Funciones de seguridad
que ayudan a alcanzar sus objetivos comerciales

Lotus. software

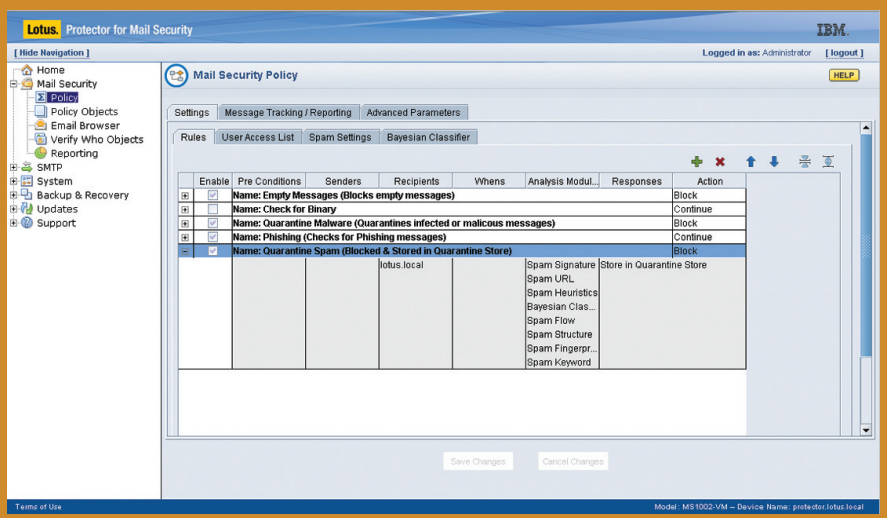
IBM

Proteja proactivamente su infraestructura de mensajería con la solución IBM Lotus Protector for Mail Security.

Protección preventiva y control de spam para su infraestructura de mensajería

Las plantillas distribuidas, equipos virtuales, empleados itinerantes y la globalización corporativa hacen del correo electrónico la aplicación más indispensable para su organización. De hecho, la productividad de su personal y la satisfacción del cliente se basan en él. Por esta razón, proteger su infraestructura de mensajería es vital para sus operaciones diarias. Sin embargo, en numerosas organizaciones, el correo electrónico está sometido al acoso no sólo del spam, sino también del phishing, ataques de denegación de servicio, robos de directorio, virus, gusanos y otras clases de código malintencionado. Además, los requisitos reguladores y otras normas sobre la gestión de la información son cada vez más estrictas. En consecuencia, su solución de seguridad para el correo debe combinar tecnologías anti-spam con una completa protección preventiva antivirus y del servidor de correo.

Como administrador de IBM Lotus® Domino®, ya sabe que el software IBM Lotus Domino es una de las plataformas más seguras que existen. Sin embargo, algunos riesgos para la seguridad tienen su origen en Internet, fuera del entorno Lotus Domino, lo que usted no siempre puede controlar. Ahora existe una solución que no solamente puede proporcionarle la protección que necesita, sino, además, simplificar sus procesos administrativos. La solución IBM Lotus Protector for Mail Security, primer producto de una amplia línea de ofertas de seguridad prevista actualmente para el software Lotus Domino[1], dota de protección preventiva y control de spam a su infraestructura de mensajería, al tiempo que simplifica la administración gracias a su perfecta integración con la plataforma IBM Lotus Notes® y Lotus Domino ya existente. Esta solución ayuda a garantizar la conformidad del contenido saliente y el cumplimiento de las políticas de usos permitidos mediante módulos de análisis personalizables diseñados para ser fácilmente adaptables a las diversas necesidades de las empresas. Además, la tecnología de Lotus Protector for Mail Security es un elemento clave de la suite de productos Lotus Protector, concebida para ayudarle a subsanar los riesgos de seguridad que puedan afectar al entorno Lotus Domino.



La solución Lotus Protector for Mail Security puede descargar actualizaciones del IBM Internet Security Systems™ (ISS) Global Data Center cada 60 minutos para ayudarle a responder a las nuevas amenazas y tácticas de spam.

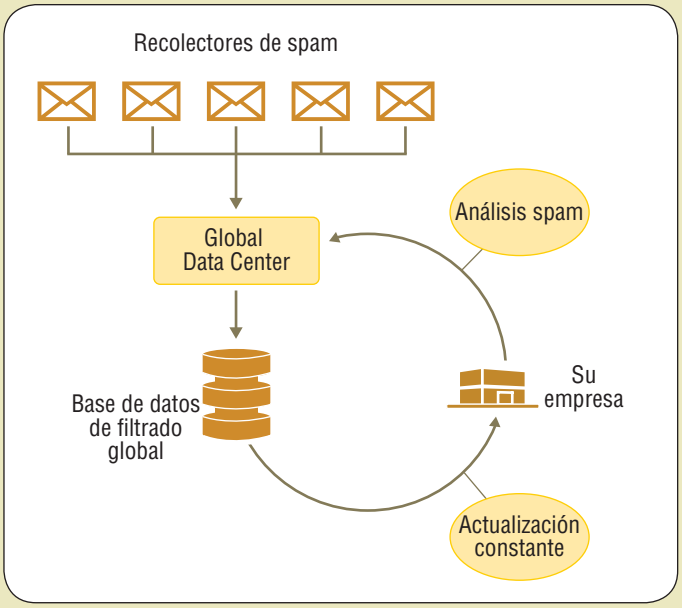
No sólo control de spam

El spam continúa filtrándose diariamente en las bandejas de entrada, en ocasiones superando en número a los correos electrónicos legítimos. La lucha contra el spam puede perjudicar a la productividad y forzar la capacidad de redes y servidores, lo que afecta tanto a los usuarios finales como a los administradores del sistema.

Optimizada para la plataforma Lotus Notes y Domino, la solución Lotus Protector for Mail Security reduce la carga de spam de varias maneras. En primer lugar, puede configurarse rápidamente para bloquear el spam empleando políticas de filtrado, tanto por defecto como personalizadas. La innovación en el filtrado de contenidos viene dada por el equipo de investigación y desarrollo de la IBM ISS X-Force®. El equipo de la X-Force estudia a diario las nuevas técnicas y métodos de distribución de spam. Por defecto, la solución Lotus Protector for Mail Security comprueba cada hora si hay actualizaciones de IBM que incluyan nuevas identificaciones de spam y URL potencialmente peligrosas. Como resultado, la tecnología de Lotus Protector for Mail Security le permite anticiparse a las últimas tendencias en spam, incluyendo fraudes bursátiles y spam basado en imágenes.

Además, la solución incluye tecnología de filtrado dinámico de host por reputación — la cual hace uso de la sofisticada investigación de IBM sobre los puntos de origen más probables del spam — con el fin de detener el spam antes incluso de que llegue a su sistema. Analizando la dirección IP de origen de todos los correos recibidos, puede dictaminar matemáticamente si la fuente de éstos es fiable o no. Cuando se considera que un correo proviene de una fuente poco fiable, se interrumpe la conexión antes de que éste sea entregado. Como resultado, ayuda a reducir la carga del sistema asociada con el tratamiento del spam evitando que éste llegue en primer lugar al filtro.

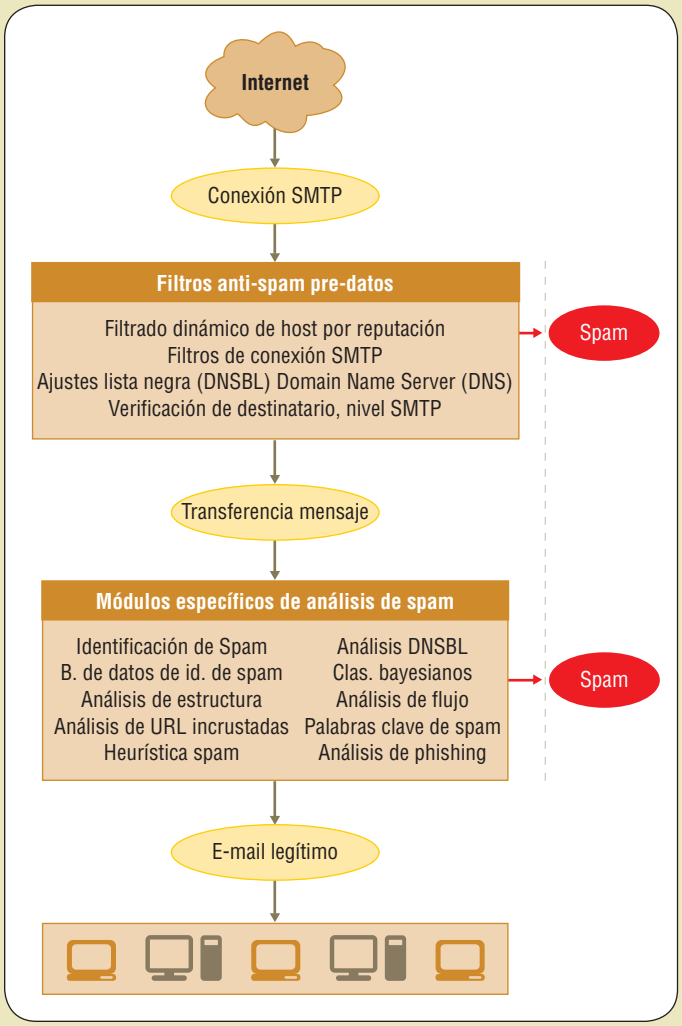
En el IBM ISS Global Data Center, IBM mantiene una base de datos de seguridad que contiene más de 95 millones de páginas Web e identificaciones relevantes de spam hasta la fecha. IBM dispone de “recolectores de spam” en todo el mundo, los cuales emplean cuentas de correo electrónico, denominadas “honey pots”, que reciben cientos de miles de correos con spam confirmado todos los días. Los datos reunidos a partir de estos mensajes se transmiten al Global Data Center. IBM ha establecido, además, una red de IBM Business Partners y usuarios corporativos IBM de confianza que aportan datos sobre el spam a la base de datos. Las tecnologías de protección anti-spam de IBM hacen uso de los datos recogidos de todas estas fuentes para incrementar la eficacia del filtrado. Asimismo, con la característica opcional Spam Learn, IBM permite enviar informes anónimos automáticos al Global Data Center para su inclusión en la base de datos.



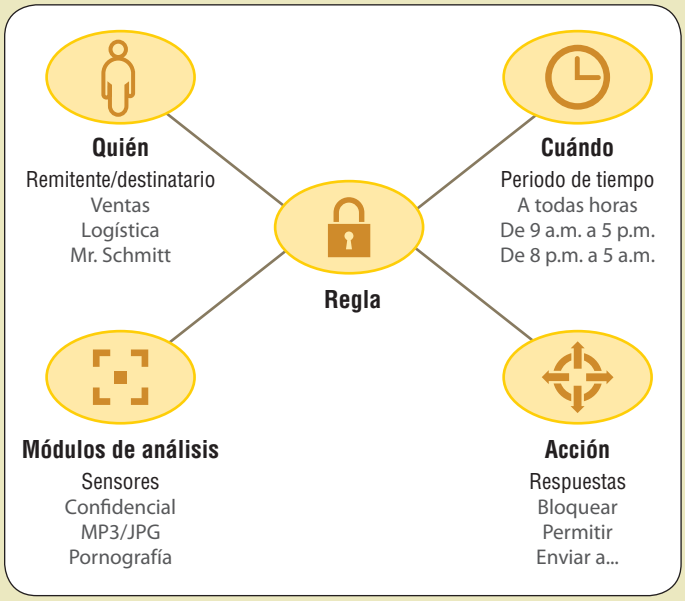
La solución Lotus Protector for Mail Security recibe actualizaciones del IBM ISS Global Data Center ocho veces al día para ayudarle a responder a las nuevas amenazas y tácticas de spam.

Más de 20 módulos de análisis personalizables para ayudarle a satisfacer sus necesidades específicas

La tecnología de Lotus Protector for Mail Security combina múltiples módulos de análisis para una mayor personalización, lo que le permite definir políticas o adaptarlos para cumplir los requisitos legales y normativos relacionados con los datos. Es igualmente posible detectar palabras ofensivas, términos clave personalizables y tipos de adjuntos, mientras que sus funciones de análisis especializadas evitan que información confidencial, como los números de la seguridad social y de las tarjetas de crédito, lleguen a salir de su red. Además, el módulo de phishing dispone de una técnica de análisis independiente con el fin de proteger a sus empleados contra mensajes de correo electrónico destinados a obtener sus datos personales.



La solución Lotus Protector for Mail Security filtra el spam antes de que llegue a su red, ahorrando un valioso ancho de banda.



Puede desarrollar reglas de filtrado de spam acordes con las políticas de su organización y adaptarlas a cada usuario.

La configuración de reglas facilita su uso, reduciendo la carga del personal administrativo

El control granular de política incluye la creación de políticas sencilla a partir de reglas — lo que permite actuar basándose en factores como quién, qué y cuándo — y más de 10 tipos de actuación personalizables distintos, como modificaciones y notificaciones. Las políticas pueden aplicarse generalmente, por grupo de usuario o por usuarios individuales. Además, la solución Lotus Protector for Mail Security es compatible con Lightweight Directory Access Protocol (LDAP), lo que incluye las tecnologías Lotus Domino y Microsoft® Active Directory. Los usuarios finales pueden crear sus propias listas de permisos y bloqueos, por lo que pueden controlar personalmente sus preferencias anti-spam. También pueden ver y controlar los mensajes puestos en cuarentena si el administrador lo autoriza.

Anticípese a las amenazas para sus sistemas de mensajería

Aparte del control de spam, la solución Lotus Protector for Mail Security dispone de tecnologías de protección avanzadas con funciones de seguridad que se anticipan a las amenazas. Gracias al galardonado motor IBM Proventia® Network Intrusion Prevention System (IPS) y la tecnología IBM Virtual Patch®, la aplicación contribuye a mejorar la seguridad esencial necesaria en los entornos de TI actuales.

La seguridad de la capa de transporte proporciona un nivel adicional de protección entre su empresa y sus socios o proveedores

La compatibilidad con el protocolo Transport Layer Security (TLS) permite encriptar automáticamente todos los correos electrónicos intercambiados entre su empresa y sus socios y proveedores de confianza. Estableciendo certificados públicos mutuos en su servidor puede asegurarse de que la comunicación entre su empresa y estas organizaciones está protegida. El agente de transporte de mensajes situado en el límite de su red encripta automáticamente todos los correos electrónicos enviados a y desde dichas organizaciones, proporcionando una experiencia de usuario satisfactoria.

La tecnología de verificación de destinatarios y el mecanismo de disposición en cola garantizan que su infraestructura de mensajería no se verá comprometida

La tecnología de verificación de destinatarios y el mecanismo de disposición en cola de la solución protegen su servidor de correo frente a ataques de día cero, incluyendo denegación de servicio y robo de directorio.

Muchos spammers dirigen su spam hacia un dominio concreto simplemente adivinando nombres de usuarios o sus convenciones de nomenclatura. La tecnología de verificación de destinatarios minimiza los efectos de esta práctica confirmando que el nombre de usuario específico al cual está destinado el correo electrónico existe realmente antes de aceptar el mensaje. Todo mensaje dirigido a un destinatario desconocido se rechaza antes de aceptar la conexión, lo que ayuda a ahorrar un valioso ancho de banda.

Todas las ofertas de Lotus Protector están concebidas para su fácil integración en su entorno de usuario y seguridad Lotus Domino existentes, lo que proporciona una experiencia de usuario perfecta y simplifica su administración general.[1]

El mecanismo de cola está diseñado para proporcionar varios niveles de protección contra ataques de denegación de servicio basados en spam. La aplicación tiene dos umbrales predefinidos para la cola no verificada, que comienza a crecer durante un ataque de denegación de servicio. Cuando el número total de mensajes en la cola no verificada alcanza el primer umbral, la aplicación comienza a regular las nuevas conexiones Simple Mail Transfer Protocol (SMTP) en función de un periodo de tiempo predefinido. Cuando el número de mensajes de la cola no verificada llega al segundo umbral, todas las nuevas conexiones SMTP reciben como respuesta un mensaje con el texto “temporarily not available” (no disponible temporalmente) y solicitando que se intente más adelante, de acuerdo con las normas SMTP. Los spambots típicos no admiten este tipo de rechazo y fallan al llegar a este punto, mientras que los servidores SMTP válidos lo volverán a intentar transcurrido un periodo de tiempo predeterminado.

La protección antivirus multicapa ayuda a bloquear los virus de día cero en tiempo real

La solución Lotus Protector for Mail Security incluye detección remota de malware, que se distribuye automáticamente a su aplicación mediante la actualización de las identificaciones de la base de datos de filtrado. Además, las tecnologías de genotipo de comportamiento e identificación de virus actúan contra los códigos sospechosos para detectar virus conocidos o desconocidos. Esta tecnología analiza tanto los correos electrónicos recibidos como salientes de forma paralela a los componentes anti-spam de la aplicación.

Funciones de administración inteligentes para facilitar su utilización

La solución Lotus Protector for Mail Security proporciona diversas funciones de administración inteligentes que pueden adaptarse al entorno de red específico de su organización. Éstas incluyen:

- **Una interfaz de administración local independiente, segura y basada en Web.** La interfaz ofrece un acceso sencillo a las políticas de seguridad y anti-spam.
- **Informes estándar o personalizados.** Los informes estándar centralizados aportan información valiosa que permite identificar, por ejemplo, cuáles son los spammers que causan más problemas a la infraestructura de mensajería. También es posible crear informes personalizados para mayor flexibilidad.
- **Función de agrupación excepcional.**[2] Debido a que no se necesita una consola de administración separada, es posible administrar fácilmente varios servidores a través de un solo dispositivo. De hecho, la tecnología Lotus Protector for Mail Security proporciona acceso a todos los mensajes puestos en cuarentena e información de búsqueda a través del equipo designado como dispositivo central, con independencia del punto de entrada inicial del tráfico en la red.

La solución IBM Lotus Protector for Mail Security es eficaz

Creada para proteger a organizaciones de todos los tamaños, la aplicación está disponible tanto en forma de equipo de hardware como de dispositivo virtual. En ambas formas se actualiza automáticamente para mantener a raya al spam, los virus y otro tráfico malintencionado. Si está migrando hacia la virtualización dentro de su empresa para beneficiarse de la avanzada tecnología de procesadores actual, ejecutar la tecnología Lotus Protector for Mail Security en un entorno virtualizado ofrece un coste total de propiedad muy atractivo, un despliegue inmediato y operaciones de copia de seguridad y recuperación sencillas.

Una plataforma unificada para responder a sus problemas de seguridad

Cree una plataforma unificada para mitigar sus problemas de seguridad. Infórmese acerca de cómo la solución Lotus Protector for Mail Security puede ayudar a resolver los quebraderos de cabeza que supone la protección de los mensajes y mejorar su política de seguridad contra futuras amenazas como parte de la dinámica plataforma Lotus Protector. Diseñada específicamente para el entorno Lotus Domino, esta aplicación se integra perfectamente en la plataforma Lotus Domino, simplificando la administración de su entorno de mensajería.

Especificaciones técnicas del equipo MS3004LP	
Unidades de bastidor	2U
Capacidad de ampliación	Capacidad de agrupación para grandes despliegues
Rendimiento máximo	Visite ibm.com/software/lotus/protector para ver datos actualizados
Almacenamiento	4 x 80 GB + 2 x 250 GB (RAID1)
Redundancia	Disco duro, fuente de alimentación y ventiladores
Dimensiones	• Altura (mm/in): 86,36/3,40 • Anchura (mm/in): 482,6/19 • Profundidad (mm/in): 609.6/24 • Peso (kg/lb): 27/60
Disipación de potencia	• Unidades: CA • Voltaje (V): 115/220 • Intervalo de entrada (V): 100–127/200–240
Temp. de funcionamiento	+10 ˚C a +35 ˚C (+50 ˚F a +95 ˚F)
Temperatura (apagado)	-40 ˚C a +70 ˚C (-40 ˚F a +158 ˚F)
Humedad relativa (apagado)	95% a 30 ˚C (90 ˚F)
Emisiones	Clase A FCC

Especificaciones técnicas del dispositivo virtual	
Capacidad de ampliación	Idóneo para empresas de tamaño pequeño a medio con menos de 1.000 usuarios y ampliable a especificaciones más estratégicas según sea preciso, dependiendo de la base de hardware
Requisitos del sistema	Los siguientes son los recursos de sistema mínimos necesarios para instalaciones virtuales VMware. Uno de los siguientes: • VMware Server 1.0.2 o posterior • VMware Workstation 5.5 o posterior • VMware Player 1.0.3 o posterior • VMware ESX 3.x o posterior Hardware del host: • 2 GB de RAM (512 MB necesarios para cada instancia virtual) • 100 GB de espacio en disco duro (30 GB exclusivos para cada instancia virtual) • Dos interfaces de red: – Una interfaz únicamente para host – Una interfaz de red enlazada Requisitos de hardware virtual (para cada instalación virtual): • 512 MB de RAM (como mínimo) • 30 GB de espacio en disco

Para más información

Para más información sobre servicios complementarios para los productos Lotus e IBM WebSphere® Portal, visite:

ibm.com/software/lotus/services

Para más información sobre la solución IBM Lotus Protector for Mail Security, póngase en contacto con su agente de ventas IBM o visite:

ibm.com/software/lotus/protector

Lotus Software
IBM Software Group
One Rogers Street
Cambridge, MA 02142
EE.UU.

Producido en los Estados Unidos de América
07-08

1 Estas afirmaciones representan los planes y directrices actuales de IBM y pueden ser modificadas sin previo aviso.

2 Solamente disponible en MS3004LP. El agrupamiento no implica alta disponibilidad.

LOB14005-USEN-01