LIBRO ELECTRÓNICO

Proteger sus datos en un mundo de trabajo desde cualquier lugar

Mantenga sus datos fundamentales para la empresa a salvo con Zscaler Data Protection

Índice

Proteger sus datos es ahora más difícil que nunca

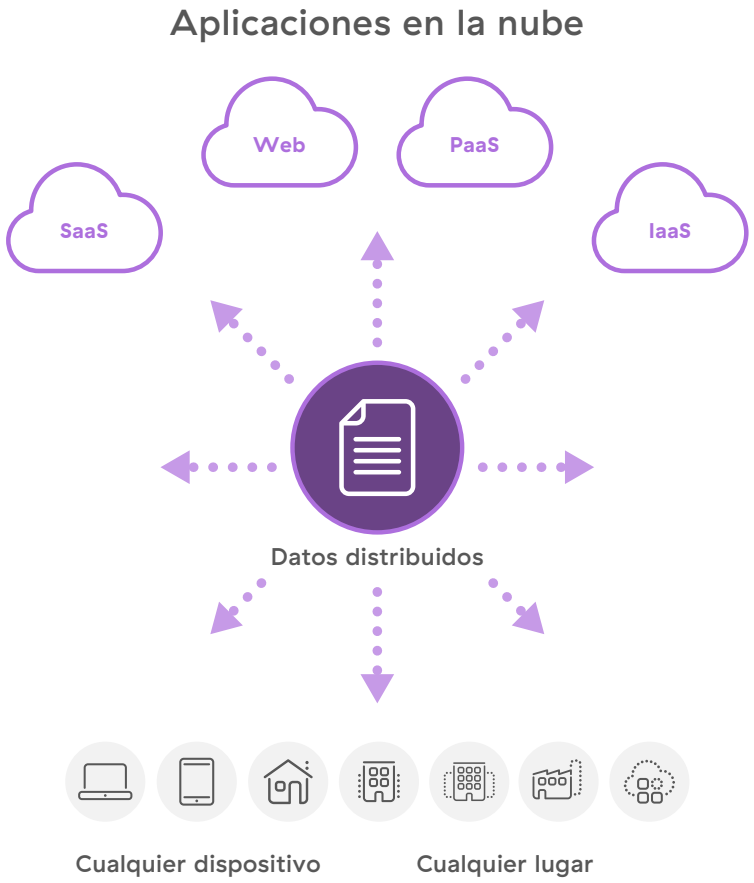
Con las aplicaciones en la nube, sus datos están ampliamente diseminados y sus empleados se conectan desde el lugar en el que trabajen, que puede estar en cualquier parte. Los enfoques tradicionales de protección de datos no pueden ofrecerle un control adecuado sobre sus datos. He aquí los motivos:

No se puede seguir a los usuarios
No puede ofrecer una protección de datos adecuada porque el acceso a sus aplicaciones se produce en la nube a través de Internet, lejos de su red y de los controles de datos.

Se desconoce el estado de cumplimiento
Hacer el correcto seguimiento del estado de su cumplimiento se ha vuelto difícil porque sus aplicaciones en la nube están dispersas en múltiples ubicaciones y grupos.

Inspección TLS/SSL limitada
La mayoría del tráfico está cifrado, pero debido a que los enfoques tradicionales de protección de datos no pueden inspeccionar el tráfico SSL/TLS a escala, usted no ve los riesgos potenciales.

Falta el panorama general
Los productos puntuales y los enfoques adicionales crean complejidad y evitan la visión unificada que necesita para comprender la exposición.



Solución Zscaler

Recupere el control de todos sus datos con Zscaler

Zscaler Data Protection puede ayudarle a lograr una protección de datos incomparable, ya que se basa en estos principios fundamentales:

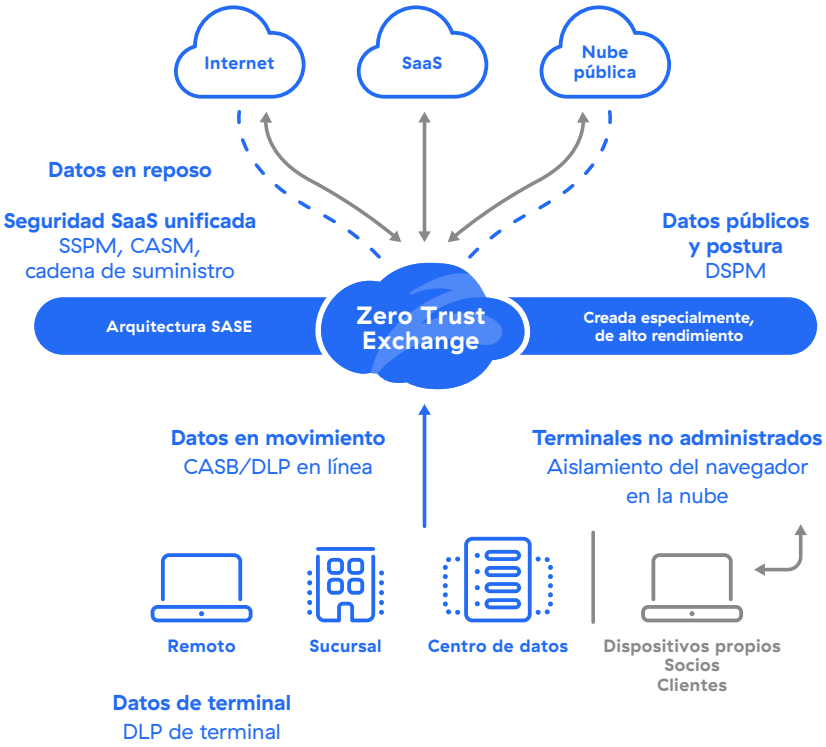
Arquitectura SASE desarrollada con un fin determinado
Ofrezca protección en tiempo real a todos los usuarios desde una nube en línea de alto rendimiento distribuida en 150 centros de datos globales.

Inspección SSL a escala
Inspeccione todo el tráfico SSL para comprobar la exposición de datos con una capacidad de inspección ilimitada por usuario.

Visibilidad del cumplimiento
Mantenga fácilmente el cumplimiento normativo analizando su SaaS, Microsoft 365 y las nubes públicas en busca de infracciones y configuraciones incorrectas.

Una plataforma, una política, visibilidad total
Proteja todos sus canales de datos en la nube (datos en movimiento, en reposo y en terminales y nubes) con una plataforma simple y unificada.

Zscaler Data Protection: visión general de la solución



Gestione de forma segura las aplicaciones sancionadas con CASB fuera de banda

Sus aplicaciones en la nube pueden favorecer una mejor colaboración, especialmente ahora que muchos empleados trabajan a distancia, pero que también pueden exponer sus datos. A menudo, los empleados hacen un mal uso involuntario de estas aplicaciones, lo que puede dar lugar a actividades maliciosas.

Cómo puede proteger sus aplicaciones y datos en la nube con CASB fuera de banda de Zscaler:

- **Proteja los datos expuestos en reposo**
  Identifique datos críticos en aplicaciones en la nube, correo electrónico y uso compartido de archivos. Haga cumplir las políticas de DLP para controlar el acceso y la exposición.

- **Evite el intercambio indebido de datos**
  Aplique políticas granulares sobre los datos confidenciales en reposo para garantizar que no se compartan fuera de la organización.

- **Corrección de amenazas**
  Analice depósitos de datos en los servicios de alojamiento de archivos, como OneDrive o Box, para encontrar y poner en cuarentena rápidamente el contenido malicioso.

- **Simplifique la protección de datos**
  Evite la complejidad de productos específicos con una plataforma unificada que ofrece una política de datos y amenazas en todos los datos en movimiento y en reposo.

Ofrezca visibilidad y el control en tiempo real con CASB en línea

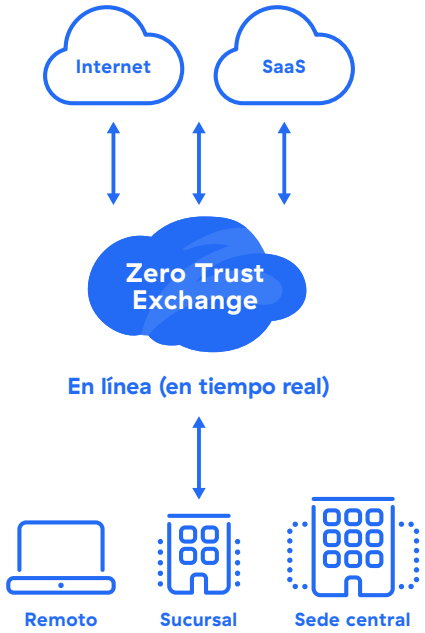
Aunque el CASB fuera de banda ayuda a proteger los datos en reposo, sigue siendo necesario el control en tiempo real de las aplicaciones en la nube. ¿Cómo permite el CASB en línea pasar a la nube de forma segura?

- **Reduce el riesgo de TI en la sombra**
  Comprenda rápidamente qué aplicaciones en la nube seguras o inseguras se están utilizando en toda la organización.

Ejemplo: bloquee la actividad de las aplicaciones de riesgo que acceden a sus datos, como los convertidores de PDF en línea o los sitios de intercambio de archivos.

- **Hace cumplir las aplicaciones aprobadas oficialmente**
  Limite la actividad del usuario a las aplicaciones en la nube aprobadas por TI y la organización.

Ejemplo: mejore el uso compartido y la productividad de Microsoft 365 permitiendo únicamente OneDrive y bloqueando Box.



Trabajo desde cualquier lugar

- **Previene la pérdida de datos con controles de tipo de archivo**
  Restrinja la transferencia de datos por tipo de archivo con bloqueo condicional y alertas.

Ejemplo: impida que usuarios o grupos carguen o descarguen archivos de Word, Excel o PowerPoint.

- **Aplicación de restricciones de arrendamiento**
  Controle los flujos de datos al permitir sólo instancias específicas de aplicaciones en la nube.

Ejemplo: Evite la fuga de datos a instancias personales de Microsoft 365 permitiendo únicamente el acceso a Microsoft 365 para empresas.

DLP de punto final

Simplifique la forma de controlar los datos del dispositivo con Endpoint DLP

Una excelente protección de datos requiere una estrategia de terminales. Con Endpoint DLP obtiene protección total del dispositivo, sin la complejidad de los enfoques tradicionales.

- **Política y visibilidad unificadas**
  Con un motor DLP centralizado, obtiene alertas consistentes en terminales, en línea y en la nube.
- **Agente único ligero**
  Integrado en el agente existente de Zscaler, obtiene una mejor experiencia de usuario al reducir los agentes necesarios en su terminal.
- **Implementación rápida**
  Aproveche sus políticas Zscaler DLP existentes para comenzar a funcionar rápidamente.
- **Gestión de incidentes más rápida**
  Responda a los incidentes más rápidamente con automatización del flujo de trabajo, y paneles y análisis forenses detallados

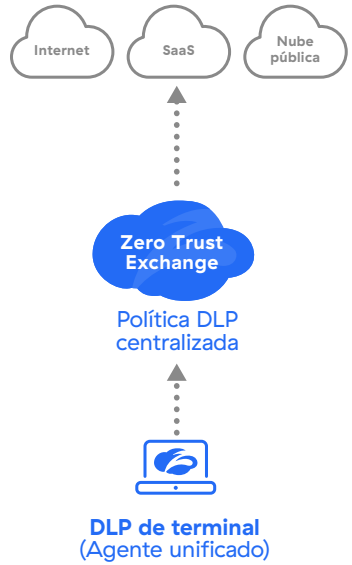
Principales casos de uso de Endpoint DLP

Mejore la cobertura de datos
Garantice que los datos valiosos se rastreen y protejan adecuadamente en todas partes, sin espacios vacíos

Renuncias seguras de los empleados
Asegúrese de que los empleados que dejan la empresa no copien los datos del dispositivo y los lleven a su próxima empresa.

Retire DLP de terminales heredados
Deshágase de productos puntuales complicados y ofrezca una plataforma unificada

Mejore el cumplimiento
Mantenga el cumplimiento normativo en todos los archivos y dispositivos



Canales protegidos

Dispositivos extraíbles	Sincronización de almacenamiento personal en la nube
Datos compartidos en red	Impresión

Reduzca la complejidad con un enfoque unificado para DLP de correo electrónico en tiempo real

Uno de los mayores riesgos para los datos es el correo electrónico. Con DLP de correo electrónico de Zscaler, las organizaciones obtienen un enfoque potente para agregar control DLP total sobre los datos del correo electrónico.

Los enfoques heredados para proteger los datos del correo electrónico pueden ser engorrosos y complejos. Con la adopción de SSE, los equipos de TI buscan enfoques unificados para proteger los datos en los canales de correo electrónico que reduzcan la complejidad.

Con DLP de correo electrónico de Zscaler aprovechando Smarthost, la protección de datos se puede escalar fácilmente al correo electrónico en tiempo real. Al utilizar SMTP relay, Zscaler permite una integración sin esfuerzo en las arquitecturas de correo electrónico existentes, con control total sobre los datos y archivos adjuntos del correo electrónico.

Ventajas del DLP de correo electrónico de Zscaler:

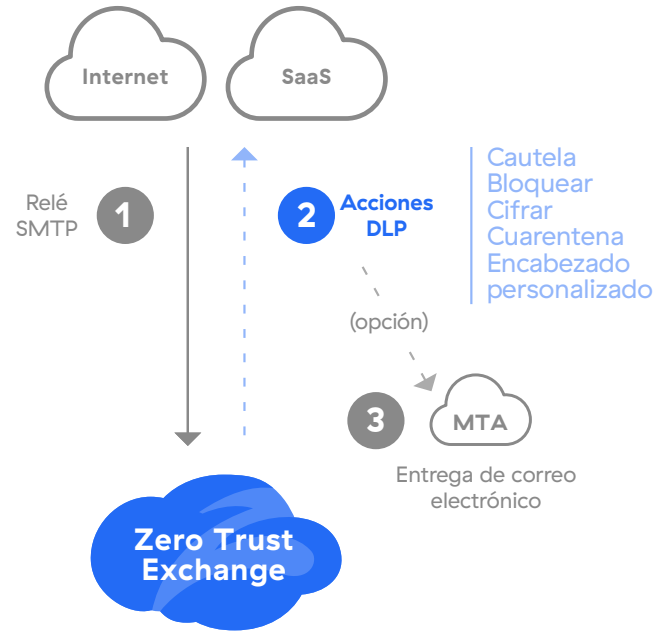
Independiente del protocolo
Funciona en dispositivos administrados, no administrados e incluso móviles

Fácil implementación
No se requieren cambios en los registros MX

Política flexible
Definiciones de políticas ajustables y evaluaciones granulares de políticas

Motores DLP y UI única
centralizados y unificados para todos los canales

DLP de correo electrónico en tiempo real



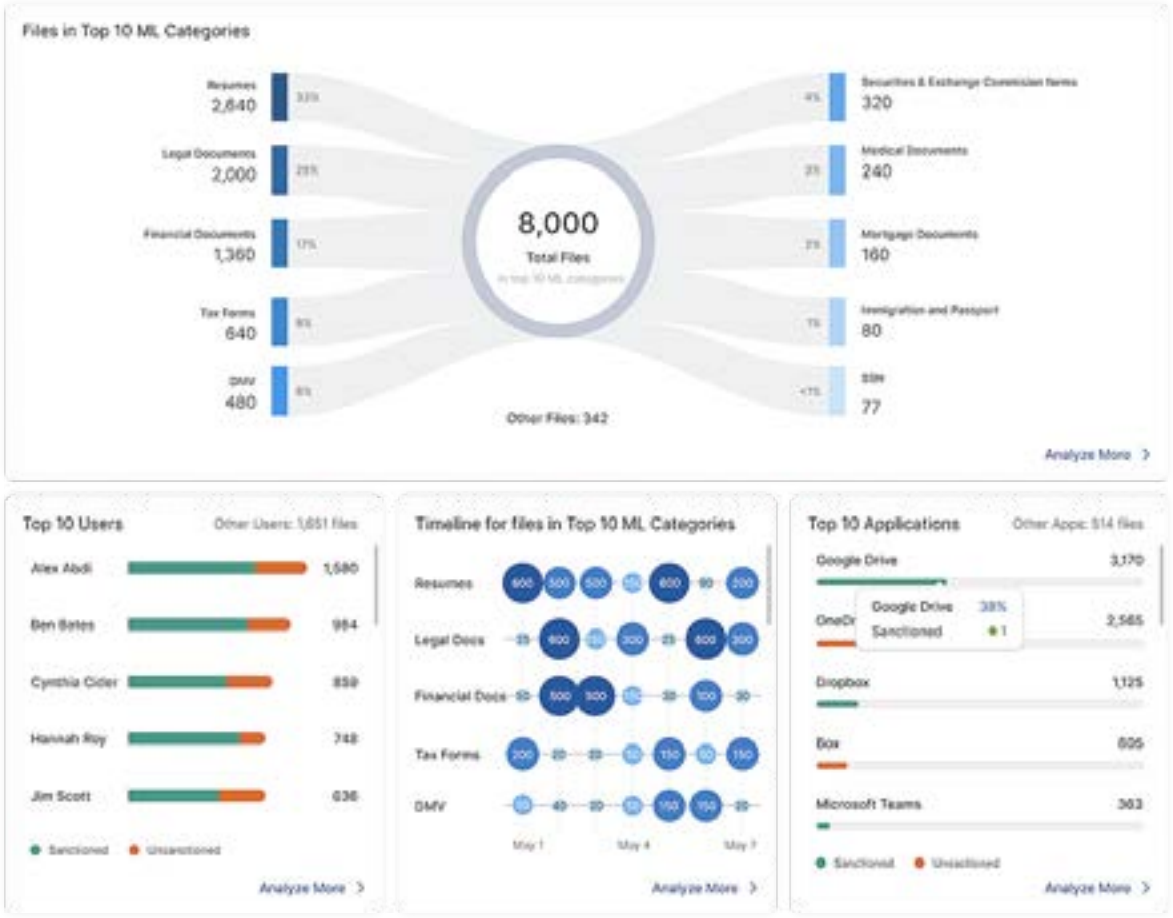
Detección automática de datos impulsado por IA

Encuentre y proteja datos al instante con la detección de datos impulsada por IA

En ocasiones, implementar y poner en funcionamiento un programa de protección de datos puede llevar meses. Con el innovador descubrimiento de datos de Zscaler, puede comprender rápidamente el riesgo y los comportamientos asociados con sus datos.

Detección de datos con IA:

- Descubra datos en terminales, nubes públicas y en línea
- Comprenda rápidamente los riesgos de pérdida por parte de usuarios y aplicaciones
- Pase a la creación de políticas con unos pocos clics



Clasifique y proteja datos, formularios e imágenes personalizados frente a pérdidas

La clasificación de datos es el núcleo de cualquier buen programa DLP. Con la clasificación de datos avanzada, las organizaciones pueden proteger tipos especiales de datos confidenciales frente a pérdidas.

Coincidencia exacta de datos (EDM)

Tome huellas digitales y proteja datos empresariales personalizados. Ejemplo: active los números de tarjetas de crédito de los clientes, no todos los números de tarjetas de crédito (como los de una compra en Amazon).

Coincidencia de documentos indexados (IDM)

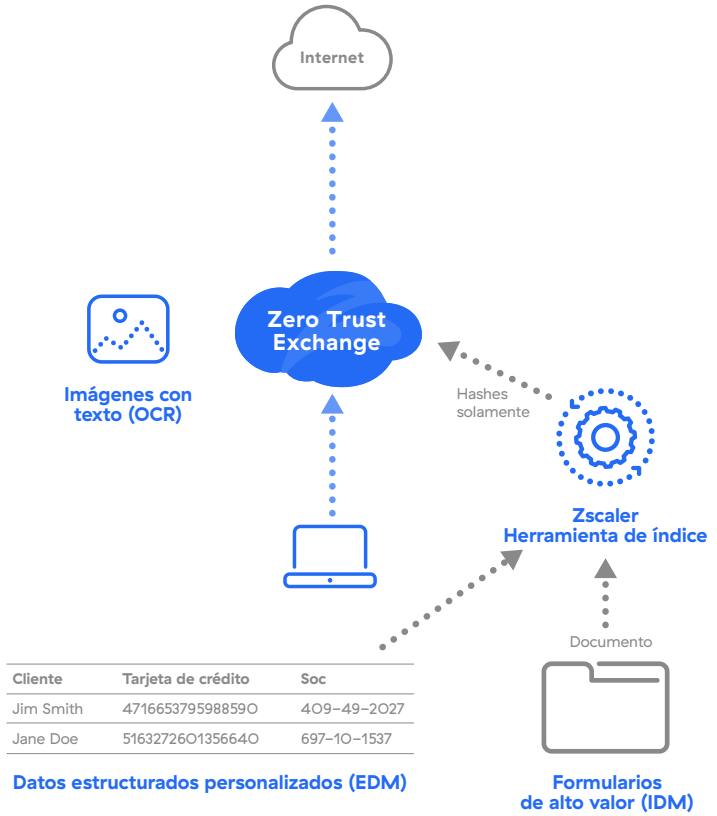
Tome huellas digitales y proteja documentos y formularios personalizados. Ejemplo: tome las huellas digitales de un formulario de impuestos o hipoteca en blanco y bloquee cualquier otra copia completa.

Reconocimiento óptico de caracteres (OCR)

Encuentre y evite la pérdida de datos identificando el texto dentro de las imágenes. Ejemplo: supervise las capturas de pantalla que puedan contener contenido confidencial.

Herramienta de indexación de Zscaler

Herramienta complementaria de huellas dactilares para EDM e IDM. Crea hashes de datos de EDM e IDM, y los carga en Zscaler Cloud para la creación de políticas.



Obtenga máxima visibilidad y control sobre las aplicaciones de IA generativa

Controlar la pérdida de datos confidenciales en aplicaciones de IA generativa es clave para permitir que estas aplicaciones en la sombra sean productivas. El nuevo enfoque innovador de Zsclaer reúne toda la protección y visibilidad en un solo lugar

Las aplicaciones de IA generativa tienen el potencial de mejorar la productividad en toda su organización, pero necesita visibilidad y control completos sobre estas aplicaciones para tomar mejores decisiones de bloqueo.

La innovadora seguridad de la IA generativa de Zscaler permite a los equipos de TI descubrir todas las aplicaciones de IA generativa en toda la organización y ofrece una visibilidad sin precedentes que incluye entradas de nivel rápidas, todo para que se puedan tomar mejores decisiones de bloqueo.

Ventajas

- Consulte las indicaciones de entrada enviadas por los usuarios a la aplicación IA para obtener una visibilidad contextual completa
- Controles de políticas flexibles en la inspección DLP y el control de aplicaciones en la nube
- Aplique el acceso aislado y proteja los datos en el navegador en la nube de Zscaler.

Visibilidad de la IA generativa

Descubrimiento de IA en la sombra
Catálogo completo de aplicaciones de IA populares

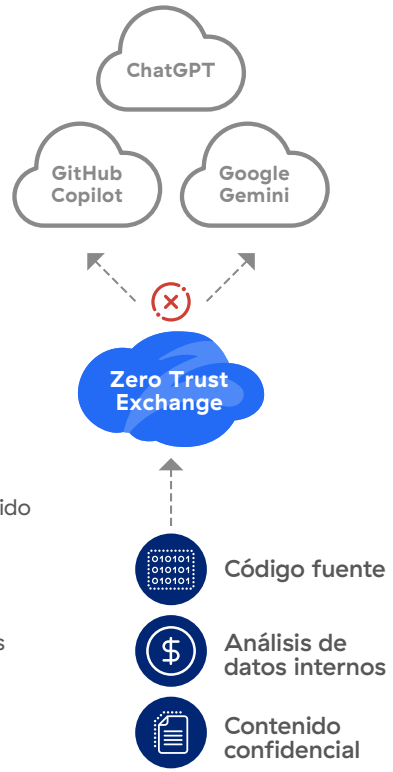
Visibilidad de la solicitud de entrada
Vea los mensajes de entrada reales que los usuarios envían a las aplicaciones de IA

Controles de aplicaciones de IA generativa

Inspección DLP
Bloquee los datos confidenciales y el contenido que se dirige a las aplicaciones de IA

Control de aplicaciones en la nube
Controle el acceso a las aplicaciones de IA entre usuarios, departamentos y ubicaciones

Aislamiento del navegador
Limite el uso de datos y aplicaciones en un navegador seguro en la nube



Defienda su plataforma SaaS con un enfoque completamente integrado

Proteger las nubes y los datos SaaS requiere demasiadas herramientas. Unificar SSPM con otros enfoques clave de seguridad de SaaS ayuda enormemente a simplificar la forma en que los equipos de TI protegen los datos y la postura de SaaS.

Muchas vulneraciones de la nube son causadas por configuraciones incorrectas peligrosas o aplicaciones de terceros conectadas a plataformas SaaS. Comprender y controlar su postura SaaS es un paso importante para proteger las grandes cantidades de datos confidenciales en estas nubes.

Con SaaS Security Posture Management (SSPM) de Zscaler, las organizaciones obtienen un enfoque unificado para analizar y proteger plataformas SaaS como Office 365 o Google. Obtenga visibilidad detallada de las integraciones de aplicaciones y configuraciones erróneas peligrosas, con corrección automática, orientación y control sobre la revocación de aplicaciones conectadas de riesgo.

Gestión de la postura de seguridad de los datos (DSPM)

Proteja los datos y las nubes públicas con un enfoque de protección de datos totalmente integrado

Los equipos de protección de datos necesitan un enfoque unificado para proteger los datos de las nubes públicas. Zscaler DSPM se integra perfectamente en los programas de protección de datos existentes.

Los datos confidenciales almacenados en nubes públicas como AWS y Azure pueden ser muy dinámicos. Desde privilegios y vulnerabilidades excesivos hasta datos ocultos, los equipos de TI necesitan una mejor manera de detectar, clasificar y proteger los datos de la nube pública.

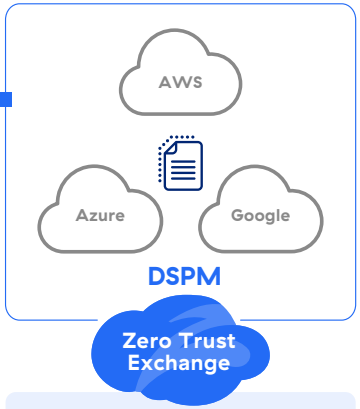
Zscaler DSPM descubre rápidamente datos confidenciales, comprende los riesgos y controla el acceso y la postura. Lo mejor de todo es que el DSPM integrado de Zscaler aprovecha el mismo motor DLP que todos los demás canales (terminal, red, SaaS), por lo que las alertas son uniformes, sin importar a dónde se muevan sus datos.

Ventajas

- Encuentre rápidamente datos confidenciales con la detección automática impulsado por IA
- Correlacione configuraciones erróneas, exposición y vulnerabilidades para comprender mejor el riesgo de los datos en la nube
- Amplíe los diccionarios DLP existentes a los datos de la nube pública para mejorar la visibilidad y el contexto
- Cierre rápidamente los riesgos con orientación práctica sobre corrección

Proteja los datos y la postura en la nube
Encuentre y proteja los datos y comprenda completamente los riesgos de exposición

1. **Haga un mapa de almacenes de datos**
   Asigne cubos, máquinas virtuales y bases de datos con detección automática de datos
2. **Priorice el riesgo**
   Comprenda las configuraciones incorrectas y el riesgo de exposición a los datos
3. **Remedie los riesgos**
   Tome medidas con guía y políticas de corrección



DLP centralizado:
Defina una vez, implemente en todas partes

Datos seguros de aplicaciones web y acceso para dispositivos propios del usuario

En ocasiones, los socios, contratistas o empleados requieren acceso a sus datos mientras utilizan sus dispositivos personales. ¿Cómo mantener el control sobre estos datos cuando estos dispositivos no están administrados?

Con Zscaler User Portal 2.0 y Browser Isolation, las organizaciones pueden trabajar de forma segura dispositivos no administrados. Veamos cómo:

Cómo protege User Portal 2.0 las evaluaciones y los datos:

- Los usuarios, sin requisitos de agente de terminal, se autentican en el portal para obtener una vista del panel de las aplicaciones web autorizadas (SaaS o privadas).
- Los usuarios acceden a la aplicación dentro de un navegador contenido/aislado. Luego, los datos se transmiten de forma segura al terminal en forma de píxeles.
- Las aplicaciones son completamente interactivas; sin embargo, las funciones de cortar, pegar, descargar e imprimir están bloqueadas, y las capturas de pantalla incluso tienen marcas de agua.

Ventajas del uso de dispositivos propios de los usuarios:

Protección de datos y amenazas

Inspeccione todo el tráfico en línea, garantizando el mismo nivel de seguridad que los dispositivos administrados.

Aislamiento de datos y archivos

Vea documentos o comparta archivos (entre aplicaciones), sin capacidad de descarga ni portapapeles en el punto final.

Políticas DLP integradas

Aproveche las políticas comerciales para garantizar una protección y alertas uniformes de datos confidenciales.

Gestione mejor los incidentes de pérdida de datos con automatización del flujo de trabajo

Para llevar su programa de protección de datos al siguiente nivel, necesita una potente herramienta de gestión de incidentes que agilice las operaciones y permita el entrenamiento de los usuarios.

Muchos programas de protección tienen problemas debido a incidentes y herramientas inconexos. Además, los usuarios nunca llegan a saber qué comportamientos de riesgo tuvieron al manejar datos incorrectamente.

Zscaler Workflow Automation ofrece una herramienta dedicada para que los administradores de DLP potencien la gestión de incidentes.

Con todos los análisis forenses en un solo lugar, los administradores pueden comprender rápidamente los comportamientos de riesgo, asignar incidentes a los usuarios para su justificación e implementar rápidamente acciones de políticas para resolver incidentes.

Cómo ayuda la automatización del flujo de trabajo a su programa de protección de datos

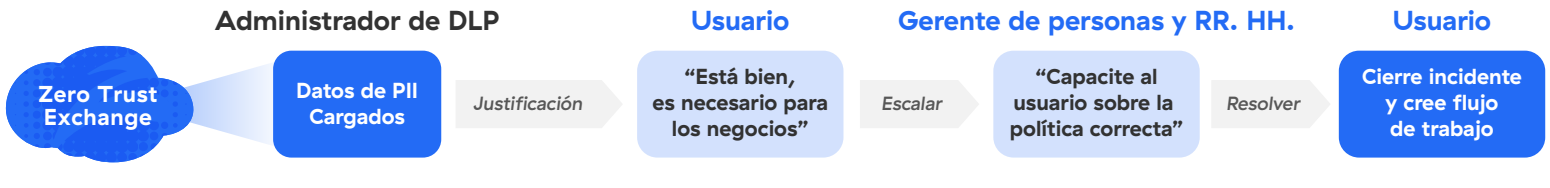
Gestión de incidentes más rápida
Ahorre tiempo con una plataforma diseñada específicamente para la gestión de incidentes de pérdida de datos

Rutinas automatizadas
Optimice las operaciones diarias mediante el uso de flujos de trabajo para automatizar tareas repetitivas y escaladas

Formación de usuarios
Justifique incidentes con usuarios a través de Slack, Teams o correo electrónico, mientras proporciona información sobre las mejores prácticas de protección de datos

Totalmente integrado
Evite fallos comunes en el programa de protección brindando un sistema integral de gestión de incidentes

Flujos de trabajo potentes
Gestione incidencias, eduque a los usuarios y automatice los flujos de trabajo



Resumen

Máxima protección, mínimo esfuerzo

La protección de datos de Zscaler sigue a sus usuarios y las aplicaciones a las que acceden para proteger sus datos en la nube y en el mundo móvil. Zscaler Zero Trust Exchange™ es una plataforma diseñada específicamente que ofrece la protección y la visibilidad que necesita para simplificar el cumplimiento y hacer que la protección de datos sea sencilla.

Zero Trust Exchange:

- **Proporciona protección idéntica** para que pueda ofrecer una política de protección de datos uniforme para todos los usuarios, independientemente de su conexión o ubicación.
- **Inspecciona todo su tráfico TLS/SSL** para eliminar puntos ciegos, todo respaldado por los mejores SLA del sector.
- **Simplifica el cumplimiento** para que pueda encontrar y controlar datos PCI, PII y PHI con facilidad mientras mejora su capacidad para mantener los requisitos de cumplimiento.
- **Elimina la complejidad** con una plataforma unificada que le permite proteger todos sus canales de datos en la nube: datos en movimiento, en reposo y en terminales y nubes.

Obtenga una protección de datos diseñada para un mundo móvil que prioriza la nube

Sus datos ya no residen en el centro de datos. Está en todas partes y pueden acceder a ellos los empleados que trabajan desde fuera de la oficina y prácticamente desde cualquier lugar. Sus enfoques de seguridad actuales no pueden proteger los datos en un mundo móvil y en la nube. Con los servicios de protección de datos de Zscaler, puede proporcionar una protección idéntica para sus datos críticos independientemente de dónde se conecten los usuarios o dónde se alojen las aplicaciones. **Permítanos mostrarle cómo.**

Vea historias de éxito de clientes sobre Zscaler Data Protection >

Obtenga el libro electrónico

Obtenga más información sobre la plataforma Zscaler Data Protection >

Visítenos en línea

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com/es