netskope

Manual de seguridad unificada de datos

Revolucione la protección de los datos combinando DSPM y DLP en una única solución

Manual de seguridad unificada de datos

Índice

Resumen ejecutivo

Los equipos de seguridad, gestión de riesgos y cumplimiento normativo de las empresas pueden tener la sensación de que se encuentran en una carrera sin fin, tratando de adelantarse a una serie de actores de amenazas. Y no se equivocan. Las filtraciones de datos son cada año más frecuentes, y ninguna organización es inmune a ellas. El problema afecta a empresas de todos los tamaños, sectores y zonas geográficas.

Puede que los consumidores sean conscientes del riesgo, pero esperan que las empresas con las que hacen negocios protejan su información. Pocos acontecimientos tienen más impacto sobre la reputación de la marca de una empresa que un ciberataque a gran escala.

El panorama de las amenazas ha llevado a los reguladores a aumentar las expectativas sobre la privacidad de los datos corporativos. Las infracciones suelen producirse cuando las organizaciones no cumplen las normas diseñadas para mantener a salvo los datos confidenciales. Los reguladores que descubren que una empresa en cuestión no cumplía la normativa obligatoria tienden a reaccionar con dureza, imponiendo multas punitivas.

Garantizar la seguridad y el cumplimiento de la normativa ya era un reto cuando toda la información valiosa de una empresa se encontraba dentro de su propio perímetro corporativo. Actualmente es aún más difícil porque el 60 % de los datos de los clientes de una empresa media está en la nube.[1] Esta información tan valiosa se encuentra fuera del ámbito de control tradicional del equipo de TI.

Proteger los activos digitales en la empresa moderna exige una nueva forma de pensar. La seguridad unificada de datos combina las funciones de detección de datos, clasificación, control de acceso y evaluación de riesgos (que son las que se encuentran en las herramientas de gestión de la posición de seguridad de los datos [DSPM]), con las protecciones en tiempo real de las tecnologías de prevención de pérdida de datos (DLP). Totalmente integradas, estas soluciones bloquean los datos de una empresa, incluso los almacenados en la nube y en aplicaciones en la sombra no gestionadas por el departamento de TI corporativo, mediante seis funciones clave.

- Descubrir/proteger los datos en cualquier lugar
- Uso seguro de la IA generativa
- Responder a los riesgos de filtración de datos
- Aprovechar la gestión de la seguridad de los datos
- Minimizar la exposición maliciosa y negligente de los datos
- Respaldar la privacidad y el cumplimiento

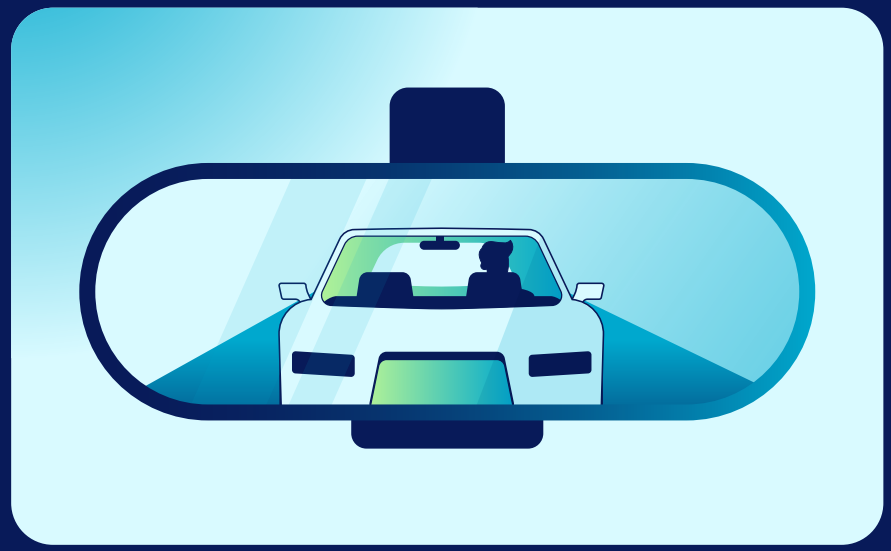
1. Fuente: Statista. «Share of corporate data stored in the cloud in organizations worldwide», marzo de 2022.

Fundamentos de la seguridad de los datos en la era de la IA

Las empresas deben reconocer sus puntos ciegos en materia de seguridad para bloquear eficazmente los intentos de los ciberatacantes de burlar las salvaguardias. Para asegurarse de que tienen una línea de visión clara de todas las aplicaciones y datos a los que acceden los usuarios, los equipos de TI deben plantearse varias preguntas clave:

- ¿Dónde están todos nuestros datos?
- ¿Cuál es la naturaleza de estos datos?
- ¿Quién tiene acceso a los datos confidenciales?
- ¿Hasta qué punto son arriesgadas nuestras interacciones con los datos?

El objetivo de este ejercicio es sencillo: si una solución o base de datos en la nube contiene información personal identificable (IPI) de los clientes, como direcciones o números de la Seguridad Social, o cualquier otra información confidencial de la empresa, la organización debe saber qué protecciones tiene establecidas para no perder de vista el riesgo de los datos.



Consejo profesional

Si una solución o base de datos en la nube contiene IPI de los clientes o cualquier otra información confidencial de la empresa, la organización debe saber qué protecciones tiene establecidas para no perder de vista el riesgo de los datos.

Gestionar el riesgo de los datos

El reto de identificar los puntos ciegos de los datos es que las empresas necesitan proteger mucha información diferente, y esta no siempre se mueve de forma ordenada por los lugares previstos. Los equipos de seguridad pueden tener que gestionar datos en una amplia gama de terminales, sitios web y sistemas de correo electrónico. La información confidencial también puede residir en bases de datos, lagos de datos o almacenes de datos, así como en una serie de sistemas en la nube, no solo de software como servicio (SaaS), sino también de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS).

Algunos de estos datos se encuentran en las instalaciones, otros en la nube. Todos deben protegerse mientras están en movimiento, mientras se utilizan y mientras están en reposo.

Para complicar aún más el reto, aproximadamente el 90 % de los datos corporativos no están estructurados.[2] Existe información crucial en documentos Word, PDF, archivos de imagen y otros formatos. Aunque estos datos no puedan consultarse fácilmente, requieren tanta protección como la información de las bases de datos y otras aplicaciones estructuradas.

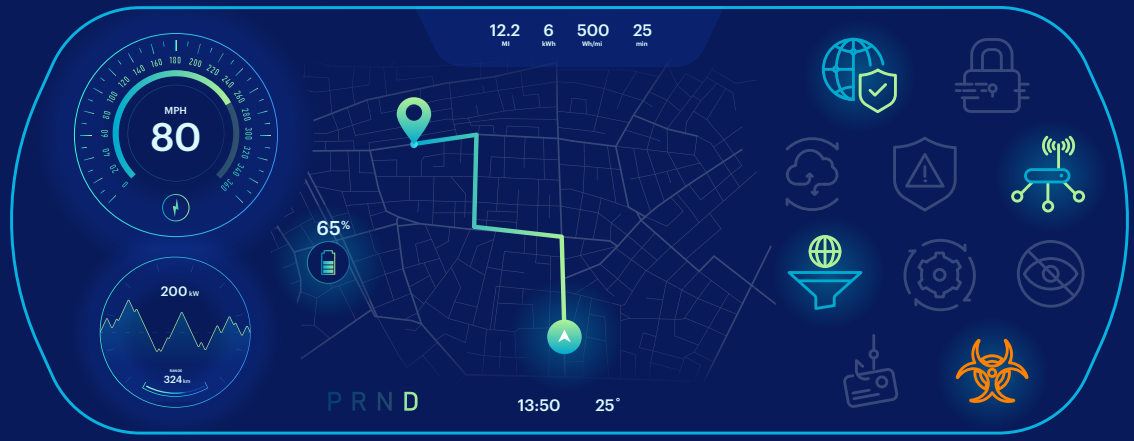
Por último, aunque los datos críticos para la empresa deben residir en aplicaciones gestionadas por la TI corporativa, la TI en la sombra es un problema constante. Con frecuencia, las unidades de negocio implementan tecnologías no gestionadas para un fin específico sin contar con la aprobación de TI. El 97 % de las aplicaciones en la nube que utilizan los empleados de una empresa típica existe fuera del conocimiento de TI.[3]

el **90 %**

de los datos corporativos no están estructurados.

el **88 %**

de los usuarios interactúan con aplicaciones personales en la nube: TI en la sombra[4]



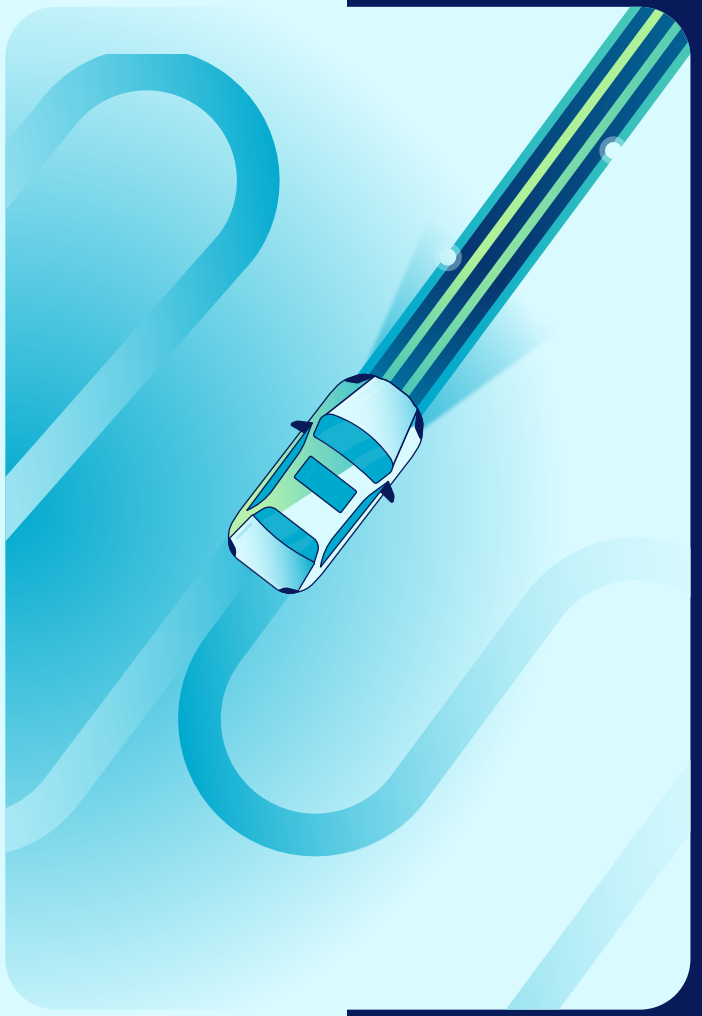
2. IDC. «Untapped Value: What Every Executive Needs to Know About Unstructured Data», agosto de 2023.
3. Informe sobre la nube y amenazas de Netskope Threat Labs: 2025.
4. Informe sobre la nube y amenazas de Netskope Threat Labs: IA generativa, 2025.

Las tecnologías dispares no responden al reto

A las empresas no les faltan opciones para proteger tipos de datos individuales, pero normalmente necesitan un conjunto soluciones para abarcar todos sus datos. Los equipos de seguridad han tenido que aumentar la cobertura a lo largo de los años, y se espera que esta tendencia continúe a medida que surjan nuevas tecnologías y vulnerabilidades.

Los sistemas DLP para terminales hacen un buen trabajo protegiendo los datos en los terminales corporativos. Sin embargo, para proteger la información confidencial de los correos electrónicos, una empresa necesita DLP de correo electrónico u otra solución. Algunas organizaciones disponen de una solución independiente para proteger el uso de la IA generativa (IAgen) en su entorno. La funcionalidad de esta solución podría incluir la prevención de filtraciones accidentales de datos corporativos en el dominio público, pero podría no cubrir las necesidades de cumplimiento normativo de la empresa. En el caso de las amenazas internas, la organización podría disponer de una herramienta de análisis del comportamiento para evitar sabotajes. Y para la detección y la clasificación de los datos confidenciales, DSPM es la mejor opción.

El problema es que la implementación de todas estas soluciones diferentes crea un complejo panorama de tecnologías dispares que sobrecargan los recursos informáticos y pueden mermar la seguridad de los datos corporativos.



«Ha llegado el momento de replantearse la seguridad de los datos si ha estado tratando la DSPM y la DLP como elementos independientes. Ambas pueden funcionar juntas para formar el pilar de un método integral que no solo proteja sus datos, sino que posicione competitivamente a su organización para liderar en la economía actual impulsada por los datos».

Ankur Chadda

Director de Marketing de Seguridad de Datos de Netskope

Seguridad unificada de datos

Los equipos de TI necesitan una plataforma de seguridad capaz de proteger todo tipo de datos y que, al mismo tiempo, ofrezca visibilidad desde un único punto de vista. Ese es el objetivo de las plataformas de seguridad unificada de datos, que aúnan las capacidades de DSPM y DLP en una única solución.

Reunir todos los datos de una empresa en la misma solución tiene varias ventajas importantes:

- **Mayor visibilidad.** El personal de TI puede consultar un único cuadro de mandos para comprender los problemas de seguridad de los datos que puedan existir en las instalaciones o en la nube, y en los datos gestionados y no gestionados que estén en movimiento, en uso o en reposo.
- **Mayor seguridad.** Los sistemas dispares suelen dar lugar a una respuesta inconexa ante cualquier amenaza. A la inversa, una plataforma estrechamente integrada garantiza que la información sobre riesgos o amenazas recopilada por una solución se comparta con las demás, lo que permitirá una respuesta coordinada en todos los lugares donde la empresa almacene datos.
- **Facilidad de gestión.** La administración de la infraestructura de seguridad requiere menos tiempo del personal, por lo que el equipo de seguridad pasa de la constante lucha reactiva «para apagar incendios» a la corrección de vulnerabilidades, la planificación a largo plazo y otras iniciativas estratégicas.

«Entiendo cómo es mi conjunto de políticas a través de múltiples funciones y aplicaciones, en comparación con algunas de nuestras aplicaciones heredadas en las que existían cuatro lugares diferentes para gestionar una única aplicación y sus funciones».

Vicepresidente de Infraestructura

Tecnología

El enfoque de Netskope One para la seguridad unificada de datos

Netskope One ayuda a las organizaciones a dar un cambio rápido proporcionando una plataforma unificada para la seguridad integral de los datos. Une la DSPM y la DLP con el objetivo de aportar precisión y exactitud a la detección de riesgos y la reducción de amenazas.

La capacidad de la plataforma Netskope One para proteger los datos en reposo, en movimiento y en uso frente a todos los vectores de amenazas clave es un elemento diferenciador fundamental con respecto a las soluciones alternativas. Al consolidar tantas capacidades, permite que todas las herramientas que protegen la información confidencial compartan contexto entre usuarios, aplicaciones y acciones.

Este enfoque refuerza la seguridad de cinco maneras esenciales:

1. Reduce la exposición de riesgo de la empresa: Netskope One controla el acceso a todas las aplicaciones web, SaaS y privadas en las que residen los datos.
2. Acelera la detección de datos.
3. Respalda una mejor comprensión de los datos corporativos, incluidos su linaje y movimientos.
4. Facilita un control automatizado y en tiempo real del riesgo de los datos.
5. Es compatible con la escalabilidad: Las políticas y los perfiles de datos pueden crearse una sola vez y después utilizarse en todas partes.

Netskope One proporciona la mejor cobertura en amplitud y profundidad de su clase en cualquier lugar donde residan los datos de una empresa. Veamos ahora las tres preguntas que le ayudarán a evaluar el entorno de su organización:

Pregunta 1: ¿Cuánto riesgo presenta su área expuesta?

Pregunta 2: ¿Con qué rapidez responden sus soluciones de seguridad ante los comportamientos de riesgo?

Pregunta 3: ¿Cómo aplica las políticas de DLP al resto del tráfico?

«Netskope nos permite cuantificar la filtración de datos y vincular los comportamientos de riesgo a las personas, lo que nos permite tomar medidas a tiempo».

Director General

Programa Global de Riesgos de Información Privilegiada, importante empresa de servicios financieros

Pregunta 1: ¿Cuánto riesgo presenta su área expuesta?

Netskope One toma decisiones sobre políticas continuas, adaptables y basadas en la confianza en tiempo real. Cada vez que un usuario intenta almacenar, mover o manipular datos, la plataforma evalúa el riesgo a través de cuatro vectores:

- **Riesgo del usuario:** ¿Están sus datos a salvo de suplantadores? ¿Puede verificar que los usuarios son quienes dicen ser?
- **Riesgo del dispositivo:** ¿Está la persona en un dispositivo gestionado, en un lugar conocido y de confianza?
- **Riesgo de la aplicación:** ¿Se trata de una aplicación gestionada por TI? ¿Y se trata de una instancia empresarial o personal de la aplicación?
- **Riesgo de los datos:** ¿Se trata de datos o información empresarial de carácter confidencial?

Netskope ha analizado y clasificado más de 80 000 aplicaciones y ha desarrollado 130 categorías para las URL. La plataforma Netskope One clasifica el tráfico según estos parámetros, para acelerar la gestión de cualquier amenaza. La plataforma también puede diferenciar entre miles de instancias de SaaS.

Netskope One reúne toda esta información y, a continuación, aprovecha el análisis del comportamiento de usuarios y entidades (UEBA), junto con la información sobre amenazas en tiempo real, para clasificar la actividad que ha intentado llevar a cabo el usuario en una escala de comportamientos de riesgo.

Pregunta 2: ¿Con qué rapidez responden sus soluciones de seguridad ante los comportamientos de riesgo?

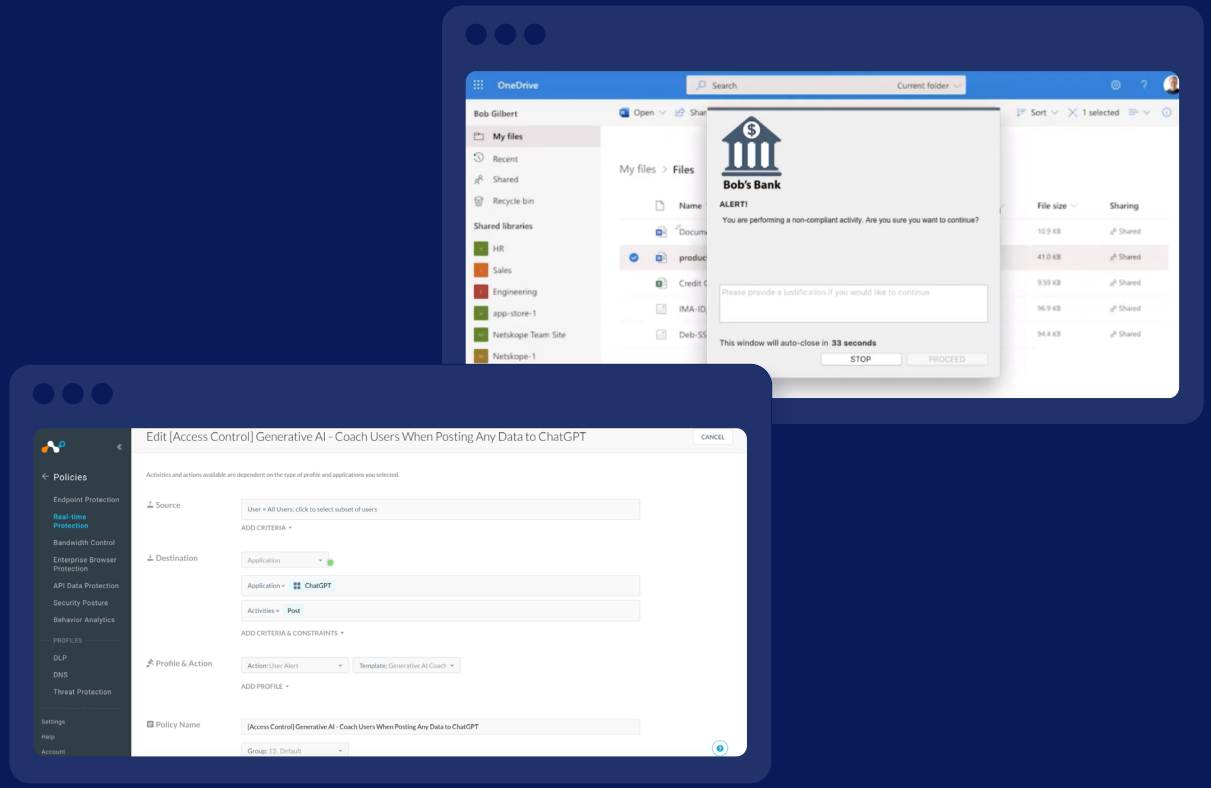
Tras completar el análisis de riesgos, el cumplimiento de las políticas de Netskope One Data Security interrumpe el tráfico sospechoso mientras el usuario se vuelve a autenticar o proporciona una justificación de su comportamiento. De forma alternativa, puede bloquear automáticamente el tráfico, en el peor de los casos, aislando al usuario o al dispositivo hasta que una persona pueda evaluar la actividad.

Las empresas pueden utilizar Netskope One Data Security para introducir controles granulares que, entre otras cosas:

- Bloquean los programas maliciosos y los contenidos que infringen la política de uso aceptable (AUP).
- Detienen las actividades o aplicaciones en la nube que se sabe que entrañan riesgos.
- Impiden subir material a cualquier aplicación en la nube, o instancia de aplicación, que TI no gestione.
- Restringen las actividades de compartir a determinados dominios web.
- Limitan el tráfico en función de información adicional, como las características del usuario.

Una característica exclusiva de Netskope One Data Security es que puede configurarse para que ofrezca formación en tiempo real a los usuarios cuyo comportamiento infrinja la política de datos corporativa.

> «Nos preocupa mucho la agresividad de los [actores de amenazas persistentes avanzadas] que persiguen nuestros datos. La solución Netskope SSE nos ayuda a controlarla de forma mucho más eficaz».
>
> **Vicepresidente de Infraestructura,**
> empresa de tecnología



Pregunta 3: ¿Cómo aplica las políticas de DLP al resto del tráfico?

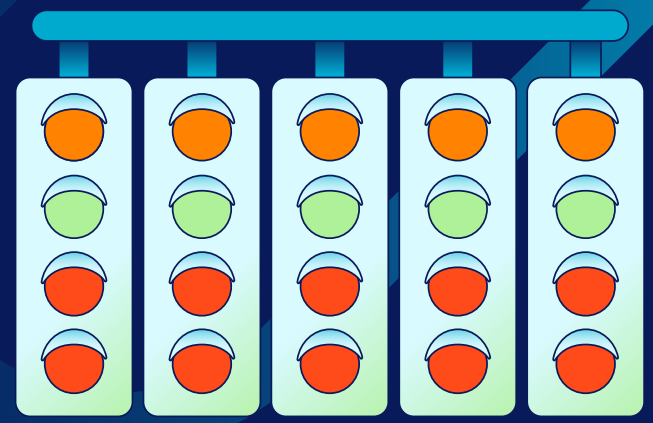
Al tráfico que supera el análisis de DSPM, Netskope One Data Security aplica técnicas de DLP para garantizar que los usuarios no filtren ningún dato. Las capacidades de la plataforma examinan los datos procedentes de correos electrónicos, terminales, sitios web y diversos formatos de almacenamiento de datos, tanto a nivel local como en la nube.

Al igual que las iteraciones anteriores de DLP, Netskope One Data Security utiliza expresiones regulares personalizadas, palabras clave, diccionarios, correspondencia exacta de datos (EDM) y correspondencia indexada de documentos (IDM) para identificar los datos. Recoge pistas contextuales tanto de la plataforma, factores como el riesgo del usuario o la información del agente de seguridad de acceso a la nube (CASB) o las funciones de gestión de la posición de seguridad SaaS (SSPM), como de fuentes externas, como el inicio de sesión único (SSO) o las integraciones de la pasarela de correo electrónico seguro (SEG). Al igual que la DSPM, Netskope One DLP aprovecha la inspección de contenidos mediante modelos de aprendizaje automático (ML) para encontrar PII, PHI y otros tipos de datos.

Para el 84 % de las organizaciones que deben atenerse a algún tipo de marco de cumplimiento externo,[5] estas capacidades son cruciales. Netskope One incluye 38 plantillas predefinidas de cumplimiento legal y normativo que ayudan a las unidades de negocio de todo el mundo a cumplir los requisitos locales. Lo mejor de todo es que, aunque la plataforma mejora el cumplimiento de las normas, reduce las fricciones de seguridad para los usuarios, de modo que no impide la productividad de la empresa.

«Netskope nos proporciona las herramientas y capacidades para adoptar de forma segura las tecnologías en la nube manteniendo el control y el cumplimiento».

Jefe de Seguridad
Apex Group



5. Fuente: Coalfire. «Securealities Report: Compliance 2023», mayo de 2023.

Netskope One ML interpreta datos estructurados y no estructurados

Netskope One utiliza el aprendizaje automático (ML) tanto para determinar el contenido de los datos no estructurados como para categorizarlos. Por ejemplo, el proceso de clasificación de imágenes de la plataforma utiliza un algoritmo de ML entrenado para identificar documentos confidenciales como pasaportes o permisos de conducir sin examinar el texto. Por su parte, la tecnología de reconocimiento óptico de caracteres (OCR) de la plataforma puede extraer texto de las imágenes para su análisis.

Las capacidades de ML integradas en Netskope One utilizan atributos de datos estructurados y no estructurados para etiquetarlos como IPI o información personal de salud (IPS), sujetos al Reglamento General de Protección de Datos (RGPSD) o a la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), etc. La plataforma incorpora más de 3000 clasificadores de riesgo de datos y las empresas también pueden elaborar sus propios clasificadores basados en ML.

Netskope One también puede entrenarse para buscar combinaciones de identificadores, como números de la Seguridad Social en documentos fiscales, o para realizar un análisis de privilegios comparando datos y características de usuarios. Aprovechar el aprendizaje automático de esta forma reduce la sobrecarga operativa de la seguridad al minimizar la participación humana en la toma de decisiones rutinarias, a la vez que mejora la eficacia de las decisiones porque se elimina la posibilidad de error humano.

Consejo profesional

El aprendizaje automático reduce la sobrecarga operativa de la seguridad al minimizar la participación humana en la toma de decisiones rutinarias, a la vez que mejora la eficacia de las decisiones.

Netskope One: la elección correcta para la seguridad unificada de datos

Netskope One se adelanta a los posibles atacantes combinando las funciones de DSPM con un motor de DLP unificado que gestiona todas las fuentes de datos, tanto a nivel local como en la nube. La plataforma ofrece un panel único que muestra los problemas, los controles y la respuesta a las amenazas a lo largo de todo el ciclo de vida de los datos. Y la información que genera permite aplicar las políticas en tiempo real.

La plataforma Netskope One protege todos los datos de una empresa, ya sean estructurados o no estructurados, gestionados o no gestionados, y tanto si están en el centro de datos como en la nube. Según un estudio de Forrester sobre el impacto económico total, el cliente típico de Netskope consigue estos resultados empresariales:[6]

> «Sin lugar a dudas, diría que el riesgo se ha reducido [al implementar Netskope SSE] porque no estamos apagando fuegos todo el tiempo y, en su lugar, podemos concentrarnos en las vulnerabilidades y en el trabajo real».
>
> **Vicepresidente de Experiencia Digital**
> Empresa de servicios financieros

Resultados empresariales

- ✓ **Reducción del 80 % en el riesgo de violación grave de los datos por ataque externo.**
- ✓ **Reducción del 60 % en el tiempo medio de resolución (MTTR).**
- ✓ **Reducción del 10 % en los costes de infraestructura.**
- ✓ **Reducción del 80 % en el volumen de incidencias de servicio técnico.**
- ✓ **Reducción del 15 % de los tiempos de inactividad imprevistos.**
- ✓ **Aumento del 30 % en la eficacia de las operaciones de red y la seguridad.**
- ✓ **Mayor protección de la propiedad intelectual (PI) gracias a la DLP.**
- ✓ **Mejor preparación y capacidad de respuesta para el cumplimiento de las normativas.**
- ✓ **Mayor alineación con los objetivos ambientales, sociales y de gobernanza (ESG).**

6. Forrester. «The Total Economic Impact of Netskope SSE», octubre de 2024.

La vuelta de honor con Netskope One

Ganar la carrera contra los ciberatacantes requiere estrategia, preparación y ejecución. Cuando se pisa el acelerador, es todo o nada.

La seguridad unificada de datos con Netskope One ofrece todas las capacidades que los mecánicos de la seguridad necesitan para proteger sus máquinas de gran valor:

- **Automatización de la detección y clasificación de los datos corporativos dondequiera que residan y se muevan.**
- **Respuesta rápida ante los riesgos de filtración de datos.**
- **Cumplimiento de la normativa y protección de la privacidad de los datos de forma eficaz.**
- **Disminución significativa del riesgo de uso malintencionado de la información privilegiada.**
- **Reducción al mínimo de la exposición negligente de los datos.**
- **Una experiencia de usuario final sin fricciones.**
- **Garantía de uso seguro de la IAgen en la organización.**
- **Gestión integral del ciclo de vida de los datos.**

«La ciberseguridad es un diferenciador competitivo para nosotros porque nos ayuda a atraer nuevos clientes, especialmente de aquellos sectores que valoran una sólida protección de los datos».

CISO

Empresa de servicios globales

«Netskope SSE nos hizo ver todos estos problemas de los que realmente no sabíamos nada. Encontramos sistemas en Internet que no pasaban por nuestros controles de seguridad... Nos pilló por sorpresa [y] solucionamos [los problemas]».

Vicepresidente de Experiencia Digital

Empresa de servicios financieros[7]

Netskope One

Proteja sus datos con Netskope One Data Security.

Más información →

[7] Forrester. «The Total Economic Impact of Netskope SSE», octubre de 2024.

Acerca de Netskope

Netskope, líder en seguridad y redes modernas, atiende las necesidades tanto de los equipos de seguridad como de redes proporcionando acceso optimizado y seguridad basada en contexto en tiempo real para las personas, dispositivos y datos estén donde estén. Miles de clientes, incluidas más de 30 empresas de Fortune 100, confían en la plataforma Netskope One, su motor Zero Trust y su potente red NewEdge para reducir riesgos y obtener una visión completa de cualquier actividad en la nube, la IA, la web y las aplicaciones privadas, ofreciendo siempre seguridad y acelerando el rendimiento sin renunciar a nada.

¿Le gustaría obtener más información?

Solicite una demostración

Recursos

- El valor de la seguridad unificada de datos
- Informe sobre el estado de la gestión del riesgo de datos
- Introducción al laboratorio práctico de Netskope One SSE
- Introducción al laboratorio práctico de Netskope One Data Loss Prevention (DLP)

netskope