Cambiando el antivirus por la Seguridad como Servicio (SaaS)

Panda
ManagedOfficeProtection

PANDA SECURITY | One step ahead.

ÍNDICE:

Aspectos sobre la seguridad

Necesidades específicas de seguridad de las PYMEs

Las PYMEs son perfectamente conscientes de que se enfrentan a los mismos riesgos y normativas de seguridad que las grandes empresas. Además, el creciente número de amenazas hace que sus necesidades de protección sean cada vez más complejas:

- Existen más amenazas que nunca (PandaLabs ha recibido más malware el año pasado que en los anteriores 16 años juntos)
- El malware es más silencioso y más difícil de combatir, ya que permanece oculto mientras lleva a cabo robos de identidad, causa pérdidas económicas y de productividad y realiza otras acciones maliciosas.

El panorama al que se enfrentan las empresas requiere de un conjunto de tecnologías avanzadas para la detección de malware.

Cuando las PYMEs implementan una solución de seguridad, deben elegir una que les proporcione una protección adecuada y que se adapte a sus necesidades específicas. En muchos casos, los recursos limitados de los que disponen no resultan suficientes para conseguir un nivel alto de seguridad.

- Normalmente, las **pequeñas y medianas empresas no disponen de recursos especializados** para proteger y gestionar la seguridad de sus redes. Tienden a invertir todos los recursos posibles en la actividad principal de la empresa y eso les impide asignar una parte adecuada de su presupuesto a la seguridad informática. También necesitan un sistema de monitorización continua para reducir el riesgo.

- Las **oficinas remotas y las filiales** se encuentran **geográficamente alejadas** grandes distancias unas de otras. Necesitan ser **gestionadas de forma** remota desde un punto centralizado. Además, necesitan **simplificar** la gestión de la seguridad lo máximo posible, y disponer de un servicio de monitorización continua con un **reducido consumo de ancho de banda**.

- Las **empresas domésticas** no disponen de nadie que se haga cargo de la gestión de la seguridad y tampoco cuentan con presupuestos dedicados a ello.

Los productos antivirus suponen demasiado tiempo y esfuerzo a las PYMEs

Los productos antivirus requieren demasiado tiempo y esfuerzo para las pequeñas y medianas empresas. Tras comprar el antivirus, deben invertir tiempo y esfuerzo en:

- **Hardware adicional**, como servidores que alojen una consola centralizada con sus servicios y bases de datos.

- **Licencias de software**, como software de bases de datos para generar informes o configurar la protección.

- **Personal especializado en seguridad**, que se encargue de gestionar y monitorizar la seguridad sin estar dedicado a la actividad principal de la empresa.

Muchas PYMEs prefieren no ocuparse de todas estas complicaciones, ya que estas tareas les distraen de la actividad principal de su negocio.

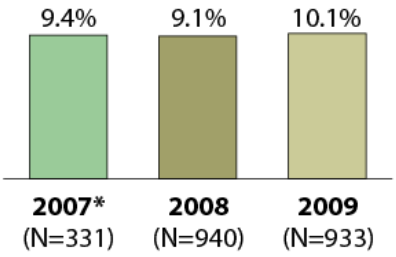
Soluciones de Seguridad como Servicio

Las Pequeñas y Medianas Empresas disponen de recursos y presupuestos **muy limitados** para enfrentarse a esta situación.

Según encuestas realizadas en Estados Unidos a responsables de seguridad de varias empresas, el presupuesto de seguridad representa aproximadamente el 9% del presupuesto total de TI.

SMB IT Security Budgets Stay Flat In 2008, Will Rise In 2009

"What percent of your company's IT operating budget will be devoted to IT security in 2008? And in 2009?"

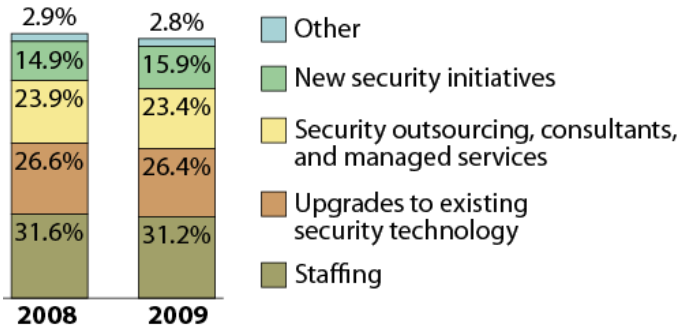


Base: North American and European SMB decision-makers responsible for setting IT budgets

*Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2007

Budget Allocations Will Hold Steady Going Into 2009

"How will your IT security budget break out across the following categories this year? How will this allocation change next year?"



Base: 967 North American and European SMB decision-makers responsible for setting IT budgets (percentages may not total 100 because of rounding)

Fuente: Forrester. Diciembre 2008 **"The State Of SMB IT Security: 2008 To 2009"**. Presupuestos y planes de inversión en Seguridad IT.

La **mejor alternativa** para las pequeñas y medianas empresas consiste en **alojar** sus soluciones de seguridad en una infraestructura de hardware externa, disminuyendo así los costes operativos y el coste total de propiedad.

El hardware y su mantenimiento representan un coste y un esfuerzo importantes para las pequeñas y medianas empresas.

La **Seguridad como Servicio** (SaaS, por sus siglas en inglés) ofrece a los clientes aplicaciones tradicionales de seguridad en forma de servicios Web. Las Soluciones de Seguridad como Servicio tienen las siguientes características:

- **Servicio de suscripción:** Ya que SaaS es un servicio de suscripción, las empresas que lo ofrecen prestan más atención a la calidad del servicio y del soporte. Esto les obliga a ofrecer lo mejor en cuanto a calidad, mantenimiento y servicio.
- **Servicio alojado:** SaaS permite que varios clientes puedan acceder a Internet y utilicen una única aplicación simultáneamente. Esto obliga a diseñar el software de forma que

permita la posibilidad de compartir clientes mientras mantiene los datos de cada cliente separados y seguros.

- **Alta disponibilidad 24x7**: Las empresas que ofrecen soluciones de Seguridad como Servicio deben proporcionar una alta disponibilidad y continuidad del servicio 24x7. Para ello, las empresas de SaaS debe disponer de servidores en un centro de datos que disponga de una fuente de alimentación redundante UPS, generadores de respaldo, interconexión total de nivel 1 con múltiples proveedores backbone y monitorización exhaustiva 24x7, entre otras características. Además, deber de ser capaces de responder de forma inmediata ante cualquier problema de hardware, software o administración de bases de datos. Por último, los clientes de SaaS necesitan disponer de un servicio de soporte 24x7.

- **Interfaz web:** El interfaz de la aplicación es un interfaz web que permite al cliente final acceder a la aplicación a través de Internet en cualquier momento (24x7) y desde cualquier lugar.

- **Siempre actualizado:** Como las actualizaciones de software SaaS sólo requieren de la realización de cambios en una plataforma única en servidores centralizados, el despliegue de las actualizaciones es mucho más sencillo.

- **Ciclo corto de actualizaciones:** Las empresas de SaaS pueden monitorizar constantemente y en tiempo real la forma en que los usuarios emplean las aplicaciones. Analizan inmediatamente qué funciona bien y que no. Estas empresas utilizan esta información para responder rápidamente, implementando actualizaciones de software de ciclos más cortos que los empleados por el software instalado en la red del cliente.

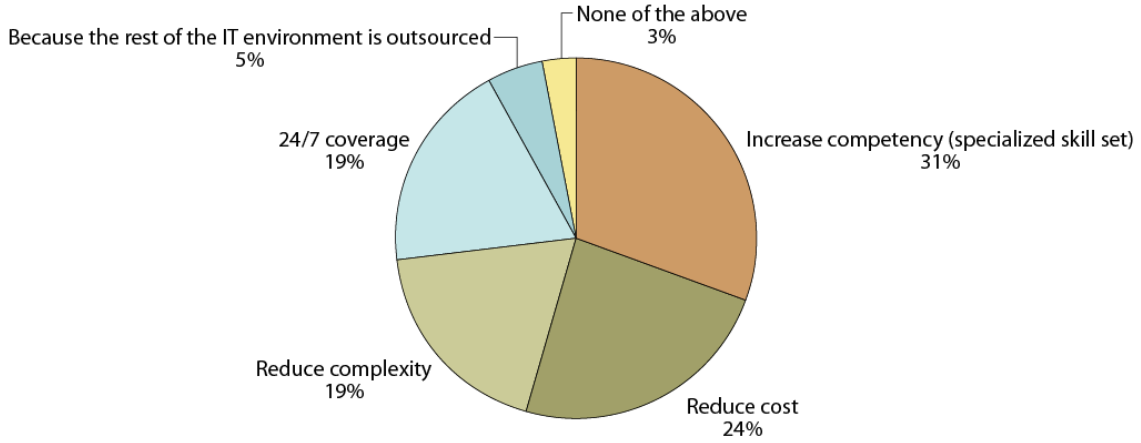
- **Bajo coste total de propiedad:** Los servicios alojados no requieren de infraestructura dedicada en la empresa del cliente. No se requiere de inversiones en infraestructura ni de gastos de mantenimiento o dimensionamiento ante un posible crecimiento de la compañía. Las actualizaciones automáticas de los programas SaaS tienen un coste total de propiedad (TCO) más bajo dado que SaaS elimina muchos de los recursos necesarios para actualizar las soluciones. De hecho, las aplicaciones SaaS presentan un coste total de propiedad un 50% más bajo que el software instalado en la red del usuario, lo que permite a las empresas destinar recursos a otras áreas. Su rápida instalación se traduce además en un retorno de la inversión más rápido.

El uso de Software como Servicio es una tendencia confirmada: Hoy en día, casi el 50% de todas las pequeñas y medianas empresas que emplean el modelo SaaS lo utilizan para la gestión de su seguridad.

Alojar soluciones de seguridad en infraestructuras externas puede **complementarse** con la posibilidad de **subcontratar los servicios**. Esta opción permitiría a las pequeñas y medianas empresas dejar su seguridad en manos expertas, pudiendo centrarse en la actividad principal de su negocio y por lo tanto incrementar su competitibidad.

SMBs Adopt Managed Security Services For Added Competency And Cost Savings

"What is your primary driver for using a managed security service provider (MSSP)?"



Base: 685 North American and European SMB IT security sourcing and services decision-makers
(percentages do not total 100 because of rounding)

Fuente: Forrester. Diciembre 2008 **"The State Of SMB IT Security: 2008 To 2009"**. Las pequeñas y medianas empresas adoptan los servicios gestionado de seguridad, para incrementar su competitibidad y ahorrar costes.

Según las predicciones de Gartner, se espera que el mercado de SaaS crezca a un ritmo del 15% hasta el año 2010, alcanzando los 11 mil millones de dólares para el año 2011[1].
SaaS prometer ser una revolución en la industria.

Además, y según Gartner, para el año 2010 el 90% del gasto en nuevas estructuras de protección global en organizaciones de menos de 500 empleados irá destinado a plataformas de seguridad (por ejemplo, suites de seguridad para los equipos, seguridad multifuncional en la nube, seguridad multifuncional para el correo electrónico, etc).[2]

Panda Managed Office Protection

¿Qué es Panda Managed Office Protection?

Panda Managed Office Protection es un **servicio de seguridad por suscripción** basado en **web**. Libera a la pequeña y mediana empresa de tener que adquirir hardware adicional, personal de mantenimiento u otros recursos dedicados al antivirus, manteniendo un **alto nivel de seguridad** para todos sus PCs, portátiles y servidores.

Al ser un Servicio Alojado (**Hosted Service**), la consola web siempre está **disponible** y permite gestionar la protección en cualquier momento desde cualquier lugar, incluyendo las oficinas **remotas** no conectadas a la LAN.

Ofrece Seguridad como Servicio (SaaS) a través de un **portal** de gestión y permite a las empresas **delegar**, si quieren, la gestión de su seguridad a **proveedores de servicios especializados**.

Panda Managed Office Protection está complementado por **auditorías** de seguridad periódicas, beneficiándose de las tecnologías de **Inteligencia Colectiva**.

Suscríbase al servicio de seguridad y olvídese de hardware dedicado al antivirus, software de apoyo y recursos de personal adicionales.

Beneficios de Managed Office Protection

Panda Managed Office Protection está diseñado para cubrir las necesidades de las PYMEs. Al ser un **Servicio Alojado**, presenta importantes beneficios. Managed Office Protection tiene además las siguientes ventajas adicionales:

- **Minimiza los costes operativos.** No se requiere infraestructura adicional ya que es un servicio alojado (**Hosted Service**) que se gestiona a través de una **consola web**. Además, le permite **delegar**, si lo desea, la gestión de su seguridad a **proveedores de servicios** especializados.

- **Elimina la complejidad.** La consola web permite a los administradores instalar, gestionar y monitorizar **fácilmente** la protección, **incluso la de oficinas remotas**, evitando personal de mantenimiento adicional especializado.

- **Reduce las pérdidas de productividad**. Detecta malware que causa consumo de recursos o que es molesto para los empleados. Las **actualizaciones** (updates / upgrades) son **automáticas** y desatendidas y permiten al administrador focalizarse en otras prioridades. Las estaciones se actualizan conectándose **P2P** a la estación más cercana, minimizando el consumo de ancho de banda.

- **Mejora la gestión del riesgo.** La consola web informa en **tiempo real** de la actividad de detección en la red, incluyendo las oficinas remotas**.** Además permite realizar **auditorías** periódicas con **informes** detallados sobre el estado de la red.

- **Asegura la continuidad de la actividad.** Al ser un servicio alojado (**Hosted Service**), ofrece **alta disponibilidad**, soporte 24x7 y siempre utiliza la última versión de las tecnologías y fichero de firmas.

- **Previene el robo de identidad.** Localiza malware **oculto** que puede robar información sensible de su organización**.**

- **Ayuda en el cumplimiento de la normativa vigente**. Ayuda a reforzar el cumplimiento de **SOX, PCI, HIPAA** realizando **auditorías** de seguridad periódicas de toda la red.

Características de Managed Office Protection

Panda Managed Office Protection permite a las organizaciones gestionar **fácilmente** su protección desde cualquier sitio y en cualquier momento, mediante las siguientes características**:**

- **Consola de administración Web.** El administrador sólo necesita un navegador para gestionar centralizada y **fácilmente** las protecciones de todas las estaciones, incluyendo las de **oficinas remotas** no conectadas a la LAN.

- **Protección proactiva** para estaciones y servidores contra amenazas conocidas, y desconocidas, incluso amenazas **ocultas**. Incluye tecnologías **heurísticas** y protección para **ficheros**, **correo electrónico**, **navegación por Internet** y **mensajería instantánea** con bajo consumo de recursos.

- **Firewall personal gestionado**. Los firewalls se pueden gestionar **de forma centralizada** mediante la consola web o **de forma local** desde los equipos a través de una consola local, si el administrador delega la gestión en los usuarios. El firewall ofrece **filtrado de aplicaciones, control de acceso** a la red, **IPS** (Intrusion Prevention System), **prevención de virus de red** y configuración basada en zonas.

- **Servicio de auditoría exhaustiva de malware**. Panda Managed Office Protection incluye **Malware Radar**, un **servicio de auditoría de malware** para evaluar periódicamente el estado de su red. Basado en la tecnología de **Inteligencia Colectiva** única de Panda, aumenta la cantidad de malware que es capaz de detectar de forma exponencial. Ofrece **informes** de auditoría detallados y permite **automatizar** las tareas de desinfección.

- **Actualizaciones automáticas vía P2P**. Las estaciones actualizan su protección **conectándose P2P** a la **estación más cercana**, minimizando el consumo de ancho de banda. El administrador puede configurar la frecuencia de las actualizaciones desde la consola web centralizada. También es posible forzar actualizaciones **bajo demanda y por grupos**.

- **Protección basada en perfiles de usuario y grupos** Esta característica permite al administrador asignar distintas **políticas** o diferentes **perfiles de protección** a los usuarios, de acuerdo a las necesidades de la organización.

- **Delegación de la gestión administrativa**. Permite **dividir** las diferentes tareas de administración entre distintos usuarios asignándoles privilegios (monitorización, administración) y definiendo sobre qué equipos tienen acceso.

- **Instalación flexible.** Existen diferentes opciones para instalar la protección, con o sin la intervención de los usuarios. La **Herramienta de Distribución** permite realizar la instalación a los equipos seleccionados de manera **transparente** a los usuarios. También es posible realizar instalaciones MSI.

- **Gestión de licencias basada en grupos**. El administrador puede asignar un número máximo de licencias y una fecha de caducidad para cada grupo de ordenadores, según las necesidades de la organización. .

- **Informes ejecutivos, detallados y resumidos**. Los informes son **configurables** y ofrecen gráficos con información sobre la actividad de detección de **malware,** los elementos enviados a **cuarentena** y el **estado de la protección**. Se pueden **exportar** a distintos formatos como archivos de texto, PDF, XML, HTML o Excel.

¿Qué es la Inteligencia Colectiva?

La Inteligencia Colectiva es una **plataforma de seguridad** que proporciona a los usuarios **protección proactiva en tiempo real**. Se aprovecha del conocimiento colectivo y automatiza el análisis, correlación, clasificación y los procesos de creación de firmas **aumentando de forma exponencial** la cantidad de malware detectado cada día.

Figura 1: Inteligencia Colectiva

Esta tecnología acelera la respuesta de Panda Security ante cualquier amenaza, **maximizando la capacidad de detección** y minimizando el uso de recursos (todo el trabajo se realiza en una "nube", en nuestros centros de datos, en lugar de en los ordenadores de nuestros clientes).

"Para los fabricantes de antivirus es una cuestión de supervivencia. Buscan formas de reinventarse constantemente mientras sus productos luchan por neutralizar nuevos tipos de infecciones.

Los servicios de **inteligencia colectiva** en la nube son el próximo gran paso para combatir el malware. Creo que todas las empresas de AV deberán asumir una estrategia de este tipo si desean sobrevivir"[3].

Andrew Jaquith, analista de Yankee Group

¿Cómo funciona Managed Office Protection?

La **arquitectura** de Panda Managed Office Protection permite gestionar la protección en cualquier momento y desde cualquier lugar. Independientemente de la ubicación del administrador, éste sólo necesita un navegador web para gestionar la protección, incluyendo la de las oficinas remotas o usuarios móviles que no estén conectados a la LAN.

Figura 2: Arquitectura de Panda Managed Office Protection

Acceda a la **consola web** y **despliegue la protección** a todos sus ordenadores. Existen dos formas de hacerlo:

- **Enviar un correo electrónico a los usuarios finales**. Cada usuario debe **hacer clic** en un enlace **para instalar la protección**. El agente de la protección se instalará en todas las estaciones de trabajo.

- **Instalar la protección en todos los ordenadores** sin intervención del usuario.

    - Panda Managed Office Protection proporciona una **Herramienta de Distribución** que permite seleccionar los ordenadores (por nombre, dominio, dirección IP y rango IP) y desplegar el agente de forma transparente.

- Además, ofrece el archivo de instalación en formato **MSI**, compatible con herramientas de distribución estándar como Tivoli, SMS, LanDesk, Active Directory, etc.

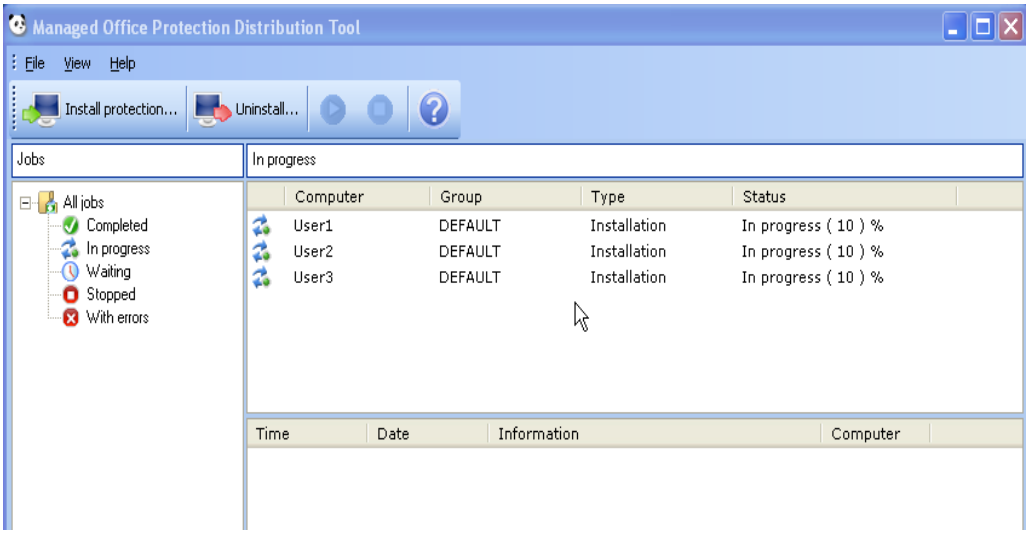


Figura 3: Herramienta de distribución de Managed Office Protection

A partir de ese momento, los usuarios recibirán **actualizaciones automáticas** (**updates** y **upgrades**) directamente desde Panda, y el administrador podrá **monitorizar** el estado de la red y aplicar las políticas de seguridad necesarias.

Las estaciones actualizarán su protección conectándose mediante **P2P** al ordenador más cercano, **minimizando el consumo de ancho de banda**. De esta forma, todas las estaciones que estén en la misma red podrán compartir la última actualización disponible. Cada estación buscará el paquete de actualización en primer lugar dentro de su LAN. Si el paquete de actualización no se encuentra en la LAN, lo obtendrá de Panda a través de Internet. Esta funcionalidad evita que las estaciones consuman excesivo ancho de banda ya que no tendrán que conectarse a Internet cada vez que necesiten actualizarse.

El panel principal de la consola web ofrece información en tiempo real sobre la **actividad de detección** en la red -por tipo de malware y fuente de infección- así como sobre la **utilización de las licencias**.

Figura 4: Consola web de Managed Office Protection

El administrador puede **monitorizar** fácilmente la actividad de detección y el grado de actualización de toda la red, crear perfiles de protección para los diversos usuarios, aplicar las **políticas** que sean necesarias y gestionar la cuarentena.

Es posible **configurar** los **informes** y **exportarlos** a diversos formatos: PDF, Excel, ficheros de texto, XML o HTML. También es posible configurar el **envío periódico** de los mismos vía email. Los informes pueden ser resumidos o detallados, con información y gráficos sobre el estado de la protección y la actividad de detección. He aquí algunos ejemplos de informes resumen e informes detallados:

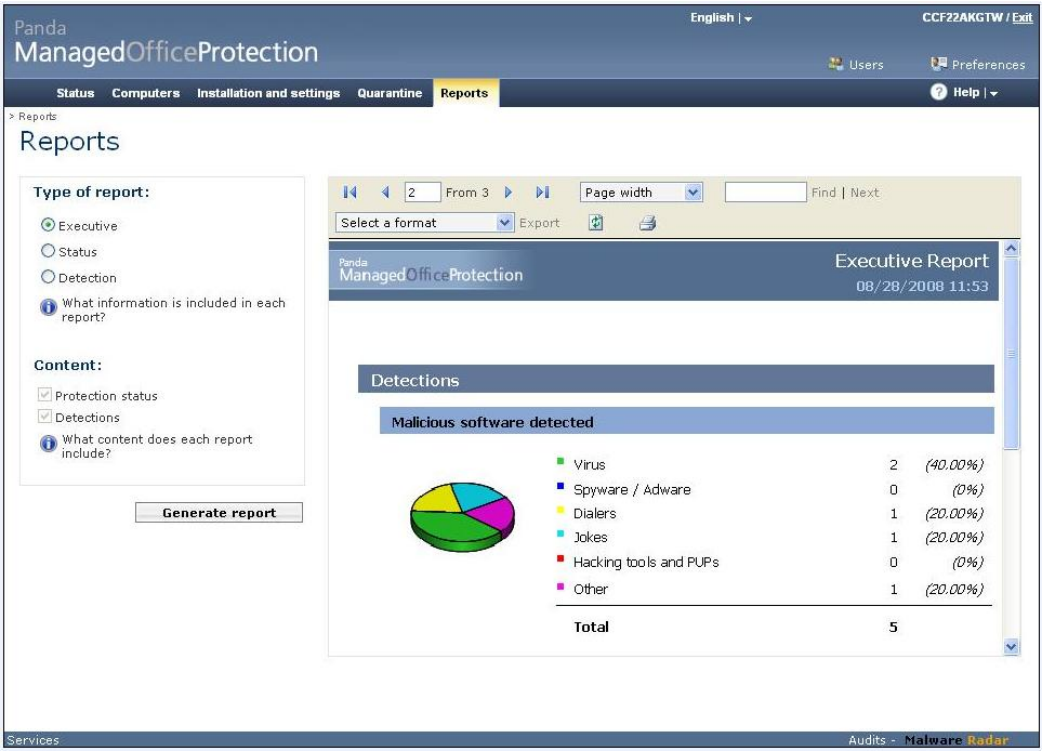


Figura 5: Consola web de Managed Office Protection – Informes resumen

Detail information

Computer	Name	Detection	Action	Date
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/20/2008 11:17
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/20/2008 03:50
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/19/2008 18:03
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/19/2008 14:01
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/19/2008 13:44
PORTÁTIL		Wrong TCP Flags Combination	Blocked	04/19/2008 06:12

Detail information

Computer	Group	Updates		Protections	Last connection
		Protection	Signatures		
BIOACABEZAS	GQA_RedGeneral Firewall Personal	✓	✓	✓	04/11/2008 13:13
BIOACASTREJON	GQA_RedGeneral Firewall Personal	✓	✓	✓	04/08/2008 09:02
BIOAFRIAS	GQA_RegGenral	✓	✓	✓	04/18/2008 12:11
BIOAINTXAURRAGA	GQA_RegGenral	✓	✓	✓	04/20/2008 11:58
BIOALOZANO	GQA_RegGenral	✓	✓	✓	04/17/2008 11:51
BIOAMARTINEZ1	GQA_RedGeneral Firewall Personal	✓	✓	✓	04/18/2008 10:57
BIOAROLDAN	GQA_RegGenral	✓	✓	✓	04/18/2008 12:38
BIODFORTEA	GQA_RegGenral	✓	✗	✗	04/18/2008 14:20
BIODIEGOMEZ	GQA_RedGeneral Firewall Personal	✓	✓	✓	04/18/2008 08:13

Figura 6: Consola web de Managed Office Protection – Informes detallados

Conclusiones

Panda Managed Office Protection es una alternativa sólida para las PYMEs que deseen:

- No tener que disponer de una infraestructura de hardware dedicada a la seguridad (Servicio Alojado)
- No tener que disponer de personal adicional especializado en seguridad
- Gestión remota. No hay necesidad de estar en las instalaciones del cliente.
- Alto nivel de seguridad para PCs, portátiles, servidores y oficinas remotas.
- Delegar la gestión de la seguridad en terceros, Proveedores de Servicios especializados. (Seguridad como Servicio, SaaS)

Céntrese en su negocio, **cambie su antivirus por la seguridad como servicio** y comience a disfrutar de sus beneficios.

Referencias

[1] Gartner Says Worldwide Software as a Service Revenue in the Enterprise Application Software Markets to Grow 21 Percent in 2007
http://www.gartner.com/it/page.jsp?id=511899

[2] Gartner, Predicts 2008: SMBs Will Use Simplified IT Solutions to Drive Business Success, December 2007

[3] Herd Intelligence Will Reshape the Anti-Malware Landscape. Yankee. Andrew Jaquith. December 2007

http://www.yankeegroup.com/ResearchDocument.do?docId=16150