CISCO SECURE EMAIL

Defensa integral contra las amenazas del vector de ataque #1

Los atacantes siguen recurriendo al correo electrónico como principal vector para la propagación de malware, ransomware, phishing, spam, dominio comprometido, apropiación de cuentas, suplantación de identidad, amenazas internas, etc.

Las organizaciones de hoy se enfrentan a un desafío abrumador.
El correo electrónico es al mismo tiempo la herramienta de comunicación empresarial más importante y el principal vector de ataque para las brechas de seguridad.

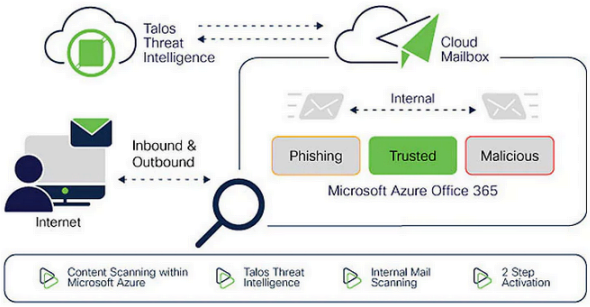
Cisco Secure Email incluye capacidades avanzadas de defensa contra amenazas que detectan, bloquean y remedian las amenazas en el correo electrónico entrante más rápido. Al mismo tiempo, protege la marca de una organización, evita la pérdida de datos y asegura la información importante en tránsito con cifrado de extremo a extremo.

BENEFICIOS

- Detecte y bloquee más amenazas con la inteligencia de amenazas global de Talos ™ y la inteligencia local de varios modelos de aprendizaje automático patentados.
- Obtenga una comprensión en tiempo real de los remitentes y aprenda y autentique las identidades de correo electrónico y las relaciones de comportamiento para protegerse contra ataques BEC.
- Combata el malware sigiloso que evade la detección inicial y corríjalo rápidamente para contener su impacto.
- Obtenga la máxima flexibilidad con una implementación en la nube, virtual, local o híbrida o muévase a la nube en fases
- Proteja el contenido sensible en los correos electrónicos salientes con Prevención de pérdida de datos (DLP) y cifrado de correo electrónico fácil de usar.
- Elimine automáticamente los correos electrónicos con enlaces peligrosos o bloquee el acceso a sitios recién infectados con análisis de URL en tiempo real para protegerse contra la suplantación de identidad (phishing).
- Evite el abuso de marca por parte de atacantes que utilizan su dominio para llevar a cabo campañas de phishing con la automatización del proceso de autenticación de mensajes basada en dominios (DMARC).

Proteja a los usuarios de las amenazas en los correos electrónicos entrantes

- Detecte y rechace más amenazas con inteligencia de amenazas integral.
- Combatir el malware más sigiloso escondido en adjuntos de correo electrónico.
- Bloquear amenazas basadas en URL como el phishing.
- Aumentando las cazas de captura de spam.
- Proteger a las usuarias de remitentes fraudulentos.



Proteja su marca y sus datos confidenciales en el correo electrónico saliente

El abuso de suplantación de dominio incontrolado y la pérdida de datos reduce en gran medida la reputación de su marca y afecta su capacidad para comunicarse fácilmente con sus socios y clientes. Los datos confidenciales también pueden caer en las manos equivocadas cuando se envían en un correo electrónico no seguro. Esto puede dar lugar a infracciones de cumplimiento.

- Conserve la reputación de su dominio.
- Protéjase contra el abuso de marca.
- Evite la pérdida de datos.
- Asegure los datos importantes en el correo electrónico saliente
- Opciones de implementación: El correo electrónico seguro se puede implementar en la nube, virtual, local o híbrido, y las organizaciones pueden migrar a la nube en fases, lo que permite la máxima flexibilidad.

INTEGRACION:

La integración de Cisco Secure Email en la plataforma SecureX proporciona una mayor visibilidad y automatización en todo el conjunto de productos de seguridad de Cisco, proporcionando la protección que garantiza que las empresas funcionen de forma segura. La plataforma robusta simplifica su experiencia de correo electrónico seguro al coordinarse con otros componentes dentro de su infraestructura para acelerar el tiempo de detección en múltiples componentes. Ese nivel de visibilidad maximiza la eficiencia del correo electrónico seguro y la productividad de sus equipos.

boyra
comunica tus sueños

TELEFONOS: 57 601 9156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM