SONICWALL

Dispositivos y software Email Security

Proteja su infraestructura ante las amenazas de correo electrónico avanzadas y las infracciones de cumplimiento con soluciones potentes y fáciles de usar

Si bien es cierto que el correo electrónico es una herramienta de comunicación imprescindible en las empresas, también es el principal vector de amenazas como el *ransomware*, el *phishing*, los ataques *Business Email Compromise* (BEC), el *spoofing*, el *spam* y los virus. Además, hoy en día la legislación hace responsable a las empresas de la protección de la información confidencial, de prevenir su filtración y de que los mensajes de correo electrónico que contengan datos sensibles de clientes o información confidencial se intercambien de forma segura. Tanto si su organización es una pyme en crecimiento, como una empresa grande distribuida o un proveedor de servicios gestionados (MSP), lo que usted necesita es una solución económica de seguridad y cifrado del correo electrónico que ofrezca suficiente escalabilidad para aumentar fácilmente la capacidad a través de unidades y dominios organizativos, y para delegar en ellos las tareas de gestión.

Los dispositivos y el software Email Security de SonicWall proporcionan protección multicapa ante las amenazas de correo electrónico entrantes y salientes y las infracciones de cumplimiento analizando todo el contenido, las URL y los archivos adjuntos del correo electrónico entrante y saliente en busca de datos sensibles y ofreciendo protección en tiempo real ante el *ransomware*, los ataques de *phishing* selectivos, el *spoofing*, los virus, las URL maliciosas, los zombis, la recolección de directorios (DHA), la denegación de servicio (DoS) y otros ataques. La solución utiliza múltiples técnicas patentadas de detección de amenazas de SonicWall y una exclusiva red mundial de identificación y supervisión de ataques.

El servicio Capture Advanced Threat Protection de SonicWall ofrece *sandboxing* multimotor líder en el sector, con tecnología de inspección profunda de memoria en tiempo real (RTDMI™) pendiente de patente, para aislar las amenazas desconocidas encontradas en las URL y los archivos adjuntos sospechosos, a fin de que pueda detener las amenazas avanzadas antes de que lleguen a las bandejas de entrada de sus usuarios. La solución Email Security con Capture ATP le brinda una defensa altamente eficaz y reactiva al *ransomware* y a los ataques de día cero.

La solución también incluye DKIM (correo identificado por claves de dominio), SPF (marco de directivas de remitente), Autenticación de mensajes, informes y conformidad basada en dominios (DMARC), un potente método de autenticación de correo electrónico que ayuda a identificar los mensajes que han sufrido un ataque de *spoofing*, reduciendo el *spam* y los ataques de *phishing* selectivos, como el *spear-phishing*, el *whaling*, la suplantación de CEO y los ataques *Business Email Compromise*. También informa de las fuentes y los remitentes de correo electrónico, para que pueda identificar y bloquear a los remitentes no autorizados que falsifiquen el correo electrónico con su dirección y proteger así su marca. Asimismo, evita la filtración de datos confidenciales y el incumplimiento de normativas gracias a funciones avanzadas de análisis y gestión del cumplimiento, que incluyen un servicio integrado de cifrado de correo electrónico en la nube para garantizar el intercambio seguro de datos sensibles.

La gestión de la solución Email Security es intuitiva, rápida y sencilla. Con Email Security, además, puede delegar la gestión del *spam* en los usuarios finales sin perder el control sobre la seguridad. Por otra parte, puede gestionar fácilmente las cuentas de usuarios y grupos gracias a las sencillas funciones de sincronización multi-LDAP. En entornos distribuidos de gran envergadura, el soporte multiusuario permite delegar la gestión de configuraciones en subadministradores de otras unidades (como divisiones empresariales o clientes MSP) dentro de una única implementación de Email Security.

Ventajas

- Evite que el *ransomware* y el *malware* de día cero lleguen a su bandeja de entrada con Capture Advanced Threat Protection
- Impida que los usuarios hagan clic en vínculos maliciosos a través de cualquier dispositivo y desde cualquier lugar con la protección frente a URL al hacer clic
- Técnicas de análisis avanzadas para detener los ataques selectivos de *phishing*, el fraude por correo electrónico y los ataques *Business Email Compromise* (BEC)
- Bloquee las nuevas amenazas con actualizaciones de información sobre amenazas en tiempo real de Capture Labs de SonicWall
- Mantenga la higiene del correo electrónico con potentes sistemas antispam y antivirus
- Proteja sus datos aplicando políticas de protección granular contra la pérdida de datos (DLP) y cumplimiento normativo
- Simplifique la gestión mediante la automatización inteligente, la delegación de tareas, un panel de control personalizable y de un solo vistazo e informes eficaces
- Aproveche las opciones de implementación flexibles y escalables, como los dispositivos físicos reforzados, los dispositivos virtuales robustos y el potente software Windows Server®

[1] Patentes estadounidenses 7.814.545; 7.343.624; 7.665.140; 7.653.698; 7.546.348

Prestaciones

Protección avanzada ante amenazas

Detecte y bloquee las amenazas avanzadas hasta que se emita un veredicto. Se trata del único producto de detección de amenazas avanzadas que combina el *sandboxing* multicapa, incluida la inspección profunda de memoria en tiempo real (RealTime Deep Memory Inspection), la emulación del sistema completo y técnicas de virtualización, a fin de analizar comportamientos de código sospechosos en los correos electrónicos para proteger a los clientes ante el creciente peligro de las amenazas de día cero. El servicio incluye protección avanzada de URL que analiza de forma dinámica las URL incrustadas con el objetivo de bloquear y poner en cuarentena los mensajes con URL malintencionadas antes de que lleguen a la bandeja de entrada, de modo que los usuarios no puedan hacer clic en ellas y poner su información en peligro. El servicio Capture ATP ofrece mayor granularidad con análisis de archivos adjuntos y URL, funciones adicionales de generación de informes en profundidad y una experiencia de usuario optimizada.

Por otro lado, Email Security de SonicWall reescribe todas las URL incrustadas para bloquear los mensajes de correo electrónico con URL maliciosas o de *phishing*, de modo que los usuarios estén protegidos al hacer clic desde cualquier dispositivo y ubicación.

Algunas organizaciones y organismos gubernamentales no pueden utilizar técnicas basadas en la nube para la inspección de archivos, como Capture ATP, por motivos de cumplimiento o latencia. Integre su dispositivo Email Security con el dispositivo Capture Security de SonicWall (CSa) para examinar los archivos sospechosos que llegan a través del correo electrónico dentro de su propio centro de datos. Se puede hacer referencia al CSa por dirección IP o FQDN, lo que lo convierte en un excelente recurso para la prevención de amenazas.

Protección contra ataques selectivos

La tecnología *antiphishing* de SonicWall emplea una combinación de métodos como el aprendizaje automático, la heurística y el análisis de la reputación y del contenido para detener los ataques sofisticados de *phishing*. La solución también incluye potentes estándares de autenticación de correo electrónico, como SPF, DKIM y DMARC, para detener los ataques de *spoofing* y *Business Email Compromise*, así como el fraude de correo electrónico.

Información sobre amenazas en tiempo real

Obtenga la protección más precisa y actual frente a nuevos ataques de *spam*, al tiempo que garantiza la entrega de los correos electrónicos inofensivos, gracias a la información sobre amenazas en tiempo real de la red Capture Threat Network de SonicWall, que recopila información de millones de fuentes de datos. Capture Labs de SonicWall analiza esa información y lleva a cabo rigurosas pruebas para puntuar la reputación de los remitentes y del contenido, identificando las nuevas amenazas en tiempo real.

Protección antivirus y antispyware

Obtenga la última protección antivirus y *antispyware*. La solución utiliza firmas de bases de datos de antivirus líderes del sector y funciones de detección de URL malintencionadas para ofrecer una protección multicapa superior a la que ofrecen las soluciones que confían en una única tecnología antivirus.

Además, el análisis predictivo le permite proteger su red desde el momento en que surge un nuevo virus hasta el momento en que esté disponible una actualización de las firmas antivirus.

Automatización inteligente, delegación de tareas e informes eficaces

Simplifique la gestión mediante la automatización inteligente, la delegación de tareas y unos informes eficaces. Gestione las direcciones de correo electrónico, las cuentas y los grupos de usuarios de manera automática. Integre su solución con múltiples servidores LDAP de forma sencilla. Delegue con toda confianza la gestión del *spam* a los usuarios finales gracias al complemento descargable Junk Button for Outlook®, sin dejar de tener el control total. Localice cualquier correo electrónico en cuestión de segundos con el motor de búsqueda rápida de mensajes. Los informes centralizados (incluso en el modo dividido) le proporcionan información granular fácilmente personalizable a nivel de sistema sobre los tipos de ataques, la eficacia de la solución y la supervisión integrada del rendimiento. Los informes están disponibles en formatos PDF y JPEG.

Gestión de políticas de cumplimiento

Este servicio adicional permite cumplir las normativas ayudándole a identificar, supervisar y generar informes sobre los correos electrónicos que infrinjan las normativas y directrices de cumplimiento (p. ej., HIPAA, SOX, GLBA y PCI-DSS) o las directrices corporativas sobre la pérdida de datos. El servicio de suscripción también permite el enrutamiento basado en políticas del correo para su aprobación, archivado y cifrado.

Cifrado del correo electrónico

Añada un potente marco para detener las filtraciones de datos, gestionar y hacer cumplir los requisitos de cumplimiento y proporcionar un intercambio de correo electrónico seguro habilitado para dispositivos móviles en organizaciones de todos los tamaños.

Se puede llevar a cabo un seguimiento del correo electrónico cifrado para confirmar la hora de recepción y de apertura. Para hacer que el proceso resulte más intuitivo para el destinatario, se envía un correo electrónico de notificación a la bandeja de entrada del mismo con instrucciones para iniciar sesión en un portal seguro y leer o descargar el correo electrónico con todas las garantías. Se trata de un servicio basado en la nube y no requiere de ningún software cliente adicional y, a diferencia de las soluciones de la competencia, se puede acceder y leer el correo electrónico cifrado desde dispositivos móviles o portátiles.

Opciones de implementación flexibles

Obtenga un valor escalable a largo plazo configurando su solución para el crecimiento y la redundancia con unos costes iniciales mínimos. Puede implementar la solución Email Security de SonicWall como un dispositivo reforzado de alto rendimiento, como software que utiliza la infraestructura existente o como un dispositivo virtual que utiliza los recursos informáticos compartidos para optimizar el uso, facilitar la migración y reducir los costes de capital. Comience con un único sistema y, a medida que su empresa crezca, añada capacidad y pase a una arquitectura de modo dividido que permite la recuperación en caso de fallos. Gracias al soporte multiusuario, las grandes empresas o los proveedores de servicios gestionados con varios departamentos o clientes pueden establecer unidades organizativas con uno o varios dominios.

Aunque la implementación puede gestionarse de forma centralizada, una determinada unidad organizativa puede tener sus propios usuarios y subadministradores, sus propias normas y sus propias bandejas de *spam*, entre otras cosas.

Opciones de implementación de Email Security de SonicWall

Gracias a la gran flexibilidad de su arquitectura, la solución Email Security de SonicWall puede implementarse en organizaciones que requieren una solución de protección del correo electrónico altamente escalable, redundante y distribuida que se pueda gestionar de manera centralizada. Email Security de SonicWall puede implementarse como una solución integrada o en modo dividido.

En el modo dividido, los sistemas pueden configurarse como un dispositivo de análisis remoto o como un centro de control. En una configuración típica de modo dividido, uno o varios dispositivos de análisis remotos están conectados a un centro de control. El dispositivo de análisis remoto recibe correos electrónicos desde uno o más dominios y aplica funciones de gestión de las conexiones, filtrado del correo electrónico (*antispam*, *antiphishing* y antivirus) y técnicas de políticas avanzadas para enviar el correo electrónico inofensivo al servidor de correo electrónico posterior. El centro de control gestiona de manera centralizada todos los dispositivos de análisis remotos y recoge y almacena el correo electrónico no deseado de dichos dispositivos. La gestión centralizada abarca la elaboración de informes y la supervisión de todos los sistemas relacionados. Este paradigma permite a la solución escalar y proteger de manera rentable el correo electrónico entrante y saliente para las organizaciones en crecimiento. Con los dispositivos virtuales de Email Security de SonicWall, el modo dividido se puede implementar completamente en uno o varios servidores para lograr la máxima eficiencia de escala.

Prestaciones

	DISPOSITIVO, DISPOSITIVO VIRTUAL	WINDOWS SERVER®
Suscripción Advanced Total Secure – Paquete de protección avanzada		
Incluye la protección avanzada de archivos adjuntos y URL Capture ATP de SonicWall, además de la suscripción a Total Secure	Sí	Sí
Protección de URL al hacer clic	Sí	Sí
Suscripción Total Secure – Paquete de protección básica		
Incluye suscripción a Email Protection con soporte dinámico 24x7, además de antivirus multicapa, detección de URL malintencionadas y funciones de suscripción de gestión de cumplimiento	Sí	Sí
Protección contra *ransomware* y ataques de día cero – opcional		
Complemento de protección avanzada de URL y archivos adjuntos de Capture ATP de SonicWall para la suscripción Total Secure	Sí	Sí
Protección completa del correo electrónico entrante y saliente		
Antispam	Sí	Sí
Gestión de conexiones con reputación IP avanzada	Sí	Sí
Detección, clasificación y bloqueo de mensajes de *phishing*	Sí	Sí
Protección contra ataques por recolección de directorios, denegación de servicio y ataques NDR	Sí	Sí
Antispoofing con soporte para SPF, DKIM y DMARC	Sí	Sí
Políticas para usuarios individuales, para grupos o para todos los usuarios	Sí	Sí
Agente de transferencia de mensajes (MTA) en memoria para un mayor rendimiento	Sí	Sí
Fácil administración		
Instalación	< 1 hora	< 1 hora
Gestión semanal	< 10 min	< 10 min
Sincronización multi-LDAP automática para usuarios y grupos	Sí	Sí
Compatible con todos los servidores de correo electrónico SMTP	Sí	Sí
Compatibilidad con la autenticación SMTP (SMTP AUTH)	Sí	Sí
Permitir/bloquear los controles de los usuarios finales	Sí	Sí
Personalización, planificación y envío por correo electrónico de más de 30 informes	Sí	Sí
Detalles de la valoración	Sí	Sí
Panel de gestión personalizable y de un vistazo	Sí	Sí
Motor de búsqueda rápida de mensajes	Sí	Sí
Arquitectura escalable en modo dividido	Sí	Sí
Agrupación y agrupación remota	Sí	Sí
Fácil para los usuarios finales		
Inicio de sesión único	Sí	Sí
Bandejas de spam por usuario, correo electrónico configurable de resumen de bandeja de spam	Sí	Sí
Agresividad del *antispam* por usuario, listas de admitidos/bloqueados	Sí	Sí
Suscripción a Email Protection con soporte dinámico – necesario		
Actualizaciones automáticas cada minuto de las tecnologías antivirus, *antispam* y *antiphishing* en la nube de SonicWall	Sí	Sí
Soporte 24x7	Sí	Sí
RMA (sustitución de dispositivos)	Sí	Sí
Actualizaciones de software/firmware	Sí	Sí
Suscripción antivirus – opcional		
Firmas antivirus de bases de datos líderes en el sector	Sí	Sí
Antivirus TimeZero de SonicWall	Sí	Sí
Detección de zombis	Sí	Sí
Suscripción para el cumplimiento normativo – opcional		
Gestión eficaz de políticas	Sí	Sí
Análisis de adjuntos	Sí	Sí
Coincidencia de ID de registro	Sí	Sí
Diccionarios	Sí	Sí
Bandejas/flujo de trabajo de aprobación	Sí	Sí
Archivado de correos electrónicos	Sí	Sí
Elaboración de informes de cumplimiento	Sí	Sí
Suscripción a servicios de cifrado – opcional		
Suscripción al servicio de cumplimiento con cifrado de correo electrónico basado en políticas e intercambio seguro de correo electrónico	Sí	Sí

Especificaciones del sistema

DISPOSITIVOS EMAIL SECURITY	5000	7000	9000
Dominios	Sin restricciones		
Sistema operativo	Dispositivo reforzado con sistema operativo SonicWall Linux		
Chasis de montaje en bastidor	1RU	1RU	1RU
CPU(s)	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Disco duro	500 GB	1 TB	1 TB
Array de discos redundantes (RAID)	—	RAID 1	RAID 5
Unidades intercambiables en caliente	No	Sí	Sí
Alimentación redundante	No	No	Sí
Modo SAFE Flash	Sí	Sí	Sí
Dimensiones	17,0 x 16,4 x 1,7 pulg. / 43,18 x 41,59 x 4,44 cm	17,0 x 16,4 x 1,7 pulg. / 43,18 x 41,59 x 4,44 cm	27,5 x 19,0 x 3,5 pulg. / 69,9 x 48,3 x 8,9 cm
Peso	7,26 kg/16 libras	7,26 kg/16 libras	22,7 kg/50,0 libras
Peso WEEE	7,37 kg/16 libras	22,2 kg/16 libras	22,2 kg/48,9 libras
Consumo eléctrico (vatios)	46	48	158
BTU	155	162	537
MTBF a 25 °C en horas	130.919	150.278	90.592
MTBF a 25 °C en años	14,9	17,2	10,3
SOFTWARE EMAIL SECURITY			
Dominios	Sin restricciones		
Sistema operativo	Microsoft Hyper-V Server 2012 (64 bits) o superior Windows Server 2008 R2 o superior solo x64 bit		
CPU	Procesador Intel o AMD de 64 bits		
RAM	Configuración mínima de 8 GB		
Disco duro	Configuración mínima de 160 GB		
DISPOSITIVO VIRTUAL EMAIL SECURITY			
Hipervisor	ESXi™ y ESX™ (versión 5.0 y posterior)		
Sistema operativo instalado	8 GB (ampliable)		
Memoria asignada	4 GB		
Tamaño de disco del dispositivo	160 GB (ampliable)		
Guía de compatibilidad de hardware de VMware	http://www.vmware.com/resources/compatibility/search.php		

Servicios habilitados por partners

¿Necesita ayuda para planificar, desplegar u optimizar su solución de SonicWall? Los *partners* de servicios avanzados de SonicWall están formados para prestarle servicios profesionales de primera clase. Obtenga más información en www.sonicwall.com/PES.

Información para pedidos de Email Security de SonicWall

Dispositivos Email Security de SonicWall

Producto	SKU
Sonicwall Email Security Appliance 9000	01-SSC-7605
Sonicwall Email Security Appliance 7000	01-SSC-7604
Sonicwall Email Security Appliance 5000	01-SSC-7603
SonicWall Email Security Software	01-SSC-6636
SonicWall Email Security Virtual Appliance	01-SSC-7636

Suscripciones a Email Security de SonicWall

Suscripción	SKU
Suscripción a Email Protection de SonicWall	
Suscripción a Email Protection de SonicWall y soporte 24X7 para 25 usuarios – 1 servidor (1 año)	01-SSC-6669
Suscripción a Email Protection de SonicWall y soporte 24X7 para 1000 usuarios – 1 servidor (1 año)	01-SSC-6678
Suscripción a Email Protection de SonicWall y soporte 24X7 para 10 000 usuarios – 1 servidor (1 año)	01-SSC-6730
Suscripción a Email Anti-Virus de SonicWall	
Email Anti-Virus de SonicWall para 25 usuarios – 1 servidor (1 año)	01-SSC-6759
Email Anti-Virus de SonicWall para 1000 usuarios – 1 servidor (1 año)	01-SSC-6768
Email Anti-Virus de SonicWall para 10 000 usuarios – 1 servidor (1 año)	01-SSC-7562
Suscripción a Email Encryption de SonicWall	
Servicio Email Encryption de SonicWall para 25 usuarios (1 año)	01-SSC-7427
Servicio Email Encryption de SonicWall para 1000 usuarios (1 año)	01-SSC-7471
Servicio Email Encryption de SonicWall para 10 000 usuarios (1 año)	01-SSC-7568
Suscripción a Email Compliance de SonicWall	
Servicio Email Compliance de SonicWall para 25 usuarios – 1 servidor (1 año)	01-SSC-6639
Servicio Email Compliance de SonicWall para 1000 usuarios – 1 servidor (1 año)	01-SSC-6648
Servicio Email Compliance de SonicWall para 10 000 usuarios – 1 servidor (1 año)	01-SSC-6735
Suscripción a TotalSecure Email de SonicWall	
Suscripción a TotalSecure Email de SonicWall para 25 usuarios (1 año)	01-SSC-7399
Suscripción a TotalSecure Email de SonicWall para 1000 usuarios (1 año)	01-SSC-7398
Suscripción a TotalSecure Email de SonicWall para 10 000 usuarios (1 año)	01-SSC-7405
Complemento Capture ATP para la suscripción a TotalSecure Email	
Capture ATP para la suscripción TotalSecure Email de SonicWall para 25 usuarios (1 año)	01-SSC-1526
Capture ATP para la suscripción TotalSecure Email de SonicWall para 1000 usuarios (1 año)	01-SSC-1874
Capture ATP para la suscripción TotalSecure Email de SonicWall para 10 000 usuarios (1 año)	01-SSC-1883
Suscripción a Advanced TotalSecure Email de SonicWall (incluye Capture ATP)	
Suscripción a Advanced TotalSecure Email de SonicWall para 25 usuarios (1 año)	01-SSC-1886
Suscripción a Advanced TotalSecure Email de SonicWall para 1000 usuarios (1 año)	01-SSC-1904
Suscripción a Advanced TotalSecure Email de SonicWall para 10 000 usuarios (1 año)	01-SSC-1913

Los paquetes de los dispositivos y las suscripciones Email Security de SonicWall están disponibles en paquetes de 25, 50, 100, 250, 500, 1000, 2000, 5000 y 10 000 usuarios con opciones de 1, 2 y 3 años. El soporte también está disponible como opción 8X5. Consulte con su distribuidor local de SonicWall para obtener una lista completa de los SKU.

Acerca de SonicWall

SonicWall lleva más de 27 años combatiendo el crimen cibernético y defendiendo a pequeñas y medianas empresas, así como a compañías y agencias gubernamentales de todo el mundo. Con el respaldo de SonicWall Capture Labs, nuestras galardonadas soluciones de detección y prevención de violaciones de seguridad en tiempo real protegen más de un millón de redes, sus correos electrónicos, aplicaciones y datos, en más de 215 países y territorios. Estas organizaciones funcionan con mayor eficacia y menos temor a la seguridad. Si desea más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
(Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150