Censornet Email Security (EMS)

Protección contra amenazas de correo electrónico conocidas, desconocidas y emergentes.

Email Security (EMS) de Censornet proporciona una protección integral contra las amenazas tradicionales de correo electrónico, como spam, virus, ataques de phishing a gran escala y URL maliciosas.

EMS también incluye una combinación única de tecnologías avanzadas e innovadoras para abordar los objetivos modernos y sofisticados, amenazas de correo electrónico, incluidos ataques de suplantación de identidad (compromiso de correo electrónico empresarial o fraude de CEO) y malware desconocido.

El patrón tradicional, el atributo del mensaje y la coincidencia de características se complementan con un análisis algorítmico para una detección de amenazas definitiva sin afectar la precisión.

El análisis de comportamiento solo incluye más de 10,000 algoritmos que analizan más de 130 variables extraídas de cada mensaje de correo electrónico.

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

- 99,999% de detección de spam con casi cero falsos positivos
- 100% de protección contra virus

El núcleo de EMS es un motor de políticas sofisticado que permite al administrador de TI personalizar exactamente cómo fluye el correo electrónico dentro y fuera de la organización. El motor puede inspeccionar todos los aspectos del correo electrónico, incluido el tamaño, contenido, los archivos adjuntos, encabezados, remitente, destinatarios y tomar las medidas adecuadas, como entregar, poner en cuarentena, poner en cuarentena la empresa, redireccionar, notificar y rechazar.

EMS es tanto una solución de seguridad de correo electrónico avanzada como un motor de enrutamiento de correo electrónico completo, basado en la nube con cuarentenas personales y de la empresa con todas las funciones para la gestión de mensajes. La categorización profunda (por ejemplo: distinguir entre marketing profesional y mensajes sospechosos de campañas de correo electrónico masivo), permite políticas flexibles que detallan con precisión cómo se procesan los diferentes tipos de mensajes y etiquetado.

EMS está completamente administrado y entregado a través de la plataforma Censornet que también incluye seguridad web, seguridad de aplicaciones en la nube y autenticación multifactor. La plataforma Censornet proporciona una única interfaz web para la configuración y gestión de políticas centrales, así como la visualización y generación de informes de datos.

EMAIL SECURITY

- 100% basado en la nube y fácil de implementar con un simple cambio de registro MX.
- Incorpora múltiples tecnologías para garantizar tasas de detección de amenazas de clase empresarial con una precisión muy alta.
- Análisis completo de correo electrónico entrante con análisis de correo electrónico saliente, opcional usando listas ilimitadas de palabras clave.
- Múltiples motores AV tradicionales basados en firmas y comportamientos, incluido el sandboxing estático de archivos adjuntos.
- Censornet LinkScan ™ brinda protección en el momento de hacer clic contra URL maliciosas en correos electrónicos con la opción de escanear enlaces en el momento de la entrega.

Para los administradores de correo electrónico, el seguimiento detallado de mensajes es invaluable para poder ver de forma rápida exactamente por qué se entregó o rechazó un correo electrónico, incluidos los encabezados y la conversación completa con el servidor de correo electrónico remoto.

SERVICIOS ADICIONALES

Email Backup

Almacena copias de mensajes hasta por 7 años con búsqueda de texto completo.

Email Archiving

Proporciona un archivo totalmente compatible con almacenamiento ilimitado durante un tiempo ilimitado.

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 sencilla para enviar correos electrónicos cifrados a destinatarios específicos.

censornet.

PRINCIPALES CARACTERÍSTICAS

Anti-spam	• Varios motores utilizan una combinación de tecnologías para detectar spam, así como ataques de suplantación de identidad y phishing dirigidos más sofisticados.
Anti-malware	• Múltiples motores antivirus tradicionales basados en firmas y comportamientos para la detección de malware.
Censornet LinkScan™	• LinkScan reescribe las URL en los mensajes de correo electrónico y proporciona protección de punto de clic mediante múltiples servicios de reputación. • Opciones para redireccionar automáticamente, hacer clic en continuar, bloquear en caso de amenaza y mostrar / ocultar la URL de destino. • Opción para escanear enlaces en el momento de la entrega del mensaje, así como en el momento del clic.
Listas seguras y denegadas	• Cree listas Safe & Deny para toda la empresa y / o usuarios individuales.
TLS / TLS Oportunista	• 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 retroceso al texto sin formato si el servidor de correo receptor no admite TLS.
Verificación de Email	• Soporte para SPF, DKIM y DMARC.
Lista de seguimiento ejecutivo	• Utilice detalles sincronizados desde Active Directory para detectar automáticamente los nombres reales de los usuarios dentro de los campos de dirección de encabezado, Hacia/ De, para proteger contra ataques de suplantación de identidad / fraude de CEO.
Dominios cercanos (cousin)	• Compara el dominio del remitente con los nombres de dominio legítimos para identificar los dominios cercanos (que varían del nombre de dominio real en uno o dos caracteres). • Protege contra ataques de suplantación de identidad / fraude de CEO.
Etiquetas de asunto y encabezados	• Agregue etiquetas como [EXTERNAL] o [MARKETING] a las líneas de asunto del mensaje. • Agregue HTML o encabezados de texto sin formato a los mensajes entrantes para alertar a los usuarios sobre riesgos potenciales.
Archivos adjuntos	• Verificación de tipo MIME de archivos adjuntos con capacidad para bloquear tipos de archivos peligrosos. • Detectar archivos protegidos con contraseña.
Listas de palabras clave	• Cree listas ilimitadas de palabras clave. Utilice reglas para analizar mensajes y tomar medidas basadas en contenido confidencial o sensible.
Envío de supervisión de límite	• Protección automática contra intentos de enviar grandes volúmenes de mensajes salientes para evitar la lista negra de dominios.
Cola de correo	• El correo electrónico se pone en cola automáticamente durante 7 días en caso de falla o interrupción del servicio / servidor principal de correo electrónico.
Prevención de Directory Harvest Attack (DHA)	• Elimine el correo electrónico destinado a direcciones de correo electrónico falsas o no válidas.

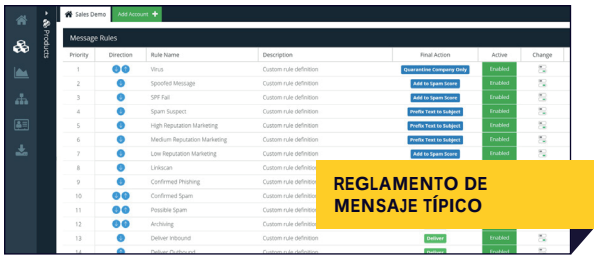
ADMINISTRACIÓN

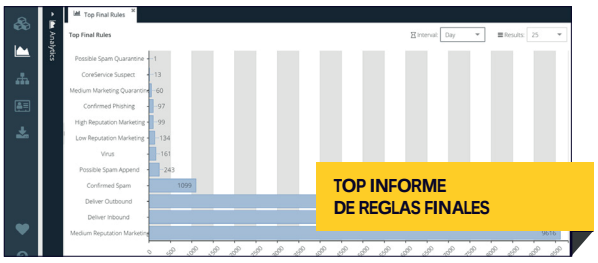
Motor de políticas	• Más de 20 activadores condicionales para controlar la entrega de correo electrónico y filtrar mensajes según el tamaño, palabras clave, puntuación de spam, hora, fuente, destino, tamaño de los archivos adjuntos, encabezados, atributos de AD y más.
Sincronización de usuarios	• El servicio de sincronización de Active Directory garantiza la replicación de los cambios. Aplique reglas basadas en la membresía del grupo AD si es necesario.
Interfaz web	• Totalmente gestionado y entregado a través de la plataforma 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.

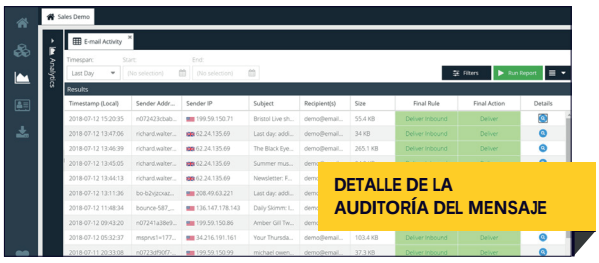
Resumen de cuarentena	• Los correos electrónicos de resumen enumeran todos los mensajes dentro de la cuarentena del usuario y permiten obtener una vista previa, liberar o bloquear los mensajes. La interacción con el resumen permite al usuario administrar sus listas individuales de Safe & Deny. Los usuarios pueden establecer la frecuencia y los días en los que se reciben los correos electrónicos de resumen.
Descargos de responsabilidad	• Agregue una renuncia de responsabilidad en HTML y / o texto sin formato a todos los correos electrónicos salientes. Establezca diferentes renuncias de responsabilidad para diferentes dominios.

INFORMES

Visibilidad en tiempo real	• Los gráficos brindan visibilidad detallada del flujo de correo entrante y saliente, así como las reglas activadas y las acciones tomadas. Capacidad para desglosar desde gráficos y tablas de alto nivel hasta informes detallados.
Generador de informes	• Los administradores pueden definir sus propios informes según los nombres y criterios de campo 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 y nombre de la regla. Al marcar los informes como "Favoritos", se agregan a un área de acceso rápido.
Programación y alertas	• Vincular informes a horarios y, opcionalmente, recibir un informe solo cuando haya contenido (modo de alerta). Alerta sobre reglas, acciones, contenido, etc.
TOP de informes	• Una selección de informes de tendencias predefinidos con gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviar por correo electrónico a los destinatarios.
Vistas múltiples	• Analizar e informar por tiempo, usuario, dirección del remitente, asunto, IP del remitente, destinatario, dirección, acción final y nombre de la regla.
Auditoría detallada (seguimiento de mensajes)	• Vista detallada del análisis de mensajes individuales con la razón exacta por la que se entregó o rechazó un correo electrónico. Incluye encabezados de correo electrónico y conversación completa con el servidor de correo electrónico.
Retención de registros y archivado automático	• Los datos de registro de Email Security se archivan automáticamente después de 90 días y están disponibles para descargar desde la plataforma Censornet por un período de 12 meses más. Hay disponibles períodos de retención más prolongados.







DESPLIEGUE

Implementación rápida y sencilla	• Redirigir los registros MX del dominio a la nube Censornet EMS.
Soporte del proveedor de servicios de correo electrónico	• Funciona con todos los proveedores de servicios de correo electrónico. Envíe correo electrónico a diferentes proveedores según la membresía del grupo AD del usuario, que admite entornos híbridos utilizando Exchange en las instalaciones con O365 Exchange Online o Gmail.

censornet.

PLATAFORMA CENSORNET

Nuestra plataforma

Nuestra plataforma de seguridad en la nube integra seguridad web y de correo electrónico, CASB (Agente de seguridad de acceso a la nube) y MFA (Autenticación multifactorial) adaptativa que activa el Motor de Seguridad Autónomo (ASE), para llevarlo más allá de la seguridad impulsada por alertas, con prevención automatizada de ataques en tiempo real.

E. EMAIL

Proteja a toda su organización contra amenazas de seguridad por correo electrónico conocidas, desconocidas y emergentes, incluido el fraude por correo electrónico.

W. WEB

Proteja a los usuarios contra malware transmitido por Internet, contenido ofensivo o inapropiado y mejore la productividad.

C. CASB

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

M. MFA

Reduzca el impacto de las filtraciones de datos a gran escala protegiendo las cuentas de los usuarios con algo más que contraseñas.

Autonomous Security Engine — ASE

Permita que los productos tradicionalmente aislados compartan y reaccionen a eventos de seguridad y datos estatales mientras aprovechan la inteligencia de amenazas de clase mundial. Evite los ataques antes de que entren en la cadena "Cyber Kill Chain".

ASE proporciona seguridad las 24 horas del día, los 7 días de la semana.

Acceso completo a la inteligencia de amenazas sin costo.

Parte integral de la Plataforma Censornet.

PC COM Mayorista

https://pccommayorista.com
+52 (55) 5599-0670
contacto@pccommayorista.com

censornet.