Cloud Access Security Broker (CASB)

Cloud Access Security Broker (CASB) de Censornet proporciona un único panel para descubrir, analizar y administrar la actividad de la nube en múltiples redes y dispositivos, ya sea que los usuarios estén en la red corporativa o trabajando de forma remota.

CASB está completamente integrado con la plataforma de Censornet que también incluye seguridad de correo electrónico, seguridad web 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.
El modo en línea CASB se implementa mediante agente, proxies o una combinación de ambos, para satisfacer las necesidades de organizaciones de todos los tamaños. Esta arquitectura flexible reduce significativamente el esfuerzo involucrado en implementar y administrar la solución, acelerando el tiempo de generación de valor.
Utilizando únicamente agentes en los endpoints, CASB ofrece un enfoque sin proxy que reduce significativamente la latencia, preserva la dirección IP real del usuario y mantiene la privacidad al permitir que el navegador mantenga una comunicación directa con el servidor de aplicaciones en la nube.
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.

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 un único gateway extiende rápidamente las políticas de seguridad a toda la red.
El modo API utiliza conectores API para las principales aplicaciones de almacenamiento en la nube, como box, Dropbox y Microsoft OneDrive. El modo API amplía la visibilidad de la actividad del usuario para incluir el acceso móvil mediante aplicaciones móviles (fuera del navegador).

CLOUD ACCESS SECURITY BROKER

- Proporciona descubrimiento y visibilidad de todas las aplicaciones en uso en la nube.
- La solución CASB "multimodo" en línea y API maximiza la visibilidad y protección.
- Protege los servicios en la nube autorizados como Salesforce, Office365 y Box, lo que permite una adopción segura de la nube.
- Protege contra malware y otras amenazas en la nube mediante múltiples capas de seguridad y una poderosa combinación de tecnologías.
- Visibilidad completa, incluida una inspección profunda del tráfico cifrado SSL.
- El equipo dedicado actualiza constantemente el catálogo de aplicaciones en la nube de Censornet que cubre miles de funciones y acciones en cientos de aplicaciones en la nube.
- Las aplicaciones se evalúan, clasifican y categorizan por riesgo con la capacidad de anular calificaciones predefinidas.
- Las políticas se pueden establecer a nivel granular en función de la persona o función, el dispositivo que se utiliza, red conectada, función dentro de la aplicación y la ubicación del usuario.
- Opciones de implementación flexibles: agente, proxy o ambos.
- Agentes para Microsoft Windows y MAC OS X.
- Cobertura de dispositivos móviles mediante el enrutamiento del tráfico (a través de VPN) por medio de Censornet Cloud Gateway, en las instalaciones, en la nube o mediante el modo API.

El modo API también incluye la capacidad de escanear archivos al cargarlos y cambiarlos por contenido específico, utilizando plantillas DLP predefinidas, así como escanear archivos en busca de malware. Se incluyen plantillas de políticas para información de identificación personal, propiedad intelectual, información confidencial, riesgo interno, PCI DSS e HIPAA. Se pueden crear listas de palabras clave adicionales si es necesario.
Image Analysis escanea archivos de imagen al cargarlos y cambiarlos en busca de contenido inadecuado, “Not Safe For Work” (NSFW).

El modo API funciona vinculando Censornet CASB a cuentas corporativas en aplicaciones de almacenamiento en la nube compatibles y se puede utilizar de forma independiente (sin la necesidad de agentes o gateways) o en combinación con el modo Inline.

Un motor de políticas sofisticado habilita reglas que auditan o administran el acceso a las aplicaciones, así como las acciones del usuario dentro de las aplicaciones. Las actividades genéricas se pueden bloquear en todas las aplicaciones, dentro de una o varias clases o aplicaciones específicas. Las condiciones refinan aún más las reglas para limitar el control por usuario, dispositivo, red, tiempo o nivel de riesgo. Las reglas también pueden activarse en función del contenido, como la dirección de correo electrónico utilizada para iniciar sesión o las palabras clave en las publicaciones de las redes sociales.

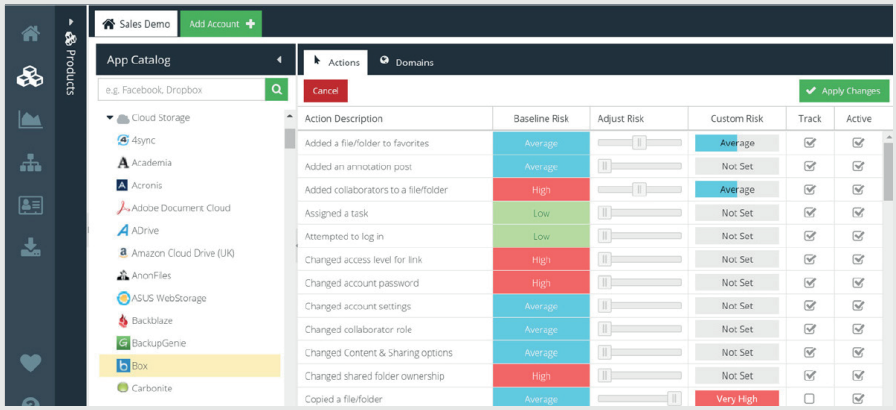
censornet.

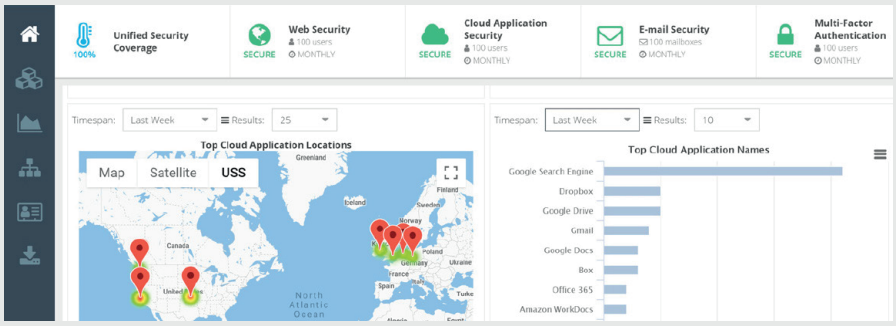
Ficha Tecnica: Cloud Access Security Broker (CASB)

En el corazón del servicio CASB se encuentra el catálogo de aplicaciones en la nube de Censornet, que contiene información detallada y actualizada constantemente sobre miles de funciones dentro de cientos de aplicaciones en la nube. Las aplicaciones se clasifican en clases (por ejemplo: CRM en la nube, almacenamiento en la nube y redes sociales) de riesgo evaluado y calificado. Las calificaciones predefinidas se pueden modificar fácilmente para reflejar el nivel de riesgo general de una organización, preocupaciones específicas o para alinearse con la actividad esperada del usuario en roles particulares.

CASB está completamente integrado con el portal de 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, clase de aplicación, nombre de la aplicación, acción de la aplicación, palabras clave, nivel de riesgo y resultado (bloquear o permitir).

Si los datos de auditoría se requieren únicamente para la visibilidad del uso de aplicaciones no autorizadas (o Shadow IT), para comprender el alcance del uso de dispositivos móviles personales (BYOD), para una certificación más formal del cumplimiento de políticas internas o estándares externos, regulaciones y legislación, Cloud Application Security proporcionará la evidencia necesaria.





PRINCIPALES CARACTERÍSTICAS

Descubrimiento de aplicaciones en la nube	• Detecte el uso y actividad de las aplicaciones en la nube, revele qué aplicaciones están en uso, incluidas las aplicaciones que usan un dominio personalizado. • Las aplicaciones dentro del catálogo se evalúan, clasifican y categorizan por riesgo con la capacidad de anular las calificaciones predefinidas. Los perfiles de proveedores proporcionan información sobre ingresos / tamaño para aumentar la confianza al sancionar aplicaciones.
Control de aplicaciones en la nube	• Controle el acceso a las aplicaciones a un nivel granular, hasta las funciones y acciones individuales dentro de las aplicaciones. • Bloquear actividades genéricas en todas las aplicaciones (por ejemplo: carga de archivos y compartir archivos), clases de aplicaciones (CRM, redes sociales y almacenamiento de archivos) o aplicaciones específicas. Aplicar condiciones para limitar el control por usuario, dispositivo, red, tiempo y nivel de riesgo. • Bloquear acciones basadas en contenido como la dirección de correo electrónico utilizada para iniciar sesión o palabras clave dentro de publicaciones en redes sociales.
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.
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.
Detección de proxy anónimo	• Evite el acceso a sitios proxy anónimos.

Ficha Tecnica: Cloud Access Security Broker (CASB)

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 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 asegura que los cambios en Active Directory se replican.
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.

INFORMES

Visibilidad en tiempo real	• Los gráficos de productividad muestran visibilidad instantánea sobre el cumplimiento de las políticas de acceso definidas. • Consulta en tiempo real la actividad web por usuario, dominio, aplicación y categoría. Vea exactamente qué usuarios acceden a qué aplicaciones y funciones dentro de esas aplicaciones.
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 a CSV o PDF. • Los informes de auditoría se pueden buscar utilizando criterios que incluyen tiempo, usuario, dispositivo, clase de aplicación, nombre de la aplicación, acción de la aplicación, palabras clave (por ejemplo, nombre de archivo, comentario, detalles de inicio de sesión), nivel de riesgo, tipo de amenaza (modo API), nombre de política, resultado (bloquear o permitir).
Programación y alertas	• Vincular informes a horarios y, opcionalmente, recibir un informe solo cuando haya contenido (modo de alerta). Alerta sobre acciones de alto riesgo, palabras clave, actividad permitida, 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.
Vistas múltiples	• Analizar e informar por usuario, dispositivo, categoría web y acción.

DESPLIEGUE

Gateway (modo en línea)	• 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 (modo en línea)	• 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.
Modo API	• Gateway API basada en la nube con conectores API para aplicaciones comunes de almacenamiento en la nube. Vincule cuentas corporativas en aplicaciones compatibles y, opcionalmente, escanee archivos en busca de contenido (escaneo DLP) y /o malware. • Análisis de imagen opcional escanea archivos de imagen en busca de contenido inapropiado. "Not Safe For Work" (NSFW). • Las categorías admitidas incluyen Gore, Adultos, Ropa interior (incluidos trajes de baño) y Extremismo. • Las aplicaciones compatibles incluyen box, Dropbox, Google Drive, Microsoft OneDrive y SharePoint.
Modos de implementación	• Agente de Software, proxy directo (establecido por política de grupo, WPAD o manualmente) o modo de 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.

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.