EBOOK

Proteger sus datos en un mundo de trabajo desde cualquier lugar

Mantenga segura su información crítica con Zscaler Data Protection

Contenido

Proteger sus datos es más difícil que nunca

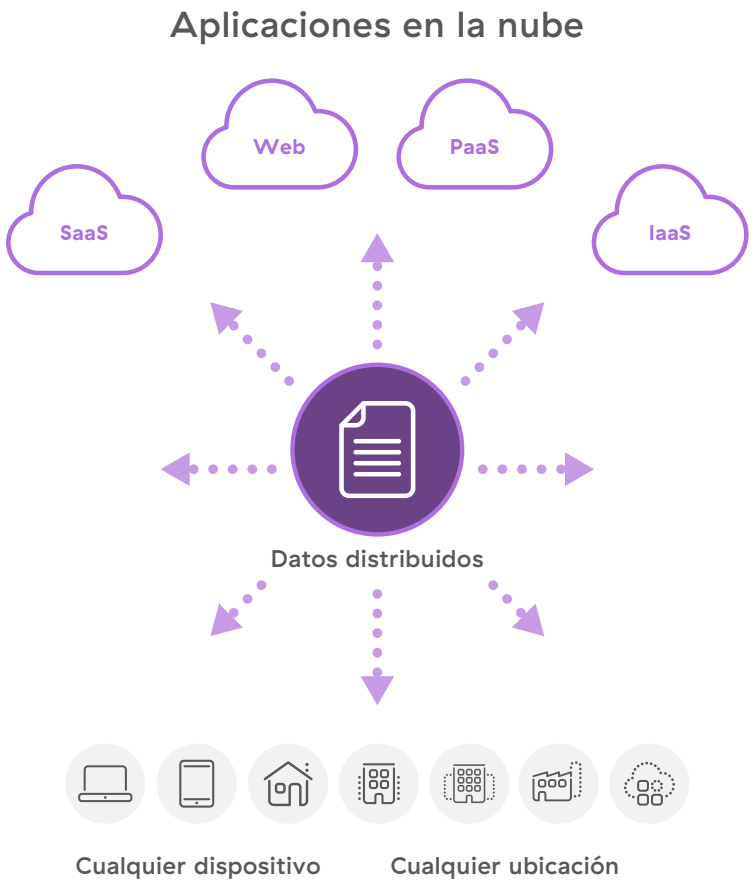
Con las aplicaciones en la nube, sus datos ahora están ampliamente distribuidos y sus empleados se conectan desde dondequiera que estén trabajando, que podría ser cualquier lugar. Los enfoques tradicionales de protección de datos no pueden brindarle un control adecuado sobre sus datos. Y he aquí el por qué:

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

El estado de cumplimiento es desconocido
Comprender el estado de cumplimiento se ha vuelto difícil porque sus aplicaciones en la nube están distribuidas en múltiples ubicaciones y grupos.

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

Pierde la visión de conjunto
Los productos puntuales y los enfoques complementarios crean complejidad e impiden 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 al cumplir con estos principios básicos:

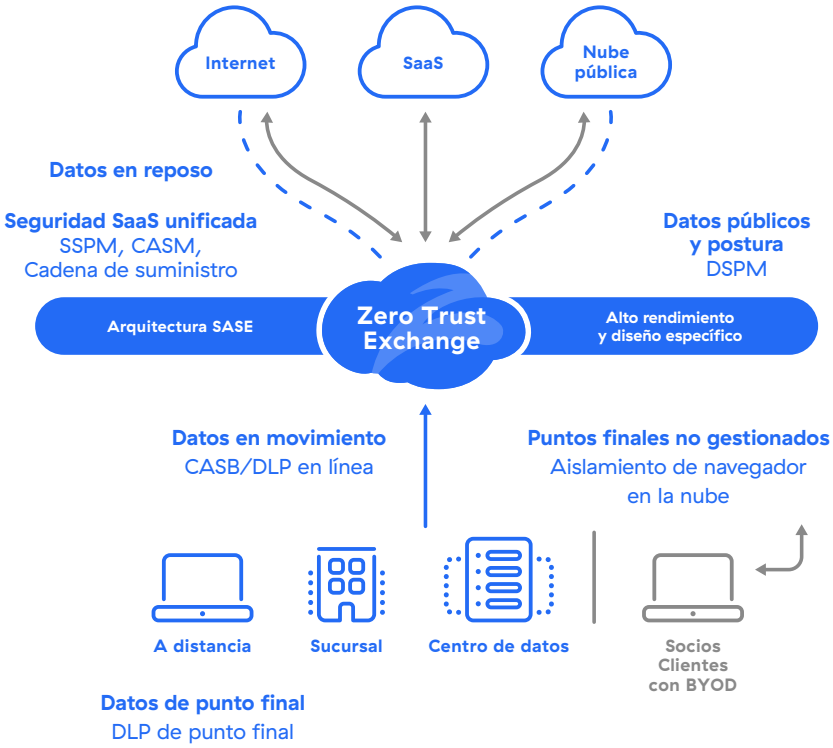
Arquitectura SASE diseñada específicamente
Ofrezca protección en tiempo real a todos los usuarios desde una nube en línea de alto rendimiento distribuida en 150 centros de datos globales.

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

Visibilidad del cumplimiento
Mantenga fácilmente el cumplimiento escaneando su SaaS, Microsoft 365 y las nubes públicas en busca de violaciones 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: Descripción general de la solución



Gobierne de manera segura aplicaciones autorizadas con CASB fuera de banda

Sus aplicaciones en la nube pueden permitir una mejor colaboración, especialmente con muchos empleados que trabajan de manera remota, pero también pueden exponer sus datos. Los empleados a menudo 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 los datos críticos en aplicaciones en la nube, correo electrónico y archivos compartidos. Aplique las políticas de DLP para controlar el acceso y la exposición.

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

- **Remedie amenazas**
  Escanee repositorios de datos en servicios de alojamiento de archivos, como OneDrive o Box, para encontrar y poner en cuarentena rápidamente contenido malicioso.

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

Ofrezca visibilidad y control en tiempo real con CASB en línea

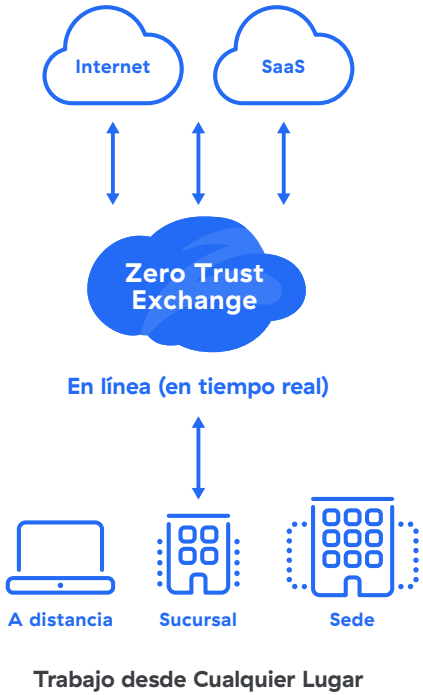
Si bien CASB fuera de banda ayuda a proteger los datos en reposo, aún necesita control en tiempo real sobre sus aplicaciones en la nube. ¿Cómo le permite CASB en línea migrar de manera segura a la nube?

- **Reduce el riesgo de Shadow IT**
  Comprenda rápidamente qué aplicaciones en la nube seguras o no seguras se utilizan en toda la organización.

Ejemplo: Bloquee la actividad de aplicaciones riesgosas que acceden a sus datos, como convertidores de PDF en línea o sitios para compartir archivos.

- **Hace cumplir las aplicaciones autorizadas oficialmente**
  Limita 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 solo OneDrive mientras bloquea Box.



Trabajo desde Cualquier Lugar

- **Evita 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 la carga o descarga de archivos de Word, Excel o PowerPoint por usuario o grupos.

- **Aplica restricciones de usuarios**
  Controle los flujos de datos permitiendo solo instancias específicas de aplicaciones en la nube.

Ejemplo: Evite la fuga de datos en instancias personales de Microsoft 365 permitiendo solo el acceso a Microsoft 365 para Empresas.

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

Una gran protección de los datos requiere una estrategia para los puntos finales. Con Endpoint DLP obtendrá una protección total de los dispositivos, sin la complejidad de los enfoques tradicionales.

- **Política y visibilidad unificadas**
  Con un motor DLP centralizado, obtiene alertas uniformes en puntos finales, en línea y en la nube.
- **Agente único y ligero**
  Integrado en el agente Zscaler, obtendrá una mejor experiencia de usuario al reducir los agentes necesarios en su punto final.
- **Implementación rápida**
  Aproveche sus políticas DLP de Zscaler existentes para ponerse en marcha rápidamente.
- **Gestión de incidentes más rápida**
  Responda a los incidentes más rápido con automatización de flujos de trabajo y paneles y análisis forenses detallados.

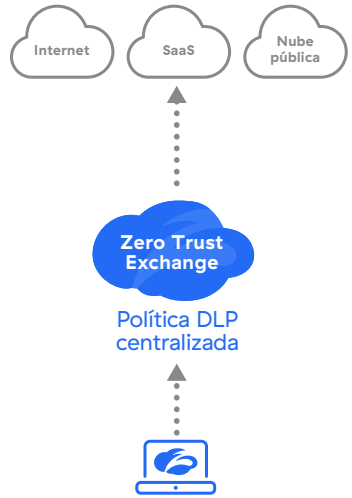
Principales casos de uso de Endpoint DLP

Mejore la cobertura de los datos
Asegúrese de que los datos valiosos se rastrean y protegen adecuadamente en todas partes, sin brechas

Protéjase de las renuncias de los empleados
Asegúrese de que los empleados que se marchan no copien los datos de los dispositivos y se los lleven a su nueva empresa

Retire la DLP de puntos finales heredada
Deshágase de los complicados productos puntuales y ofrezca una plataforma unificada

Mejore el cumplimiento de la normativa
Mantenga el cumplimiento de la normativa en todos los archivos y dispositivos



Canales protegidos

- Medios extraíbles
- Sincronización de almacenamiento personal en la nube
- Recursos compartidos en red
- Impresión

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

Uno de los mayores riesgos para los datos es el correo electrónico. Con Email DLP de Zscaler las organizaciones obtienen un potente enfoque para aplicar un control de DLP total sobre los datos de 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 Email DLP de Zscaler que utiliza Smarthost, la protección de datos se puede escalar fácilmente al correo electrónico en tiempo real. Utilizando el relé SMTP, Zscaler permite una integración sin esfuerzo en las arquitecturas de correo electrónico existentes, con un control total sobre los datos y archivos adjuntos del correo electrónico.

Ventajas de Email DLP de Zscaler:

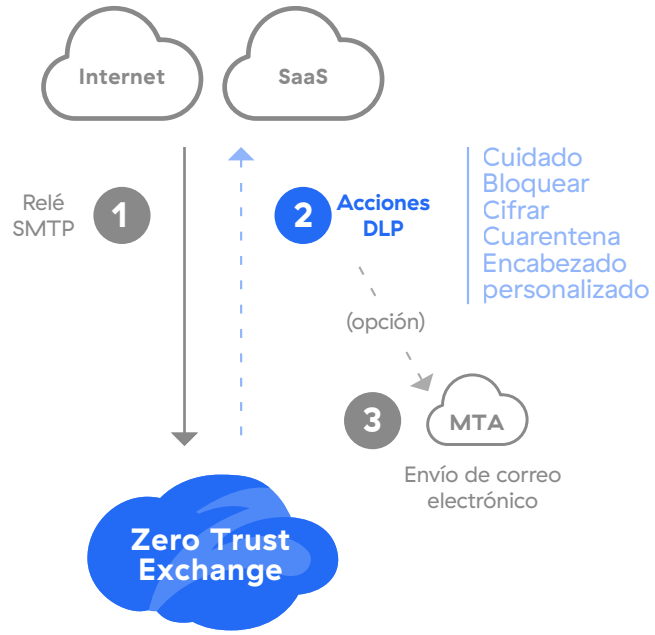
Independiente del protocolo
Funciona en dispositivos administrados, no administrados, incluso móviles

Implementación sencilla
No se requieren cambios en los registros MX

Política flexible
Definiciones de políticas ajustables y evaluaciones granulares de políticas

centralizada y unificada
y motores DLP EN todos los canales

DLP de correo electrónico en tiempo real

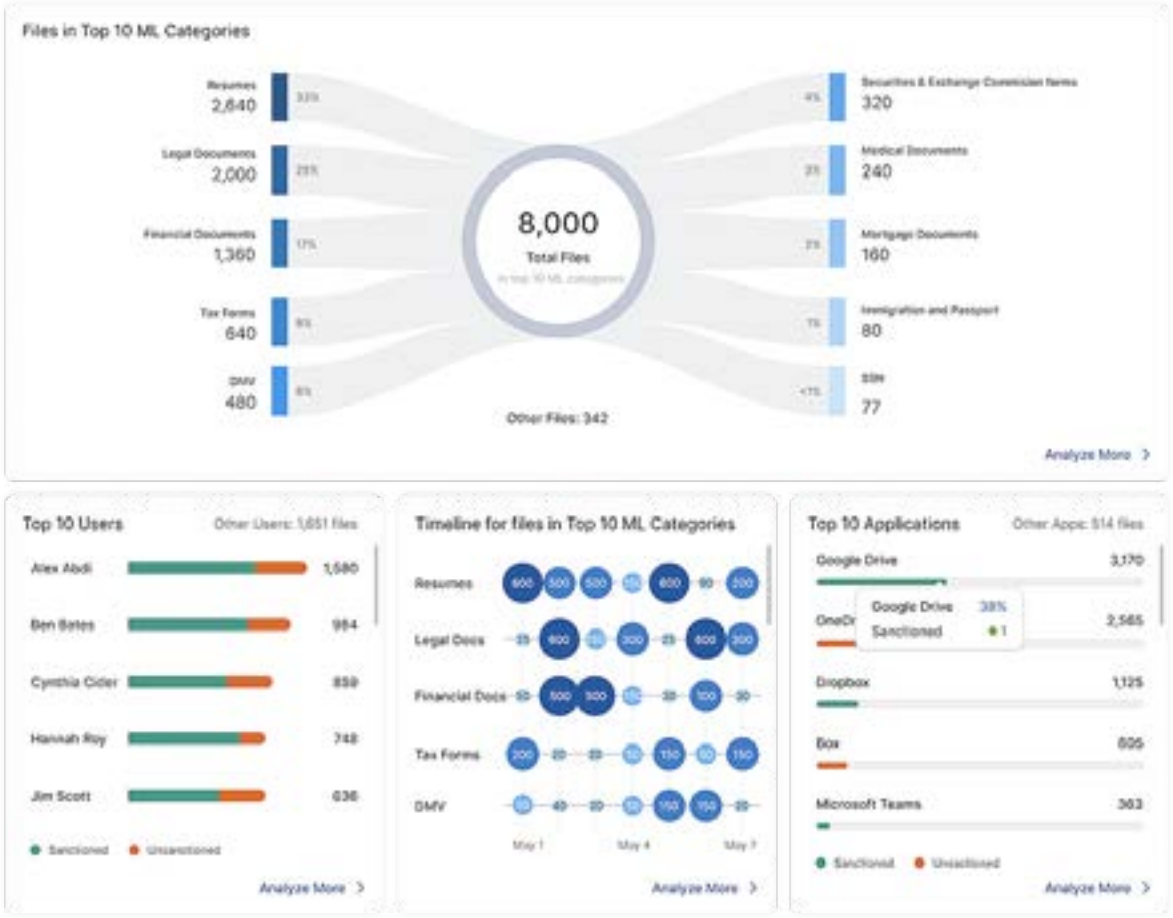


Encuentre y proteja datos al instante con la detección de datos impulsada por la IA

A veces, 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 la IA:

- Descubra datos en puntos finales, 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 contra pérdidas

La clasificación de datos es la base de un buen programa DLP. Con la clasificación de datos avanzada, puede proteger tipos especiales de datos confidenciales contra pérdidas.

Coincidencia exacta de datos (EDM)

Identifique y proteja datos empresariales personalizados. Ejemplo: Activación con 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)

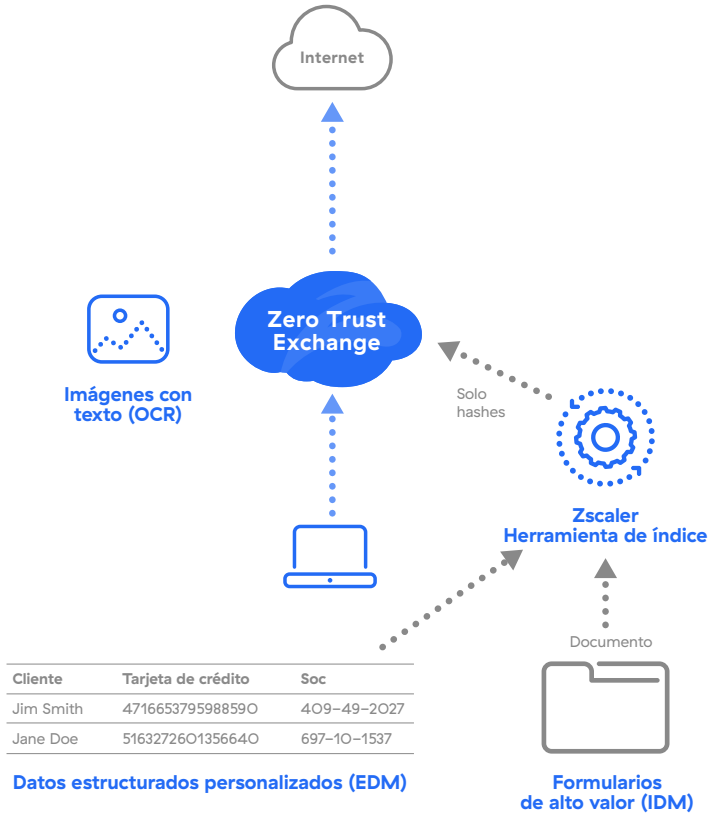
Identifique y proteja documentos y formularios personalizados. Ejemplo: Identifique un formulario de impuestos o hipoteca en blanco y bloquee cualquier otra copia completa.

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 tener contenido confidencial.

Herramienta de indexación Zscaler

Herramienta complementaria de identificación para EDM e IDM. Crea hashes de datos EDM e IDM y los carga la nube de Zscaler para la creación de políticas.



Obtenga máxima visibilidad y control sobre las aplicaciones de IA generativa

Controlar la pérdida de datos confidenciales en las aplicaciones de IA generativa es clave para habilitar estas aplicaciones sombra para la productividad. El nuevo enfoque innovador de Zscaler 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 usted necesita una visibilidad y un 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, incluidas las entradas a nivel de solicitud, para que puedan tomar mejores decisiones de bloqueo.

Ventajas

- Consulte las indicaciones de entrada enviadas por los usuarios a la aplicación de IA para obtener una visibilidad contextual completa.
- Controles de políticas flexibles en la inspección de 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

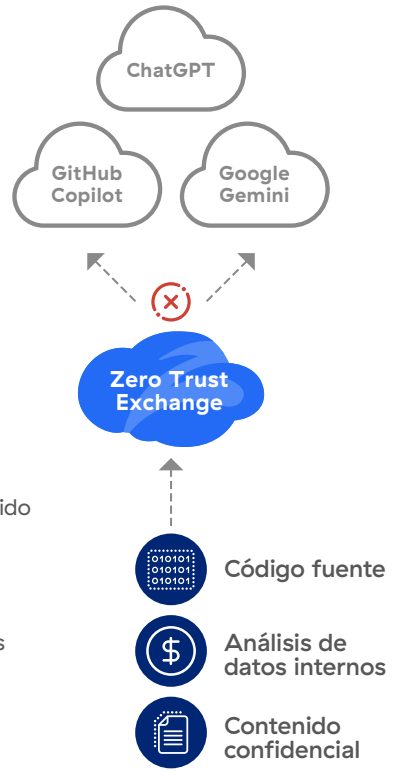
Visibilidad de la solicitud de entrada
Ver las solicitudes de entrada reales que los usuarios envían a las aplicaciones de IA

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 manera en que los equipos de TI protegen los datos y la postura de SaaS.

Muchas violaciones en la nube están causadas por configuraciones erróneas 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 Zscaler SaaS Security Posture Management (SSPM), obtendrá un enfoque unificado para escanear y asegurar 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 datos (DSPM)

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

Los equipos de protección de datos necesitan un enfoque unificado para proteger los datos de la nube pública. 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 descubrir, clasificar y proteger los datos de la nube pública.

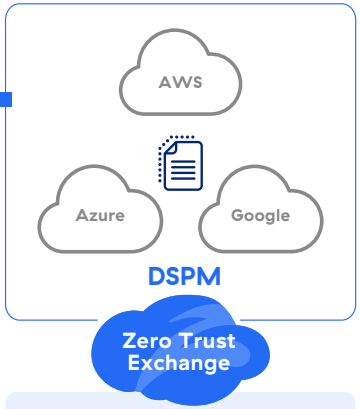
Zscaler DSPM descubre rápidamente datos confidenciales, comprende los riesgos y controla el acceso y la postura. Lo mejor de todo es que la DSPM integrada de Zscaler aprovecha el mismo motor DLP que todos los demás canales (punto final, red, SaaS), por lo que las alertas son uniformes, sin importar a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

Ventajas

- Encuentre rápidamente datos confidenciales con la detección automática impulsada por la IA
- Correlacione las configuraciones erróneas, la exposición y las 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
- Elimine rápidamente los riesgos con orientación práctica sobre remediación

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

1. **Mapee almacenes de datos**
   Asigne buckets, máquinas virtuales y bases de datos con detección automática de datos
2. **Priorice el riesgo**
   Comprenda las configuraciones erróneas y el riesgo de exposición a los datos
3. **Remedie los riesgos**
   Tome medidas con la guía y las políticas de corrección



DLP centralizado:
Defina una vez, implemente en todas partes

Datos seguros de aplicaciones web y acceso para dispositivos BYOD

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

Con Zscaler User Portal 2.0 y Cloud Browser, las organizaciones pueden admitir de manera segura a dispositivos no gestionados. Veamos cómo:

Cómo User Portal 2.0 asegura el acceso y los datos:

- Los usuarios, sin requisitos de agente de punto final, 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 manera segura al punto final como píxeles.
- Las aplicaciones son totalmente interactivas, pero cortar, pegar, descargar e imprimir está bloqueado, y las capturas de pantalla llevan incluso marcas de agua.

Ventajas para los equipos propios (BYOD):

Protección contra amenazas y datos

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

Aislamiento de datos y archivos

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

Políticas de DLP integradas

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

Automatización del flujo de trabajo

Gestione mejor los incidentes de pérdida de datos con Workflow Automation

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 la capacitación de los usuarios.

Muchos programas de protección tienen problemas debido a incidentes y herramientas inconexos. Además, los usuarios nunca se enteran de los riesgos que han asumido al gestionar los datos de manera incorrecta.

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 riesgosos, asignar incidentes a los usuarios para su justificación e implementar rápidamente acciones a nivel de políticas para resolver incidentes.

Cómo Workflow Automation ayuda a su programa de protección de datos

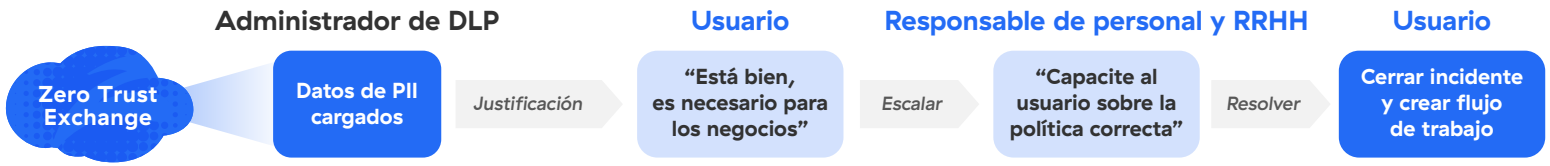
Gestión de incidentes más rápida
Ahorre tiempo con una plataforma diseñada específicamente para la gestión de incidentes de pérdida de datos

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

Capacitación de usuarios
Justifique incidentes con usuarios a través de Slack, Teams o correo electrónico, mientras ofrece capacitación sobre las mejores prácticas de protección de datos

Totalmente integrado
Evite las fallas habituales de los programas de protección mediante un sistema completo 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 el mundo móvil. Zscaler Zero Trust Exchange™ es una plataforma diseñada específicamente que brinda la protección y visibilidad que necesita para simplificar el cumplimiento y hacer que la protección de datos sea sencilla.

Zero Trust Exchange:

- **Proporciona una 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 los puntos ciegos, con el respaldo de los mejores SLA del sector.
- **Simplifica el cumplimiento** para que pueda encontrar y controlar datos de 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 puntos finales y nubes.

Obtenga protección de datos diseñada para un mundo móvil que da prioridad a la nube

Sus datos ya no residen en el centro de datos. Están en todas partes y son accesibles para 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 Zscaler Data Protection, 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, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ataques cibernéticos y pérdida de datos al conectar de forma segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134

zscaler.com/mx