

Forefront Security de Microsoft para Exchange Server

Protección Multi-motor frente a las amenazas contra la seguridad del correo electrónico

Forefront Security de Microsoft® para Exchange Server incluye múltiples motores de análisis de firmas de virus de las empresas de seguridad más importantes del sector, integrados dentro de una solución única para una máxima protección del entorno de correo electrónico Exchange frente a virus, gusanos y spam.

Microsoft Forefront Security para Exchange Server es uno de los múltiples productos que ofrece Microsoft en su portfolio de Seguridad. Anteriormente conocido como Antigen para Exchange, este apreciado producto se encuentra en su décima iteración, presentado ahora bajo la marca Forefront. Se distribuye con múltiples motores de análisis para establecer una barrera de protección amplia y a diferentes niveles para los servidores Exchange de correo electrónico y además optimiza el rendimiento de estos servidores y simplifica la gestión de la seguridad.

Los virus en el email siguen siendo la amenaza más peligrosa para las empresas en términos de pérdidas de servicio y productividad*. Los virus, gusanos, spam y demás malware pueden paralizar las comunicaciones, saturar los recursos del servidor, colapsar los sistemas, y provocar la detención de la actividad en la empresa. A pesar de que casi el 97 por ciento de las organizaciones utilizaron software antivirus en el 2006, el 65 por ciento ha sufrido ataques de virus*.

¿Por qué ocurre esto? Una de las razones es que las empresas tratan de proteger a todos los servidores de misión-crítica utilizando software con un único motor de análisis antivirus. Si el motor no alcanza a reconocer de forma inmediata la nueva amenaza, el virus puede extenderse a través de la organización al romper las barreras protectoras en cada uno de los nodos de la red que utilizan el mismo motor vulnerable.

Por otro lado las prácticas de defensa extremadamente restrictivas tienen también desventajas ya que bloquean mensajes enteros cuando solamente una parte es sospechosa, ocasionando la pérdida de correo vital para el cliente.

Escanear cada mensaje en cada servidor retrasa su entrega y supone un derroche de recursos. La instalación y gestión de múltiples productos antivirus no integrados provoca verdaderos quebraderos de cabeza a los administradores. El escaneado redundante de correos anteriores, sin importar su antigüedad agota los recursos del servidor.

Todo esto se va acumulando y provoca la ralentización en el envío de los mensajes, una mayor vulnerabilidad en algún punto, enormes costes de gestión y pérdida de productividad.

Incrementar las Oportunidades sin Incrementar los Gastos

Microsoft Forefront Security para Exchange Server resuelve estos problemas proporcionando una protección antivirus de amplio alcance y a diferentes niveles, que además preserva el rendimiento del servidor, optimiza su ejecución y simplifica la gestión de los sistemas de seguridad Exchange Server.

Una amplia protección contra las más recientes amenazas

Forefront Security para Exchange Server integra varios motores antivirus, ofrecidos por varios fabricantes líderes en seguridad, para maximizar la protección contra las amenazas. Los administradores de IT pueden activar hasta cinco motores de análisis al mismo tiempo y en varias capas a través del entorno de Exchange Server. Cuando un motor se detiene para una actualización, los otros continúan escaneando el correo en los servidores de Exchange 2007 perimetrales, concentradores y de almacenamiento — incluso el correo proveniente de teléfonos. Las actualizaciones de las firmas para todos los motores son rápidas y automatizadas lo que refuerza la protección contra nuevas amenazas en cuanto aparecen.

En la protección contra spam, Forefront Security para Exchange Server aprovecha

las tecnologías y filtros antispam más innovadoras que incorpora Exchange 2007 y ayuda a mantenerlos al día con actualizaciones automatizadas. Además con sus tecnologías heurísticas y sus filtros de archivo protege a la empresa contra nuevas amenazas detectando el virus por su comportamiento y capturando archivos peligrosos, como los ejecutables, aunque se hayan modificado las extensiones.

Máximo rendimiento para mantener activo el servicio de correo electrónico

Forefront Security para Exchange Server se integra con Exchange 2007 para evitar repeticiones innecesarias del análisis de los mensajes después de haber pasado el control de seguridad del primer servidor. Al evitarse estas redundancias en el tráfico, el correo fluye a mayor velocidad y los servidores no se ralentizan por sobrecarga.

Para mejorar su operatividad en los servidores de almacenamiento, los administradores de IT pueden, de forma selectiva, escanear los buzones de correo en busca de los más susceptibles de portar un virus.

Este análisis incremental realizado en background libera recursos del servidor ya que evita tener que volver a analizar miles de correos antiguos.

Gestión simplificada para aligerar la carga de trabajo de los departamentos de IT

La actualización automática de archivos de firmas y los motores de análisis, la protección de la migración a servidores Exchange 2007 y un control y gestión centralizadas conducen a una mayor eficacia y reducción de costes. La configuración de Forefront Security para Exchange Server puede centralizarse, instalarse y actualizarse en entornos multiservidor utilizando el Microsoft® Forefront™ Server Security Management Console. Además da soporte a Microsoft Operations Manager (MOM), para la monitorización de los servidores Exchange en todo el ámbito corporativo.

Funcionalidades y características de Microsoft Forefront Security para Exchange Server

Protección total

- **Escaneado multimotor sin puntos únicos de fallo.** Replica y gestiona automática y simultáneamente hasta cinco motores scan antivirus y utiliza distintas combinaciones para servidores Exchange 2007 de transporte (perimetral, "Edge" y concentrador, o "Hub") y de almacenamiento (Buzones/carpetas públicas). Además, si alguno de los motores está fuera de línea o no ha detectado una amenaza, el correo sigue siendo analizado por los otros motores, evitando el punto único de fallo. El producto opera con motores de Ahnlab, Authentium, CA, Kaspersky Labs, Microsoft, Norman Data Defense, Sophos, y VirusBuster.
- **La mejor protección antispam.** Forefront Security para Exchange Server dispone el mejor servicio antispam para Exchange 2007, que incluye Microsoft IP Reputation Service, Intelligent Message Filters (IMF) para filtrar los contenidos, y archivos de firmas antispam. Estas herramientas se activan durante la instalación y se actualizan automáticamente varias veces al día.
- **Protección multinivel.** Permite instalar y activar varios niveles de verificación para que en caso de que falle algún escáner en el servidor perimetral, el correo se siga analizando en los hubs. Esta protección multinivel supone una barrera fundamental para detener ataques maliciosos antes de que afecten a la red o a la productividad del usuario final.
- **Protección contra amenazas nuevas y ocultas.** Bloquea el código malintencionado analizando su comportamiento, para lo que aplica una tecnología heurística propia y permite configurar reglas para filtrar archivos y eliminar los archivos habitualmente empleados como portadores de virus (por ejemplo, .exe), aunque se haya cambiado la extensión del archivo. Forefront Security para Exchange Server puede también descomprimir y volver a comprimir archivos adjuntos (p.ej. archivos .zip) de manera selectiva, después de haber eliminado un correo infectado o no deseado.
- **Respuesta de multivendedor frente a nuevas amenazas.** Aumenta la capacidad de detección para resolver cualquier nuevo ataque en un tiempo mínimo. Con Forefront Security para Exchange Server, múltiples fabricantes trabajan en su beneficio para bloquear el acceso de los virus más recientes. El acceso a cualquier actualización se hace mediante descargas automáticas que garantizan la disponibilidad inmediata de una solución tan pronto se desarrolla en los laboratorios de los fabricantes de antivirus.

Rendimiento optimizado

- **Configuraciones que garantizan el máximo rendimiento.** Mejora el funcionamiento del servidor y el rendimiento del correo ejecutando el análisis en memoria (para evitar el encolamiento de datos hacia el disco duro) y en varios threads simultáneos (para procesar más cantidad de correo en menos tiempo). Forefront Security para Exchange Server también ayuda a conseguir un buen equilibrio entre el rendimiento del servidor y el nivel de seguridad mediante controles de rendimiento con los que se pueden administrar dinámicamente el número de motores que han de utilizarse para una tarea de análisis concreta.
- **Escaneo más eficiente en el transporte y almacenamiento.** Elimina análisis redundantes de los mensajes. Forefront Security para Exchange Server asigna a cada correo una marca en la cabecera para indicar que está libre de virus cuando se escanea por primera vez en el servidor perimetral o en un hub de Exchange 2007. El correo se encamina sin más análisis, ahorrando carga de procesamiento a los demás servidores hub y de almacenamiento. Además el servidor de almacenamiento evita el análisis de los correos con antigüedad superior a un determinado número de semanas, reduciendo más aún la carga de trabajo. El análisis incremental en background se puede configurar para que afecte únicamente a los correos que tienen más probabilidades de estar infectados, como son los que tienen una antigüedad de pocos días.
- **Flujo de correo sin interrupción durante las actualizaciones.** Mantiene las firmas del motor de análisis al día sin originar encolamientos o retenciones del correo. La solución multimotor de Forefront Security para Exchange Server permite que un motor esté fuera de línea por una actualización, mientras otros motores siguen en línea analizando el correo.
- **Alta eficiencia en entorno de cluster.** Mantiene la seguridad del correo electrónico en caso de fallo de un nodo y paso de la actividad a otro dentro de un cluster. Forefront Security para Exchange Server garantiza que ambos nodos, tanto el activo como el pasivo, mantienen sus firmas de virus actualizadas, así como la configuración y demás información de seguridad. Soporta configuraciones de cluster CCR de Exchange Server 2007

Gestión Simplificada

- **Forefront Server Security Administrator.** Con esta consola de gestión integrada se puede configurar totalmente el entorno de Forefront Security para Exchange Server de forma local o remota.

- **Control centralizado y basado en la Web.** La consola de gestión de Forefront Security para Exchange resuelve de manera sencilla la administración remota de servidores, genera informes completos y recibe alertas de ataque en cualquier punto de la infraestructura de correo. Esta consola de administración es el punto central para la configuración, instalación y actualización de todos los productos de seguridad de la familia Forefront.
- **Proceso unificado de actualización.** Actualiza múltiples motores de análisis sin intervención del personal de IT. Desde Microsoft se hace un seguimiento continuo de las novedades de los fabricantes de antivirus para obtener nuevas firmas y actualizaciones de sus motores. En unos minutos estas actualizaciones se contrastan con una base de datos de virus, se confirman y se lanzan para una descarga automática desde los sistemas Forefront Security para Exchange Server o desde la Consola de Gestión.
- **Protección de migraciones.** Ayuda a mantener todo el entorno de correo protegido durante una migración a Exchange 2007. Con la compra de licencias de Forefront Security para Exchange Server para proteger los servidores Exchange 2007 los clientes dispondrán también de licencia para usar Microsoft Antigen para Exchange, Microsoft Antigen para Gateways SMTP, y Antigen Spam Manager para proteger sus entornos Microsoft Exchange Server 2003 y Microsoft Exchange Server 2000.
- **Disponible en 11 idiomas.** Administra la seguridad del entorno de correo en inglés, alemán, francés, japonés, italiano, español, coreano, chino (simplificado), chino (tradicional), portugués (Brasil) y ruso.
- **Monitorización integrada.** Mediante el correspondiente paquete de gestión de System Center Operations Manager, se puede monitorizar la salud del entorno Forefront Security para Exchange Server dentro de las operaciones habituales de la organización.

Requisitos del sistema para Microsoft Forefront Security para Exchange Server

Todas las funcionalidades descritas requieren Windows Server® 2003, Microsoft Exchange Server 2007, un equipo con arquitectura basada en procesador de 64 bits, 512MB de RAM mínimo por servidor (recomendado 1 GB), y 300MB de capacidad de disco. Forefront Security para Exchange Server soporta instalaciones de Exchange basadas en Microsoft Cluster Server.

Para más información sobre Microsoft Forefront Security para Exchange Server, visite <http://www.microsoft.com/forefront>.