

BITDEFENDER SECURITY FOR MAIL SERVERS

LA NECESIDAD DE PROTEGER LOS BUZONES DE CORREO Y MANTENERLOS LIBRES DE SPAM

El e-mail se ha convertido en un servicio indispensable que las empresas necesitan proteger a cualquier precio. Cuando el servidor de correo deja de funcionar, también lo hace su negocio. El impacto de la pérdida de productividad, combinado con un brote grave de virus propagado vía e-mail, puede poner en una situación muy complicada a la empresa. Muchas empresas consideran importante el impacto interno que pueden provocarles virus propagados vía e-mail, pero aún debe ser mayor la preocupación que pueda causarles la pérdida de reputación y los daños accidentales causados si un empleado envía un e-mail infectado a socios o clientes. El daño provocado en la reputación de una empresa puede ser irreversible.

El sistema de e-mail de una empresa proporciona una de las principales entradas y salidas dentro de una red para la propagación de código malicioso y fuga de datos. Por tanto, las soluciones de seguridad de correo deben ser capaces de contrarrestar las diferentes amenazas que aprovechan el sistema de e-mail de una empresa para propagarse – estos incluyen:

- Envío o recepción de código malicioso a través de adjuntos de correo.
- Comunicación no solicitada en forma de spam.
- Intentos de phishing para sustraer información confidencial.
- Suministro de información confidencial vía e-mail por parte de usuarios legítimos.
- Ataques de Directorio, Dictionary Harvesting Attacks (DHA).

Debido a los mecanismos utilizados para propagar amenazas por e-mail, éstas se están volviendo cada vez más virulentas y puede ser demasiado tarde el detenerlas en el equipo cliente. Por tanto, una solución implementada en la red y el servidor de correo puede minimizar el impacto del malware a la hora de limpiar documentos infectados y garantizar la protección de los activos críticos de la empresa.

PROTEGIENDO LOS SERVICIOS DE EMAIL CON BITDEFENDER

BitDefender Security for Mail Servers protege servidores basados en Windows o UNIX frente a amenazas de seguridad conocidas y desconocidas mediante su protección antivirus, antispymware, antispam, antiphishing y sus premiadas tecnologías de filtrado de contenido y adjuntos. Esta solución protege los servicios de correo electrónico de la empresa y proporciona una mejora en la productividad bloqueando el spam y proporcionando herramientas comunes de administración centralizada.

BitDefender Security for Mail Servers analiza los emails en múltiples niveles comprobando primero si el servidor de correo del remitente es sospechoso o está bloqueado y, después, si el contenido o sus adjuntos contienen código malicioso o encajan con las reglas relacionadas con el spam.



CARACTERÍSTICAS PRINCIPALES Y BENEFICIOS

- Análisis del tráfico entrante de correo para garantizar la protección en tiempo real frente al malware y minimizar así el riesgo de propagación de virus a través de la red.
- Análisis del correo saliente para evitar que las amenazas de seguridad se extiendan a socios y clientes.
- Análisis del correo una sola vez mediante el uso del método de análisis seleccionado, para minimizar la carga del servidor.
- Filtro de Contenido para e-mails entrantes y salientes, identificando las palabras específicas que contienen, definidas por el administrador tales como datos de la tarjeta de crédito.
- Alta Precisión en los filtros Antispam y Antiphishing con la Tecnología Heurística NeuNet.
- Protección de directorio de usuario frente a ataques de directorio utilizados por spammers que intentan obtener direcciones de correo legítimas mediante técnicas de fuerza bruta.
- Configuración remota de cualquier equipo de la empresa a través del Servidor de Administración Centralizado de BitDefender.
- Reducción de los costes de recursos y gastos generales para incrementar la productividad global empresarial.
- Disminución del tiempo de inactividad de la red para incrementar la eficiencia operativa.

TECNOLOGÍAS BITDEFENDER

b-have Todas las soluciones BitDefender incluyen B-HAVE, tecnología pendiente de patente, que analiza el comportamiento de códigos potencialmente peligrosos dentro de una máquina virtual, eliminando así los falsos positivos y aumentando significativamente la tasa de detección frente a malware nuevo y desconocido.

NeuNet Para combatir mejor las nuevas oleadas de spam, los laboratorios de BitDefender han creado el potente filtro antispam NeuNet. En los laboratorios antispam, NeuNet es preentrenado sobre una serie de mensajes para que aprenda a reconocer el nuevo tipo de spam percibiendo sus similitudes con los mensajes que ya ha examinado.

DEFENSA EN PROFUNDIDAD

BitDefender Security for Mail Servers es solamente un elemento dentro de un conjunto integral de soluciones que proporcionan protección de red de extremo a extremo, desde la puerta de enlace hasta el escritorio. Las soluciones proactivas y multiplataforma de BitDefender detectan y detienen las amenazas de virus, spyware, adware y troyanos que puedan comprometer la integridad de su red.

REQUISITOS DEL SISTEMA

Sistemas Operativos basados en Windows:

- Windows Server 2000 SP4 + Update Rollup 1
- Windows Server 2003 con SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Internet Explorer version 6.0 o posterior

Sistemas Operativos basados en UNIX:

- Linux, FreeBSD, Solaris
- Linux Kernel: 2.6.18 o posterior
- glibc: 2.3.1 o posterior, libstdc++ de gcc 4 o posterior

Distribuciones Admitidas:

- Debian GNU/Linux 3.1 o posterior
- Fedora Core 1 o posterior
- FreeBSD: 5 (o posterior con compat5x)
- Mandrake/Mandriva 9.1 o posterior
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 o posterior
- OpenSolaris 2008 o 2009 (x86 plataforma)
- Oracle Linux 5 o posterior
- RedHat Enterprise Linux 3 o posterior, Linux 9 o posterior
- Slackware 9.x o posterior
- Solaris 9 o 10 (plataforma x86)



Protección Proactiva



Administración Centralizada



BitDefender Security for Mail Servers ofrece protección proactiva y administración centralizada de los servicios de correo

PROTECCIÓN Y DETECCIÓN PROACTIVA AVANZADA

Los galardonados motores de análisis de BitDefender han sido reconocidos por los principales organismos de certificación - incluyendo ICISA Labs, Virus Bulletin y West Coast Labs - por su efectiva protección proactiva antimalware. BitDefender proporciona múltiples niveles de protección avanzada:

Antivirus. Además de la detección basada en firmas, BitDefender proporciona la detección heurística que emula una máquina virtual dentro del equipo, comprobando todos los archivos y códigos en busca de comportamiento malicioso. Esta técnica produce menos falsos positivos y una mayor tasa de detección para las amenazas desconocidas y de "día cero".

Antispam. Mediante el uso de listas blancas y negras de conocidos sitios de spam, constantemente actualizadas, el aprendizaje Bayesiano proporciona otra capa de detección que se adapta a los cambios realizados por los spammers para los filtros de spam estáticos.

Antispyware. BitDefender detecta y previene el spyware y adware conocidos a través de diversos métodos de filtrado diferentes para prevenir las infecciones por spyware que puedan causar fuga de información.

Antiphishing. Si bien se considera más una amenaza para usuarios domésticos que corporativos, los sitios de phishing pueden también sustraer información de sus empleados. Utilizando una combinación de listas negras constantemente actualizadas y unas reglas de inspección de contenido configurables, BitDefender bloquea mensajes que piden a los usuarios que accedan a sitios de phishing, evitando así comprometerlos.

Filtrado de Contenido. El filtrado de contenido permite la detección de información predefinida, como puede ser la información de tarjetas de crédito o cuentas bancarias, nombres de informes, bases de datos de clientes, etc., para evitar que se escape del control de la empresa.

Protección contra Ataques de Recolección de Directorio (DHA). Utilizado por los spammers para obtener direcciones e-mail válidas o existentes, la recolección de directorios es más efectiva a nivel empresarial debido a que se ajustan más a un estándar. Los e-mails pueden utilizarse para eludir los filtros de spam y dirigirse a usuarios legítimos.

Lista Blanca/Lista Negra para excluir determinados servidores de correo o permitir ciertos servidores de correo de confianza, con opción de validación de sus direcciones IP para que coincidan con el dominio del remitente.

OPCIONES DE ANÁLISIS SEGURAS Y CONFIGURABLES

BitDefender Security for Mail Servers proporciona métodos de análisis continuo, bajo demanda, de transporte y en profundidad, para detectar código malicioso con el objetivo de salvaguardar la integridad de los servicios de correo electrónico. Los e-mails se analizan una sola vez y puede incluirse un pie de página opcional en cada mensaje como medio para validar su seguridad y proporcionar garantías al usuario final. Pueden configurarse métodos de análisis adicionales para el contenido, evitando que se envíe información confidencial a través de e-mails salientes a destinatarios externos desconocidos.

