CASB

Censornet CASB

cobranetworks.lat

Tel. +52 55 5599 0691

ventas@cobranetworks.lat

Agente de seguridad de acceso en la nube (CASB)

Censornet CASB le permite a su empresa descubrir, analizar, proteger y administrar la interacción del usuario con las aplicaciones en la nube. Consiga visibilidad y control completo de las funciones y características de cada aplicación, proteja a toda su fuerza de trabajo desde cualquier lugar donde se encuentren laborando, además trabaja y se combina con Censornet Web Security.

CASB es una solución totalmente integrada a Censornet suite, que también incluye seguridad de correo, seguridad web y autenticación multi-factor. La suite Censornet proporciona una consola central web, para configuración y gestión de políticas, así como visualización de datos e informes.

CASB se implementa mediante agentes para usuarios distribuidos o a través de máquinas virtuales en ubicaciones con una alta concentración de usuarios o una combinación de ambos, para satisfacer las necesidades de empresas de todos los tamaños. Esta arquitectura reduce el esfuerzo involucrado en la implementación y administración de la solución.

Usando agentes en los dispositivos móviles, CASB ofrece una tecnología sin proxy que reduce significativamente la latencia, conserva la dirección IP real del usuario y mantiene privacidad al permitir que el navegador mantenga comunicación directa con el servidor de aplicaciones en la nube.

Los usuarios disfrutan de una experiencia rápida, silenciosa y la libertad de trabajar, cuando y donde quieran, una experiencia consistente independientemente del dispositivo utilizado, mientras las áreas mantienen visibilidad y control de las actividades de los usuarios.

Los agentes se pueden utilizar en combinación con máquinas virtuales en la nube de Censornet para sitios con alta poblaciones de equipos de escritorio. Al instalar una máquina virtual en los enlaces de la oficina, extiende rápidamente las políticas de seguridad a toda la red, no importando el número de usuarios o el tipo de dispositivo que estén usando los usuarios empresariales.

En modo API (offline) utiliza conectores para las aplicaciones de almacenamiento más usadas en la nube, tales como, Dropbox y Microsoft OneDrive. La API amplía la visibilidad y previene la actividad del usuario al compartir información empresarial de forma no autorizada, al ingresar a las aplicaciones en la nube en dispositivos no monitoreados por las áreas.

AGENTE DE SEGURIDAD DE ACCESO EN LA NUBE

- Proporciona descubrimiento y visibilidad de todas las aplicaciones en la nube que usan los usuarios, de forma autorizada o no autorizada.
- Solución CASB en línea y API "multimodo" maximiza la visibilidad y la protección.
- Protege los servicios en la nube como SalesForce, Office 365, Dropbox entre muchos otros, lo cual permite una adopción de la nube de forma segura.
- Protege contra malware y otras amenazas utilizando múltiples capas de seguridad y una poderosa combinación de tecnologías.
- Visibilidad completa, incluyendo inspección profunda de tráfico SSL.
- Un equipo especializado actualiza constantemente el catálogo de cientos de aplicaciones en la nube de Censornet, cubriendo miles de funciones y acciones.
- Las aplicaciones son evaluadas y clasificadas por Censornet, sin embargo, los administradores, tienen la capacidad de reclasificar las aplicaciones en la categoría que más se adecue a sus necesidades.
- Las políticas se pueden establecer a un nivel granular, ya sea por usuario, por la función de alguna aplicación, el tipo de dispositivo que se está utilizando, la red a la que está conectado, ubicación del usuario, entre otras características.
- Opciones de implementación flexibles: agente o proxy, o ambos.
- Agentes para Microsoft Windows y MAC OS X.
- 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, o usando el modo API.

El modo API también incluye la capacidad de escanear archivos al cargarlos y cambiarlos por contenido específico: usando plantillas DLP predefinidas, así como escaneando archivos en busca de malware. Las plantillas de políticas son incluidas para información de identificación personal, propiedad intelectual, información confidencial, riesgo interno, PCI DSS e HIPAA. Si es necesario, se pueden crear listas de palabras clave adicionales.

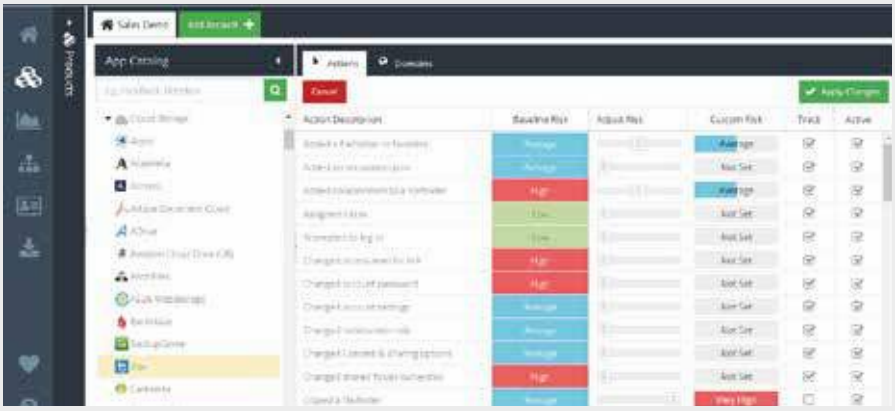
El módulo de análisis de imágenes busca contenido inapropiado al cargarlos en las aplicaciones, sustituye las imágenes con texto "No seguro para el trabajo".

El módulo Censornet API trabaja vinculado a las cuentas corporativas de almacenamiento en la nube (tales como OneDrive, Dripbox, etc.) sin la necesidad de uso de agentes, aun cuando los usuarios entren a las aplicaciones usando computadoras no pertenecientes a la empresa.

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

En el corazón del servicio CASB está el catálogo de aplicaciones en la nube de Censornet, que constantemente es actualizada, con detalle de miles de características (acciones) dentro de los cientos de aplicaciones en la nube.

Las aplicaciones se organizan en clases (por ejemplo, Cloud CRM, Cloud Storage, Social Media) o también se clasifican por riesgo (evaluado y calificado), las calificaciones predefinidas se pueden modificar fácilmente para reflejar el riesgo de una organización en particular.



CASB está completamente integrado a la suite Censornet, la plataforma proporciona datos detallados, visualización e informes a través de un amplio conjunto de atributos y criterios.

El análisis y los informes están disponibles por período, usuario, dispositivo, clase de aplicación, nombre de la aplicación, acciones de aplicación, palabras clave, nivel de riesgo y resultado (bloquear o permitir).

CARACTERÍSTICAS

Detección de aplicaciones en la nube	• Detecta el uso y actividad de aplicaciones en la nube por parte de los usuarios, incluidas las aplicaciones que utilizan un dominio personalizado creando un registro detallado para auditorias. • Las aplicaciones dentro del catálogo se evalúan y clasifican según el riesgo.
Control de aplicaciones en la nube	• Controle el acceso a las aplicaciones a nivel granular, seleccionando funciones y acciones permitidas, en cada aplicación. • Bloquee actividades genéricas en todas las aplicaciones (ej. carga de archivos, compartir archivo, etc.), clase de aplicación (CRM, redes sociales, almacenamiento de archivos) o aplicaciones específicas. • Puede aplicar condiciones para limitar el control por usuario, dispositivo, red, período de tiempo, nivel de riesgo o ubicación. • Bloquee acciones según el contenido, como la dirección de correo electrónico utilizada para iniciar sesión o las palabras clave dentro de las publicaciones en las redes sociales.
Anti-malware en tiempo real	• Incorpora varias capas de seguridad, cada una de las cuales utiliza una combinación potente y eficaz de herramientas técnicas, incluida la detección de amenazas en línea, la reputación y la heurística.
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.
Detección de proxy anónimo	• Impide el acceso a sitios proxy anónimos que permite burlar las soluciones de filtrado de contenido y control de aplicaciones.

ADMINISTRACIÓN

Motor de políticas	• Motor de políticas sofisticado que incluye atributos de Active Directory, dirección IP, direcciones MAC del dispositivo, tipo de dispositivo, etiqueta y/o ubicaciones.
Horario	• Las políticas pueden configurarse con horarios, de tal forma que serán activados o desactivados en forma automática.
Autenticación de usuario	• Se admiten varios métodos de autenticación, incluidos Active Directory Kerberos, inicio de sesión único, portal cautivo y RADIUS.
Sincronización de usuarios	• El servicio de sincronización de Active Directory garantiza que se repliquen los cambios en Active Directory.
Interfaz web	• Plataforma de administración 100% integrada con la suite 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. • Ver exactamente cuál de los usuarios están accediendo a qué aplicaciones y características dentro de esas aplicaciones.
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 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	• Vincule informes a programaciones y opcionalmente, solo reciba un informe cuando haya contenido (modo de alerta). Alerta sobre acciones de alto riesgo, palabras clave, actividad permitida, 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.
Múltiples vistas	• Analizar e informar por usuario, aplicación, dispositivo, característica/acción, nivel de amenaza y detalle (modo API).

DESPLIEGUE

Gateway (modo en línea)	• 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 en ubicaciones con una alta población de usuarios. También disponible en la nube.
Agentes (modo en línea)	• Los agentes para Microsoft Windows y MAC OS X aplican políticas directamente en los dispositivos, para usuarios dispersos en diferentes ubicaciones. A prueba de manipulaciones y fácil de implementar mediante un asistente de instalación o mediante la política de grupo de AD.
Modo API (offline)	• Puede hacer uso de la API para aplicaciones de almacenamiento nube empresariales. Vincule cuentas corporativas en aplicaciones compatibles y, opcionalmente, escaneé archivos en busca de contenido (escaneado DLP) y/o malware. • El módulo de análisis de imágenes examina los archivos en busca de contenido inapropiado "no seguro para el trabajo". • Las aplicaciones empresariales compatibles incluyen: Box, Dropbox, Google Drive, Microsoft OneDrive y SharePoint.
Modos de implementación	• Agente por software, proxy (establecido por política de grupo, WPAD o manualmente) o modo máquina virtual.
Soporte WPAD	• Creación automática de archivos para configuración 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.

+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