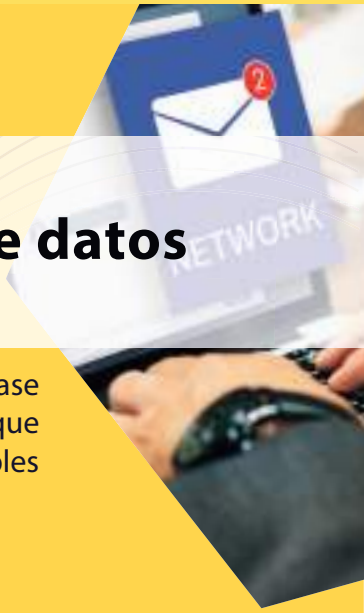
D.
DLP

Censornet Data Loss Prevention

www.cobranetworks.lat
Tel. +52 55 5599 0691
ventas@cobranetworks.lat



Prevención avanzada de pérdida de datos

Advanced DLP de Censornet proporciona prevención de pérdida de datos (DLP) de clase empresarial para correo electrónico, web y datos de aplicaciones en la nube, lo que permite el descubrimiento en tiempo real y el bloqueo de datos confidenciales o sensibles en tránsito.

DLP avanzado protege a las organizaciones contra la pérdida de datos asociada con el correo electrónico y el uso de aplicaciones en la nube, reduciendo riesgo y garantizar el cumplimiento de legislación y reglamentos, incluidos GDPR, con soporte para datos personales (Información de identificación personal) en 59 países y 38 idiomas.
Con Censornet la seguridad en la nube esta integrada de forma autónoma la plataforma con un único DLP central (motor de políticas). Las reglas DLP pueden identificar datos personales (PII), tarjeta de pago industria (PCI) y salud protegida tipos de datos de información (PHI) que utilizan las plantillas predefinidas listas para usar.
Censornet DLP es totalmente extensible, se pueden definir tipos de datos personalizados rápida y fácilmente para detectar datos que es de particular interés o exclusivo de un organización, como un proyecto sensible nombres en clave o palabras clave y frases relacionados con propiedad intelectual específica (IP).

Capa de protección crítica

Organizaciones de todos los tamaños y en todos los sectores se centran cada vez más en proteger mejor sus datos.
Si es GDPR, PCI DSS, HIPAA u otros legislación, regulaciones, externos, auditorías o políticas organizativas y evaluaciones internas: la protección de datos es crítico.
Simplemente permitiendo la carga de cualquiera presentar ante un tribunal aprobado o sancionado aplicación en la nube, como M365 (OneDrive, SharePoint) ya no está suficiente.

DLP AVANZADO

- Protección instantánea, solo habilíte las licencias complementarias para Censornet correo electrónico, web o nube seguridad de aplicaciones (CASB).
- Previene la pérdida de datos en el correo electrónico texto del mensaje (y archivos adjuntos) poniendo en cuarentena la salida correos electrónicos.
- Previene las fugas de datos asociadas con acciones de aplicaciones en la nube como "cargar".
- Cargar escáneres, aislar archivos y bloquear cargas en tiempo real donde los archivos contienen datos confidenciales y/o datos sensibles, que infringe la política de DLP
- Aplicar DLP uniforme en cualquier combinación de aplicaciones, usuarios, dispositivos y ubicaciones.

La capacidad de extraer, escanear archivos y contenido contra una política de DLP, impidiendo la acción si es confidencial o datos sensibles son identificados, son rápidamente siendo obligatorio incluso fuera industrias reguladas.
DLP avanzado permite un DLP Mosaico del escáner para seguridad del correo electrónico y extiende el mosaico "Escáner de contenido" para Web/CASB dentro del visual existente constructores de reglas de la plataforma Censornet.

Agregar DLP a las reglas de Censornet toma segundos.

Análisis y acciones exactas del contenido DLP se puede implementar sobre las existentes. reglas para proporcionar datos inmediatos centrados y evitar la pérdida de datos en tiempo real.

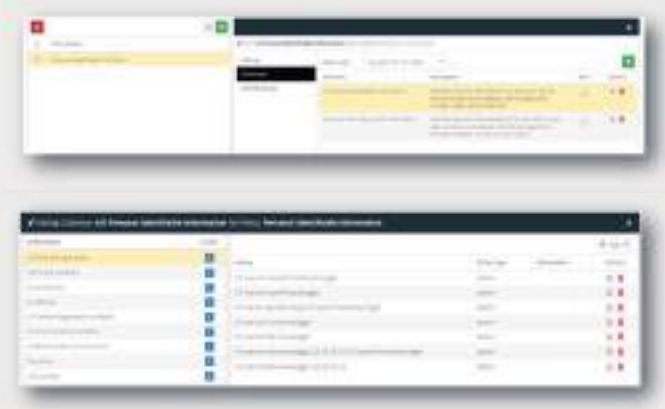
EL VALOR DE LA PREVENCIÓN DE PÉRDIDA DE DATOS

- Hasta el 94% de las empresas que experimentan una pérdida grave de datos y nunca se recuperan.
- El error humano se encuentra entre las tres causas principales de pérdida de datos y desempeña un papel en el 82% de las incumplimientos.
- El 72% de los empleados ha enviado accidentalmente información confidencial a la persona equivocada.

CARACTERÍSTICAS

Políticas, Gramáticas y Entidades (tipos de datos).

Las políticas de DLP se crean utilizando gramáticas (también conocidas como diccionarios). Las gramáticas contienen entidades (tipos de datos) que incluyen palabras clave, patrones (Reg Ex) y sinónimos.
Las preconfiguraciones listas para usar son extensas, proporcionar flexibilidad que se traduzca en políticas rápidas.
Las gramáticas se pueden combinar en reglas y políticas que utilizan lógica Y, O y NO. Una vez creadas, las políticas DLP se pueden utilizar en correo electrónico, web y reglas CASB en línea.
Para un mayor control, las puntuaciones de gravedad se pueden ajustar para tipos de datos que representan el mayor riesgo o exposición basado en atributos y actividades organizacionales.
Las políticas también se pueden aplicar a tipos de archivos específicos (predeterminado es todo).
Advanced DLP está totalmente integrado con Censornet la plataforma y el portal de administración proporcionan datos enriquecidos.
Visualiza informes a través de un amplio conjunto de atributos y criterios,



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 de datos en vuelo, o para una certificación más formal de cumplimiento con políticas internas o estándares externos, regulaciones y legislación, Advanced DLP proporcionará la evidencia
necesario.

ADMINISTRACIÓN

Motor de políticas	• Datos personales (PII) – Reino Unido – inc. nombres, pasaporte y números NI • Datos personales (PII) – EE. UU. – inc. nombres, pasaporte y números de seguro social • Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) • Información de salud personal (PHI) – inc. condiciones médicas, procedimientos y drogas • Credenciales API: información clave y de credenciales para servicios web comunes • Direcciones de computadoras – inc. HTTP, FTP, IP (v4/v6) MAC y direcciones de archivos • Blasfemias – inc. términos sociales, homofóbicos y sexualmente ofensivos
Configuración de políticas	• Seleccione si la política debe aplicarse a "Todos los productos", "Seguridad del correo electrónico", "Seguridad web". Seguridad / CASB en línea • Coincidencia entre mayúsculas y minúsculas/no distingue entre mayúsculas y minúsculas, configuración regional (tokenización de chino, japonés, coreano y tailandés), incluyen caracteres de puntuación. • Niveles de gravedad: bajo, medio, alto y crítico. Cada Gramática es evaluada y devuelve una puntuación normalizada (0-100); los valores predeterminados se pueden modificar si es necesario
Gramáticas	• Las gramáticas son diccionarios que definen qué tipos de datos (Entidades) se detectan. • Las gramáticas contienen entidades en varios idiomas y formatos regionales. • Todas las gramáticas son extensibles. • Se pueden combinar varias gramáticas usando la lógica AND, OR y NOT
Personalización de gramática	• Eliminar entidades • Agregar/cambiar entidades – basado en patrones/expresiones regulares inc. Sinónimos

CARACTERÍSTICAS

Tipos de archivo	• Las políticas se aplican a todo el contenido de forma predeterminada. • Las políticas se pueden limitar a tipos de archivos específicos, por extensión y tipo MIME.
Categorías gramaticales	• Dirección: direcciones físicas, código postal, código postal • Credenciales API – inc. AWS, Facebook, LinkedIn, Twitter • Matrícula de automóvil: registros de vehículos en múltiples formatos regionales • Empresas – empresas importantes en diferentes países • Computadora: dirección IP (v4/v6), HTTP, FTP, dirección MAC y dirección de archivo • Fecha/Hora – en diferentes formatos regionales • Licencia de conducir: números de licencia de conducir en diferentes formatos regionales • Títulos de Trabajo – títulos de trabajo incluyendo abreviaturas inc. títulos de gobierno y gabinete • Médico: nombres de enfermedades, términos médicos, medicamentos (comerciales y genéricos). nombres) • Pasaporte: números de pasaporte en diferentes formatos regionales • PCI: números de tarjetas de crédito (PAN), números de cuentas bancarias, códigos de clasificación, IBAN/ RÁPIDO • Números de teléfono (requiere caracteres tangibles como '+' y '(' • PII: edad, nacionalidad, origen étnico, direcciones de correo electrónico, NI/números de Seguro Social, identificación médica, nombre y apellido de la persona, saludos • Lugares: identifica asentamientos en diferentes países inc. tamaño de la poblacion • Blasfemias: blasfemas, homofóbicas, despectivas raciales, sexuales, biológicas o palabras censuradas para diferentes regiones y países

DESPLIEGUE

Seguridad del correo electrónico	• Se requiere una licencia adicional de DLP avanzado para Email Security
CASB en línea y web	• Se requiere una licencia adicional de DLP avanzada para CASB y Web
Modo API CASB	• Próximamente DLP avanzado para el modo CASB API • Las aplicaciones compatibles incluyen Box, Dropbox, Google Drive, Microsoft OneDrive y compartirpunto • Permite el escaneo DLP de todos los datos en reposo (Administración de la postura de seguridad de los datos)

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