

Cómo proteger el servicio de correo del malware sin necesidad de sobredimensionar los recursos dedicados al mismo

El correo electrónico es la **principal vía de penetración del código malicioso** en las empresas poniendo en peligro la reputación corporativa al poder infectar a nuestros clientes, socios y proveedores. Como consecuencia, debemos aplicar una estrategia de protección por capas que sea capaz de hacer frente en cada punto de la red al spyware, los virus y gusanos, el spam, los ataques de phishing y otras amenazas que procedentes de Internet llegan al servidor SMTP.

Sin embargo, el ahorro de recursos de almacenamiento y ancho de banda que origina el filtrado de virus y correo basura no debe hacerse a costa de complicar la administración de la protección, ni de aumentar significativamente el tiempo de respuesta del sistema.

Basta una solución antimalware fácil de usar y configurar que saque el máximo partido a los recursos informáticos disponibles en el servidor

Panda Security for Qmail ofrece una efectiva protección en tiempo real para todo el tráfico de correo SMTP que circula por los servidores y pasarelas de correo Qmail de su compañía, evitando la saturación de sus recursos y la propagación de virus y códigos malignos por su red.

Además de su avanzado motor heurístico, **Panda for Qmail** detecta y bloquea correo no solicitado automáticamente reduciendo el ancho de banda consumido y las interrupciones que sufren sus empleados. Y con la flexible configuración de esta solución, podrá incluir y excluir dominios y direcciones de correo de los análisis de manera rápida e intuitiva.

Estrategia de protección preventiva por capas

Panda Security for Qmail protege la capa perimetral de pasarelas SMTP.



Beneficios Principales

- Protege la **buena imagen** de la empresa y evita el **pago de multas** por incumplimiento de leyes reguladoras, el **espionaje empresarial**, el robo de datos, etc. al ofrecer la posibilidad de establecer políticas de seguridad.
- **Aumenta la productividad** de los usuarios finales y administradores de la red.
- **Maximiza la seguridad** de las comunicaciones vía correo electrónico porque evita la propagación de infecciones.

Características Clave

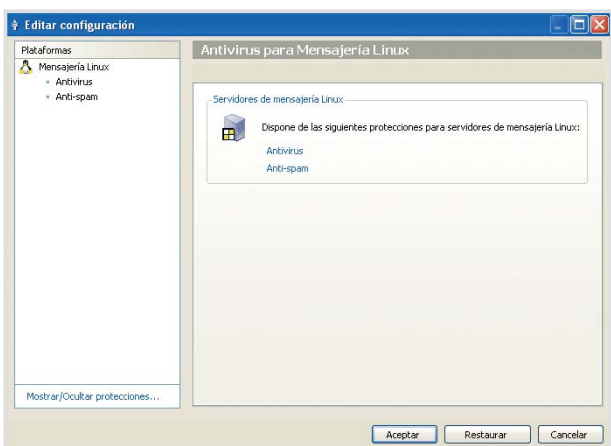
- **Análisis y desinfección en tiempo real** de todo el tráfico SMTP entrante y saliente de su organización.
- **Completa y precisa protección antispam** de fácil configuración y puesta en marcha.
- **Detección y bloqueo de código malicioso** de todo tipo: virus, gusanos, troyanos, software espía, hoaxes, ataques de phishing, marcadores telefónicos, riesgos de seguridad...
- **Flexible configuración de la protección**, de dominios y cuentas de correo a inspeccionar, así como de alertas y notificaciones del sistema.
- **Administración centralizada y remota** a través de una consola basada en web y AdminSecure, la herramienta de gestión y despliegue con interfaz Windows.
- **Perfecta integración** de la solución con los servidores de correo Qmail que protege.
- **Óptimo rendimiento de las pasarelas Linux** gracias a las avanzadas tecnologías de análisis de malware.

Análisis en tiempo real del tráfico SMTP

Panda for Qmail destaca por su capacidad de análisis en tiempo real de las comunicaciones SMTP, tanto de mensajes salientes como entrantes que deben encaminarse a otros servidores de correo. De esta manera, el sistema de correo electrónico estará protegido gracias a la detección de todo tipo de malware, aunque se oculten en mensajes o archivos comprimidos (a cualquier nivel de anidamiento en ambos casos), en documentos adjuntos o incluso en el propio cuerpo del mensaje independientemente del formato utilizado (texto o HTML).

Completa y precisa protección antispam

Panda for Qmail incorpora un avanzado motor antispam basado en **reglas, listas, patrones, algoritmos bayesianos y aprendizaje remoto** con el fin de alcanzar la máxima precisión en la determinación del correo basura impidiendo que llegue a los buzones de los usuarios. **Panda for Qmail** detecta hoaxes y el correo basura que emplea falsos mensajes NDR. Además, cuenta con varios niveles de sensibilidad, incluye remitentes y dominios en listas blancas y negras e identifica el spam en el asunto del mensaje para asistir al usuario de manera no intrusiva.



Detección y bloqueo de malware

Panda for Qmail comprueba permanentemente todo su correo en busca de malware, incluyendo virus, gusanos, troyanos, software espía, adware, ataques de phishing, marcadores telefónicos, riesgos de seguridad, etc.

Además, el avanzado *Genetic Heuristic Engine* (GHE) incorporado a **Panda for Qmail** detecta las nuevas amenazas y aísla el código sospechoso. Al mismo tiempo, solicita automáticamente un análisis diferido a Panda para proceder, a las pocas horas, a su desinfección y notificación al remitente o destinatario del mensaje.

Flexible configuración de la protección

La **flexible configuración** de **Panda for Qmail** permite que se **adapte** a sus necesidades, hasta el punto de poder configurar y seleccionar aquellos dominios y direcciones de correo que se desean analizar o excluir del análisis, así como la opción de borrar completamente el mensaje para evitar la saturación y ataques de denegación de servicio (DoS) sobre el servidor.

Administración centralizada y remota

Panda for Qmail puede administrarse en todo momento desde dos consolas de gestión completamente intercambiables con el

fin de facilitar la instalación y monitorización de incidencias y actualizaciones desde cualquier punto de la red.

Además de una consola web basada en el servidor Apache, **Panda for Qmail** admite la administración desde Windows con **Panda AdminSecure**. Esta herramienta multiidioma controla de forma remota el nivel de protección de cada servidor de correo y del resto de soluciones de Panda. Para ello, cuenta con vistas, informes gráficos, notificaciones, etc. obteniendo una visión global y en tiempo real de la protección de toda su empresa.

Completa integración con servidores SMTP

Las nuevas técnicas de propagación del malware exigen que la protección de la zona perimetral sea altamente eficaz y totalmente compatible con su sistema. **Panda for Qmail** se integra perfectamente con gateways o pasarelas SMTP bajo servidores Linux hasta el punto de poder bloquear mensajes que han sido parcialmente enviados y detectar mensajes con vulnerabilidades sin que su equipo se resienta.

Óptimo rendimiento de las pasarelas Linux

Las más modernas técnicas de desarrollo de software se han aplicado en la construcción de una solución de protección **fiable y de alto rendimiento** para servidores Qmail. Estos resultados han sido posibles entre otras por la capacidad de analizar los archivos comprimidos en memoria en lugar de utilizar el disco duro para ello.

Requerimientos técnicos

Procesador Pentium II a 200 MHz (o superior), con 64 MB de memoria RAM y 90 MB de espacio libre en disco duro. Sistema operativo para integración con AdminSecure o instalación independiente: Red Hat 7.2, 9, Red Hat Enterprise 2.1, 3 AS, 3 ES, 4 AS, 4 ES, Debian 3.0, 3.1, Mandrake 9.0, 9.1, 10, Mandrake Corporate Server 4.0, Suse 8.1, 8.2, 9.0, Suse 9.1 Professional, Suse 9.2 Professional, Suse 9 Enterprise Server, Suse 10 Enterprise Server.

Consola web: Internet Explorer 4.0 (o superior) o Netscape Navigator 4.6 (o superior).

Panda AdminSecure: Pentium III 800 MHz. 512 MB RAM. 512 MB disco duro. Sistemas operativos: Windows 2000, XP, Vista 32 bits / 64 bits y Server 2003.

"Nos decidimos por Panda Security por [...] contrastadas razones financieras. La gestión es muy simple, nos ahorra mucho tiempo y nos permite centrarnos en otras tareas diarias."

Nico Lautenbach, Director de Informática. HOLANDA.



Powered by:



Recuerde que **Panda for Qmail** se puede adquirir de forma independiente o integrado en **Panda Security for Enterprise**.