Log in

Hoja de datos de protección avanzada de correo electrónico de Cisco Secure Email

Actualizado: 13 de junio de 2021

Lenguaje libre de sesgos

La diferencia del correo electrónico seguro de Cisco

Los clientes de todos los tamaños se enfrentan al mismo desafío abrumador: el correo electrónico es, al mismo tiempo, la herramienta de comunicación comercial más importante y el principal vector de ataque para las infracciones de seguridad. Cisco® Email Security

permite a los usuarios comunicarse de forma segura y ayuda a las organizaciones a combatir el Business Email Compromise (BEC), el ransomware, el malware avanzado, el phishing, el spam y la pérdida de datos con un enfoque de seguridad de varias capas.

Descripción del producto

Cisco Secure Email incluye capacidades avanzadas de protección contra amenazas para detectar, bloquear y remediar amenazas más rápido, evitar la pérdida de datos y proteger la información importante en tránsito con cifrado de extremo a extremo.

Con el correo electrónico seguro de Cisco, los clientes pueden:

- Detecte y bloquee más amenazas con la inteligencia de amenazas superior de Talos , nuestro equipo de investigación de amenazas.
- Combata el ransomware oculto en archivos adjuntos que evaden la detección inicial con Cisco Secure Email Malware Defense y Cisco Threat Grid.
- Descarte correos electrónicos con enlaces peligrosos automáticamente o bloquee el acceso a sitios recién infectados con análisis de URL en tiempo real para protegerse contra el phishing y BEC.
- Prevenga el abuso de marca y los sofisticados ataques de correo electrónico basados en la identidad con los servicios Cisco Secure Email Domain Protection y Cisco Secure Email Phishing Defense.
- Proteja el contenido confidencial de los correos electrónicos salientes con Data Loss Prevention (DLP) y el cifrado de correo electrónico fácil de usar, todo en una sola solución.
- Proporcione capacitación sobre el comportamiento de los usuarios con Cisco Secure Awareness Training para ayudar a los usuarios a trabajar de manera más inteligente y segura.
- Maximice la flexibilidad de la implementación con una implementación en la nube, virtual, local o híbrida, o muévase a la nube en fases.
- Integre una cantidad cada vez mayor de productos de seguridad de Cisco y acelere funciones clave de operaciones de seguridad como visibilidad, detección, automatización, investigación y reparación con SecureX.

Características y Beneficios

Las amenazas de seguridad de correo electrónico actuales consisten en ransomware, malware avanzado, BEC, phishing y spam. La tecnología Cisco Secure Email bloquea las amenazas para que las empresas reciban solo mensajes legítimos. Cisco utiliza múltiples capas para brindar lo

máximo en seguridad de correo electrónico integral, incorporando medidas preventivas y reactivas para fortalecer su defensa. La Tabla 1 resume las principales capacidades de nuestras soluciones de seguridad de correo electrónico.

Tabla 1. Capacidades principales

Rasgo	Beneficio
Inteligencia de amenazas globales	Obtenga una protección de correo electrónico rápida y completa respaldada por Talos, una de las redes de detección de amenazas más grandes del mundo. Talos proporciona una amplia visibilidad y una gran huella, que incluye: ● 600 mil millones de correos electrónicos por día ● 16 mil millones de solicitudes web por día ● 1,5 millones de muestras de malware Talos proporciona una vista de 24 horas de la actividad de tráfico global. Analiza anomalías, descubre nuevas amenazas y monitorea las tendencias del tráfico. Talos ayuda a prevenir los ataques de hora cero mediante la generación continua de reglas que alimentan las actualizaciones de las soluciones de seguridad de correo electrónico de los clientes. Estas actualizaciones ocurren cada tres a cinco minutos, brindando una defensa contra amenazas líder en la industria.
Filtrado de reputación	Bloquee el correo electrónico no deseado con el filtrado de reputación, que se basa en la inteligencia de amenazas de Talos. Para cada hipervínculo incrustado, se realiza una verificación de reputación para verificar la integridad de la fuente. Los sitios web con mala reputación conocida se bloquean automáticamente. El filtrado de reputación detiene el 90 % del spam incluso antes de que ingrese a su red, lo que permite escalar la solución mediante el análisis de una carga mucho más pequeña.
Protección contra el spam	El spam es un problema complejo que exige una solución sofisticada. Cisco lo hace fácil. Cisco Secure Email bloquea los correos electrónicos no deseados mediante una arquitectura de escaneo de varias capas

Rasgo	Beneficio
	que ofrece la tasa más alta de detección de spam de más del 99 por ciento, con una tasa de falsos positivos de menos de uno en un millón. La funcionalidad antispam de Cisco Secure Email utiliza el motor de análisis adaptable al contexto de Cisco (CASE). Este motor examina el contexto completo de un mensaje, incluido el contenido del mensaje, cómo se construye el mensaje, quién envía el mensaje y a dónde lo lleva la llamada a la acción del mensaje. Al combinar estos elementos, Cisco Secure Email detiene la gama más amplia de amenazas con una precisión líder en la industria.
Detección de correo electrónico falsificado	La detección de correo electrónico falsificado protege contra los ataques BEC centrados en los ejecutivos, que se consideran objetivos de alto valor. La detección de correo electrónico falsificado lo ayuda a bloquear estos ataques personalizados y proporciona registros detallados de todos los intentos y acciones realizadas.
Defensa contra el phishing de correo electrónico seguro de Cisco	CAPP detiene los ataques basados en el engaño de identidad, como la ingeniería social, los impostores y BEC, al combinar la inteligencia de amenazas global de Cisco Talos con inteligencia de correo electrónico local y técnicas avanzadas de aprendizaje automático para modelar el comportamiento confiable del correo electrónico en Internet, dentro de las organizaciones y entre individuos. ● Integra técnicas de aprendizaje automático para impulsar actualizaciones diarias del modelo, manteniendo una comprensión en tiempo real del comportamiento del correo electrónico para detener el engaño de identidad. ● Combina informes y conformidad rápidos de autenticación de mensajes de dominio (DMARC), protección avanzada de nombres para mostrar y detección impulsada por impostores de dominios similares para detener los ataques BEC. ● Modela el comportamiento de amenazas de apropiación de cuentas para bloquear los ataques que se originan en cuentas de correo electrónico comprometidas. ● Se implementa como un sensor liviano a través de la nube o en las instalaciones en el entorno del cliente como una máquina virtual (VM) alojada de su elección o instalaciones completas. Consulte la Tabla 7 para

Rasgo	Beneficio
	ver las especificaciones de hardware de la máquina virtual. Se proporciona un sensor basado en la nube como parte de la implementación de Cisco Cloud Email Security. ● Admite el modo de entrega dual. En este modo, el sensor acepta copias de mensajes de correo electrónico a través del Protocolo simple de transferencia de correo (SMTP) y extrae metadatos en forma de transmisión.
Protección de dominio de correo electrónico seguro de Cisco	CDP para correo electrónico externo ayuda a evitar que se envíen correos electrónicos de phishing utilizando los dominios de un cliente. Automatiza el proceso de implementación del estándar de autenticación de correo electrónico DMARC para proteger mejor a los empleados, clientes y proveedores de los ataques de phishing utilizando los dominios de un cliente. Esto protege la identidad de marca de los clientes y aumenta la eficacia del marketing por correo electrónico al reducir los mensajes de phishing que llegan a las bandejas de entrada.
defensa contra virus	Al ofrecer una solución de detección de virus de alto rendimiento integrada en la puerta de enlace, Cisco Secure Email proporciona un enfoque de múltiples capas y múltiples proveedores para el filtrado de virus.
Detección de correo gris y cancelación segura de suscripción	Graymail consiste en marketing, redes sociales y mensajes masivos. La función de detección de correo gris clasifica y supervisa con precisión el correo gris que ingresa a una organización. Luego, un administrador puede tomar las medidas apropiadas en cada categoría. A menudo, graymail tiene un enlace para darse de baja donde los usuarios finales pueden indicar al remitente que les gustaría optar por no recibir dichos correos electrónicos. Dado que imitar un mecanismo de cancelación de suscripción es una técnica de phishing popular, los usuarios deben tener cuidado al hacer clic en estos enlaces para cancelar la suscripción. La solución segura para darse de baja proporciona: ● Protección contra amenazas maliciosas que se hacen pasar por enlaces para darse de baja. ● Una interfaz uniforme para administrar todas las suscripciones. Mejor visibilidad para los administradores de correo electrónico y los usuarios finales en dichos correos electrónicos.

Rasgo	Beneficio
Defensa contra malware y Cisco Threat Grid	Malware Defense y Threat Grid brindan puntaje y bloqueo de reputación de archivos, sandboxing de archivos y retrospección de archivos para el análisis continuo de amenazas. Los usuarios pueden bloquear más ataques, rastrear archivos sospechosos, mitigar el alcance de un brote y remediarlo rápidamente. Cisco Secure Email también se integra con Malware Defense for Endpoints. Malware Defense for Endpoints comparte inteligencia sobre amenazas en todo el entorno de un cliente, unificando la seguridad en los puntos finales, la red, el correo electrónico, la nube y la web. A través de estas integraciones, Malware Defense correlaciona automáticamente archivos, datos de telemetría, comportamiento y actividad para defenderse de forma proactiva contra amenazas avanzadas en todos los vectores posibles. La corrección automática de buzones para clientes de Microsoft 365 ayuda a reparar las infracciones más rápido y con menos esfuerzo. Los clientes simplemente configuran su solución de seguridad de correo electrónico para realizar acciones automáticas en esos correos electrónicos infectados. Los clientes pueden comprar una licencia adicional para implementar su sistema Malware Defense completamente en las instalaciones con la nube privada de Malware Defense. Esto, junto con Threat Grid, trae toda la oferta de Malware Defense completamente local.
SeguroX	Nuestro enfoque arquitectónico para los productos de seguridad integrados significa compartir inteligencia de amenazas de manera efectiva y más. La respuesta a amenazas SecureX proporciona una respuesta más rápida y sincronizada en toda la cartera.
Protección y control relacionados con URL	Los usuarios están protegidos contra URL maliciosas con filtrado de URL, escaneo de URL en archivos adjuntos y URL administradas (acortadas). Se aplican políticas apropiadas a los mensajes en función de la reputación o la categoría de las URL.

Rasgo	Beneficio
Filtros de brotes	Los filtros de brotes protegen contra las amenazas emergentes y los ataques combinados. Pueden emitir reglas sobre cualquier combinación de seis parámetros, incluido el tipo de archivo, el nombre del archivo, el tamaño del archivo y las direcciones URL en un mensaje. A medida que Talos aprende más sobre un brote, puede modificar las reglas y liberar los mensajes de la cuarentena en consecuencia. Los filtros de brotes también pueden reescribir las URL vinculadas en mensajes sospechosos. Cuando se hace clic, las nuevas URL redirigen al destinatario a través del proxy de Cisco Web Security. Luego, el contenido del sitio web se escanea activamente y los filtros de brotes mostrarán una pantalla de bloqueo al usuario si el sitio contiene malware.
Seguimiento de interacciones web	El seguimiento de la interacción web es una solución totalmente integrada que permite a los administradores de TI realizar un seguimiento de los usuarios finales que hacen clic en las URL que Cisco Secure Email ha reescrito. Los informes muestran: ● Principales usuarios que hicieron clic en direcciones URL maliciosas. ● Las principales URL maliciosas en las que los usuarios finales hicieron clic. Fecha y hora, motivo de reescritura y acción realizada en las URL.
Seguridad de datos para contenido confidencial en correos electrónicos salientes	Cisco Secure Email ofrece DPL efectivo y encriptación de correo electrónico. La gestión y los informes centralizados simplifican la protección de datos. **DLP** Proteja los mensajes salientes con Cisco Secure Email DLP. Cumpla con las regulaciones gubernamentales y de la industria en todo el mundo y evite que los datos confidenciales salgan de su red. Elija entre una amplia biblioteca de políticas de más de 100 políticas de expertos que cubren regulaciones gubernamentales, del sector privado y específicas de la empresa. Las políticas de DLP predefinidas se incluyen con el correo electrónico seguro de

Rasgo	Beneficio
	Cisco y simplifican la aplicación de la política de correo electrónico saliente con reconocimiento de contenido. Las opciones de remediación incluyen el cifrado, la adición de pies de página y descargos de responsabilidad, la adición de copias ocultas (BCC), la notificación y la cuarentena. Para las empresas que necesitan una política personalizada compleja, los componentes básicos de las políticas predefinidas están disponibles para que el proceso sea rápido y fácil.
	Cifrado Otorgue a los remitentes el control de su contenido, incluso después de que se hayan enviado los mensajes. Con el cifrado de correo electrónico, los remitentes no temen las direcciones de destinatario mal escritas, los errores en el contenido o los correos electrónicos urgentes porque siempre pueden bloquear un mensaje. El remitente de un mensaje cifrado recibe una confirmación de lectura una vez que el destinatario abre el mensaje, y las respuestas y los reenvíos de alta seguridad se cifran automáticamente para mantener la privacidad y el control de extremo a extremo. No hay infraestructura adicional para implementar. Para mayor seguridad, el contenido del mensaje va directamente desde su puerta de enlace al destinatario, y solo la clave de cifrado se almacena en la nube. Cumpla con los requisitos de encriptación para regulaciones como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), la Ley de portabilidad y responsabilidad de seguros médicos (HIPAA), la Ley Gramm-Leach-Bliley (GLBA) o la Ley Sarbanes-Oxley (SOX) —así como las regulaciones estatales de privacidad y las directivas europeas— sin

Rasgo	Beneficio
	sobrecargar a los remitentes, destinatarios o administradores de correo electrónico. Ofrezca el cifrado no como un mandato, sino como un servicio que es fácil de usar y le da al remitente un control total.
Manejabilidad	**Compatibilidad con dispositivos universales** Asegúrese de que todos los usuarios puedan acceder a los mensajes cuando sea necesario, independientemente de si se encuentran en teléfonos inteligentes, tabletas, computadoras portátiles o de escritorio. La compatibilidad con dispositivos universales está diseñada para garantizar que cualquier destinatario pueda leer mensajes altamente seguros, sin importar qué dispositivo se use para abrir el mensaje. Las aplicaciones complementarias dedicadas ofrecen una experiencia de usuario mejorada para Microsoft Outlook y en los teléfonos inteligentes y tabletas Apple iOS y Google Android. **Tablero de información general del sistema** Supervise e informe sobre los mensajes salientes desde un panel de información general centralizado y personalizado del sistema. Los informes comerciales unificados ofrecen una vista única para una visión integral de toda su organización. Obtenga los detalles de cualquier informe para una visibilidad avanzada. **Seguimiento detallado de mensajes** Realice un seguimiento de un mensaje por destinatario del sobre, remitente del sobre, asunto, archivos adjuntos y eventos del mensaje, incluida la política de DLP o los ID. Cuando envía un mensaje a Cisco Secure Email, la base de datos de seguimiento de mensajes se completa en uno o dos minutos, y

Rasgo	Beneficio
	puede ver qué sucedió con los mensajes que cruzan el sistema en cada paso del procesamiento.
Capacitación de concientización segura	Brinda flexibilidad y soporte para implementar de manera efectiva simulaciones de phishing y capacitación de concientización, así como para medir e informar los resultados. Se enfoca en la capacitación del comportamiento del usuario para realizar cambios a largo plazo y capacita al equipo de operaciones de seguridad con la capacidad de abordar amenazas en tiempo real. **Contenido de alta calidad** que incluye un creador de cursos con más de 150 módulos de aprendizaje para elegir, aprendizaje basado en roles y contenido altamente interactivo con ludificación para mantener a los usuarios interesados. **Simulador de phishing intuitivo** que proporciona escenarios de phishing listos para usar que reflejan amenazas cibernéticas y de phishing de la vida real, que se integran con capacitación para recibir comentarios justo a tiempo. **Plataforma y contenido multilingüe** con soporte para más de 40 idiomas (narración y texto) para que los programas de concientización sobre seguridad estén disponibles a nivel mundial. **Materiales de comunicación y refuerzo** proporcionados por grandes bibliotecas de contenido y plantillas prediseñadas para la promoción de campañas internas y refuerzo de contenido (incluidos videos, carteles y boletines). Enfoque consultivo con ofertas únicas, que incluyen capacitación de CISO, servicios administrados y personalización de contenido, para ayudar a las

Rasgo	Beneficio
	organizaciones a desarrollar y optimizar una estrategia de concienciación sobre seguridad.

Licencias de software de correo electrónico seguro de Cisco

Hay tres paquetes de software de seguridad de correo electrónico: Cisco Secure Email Inbound Essentials, Cisco Secure Email Outbound Essentials y Cisco Secure Email Premium; También hay disponibles opciones adicionales independientes (consulte la Tabla 2). Simplemente compre las licencias apropiadas para la cantidad de buzones que necesita admitir. Para dispositivos en la nube y virtuales, simplemente solicite las licencias de software para obtener derechos.

Licencias de suscripción basadas en plazos

Las licencias son suscripciones basadas en plazos de 1, 3 o 5 años.

Licencias de suscripción basadas en la cantidad

La cartera de correo electrónico seguro de Cisco utiliza precios escalonados según la cantidad de buzones. Los representantes de ventas y socios lo ayudarán a determinar la implementación correcta del cliente.

Los principales componentes de cada oferta de software se proporcionan en la Tabla 2.

Tabla 2. Componentes de software

manojos	Descripción
Aspectos esenciales de la entrada segura	El paquete Cisco Secure Email Inbound Essentials brinda protección contra amenazas basadas en correo electrónico e incluye antispam, detección de correo gris, solución antivirus de Sophos, filtros de brotes y

manojos	Descripción
de correo electrónico de Cisco	detección de correo electrónico falsificado.
Microsoft 365 Cisco Secure Email Inbound Essentials	El paquete Cisco Secure Email Inbound Essentials brinda protección contra amenazas basadas en correo electrónico e incluye antispam, detección de correo gris, filtros de brotes y detección de correo electrónico falsificado.
Cisco Secure Email Inbound Essentials más Malware Defense y Cisco Threat Grid	El paquete Cisco Secure Email Inbound Essentials brinda protección contra amenazas basadas en correo electrónico e incluye antispam, detección de correo gris, solución antivirus de Sophos, filtros de brotes y detección de correo electrónico falsificado. Malware Defense se puede comprar junto con cualquier paquete de software Cisco Secure Email. Threat Grid and Malware Defense aumenta las capacidades de detección y bloqueo de malware que ya se ofrecen en Cisco Secure Email con puntaje y bloqueo de reputación de archivos, sandboxing y retrospección de archivos para el análisis continuo de amenazas, incluso después de que hayan atravesado la puerta de enlace de correo electrónico. Malware Defense y Threat Grid ahora se pueden implementar completamente en las instalaciones con Malware Defense Private Cloud Virtual Appliance. Esto es importante para los clientes que tienen requisitos de políticas estrictos que no permiten el uso de la nube pública de Malware Defense.
Aspectos esenciales de la salida segura de correo electrónico de Cisco	El paquete Cisco Secure Email Outbound Essentials protege contra la pérdida de datos con el cumplimiento de DLP y el cifrado de correo electrónico.
Correo electrónico	El paquete Cisco Secure Email Premium combina las protecciones entrantes y salientes incluidas en las

manojos	Descripción
seguro de Cisco Premium	licencias Cisco Secure Email Inbound y Outbound Essentials mencionadas anteriormente para la protección contra amenazas basadas en correo electrónico y DLP y cifrado esenciales.
Correo electrónico seguro de Microsoft 365 Cisco Premium	El paquete Cisco Secure Email Premium combina las protecciones entrantes y salientes incluidas en las licencias de Office 365 Cisco Secure Email Inbound y Cisco Secure Email Outbound Essentials mencionadas anteriormente para la protección contra amenazas basadas en correo electrónico y DLP y cifrado esenciales.
Cisco Secure Email Premium más Malware Defense y Cisco Threat Grid	El paquete Cisco Secure Email Premium combina las protecciones entrantes y salientes incluidas en las licencias Cisco Secure Email Inbound y Outbound Essentials mencionadas anteriormente para la protección contra amenazas basadas en correo electrónico y DLP y cifrado esenciales. Malware Defense se puede comprar junto con cualquier paquete de software Cisco Secure Email. Threat Grid y Malware Defense aumentan las capacidades de detección y bloqueo de malware que ya se ofrecen en Cisco Secure Email con puntaje y bloqueo de reputación de archivos, sandboxing y retrospección de archivos para el análisis continuo de amenazas, incluso después de que hayan atravesado la puerta de enlace de correo electrónico. Malware Defense y Threat Grid ahora se pueden implementar completamente en las instalaciones con Malware Defense Private Cloud Virtual Appliance. Esto es importante para los clientes que tienen requisitos de políticas estrictos que no permiten el uso de la nube pública de Malware Defense.
Defensa contra malware y Cisco Threat Grid	Malware Defense se puede comprar junto con cualquier paquete de software Cisco Secure Email. Threat Grid and Malware Defense aumenta las capacidades de detección y bloqueo de malware que ya se ofrecen en Cisco Secure Email con puntaje y bloqueo de reputación de archivos, sandboxing y retrospección de archivos para el análisis continuo de amenazas, incluso después de que hayan

manojos	Descripción
	atravesado la puerta de enlace de correo electrónico. Malware Defense y Threat Grid ahora se pueden implementar completamente en las instalaciones con Malware Defense Private Cloud Virtual Appliance. Esto es importante para los clientes que tienen requisitos de políticas estrictos que no permiten el uso de la nube pública de Malware Defense.
Escaneo múltiple inteligente	Intelligent Multi-Scan (IMS) es una solución antispam multicapa de alto rendimiento que utiliza una combinación de motores antispam, incluido Cisco Anti-Spam, para aumentar las tasas de captura de spam. No puede configurar el orden de los motores de exploración utilizados en Cisco Intelligent Multi-Scan; Cisco Anti-Spam siempre será el último en escanear un mensaje y Cisco Intelligent Multi-Scan no lo omitirá si un motor de terceros determina que un mensaje es spam. El uso de Cisco Intelligent Multi-Scan puede reducir el rendimiento del sistema. Comuníquese con su representante de soporte de Cisco para obtener más información. Para usar el motor IMS actualizado, debe agregar la clave de función IMS y aceptar la licencia en su dispositivo. Para los usuarios de IMS existentes, todas las políticas de correo para IMS se migran para funcionar sin problemas con el motor de IMS actualizado.
Cancelación de suscripción segura de Graymail	Graymail ahora se puede etiquetar con una opción de cancelación de suscripción verdaderamente segura. Esta etiqueta administra una acción de cancelación de suscripción altamente segura en nombre del usuario final. También monitorea las diferentes solicitudes de cancelación de suscripción de correo gris. Todo esto se puede administrar a nivel de grupo de protocolo ligero de acceso a directorios (LDAP).
Defensa contra el phishing de correo electrónico seguro de Cisco	CAPP se puede comprar junto con cualquier paquete de software Cisco Secure Email. CAPP detiene los ataques basados en el engaño de identidad, como la ingeniería social, los impostores y BEC. Proporciona inteligencia de correo electrónico local y técnicas avanzadas de aprendizaje automático para modelar el comportamiento confiable del correo electrónico en Internet, dentro de las organizaciones y entre

manojos	Descripción
	individuos. CAPP también integra técnicas de aprendizaje automático para impulsar actualizaciones diarias de modelos, manteniendo una comprensión en tiempo real del comportamiento del correo electrónico para detener el engaño de identidad. Se ofrece solo para suscripciones de uno y tres años.
Protección de dominio de correo electrónico seguro de Cisco	CDP se puede comprar junto con cualquier paquete de software Cisco Secure Email. CDP para correo electrónico externo ayuda a evitar que se envíen correos electrónicos de phishing utilizando los dominios de un cliente. El servicio CDP automatiza el proceso de implementación del estándar de autenticación de correo electrónico DMARC para proteger mejor a los empleados, clientes y proveedores de los ataques de phishing utilizando los dominios de un cliente. Esto protege la identidad de marca de los clientes y aumenta la eficacia del marketing por correo electrónico al reducir los mensajes de phishing que llegan a las bandejas de entrada. Se ofrece solo para suscripciones de uno y tres años.
Analizador de imagen	Detecta contenido ilícito en el correo electrónico entrante y saliente, lo que permite a los clientes identificar, monitorear y educar a los usuarios infractores.
Antivirus de McAfee	Ofrece la tecnología de análisis antivirus de McAfee.
Capacitación de concientización segura de Cisco	Cisco Secure Awareness Training se puede comprar junto con cualquier paquete de software Cisco Secure Email. Está diseñado para ayudar a promover y aplicar el sentido común de ciberseguridad efectivo al modificar el comportamiento del usuario final y capacitar a los empleados para que trabajen de manera más inteligente y segura. Esta suscripción entregada en la nube proporciona simulación, capacitación e informes integrales para que el progreso de los empleados pueda monitorearse y rastrearse continuamente. Ayuda a las organizaciones a mantenerse seguras con contenido atractivo y relevante basado en computadora con varios métodos de ataque simulados y permite que las personas de su organización desempeñen un papel fundamental en su seguridad general con Cisco Secure Awareness Training.

manojos	Descripción

Acuerdos de licencia de software

El Acuerdo de licencia de usuario final de Cisco se proporciona con cada compra de licencia de software.

Soporte de suscripción de software

Todas las licencias de seguridad de correo electrónico incluyen soporte de suscripción de software que es esencial para mantener las aplicaciones críticas para el negocio disponibles, altamente seguras y operando al máximo rendimiento. Este soporte le da derecho a los servicios enumerados a continuación durante el plazo completo de la suscripción de software adquirida.

- Las actualizaciones de software y las mejoras importantes hacen que las aplicaciones funcionen al máximo, con las funciones más actualizadas.
  - El Centro de asistencia técnica de Cisco brinda soporte rápido y especializado.
  - Las herramientas en línea crean y amplían la experiencia interna y aumentan la agilidad comercial.
  - El aprendizaje colaborativo brinda conocimientos adicionales y oportunidades de capacitación.

Dónde implementar

Todas las opciones de implementación de Cisco Secure Email comparten un enfoque simple para la implementación. El asistente de configuración del sistema puede manejar incluso entornos complejos y lo tendrá listo y protegido en solo minutos, haciéndolo más seguro más rápido. Las licencias se basan en usuarios únicos, no en dispositivos, por lo que puede aplicarlas por usuario único en lugar de por dispositivo para proporcionar protección de puerta de enlace de correo electrónico entrante y saliente sin costo adicional.

Nube

Cisco Secure Email en la nube le proporciona un modelo de implementación flexible para la seguridad del correo electrónico. Le ayuda a reducir costos con administración conjunta y sin infraestructura de seguridad de correo electrónico en el sitio. Las implementaciones de seguridad de correo electrónico dedicadas en múltiples centros de datos resistentes de Cisco brindan los niveles más altos de disponibilidad

del servicio y protección de datos. Los clientes conservan el acceso a (y la visibilidad de) la infraestructura de la nube, y los informes integrales y el seguimiento de mensajes ayudan a garantizar la flexibilidad administrativa. Este servicio es todo incluido, con software, potencia de cómputo y soporte integrado para simplificar.

Virtual

El dispositivo virtual de correo electrónico seguro de Cisco reduce significativamente el costo de implementar la seguridad del correo electrónico, especialmente en redes altamente distribuidas. Este dispositivo le permite a su administrador de red crear instancias donde y cuando se necesiten, usando su infraestructura de red existente. Una versión de software del dispositivo físico se ejecuta sobre un hipervisor VMware ESXi y servidores Cisco Unified Computing System™ (Cisco UCS®). Recibe una licencia ilimitada para el dispositivo virtual con la compra de cualquier paquete de software Cisco Secure Email.

Con el dispositivo virtual, puede responder instantáneamente al aumento del crecimiento del tráfico con una planificación de capacidad simplificada. No necesita comprar y enviar dispositivos, por lo que puede respaldar nuevas oportunidades comerciales sin agregar complejidad a un centro de datos o tener que contratar personal adicional.

En las instalaciones

El dispositivo de correo electrónico seguro de Cisco es una puerta de enlace que normalmente se implementa en un extremo de la red fuera del firewall (la llamada zona desmilitarizada). El tráfico SMTP entrante se dirige a la interfaz de datos del dispositivo según las especificaciones establecidas por sus registros de intercambio de correo. El dispositivo lo filtra y lo vuelve a enviar a su servidor de correo de red. Su servidor de correo también dirige el correo saliente a la interfaz de datos, donde se filtra de acuerdo con las políticas salientes y luego se envía a destinos externos.

Híbrido

La solución híbrida le proporciona la máxima flexibilidad. Puede combinar cualquier opción de implementación para que se adapte mejor a sus necesidades. Por ejemplo, puede aprovechar el correo electrónico seguro de Cisco en la nube para protegerse contra las amenazas en los mensajes entrantes mientras implementa el control de salida de los mensajes confidenciales en el sitio. También puede optar por implementar la protección contra amenazas entrantes en las instalaciones y en la nube para realizar la transición a la nube a su propio ritmo.

También puede ejecutar Cisco Secure Email local y virtual en la misma implementación. Por lo tanto, sus sucursales pequeñas o ubicaciones remotas pueden tener la misma protección que obtiene en la sede central sin la necesidad de instalar y brindar soporte al hardware en esas

ubicaciones. Puede administrar fácilmente implementaciones personalizadas con Cisco Secure Email and Web Manager o Cisco Secure Email and Web Manager Virtual.

Especificaciones del correo electrónico seguro de Cisco

La Tabla 3 presenta las especificaciones de rendimiento para Cisco Secure Email, mientras que la Tabla 4 presenta las especificaciones de hardware y la Tabla 5 presenta las especificaciones para una implementación virtual. La Tabla 6 presenta las especificaciones para la

plataforma M-Series de Secure Management Appliance. La Tabla 7 incluye información sobre los requisitos de hardware de la máquina virtual para la implementación del sensor local de Cisco Secure Email Phishing Defense.

Tabla 3. Especificaciones de rendimiento del correo electrónico seguro de Cisco

	Modelo	Espacio del disco	Duplicación de incursiones	Memoria	CPU
Gran empresa	ESA C695	4,8 TB (600x8)	Sí (RAID 10)	DDR4 de 32GB	1 x 2,6 GHz, 12 núcleos
Gran empresa	ESA C690	2,4 TB (600x4)	Sí (RAID 10)	DDR4 de 32GB	2 x 2,4 GHz, 12 núcleos
Empresa mediana	ESA C395	1,2 TB (600x2)	Sí (RAID 1)	DDR4 de 16GB	1 x 2,1 GHz, 12 núcleos
Empresa mediana	ESA C390	1,2 TB (600x2)	Sí (RAID 1)	DDR4 de 16GB	1 x 2,4 GHz, 6 núcleos
Pequeñas y medianas empresas o sucursales	ESA C195	1,2 TB (600x2)	Sí (RAID 1)	DDR4 de 16GB	1 x 2,1 GHz, 8 núcleos
Pequeñas y medianas empresas o sucursales	ESA C190	1,2 TB (600x2)	Sí (RAID 1)	DDR4 de 8GB	1 x 1,9 GHz, 6 núcleos

Nota: Para conocer el tamaño exacto, verifique su elección consultando las tasas máximas de flujo de correo y el tamaño promedio de los

mensajes con un especialista en seguridad de contenido de Cisco.

Tabla 4. Especificaciones del hardware de correo electrónico seguro de Cisco

Modelo	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
Unidades de rack (RU)	1RU	2RU	1RU	1RU	1RU	1RU
Dimensiones incluyendo manijas (alto x ancho x profundidad)	1,7x16,89x 29,8 pulg. (4,32 x 43,0 x 75,6 cm)	3,4 pulg. x 19 pulg. x 29 pulg. (8,6 x 48,3 x 73,7 cm)	1,7x16,89x 29,8 pulg. (4,32 x 43,0 x 75,6 cm)	1,7x16,89x 29,8 pulg. (4,32 x 43,0 x 75,6 cm)	1,7x16,89x 29,8 pulg. (4,32 x 43,0 x 75,6 cm)	1,7x16,89x 29,8 pulg. (4,32 x 43,0 x 75,6 cm)
Opción de alimentación de CC	No	Sí (930W)	No	No	No	No
Ciclo de energía remoto	Sí	Sí	Sí	Sí	Sí	Sí
Opción de alimentación de CC	No	Sí (930W)	No	No	No	No

Modelo	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
Ciclo de energía remoto	Sí	Sí	Sí	Sí	Sí	Sí
Fuente de alimentación redundante	Sí	Sí	Sí	Sí	Sí, opción de accesorios	Sí, opción de accesorios
Disco duro intercambiable en caliente	Sí	Sí	Sí	Sí	Sí	Sí
El consumo de energía	2626 BTU/h	2216,5 BTU/h	2626 BTU/h	2626 BTU/h	2626 BTU/h	2626 BTU/h
Fuente de alimentación	770W	650W	770W	770W	770W	770W
interfaces ethernet	6 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45	6 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45	6 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45	6 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45	2 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45	2 puertos 1GBASE-T interfaz de red de cobre (NIC), RJ-45

Modelo	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
Velocidad (Mbps)	10/100/1000, negociación automática	10/100/1000, negociación automática	10/100/1000, negociación automática	10/100/1000, negociación automática	10/100/1000, negociación automática	10/100/1000, negociación automática
Opción de fibra	Sí, SKU separado, 1GBASE-SX de 2 puertos Fibra o 10GBASESR Fibra seleccionable bajo pedido (módulos incluidos): ESA-C695F	Sí, SKU separados, 1GBASE-SX de 2 puertos Fibra: ESA-C690-1G 2-puerto 10GBASESR Fibra: ESAC690-10G	No	No	No	No
Tamaño HD	Se instalan ocho unidades de disco duro de 600 GB (2,5” 12G SAS 10K RPM) en los compartimientos para unidades del panel frontal	Cuatro unidades de disco duro de 600 GB (2,5” 10K SAS 4Kn) se instalan en bahías de unidad del	Dos 600GB las unidades de disco duro (2,5” 12G SAS 10K RPM) se instalan en los compartimientos para unidades del panel frontal	Dos 600GB unidades de disco duro (2,5” 10K SAS 4Kn) se instalan en bahías de unidad del panel frontal	Dos 600GB las unidades de disco duro (2,5” 12G SAS 10K RPM) se instalan en los compartimientos para unidades del panel frontal	Dos 600GB unidades de disco duro (2,5” 10K SAS 4Kn) se instalan en bahías de unidad del panel frontal

Modelo	ESA C695	ESA C690	ESA C395	ESA C390	ESA C195	ESA C190
	que brindan acceso intercambiable en caliente para unidades SAS	panel frontal que proporcionan acceso intercambiable en caliente para unidades SAS	que brindan acceso intercambiable en caliente para las unidades SAS	que proporcionan acceso intercambiable en caliente para unidades SAS	que brindan acceso intercambiable en caliente para las unidades SAS	que proporcionan acceso intercambiable en caliente para unidades SAS
UPC	Un procesador de 2,6 GHz 12c 2666 MHz	Dos procesadores E5-2620 v3	Un procesador de 2,1 GHz 12c 2400 MHz	Un procesador E5-2620 v3	Un procesador de 2,1 GHz 8c 2400 MHz	Un procesador E5-2609 v3
RAM	Dos DIMM1 DDR4-2666 de 16 GB	Cuatro DIMM1 DDR4-2133 de 8 GB	Una DIMM1 DDR4-2666 de 16 GB	Dos DIMM1 DDR4-2133 de 8 GB	Una DIMM1 DDR4-2666 de 16 GB	Una DIMM1 DDR4-2133 de 8 GB

Tabla 5. Especificaciones del dispositivo virtual de Email Security

	Modelo	Disco	Memoria	Núcleos
Solo evaluaciones	ESAV C000v	200 GB (SAS de 10 000 rpm)	4 GB	1 (2,7 GHz)
Pequeña empresa	ESAV C100v	200 GB (SAS de 10 000 rpm)	6GB	2 (2,7 GHz)

	Modelo	Disco	Memoria	Núcleos
(hasta 1000 empleados)				
Mediana empresa (hasta 5000 empleados)	ESAV C300v	500 GB (SAS de 10 000 RPM)	8GB	4 (2,7 GHz)
Gran empresa o proveedor de servicios	ESAV C600v	500 GB (SAS de 10 000 RPM)	8GB	8 (2,7 GHz)
Servidores				
Cisco UCS Cisco UCS	VMware ESXi 6.0 y 6.5 Hipervisor			

Tabla 6. Especificaciones de la plataforma de la serie M del dispositivo de gestión segura

Modelo	SMA M695/690	SMA M395/390	SMA M195/190
Número de usuarios únicos	10,000 o más	Hasta 10.000	hasta 1000

Tabla 7. Requisitos de hardware de la máquina virtual para la implementación de sensores locales de Cisco Secure Email Phishing

Defense

Sistema operativo	UPC	Memoria	Disco	La red	Estibador
Linux moderno de 64 bits: ● Red Hat Enterprise Linux ● 7.4 o posterior ● CentOS 7.4 o posterior ● Ubuntu 16 o posterior	Intel o AMD x 86_64 8 núcleos	16 GB mínimo 32 GB Recomendado	Las siguientes asignaciones mínimas: ● /var/opt/agari/: 100 GB ● /opt/agari/: 20 GB ● /var/lib/docker: 20 GB	1 Gbit/seg recomendado	17.06 o posterior

Cómo evaluar el correo electrónico seguro de Cisco

- Para probar Cisco Secure Email en la nube, solicite una prueba gratuita de 45 días en https://www.cisco.com/go/emailsecurity .
- Para probar nuestro dispositivo virtual, vaya a https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html#anc6 y siga los pasos indicados.
- Para comprender los beneficios de los dispositivos Cisco Secure Email C-Series y X-Series, visite https://www.cisco.com/c/en/us/partners/sell-integrate-consult/promotions/try-buy- program.html para una prueba de 45 días.

Servicios de Cisco

- Servicios de asesoramiento: nuestros expertos alinean la gestión de riesgos, cumplimiento, seguridad y amenazas con sus objetivos empresariales.
- Servicios de implementación: con experiencia y mejores prácticas trabajando con miles de clientes en todas las industrias alrededor del mundo, lo ayudaremos a obtener y aumentar más rápidamente los beneficios de su inversión en soluciones de seguridad avanzadas, incluida la seguridad del correo electrónico.
- Servicios técnicos: Brindamos servicios técnicos proactivos y preventivos para hardware, software, soluciones de múltiples

proveedores y entornos de red. Nuestro equipo global mejora las operaciones de TI, lo que ayuda a garantizar que su TI funcione de manera simple, consistente y segura para que su negocio funcione sin problemas.

Servicios de soporte de Cisco Smart Net Total Care

Para obtener el máximo valor de su inversión en tecnología, puede comprar el servicio Cisco Smart Net Total Care® para usar con Cisco Secure Email. El servicio lo ayuda a resolver problemas de red rápidamente con acceso directo en cualquier momento a expertos de Cisco,

herramientas de soporte de autoayuda y reemplazo rápido de hardware. Para obtener más información, visite https://www.cisco.com/c/en/us/services/technical/smart-net-total-care.html . Información de garantía

Encuentre información sobre la garantía en Cisco.com en la página Garantías de productos.

Sostenibilidad medioambiental de Cisco

La información sobre las políticas e iniciativas de sostenibilidad ambiental de Cisco para nuestros productos, soluciones, operaciones y operaciones extendidas o cadena de suministro se proporciona en la sección "Sostenibilidad ambiental" del Informe de responsabilidad social corporativa (RSC) de Cisco .

Los enlaces de referencia a información sobre temas clave de sostenibilidad ambiental (mencionados en la sección "Sostenibilidad ambiental" del Informe de RSE) se proporcionan en la siguiente tabla:

Tema de sostenibilidad	Referencia
Información sobre leyes y reglamentos sobre el contenido del material del producto	Materiales
Información sobre leyes y reglamentos sobre desechos electrónicos, incluidos productos, baterías y empaques	Cumplimiento de RAEE

Cisco pone a disposición los datos del paquete únicamente con fines informativos. Es posible que no refleje los desarrollos legales más actuales, y Cisco no declara ni garantiza que sea completo, preciso o actualizado. Esta información esta sujeta a cambios sin previo aviso.

capital de cisco

Soluciones de pago flexibles para ayudarlo a lograr sus objetivos

Cisco Capital facilita la obtención de la tecnología adecuada para lograr sus objetivos, permitir la transformación empresarial y ayudarlo a mantenerse competitivo. Podemos ayudarlo a reducir el costo total de propiedad, conservar el capital y acelerar el crecimiento. En más de

100 países, nuestras soluciones de pago flexibles pueden ayudarlo a adquirir hardware, software, servicios y equipos complementarios de terceros en pagos fáciles y predecibles. Más información

Para más información

Puede encontrar más información sobre el correo electrónico seguro de Cisco en https://www.cisco.com/go/emailsecurity , donde puede solicitar una prueba gratuita de 45 días.

Quick Links

Acerca de Cisco

Contáctenos

Carreras

Conozca a nuestros socios

Resources and Legal

Retroalimentación

Ayuda

Términos y condiciones