eBook

5 requisitos para un enfoque DLP moderno

netskope

En un mundo actual basado en la nube e impulsado por la transformación digital y el trabajo híbrido, las organizaciones deben alinear las iniciativas de seguridad de datos con las tendencias modernas que van cambiando al ritmo de la nube. Además, cada organización tiene sus propias necesidades de protección de datos y casos de uso únicos, ya que los programas de protección de datos nunca son idénticos. Por tanto, solo es posible garantizar una alta flexibilidad, una gran escalabilidad y una potencia informática sin limitaciones mediante una arquitectura de prevención de pérdida de datos (DLP) en la nube. La nube también obliga a estar siempre actualizado, con protecciones activas en todo momento y actualizaciones disponibles en tiempo real. Obviamente, el enfoque adecuado para la protección de datos empresariales es mediante una tecnología DLP en la nube como servicio, pero no debería ser el único criterio que se debe considerar al pasar a una estrategia de protección de datos eficaz.

Una tecnología DLP debe ser adaptable, con multitud de funciones, gran cobertura y eficiencia. Asimismo, debe ofrecer un alto grado de eficacia que garantice una protección de datos precisa para cualquier tipo de datos, en todos los entornos y frente a cualquier riesgo de pérdida de datos.

Existen directrices arquitectónicas útiles y recomendaciones tecnológicas que deben tenerse en cuenta en todo momento antes de pasar de la implementación de DLP existente a otra que satisfaga las necesidades del trabajo híbrido moderno:

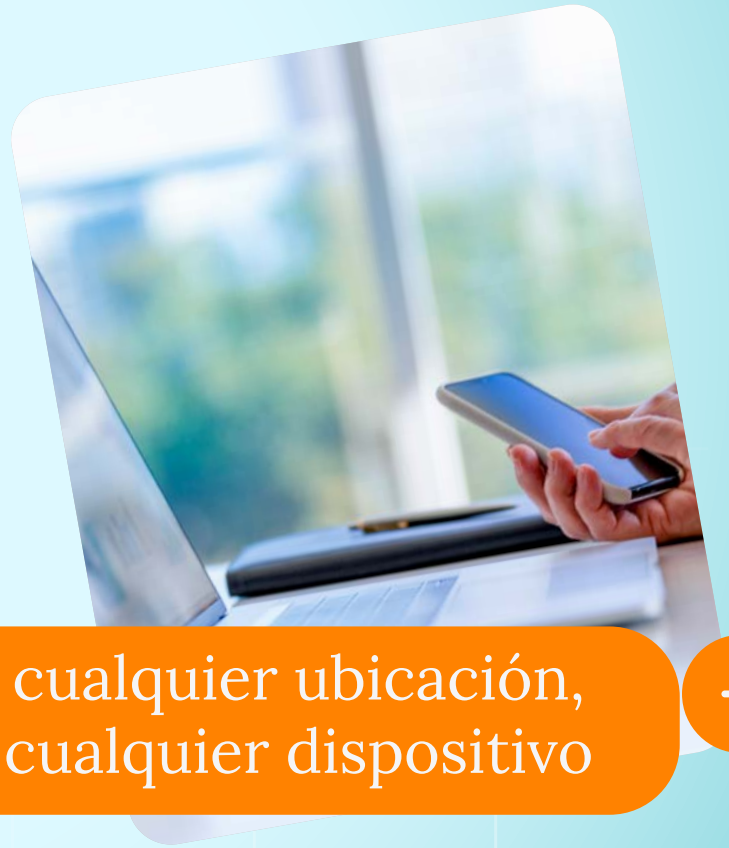
01

Amplitud de la cobertura

Lo que no se ve no puede protegerse y, hoy en día, los datos circulan a través de muchos más entornos que antes. La DLP empresarial heredada, implementada de forma tradicional en la red física, ofrece una amplia cobertura de los canales de datos en las instalaciones, como las transmisiones web, el protocolo SMTP de correo electrónico y los *endpoints*. Es de esperar que una solución moderna en la nube amplíe la protección llegando a los repositorios en la nube, como aplicaciones SaaS, IaaS y correo electrónico en la nube, además de garantizar la cobertura de entornos locales como redes, *endpoints* y el correo electrónico. Siempre es recomendable garantizar que una solución DLP en la nube proporcione una cobertura empresarial completa tanto para la nube como para las ubicaciones locales tradicionales. En ese aspecto, también es importante saber que la mayoría de las soluciones DLP en la nube se han diseñado para resolver solamente los casos de uso en la nube y no abarcan ciertas ubicaciones locales, como los *endpoints*.

01

Actualmente, hay muchos casos de uso que son fundamentales y se deben abordar de forma adecuada, como la transferencia de información confidencial mediante miles de aplicaciones SaaS peligrosas no autorizadas o para instancias personales de aplicaciones SaaS autorizadas, como una cuenta personal de Gmail o una instancia personal de OneDrive, o para aplicaciones privadas en la nube pública o en el centro de datos. En el caso de una empresa moderna ampliamente distribuida formada por diferentes oficinas y trabajadores remotos híbridos, la DLP debe proteger todas las transmisiones de datos desde cualquier ubicación y dispositivo, incluidos los dispositivos administrados y no administrados, e incluso la Internet de las cosas (IoT). La transferencia de información confidencial de *endpoints* a un USB es también una forma importante de pérdida de datos que debe controlarse, incluso cuando dichos *endpoints* no están en línea. Los correos electrónicos salientes, de índole privada, son otro vector importante de pérdida de datos, además de comunicaciones confidenciales en aplicaciones de colaboración como Slack y Teams.



cualquier ubicación,
cualquier dispositivo

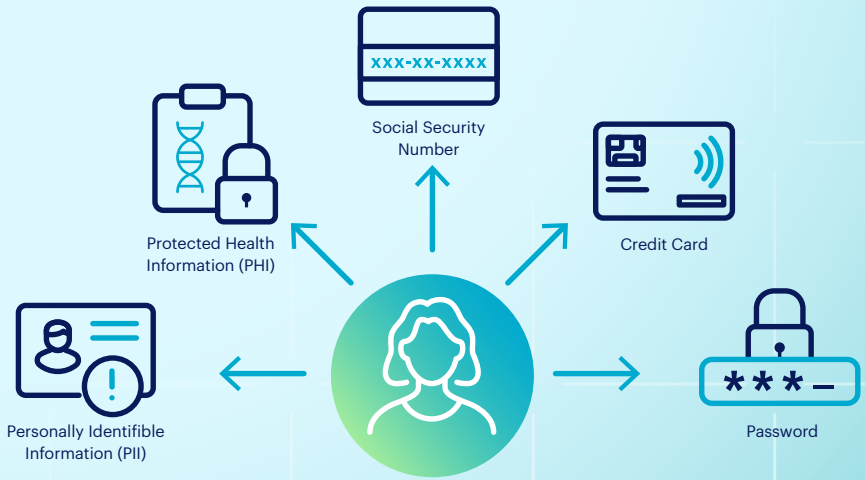
02

Capacidades fundamentales para la detección de datos

Una visibilidad precisa de los datos es una necesidad táctica para evaluar el entorno operativo e implementar una estrategia de protección adecuada. Todo empieza con el descubrimiento y la clasificación de los datos privados, incluida la información de identificación personal (PII) estructurada y no estructurada, la propiedad intelectual (PI), la información confidencial y los secretos comerciales.

Debido a que la clasificación manual de los datos por parte de sus propietarios puede ser un proceso poco fiable, esta labor también debe automatizarse con DLP a través de un conjunto completo, no parcial, de motores de detección. Dichos motores establecen las políticas de detección o los perfiles de datos preestablecidos de la organización. En concreto:

- Los **identificadores de datos** han sido y siguen siendo imprescindibles en cualquier solución DLP. Su labor es identificar miles de tipos de datos confidenciales diferentes según los criterios de coincidencia descritos que normalmente caracterizan objetos como SSN, información de tarjetas de pago o números de pasaporte, como número de dígitos, patrones de texto, secuencias, separaciones y la proximidad de palabras clave. Contar con capacidades de expresiones regulares (regex) es fundamental, pero no puede ser una característica de verificación. Han surgido más tipos de datos y casos de uso modernos con nuevos requisitos de cumplimiento que exigen proteger la privacidad de las personas de una forma más exhaustiva. De hecho, el primer elemento que debe tenerse en cuenta es el gran número de identificadores de datos preestablecidos, pero también la granularidad de las personalizaciones de las reglas, como los niveles de gravedad, el alcance de las comprobaciones de proximidad, la lógica booleana, etc.



02

- El número de **tipos de archivos** compatibles es otro elemento clave. Existen miles de tipos de datos que pueden contener información confidencial: texto, presentación, correo electrónico, imágenes y capturas de pantalla, hoja de cálculo, diseño asistido por ordenador (CAD), publicaciones en redes sociales, formularios en línea, mensajes de Slack y otros canales de chat, encapsulación, archivos adjuntos, gráficos e imágenes como JPEG y PDF, etc.
- Los **clasificadores de datos de inteligencia artificial/aprendizaje automático (IA/AA)** ayudan a descubrir e identificar datos. Las reglas establecidas manualmente son la base de la detección de datos, pero en el mundo moderno, los motores automatizados proporcionan una ayuda inestimable logrando una detección y categorización más precisas de los datos confidenciales. También se adaptan a las condiciones cambiantes e identifican similitudes en términos de contenido.
- La **coincidencia exacta de datos (EDM)** es un método tradicional, pero casi infalible, que ha sido pensado para detectar información específica obtenida de fuentes de datos estructurados, como hojas de cálculo y bases de datos. Gracias a la EDM, una solución DLP puede realizar una huella digital e indexar conjuntos de datos de registros confidenciales, información que, de forma conjunta, puede identificar a una persona, como nombres completos de clientes, números de la Seguridad Social, direcciones, números de identificación, etc., o registros económicos que definen los activos financieros de una persona, como números de tarjetas de crédito o números de cuentas bancarias, incluso información sanitaria o bases de datos de precios e identificación de productos. Posteriormente, dicha información indexada se debe rastrear y encontrar en cualquier lugar donde se espere que circulen los datos.

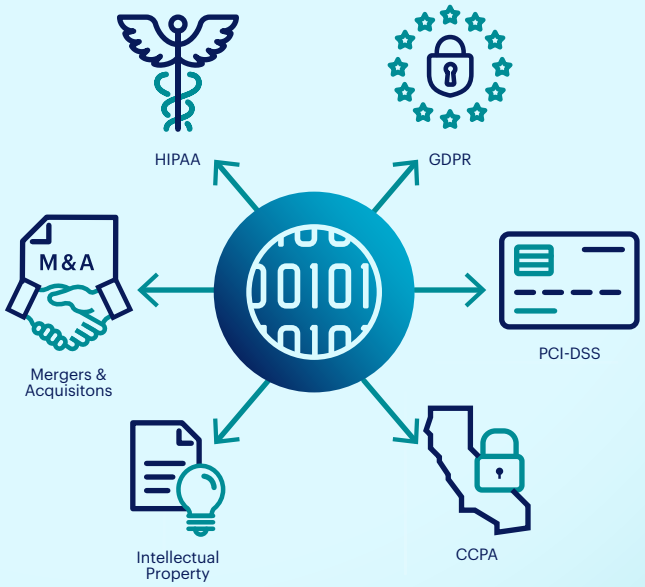
Un comentario sobre la EDM

Para que la EDM sea eficaz y precisa, debe poder aprovechar las condiciones granulares que hacen coincidir varias partes de los datos indexados y las combinaciones de campos de datos de un registro particular, aquellos que son importantes. La EDM a gran escala es un factor muy importante, en particular para las grandes empresas y para las organizaciones que desean crecer en el futuro. Debe admitir millones o incluso miles de millones de registros.

03

Creación de perfiles de datos para el futuro

No se centre únicamente en los identificadores de datos que necesita en la actualidad. Busque miles de identificadores de datos preestablecidos, que incluyan patrones localizados como tarjetas de identificación por países, ya que es probable que sus necesidades futuras aumenten al ritmo del crecimiento de su organización y la madurez de la protección de datos. Busque la presencia de las plantillas de cumplimiento normativo necesarias para comprobar que estén actualizadas: RGPD, CCPA, PII, PCI, PHI, por citar algunos de los reglamentos y tipos más conocidos. Comprenda el nivel de compromiso del proveedor por mantenerse al día con los requisitos de cumplimiento más recientes y averigüe si es probable que el proveedor los amplíe en el futuro. La posibilidad de editar expresiones regulares o identificadores existentes o de crear identificadores de datos personalizados con controles granulares es fundamental, ya que cada organización tiene sus propias necesidades, como un tipo específico de información que es confidencial únicamente para esa organización concreta.



04

Capacidades avanzadas de detección de datos

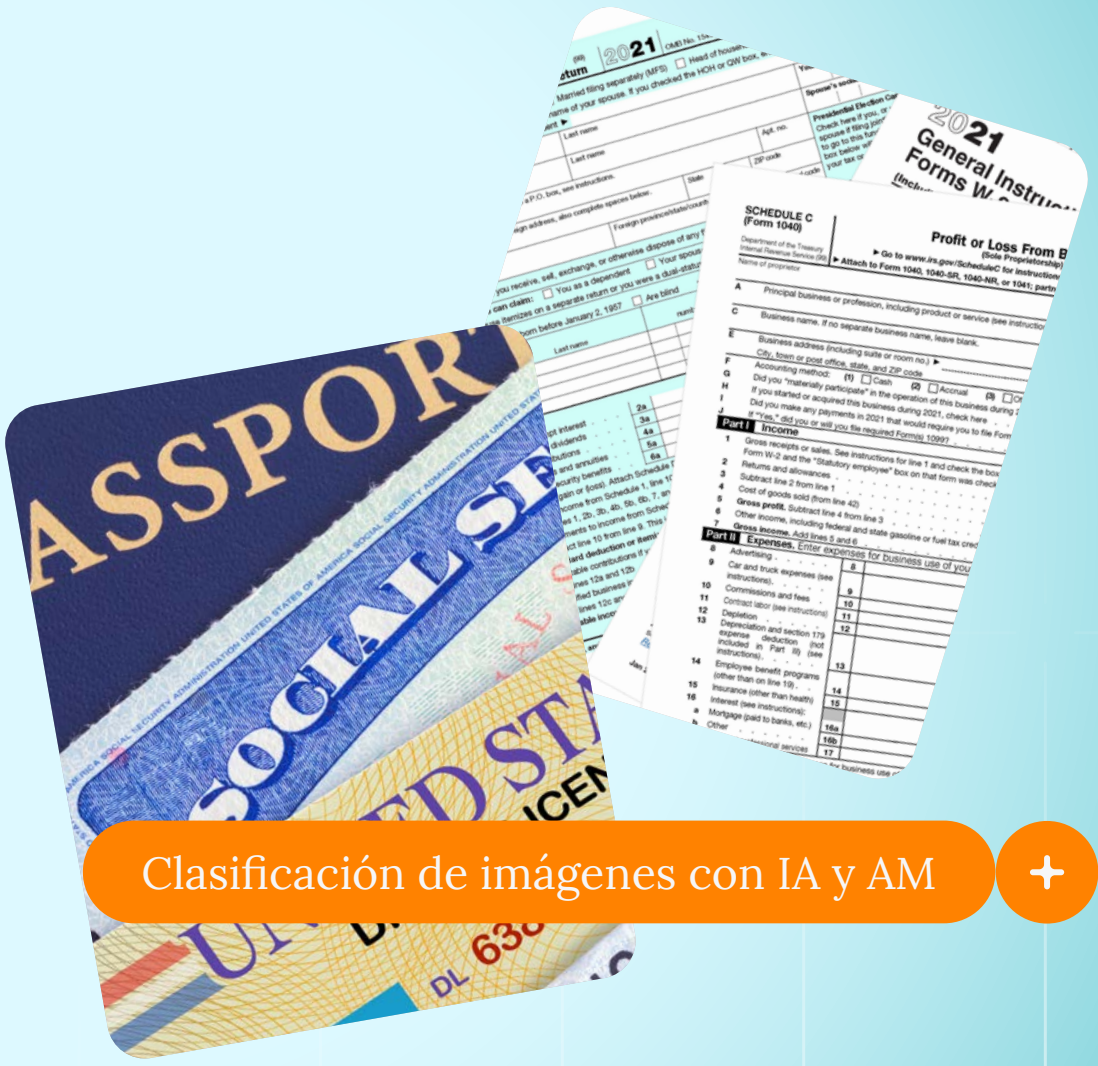
A lo largo de los años, los datos también han vivido una importante evolución, aumentando su volumen, variedad y velocidad, y ahora están más desestructurados que nunca. La introducción de unos tipos de datos más nuevos y formas modernas de compartirlos y transmitirlos, el crecimiento masivo de los volúmenes de datos y los nuevos requisitos de cumplimiento normativo exigen métodos más avanzados para detectar la información confidencial. Las soluciones DLP heredadas introdujeron capacidades de detección avanzadas en el pasado, pero empezaron a fallar a la hora de dar unos resultados de detección precisos debido a la ausencia de potencia y escala informáticas. Por lo tanto, generan cada vez más falsos positivos que dificultan el flujo de información y sobrecargan a los equipos de respuesta a incidentes.

En cambio, puede que la mayoría de las nuevas soluciones DLP en la nube sean aún inmaduras y su eficacia todavía no se haya demostrado. Es fundamental comprobar la presencia y el nivel de sofisticación de las siguientes capacidades de detección avanzada:

- En el mundo actual, a los usuarios les resulta muy conveniente tomar fotos de documentos, formularios, carnets de identidad, pizarras e incluso fotografías de otras imágenes. Por ejemplo, las capturas de pantalla son un medio muy habitual de recoger información rápidamente y compartirla de forma inmediata con un compañero. Por tanto, el **reconocimiento óptico de caracteres (OCR)** y el reconocimiento de imágenes basado en IA son cada vez más importantes en una estrategia de protección de datos moderna y con visión de futuro. Gracias al OCR, una solución DLP puede obtener información textual de una imagen y aplicar la clasificación de datos según las políticas de detección vigentes.
- La **clasificación de imágenes con IA y AA**es fundamental para reconocer tipos de archivos y documentos habituales, como tarjetas SSN, patentes y documentos de fusiones y adquisiciones, formularios de impuestos, código fuente, capturas de pantalla del ordenador, pasaportes y otros documentos de identificación, etc., sin extraer necesariamente el contenido incluido en dichos activos. Estos métodos de detección deben ofrecer un gran nivel de sofisticación para poder identificar imágenes a través de variaciones como contenido borroso, arrugado y dañado, con información que no se puede leer con claridad. Esto sucede cuando las imágenes y las capturas de pantalla se realizan rápidamente y en condiciones de poca o mucha luz, o cuando un documento tiene daños o está viejo.

04

- La **huella digital de archivos y documentos («*fingerprinting*»)** es otra prestación avanzada que es fundamental para muchas organizaciones. Algunos documentos claves, de propiedad intelectual y archivos sumamente confidenciales se deben proteger a cualquier precio frente a la exfiltración total o parcial y las copias duplicadas. Las huellas digitales de archivos pueden indexar documentos completos y posteriormente detectar copias exactas o incluso parciales de su información con un determinado nivel de similitud, cuando dicho contenido se encuentra en entornos y canales de transmisión que se consideran peligrosos, como ocurre cuando se suben a una instancia privada de una aplicación de correo electrónico.



05

Una protección de datos consciente de los riesgos: un modelo listo para la confianza cero

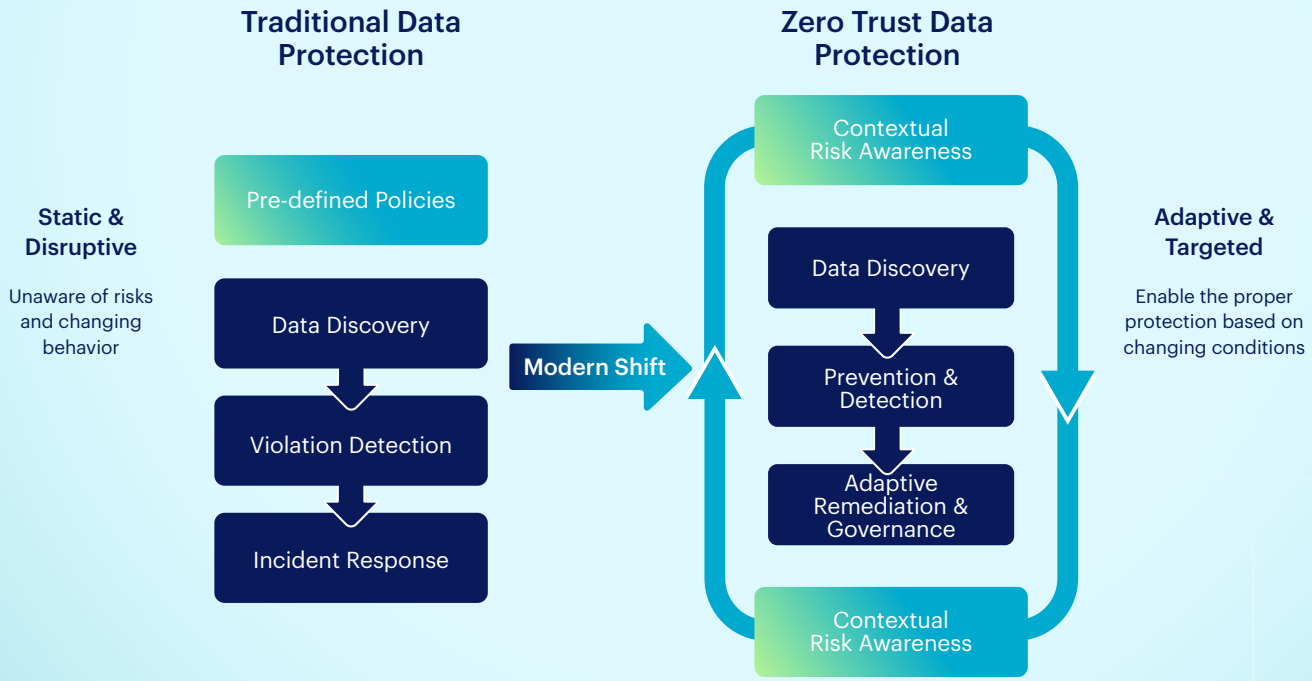
La transformación digital ha cambiado para siempre nuestro modelo existente, por lo que necesitamos otro que se ajuste a dicha transformación. La confianza cero es una estrategia moderna que lleva los controles de seguridad a los propios datos como un nuevo perímetro y sustituye la confianza implícita por una evaluación de riesgos continua y adaptable, que se amolda constantemente a la evolución de las condiciones de riesgo. Se ha demostrado que los controles de datos del pasado causaban problemas operativos y dificultaban la generación de valor porque carecían de contexto. Por este motivo, la DLP tradicional ha fracasado: no existía suficiente contexto comercial ni la conciencia sobre riesgos que se necesitan para ofrecer confianza y prevenir el movimiento de los datos. El equipo de respuesta a incidentes, que tampoco contaba con suficiente contexto de riesgos y comportamiento, era el encargado de tomar manualmente la mayoría de las decisiones sobre resolución de incidentes en la DLP. Por este motivo, la DLP tradicional se percibe hoy como un impedimento para el negocio, en especial cuando se activa el modo de bloqueo, en lugar de considerarse una solución eficaz para la protección de datos. De hecho, la mayoría de las organizaciones la utilizan como una herramienta de descubrimiento de datos y cumplimiento normativo, que funciona en modo de supervisión para evitar problemas.

Estos problemas se solucionan aplicando la confianza cero. La tecnología de protección de datos es necesaria para pasar de un modelo estático formado por políticas fijas predefinidas, sin contexto y sin conocimiento de los riesgos ni de la evolución de los comportamientos, a un enfoque de confianza cero dinámico y adaptable que pueda aprovechar el contexto de seguridad y permitir de forma continua medidas de protección adecuadas, basadas automáticamente en los cambios que puedan producirse.

Para lograr una respuesta de protección de datos automatizada se necesitan procesos establecidos y políticas granulares, además de reglas claras de compromiso, las medidas que haya que adoptar, en qué condiciones y con qué nivel de confianza. La DLP debe integrarse con el mayor número de puntos de control de seguridad, procesar continuamente sus registros y resultados, y aprovecharlos dinámicamente. Una DLP preparada para la confianza cero debe tener en cuenta los riesgos organizacionales de usuarios, dispositivos, datos, redes y aplicaciones para tomar conciencia sobre los riesgos y proporcionar la solución adecuada en todo momento. Por ejemplo, la supervisión del comportamiento de usuarios, dispositivos y aplicaciones proporciona información importante sobre la actividad anómala del usuario, acciones potencialmente maliciosas, aplicaciones peligrosas, ubicaciones de conexión no seguras, posiciones poco seguras e indicadores de compromiso.

05

Para que una solución de protección de datos de confianza cero sea realmente eficaz debe supervisar lo que está pasando y quién hace qué en toda la infraestructura corporativa, incluidas las nubes, los usuarios remotos y los dispositivos no administrados.



Más información

Netskope, líder mundial en ciberseguridad, está redefiniendo la seguridad de la nube, los datos y la red con el objetivo de ayudar a las organizaciones a aplicar los principios de confianza cero para proteger sus datos. La solución Intelligent Security Service Edge (SSE) de Netskope es rápida y fácil de usar, y protege a las personas, los dispositivos y los datos en cualquier lugar.

Conozca la forma en que Netskope ayuda a los clientes a prepararse para cualquier incidencia durante su recorrido hacia la protección de datos.

netskope

©2022 Netskope, Inc. Todos los derechos reservados. Netskope es una marca comercial registrada y Netskope Active, Netskope Discovery, Cloud Confidence Index, Netskope Cloud XD y SkopeSights son marcas comerciales de Netskope, Inc. El resto de marcas comerciales son marcas comerciales de sus respectivos propietarios. 10/22 EB-599-1