W. WEB

Censornet Web Security

cobranetworks.lat

Tel. +52 55 5599 0691

ventas@cobranetworks.lat

Seguridad web de Censornet (WS)

Proteja su organización del malware transmitido por la web, además de bloquear contenido ofensivo o inapropiado y administre el tiempo que pasa en sitios web que afectan la productividad con Censornet Web Security. Impulsado por una arquitectura única que garantiza tiempos de respuesta ultrarápidos para todos los usuarios sin importar en qué parte del mundo se encuentren.

Múltiples capas de seguridad en la puerta de enlace ofrecen una protección integral contra el malware transmitido por la web y otras amenazas mediante una poderosa combinación de inspección de tráfico en tiempo real, análisis de reputación de URL y heurística.

Web Security está completamente integrado con la plataforma Censornet que también incluye Email Security, Cloud Application Security y Multi-Factor Authentication. La plataforma Censornet proporciona una interfaz web única para la configuración y administración de políticas centrales, así como para la visualización y generación de informes de datos.

Web Security se implementa mediante agentes o proxies locales, o una combinación de ambos, para satisfacer las necesidades de organizaciones de todos los tamaños. Las opciones de implementación flexibles simplifican la implementación, lo que acelera el tiempo de generación de valor.

El servicio se basa en el protocolo ligero ICAP con servidores implementados en múltiples ubicaciones en todo el mundo. Más sofisticado que las soluciones basadas en DNS, el servicio tiene una sobrecarga significativamente menor que los proxies basados en la nube, lo que elimina la necesidad de representar todo el tráfico, sin impacto percibido por el usuario en el uso de aplicaciones web o en la nube. Solo los metadatos de solicitud http se envían a Censornet Cloud y se comparan con la política.

Web Security proporciona un solo panel de administración para analizar y administrar la actividad de navegación web en múltiples redes y dispositivos, ya sea que los usuarios estén en la red corporativa o trabajen de forma remota.

Mediante el uso exclusivo de agentes en los dispositivos móviles, Web Security ofrece un enfoque sin proxy, ni puerta de enlace que reduce significativamente la latencia y conserva la dirección IP real del usuario y mantiene la privacidad al permitir que el navegador mantenga una comunicación directa con el servidor de aplicaciones web. Los dispositivos móviles se puede utilizar para acceder a aplicaciones web sin provocar que el contenido sirva en función de la ubicación de un proxy en la nube, generar falsas alertas de robo de identidad o presentar mensajes de error frustrantes o confusos para los empleados móviles.

Los usuarios disfrutan de una experiencia rápida, discreta y de la libertad de trabajar como, cuando y donde quieran, con una experiencia uniforme independientemente del dispositivo utilizado. TI mantiene la visibilidad y, en su caso, el control sobre la navegación web.

SEGURIDAD WEB

- Administre más de 500 categorías de contenido web y miles de millones de páginas web.
- Opcionalmente, protege contra malware y otras amenazas web en la puerta de enlace utilizando múltiples capas de seguridad y una poderosa combinación de tecnologías.
- Protección completa, incluida la inspección profunda del tráfico cifrado SSL.
- Las nuevas URL se analizan en tiempo real en busca de malware y se clasifican automáticamente mediante técnicas de aprendizaje automático.
- BYOD y dispositivo invitado listo con Captive Portal para filtrado sin contacto.
- Las políticas se pueden establecer en función de categorías web predefinidas o categorías de URL personalizadas o palabras clave, y se pueden aplicar a grupos de usuarios o grupos de dispositivos.
- Opciones de implementación flexibles: agente o proxy, o ambos.
- Los agentes para Microsoft Windows y MAC OS X complementan el punto final AV y aseguran que las políticas de administración de contenido web sean persistentes cuando los usuarios móviles trabajan de forma remota.
- Cobertura de dispositivos móviles mediante el enrutamiento del tráfico (a través de VPN) a través de Censornet Cloud Gateway, en las instalaciones o en la nube.
- El complemento de la puerta del enlace de análisis de imagen opcional analiza el contenido de la imagen en tiempo real en busca de imágenes inapropiadas "No seguras para el trabajo" (NSFW).
- Cloud Application Security puede habilitarse instantáneamente sin necesidad de ningún hardware, software o cambios de configuración adicionales para proporcionar además de descubrimiento, visibilidad y administración del acceso a cientos de aplicaciones en la nube y miles de acciones dentro de las aplicaciones.

Cloud Application Security se puede habilitar instantáneamente sin necesidad de ningún hardware, software o cambios de configuración adicionales para brindar además descubrimiento, visibilidad y administración del acceso a cientos de aplicaciones en la nube y miles de acciones dentro de las aplicaciones.

Los agentes se pueden usar en combinación con Censornet Cloud Gateway para sitios con poblaciones de escritorios fijos, como centros de llamadas. La instalación de una sola puerta de enlace extiende rápidamente las políticas de seguridad del contenido web a toda la red y opcionalmente, agrega varias capas de seguridad para defenderse contra el malware transmitido por la web y otras amenazas.

Un sofisticado motor de políticas habilitan reglas que bloquean, permiten y rastrean la actividad de navegación web. Las cuotas de tiempo se pueden aplicar a las reglas para limitar el tiempo dedicado a los sitios de compras a 1 hora por día, por ejemplo, lo que permite a las organizaciones mantener la productividad y la eficacia.

Las reglas pueden basarse en el usuario, el dispositivo o el tiempo y aplicarse al contenido web según la categoría web, la categoría de URL personalizada o coincidencia de palabras clave. Las condiciones se pueden combinar usando la lógica AND OR para la potencia y flexibilidad.

Web Security está totalmente integrado con la plataforma Censornet, que proporciona visualización de datos enriquecidos e informes a través de un amplio conjunto de atributos y criterios. El análisis y los informes están disponibles por hora, usuario, dispositivo, categoría web, categoría de URL, dominio, palabra clave y resultado (permitir, bloquear, redirigir, advertir).

Ya sea que los datos de auditoría se requieran únicamente para la visibilidad de la actividad de navegación web, o para una certificación más formal del cumplimiento de las políticas internas o los estándares, las reglamentaciones y la legislación externos, Web Security proporcionará la evidencia necesaria.

DESPLIEGUE

Gateway	• Censornet Cloud Gateway se puede instalar en una máquina virtual o en un servidor físico en 30 minutos para extender las políticas de seguridad a toda la red. También disponible en la Nube.
Agentes	• Los agentes para Microsoft Windows y MAC OS X aplican políticas en el dispositivo. A prueba de manipulaciones y fácil de implementar mediante un asistente de instalación o mediante la política de grupo de AD. Complemente el AV de punto final existente con la gestión de contenido web.
Modos de implementación	• Software de agente, proxy directo (establecido por política de grupo, WPAD o manualmente) o modo de puerta de enlace para dispositivos invitados, personales (BYOD) o sin dominio.
Soporte WPAD	• Creación automática de archivos de detección automática de proxy web (WPAD) en función de la configuración de la red.
Compatibilidad con WCCPv2	• Admite el protocolo de comunicación de caché web (WCCP) v2 para la redirección de tráfico transparente desde los enrutadores/conmutadores de Cisco.

CARACTERÍSTICAS

ICAP	• Los servidores ICAP en varias ubicaciones en todo el mundo comparan los metadatos de las solicitudes web con las políticas, lo que elimina la necesidad de utilizar proxy para todo el tráfico en cuanto a velocidad, confiabilidad y escalabilidad.
Análisis anti-malware en tiempo real	• Incorpora varias capas de seguridad, cada una de las cuales utiliza una combinación potente y eficaz de herramientas y técnicas, incluida la detección de amenazas en línea, la reputación y la heurística.
Filtrado de URL	• Más de 500 categorías de contenido web cubren miles de millones de páginas web en varios idiomas, constantemente actualizadas para mayor precisión y protección. Las subcategorías se agrupan en categorías para facilitar la administración.
Clasificación automática de URL desconocidas	• Las nuevas URL se analizan en tiempo real para garantizar que solo se acceda al contenido aceptable.
Detección de proxy anónimo	• Impedir el acceso a sitios proxy anónimos.

Inspección HTTPS	• La inspección profunda de HTTPS permite escanear el contenido cifrado SSL en busca de malware (requiere Censornet Cloud Gateway en las instalaciones o en la nube). • Capacidad para deshabilitar la inspección SSL para aplicaciones de confianza específicas. • Opción de usar la Indicación de nombre de servidor (SNI) dentro del protocolo TLS para determinar el dominio de destino cuando se inicia una conexión, para el filtrado de URL de toque ligero de BYOD o dispositivos invitados sin problemas de administración de certificados (usado junto con el Portal cautivo).
Búsqueda segura	• Use el modo búsqueda segura en los portales de búsqueda más populares como Google, Yahoo, Bing y YouTube.
BYOD / Compatibilidad con dispositivos invitados	• Permita de forma segura el acceso a dispositivos invitados y BYOD a través del portal cautivo integrado (con soporte SNI para filtrado sin contacto). Permite a los usuarios existentes iniciar sesión desde dispositivos personales utilizando credenciales válidas (por ejemplo, Active Directory).
Anulaciones de URL	• Cree categorías de URL que se puedan aplicar para anular o crear excepciones dentro de las políticas de filtrado.
Modos de gateway	• Censornet Cloud Gateway puede operar en modo explícito o transparente.

ADMINISTRACIÓN

Motor de políticas	• Motor de políticas sofisticado que incluye atributos de Active Directory, dirección IP y MAC del dispositivo, tipo de dispositivo, etiqueta y acciones diferenciales.
Horario	• Las políticas se pueden aplicar en un cronograma continuo de 7 días.
Autenticación de usuario	• Se admiten varios métodos de autenticación, incluidos Active Directory Kerberos, inicio de sesión único, portal cautivo y contabilidad RADIUS.
Sincronización de usuarios	• El servicio de sincronización de Active Directory garantiza que se repliquen los cambios en Active Directory.
Interfaz web	• Totalmente integrado con la Plataforma Censornet.
Administración delegada	• Permite la creación de múltiples administradores con diferentes niveles de acceso a la Plataforma Censornet.
Páginas de notificación personalizadas	• Páginas de notificación de marca (Bloque, Portal cautivo, etc.) con logotipo, texto e información de términos de servicio.

INFORMES

Visibilidad en tiempo real	• Los gráficos de productividad muestran visibilidad instantánea sobre el cumplimiento de las políticas de acceso definidas. Consulta la actividad web en tiempo real por usuario, dispositivo, dominio y categoría. Vea exactamente qué usuarios acceden a qué sitios web.
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 tiempo, usuario, dispositivo, categoría web, categoría de URL, dominio, palabra clave y resultado (permitir, bloquear, redirigir, advertir).
Programación y alertas	• Vincule los informes a los horarios y opcionalmente, solo reciba un informe cuando haya contenido (modo de alerta). Alerta sobre palabras clave, categorías bloqueadas, dominios específicos, etc.
Informes de tendencias principales	• Una selección de informes de tendencias predefinidos con datos de gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviar por correo electrónico a los destinatarios.
Informes web extendidos	• El complemento opcional proporciona informes adicionales por grupo de Active Directory, incluidas las principales categorías web por grupo, los principales dominios y el tiempo empleado.
Múltiples vistas	• Analice e informe por usuario, dispositivo, categoría web o acción.
Retención de registros y archivo automático	• Los datos de registro de Web Security se archivan automáticamente después de 90 días y están disponibles para descargar desde la Plataforma Censornet por un período de 12 meses. Ademas están disponibles períodos de retención más largos.

+52 (55) 5599-0691 ventas@cobranetworks.lat cobranetworks.lat

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:

Prolongación División del Norte 4318, C.P. 14300 Ciudad de México, México.

Teléfono:

+52 (55) 5599-0691

Correo Electrónico:

ventas@cobranetworks.lat

cobranetworks.lat

COBRA NETWORKS