  - ☒ 400 personas en España y cerca de 1000 en el mundo.
  - ☒ Tecnología propia contra virus e intrusos.
  - ☒ Oficinas locales en 47 países.
  - ☒ Empresa antivirus con mayor crecimiento a nivel mundial (IDC 2002-2003).
  - ☒ 26<sup>a</sup> empresa europea de mayor crecimiento de todos los sectores.



# Quién es Panda Software

- ☒ Una de las empresas líderes antivirus.
- ☒ Nuestra misión es ser el principal proveedor de tecnología contra virus e intrusos.



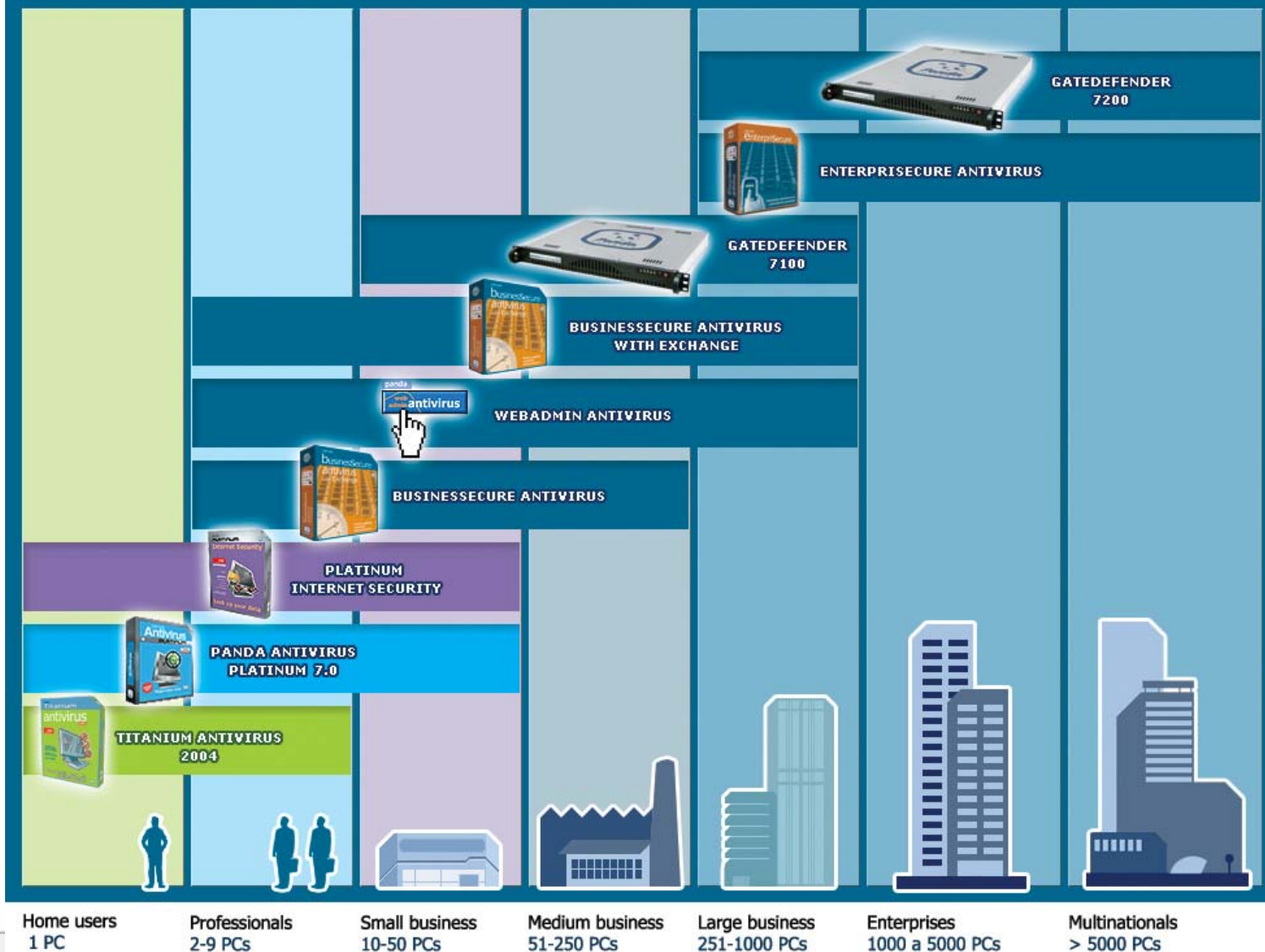
# Soluciones para Grandes Empresas





# Soluciones Panda Software

A Panda solution for every user and layer in the organization.





# Soluciones Corporativas



- Protección para toda la empresa
- Antivirus punto-a-punto, desde estaciones hasta pasarelas.
- Protege contra malware adicional y vulnerabilidades críticas
- Gestión realmente centralizada y arquitectura abierta



- GateDefender 7200. Detiene virus antes de que entren en la red.
- Analiza 7 protocolos TCP.
- Alto rendimiento (más de 200.000 mensajes por hora).
- Gestión a través de consola web.



# Soluciones Corporativas

## 1. ClientShield

Seguridad antimalware completa para estaciones (antivirus, anti-spam, anti-dialers, SmartClean2, ...)

## 2. FileSecure

Protección antivirus de alto rendimiento para servidores Win32 y Novell (certificación YES).

## 3. ExchangeSecure

Antivirus + Antispam para las plataformas Exchange

## 4. DominoSecure

Antivirus de nueva generación para Notes/Domino (certificación IBM).

## 5. ProxySecure

Navegación corporativa segura sin virus ni aplicaciones maliciosas (ActiveX, Java Applets, ...)





# Soluciones Corporativas

## 6. ISASecure

Antivirus en colaboración con Microsoft, filtrado de contenido y protección de aplicaciones maliciosas.

## 7. CVPSecure

Protección antivirus y de filtrado preventivo certificada por CheckPoint.

## 8. SendmailSecure

Protección SMTP de alto rendimiento con MilterAPI para las pasarelas Sendmail bajo Linux.

## 9. PostfixSecure

Protección nativa de alto rendimiento para MTAs Postfix.

## 10. QmailSecure

Protección nativa de alto rendimiento para MTAs Qmail.



# Soluciones Corporativas

## AdminSecure

Consola de gestión flexible que se adapta a la estructura de red.

Disponibile en inglés, francés, alemán y castellano. A finales de año planificado también en japonés, italiano, portugués y chino.

Arquitectura basada en componentes independientes (Servidor de Administración, Servidores Repositorio, Agentes de Comunicación) con comunicaciones XML via TCP/IP optimizado para redes WAN.

Base de datos centralizada y de acceso ilimitado para informes personalizados y predeterminados.

Actualizaciones automáticas a todas las plataformas por defecto.



# AdminSecure

AdminSecure console (Server: ADMINSECURE)

File View Antivirus Tools Help

Install antivirus Uninstall antivirus Update antivirus

Administration

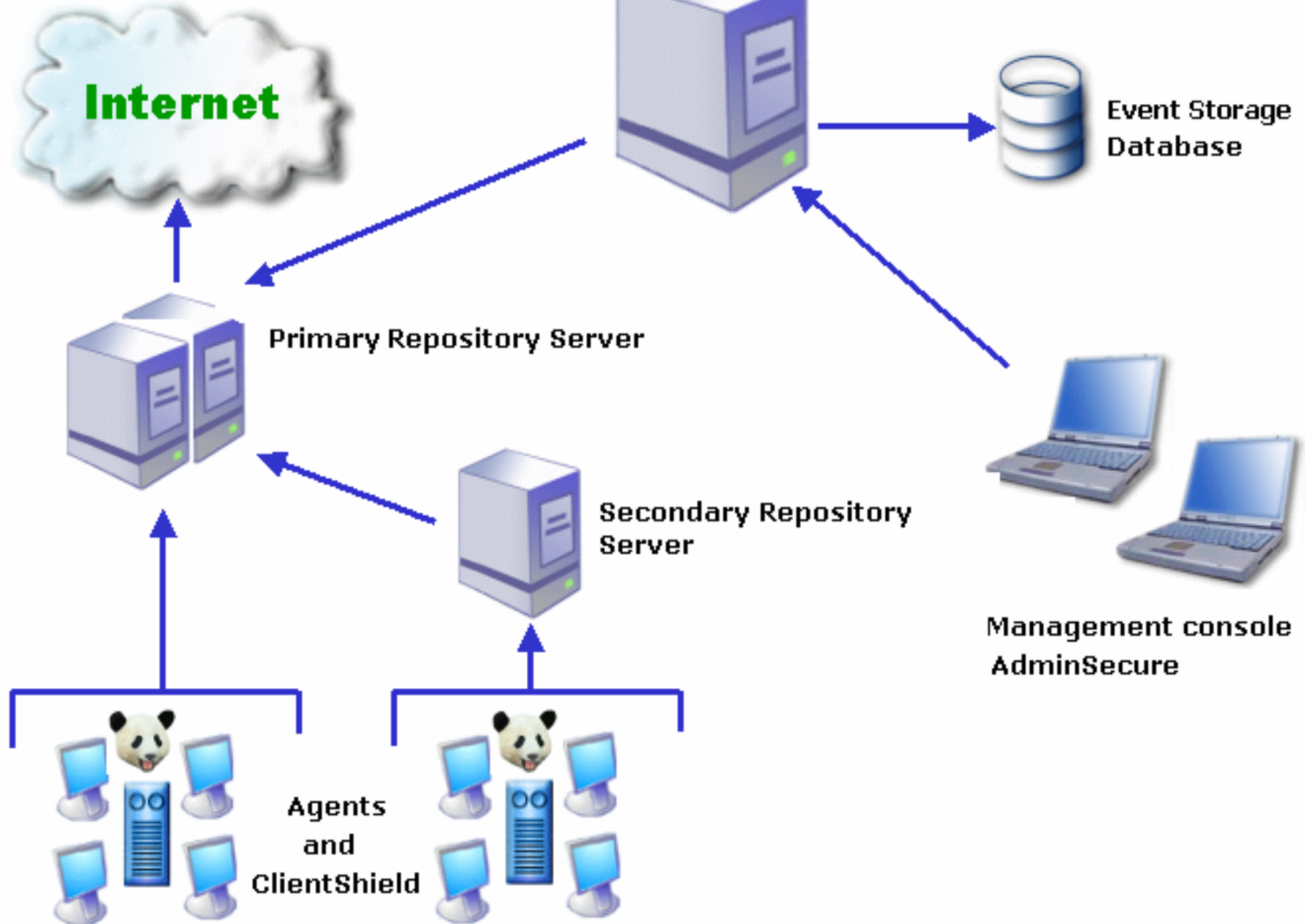
- My organization
  - Lost and found
  - CVP Servers
  - Domino Servers
  - Exchange Servers
  - ISA Servers
  - Linux mail servers
  - Novell Servers
  - Proxy Servers
  - Windows Servers
  - Windows workstations

Self-diagnosis Modules Jobs Events Settings Scan Report

'My organization' content  Include content of subgroups

Module	Platform	Product installed	AV enabled
ADMINSECURE	CVP-Antivirus	Panda CVPSecure (3.46.00)	Yes
ADMINSECURE	Windows Server	Panda FileSecure (6.06.00)	No
ADVSRV	CVP-Antivirus	Panda CVPSecure (3.46.00)	Yes
ADVSRV	Windows Server	Panda FileSecure (6.06.00)	Yes
ESCUCAMBIADO	Windows workstation	Panda ClientShield (1.81.08)	Partially
FORTUNA	CVP-Antivirus	Panda CVPSecure (3.46.00)	Yes
FORTUNA	Proxy Server	Panda ProxySecure (2.36.00)	Yes
FORTUNA	Lotus Domino Server	Panda DominoSecure (2.35.00)	Yes
FORTUNA	Windows Server	Panda FileSecure (6.06.00)	Yes
JANO	Windows workstation	Panda ClientShield (1.00.00)	Yes
NTWS	Windows workstation	Panda ClientShield (1.81.08)	Yes
SATURNO	CVP-Antivirus	Panda CVPSecure (3.46.00)	Yes
SATURNO	ISA Server	Panda ISASecure (1.57.00)	Yes
SATURNO	Exchange Server	Panda ExchangeSecure (2.35.00)	Yes
SATURNO	Lotus Domino Server	Panda DominoSecure (2.35.00)	Yes
SATURNO	Windows Server	Panda FileSecure (6.06.00)	No
SILVANO	CVP-Antivirus	Panda CVPSecure (3.46.00)	Yes
SILVANO	Exchange Server	Panda ExchangeSecure (2.35.00)	Yes

# Architecture of AdminSecure Scenario 2





# Comparando ...



	<b>Panda ClientShield</b>	<b>NAI VirusScan Thin Client</b>
<b>Anti-virus</b>	✓	✓
<b>Anti-spyware</b>	✓	
<b>Anti-dialers</b>	✓	
<b>Anti-spam</b>	✓	
<b>Anti-hoaxes</b>	✓	
<b>Anti-jokes</b>	✓	Detecta como virus
<b>Cobertura del residente</b>	Ficheros POP3 SMTP MAPI NNTP	Ficheros
<b>Análisis bajo demanda</b>	✓	
<b>Protección contra ActiveX, Java Applets</b>	✓	
<b>Tecnología de reparación</b>	SmartClean	
<b>Interfaz intuitivo</b>	✓	



# Soluciones Corporativas

Nuestros productos están disponibles en 23 idiomas, incluidos:

- ☒ Alemán
- ☒ Vasco
- ☒ Búlgaro
- ☒ Checo
- ☒ Chino simplificado
- ☒ Chino tradicional
- ☒ Inglés
- ☒ Finlandés
- ☒ Francés
- ☒ Griego
- ☒ Holandés
- ☒ Húngaro
- ☒ Italiano
- ☒ Japonés
- ☒ Polaco
- ☒ Portugués
- ☒ Ruso
- ☒ Eslovaco
- ☒ Esloveno
- ☒ Castellano
- ☒ Sueco

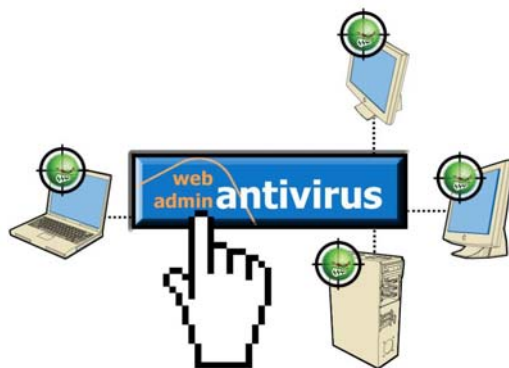
# Soluciones para Application Service Providers (ASP)





# Soluciones para ASPs

## Panda Antivirus API



- Motor antivirus de alto rendimiento de Panda Software.
- Para integraciones en servicios y aplicaciones bajo Win32 y Linux.
- Soporte de integración y desarrollo de segundo nivel.

- WebAdmin Antivirus. El antivirus más fácil para empresas.
- No necesita infraestructura. Alojado en nodo Panda.
- Gestión, reporting y distribución vía web.

- GateDefender 7100. Instalar y olvidar.
- Analiza 7 protocolos.
- Detecta y desinfecta más de 80.000 correos por hora.
- Gestión por consola web.





# Soluciones para ASPs



## CVPSecure

- Antivirus y filtrado de contenidos para Firewalls CVP
- Integrado en servidor (Win32)
- Integración y redirección de tráfico a servidores antivirus dedicados.

## Sendmail Qmail Postfix

- Motor antivirus de alto rendimiento para MTA bajo Linux
- Integrado en los mismos servidores o soluciones turn-key
- Uso de tecnologías MilterAPI



# Panda Antivirus API



- ☒ Librerías y motor antivirus para plataformas Win32 y Linux.
- ☒ Para integraciones en sistemas servidor y aplicaciones web.
- ☒ Ejemplos:
  - Protección de Webmail (visible o transparente)
  - Integración en pasarelas SMTP / POP3
  - Integración en sistemas de backup y almacenamiento
  - Integración en firewalls y gateways
  - Integración en aplicaciones corporativas



# WebAdmin Antivirus



**panda software**

Bienvenido NOMBRE - [Administrar antivirus](#) | [Cerrar sesión](#)

INICIO ADMINISTRACIÓN SERVICIOS VIRUS INFO

POWERED BY SECURE | RESOLUTIONS

## Administrar WebAdmin Antivirus

**WebAdmin Antivirus**

- Configurar
  - [Asistente de configuración](#)
  - [Políticas](#)
  - [Grupos](#)
- Ver Informes
  - [Incidencias de virus](#)
  - [Instalaciones](#)
  - [Errores](#)
  - [Instalación remota](#)
  - [Perfiles de instalación](#)

Para administrar su antivirus, seleccione la opción deseada entre las que aparecen a continuación.

Políticas y grupos

Puede crear grupos con los equipos de su organización y establecer las políticas que desea asignar a cada grupo de equipos.

[Editor de políticas](#) [Editor de grupos](#)

Instalación remota

Use la herramienta de instalación remota para instalar los antivirus en su organización de forma transparente.

[Instalación remota](#)

Informes

Los informes le proporcionan información actualizada sobre incidencias de virus y el estado de la protección antivirus.

[Virus](#) [Instalaciones](#) [Errores](#)

Perfiles de instalación

Los perfiles de instalación le proporcionan un alto nivel de control sobre la instalación de antivirus en su organización.

[Perfiles de instalación](#)

© Panda Software 2003. Todos los derechos reservados.

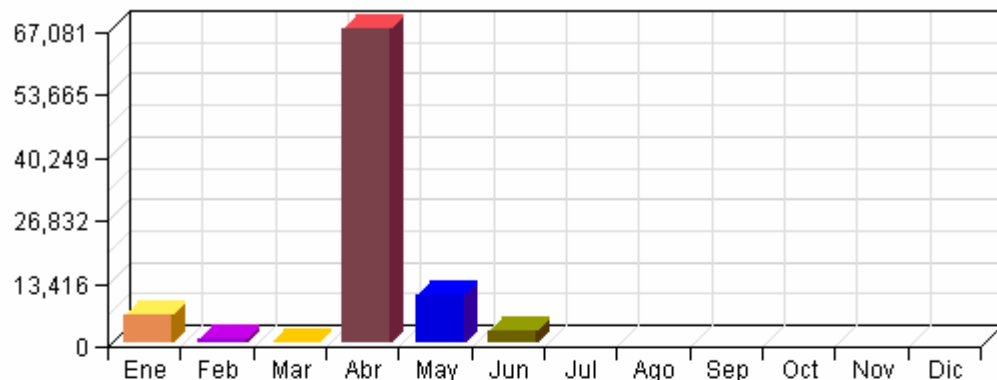


# WebAdmin Antivirus



- Instalación y gestión via web (URL) y a través de red
- Múltiples políticas de configuración
- Reporting online
- Actualizaciones incrementales automáticas
- Updates y upgrades peer-2-peer

Vista por meses



Incidencias de virus de: Año - 2003

Pulse sobre el gráfico para obtener información más detallada.

## RESUMEN DE INCIDENCIAS DE VIRUS DE: Año - 2003

[Total de virus detectados:](#) 87172

[Total de archivos sobre los que no se ha actuado:](#) 2417

[Total de virus desinfectados:](#) 29525

[Total de archivos eliminados:](#) 2

[Total de archivos movidos a cuarentena:](#) 9057

### TOP 5: VIRUS DETECTADOS

1. [TMC.A](#) - (3326 encontrados)
2. [Bachkhoa.3999](#) - (2732 encontrados)
3. [W97M/Melissa.A](#) - (2673 encontrados)
4. [HLL.Gen](#) - (2482 encontrados)
5. [Natas.4744](#) - (2165 encontrados)

[más...](#)

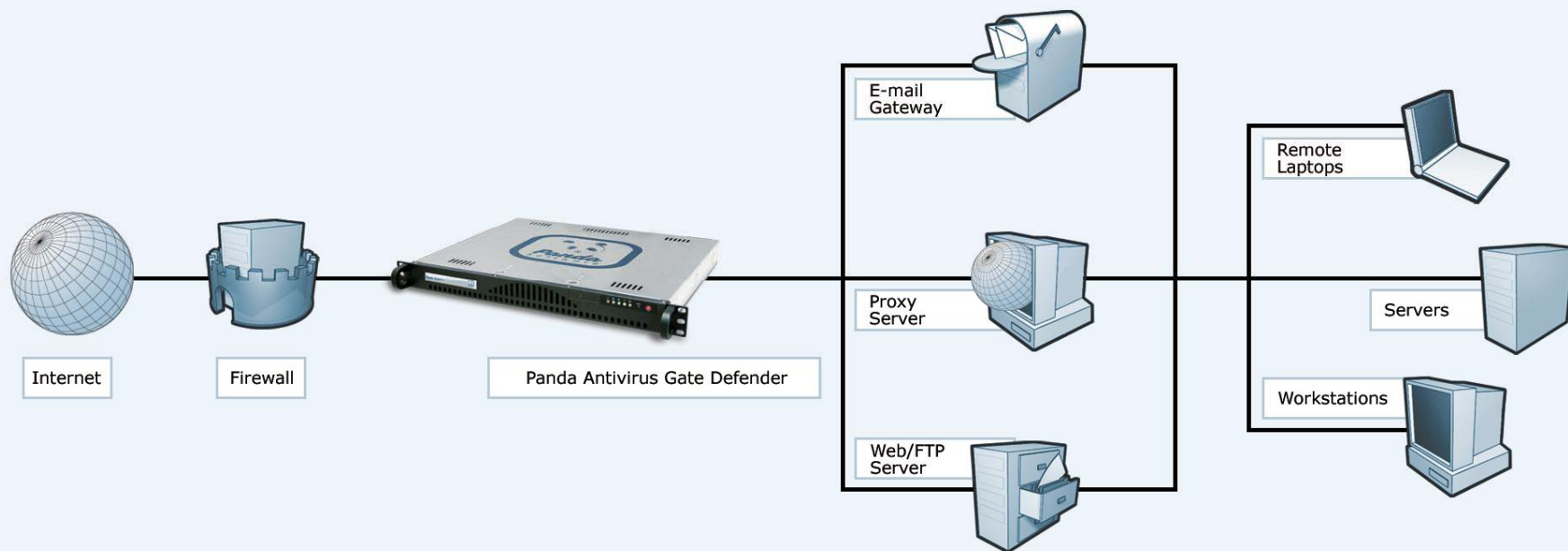
### TOP 5: ORDENADORES INFECTADOS

1. [PC6](#) - (23047 infecciones)
2. [XPIE](#) - (15929 infecciones)
3. [PC5](#) - (9375 infecciones)
4. [PSI](#) - (9032 infecciones)
5. [PSI](#) - (8740 infecciones)

Ver detalles



# Panda GateDefender



- **Completo:**

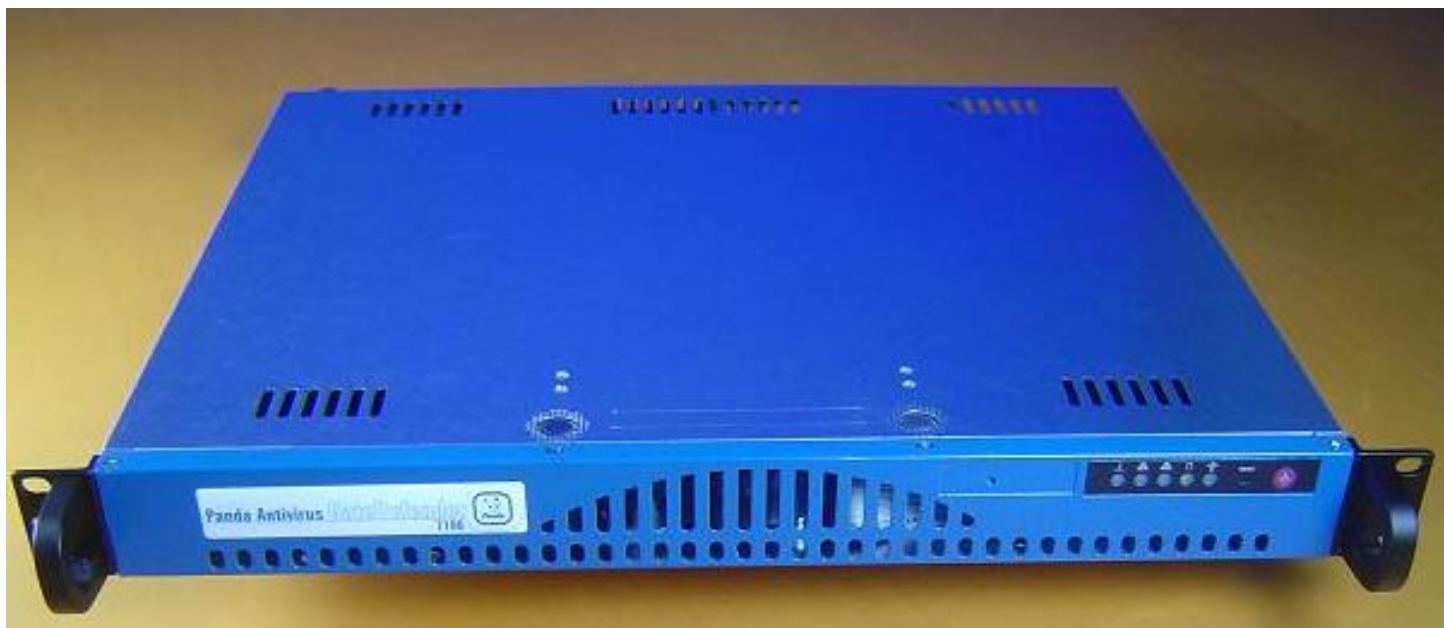
- Detecta y desinfecta tráfico entrante y saliente.
- Se actualiza automáticamente cada hora y media.
- Analiza SMTP, HTTP, FTP, POP3, NNTP, IMAP4, SOCKS.

- **Alto rendimiento:**

- 80.000 y 200.000 mensajes por hora respectivamente.
- Balanceo de carga automático.



# Panda GateDefender



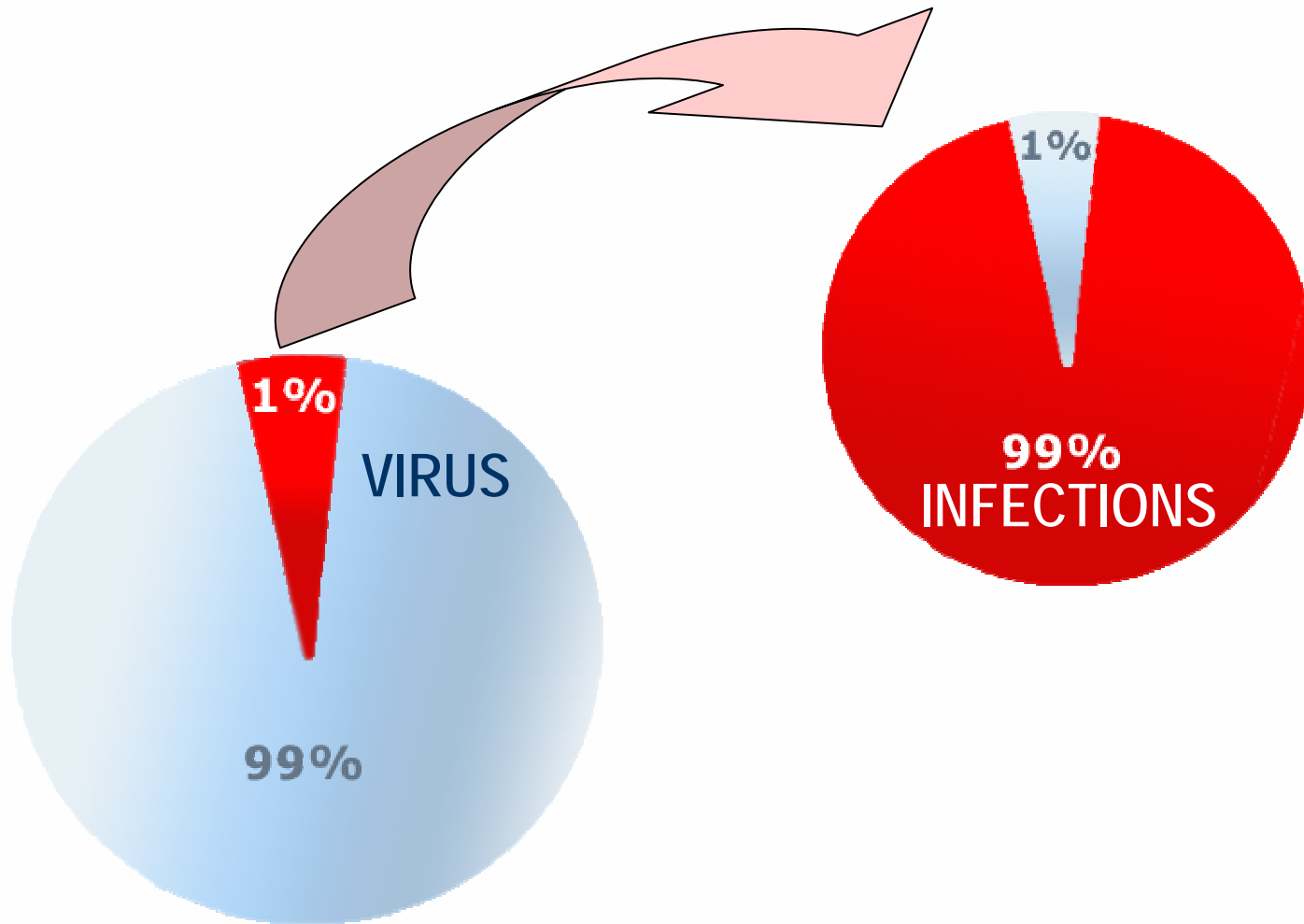
- ☒ Antivirus, filtrado de contenidos, Anti-Spam, filtrado Web (URL) y alto rendimiento.
- ☒ 3 nuevos modelos para pequeñas (8050), medianas (8100) y grandes empresas (8200).

# Nuevas Tecnologías





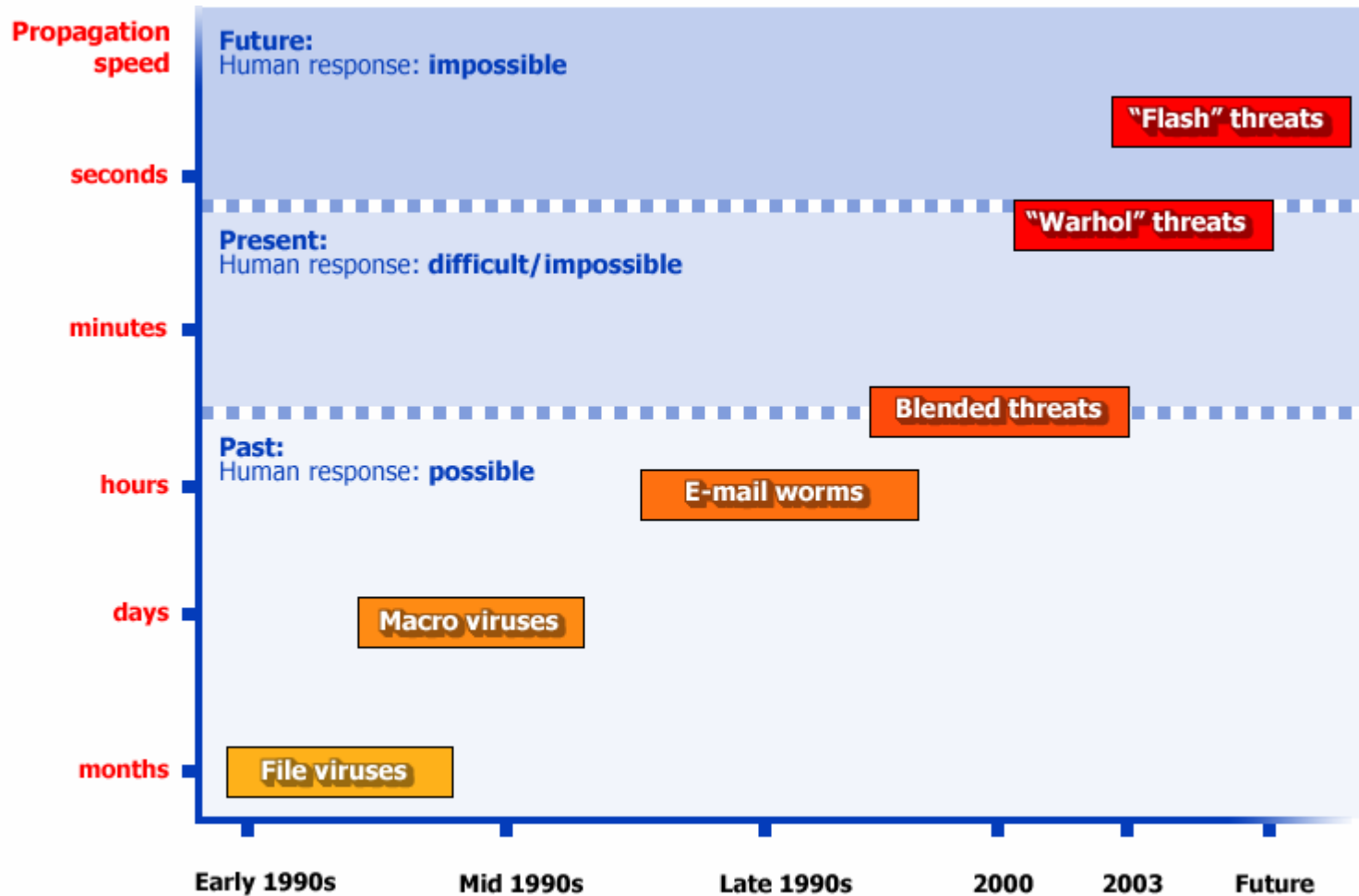
# Los antivirus no detectan todo ...







# Las amenazas evolucionan ...





# En conclusión ...

## ☒ Evolución de las amenazas:

Vulnerabilidades de sistemas, nuevos vectores de infección, ignorancia de los usuarios y naturaleza reactiva de sistemas de seguridad.

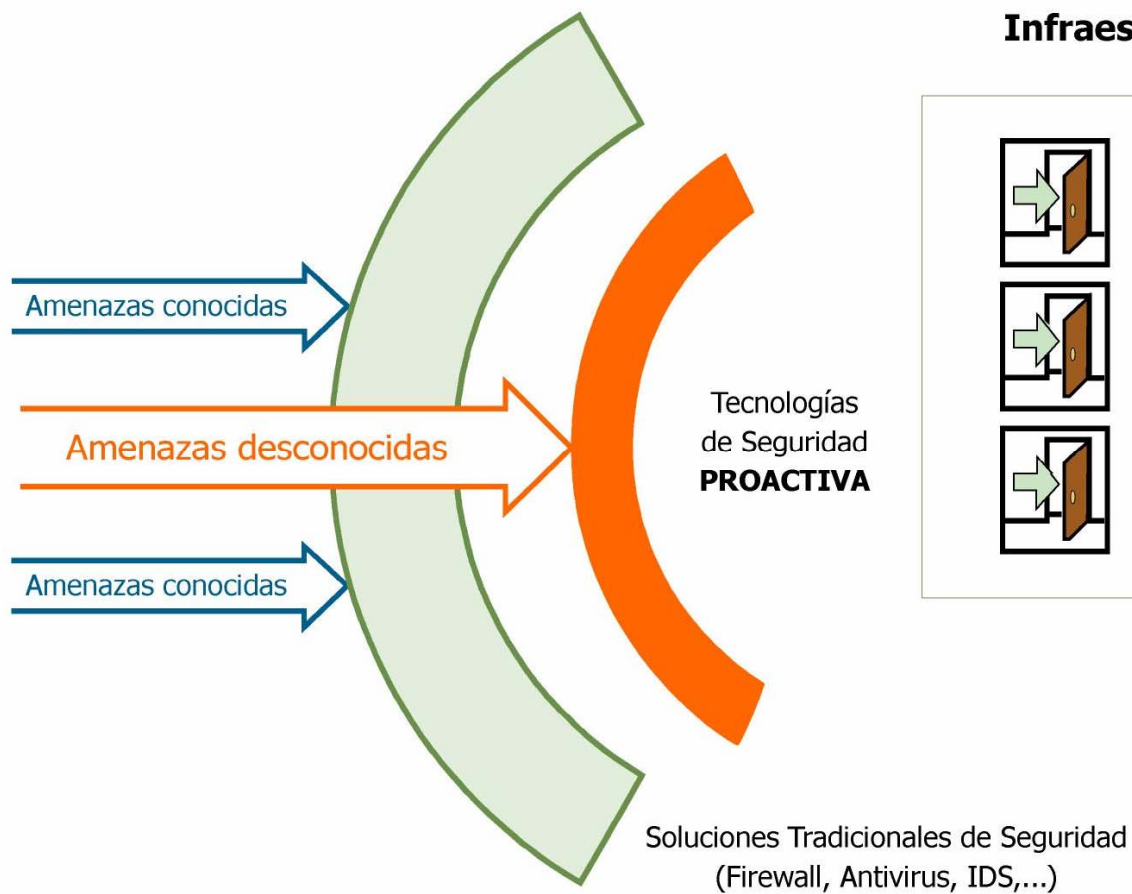
## ☒ Las empresas se siguen infectando:

60% del nuevo malware son gusanos, el 30% troyanos y menos de un 10% son virus.

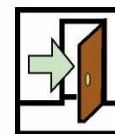
## ☒ ¿Por qué?

Tecnología AV es buena para virus conocidos únicamente. El mercado necesita nueva tecnología para protegerse contra los virus y amenazas desconocidas.

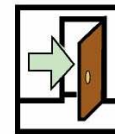
## ☒ *Respuesta de Panda → TruPrevent*



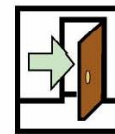
## Infraestructura corporativa



**Vulnerabilidades en sistemas y aplicaciones**



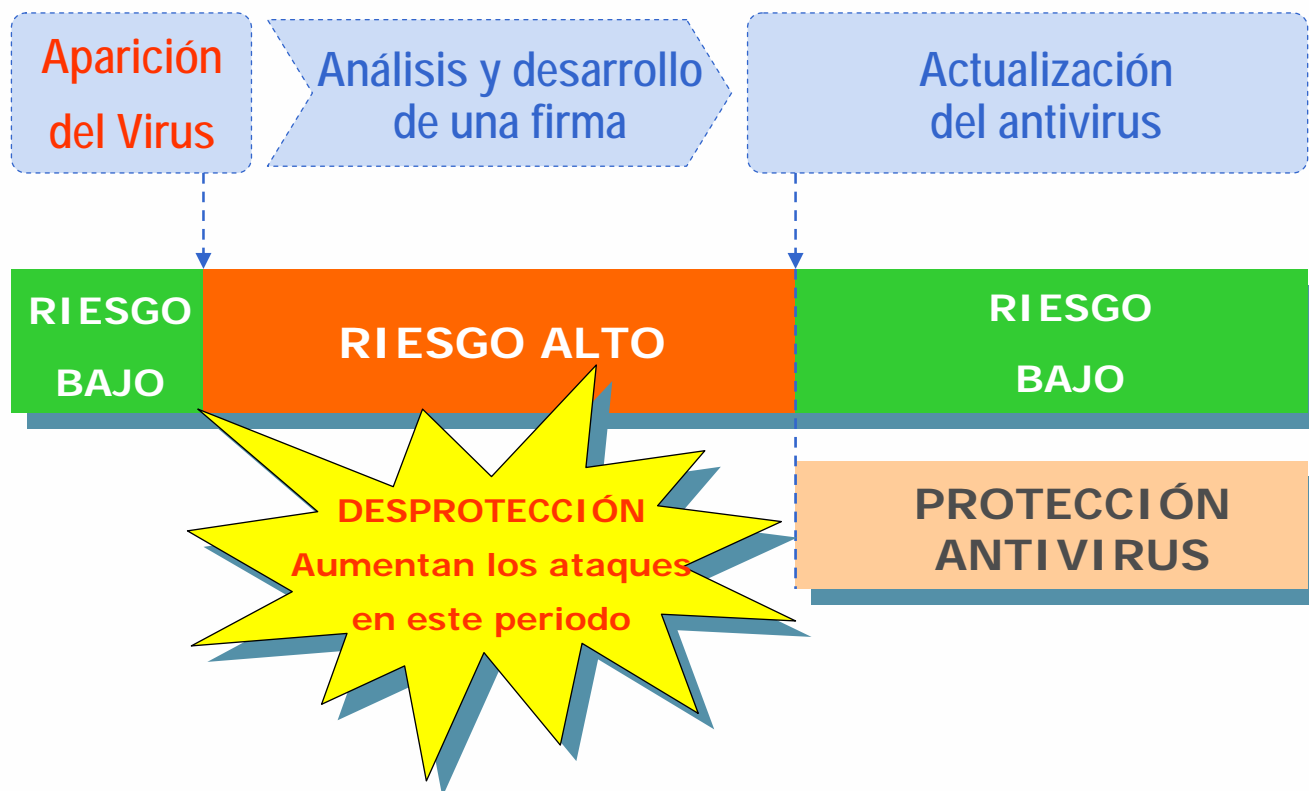
**Descuido de los usuarios**



**Infraestructura de IT desprotegida**  
(debido a la complejidad en la gestión de la seguridad)



## EL PROBLEMA: Los clientes siguen infectándose



- ☒ Este es un problema que tienen todos los desarrolladores de antivirus.
- ☒ OJO: La heurística no resuelve el problema.



## ☒ **Análisis de Comportamiento**

Bloquea gusanos y troyanos desconocidos.

## ☒ **Detector de Paquetes Maliciosos**

Bloquea gusanos de red desconocidos y otras amenazas.

## ☒ **Protección contra Buffer Overflow**

Protege contra vulnerabilidades desconocidas.

## ☒ **Kernel Rules Enforcement (KRE)**

Políticas globales de seguridad para controlar las estaciones y servidores.



- ☒ **Algunos datos acerca de TruPrevent:**
- ☒ Llevamos desarrollando casi dos años.
- ☒ Ya detecta nuevos virus sin firma, únicamente con análisis de comportamiento:
  - ⑩ BugBear, Nimda, Klez, PrettyPark, SirCam, Navidad, LovaGate, Lentin, Loveletter, Gaobot, Spybot, Dumaru, Opaserv, Netsky, Gibe, Mydoom, Mapson, Sobig , ...
- ☒ Es complementario a los sistemas antivirus, incluso los de otras empresas (McAfee, Symantec, Trend, ...).
- ☒ Productos corporativos TruPrevent disponibles en breve.

**Gracias !**

