Censornet Web Security (WS)

La seguridad web de Censornet brinda protección contra contenido dañino, ofensivo o inapropiado, además de administrar el tiempo dedicado a sitios web que pueden tener un impacto significativo en la productividad.

Las múltiples capas de seguridad en el gateway ofrecen una protección integral contra 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 seguridad de correo electrónico, seguridad de aplicaciones en la nube y autenticación multifactor. La plataforma Censornet proporciona una única interfaz web para la configuración y gestión central de políticas, así como la visualización y generación de informes de datos.

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

El servicio se basa en el protocolo ICAP, ligero con servidores desplegados 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 usar un proxy para 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 único panel 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 trabajando de forma remota.

Utilizando exclusivamente agentes en los endpoints , Web Security ofrece un enfoque sin proxy y sin gateway que reduce significativamente la latencia, conservando la dirección IP real del usuario.

WEB SECURITY

- Gestionar más de 500 categorías de contenido web y miles de millones de páginas.
- Opcionalmente protege contra malware y otras amenazas web en el gateway usando múltiples capas de seguridad y una poderosa combinación de tecnologías.
- Protección completa, incluida una 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 machine learning.
- BYOD y dispositivo invitado listo con portal cautivo para filtrado sin intervención.
- Las políticas se pueden establecer en función de categorías web predefinidas, categorías de URL personalizadas o palabras clave, se pueden aplicar a grupos de usuarios o grupos de dispositivos.
- Opciones de implementación flexibles: agente, proxy o ambos.
- Los agentes para Microsoft Windows y MAC OS X complementan el AV del endpoint y garantizan que las políticas de administración de contenido web sean persistente cuando los usuarios móviles están trabajando de forma remota.
- Cobertura de dispositivos móviles mediante el enrutamiento del tráfico (a través de VPN) por medio de Censornet Cloud Gateway, en las instalaciones o en la nube.
- El gateway opcional de análisis de imagen analiza el contenido en tiempo real para las imágenes inapropiadas, "Not Safe For Work" (NSFW).
- La seguridad de aplicaciones en la nube se puede habilitar instantáneamente sin la necesidad de ningún hardware, software o cambios de configuración adicionales para roporcionar, descubrimiento, visibilidad y administración del acceso a cientos de aplicaciones en la nube y miles de acciones dentro de las aplicaciones.

y mantiene la privacidad al permitir que el navegador mantenga una comunicación directa con el servidor de aplicaciones web. Los dispositivos móviles se pueden utilizar para acceder a aplicaciones web sin que el contenido dependa de la ubicación de un proxy en la nube, generando falsas alertas de robo de identidad o presentando mensajes de error frustrantes o confusos a los empleados móviles.

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

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

censornet.

Ficha Técnica: Censornet Web Security (WS)

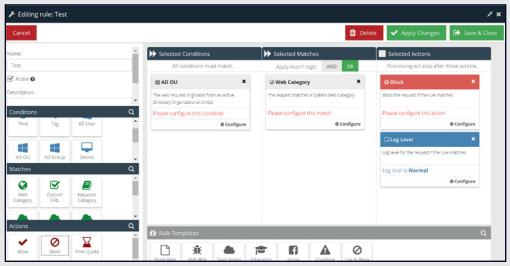
Los agentes se pueden usar en combinación con Censornet Cloud Gateway para sitios con usuarios de escritorios fijos, como centros de llamadas. La instalación de un único gateway extiende rápidamente las políticas de seguridad del contenido web a toda la red, opcionalmente agrega varias capas de seguridad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

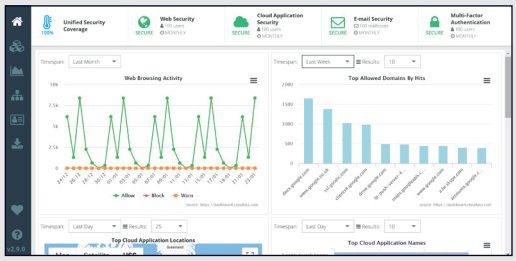
Un motor de políticas sofisticado habilita reglas que bloquean, permiten o realizan un seguimiento de la actividad de navegación web. Por ejemplo: Las cuotas de tiempo se pueden aplicar a las reglas para limitar el tiempo dedicado a los sitios de compras a 1 hora por día, lo que permite a las organizaciones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

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

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

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





IMPLEMENTACIÓN

Gateway	• Censornet Cloud Gateway se puede instalar en una máquina virtual o 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 hacen cumplir las 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 del endpoint existente con la gestión de contenido web.
Modos de Implementación	• Agente de software, proxy directo (establecido por política de grupo, WPAD o manualmente) o modo gateway para dispositivos invitados, personales (BYOD) o que no pertenecen al dominio.
Soporte WPAD	• Creación automática de un archivo de descubrimiento automático de proxy web (WPAD) basado en la configuración de la red.
Soporte WCCPv2	• Admite el protocolo de comunicación de caché web (WCCP) v2 para redireccionar el tráfico transparente desde los enrutadores / conmutadores de Cisco.

PRINCIPALES CARACTERÍSTICAS

ICAP	• Los servidores ICAP en múltiples ubicaciones en todo el mundo comparan los metadatos de las solicitudes web con las políticas, lo que elimina la necesidad de utilizar un proxy para todo el tráfico para lograr velocidad, confiabilidad y escalabilidad.
Escaneo anti-malware en tiempo real	• Incorpora múltiples capas de seguridad, cada una de las cuales utiliza una combinación poderosa y eficaz de herramientas y técnicas, incluida la detección de amenazas en línea, reputación y heurística.
Filtrado de URL	• Más de 500 categorías de contenido web que cubren miles de millones de páginas web en varios idiomas, actualizadas constantemente para brindar 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.
Análisis de imagen	• El complemento opcional de gateway proporciona un análisis en tiempo real del contenido de la imagen, para las imágenes inapropiadas, "Not Safe For Work" (NSFW). Incluye tres niveles de sensibilidad: alta, media y baja.
Detección de proxy anónimo	• Evite el acceso a sitios proxy anónimos.

Inspección HTTPS	• La inspección profunda de HTTPS permite que el contenido cifrado con SSL se escanee en busca de malware (requiere Censornet Cloud Gateway en las instalaciones o en la nube). • Posibilidad de desactivar la inspección SSL para aplicaciones de confianza específicas. • Opción de utilizar la indicación de nombre de servidor (SNI) dentro del protocolo TLS para determinar el dominio de destino cuando se inicia una conexión, para un filtrado ligero de URL de dispositivos BYOD o invitados sin problemas de gestión de certificados (utilizado junto con el portal cautivo).
Búsqueda segura	• Aplique el modo de búsqueda segura en los motores de búsqueda más populares, incluidos Google, Yahoo, Bing y YouTube.
Soporte para dispositivos BYOD / invitados	• Permita de forma segura el acceso a dispositivos invitados y BYOD a través del portal cautivo integrado (con soporte SNI para filtrado sin intervención). 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.
Modo 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.
Programación	• Las políticas se pueden aplicar en un programa de tiempo 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 la replicación de 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 sobre 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 según los nombres y criterios de campo disponibles. • Los informes se pueden guardar y luego exportar. • Los informes de auditoría se pueden buscar usando criterios que incluyen tiempo, usuario, dispositivo, categoría web, categoría URL, dominio, palabra clave y resultado (permitir, bloquear, redireccionar, advertir).
Programación y alertas	• Vincular informes a horarios y, opcionalmente, recibir un informe solo cuando haya contenido (modo de alerta). Alerta sobre palabras clave, categorías bloqueadas, dominios específicos, etc.
Top de informes	• Una selección de informes de tendencias predefinidos con gráficos y tablas. Los informes se pueden exportar a PDF y enviar por correo electrónico a los destinatarios.
Informes web amplios	• El complemento opcional proporciona informes adicionales por grupo de Active Directory, incluidas las principales categorías web por grupo, los principales dominios y el tiempo invertido.
Vistas múltiples	• Analizar e informar por usuario, dispositivo, categoría web y 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 más. Hay disponibles períodos de retención más prolongados.

censornet.

PLATAFORMA CENSORNET

Nuestra plataforma

Nuestra plataforma de seguridad en la nube integra seguridad web, 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.

PCCOM Mayorista

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

censornet.