E.
EMAIL

Censornet Email Security

www.xailna.com
ventas@xailna.com
Tel. +52 (55) 8421-6690

Censornet Email Security (EMS)

Seguridad de correo electrónico multicapa para afrontar amenazas de seguridad de correo electrónico conocidas, desconocidas y emergentes. Detenga el phishing a gran escala, los ataques dirigidos de fraude y el malware adjunto en el correo, solución integral en la nube, no requiere hardware o software para ser usado, fácil de implementar en tan solo unas horas.

Censornet Email Security ofrece una protección integral contra las amenazas de correo electrónico tradicionales, incluidos spam, virus, ataques de phishing a gran escala y direcciones URL maliciosas.

Censornet Email Security también incluye una combinación única de tecnologías innovadoras avanzadas para hacer frente a amenazas de correo electrónico sofisticadas y modernas, incluidos ataques de suplantación de identidad y malware desconocido.

Los 10,000 algoritmos de inteligencia artificial analizan más de 130 variables contenidas en cada mensaje de correo electrónico.

Múltiples motores antivirus basados en firmas y comportamiento ofrecen protección contra todas las formas de malware, incluidas las variantes de día cero.

- Detección de spam del 99,999%.
- 100% de protección contra virus.

El gran poder de "Censornet Email Security" radica en su sofisticado motor de políticas que permite a los administradores personalizar el flujo de correo electrónico entrante y saliente de la organización. El motor puede inspeccionar todos los aspectos del correo electrónico, incluidos el tamaño, el contenido, los archivos adjuntos, los encabezados, el remitente, destinatario, entre otros y tomar las acciones adecuadas, como entregar, poner en cuarentena de la empresa, redirigir, notificar y/o rechazar.

"Censornet Email Security" es aprovisionado a través de Censornet suite, que también incluye seguridad web, seguridad de aplicaciones en la nube y autenticación de múltiples factores, proporciona una única interfaz web para la configuración y gestión central de las políticas, así como para la visualización y generación de reportes.

El servicio de "Email Security" en la nube, incluye un registro detallado de la actividad de correo electrónico, para que los administradores puedan dar seguimiento detallado de correos, a través de filtros avanzados, los administradores pueden rápidamente localizar mensajes con detalle del estado que guardan.

SEGURIDAD DE CORREO ELECTRÓNICO

- 100% basado en la nube y fácil de implementar con un simple cambio de registro MX.

- Incorpora múltiples tecnologías para garantizar índices de detección de amenazas de clase empresarial con una precisión muy alta.

- Análisis completo del correo electrónico entrante y saliente, e incluye algoritmos para la prevención de la fuga de información (DLP).

- Múltiples motores antivirus basados en firmas, comportamiento, y análisis por servicios avanzados de emulación (sandbox), aislando los archivos adjuntos sospechosos o positivos para malware o ataques de día cero.

- Censornet LinkScan es un servicio que proporciona en tiempo real protección al analizar cada uno de los URLs adjuntos en los correos electrónicos previniendo que los usuarios visiten ligas maliciosas.

SERVICIOS COMPLEMENTARIOS

Archivado de correo electrónico

Proporciona una copia del correo electrónico entrante y saliente en la plataforma en la nube de Censornet, con almacenamiento ilimitado durante los años que la empresa requiera, dicha copia de correo, no se puede eliminar ni modificar y puede ser consultado por los usuarios o por los administradores.

Continuidad del correo electrónico

Proporciona a los usuarios una "Bandeja de entrada de emergencia" a la que se accede a través del navegador si falla el servidor de correo electrónico principal.

Correo electrónico seguro

Proporciona una solución simple para enviar correos electrónicos cifrados a destinatarios específicos.

CARACTERÍSTICAS

Anti-spam	• Múltiples motores utilizan una combinación de tecnologías para detectar correo no deseado, así como ataques de suplantación de identidad sofisticados.
Anti-malware	• Múltiples motores antivirus tradicionales basados en firmas y comportamientos para la detección de malware.
Censornet LinkScan™	• LinkScan reescribe las direcciones URL en los mensajes de correo electrónico y brinda protección al momento que los usuarios hacen clic en las ligas adjuntas. • Con opciones para redirigir automáticamente, hacer clic en continuar, bloquear amenazas y mostrar/ocultar el URL de destino. • Los enlaces se revisan al momento de la entrega del mensaje, así como en el momento del clic.
Listas seguras y denegadas	• Cree listas de seguridad y denegación para toda la empresa y/o para usuarios individuales.
TLS / Opportunistic TLS	• Aplique el cifrado TLS y restrinja la comunicación con otros servidores de correo electrónico que no admitan el protocolo TLS. • Opción para habilitar TLS oportunista con posibilidad de intercambiar correo en texto plano si el servidor de correo receptor no admite TLS.
Verificación de email	• Soporte para SPF, DKIM y DMARC.
Lista de seguimiento de ejecutivos	• Utilice los detalles sincronizados desde Active Directory para detectar automáticamente los nombres reales de los usuarios en los campos de dirección del encabezado y del sobre para protegerse contra los ataques de suplantación de identidad/fraude del director ejecutivo.
Dominios cercanos	• Compara el dominio del remitente con nombres de dominio legítimos para identificar suplantación de dominios (que difieren del nombre de dominio real en uno o dos caracteres). • Protege contra ataques de suplantación de identidad/fraude de directivos.
Etiquetas de asunto y encabezados	• Agregue etiquetas como [EXTERNO] o [MARKETING] a las líneas de asunto del mensaje. • Agregue encabezados HTML o de texto sin formato a los mensajes entrantes para alertar a los usuarios sobre riesgos potenciales.
Archivos adjuntos	• Comprobación de tipo MIME de archivos adjuntos con capacidad para bloquear tipos de archivos peligrosos. • Detectar archivos protegidos por contraseña.
Listas de palabras clave	• Crear listas ilimitadas de palabras clave. Use reglas para analizar mensajes y tomar medidas basadas en contenido confidencial o sensible.
Supervisión del límite de envío	• Protección automática contra intentos de enviar grandes volúmenes de mensajes salientes para evitar la inclusión en listas negras de dominios.
Cola de correo (continuidad de servicio)	• El correo electrónico se pone automáticamente en cola durante 7 días en caso de falla o interrupción del servicio/servidor de correo electrónico principal.
Prevención de ataque de recolección de directorio (DHA)	• Deniegue el correo electrónico destinado a direcciones de correo electrónico falsas o no válidas.

ADMINISTRACIÓN

Motor de políticas	• Más de 20 activadores condicionales para controlar la entrega de correos electrónicos y filtrar los mensajes según el tamaño, las palabras clave, la puntuación de spam, la hora, el origen, el destino, el tamaño de los archivos adjuntos, los encabezados, los atributos de AD y más.
Sincronización de usuarios	• El servicio de sincronización de Active Directory garantiza que se repliquen los cambios. Aplique reglas basadas en la pertenencia al grupo de AD si es necesario.
Interfaz web	• Completamente administrado y entregado a través de Censornet.
Administración delegada	• Permite la creación de múltiples administradores con diferentes niveles de acceso a la Plataforma Censornet
Cuarentena	• Opción para mover mensajes a cuarentenas de Empresa y Usuario.

Compendio de cuarentena	• Los correos electrónicos de resumen enumeran todos los mensajes dentro de la cuarentena del usuario y permiten obtener una vista previa, liberar o bloquear los mensajes. La interacción con el resumen permite al usuario administrar su caja fuerte individual y denegar listas. Los usuarios pueden establecer la frecuencia y los días en que se reciben los correos electrónicos de resumen.
Descargos de responsabilidad	• Agregue un descargo de responsabilidad de HTML y/o texto sin formato a todos los correos electrónicos salientes. Establezca diferentes descargos de responsabilidad para diferentes dominios.

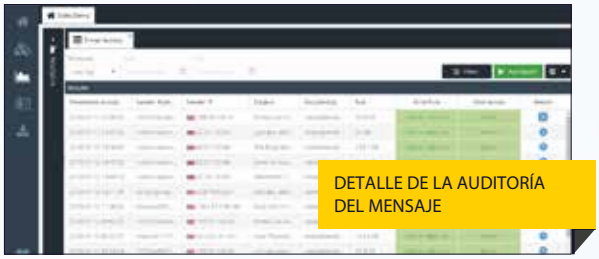
INFORMES

Visibilidad en tiempo real	• Los gráficos brindan una visibilidad detallada del flujo de correo entrante y saliente, así como las reglas activadas y las acciones realizadas. Capacidad para profundizar desde gráficos y cuadros de alto nivel hasta informes detallados.
Generador de informes	• Los administradores pueden definir sus propios informes en función de los nombres y criterios de los campos disponibles. Los informes se pueden guardar y luego exportar. Los informes de auditoría se pueden buscar utilizando criterios que incluyen hora, usuario, dirección del remitente, asunto, IP del remitente, destinatario, dirección, acción final, nombre de la regla. Marcar informes como "Favoritos" los agrega a un área de acceso rápido.
Programación y alertas	• Vincule los informes a los horarios y opcionalmente, solo reciba un informe cuando haya contenido (modo de alerta). Alerta sobre reglas, acciones, contenido, etc.
Informes de tendencias principales	• Una selección de informes de tendencias predefinidos con datos gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviar por correo electrónico a los destinatarios.
Múltiples vistas	• Analizar e informar por hora, usuario, dirección del remitente, asunto, IP del remitente, destinatario, dirección, acción final, nombre de la regla.
Auditoría detallada (seguimiento de mensajes)	• Vista detallada del análisis de mensajes individuales con la razón exacta por la que se envió un correo electrónico entregado o rechazado. Incluye encabezados de correo electrónico y conversación completa con el servidor de correo electrónico remoto.
Retención de registros y archivado automático	• Los datos de registro de Email Security se archivan automáticamente después de 90 días y están disponibles para su descarga durante un período de 12 meses más. Están disponibles períodos de retención más largos.


TÍPICO CONJUNTO DE REGLAS DE MENSAJE


CREACIÓN DE REGLAS


INFORME DE REGLAS FINAL SUPERIOR


DETALLE DE LA AUDITORÍA DEL MENSAJE

DESPLIEGUE

Implementación rápida y sencilla	• Redirigir los registros MX del dominio a la nube de Censornet EMS.
Compatibilidad con los proveedor de servicios de correo electrónico	• Funciona con todos los proveedores de servicios de correo electrónico. Envíe correos electrónicos a diferentes proveedores en función de la membresía del grupo AD del usuario: admite entornos híbridos que usan Exchange en las instalaciones con O365 Intercambio en línea o Gmail.

E. EMAIL

Protección integral contra las amenazas de correo electrónico tradicionales, incluidos spam, virus, ataques de phishing a gran escala y direcciones URL maliciosas.

S. SAT

Defiende tu organización contra los ciberdelincuentes fortaleciendo su participación y estimulación automatizada.

W. WEB

Proteja a los usuarios de la web, malware, contenido ofencivo o inapropiado y mejora la productividad.

C. CASB

Descubra, analice, asegure y administre la interacción del usuario con aplicaciones en la nube, en línea y mediante API.

M. MFA

Reducir el impacto de grandes violaciones de datos, protegiendo cuentas de usuario con algo más que contraseñas.

ID. IDaaS

Controle el acceso de los usuarios con amenaza de identidad. Automáticamente autenticar a los usuarios usando datos contextuales.

Nuestra Plataforma

Nuestra plataforma de seguridad en la nube integra seguridad de correo electrónico, web y aplicaciones en la nube, trabajando a la perfección con una identidad poderosa para activar la Autonomía del Motor de seguridad (ASE).

Esto lo lleva más allá de la seguridad basada en alertas y en ataque automatizado en tiempo real prevención.

Motor de seguridad autónomo

Habilite los productos tradicionalmente para compartir y reaccionar ante eventos de seguridad y estado de datos mientras aprovecha la amenaza de clase mundial. Prevenga los ataques antes de que ocurran.

ASE proporciona seguridad las 24 horas del día, los 7 días de la semana para que usted no tenga que hacerlo.

Acceso completo a inteligencia de amenazas.

Dirección:
Insurgentes Sur 1602
Col. Crédito Constructor
C.P. 03940 Benito Juárez
CDMX México.

Teléfono:
+52 (55) 8421-6690

Correo Electrónico:
ventas@xailna.com

xailna.com

Xailna
Internet Business Consulting