APRENDIZAJE SENCILLO

Edición especial de Netskope

DLP Moderno

para dummies
A Wiley Brand

Aprenda técnicas actualizadas de DLP

Utilice los principios *Zero Trust* para proteger los datos a donde vayan

Consiga mayor seguridad en la nube

Presentado por

netskope

Carmine Clementelli

Acerca de Netskope

Netskope, líder mundial en SASE, está redefiniendo la seguridad de la nube, los datos y la red para ayudar a las organizaciones a aplicar principios Zero Trust para proteger los datos. Rápida y fácil de usar, la plataforma Netskope proporciona acceso optimizado y seguridad en tiempo real a personas, dispositivos y datos en cualquier lugar. Netskope ayuda a los clientes a reducir riesgos, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad de aplicaciones en la nube, web y privadas. Miles de clientes, entre los que se encuentran más de 25 de las empresas incluidas en la lista Fortune 100, confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas cambiantes, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red, y los nuevos requisitos normativos. Para saber cómo Netskope ayuda a los clientes a prepararse ante cualquier cosa en su andadura hacia SASE, visita netskope.com.

Nos gustaría mostrar nuestro agradecimiento a una serie de personas que, junto al autor, han hecho posible este libro:

De Netskope: Amanda Anderson, Chad Berndtson, Jason Clark, Scott Hogrefe, Kathy Jacobsen, Naveen Palavalli, Stephenie Pang, Lauren Polito, Carolyn Robinson, Neil Thacker

De Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

DLP Moderno

Edición especial de Netskope

por Carmine Clementelli

para dummies®

DLP Moderno Para Dummies®, Edición especial de Netskope

Una publicación de
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-20764-0 (pbk); ISBN 978-1-394-20765-7 (ebk)

Para obtener información general sobre nuestros productos y servicios, o sobre cómo crear un libro *Para Dummies* personalizado para tu empresa u organización, ponte en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono +1 877 409 4177, ponte en contacto con info@dummies.biz, o visita www.wiley.com/go/custompub. Para obtener información sobre licencias de la marca *Para Dummies* para productos o servicios, ponte en contacto con BrandedRights&Licenses@Wiley.com.

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora del proyecto: Elizabeth Kuball

Editora de adquisiciones: Traci Martin

Director editorial: Rev Mengle

Responsable de cuentas de clientes: Jeremith Coward

Editor de producción: Mohammed Zafar Ali

Colaboración especial: Nicole Sholly

Introducción

La protección de datos como concepto de ciberseguridad no es algo nuevo, pero las exigencias impuestas a los sistemas de protección de datos heredados han cambiado drásticamente en la última década. Antes, los profesionales de la seguridad confiaban en que los valiosos datos que protegían estaban resguardados en centros de datos sólidamente fortificados. Pero con la transformación digital, las empresas, tanto grandes como pequeñas, trasladan sus datos a la nube y los mueven a través de ubicaciones distribuidas. Susdatos se encuentran ahora en todas partes, dondequiera que estén los usuarios. Es posible que su empresa comparta conexiones digitales con un gran número de proveedores, socios y contratistas de terceras e incluso cuartas partes. Estos escenarios traen consigo tanto oportunidades de negocio sin precedentes (buenas noticias) como retos de seguridad, sobre todo en lo que respecta a la protección de datos (no tan buenas noticias).

Las infracciones que consiguen llevarse a cabo pueden tener consecuencias devastadoras para una empresa. Los riesgos procedentes de las personas internas (malintencionadas o negligentes) son tan peligrosos para suempresa como los ataques de agentes externos que acaparan titulares. Todos amenazan con exponer información confidencial. La protección de datos es ahora una piedra angular de las normas de cumplimiento, y existen reglamentos industriales y de privacidad de datos que detallan específicamente las responsabilidades de suempresa y sanciones significativas en caso de incumplimiento.

Las empresas deben adoptar un nuevo enfoque y aplicar políticas de protección de datos allá donde vayan sus datos, y deben hacerlo de forma coherente. Lo ideal es que la protección de datos respalde los objetivos empresariales y, al mismo tiempo, proteja a la empresa. Pero gestionar las políticas de protección de datos y las herramientas necesarias para hacerlas cumplir puede ser complejo y costoso. Las organizaciones necesitan soluciones de protección de datos que simplifiquen la aplicación de las políticas y, al mismo tiempo, garanticen su eficacia. Una nueva generación de soluciones de prevención de pérdida de datos (DLP) en la nube es una solución posible. Las organizaciones deben adoptar una solución en la nube que sea menos compleja, altamente escalable y más rentable, a la vez que, idealmente, proteja los datos con mayor fiabilidad y precisión, y minimice la exposición a accesos no autorizados o usos indebidos. Es un equilibrio difícil de alcanzar, pero puedes lograrlo hoy mismo con la orientación adecuada.

Acerca de este libro

Este libro puede prepararlo para tomar decisiones informadas sobre cómo evaluar el enfoque actual de suorganización respecto a la protección de datos y evaluar nuevas soluciones de protección de datos para encontrar la que mejor se adapte a sus necesidades, utilizando los principios de *Zero Trust* (confianza cero) para guiar cómo se aplica la seguridad de forma contextual y coherente. Al explicar cómo funcionan los actuales sistemas DLP en la nube, este libro se desmarca de la maraña de marketing para identificar las características y capacidades necesarias para proteger tus datos de forma fiable en cualquier lugar donde se utilicen.

Algunas suposiciones obvias

Este libro asume que tiene un conocimiento básico de cómo las empresas han adoptado el uso de la informática en la nube para ser flexibles y estar mejor equipadas a la hora de implantar la transformación digital. También supone que está aquí porque desea garantizar la combinación adecuada de tecnología y mejoras en los procesos para proteger los datos confidenciales dondequiera que residan y dondequiera que se muevan en su entorno informático.

Iconos utilizados en este libro

Utilizamos iconos para llamar la atención sobre información importante. Esto es lo que puede encontrar:

CONSEJO

Cualquier cosa marcada con el icono «Consejo» es un atajo para facilitar una tarea concreta.

RECUERDA

El icono «Recuerda» le ofrece información que es especialmente importante conocer.

CUESTIÓN TÉCNICA

Cuando ofrecemos información muy técnica que puede omitir, utilizamos el icono «Cuestión técnica».

ADVERTENCIA

Preste atención a cualquier cosa que lleve el icono «Advertencia» para ahorrarle alguno que otro dolor de cabeza.

Más allá del libro

Aunque este libro está repleto de información, si al final piensa: «¿Dónde puedo encontrar más información?», visita `www.netskope.com`.

EN ESTE CAPÍTULO

- **Saber dónde se almacenan los datos confidenciales y cómo se controlan**
- **Descubrir en qué consiste realmente la protección de datos**
- **Aprender qué es la prevención de pérdida de datos (DLP)**
- **Averiguar por qué el DLP heredado ya no es una solución viable**
- **Cambiar a una estrategia que da prioridad a la nube con una solución DLP moderna**
- **Desmontar los mitos más habituales sobre el DLP**

Capítulo 1
Los datos confidenciales están en todas partes y son más difíciles de encontrar

En general, cuando se habla de datos confidenciales, se hace referencia a información de carácter privado o personal. Definir qué es confidencial depende en gran medida de si los datos se analizan desde una perspectiva empresarial o individual.

Guía rápida sobre los datos confidenciales

Se habrá dado cuenta de que la mayoría de los datos clasificados como confidenciales han existido de alguna forma durante años, décadas o incluso más tiempo:

- Datos/información personal como números de la Seguridad Social, números de tarjetas de crédito, números de carnés de conducir, datos sanitarios y las direcciones de domicilios particulares

- Propiedad intelectual (PI), como diseños de productos, nuevas invenciones, patentes y código fuente
- Información confidencial y secretos comerciales, como planes financieros, contratos, informes fiscales, información sobre fusiones y adquisiciones, y documentos antes de su publicación, como comunicados de prensa

La novedad es que el panorama empresarial moderno ha cambiado por completo la forma en que se comparten y (¡buf!) se exponen los datos. Muchas empresas, especialmente tras el inicio de la pandemia de COVID-19, adoptan ahora un entorno de trabajo híbrido.

Casi todos los tipos de datos confidenciales se crean, almacenan y mueven digitalmente. Los datos viajan hacia y desde los servicios en la nube, las redes corporativas y cualquier otro lugar al que los usuarios puedan acceder. Al mismo tiempo, un número cada vez mayor de aplicaciones almacena y comparte esos datos en múltiples plataformas, haciéndolos accesibles desde prácticamente cualquier dispositivo en ubicaciones remotas. A medida que la cantidad, variedad y velocidad de los datos aumenta exponencialmente, resulta cada vez más difícil identificar y proteger la información confidencial. Para empeorar las cosas, el enorme volumen de datos disponibles dificulta que las medidas de seguridad tradicionales estén a la altura de las nuevas amenazas constantes.

Un maremoto de datos

Para 2025, según IDC, el mundo estará inundado de nada menos que ¡181 zettabytes de datos! Una enorme parte se creará y almacenará directamente en la nube (creciendo cada año que pasa). Entre los retos a los que se enfrentan los sistemas de protección de datos y sus operadores se encuentran los siguientes:

- **Demasiadas categorías de datos confidenciales:** el aumento de las normativas y leyes sobre privacidad de datos que protegen a un mayor número de personas y tipos de información en todo el mundo está impulsando un crecimiento masivo de las categorías de datos confidenciales. Esto incluye información que puede identificar a una persona, como su ubicación, información financiera y sanitaria, preferencias personales, creencias religiosas y orientación sexual. Los datos confidenciales incluyen cosas como los números del carné de identidad, tarjetas de crédito, código fuente, diseños, planes financieros, cuentas bancarias, contratos, formularios fiscales, contraseñas, información de fusiones y adquisiciones, información sanitaria protegida (ISP),

correos electrónicos personales, género y religión. Hay categorías de datos confidenciales que difieren de un país a otro, en idiomas localizados, y que son específicas de cada país.

- **Demasiados formatos y tipos de datos:** PDF, imágenes gráficas (como JPG, PNG y BMP), archivos comprimidos y encapsulados (como ZIP, RAR e ISO), archivos adjuntos, mensajes de Slack, chats, formularios en línea, capturas de pantalla, hojas de cálculo, diseño asistido por ordenador (CAD), publicaciones en redes sociales, archivos de texto, presentaciones y correos electrónicos.
- **Demasiado contexto:** el contexto debe regir la decisión sobre cómo acceder, utilizar, transferir y compartir de forma segura los datos confidenciales. El contexto ayuda a definir lo que sería una acción de riesgo en torno a los datos confidenciales y lo que debería considerarse una infracción o un intento de filtración: quién, dónde, qué, cómo, por qué, cuándo, a quién y otros factores.

Frente a una oleada de datos inescrutables, los sistemas de seguridad heredados se ven obligados a pecar de precavidos, lo que ha aumentado los quebraderos de cabeza administrativos en órdenes de magnitud. ¿Por qué? Los equipos de seguridad de respuesta ante incidentes se enfrentan a un aluvión de falsos positivos, la mayoría de los cuales deben ser evaluados manualmente por un personal ya de por sí agobiado de trabajo.

La protección de datos es mucho más que «simples» datos

Las empresas necesitan nuevas estrategias automatizadas que puedan identificar, supervisar y proteger eficazmente sus valiosos datos. Al mismo tiempo, el mundo en el que opera la protección de datos sigue introduciendo nuevos retos que agravan el predicamento de la seguridad. Estos nuevos retos incluyen:

- **Más riesgos cibernéticos:** las empresas son ahora más vulnerables que nunca a las filtraciones de datos. Estas vulnerabilidades pueden ser tanto intencionadas como no intencionadas. El comportamiento interno, como el robo o la manipulación incorrecta (¡vaya!) por parte de los empleados, es una de las formas en que la información confidencial de una empresa corre riesgo de ser explotada. En el 82 % de las filtraciones de datos interviene el elemento humano, que incluye:
  - *Personas internas malintencionadas:* por ejemplo, un empleado descontento que haga capturas de pantalla de una hoja de

cálculo crítica, que envíe datos a una instancia de aplicación de *software* como servicio (SaaS) de almacenamiento personal o a través de una instancia personal de una cuenta de correo electrónico corporativa (es decir, Gmail personal frente a Gmail corporativo).

- *Exposición involuntaria:* por ejemplo, un empleado que, sin darse cuenta, envía demasiada información a un proveedor o que, por negligencia, comparte demasiados archivos en una carpeta de OneDrive. Estas son causas importantes de filtraciones de datos.

Del mismo modo, los ataques externos o los intentos de pirateo informático también ponen en peligro los secretos de la empresa, ya que pueden pedir rescates o ser revelados al público o a organizaciones de la competencia.

- **La nube, incluidos el SaaS y la infraestructura como servicio (IaaS) en la nube pública:** la adopción de aplicaciones SaaS, en particular, está aumentando a un ritmo vertiginoso. Según estudios recientes, la empresa media utiliza más de 2400 aplicaciones en la nube, de las que el 97 % se considera *TI en la sombra* (no autorizadas por el departamento de TI, desconocidas o invisibles para él). Esto plantea retos técnicos y de seguridad, ya que los datos pueden almacenarse y compartirse a través de un gran número de aplicaciones SaaS, se mueven por las redes corporativas y los dispositivos gestionados, y los empleados –e incluso los usuarios externos que se conectan desde ubicaciones remotas con dispositivos no gestionados– pueden acceder a ellos fácilmente. Las aplicaciones en la nube pueden convertirse rápidamente en un vector de ataque primario si no se supervisan y gestionan adecuadamente. Las empresas deben tomar medidas para actualizar sus soluciones de protección de datos a fin de protegerse contra tales amenazas.
- **Trabajo híbrido:** el aumento del trabajo híbrido está cambiando la forma en que las empresas almacenan y acceden a los datos confidenciales. Las cosas han cambiado drásticamente desde los días en que las empresas guardaban la mayor parte de la información crítica en un centro de datos privado controlado por la empresa. Las disposiciones del trabajo híbrido han traído una nueva era en la que los datos confidenciales están muy distribuidos en lugares más allá de las fronteras corporativas, lugares que la empresa no puede ver y no controla. Hoy en día, los datos están repartidos por diversos entornos, tanto digitales como

físicos, como centros de datos, sedes corporativas, sucursales, oficinas domésticas y dispositivos de trabajadores remotos (corporativos y personales).

- **Nuevos requisitos de cumplimiento:** el cumplimiento siempre ha sido una preocupación, pero a medida que las empresas están más reguladas y la legislación sobre privacidad de datos conlleva multas y acciones legales cada vez más cuantiosas, las empresas de todos los tamaños sienten la presión de garantizar que cumplen las normas de cumplimiento y protegen sus datos confidenciales. Las empresas deben tomar medidas para cumplir las normativas de todo el sector, siendo las más populares el estándar de seguridad de datos de la industria de tarjetas de pago (PCI-DSS), la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA) y la Ley de Gramm-Leach-Bliley (GLBA), al tiempo que se aseguran de cumplir las leyes y normativas aplicables en materia de privacidad de datos, como el Reglamento General de Protección de Datos (RGPD), la Ley de Privacidad del Consumidor de California (CCPA), la Ley de Privacidad de Colorado, la Ley de Privacidad de Datos de Connecticut, la Ley de Protección de datos de los Consumidores de Virginia y la Ley de Privacidad de Datos de los Consumidores de Utah, por nombrar solo algunas. Muchos países de todo el mundo están regulados por leyes de privacidad, entre ellos Brasil, Singapur, Japón y el Reino Unido. Ahora más que nunca, las empresas tienen que demostrar que están tomando las medidas necesarias para proteger la información personal de sus clientes y cumplir todas las políticas legislativas pertinentes, so pena de enfrentarse a graves sanciones.
- Un talento que abunda poco y es costoso: el talento especializado y cualificado necesario para ejecutar programas complejos de protección de datos escasea. Las tecnologías de protección de datos requieren una supervisión hábil para hacer frente a la ingente cantidad de incidentes que provoca el sistema. Ese problema se agrava cuando los sistemas de protección de datos heredados supervisan servicios en la nube como aplicaciones SaaS (algo para lo que no fueron diseñados inicialmente), lo que provoca un mayor número de falsos positivos y, en consecuencia, mucho trabajo adicional para el equipo. En función de las competencias requeridas, este personal informático cualificado percibe salarios elevados, lo que puede suponer un costo considerable para las empresas, tanto si se quedan en la empresa y hay que pagarles como si trabajan en exceso, se marchan y hay que sustituirlos.

¿Qué es el DLP y cómo puede ayudar?

Las tecnologías de seguridad DLP son sistemas diseñados para descubrir y proteger automáticamente el almacenamiento, el tránsito y el uso de los datos confidenciales en cualquier lugar de las redes, los usuarios y los servicios de una organización. La tecnología se aplica para detectar una amplia variedad de datos confidenciales, como datos personales/información de clientes y empleados, documentos financieros y propiedad intelectual. El DLP supervisa cómo se accede a esos datos y cómo se utilizan, evitando pérdidas, exposiciones accidentales y robos. El DLP ayuda a las empresas a mitigar sus riesgos de filtración de datos y a auditar sus archivos para evitar la publicación accidental de información confidencial. A medida que el panorama del cumplimiento normativo se ha ido ampliando y volviéndose más estricto, el DLP se ha convertido en una medida de seguridad cada vez más importante para que las empresas se protejan frente a las costosas filtraciones de datos y satisfagan las exigencias de la legislación en materia de cumplimiento de normativas.

Por qué el DLP heredado es ahora lamentablemente inadecuado

Las soluciones DLP heredadas se han utilizado para la protección de datos durante más de diez años. Sin embargo, con el paso del tiempo, el DLP heredado se ha ganado la reputación de ser complejo de implementar y gestionar, costoso, de alcance limitado, cada vez menos preciso y de no proporcionar la cobertura integral necesaria para el mundo actual del trabajo desde cualquier lugar. Las soluciones DLP se diseñaron para proteger los datos dentro de un centro de datos y las instalaciones de una empresa. Estas soluciones han tenido dificultades para adaptarse a los cambios que ha traído la era de la nube. El DLP heredado es bueno para lo que fue diseñado, pero ahora se le pide que haga un trabajo para el que nunca fue concebido: proteger los datos en la nube o mientras se mueven de unas nubes a otras. Además, su modelo basado en el perímetro no puede seguir el ritmo de los datos dispersos en múltiples ubicaciones y aplicaciones.

Los inconvenientes de los sistemas DLP heredados

La implementación y mantenimiento de los sistemas DLP heredados, formados por varios componentes de *software* y *hardware*, puede ser engorrosa. La instalación puede ser compleja y costosa, lo que no es ideal para empresas con un presupuesto o recursos informáticos limitados. La cobertura de empresas muy distribuidas es también un reto

importante y costoso, porque lo más probable es que la arquitectura DLP local deba replicarse en cada sucursal. E incluso así, el enfoque no cubre importantes requisitos modernos, como los empleados remotos, la nube y la flexibilidad del BYOD «traer su propio dispositivo».

Las tecnologías DLP heredadas también necesitan largas actualizaciones de *software* y ajustes continuos que crean interrupciones en el negocio que no se pueden simplemente ignorar. Debido a este trastorno, las organizaciones suelen evitar las actualizaciones; las organizaciones pueden encontrarse con un retraso de meses o años en las versiones de DLP, lo que significa que no están utilizando la protección más reciente frente a las últimas exigencias de los datos, el cumplimiento normativo y los riesgos.

No actualizar ni aplicar parches a un sistema DLP puede dar lugar a varios problemas que ninguna organización desea, como vulnerabilidades de seguridad, filtraciones de datos y una protección de datos inadecuada. Esto puede poner en peligro datos confidenciales y hacer que una organización no cumpla la normativa de protección de datos. Además, la complejidad inherente al DLP heredado suele dar lugar a prácticas de protección de datos incoherentes y excesivamente específicas, lo que provoca un uso ineficiente de los recursos y el tiempo.

ADVERTENCIA

Para algunas empresas, la interrupción del negocio causada por su sistema DLP heredado se considera tan grave que cambiarán sus sistemas DLP al modo «solo supervisión», lo que significa que el sistema observa lo que ocurre pero no aplica la política de protección de datos. Si utiliza el DLP sin aplicar una política es como si tuviera una caja fuerte pero abierta y esperando que nadie se lleve el dinero, las joyas y los documentos importantes.

El problema de los falsos positivos

Los sistemas DLP heredados no solo imponen implementaciones y procesos complicados, sino que también necesitan muchos recursos y mano de obra humana para supervisarlos y ajustarlos continuamente de forma eficaz. Antes he mencionado la presión que los falsos positivos ejercen sobre los equipos de seguridad, pero merece la pena analizar la situación con más detalle.

El número de incidentes que hay que reparar manualmente ha crecido hasta un punto en el que el equipo de respuesta ante incidentes no es capaz de evaluarlos todos, y mucho menos de ocuparse de ellos. Los equipos de respuesta ante incidentes reciben muchas alertas que en realidad no son problemas y carecen de contexto para determinar su nivel de riesgo *a posteriori* (básicamente, reciben estas alertas demasiado

tarde, después de que se haya producido un incidente, por lo que no solo las alertas no tienen contexto, sino que además se pide a los equipos que resuelvan incidentes que tuvieron lugar en el pasado; incluso si contactan con los empleados que los causaron, estos ya no se acordarían de lo ocurrido). Estas alertas pueden ascender a miles o cientos de miles diarias y proceder de fuentes muy diversas. Como están ocurriendo tantas cosas, los equipos de respuesta de seguridad simplemente no pueden evaluar todas estas alertas; de hecho, necesitan pasar por alto muchas de ellas simplemente para poder seguir el ritmo de la empresa.

Un factor importante es que los datos ahora residen y se mueven en y entre muchos lugares fuera de la red del centro de datos gestionado. Las soluciones DLP heredadas no están equipadas para gestionar la creciente variedad y cantidad de datos y carecen de la detección asistida por aprendizaje automático más reciente, los casos de uso compartido de datos modernos y el conocimiento del contexto. Sus políticas estáticas no pueden ajustarse eficazmente a los cambiantes riesgos y contextos empresariales, como quién utiliza los datos, de qué manera, en qué entorno e instancia de aplicación, si muestran un comportamiento seguro y cuál es el destino final.

Las herramientas de automatización y orquestación de la ciberseguridad, como el análisis del comportamiento de entidades y usuarios (UEBA), se han incorporado para ayudar parcialmente, ya que recogen las alertas y las solucionan con mayor rapidez. Sin embargo, si el sistema DLP es impreciso, carece de contexto empresarial, desconoce el riesgo y tiene muchas lagunas, los modelos UEBA no funcionarán bien.

Para proteger eficazmente los datos confidenciales, un sistema DLP debe estar integrado y automatizado para supervisar y verificar continuamente la identidad de las personas y los dispositivos autorizados, su comportamiento, su colaboración e intercambio de datos externos, las aplicaciones que utilizan y sus riesgos, y muchos otros factores contextuales. Este enfoque de confianza cero (consulta el capítulo 3) permite recomendaciones de políticas precisas y reglas de respuesta ante incidentes que se adaptan a los cambios en las condiciones de riesgo y al contexto empresarial específico en el que se utilizan los datos. Este enfoque no interrumpe las prácticas empresariales modernas, sino que permite realizarlas con seguridad.

El DLP heredado carece de cobertura crítica en la nube

Los sistemas DLP heredados se diseñaron con un modelo de seguridad basado en el perímetro que asume que todos los datos se almacenan dentro de la red corporativa y los entornos gestionados. Este modelo

ya no es suficiente en la era de la nube, en la que los datos se almacenan en múltiples ubicaciones basadas en la nube y a los que acceden usuarios y dispositivos fuera de la red corporativa. Además, los sistemas DLP heredados pueden no haber sido diseñados para integrarse con la amplia gama de servicios e infraestructuras en la nube que se utilizan actualmente, lo que dificulta o imposibilita la protección integral de los datos en la nube.

La incorporación de tecnologías adicionales, como el agente de seguridad para el acceso a la nube (CASB) y las puertas de enlace web seguras (SWG) en la nube, a un sistema DLP implementado a nivel local puede proporcionar cierta cobertura adicional para los repositorios en la nube, pero no resolverá las limitaciones fundamentales del sistema heredado. Los equipos se enfrentan además al reto de tener que abordar consolas de gestión inconexas y políticas de protección de datos desordenadas, dos efectos secundarios habituales cuando CASB y SWG se unen al DLP heredado.

Es decir, añadir tecnologías adicionales a un método DLP anticuado no lo prepara para la nube y solo añade complejidad. Un sistema DLP debe ser capaz de cumplir las normas en constante evolución de la seguridad en la nube de forma adaptable, con sus propias políticas dinámicas y capacidades de evaluación de riesgos en tiempo real, para que las empresas puedan mantener la seguridad de sus empleados, sus clientes y sus datos. Las soluciones DLP heredadas se implementan a nivel local. Sin más.

RECUERDA

Para proteger los datos en la nube, el DLP heredado debe integrarse elegantemente con las soluciones de seguridad en la nube. Los datos en la nube necesitan seguridad en la nube.

CUESTIONES TÉCNICAS

En la mayoría de las empresas actuales, hay dos soluciones de seguridad en la nube que suelen combinarse con el DLP heredado: CASB para el tráfico de aplicaciones en la nube y SWG para el tráfico web de trabajadores remotos y en sucursales. Estas soluciones están diseñadas para la nube, pero suelen tener capacidades limitadas de protección de datos. La esperanza es que la integración de estas soluciones proporcione al DLP heredado el «ojo en la nube» necesario para ampliar allí sus actuales capacidades locales y buscar datos confidenciales fuera del perímetro del centro de datos. Por desgracia, esta integración ha demostrado ser muy difícil, ya que implica un redireccionamientos del tráfico de red que depende del complicadísimo Protocolo de Adaptación de Contenidos de Internet (ICAP), que, afortunadamente, queda fuera del alcance de este libro.

Incluso cuando se logra la integración, el planteamiento no resulta sostenible. Por un lado, los CASB utilizan interfaces de programación de aplicaciones (API) para conectarse a aplicaciones corporativas en la nube como Microsoft 365, Salesforce, Slack, Zoom, Teams, Google Workspace, Amazon Web Services (AWS) y Box. Estas API proporcionan al sistema DLP heredado la ventana deseada para ver dentro de estas aplicaciones en la nube. Así, por ejemplo, si hay datos confidenciales almacenados en Salesforce, el DLP puede escanearlos y protegerlos. Los CASB también utilizan la detección en línea para examinar las cargas y descargas de datos en miles de aplicaciones SaaS.

También es difícil consolidar las políticas de protección de datos entre los sistemas locales y en la nube. Por ejemplo, los CASB a menudo no pueden duplicar las mismas políticas que los DLP heredados. Como estas tecnologías no tienen las mismas capacidades, las políticas y las consolas de gestión se fragmentan y desincronizan.

El problema de esta arquitectura es que la integración de un DLP local a través de CASB con una aplicación en la nube también crea un retraso denominado *latencia*. La latencia significa que incluso si su DLP heredado descubre una infracción de los datos en la nube, puede tardar minutos, horas o incluso más en organizar una respuesta. Piense en esta situación: la infracción se ha producido, se ha detectado, pero aún así, no la ha detenido a tiempo (¡lo que significa que sus datos están en peligro!).

En última instancia, combinar el DLP heredado con las tecnologías en la nube es como intentar combinar dos animales diferentes. Uno es un servicio en la nube (CASB), y el otro es una implementación masiva de *hardware* y *software* a nivel local (DLP heredado). El resultado es una quimera frágil que es fácil de romper, causa mucha latencia y es muy difícil de optimizar y mantener. Lo ideal sería deshacerse de esa complejidad y agilizar y simplificarlo todo para que haya menos probabilidades de que se produzcan problemas.

El hecho de estar anclada a la infraestructura local y carecer de medios para escalar de forma rápida y rentable limita significativamente la eficacia del DLP heredado en entornos de nube. Este planteamiento ya no es sostenible.

RECUERDA

Para que el DLP sea eficaz, la atención debe desplazarse del perímetro exterior del conjunto de datos a los propios datos, al lugar donde se mueven y a cómo se mueven. Las empresas ya no pueden confiar en las estrategias de DLP heredadas si esperan proteger eficazmente su información en la nube.

DLP para la era de la nube

La transformación digital ha revolucionado la forma en que las organizaciones prestan servicios al cliente y desarrollan productos y servicios. También ha tenido un impacto inmenso en la forma de proteger los datos. Las grandes y pequeñas empresas dependen en gran medida de la tecnología en la nube para lograr el crecimiento y la habilitación del negocio, por lo que las estrategias de seguridad deben seguir el ritmo de estos cambios. La arquitectura DLP debe adaptarse al crecimiento constante del trabajo híbrido cambiando a una estrategia que dé prioridad a la nube para ofrecer una cobertura más amplia, mayor eficiencia, escalabilidad, potentes capacidades informáticas y medidas de prevención de riesgos más eficaces. Con un modelo DLP replanteado, las organizaciones modernas pueden tener éxito en el mundo del trabajo híbrido y preparar a sus empresas para el futuro. Modernizar el DLP de su empresa requiere muchísimo trabajo y esfuerzo, pero con los riesgos en constante evolución y los avances en las soluciones DLP preparadas para la nube, ahora es el momento adecuado para planteárselo.

Con el DLP en la nube, no tiene que implementar nada que sea complicado, solamente habilitar un servicio en la nube . No tiene que lidiar con muchos componentes ni *software* que necesite actualizar y mantener manualmente. Ya no hay bases de datos DLP que mantener ni expertos en bases de datos que contratar. Ya no hay servidores DLP que se queden obsoletos y deban sustituirse. Y ya no hay *proxies* de *hardware* que deban actualizarse.

Las plataformas de protección de datos en la nube están diseñadas para integrarse fácilmente en la seguridad, las redes, la infraestructura y los servicios en la nube, al tiempo que recopilan de otros controles, el riesgo y el contexto organizativo de forma coherente. Los algoritmos de vigilancia y detección de datos funcionan mejor en la nube, donde el acceso a recursos infinitamente escalables reduce la carga de su infraestructura informática a la vez que mantiene el ritmo de los nuevos casos de uso y de sus innumerables y cada vez más numerosos agentes de *endpoints*. Ya no estará limitado por una infraestructura local, por lo que sus usuarios estarán protegidos dondequiera que vayan.

Además, como una arquitectura en la nube no está vinculada a su infraestructura ni a sus horarios, tu DLP se mantiene al día, con actualizaciones en tiempo real disponibles en cualquier lugar. Este enfoque constituye una herramienta mucho más eficaz para proteger los valiosos datos de su organización.

La caída de los mitos

En lo que respecta al DLP en la nube, no es ningún secreto que el mercado está saturado de palabras de moda, promesas infladas y jerga tecnológica, lo que hace que la gente se sienta abrumada y confundida por las opciones a su alcance. Pero lo cierto es que no todas las soluciones DLP son iguales. En este libro, le ayudo a distinguir entre la realidad y el bombo publicitario a la hora de sopesar sus opciones, con una guía de las características y funcionalidades más importantes de cada una de ellas.

Así pues, demos un paso atrás y empecemos por desmentir algunos mitos habituales en torno a la protección de datos ofrecida desde la nube, para que pueda abrirse paso entre el ruido y tomar una decisión informada y perfectamente adaptada a su empresa.

El mito: el nuevo DLP es el mejor DLP

La realidad: cuando se trata de programas de protección de datos, no hay que dejar nada al azar. No solo se necesitan suficientes funciones dentro del programa para garantizar la seguridad, sino también un proveedor dedicado y bien informado con experiencia consolidada en DLP. Puede que las soluciones heredadas no se construyeran pensando en la tecnología de la nube, pero pueden enseñar lecciones sobre madurez a la mayoría de las soluciones DLP distribuidas en la nube.

La solución de protección de datos más fiable ha pasado por un largo periodo de maduración y ha desarrollado nuevas funciones por el camino. Si está pensando en invertir en un programa integral de protección de datos, asegúrese de que su proveedor pueda satisfacer todas sus necesidades, desde la compatibilidad con la nube hasta la madurez de las funciones, para lograr la máxima seguridad de los datos. No hay que confundir la solución más reciente de un proveedor con la mejor.

El mito: el DLP heredado era impreciso

La realidad: los DLP heredados fueron creados por proveedores que invirtieron una década o más en desarrollar algoritmos y políticas precisas para identificar e impedir la transferencia no autorizada de información confidencial.

La precisión no es el verdadero problema. El verdadero problema, como ya he mencionado antes en este capítulo, son los falsos positivos. Los falsos positivos pueden llevar a una situación peligrosa en la que las amenazas reales pasen desapercibidas y se filtren accidentalmente datos confidenciales. También hacen que los equipos de respuesta ante incidentes cualificados (es decir, caros) sean cada vez más grandes para

hacer frente a un mayor volumen de incidentes. En el capítulo 2, hablo de por qué los sistemas DLP deben ser precisos y exactos para mantener la confianza.

El mito: cuando se trata del DLP, basta con «ser bastante bueno»

La realidad: cuando se trate de garantizar la seguridad de los datos de su empresa, no escatimes esfuerzos. ¿Está pensando en utilizar una solución en la nube que promete una seguridad «bastante buena»? Piénselo dos veces. Puede acabar con un conjunto de funciones reducido o con un método limitado a los vectores de ataque y tipos de datos más superficiales, lo que lo expone al riesgo de actividades maliciosas, falsos positivos y detección imprecisa.

En lugar de eso, invierta en un sistema DLP moderno en la nube que ofrezca una gran precisión en la detección de datos, proporcione capas de seguridad adicionales y garantice una protección completa frente a posibles amenazas para sus datos empresariales u otro material confidencial. No juegue al despiste con los datos de su empresa; asegúrese de invertir en el sistema DLP adecuado para obtener la máxima seguridad y rendimiento.

El mito: el DLP en la nube rinde menos que el DLP heredado

La realidad: en la actualidad, muchos sistemas DLP en la nube utilizan menos de 100 identificadores de datos (consulta el capítulo 2) y analizan solo unos pocos tipos de archivos, lo que significa que apenas detectan nada. La razón es la falta de madurez de la tecnología. A diferencia de los sistemas DLP desarrollados y en funcionamiento desde hace una década, estos sistemas se han diseñado para centrarse en resolver nuevos casos de uso específicos, como aplicaciones concretas en la nube, y protegen solo unos pocos tipos de archivos populares. Esta falta de amplitud de miras significa que siguen careciendo de la precisión necesaria para equilibrar eficazmente la protección de datos y las necesidades empresariales, lo que provoca continuas fricciones entre ambas. La tecnología DLP en la nube debería ser superior al DLP heredado debido a su capacidad para ofrecer una escala masiva. Es lógico pensar que, a mayor escala, se podrían resolver los falsos positivos y mejorar la precisión.

ADVERTENCIA

Cuando se trata de protección de datos, el viejo dicho es cierto: «¡La experiencia cuenta!». Aunque las nuevas y tentadoras opciones pueden parecer estupendas sobre el papel o a primera vista, las soluciones DLP maduras pueden ofrecer un nivel más profundo de seguridad y

conocimiento porque han crecido y se han perfeccionado con el tiempo. Apueste por un proveedor acreditado y pruebe usted mismo varios sistemas para estar totalmente tranquilo a la hora de proteger sus datos esenciales.

El mito: un paquete de sistemas de protección de datos es tan bueno como una solución de protección de datos completa e integrada

La realidad: cuando se trata de protección de datos, las iniciativas y programas de seguridad que intentan agrupar una serie de productos y servicios DLP independientes de distintos proveedores pueden parecer un avance lógico. Al fin y al cabo, los servicios DLP pueden venir ya integrados con determinadas aplicaciones SaaS, servicios de nube pública, cortafuegos y soluciones SWG. Pero por supuesto, tarde o temprano, estos programas de protección de datos multiservicio se quedarán cortos. Al reunir sistemas independientes que no se desarrollaron conjuntamente, la solución puede ofrecer poca información sobre el contexto empresarial y los riesgos. Además, los profesionales de la protección de datos acabarán abordando políticas de protección de datos inconexas y múltiples consolas. De hecho, el alcance de cada servicio DLP integrado suele limitarse a entornos y canales específicos, abarcando, por ejemplo, solo el tráfico web o puntos de control concretos, como una o unas pocas aplicaciones SaaS. Esto dejará sus datos vulnerables una vez que estén a la vista de todos.

Para protegerse usted mismo y proteger a su organización, busque soluciones totalmente integradas que ofrezcan una protección de datos completa para cubrir todas las áreas potenciales de riesgo en los servicios en la nube, las ubicaciones locales, los servicios de correo electrónico y los *endpoints*, y obténga una cobertura total a través de múltiples tipos de datos y controles.

EN ESTE CAPÍTULO

- **Conocer los retos a los que se enfrenta la prevención de pérdida de datos (DLP) heredada**
- **Prepararse para posibles cambios y crecimientos futuros**
- **Conocer las realidades y limitaciones del DLP en la nube**
- **Comprender cómo el DLP aumenta la eficacia de otras herramientas de seguridad**

Capítulo 2
Protección de toda la empresa centrada en la nube

¿Por qué es importante que los sistemas de protección de datos de una organización protejan a toda la empresa, incluidas sus aplicaciones en la nube? Porque la pérdida o el acceso no autorizado a los datos puede tener graves consecuencias para la organización y las partes interesadas. Este planteamiento puede parecer obvio, pero en la práctica hay muchas fuerzas que actúan en contra de este objetivo. En este capítulo, explico por qué conseguir una protección de datos completa en toda la empresa es un proceso que genera ganancias rápidas y beneficios estratégicos a largo plazo.

Empresas sin fronteras

Hace una década, el concepto de empresa se definía sobre todo por los límites físicos de un edificio o ubicación. Esto incluía normalmente a los empleados, el equipamiento y los recursos contenidos dentro de esas paredes. Sin embargo, la definición de empresa ha evolucionado con el tiempo para reflejar la naturaleza cambiante de los negocios y la tecnología: la empresa ya no se limita a una ubicación física.

Con el aumento del trabajo remoto, es probable que haya datos valiosos que crucen los dispositivos y las redes personales de sus empleados. Con el auge de los servicios en la nube, sus datos pueden estar dispersos en diversas ubicaciones en la nube, incluidas aplicaciones de software como servicio (SaaS) como Microsoft 365 y Salesforce, así como en conversaciones en línea en aplicaciones de colaboración como Slack y Microsoft Teams (consulta la figura 2-1). El ámbito de la empresa incluye hoy en día los numerosos *endpoints* que los empleados utilizan para conectarse a los recursos corporativos, así como las miles de aplicaciones en la nube aprobadas y (¡ejem!) no aprobadas que pueden utilizarse dentro de las empresas.


ADVERTENCIA

Si no sabe que existen datos confidenciales ni dónde se encuentran, no puede protegerlos. Si sabe que existen datos confidenciales pero no sabe dónde residen ni adónde viajan, sigue sin poder protegerlos.


RECUERDA

Para garantizar que todos los datos confidenciales se detecten y protejan independientemente de dónde residan o adónde viajen, es necesario adoptar un enfoque exhaustivo para detectarlos y protegerlos. Esto supone la ausencia de lagunas en la cobertura y de puntos ciegos por los que los datos podrían exfiltrarse o quedar expuestos accidentalmente sin su conocimiento.

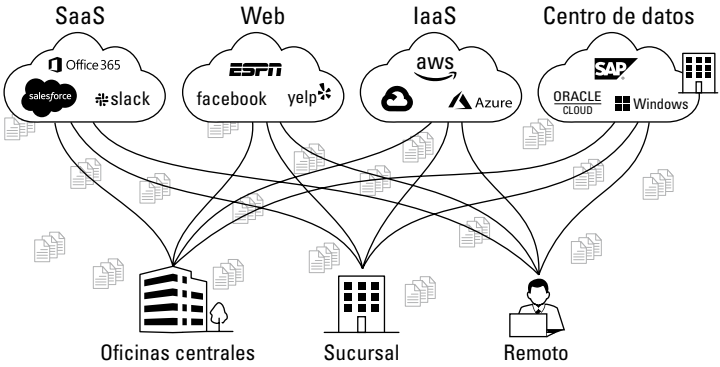

FIGURA 2-1: En la empresa actual sumamente distribuida, los datos residen y se mueven a través de muchos entornos nuevos.

El reto al que se enfrenta el DLP según va evolucionando

Como ya he explicado en el capítulo 1, los sistemas DLP se han centrado principalmente en proteger los datos almacenados *dentro de* un centro de datos corporativo. Hoy en día, es importante proteger los datos allá

donde vayan, ya sea en la nube, en dispositivos remotos, a través de la red corporativa o en ubicaciones externas. Esto significa que los sistemas DLP heredados, que se diseñaron para proteger los datos dentro de la empresa, ya no son suficientes.

RECUERDA

Aunque es necesario que identifique todas las ubicaciones en las que residen y se mueven los datos, si la protección de datos se centra en los propios datos y no en las ubicaciones en las que se originan y almacenan, puede obtener enormes ventajas de flexibilidad y eficacia. Piénsalo como si un equipo de baloncesto pasara de una defensa «en zona» a una defensa «hombre a hombre». Como explicaré más adelante, si adopta este enfoque exhaustivo, podrá proteger su información confidencial y alejarla de las manos equivocadas.

Cualquier sustitución de un sistema DLP heredado debe proporcionar a la empresa una cobertura completa, tanto de los canales en la nube como de los canales tradicionales a nivel local. Incluso la mayoría de las soluciones actuales de DLP en la nube se han diseñado para cubrir únicamente canales locales específicos. Pueden dirigirse a una red o a un conjunto determinado de *endpoints* o aplicaciones específicas, pero no abordan toda la variedad de casos de uso modernos.

Para proporcionar una cobertura empresarial completa, una solución DLP debe proteger todas las transmisiones de datos desde y hacia cualquier ubicación y dispositivo. Esto incluye dispositivos gestionados y no gestionados en todos los lugares donde se encuentren los usuarios, tanto dentro como fuera de la red corporativa, así como en aplicaciones SaaS, infraestructura como servicio (IaaS), correo electrónico, aplicaciones privadas y *endpoints*. Esto requiere una solución DLP completa y flexible que pueda adaptarse a las necesidades en constante evolución de una empresa sumamente distribuida.

En los apartados siguientes, examino los aspectos clave a la hora de diseñar una solución DLP para la nueva empresa sin fronteras.

Escalabilidad y garantía de futuro

No hace mucho tiempo, el uso de aplicaciones SaaS era bastante limitado en la empresa, pero con el tiempo, ha habido un aumento significativo en el número de aplicaciones SaaS utilizadas por los empleados dentro de las empresas. Hoy en día, no es raro que las empresas utilicen cientos de aplicaciones SaaS aprobadas, y los empleados pueden estar utilizando miles de aplicaciones adicionales de las que la empresa ni siquiera es consciente (da miedo solo de pensarlo).

CONSEJO

Escalabilidad significa no solo satisfacer las necesidades actuales, sino también prepararse para posibles cambios y crecimientos futuros. Un enfoque con visión de futuro es esencial para crear soluciones flexibles y ágiles, capaces de hacer frente a una carga de trabajo cada vez mayor o a una expansión continua sin comprometer el rendimiento ni la funcionalidad. La escalabilidad te ayuda a garantizar que sus sistemas sigan siendo eficaces y eficientes ante cambios impredecibles.

Pero la escalabilidad no consiste solo en abordar nuevos entornos y proteger nuevos lugares por donde pasan los datos. La escalabilidad también consiste en gestionar la creciente velocidad, variedad y volumen de los datos. La cantidad de datos que se generan y recopilan hoy en día no tiene precedentes. Con el auge de las aplicaciones de colaboración y las herramientas en línea, los datos pueden presentarse ahora en forma de conversaciones en aplicaciones como Slack, Teams y Zoom, así como en aplicaciones de correo electrónico en la nube como Gmail. También pueden presentarse en forma de imágenes, como fotos y capturas de pantalla. La gente tiene las mismas probabilidades de hacer capturas de pantalla de información importante como de pegarlas en un documento. Escalabilidad significa proteger todos los formatos de datos y todos estos casos de uso, incluidos los que aún no se han desarrollado.

RECUERDA

El apartado «El DLP moderno en acción» , más adelante en este capítulo, analiza los detalles de funcionamiento de los sistemas DLP. Por ahora, tenga en cuenta que la funcionalidad básica de un sistema DLP es detectar datos confidenciales y protegerlos.

Cómo el DLP pasó de ser un héroe a un niño problemático

A medida que las organizaciones adoptaban aplicaciones en la nube y se ampliaban a nuevas ubicaciones, el despliegue de los sistemas DLP heredados se hacía cada vez más difícil de controlar. Estos sistemas se diseñaron para ser instalados y mantenidos a nivel local, lo que significaba que había que duplicarlos e instalarlos en cada nueva ubicación y sucursal. Esto añadía una gran complejidad y requería muchos recursos, incluidos *hardware*, mantenimiento y personal. Además, la creciente tendencia al trabajo remoto añadió otro nivel de complejidad, ya que los empleados empezaron a acceder a datos confidenciales desde distintos dispositivos y ubicaciones. Todo ello dificultaba a las organizaciones la gestión eficaz de sus sistemas DLP, lo que se traducía en un aumento de los costes y en posibles riesgos para la seguridad.

¿Alguna vez has evitado actualizar su teléfono o portátil por miedo a que se estropée su aplicación favorita o surja algún problema molesto? Multiplique esto por mil e imagine tener que actualizar el *software* DLP

heredado en numerosos servidores y sucursales, así como en miles de dispositivos de los empleados. No es de extrañar que algunos clientes se aferren a versiones antiguas de su *software* DLP: supone mucho menos esfuerzo que intentar llevar a cabo una actualización.

ADVERTENCIA

Si no se realizan actualizaciones periódicas, los datos quedan expuestos y aumenta el riesgo de que se produzcan infracciones de la normativa y vulneraciones de la seguridad de los datos.

El DLP debe trabajar de forma más inteligente, no con más esfuerzo

Los sistemas DLP heredados escanean todos los formularios de datos e identifican la información confidencial que hay que proteger. La idea es que solo hay que proteger los datos confidenciales, ya que proteger los datos no confidenciales puede afectar negativamente a la productividad. Por ejemplo, aunque puede ser importante evitar que ciertos datos confidenciales se compartan por correo electrónico con terceros, proteger y posiblemente retrasar cualquier comunicación por correo electrónico con terceros no es necesario, porque hacerlo puede obstaculizar la comunicación y la colaboración y producir demasiadas alertas para el equipo de respuesta ante incidentes. Además, los empleados pueden utilizar los recursos de la empresa para actividades no relacionadas con el trabajo, como subir fotos personales a las redes sociales, siempre que el contenido no sea confidencial y no contenga secretos de la empresa. Dado que los sistemas DLP heredados están formados por componentes de *software* y *hardware*, hacer que escaneen todo el tráfico web y todos los repositorios de archivos, y que busquen todo tipo de datos confidenciales, requiere la implementación adicional de servidores de detección, módulos y bases de datos más grandes.

Debido a su naturaleza de implementación a nivel local, los sistemas DLP heredados dependen de recursos informáticos de *hardware* que son necesariamente limitados. Por ejemplo, los programas DLP para *endpoints* instalados en los ordenadores de los empleados están forzosamente diseñados con limitaciones en sus capacidades de detección de datos; por ejemplo, dependen de motores de detección básicos que consumen menos recursos. Esto significa que, aunque pueden detectar algunos datos confidenciales en los *endpoints*, no pueden utilizar métodos de detección avanzados, lo que puede ocasionar que no se detecten importantes cantidades de datos confidenciales. Por ejemplo, el DLP heredado no puede utilizar tecnologías avanzadas que requieren importantes recursos de procesamiento, como el aprendizaje automático (AA) y la coincidencia exacta de datos (consulta el apartado siguiente). El DLP en la nube descarga en ella las actividades que consumen muchos recursos, sin dejar de aplicarlas en el *endpoint*. La escalabilidad de este enfoque

supone una mejora espectacular, ya que permite al DLP tomar huellas digitales de los datos, como nombres concretos, números de la Seguridad Social y otra información confidencial vinculada a las personas.

RECUERDA

La nube puede proporcionar la escala efectivamente infinita que se necesita para potenciar estas capacidades de detección, permitiendo que los sistemas DLP se centren en los datos más importantes y los protejan de accesos no autorizados.

La necesidad de precisión

Un mito reinante que comento en el capítulo 1 es que el DLP heredado era impreciso. Pero la precisión no es el verdadero problema, o al menos no el principal. El principal problema son los falsos positivos (también analizados en el capítulo 1) , debidos principalmente a la falta de contexto. Sin duda, con los datos creciendo como la espuma a través de múltiples dispositivos y aplicaciones fuera de los muros perimetrales de una organización, y los datos confidenciales cada vez más difíciles de detectar a causa de la explosión de distintos tipos de datos, los DLP heredados no han podido seguir el ritmo y los niveles de precisión han disminuido. Pero el principal problema es que las soluciones DLP heredadas solían ser demasiado restrictivas, señalando acciones beneficiosas como infracciones, e incluso bloqueándolas, sin comprender el contexto empresarial ni el nivel de riesgo. En un mundo en el que la colaboración es fundamental para la nueva forma de hacer negocios, estas falsas infracciones han pasado a ser demasiadas.

Es importante que el DLP no cause fricciones en la empresa ni interrumpa el flujo de datos necesario para las prácticas empresariales beneficiosas. Por ejemplo, si un empleado quiere enviar un archivo a un contratista de confianza que está participando en un proyecto, no querrá que el DLP detenga esa transmisión. Lo ideal sería que el DLP permitiera a los equipos de respuesta ser más eficaces, amplificando los incidentes legítimos de pérdida potencial de datos y filtrando el ruido de los falsos positivos.

La exactitud y la precisión no eran los principales problemas de los sistemas DLP heredados, pero sí lo son para las nuevas soluciones DLP en la nube de menor antigüedad. Hay dos aspectos:

- La imprecisión en la detección de los datos puede detectar y proteger innecesariamente demasiados datos que no son confidenciales (es decir, identificar demasiados datos como confidenciales cuando, en realidad, no lo son) y posiblemente detener las comunicaciones comerciales legítimas.

- Puede existir una falta de métodos de detección para identificar los datos que son realmente confidenciales, básicamente pasar por alto los datos confidenciales. Por ejemplo, pasar por alto determinados tipos de archivos, como imágenes o formatos comprimidos, o números de pasaporte, información sanitaria, números de rutas internacionales y documentos nacionales de identidad específicos de cada país porque el sistema no tiene capacidad para identificar esos formatos de datos y tipos de archivos.

RECUERDA

Para mantener la confianza, los sistemas DLP deben ser precisos y exactos, señalando y bloqueando solo las transferencias de datos verdaderamente maliciosas sin generar demasiados falsos positivos.

Ingrediente clave n.º 1: identificadores de datos

Los identificadores de datos se utilizan para encontrar información confidencial, como números de la Seguridad Social o de tarjetas de crédito, a partir de contenidos descritos genéricamente, como expresiones regulares (conocidas como *regex*), una potente herramienta que ayuda al DLP a identificar automáticamente tipos de datos específicos utilizando términos, expresiones y patrones naturales y cotidianos («busca un número de nueve dígitos»). Una posible respuesta es que se trate de un número de la Seguridad Social, pero ¿cómo saberlo con seguridad?

Los identificadores de datos buscan la respuesta utilizando reglas especiales basadas en el número de dígitos numéricos, patrones de texto, secuencias, separaciones y palabras clave de proximidad (como número de la Seguridad Social [NSS], contraseña [contr], número de tarjeta de crédito [NTC], etc.) para reconocer estos números y protegerlos. He aquí algunos puntos importantes que deben tenerse en cuenta en relación con los identificadores de datos:

- Se necesitan miles de identificadores de datos predefinidos y la posibilidad de personalizarlos para adaptarlos a su empresa y mantener así su información segura, además de cumplir las normas de gobernanza. Además, la posibilidad de editar o crear identificadores de datos personalizados es fundamental: cada organización puede tener información confidencial diferente que debe protegerse.
- Los identificadores de datos deben admitir miles de tipos de archivos (Word, XLS, JPG, PNG, PDF, CSV, ZIP, RAR, etc.), formatos y categorías (imagen, análisis, archivo y comprimido, hoja de cálculo, audio, vídeo, base de datos, etc.) (consulta el capítulo 1).
- Debes tener compatibilidad con una amplia gama de números de identificación específicos de cada país (como información bancaria internacional, direcciones, códigos postales, documentos nacionales

de identidad, números de pasaporte y prefijos telefónicos) y perfiles de cumplimiento normativo y de privacidad para garantizar que la solución DLP pueda mantenerse al día con los últimos requisitos de gobernanza.

CONSEJO

Para que su sistema DLP sea eficaz, necesita miles de identificadores de datos. Esto le permite identificar y señalar con precisión la información potencialmente confiencial, en todos los estados, regiones y países, independientemente de dónde se encuentre.

Ingrediente clave n.º 2: coincidencia exacta de datos (EDM)

La coincidencia exacta de datos es una forma de encontrar información estructurada específica a partir de fuentes como hojas de cálculo y bases de datos. Con EDM, una solución DLP puede tomar huellas digitales e indexar registros confidenciales de clientes y empleados, lo que puede utilizarse para identificar a una persona a través de su nombre completo, número de la Seguridad Social, dirección y otros números de identificación. El EDM también puede utilizarse para encontrar registros financieros que identifiquen los activos de una persona, como números de tarjetas de crédito o de cuentas bancarias. Incluso puede utilizarse en el ámbito de la información sanitaria y bases de datos de identificación de productos y precios. Con EDM, una solución DLP puede indexar esta información y luego encontrarla donde se supone que debe estar. Para que el EDM sea eficaz y preciso, debe cotejar varios datos indexados y combinar campos de datos de un registro concreto. También debe ser capaz de indexar miles de millones de registros para dar soporte a organizaciones en crecimiento, a sus bases de datos en expansión y a la cada vez mayor cantidad de información actual. Por lo tanto, la escala del procesamiento es importante para el EDM.

Ingrediente clave n.º 3: funciones avanzadas de detección de datos

Ahora que existen más tipos de datos y formas de transferirlos que nunca, las organizaciones necesitan que su sistema DLP sea capaz de detectar información confidencial con precisión. El término *funciones avanzadas de detección* es un término un poco general que se refiere a cosas como:

- **Reconocimiento óptico de caracteres (OCR) y reconocimiento de imágenes basado en inteligencia artificial (IA):** estas características son cada vez más importantes para la protección de datos. Hoy en día, la gente hace fotos de documentos, formularios, carnés de identidad, pizarras y fotos de otras fotos con mucha facilidad. Por ejemplo, la gente suele hacer capturas de pantalla o fotos para

recoger información rápidamente y compartirla con un compañero. Mediante el OCR, una solución DLP puede extraer texto de una imagen y, a continuación, aplicar una clasificación de datos basada en las políticas de detección establecidas.

- **IA y AA:** la clasificación de imágenes mediante IA y AA, utilizando sofisticados métodos de detección, puede reconocer tipos de archivos y documentos habituales como pueden ser tarjetas de crédito, formularios fiscales, acuerdos de confidencialidad, formularios de fusiones y adquisiciones y patentes, sin extraer necesariamente su contenido. Estos métodos pueden detectar contenidos borrosos, de documentos arrugados y dañados, incluso cuando la información es difícil de leer con claridad. Esto se debe a que los algoritmos están entrenados para identificar patrones y características específicas de cada tipo de documento, como el diseño, las fuentes y los colores utilizados. Además, también pueden tener en cuenta el contexto en el que se utiliza el documento. Esto permite a la IA clasificar con precisión el documento incluso en condiciones difíciles, como cuando las imágenes son de baja calidad o los documentos están dañados.
- **Huella digital de expedientes y documentos:** se trata de una técnica esencial para que las organizaciones garanticen la seguridad y confidencialidad de sus documentos de misión crítica y archivos muy confidenciales. Mediante la indexación de todo el documento y la detección de copias exactas o parciales de su contenido, las organizaciones pueden evitar la exfiltración no autorizada y la duplicación de su información confidencial (como documentos de fusiones y adquisiciones, información que no se ha publicado todavía, diseños de ingeniería o datos relacionados con los inversores). Esta técnica es especialmente útil para detectar copias de archivos confidenciales en entornos y canales de transmisión de riesgo, como los correos electrónicos de salida y la subida de correos electrónicos a instancias de aplicaciones personales.

Las soluciones DLP heredadas ofrecían algunas respuestas en el pasado, pero ya no están a la altura. Sencillamente, no tienen suficiente potencia de cálculo ni escalabilidad.

Ingrediente clave n.º 4: mucho contexto y un modelo de protección de datos Zero Trust

Al igual que las olas del mar cambian y se mueven constantemente, lo mismo ocurre con las personas, las redes, las aplicaciones, los datos y las normas de gobernanza de una empresa. Para anticiparse a los posibles riesgos, un sistema DLP y su estrategia correspondiente deben ser capaces de adaptarse y responder con rapidez y eficacia ante un panorama de datos que está en constante cambio. Esto también se conoce

como *comprensión del contexto*. Esta agilidad permite que el sistema DLP proteja eficazmente los datos confidenciales, minimice los riesgos de vulnerabilidad de los datos y garantice el cumplimiento de la normativa pertinente sin que se vea afectada la productividad de los usuarios ni se causen fricciones en la continuidad de la actividad empresarial.

Para lograr tal matiz y flexibilidad, una plataforma de protección de datos en la nube debe integrarse con la infraestructura de seguridad y de red más amplia de una organización. Esa plataforma DLP también debe recopilar constantemente información de diversas fuentes, como gestión de identidades, análisis de comportamientos, registros de red, herramientas de seguridad en la nube, análisis de amenazas, seguridad de red, posturas de seguridad de SaaS y en la nube, índices de confianza nativos de la nube del agente de seguridad para el acceso a la nube (CASB) y posturas de seguridad de *endpoints*. Esta información puede utilizarse para identificar con precisión las circunstancias específicas del acceso de un usuario a datos confidenciales, el contexto empresarial y los riesgos potenciales que entraña dicha acción y, por tanto, determinar el nivel de acceso adecuado y la respuesta correcta en materia de protección de datos, todo ello en función de factores como la identidad, la ubicación y el comportamiento de una persona, la seguridad de su dispositivo, la fiabilidad de la red, la reputación de la aplicación utilizada, el destino final de una transferencia de datos, etc.

CONSEJO

Al ser consciente de los riesgos y del contexto, una plataforma de protección de datos puede adaptarse continuamente y ofrecer una gran eficacia y una respuesta precisa ante los incidentes.

En el capítulo 3 abordamos el concepto *Zero Trust* y su papel central en un DLP eficaz. Por ahora, tenga en cuenta que *Zero Trust* es una estrategia de seguridad esencial que asume que todos los usuarios, dispositivos y redes dentro del entorno de una organización son potencialmente maliciosos y debe sospecharse de ellos en todo momento.

Esto significa que todos los accesos a recursos y sistemas están estrictamente controlados y verificados, independientemente de si el usuario o el dispositivo están dentro o fuera del perímetro de la red. El contexto es el motor que impulsa una estrategia *Zero Trust*, porque hace posible que el sistema DLP tome decisiones informadas sobre cuándo permitir o no que se produzcan actividades relacionadas con los datos.

RECUERDA

Trabajar con soluciones de seguridad integradas y tecnologías de protección de datos adyacentes es lo que diferencia una *herramienta* de protección de datos de una verdadera *plataforma* de protección de datos .

El DLP moderno en acción

El DLP se sitúa en el centro del marco de seguridad de la información de una empresa y contribuye a aumentar la eficacia de otras herramientas de seguridad. Realiza varias funciones críticas, entre las que se encuentran:

- **El DLP identifica los datos confidenciales dondequiera que residan y se muevan, por ejemplo:**
  - *Datos en movimiento,* que son los que cruzan Internet, las redes, las aplicaciones y los dispositivos (como cargas y descargas).
  - *Datos en reposo,* que son los que se almacenan. Se puede tratar de cualquier cosa, desde el almacenamiento en sus aplicaciones privadas hasta una aplicación SaaS adoptada por la empresa (como cuando los datos de los clientes se introducen en Salesforce) o documentos internos almacenados y compartidos en Microsoft OneDrive o Microsoft SharePoint.
  - *Datos en uso,* que son los que se utilizan activamente y con los que se colabora, como una transferencia a USB, con actividades, impresión o datos que se envían por fax. (¡¿Aún se envían faxes?!)
- **El DLP supervisa el entorno de datos** para detectar quién accede a ellos y qué hace con ellos. Al supervisar las acciones, el DLP puede detectar incidentes, como el uso compartido no autorizado de información confidencial, que pueden infringir la política corporativa y tomar medidas para solucionarlos. Esto ayuda a garantizar que no se acceda a los datos confidenciales y que estos no se utilicen sin los privilegios adecuados (empleados frente a una persona ajena a la empresa, o dispositivo corporativo frente a uno personal) o la autorización o moderación (como descargas masivas sospechosas de grandes cantidades de archivos) y que cualquier posible vulnerabilidad de seguridad se identifique y aborde rápidamente.
- **El DLP actúa automáticamente para aplicar las políticas**, por ejemplo, deteniendo el flujo de datos, cifrando los datos, poniendo en cuarentena la información confidencial o anulando que se compartan los datos en una aplicación SaaS. Por ejemplo, si un empleado utiliza OneDrive para compartir intencionada o accidentalmente un archivo que contiene información confidencial con usuarios externos, el DLP puede anular automáticamente que se comparta ese archivo para evitar la divulgación no autorizada de la información.

- **El DLP proporciona orientación** a los usuarios notificándoles automáticamente de las infracciones y las razones que las motivan, al tiempo que los educa en prácticas seguras para la manipulación de los datos. Las notificaciones también ayudan a educar instantáneamente a los usuarios sobre las políticas de seguridad, reduciendo la necesidad de que los equipos de respuesta ante incidentes clasifiquen manualmente los problemas. Un buen DLP también debe ser capaz de avisar a los usuarios al instante y sin demora, y de enviar las notificaciones a los responsables, al equipo de respuesta o a RR. HH. según sea necesario.

Ha llegado el momento de cambiar su DLP

El DLP heredado ha sido una solución de seguridad fiable durante años, y no es de extrañar que haya tantos profesionales que continúen siendo tan entusiastas. Al fin y al cabo, como he señalado antes, esos sistemas han experimentado un intenso desarrollo en la última década para proteger las redes locales de las amenazas en la era anterior a la nube.

Los proveedores de DLP heredados han intentado salvar la distancia entre sus sistemas y los requisitos de las empresas modernas, que dan prioridad a la nube, utilizando tecnologías como las puertas de enlace web seguras (SWG) en la nube y las soluciones CASB, mediante la integración del Protocolo de Adaptación de Contenidos de Internet (ICAP).

ADVERTENCIA

Lamentablemente, la mayoría de los sistemas DLP heredados no están diseñados para abordar casos de uso de trabajo en la nube e híbridos, que requieren integraciones y capacidades con servicios en la nube que los sistemas DLP heredados no admiten fácilmente. Esto puede provocar problemas de compatibilidad y bajo rendimiento.

Todas estas limitaciones y muchas más de las que se ha hablado en capítulos anteriores han hecho que el DLP heredado sea impopular, lo que ha llevado a muchas organizaciones a desactivar por completo estas herramientas. A medida que las organizaciones trasladan cada vez más sus datos a la nube, aumenta la necesidad de sistemas DLP en la nube capaces de reconocer los cambios en los contextos y los riesgos asociados a la gestión de datos. Estos sistemas deben ser fáciles de implementar, ampliar y aumentar, al tiempo que responden a casos de uso tanto antiguos como modernos. Al estar en la nube, siempre están actualizados, lo que mejora la protección a medida que cambian el contexto y los riesgos empresariales.

EN ESTE CAPÍTULO

- **Descubrir cómo una seguridad de datos obsoleta puede perjudicar a su empresa**
- **Conocer los tipos de contexto de los datos y mantener las actividades empresariales en marcha**
- **Adaptarse a la evolución de las condiciones de riesgo para proteger sus datos**
- **Garantizar la seguridad de los casos de uso empresarial modernos**
- **Evaluar el contexto empresarial, el riesgo y el comportamiento de los usuarios para mantener sus datos seguros en el futuro**

Capítulo 3
El papel de *Zero Trust* en el DLP actual

Zero Trust es un concepto muy importante en la seguridad actual, bien se trate de DLP o de otro tipo. Una estrategia *Zero Trust* asume que todos los usuarios y dispositivos, incluso los que están dentro de la red de la organización, pueden ser perjudiciales y no se puede confiar en ellos. Esto significa que el acceso a sistemas y datos confidenciales no se concede automáticamente en función de la identificación personal y la afiliación a la organización. El acceso se concede tras una cuidadosa autenticación, comprobación de las medidas de seguridad y consideración del contexto de riesgo, que se vuelve a evaluar continuamente. *Zero Trust* no debe obstaculizar la productividad, sino permitir un uso seguro de los datos confidenciales y respaldar las prácticas empresariales actuales teniendo en cuenta la seguridad, adaptándose automáticamente a los cambios en las condiciones de riesgo.

Zero Trust vuelve a evaluar continuamente la fiabilidad de cada individuo o dispositivo y entorno operativo antes de concederle acceso a datos confidenciales o a un uso determinado de esos datos confidenciales. Incluso si a un empleado se le ha otorgado acceso anteriormente, este debe volver a ser evaluado cuidadosamente, por ejemplo, verificando su identidad, comprobando su dispositivo y conexión a la red, calibrando

los riesgos de las aplicaciones a las que accede y supervisando su comportamiento para garantizar que *sigue* siendo de confianza. Si empieza a comportarse de forma sospechosa o muestra signos de negligencia, como compartir datos en exceso, el sistema se implica en sus acciones, por ejemplo, reduciendo sus privilegios. Esto ayuda a proteger los datos confidenciales de posibles riesgos de pérdida y garantiza que solo las personas de confianza puedan acceder a ellos y compartirlos con otras personas de confianza.

Zero Trust pretende crear un entorno seguro y controlado para el acceso y la transferencia de datos, reduciendo el riesgo de vulneraciones de datos y protegiendo los datos confidenciales de accesos no autorizados. Para ello, aplica estrictos controles de acceso, además de supervisar y verificar continuamente las acciones, los riesgos contextuales y el comportamiento de los usuarios. En la prevención de pérdida de datos (DLP), el modelo de seguridad *Zero Trust* ayuda a minimizar los riesgos de vulneración de datos, proteger los datos de forma más precisa y optimizar los ciclos de respuesta ante incidentes teniendo en cuenta el contexto y los riesgos de la organización. Al permitir únicamente el acceso y uso seguros de los datos confidenciales por parte de los usuarios autorizados e impedir cualquier intento malintencionado, sospechoso, negligente o arriesgado de acceder a esos datos o transferirlos, las organizaciones pueden proteger mejor sus activos.

Los riesgos de una seguridad obsoleta

Los sistemas DLP se crearon para ayudar a evitar que la información confidencial saliera de una empresa. Las versiones heredadas abordan un número limitado de situaciones comunes de pérdida de datos; su objetivo principal es identificar los datos confidenciales y mantenerlos dentro de la organización, utilizando un enfoque basado en el perímetro que se centra en controlar el flujo de datos que entran y salen de la red de la organización.

Mediante un enfoque denominado *confianza implícita*, el DLP heredado se basa en detectar y responder a vulneraciones de datos predefinidas. Pero este enfoque carece de contexto sobre los usuarios, sus razones empresariales y los riesgos asociados de una acción específica.

Por ejemplo, un sistema DLP heredado puede buscar números de la Seguridad Social y bloquear cualquier intento de que se envíen fuera del perímetro de la empresa. En otro caso, puede impedir que se suban datos confidenciales a una aplicación SaaS de forma inequívoca, sin discernir entre una instancia corporativa de una aplicación SaaS aprobada como Microsoft Teams y una instancia personal de esa misma aplicación. Este enfoque puede parecer seguro, pero en realidad es bastante rígido y carece de la información sobre usuarios, dispositivos, redes, aplicaciones y destinos que puede revelar qué actividades están autorizadas. La

confianza implícita es un obstáculo empresarial que impide la fluidez necesaria en la comunicación y el movimiento de los datos para hacer crecer cualquier negocio en la actualidad.

ADVERTENCIA

Al no volver a analizar continuamente el contexto y el riesgo empresarial, un sistema DLP heredado no puede tomar decisiones informadas sobre la protección de datos y puede causar interrupciones innecesarias en las operaciones de la empresa.

Con políticas laxas, la confianza implícita concede acceso a datos confidenciales sin verificar constantemente la identidad y fiabilidad del usuario o el dispositivo. Esto es problemático porque deja a la organización vulnerable a un posible uso indebido de sus datos confidenciales. En cuanto los datos confidenciales abandonan el perímetro, quedan fuera del control de la seguridad de la organización.

Esta situación es un gran problema en la era de la nube. Los datos confidenciales se utilizan y comparten fuera de las fronteras de la empresa incluso en el caso de las funciones empresariales más rutinarias. Por ejemplo, aplicaciones y servicios habituales en la nube, como Dropbox y Google Drive, permiten a los empleados acceder, compartir y colaborar utilizando datos confidenciales dentro y fuera de los entornos corporativos. Pero los sistemas DLP heredados que utilizan la confianza implícita interrumpirían una colaboración legítima o permitirían por descuido que los datos se filtraran al mundo exterior, haciéndolos vulnerables a posibles amenazas.

La protección de datos *Zero Trust* permite utilizar y compartir datos confidenciales siempre que se verifiquen continuamente las condiciones de seguridad. Permite que los datos confidenciales se muevan y se compartan entre usuarios y dispositivos y se almacenen en diferentes servicios en la nube, ya que verifica constantemente las condiciones de seguridad, como la identidad del usuario, la seguridad del dispositivo, la red y la aplicación, y el comportamiento del usuario a lo largo del tiempo. La protección de datos *Zero Trust* se aplica específicamente a los datos confidenciales y garantiza que se cumplan siempre todas las condiciones de seguridad, lo que permite el trabajo híbrido, el uso de la nube y los casos actuales de uso empresarial.

RECUERDA

Un sistema DLP actual en la nube que utiliza los principios *Zero Trust* supervisa y controla los datos en cualquier lugar desde el que los usuarios corporativos quieran conectarse y acceder a los datos, y en cualquier lugar en el que los datos puedan almacenarse y transferirse, tanto en repositorios de aplicaciones en la nube como en entornos locales.

Otro problema de los enfoques de seguridad tradicionales basados en múltiples productos y en la confianza implícita es que están muy aislados, aplicando solo un control de seguridad a la vez, sin que exista integración de todos los controles de seguridad y sin compartir la

información sobre riesgos. Esto significa que los distintos controles de seguridad están aislados y no integrados en una plataforma de seguridad coherente, lo que deja lagunas en su estrategia de seguridad global. Para proteger sus datos completamente, necesita varios controles de seguridad que trabajen juntos y compartan información.

El planteamiento *Zero Trust* adopta un enfoque más holístico y dinámico en torno a la protección de datos. Tiene en cuenta el contexto del usuario, el dispositivo, la red y otros factores para tomar decisiones más informadas sobre la protección de datos. Este enfoque admite la integración del DLP con otros controles de seguridad y herramientas de productividad, y puede supervisar y adaptarse continuamente a los cambios en las amenazas, los riesgos y las condiciones empresariales.

En general, las organizaciones que utilizan un DLP basado en la confianza implícita dependen de la falsa suposición de que los usuarios de una organización son dignos de confianza, tienen cuidado con la seguridad y nunca pondrán en peligro los datos confidenciales. De hecho, debido a la falta de contexto de seguridad, una aplicación restrictiva de las políticas de DLP provocaría a menudo la interrupción de procesos empresariales legítimos. En cambio, el DLP basado en *Zero Trust* supervisa y controla de cerca cómo se utilizan los datos en todo momento para evitar de forma flexible las infracciones de las políticas de datos.

Un sistema DLP basado en la confianza implícita protegería el número de una tarjeta de crédito permitiendo a los usuarios autorizados acceder a los datos confidenciales y denegando el acceso a los usuarios no autorizados. Esto supone que se puede confiar en que los usuarios autorizados manipularán los datos de forma segura y no harán un uso indebido de ellos.

A diferencia de los sistemas DLP heredados basados en la confianza implícita, un sistema DLP basado en principios *Zero Trust* no depende de la suposición de confianza entre los usuarios. En lugar de ello, protege los datos confidenciales, como el número de las tarjetas de crédito, exigiendo a todos los usuarios que se sometan a un proceso de autenticación antes de acceder a esos datos, independientemente de su nivel de autorización. Esto podría incluir la autenticación multifactor, como una contraseña y un código de un solo uso enviado a un dispositivo móvil.

El sistema también evalúa continuamente los riesgos potenciales de dispositivos, usuarios, datos y aplicaciones. Verifica que los dispositivos sean fiables y seguros, que las aplicaciones y sus instancias utilizadas (es decir, corporativas frente a personales) sean seguras y cumplan las normativas, que la red sea segura y fiable, que los datos se compartan con destinos y destinatarios fiables, y que el comportamiento del usuario esté acorde con las directivas definidas. Estas condiciones se verifican continuamente y el sistema adapta su respuesta de protección en consecuencia. Además, el sistema supervisa y rastrea el acceso de

los usuarios a datos confidenciales, alertando a los administradores de cualquier comportamiento sospechoso o posible infracción y orientando a los usuarios sobre las prácticas seguras en el uso de los datos en caso de infracción de las políticas corporativas. Este planteamiento reduce el riesgo de acceso no autorizado a datos confidenciales porque el sistema verifica a todos los usuarios antes de concederles acceso y también minimiza los riesgos para esos datos a lo largo del tiempo al educar a los usuarios en tiempo real.

El contexto permite que su DLP diga sí a la actividad empresarial importante

Zero Trust ayuda a los sistemas de protección de datos a tomar decisiones informadas sobre la autorización o restricción de determinadas actividades. Para ello, tiene en cuenta múltiples factores o contextos, como la identidad del usuario, el dispositivo utilizado, la fiabilidad de la aplicación y el contexto de los datos implicados. (*Zero Trust* recopila el contexto con la ayuda de otras soluciones, de las que hablo en el apartado «El DLP no debe ser independiente») Al tener en cuenta todos estos contextos, la aplicación de los principios *Zero Trust* puede determinar con mayor precisión si una actividad concreta es beneficiosa y necesaria para la empresa y puede decir que sí a la misma. Esto ayuda a garantizar la protección de los datos y a minimizar el riesgo de infracciones de seguridad u otras amenazas, al tiempo que permite que las operaciones empresariales sigan funcionando sin problemas.

En la siguiente lista se definen los tipos de contexto utilizados en *Zero Trust*:

- **Contexto de usuario:** quién realiza una acción o quién es el destinatario de una acción. Esta información ayuda a determinar si el comportamiento de un usuario es bueno o si algo falla. Por ejemplo, supongamos que de repente un usuario mueve muchos más datos de lo habitual, se conecta desde lugares inusuales o actúa de forma extraña en comparación con su conducta anterior. Eso podría ser una señal de un comportamiento arriesgado o malicioso. Lo mismo ocurre si un usuario accede a datos confidenciales, los utiliza o los envía a aplicaciones personales. En función de su identidad y comportamiento, puedes cambiar los privilegios de un usuario para garantizar que los datos confidenciales se mantengan protegidos y que solo los usuarios autorizados puedan acceder a ellos, compartirlos con otros destinatarios autorizados y transferirlos a destinos seguros.
- **Contexto del dispositivo:** el dispositivo que intenta acceder a sus datos. Hay que tener en cuenta si el dispositivo es personal o corporativo, su nivel de seguridad, y si está revisado y actualizado. También

puede fijarte en factores cercanos al dispositivo, como la fiabilidad del lugar desde el que se conecta. Teniendo en cuenta todas estas cosas, puede determinar el nivel adecuado de privilegios para el dispositivo en función de lo fiable y arriesgado que sea. Incluso si un usuario es de confianza, su dispositivo puede verse comprometido o suponer un riesgo para la seguridad, por lo que el contexto del dispositivo es fundamental para determinar los privilegios que debes conceder.

- **Contexto de la aplicación:** la reputación y fiabilidad de la aplicación utilizada para acceder a los datos o manipularlos. Esto es importante porque si una aplicación tiene mala reputación o no es de fiar, podría suponer un riesgo para la seguridad de los datos a los que se accede o que se manipulan. Los sistemas de protección de datos pueden depender de otros sistemas, como un agente de seguridad para el acceso a la nube (CASB), para recopilar información sobre los atributos de la aplicación relacionados con el cumplimiento y el riesgo. Esto puede ayudar al sistema a determinar si la aplicación supone un riesgo, como infringir el Reglamento General de Protección de Datos (RGPD) al exponer excesivamente datos confidenciales.

  Un usuario puede tener acceso a varias instancias de una aplicación en la nube, lo que requiere un control más granular de los datos confidenciales para evitar que se compartan accidentalmente con cuentas personales. Las aplicaciones de comunicación colaborativa como Slack y Microsoft Teams también pueden suponer un riesgo si los canales dentro de esas aplicaciones tienen usuarios corporativos y externos, por lo que el sistema debe ser capaz de diferenciarlos para evitar fugas de datos. Ten todo esto en cuenta para asegurarte de que las aplicaciones que utilizas son de confianza y para proteger sus datos de posibles riesgos.

- **Contexto de los datos:** el grado de confidencialidad de un dato concreto, su formato, su tamaño y otros factores. Dónde se utilizan sus datos y si ese uso es legítimo. Ayuda a saber a qué tipo de datos se accede o cuáles se mueven, y si pertenecen al lugar donde se utilizan. Si se accede a datos confidenciales o si estos se transfieren a un lugar no autorizado, es necesario tomar medidas para evitar una fuga o filtración de datos. El contexto de los datos es crucial para garantizar que los datos se manipulen adecuadamente y que solo accedan a ellos los usuarios autorizados desde ubicaciones autorizadas en función de su nivel de importancia. Ayuda a determinar si una actividad es necesaria para la empresa y si merece la pena correr el riesgo.

ADVERTENCIA

La mayoría de las soluciones DLP, no solo las heredadas, causan problemas en el funcionamiento de la empresa porque normalmente no recopilan suficiente información sobre el negocio y los riesgos que conlleva. La mayoría de las soluciones DLP obligan a su organización a

depender de los equipos de respuesta ante incidentes para tomar decisiones manuales sobre qué hacer. Esto es frustrante, ineficaz y caro.

No cabe ninguna duda de que *Zero Trust* minimiza estos problemas. Un sistema DLP actual basado en los principios *Zero Trust* tiene en cuenta todos los riesgos de elementos como usuarios, dispositivos, datos, redes y aplicaciones. De este modo, el sistema comprende mucho mejor los riesgos existentes y puede tomar automáticamente las decisiones correctas sobre la protección de sus datos basándose en políticas dinámicas de protección de datos adaptadas a las necesidades específicas de su empresa. *Zero Trust* te ayuda a mantener los datos seguros y a su empresa funcionando sin problemas.

El DLP no debe ser independiente

Los controles de datos son algo que se utiliza en los sistemas DLP tanto antiguos como nuevos. De hecho, el DLP está diseñado para identificar datos confidenciales y protegerlos. El problema de la mayoría de estos controles de datos es que carecen de contexto. El DLP debe formar parte de una plataforma más amplia, basada en principios *Zero Trust*, que utilice todo el contexto disponible para tomar decisiones informadas. El DLP necesita ayuda e información de otras soluciones para recopilar todos los contextos necesarios, como son el contexto del usuario, del dispositivo, de la aplicación y de los datos. Por eso, un sistema basado en *Zero Trust* está integrado y se centra en controles de datos contextuales en lugar de confiar ciegamente en todo. Es una forma de adaptarse a las cambiantes condiciones de riesgo y proteger automáticamente sus datos en cada momento con la respuesta más adecuada.

CONSEJO

En la protección de datos *Zero Trust*, busca controles consolidados en los que cada uno de ellos comparta información y funcione en conjunto a la perfección para proteger sus datos. Por ejemplo, Netskope Intelligent Security Service Edge (SSE) habilita directamente *Zero Trust* y permite compartir y contextualizar los controles, incorporando el DLP en su núcleo, lo que hace que proteger sus datos resulte muy fácil y eficiente.

Netskope Intelligent SSE respalda su exhaustiva plataforma DLP con otras soluciones de seguridad. Algunas de las más importantes son:

- **Puerta de enlace web segura (SWG):** SWG es una solución de seguridad que se sitúa entre los usuarios e Internet, garantizando conexiones web seguras y protegiendo frente a amenazas basadas en la web. Netskope DLP a través de SWG garantiza que los datos confidenciales no se filtren a través de tráfico web no fiable e inseguro, incluido el tráfico cifrado. Detecta, supervisa y protege los datos confidenciales de la empresa para que no se filtren ni queden expuestos a través de cualquier conexión web, incluidas las oficinas locales, las sucursales y las ubicaciones wifi públicas.

- **CASB:** Netskope DLP a través de CASB descubre, supervisa y protege los datos confidenciales en aplicaciones de *software* como servicio (SaaS), infraestructura como servicio (IaaS), redes corporativas y sucursales, personal móvil, servicios de correo electrónico y los *endpoints* de los empleados. Este servicio centralizado en la nube aplica políticas unificadas de protección de datos en todos los lugares donde se almacenan, utilizan o transfieren datos confidenciales, y protege los datos sensibles en movimiento y en reposo. También abarca miles de aplicaciones SaaS y, de forma exclusiva, tiene conocimiento de los datos transmitidos a instancias de aplicaciones personales (es decir, desde OneDrive corporativo a OneDrive personal) y aplicaciones peligrosas. Analiza miles de tipos de archivos diferentes, así como mensajes y comunicaciones asíncronas a través de aplicaciones de colaboración y servicios de correo electrónico. Las políticas de protección, cumplimiento y privacidad de datos se aplican de forma coherente en todos los servicios de la nube pública y se sincronizan automáticamente en toda la plataforma DLP.
- **Gestión de la posición de seguridad SaaS (SSPM) y gestión de la postura de seguridad en la nube (CSPM):** estas tecnologías permiten gestionar la postura de los entornos SaaS y en la nube pública para garantizar la seguridad y el cumplimiento normativo. Supervisan y evalúan continuamente la postura de seguridad, identificando posibles riesgos y errores de configuración y proporcionando ideas y recomendaciones prácticas. Las funciones de corrección automatizada resuelven los problemas detectados en tiempo real.
- ***Software* de protección de *endpoints*:** Netskope Endpoint DLP es una solución que detecta, supervisa y protege los datos confidenciales en los *endpoints* de los empleados. Dado que la solución está integrada en el cliente único de Netskope, no es necesario implementar un agente independiente. Netskope Endpoint DLP minimiza la utilización de recursos a la vez que ofrece un conjunto completo de funciones, incluidos clasificadores basados en aprendizaje automático, reconocimiento óptico de caracteres (OCR), huellas digitales de archivos, coincidencia exacta de datos (EDM), etc. Aprovechar el servicio DLP en la nube y la inteligencia procedente de toda la plataforma DLP ayuda a evitar la duplicación en el análisis de los datos originados en la nube, lo que se traduce en una experiencia de usuario sin problemas y en resultados de protección más sólidos.
- **Análisis de comportamiento de entidades y usuarios (UEBA):** este control de seguridad evalúa continuamente el comportamiento de los usuarios para identificar cualquier actividad inusual o potencialmente arriesgada. En el pasado, UEBA era un control de seguridad aislado, pero debe integrarse con DLP para ser eficaz. Mediante

la asimilación de registros de infracciones de DLP y la señalización de comportamientos de riesgo para su posterior evaluación, UEBA puede informar de cambios que se lleven a cabo en la aplicación de políticas y ayudar a mantener sus datos seguros.

- **Gestión de identidades y accesos (IAM):** IAM consiste en gestionar y controlar el acceso a los recursos en función de la identidad del usuario. Incluye tecnologías como la autenticación multifactor, el inicio de sesión único y las listas de control de acceso. Netskope se integra con muchos proveedores de IAM para garantizar que solo los usuarios autorizados puedan acceder a recursos específicos y para ofrecer protección contra el acceso no autorizado. IAM es una parte esencial de la estrategia de seguridad *Zero Trust* de cualquier organización, ya que ayuda a proteger los recursos y a garantizar el cumplimiento de las políticas y normativas de seguridad.
- **Protección del correo electrónico:** Netskope proporciona una solución DLP muy amplia para correo electrónico como Microsoft 365 y Gmail, tanto para datos en movimiento como en reposo. La solución protege los correos electrónicos confidenciales de salida en tiempo real a través de un proxy SMTP y correo web, y puede distinguir los datos confidenciales que salen a través de una cuenta de correo electrónico personal de los que se envían a través de una cuenta de correo electrónico corporativa o a través de servicios de correo electrónico privados.
- **Acceso a la red *Zero Trust* (ZTNA):** Netskope DLP, suministrado a través de Netskope Private Access (NPA), la solución de acceso remoto, evita la pérdida y la filtración de datos a través de recursos privados en el centro de datos y en entornos de nube pública, garantizando la protección de los datos en el acceso a través del navegador a aplicaciones privadas desde cualquier lugar desde el que se conecten los usuarios.

Al combinar estos componentes básicos en una única plataforma integrada, la plataforma SSE de Netskope proporciona una solución de seguridad completa que puede proteger a su organización de una amplia variedad de amenazas.

Puesta en práctica de los principios *Zero Trust* con DLP

RECUERDA

El objetivo de la protección de datos *Zero Trust* no es impedir que los datos confidenciales salgan de la empresa. También se trata de permitir que se lleven a cabo casos de uso actuales sin perder nunca de vista la seguridad y los riesgos.

Esto significa dar soporte a usuarios en distintas ubicaciones y fomentar la colaboración, todo ello manteniendo la seguridad de los datos. La protección de datos *Zero Trust* consiste en poder trabajar desde cualquier lugar y seguir teniendo acceso a todos los recursos necesarios, además de poder colaborar con miembros del equipo y socios externos sin preocuparse por las fugas de datos. Con una solución unificada como Netskope SSE, puedes proteger sus datos y aprovechar todas las ventajas de los flujos de trabajo de los datos empresariales actuales. He aquí un par de ejemplos de cómo funciona esto en la práctica:

- Imagina que está trabajando en su portátil, conectado a la red de su empresa mediante Netskope SSE. Accede a algunos documentos de venta importantes y empieza a trabajar en ellos. Pero entonces, accidentalmente, intenta guardar una copia de los documentos en su cuenta personal de almacenamiento en la nube en lugar de en la instancia corporativa de esa misma aplicación de almacenamiento en la nube.

  Con el DLP basado en los principios *Zero Trust*, el sistema reconoce que está intentando enviar datos confidenciales de la empresa a una instancia de aplicación personal e impide que los datos se guarden. En su lugar, el sistema muestra una notificación de orientación para el usuario, una ventana emergente que le informa inmediatamente de la infracción y le recuerda la ubicación correcta para guardar los documentos. De este modo, puede trabajar desde cualquier lugar y seguir teniendo acceso a todos los recursos que necesita sin preocuparte de enviar accidentalmente datos confidenciales a algún lugar donde no deberían estar. Las notificaciones de orientación instruyen a los usuarios sobre las prácticas seguras y las políticas de la empresa, con el tiempo, esto minimiza el riesgo de pérdida de datos y reduce la necesidad de ofrecer largos cursos de formación a lo largo del año.

- Supongamos que está colaborando con socios externos en un proyecto y quiere compartir algunos documentos con ellos. Con el DLP basado en principios *Zero Trust*, el sistema comprobará la reputación y fiabilidad de la aplicación que utiliza para compartir documentos, su identidad y comportamiento, el dispositivo utilizado y el destino de la transmisión.

- Si utiliza una aplicación personal de almacenamiento en la nube que tiene un nivel de seguridad distinto al de la aplicación corporativa de su empresa, el sistema puede impedir que comparta los datos a través de esa aplicación. En su lugar, puede sugerirle que utilice una aplicación diferente o que envíe los documentos a través de un canal seguro. El DLP también comprobará el destino de la transmisión, por ejemplo, si el destinatario es un usuario externo o un empleado y si

el destino es seguro. El DLP puede enviarle una notificación preguntándole si está seguro de que quiere compartir datos confidenciales con el destinatario externo e incluso puede pedirle que justifique su acción. De este modo, puede colaborar con confianza, sabiendo que sus datos están protegidos y que solo los usuarios autorizados pueden acceder a ellos.

Zero Trust adaptativo

Zero Trust adaptativo consiste en reconocer que las cosas cambian con el tiempo. Esto significa que la protección de datos *Zero Trust* necesita evaluar continuamente el contexto empresarial, el riesgo y el comportamiento de los usuarios para mantener sus datos seguros.

Para visualizar este punto, piense en un guardia de una discoteca. Una noche, está en la puerta cuando se acerca un grupo de personas. El portero comprueba sus identificaciones y todo parece correcto, así que deja entrar al grupo. Pero a medida que avanza la noche, el portero empieza a notar un comportamiento extraño en una de las personas del grupo. Tal vez esté actuando de forma agresiva o intentando acceder a zonas de la discoteca a las que no tiene permitida la entrada. Con *Zero Trust* adaptativo, nuestro guardia reconocería este cambio de comportamiento y tomaría medidas para proteger a otras personas y a la propia discoteca. Puede vigilar a la persona que actúa de forma extraña más de cerca para asegurarse de que no causa problemas, o incluso pedirle que se vaya. De este modo, podrá mantener a salvo a otras personas y a su discoteca, incluso cuando el comportamiento de alguien cambia.

Piense en estos escenarios comunes a los que probablemente se enfrenta su empresa:

- **El comportamiento de alguien cambia.** Tienes un empleado de confianza que siempre ha tenido acceso a ciertos datos confidenciales de la empresa. Un día, quizá después de una revisión de su rendimiento, empieza a comportarse de forma diferente. Empieza a acceder y a descargar más datos confidenciales de lo habitual o se conecta a la red desde lugares inusuales. Con *Zero Trust* adaptativo, el sistema reconocerá este cambio de comportamiento y ajustará los privilegios del empleado en consecuencia. Por ejemplo, el sistema puede restringir su acceso a datos específicos o notificar este comportamiento inusual al equipo de seguridad para que se lleve a cabo una evaluación más detallada. De este modo, podrá proteger los datos aunque cambie el comportamiento de un empleado de confianza.

- **La reputación y la fiabilidad de las aplicaciones cambian.** Las aplicaciones cambian con el tiempo; no solo su funcionalidad, sino también su reputación, sus posturas de seguridad y su fiabilidad pueden cambiar. Por ejemplo, una aplicación de almacenamiento en la nube que antes se consideraba segura puede tener una nueva vulnerabilidad expuesta o una configuración errónea que afecte a su fiabilidad. Con *Zero Trust* adaptativo, la solución evaluará continuamente el nivel de riesgo de la aplicación y ajustará los privilegios según sea necesario. De este modo, puede proteger sus datos aunque cambie la fiabilidad de una aplicación.
- **Los dispositivos se ven comprometidos.** Los dispositivos pueden volverse más vulnerables o incluso verse comprometidos sin que el usuario se dé cuenta. Por ejemplo, un portátil que antes se consideraba seguro puede infectarse con *malware* o ver modificada su configuración de seguridad sin que el usuario lo sepa. Con *Zero Trust* adaptativo, el sistema evaluará continuamente la postura de seguridad del dispositivo y ajustará los privilegios según sea necesario. De este modo, puede proteger sus datos aunque el dispositivo se vea comprometido.
- **Cambios en el flujo de datos.** El flujo de datos puede cambiar debido a cambios en las normas de cumplimiento a distintos niveles. Por ejemplo, un flujo de datos puede considerarse aceptable, pero si el destino se vuelve inseguro o irregular, la normativa puede seguir exigiendo que la organización proteja ese flujo de datos. Este es el caso del RGPD, que establece que determinados datos privados no pueden salir de la UE a menos que exista una adecuación o un acuerdo de transferencia válido. Con *Zero Trust* adaptativo, el sistema evaluará constantemente los riesgos y ajustará los privilegios según sea necesario. De este modo, puedes proteger sus datos aunque cambien las normas.
- **Cambia la función o el estado de un usuario.** Los usuarios que ya hayan entregado el preaviso de que dejan la empresa pueden seguir teniendo acceso a datos confidenciales hasta que se vayan. Con *Zero Trust* adaptativo, el sistema evaluará continuamente los riesgos que esto conlleva y ajustará los privilegios según sea necesario. Por ejemplo, el sistema puede restringir el acceso del usuario a datos específicos o notificar al equipo de seguridad acerca de una acción que requiere una evaluación más profunda.

CONSEJO

Zero Trust adaptativo evalúa el uso de los datos desde tantas perspectivas como sea posible con el fin de ajustar los privilegios para proteger los datos confidenciales, así como la reputación de la empresa, y respaldar la actividad empresarial.

Zero Trust adaptativo desbloquea una mayor protección a la vez que hace que los datos y las personas sean más productivos. Pone en práctica una política de protección de datos dinámica y adaptable, evaluando continuamente los riesgos y ajustando los privilegios según sea necesario. Se trata de un cambio significativo con respecto al enfoque típico de los sistemas DLP, tanto heredados como nuevos, que se basan en un enfoque único de confianza implícita, lo que conduce a muchos falsos positivos y a la fatiga en la clasificación de incidentes. Con un enfoque tan engorroso, el equipo de respuesta ante incidentes se ve obligado a evaluar manualmente cada incidente para determinar si se trata de una infracción real y, a continuación, ponerse en contacto con el usuario responsable (a menudo después de que este ya haya olvidado de qué acción se trata). Después, el equipo tiene que descifrar todo el flujo de datos, un proceso largo y que consume muchos recursos. *Zero Trust* adaptativo proporciona un modelo de protección continua que facilita enormemente la seguridad de los datos y el buen funcionamiento de la empresa.

Protección de datos *Zero Trust* adaptativo de Netskope

La implementación de Netskope de una protección de datos basada en *Zero Trust* adaptativo se basa en el contexto. Al supervisar el tráfico entre usuarios, dispositivos, aplicaciones, redes y destinos, Netskope consigue comprender a fondo lo que está sucediendo en su organización. Esto permite al sistema ejercer un control granular sobre el acceso a los datos, protegiendo así susdatos confidenciales sin obstaculizar las operaciones empresariales.

Por ejemplo, imagine que un usuario intenta acceder a datos confidenciales de la empresa desde un dispositivo personal. Con Netskope, el proceso comienza con la detección precisa de esos datos confidenciales. Además, al tener en cuenta diversos factores contextuales, la respuesta a incidentes se hace más precisa y eficaz, reduciendo la necesidad de clasificación manual y minimizando la carga de trabajo de los equipos de seguridad. El sistema evaluaría la posición de seguridad del dispositivo, la identidad del usuario y su comportamiento para determinar si debe concederle el acceso.

Otros factores que se tienen en cuenta son la conexión y la ubicación de la red, las posibles vulnerabilidades, la información disponible sobre amenazas, etc. Los riesgos asociados y la reputación de la aplicación son analizados por los índices de confianza nativos de la nube (CCI) de Netskope, una base de datos de casi 60 000 aplicaciones en la nube (¡y que sigue creciendo!) que Netskope ha evaluado en función de unos 50 criterios basados en el riesgo. Estos criterios miden si una aplicación

está preparada para la empresa, teniendo en cuenta su seguridad, si es auditable y su continuidad empresarial.

Si se considera que el dispositivo es peligroso o que el comportamiento del usuario es inusual, se puede restringir el acceso o informar de ello al equipo de seguridad para que lleve a cabo una evaluación más exhaustiva. Si el dispositivo es seguro y el comportamiento del usuario es normal, puede concederse el acceso.

CONSEJO

La base de la protección de datos de Netskope es su SSE, que forma parte de la plataforma más amplia de Netskope Secure Access Service Edge (SASE). Esta solución de seguridad convergente y nativa de la nube consolida las tecnologías de seguridad vitales que he definido antes en una única plataforma integrada. Al combinar estas tecnologías en una única plataforma, Netskope facilita la gestión de su seguridad desde una ubicación central. Netskope SSE es nativo de la nube, lo que significa que puede ampliarse rápida y eficazmente para satisfacer las necesidades de su organización. También está diseñado para ser muy flexible, de modo que puedas personalizarlo para satisfacer sus necesidades específicas de seguridad.

Netskope SSE se ha diseñado teniendo en cuenta que la seguridad es algo más que la simple aplicación de políticas. También es importante formar a los empleados y fomentar un comportamiento seguro durante la manipulación de los datos. Por eso la solución preserva la capacidad del usuario para tomar decisiones empresariales, al tiempo que mantienesus datos a salvo. Por ejemplo, cuando se produce una infracción, Netskope SSE puede dirigir a los empleados a un curso de formación sobre cómo manipular los datos confidenciales, hacer preguntas para evaluar el contexto más a fondo o proporcionar orientación con consejos y mejores prácticas para trabajar de forma segura desde casa. Al adoptar un enfoque holístico de la protección de datos, Netskope te ayuda a crear una cultura de seguridad en su organización.

EN ESTE CAPÍTULO

- **Comparación de las soluciones DLP actuales y heredadas**
- **Seguridad en cualquier lugar desde donde accedas a los datos**
- **Uso de políticas y controles de acceso unificados**
- **Evaluación de las ventajas y los diferenciadores de Netskope DLP**

Capítulo 4
Por qué Netskope es la solución para un DLP actual

Los directores de seguridad de la información (CISO) y los equipos de seguridad de la información se enfrentan a menudo a una difícil decisión: ¿Deberían quedarse con soluciones heredadas de prevención de pérdida de datos (DLP) consolidadas, pero complejas y costosas, u optar por opciones en la nube fáciles de implementar que probablemente carezcan de la profundidad y amplitud que necesitan? Está preparado para responder a esa pregunta después de leer este capítulo y conocer las principales ventajas de todas las soluciones DLP basadas en la nube:

- **Pueden proporcionar una protección completa.** No importa dónde se almacenen sus datos, adónde se transfieran o cómo se acceda a ellos: un DLP en la nube puede protegerlos.
- **Pueden proteger los entornos en la nube.** Aplicaciones SaaS, servicios de IaaS en la nube pública y acceso web sin importar desde dónde se conecten los usuarios en la empresa actual habilitada para el trabajo híbrido.
- **Eliminan la necesidad de crear más infraestructuras porque pueden implementarse rápida y fácilmente como servicios en la nube.**
- **Protegen sus datos confidenciales sin sobrecargar los recursos de la red y los *endpoints*.** Un sistema DLP en la nube puede

gestionar todos los algoritmos de escaneado y detección de datos que necesita a la máxima capacidad.

- **Son más fáciles de integrar con una amplia gama de otro tipo de herramientas de seguridad.**
- **Proporcionan una mayor visibilidad de los datos que se transfieren y almacenan fuera de sus instalaciones corporativas.**
- **Son más fáciles de mantener y actualizar en tiempo real, y ofrecen la posibilidad de ampliarse más rápida y fácilmente que los modelos antiguos implementados a nivel local.**

Después de leer este capítulo, comprenderá bien cómo pueden aplicarse estas ventajas a su organización y estará bien equipado para tomar una decisión informada sobre qué DLP en la nube es el más adecuado para su empresa. A lo largo del recorrido, te ofrecemos información específica sobre los elementos diferenciadores de la plataforma Netskope.

Diferencia entre las distintas opciones de DLP en la nube

El DLP actual debe ofrecerse en la nube. Hay dos tipos disponibles. El DLP nativo de la nube suele estar integrado en plataformas de infraestructura como servicio (IaaS) y aplicaciones de *software* como servicio (SaaS) de los proveedores de servicios en la nube. Las soluciones DLP integradas en la nube suelen formar parte de un servicio o producto de seguridad, como una puerta de enlace web segura (SWG), un cortafuegos de próxima generación (NGFW) o un agente de seguridad para el acceso a la nube (CASB).

Tipo 1: Netskope DLP frente a soluciones puntuales nativas de la nube

Netskope DLP ofrece una serie de ventajas frente a las soluciones puntuales nativas de la nube más limitadas. Una ventaja clave es su protección más amplia mediante un motor único de políticas DLP de nivel empresarial, que garantiza la protección de los datos confidenciales en un conjunto más amplio de formatos, canales de comunicación y entornos, incluidas las aplicaciones SaaS, los servicios IaaS, las aplicaciones privadas, los servicios de correo electrónico, el uso compartido de archivos y las transacciones web en cualquier lugar donde se encuentren los usuarios. Netskope DLP también incluye protección DLP para *endpoints*, algo importante porque ayuda a garantizar la protección de todos sus datos sensibles, incluso en *endpoints* situados en lugares remotos que

pueden o no estar conectados a la nube a través de una red específica. El motor único de políticas DLP también reduce significativamente la complejidad en comparación con tener que gestionar diferentes reglas de políticas DLP para diferentes canales y diferentes servicios en la nube.

Otra ventaja de Netskope DLP es la precisión superior de su detección. Al escanear todos los tipos de archivos y formatos de datos posibles utilizando una amplia gama de algoritmos de detección de datos y el aprendizaje automático para comprender una gran variedad de información y documentos, así como su contexto específico, es capaz de identificar y clasificar con precisión los datos confidenciales, incluso si estos se almacenan y transfieren en diferentes estructuras, formatos, idiomas o están incrustados en imágenes. Esto es importante porque ayuda a garantizar que no se filtre ni exponga accidentalmente ningún tipo de dato confidencial (algo que podría tener graves consecuencias para una organización) y que el sistema produzca verdaderos eventos de seguridad de datos en lugar de falsos positivos.

Por último, Netskope DLP incorpora un contexto *Zero Trust*, es decir, se ha diseñado para funcionar en un marco de seguridad *Zero Trust*. Esto es importante porque ayuda a garantizar que todos los accesos a los datos confidenciales se controlen y supervisen cuidadosamente, en el contexto de riesgo adecuado, reduciendo el riesgo de acceso no autorizado, exposición excesiva o filtración de datos.

En la actualidad, muchos proveedores de servicios en la nube y proveedores de SaaS ofrecen funciones nativas de DLP en sus plataformas. Estas soluciones centradas en la nube y rápidamente disponibles suelen ser las elegidas por las organizaciones que siguen una estrategia que da prioridad a la nube o por las que acaban de iniciar su andadura en la protección de datos. Aunque estas soluciones pueden abordar los casos de uso específicos de protección de datos en la nube para los que fueron diseñadas, pueden carecer de una protección amplia y no ser tan completas como las soluciones DLP heredadas.

ADVERTENCIA

Algunas empresas empiezan con estas soluciones DLP nativas de la nube porque pueden ser rápidas y fáciles de implementar. Sin embargo, es importante acercarse a estas soluciones con los ojos bien abiertos, comprendiendo que pueden no ser suficientes para satisfacer todas las necesidades en materia de protección de datos. En algunos casos, las organizaciones pueden verse obligadas a adoptar múltiples opciones de DLP desconectadas y aisladas para casos de uso futuros, lo que genera una estrategia de protección de datos fragmentada y potencialmente menos eficaz.

Tipo 2: no todas las soluciones DLP integradas en la nube son iguales

A la hora de elegir una solución DLP en la nube, ten en cuenta que muchas de las soluciones más recientes del mercado presentan importantes deficiencias:

- Puede que ofrezcan una amplia protección, pero carecen de la profundidad tecnológica y las funciones necesarias para proteger los datos confidenciales de su organización con eficacia y precisión en todos los casos de uso actuales.
- Puede que ofrezcan algunas de las metodologías y funciones más recientes para algunos casos de uso y formatos de datos específicos, pero carecen de la amplitud de protección necesaria para proteger los datos confidenciales de tu organización de forma exhaustiva.

ADVERTENCIA

Algunas de las soluciones DLP en la nube más recientes pueden ir acompañadas de buen marketing, pero distan mucho de ser tan sofisticadas y consolidadas como las soluciones DLP heredadas a las que pretenden sustituir.

Es importante que investigue y comparea fondo las soluciones DLP para asegurarse de elegir una que satisfaga eficazmente las necesidades de su organización. Fíjese en factores como la consolidación y sofisticación de sus capacidades de detección de datos (por ejemplo, cuántos tipos de archivos puede escanear y cuántos identificadores de datos utiliza, incluidos los tipos de datos específicos de distintos países), la variedad de canales que abarca, su capacidad para adaptarse a riesgos y entornos cambiantes, y el nivel de integración y personalización que ofrece.

Si está pensando en utilizar una solución DLP en la nube, quizá se pregunte qué tipo es el mejor para usted. Veamos con más detalle qué hay que tener en cuenta:

- **Amplitud de la protección:** las soluciones DLP integradas suelen incluirse como parte de un SWG, CASB o NGFW, y a menudo forman parte de un servicio de acceso a la red *Zero Trust* (ZTNA). Estas soluciones se suministran desde la nube y se integran normalmente en un servicio de seguridad de red. Su alcance es limitado y carecen, por ejemplo, de protección de datos para correos electrónicos de salida, *endpoints*, un espectro más amplio de aplicaciones SaaS y sus instancias específicas (es decir, cuentas corporativas frente a personales).
- **Limitaciones de las soluciones:** tenga en cuenta que estas soluciones pueden no abarcar todos los casos de uso actuales y

tradicionales, como la colaboración en la nube con usuarios externos, las transferencias de datos a través de correo electrónico personal o borradores de correo electrónico, las transferencias de archivos por USB, las capturas de pantalla e imágenes de documentos confidenciales, las nuevas plantillas de cumplimiento, los datos en idiomas y formatos extranjeros, etc. Y lo que es más importante, es posible que su capacidad de detección sea más débil. Además, sus capacidades de aprendizaje automático e IA pueden ser decepcionantes.

- **Precisión de la detección de datos confidenciales:** muchas de las soluciones DLP en la nube más recientes se quedan cortas en su capacidad para detectar con precisión y granularidad los datos confidenciales. A menudo solo escanean un número limitado de tipos de archivos y carecen de la amplitud de identificadores de datos que poseen las soluciones más consolidadas. Estas soluciones pueden parecer excepcionales al centrarse en una o dos funciones llamativas, pero en última instancia se quedan cortas en su capacidad de proporcionar una protección de datos completa.

  Una solución consolidada ofrecerá miles de identificadores de datos predefinidos, incluido un amplio abanico de información de identificación personal (PII), pasaportes, cuentas bancarias, información bancaria internacional, documentos nacionales de identidad, datos financieros, datos médicos, datos personales e información específica del sector, así como idiomas de distintos países e identificadores personalizables. También proporcionaría una amplia gama de perfiles de políticas predefinidos para respaldar casos de uso y requisitos de cumplimiento, como el Reglamento General de Protección de Datos (RGPD), la Ley de Privacidad del Consumidor de California (CCPA), el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA) y la Ley de Gramm-Leach-Bliley (GLBA), por mencionar solo algunas.

- **Integración en una plataforma:** un DLP en la nube debe integrarse estrechamente con una plataforma de seguridad más amplia para proteger eficazmente los datos confidenciales dentro de todo el contexto de riesgo disponible de usuarios, dispositivos, redes, aplicaciones, comportamientos y destinos. Una solución DLP bien integrada utilizará la inteligencia de otros puntos de control (como el análisis del comportamiento de los usuarios, las puertas de enlace web seguras de próxima generación, CASB, ZTNA y la gestión de la posición de seguridad) para comprender a fondo la posición de seguridad de una organización y los riesgos asociados a cada

interacción con datos confidenciales. Esto incluye ser consciente de las instancias específicas de aplicaciones SaaS y dispositivos en uso, distinguir entre identidades de usuario de cuentas de correo electrónico personales y corporativas, los destinatarios de un intercambio de datos y mucho más. Este nivel de integración permite un enfoque más preciso y granular para detectar y proteger los datos confidenciales.

CONSEJO

No todas las soluciones de protección de datos son iguales y muchas carecen de la consolidación y sofisticación necesarias para sustituir eficazmente a las soluciones heredadas. Algunos proveedores pueden ofrecer DLP como complemento a sus productos principales, pero sin la amplitud y profundidad necesarias, estas soluciones pueden no proporcionar el nivel de protección que las organizaciones necesitan. Debe comprobar cualquier solución que esté pensando utilizar para garantizar que admite todos los tipos y volúmenes de datos necesarios hoy en día, y que protege cualquier punto de salida de datos a nivel local y en la nube sin compromisos.

Evalúe cuidadosamente las capacidades de las distintas soluciones DLP y elija una que satisfaga las necesidades de su organización, tanto en el presente como en el futuro. Para tener éxito, es esencial contar con un conjunto de funciones consolidadas y un proveedor especializado. Confiar únicamente en lo básico puede dar lugar a imprecisiones, detecciones parciales y miles de falsos positivos.

Con una década de innovación continua y plena dedicación a la protección de datos, Netskope ha sido reconocido como un abanderado del sector en comparación con otros proveedores de SASE y perímetro de servicio de seguridad (SSE). En los siguientes apartados, profundizaremos en las funciones y capacidades que distinguen a Netskope DLP.

Cómo Netskope DLP mantiene su seguridad

Netskope DLP es una solución completa e integrada en la nube que ayuda a proteger sus datos en todos los canales fundamentales, como las distintas nubes, redes, correos electrónicos, *endpoints* y usuarios que estén en cualquier lugar. Se ha diseñado para tener en cuenta los riesgos y el contexto, por lo que puedes confiar en que sus datos estarán siempre seguros a dondequiera que vayan.

Netskope DLP está *totalmente integrado* en el exhaustivo Netskope SSE descrito en el capítulo 3 y se entrega como parte de una plataforma SASE

completa. Esto significa que obtendrá una plataforma de seguridad convergente y nativa de la nube que ayuda a eliminar los puntos ciegos, proporciona coherencia, mejora el rendimiento y reduce los costos y la complejidad.

Netskope DLP abarca todos los canales y la transferencia de datos, como se muestra en la figura 4-1, por lo que puedes estar seguro de que su información confidencial estará siempre protegida. Incluyendo:

- Casi 60 000 aplicaciones SaaS, con nuevas aplicaciones clasificadas dinámicamente, y cada instancia de estas aplicaciones.
- Todos los principales proveedores de IaaS, incluidos Amazon Web Services (AWS), Google Cloud y Microsoft Azure.
- Aplicaciones privadas en el centro de datos o alojadas en la nube pública.
- Sus redes corporativas y sucursales.
- Su teléfono móvil personal.
- Todos los servicios de correo electrónico, tanto locales como en la nube, incluido el correo web.
- Todos los *endpoints* de sus empleados, dentro y fuera de las instalaciones.

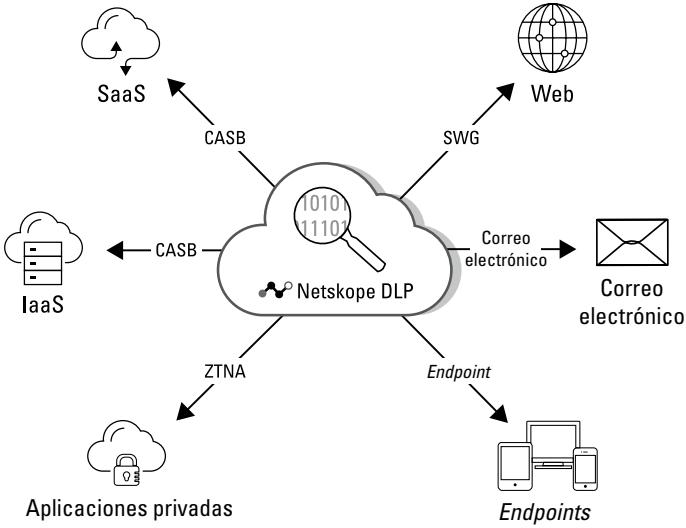

FIGURA 4-1: Netskope DLP protege sus datos, estén donde estén.

Diferenciadores clave

Un mito de las soluciones DLP heredadas es que son imprecisas; en realidad, lo peor son los falsos positivos, cuya solución requiere una mayor precisión. Lo explicamos en el capítulo 2, donde también presentamos y explicamos los ingredientes clave que pueden ayudar a los sistemas DLP a ser más precisos. Aquí explicamos cómo Netskope ha convertido estos ingredientes clave en diferenciadores clave y ha proporcionado una solución DLP actual que se puede personalizar y automatizar para satisfacer las necesidades de su empresa.

Protección total de todos los canales críticos con políticas unificadas

Los datos confidenciales que se mueven por todas partes fuera de las instalaciones corporativas tradicionales se vuelven más difíciles de rastrear y proteger y son más propensos a quedar expuestos, tanto de forma intencionada como accidental. El DLP en la nube de Netskope descubre, supervisa y protege de forma exhaustiva los datos confidenciales en movimiento, en reposo y en uso en todo el ecosistema empresarial, incluidas las aplicaciones SaaS, las nubes públicas de IaaS, las redes corporativas y las sucursales, el personal móvil, los servicios de correo electrónico y los *endpoints* de los empleados.

Proporciona políticas unificadas de protección de datos para todas las ubicaciones donde se almacenan o se utilizan los datos, o a las que se transfieren y se entregan desde un servicio centralizado en la nube.

La consola única, con control de acceso basado en funciones, garantiza que las configuraciones de políticas, la supervisión, la elaboración de informes y la respuesta ante incidentes para todos los canales sean gestionados por profesionales a través de un único panel.

Detección y protección superiores de los datos confidenciales

Los identificadores de datos son fundamentales para ayudar a una solución DLP a identificar datos confidenciales basándose en determinadas características, como palabras clave descriptivas, expresiones regulares, número de dígitos, caracteres especiales, patrones, análisis de proximidad, etc. Al comprar una solución DLP, asegúrese de que dispone de las capacidades de identificación necesarias para cubrir todos sus casos

de uso presentes y futuros. Una buena solución DLP debe ser capaz de proporcionar varios miles de identificadores predefinidos para buscar e identificar con precisión la más amplia variedad y la más mínima variación de datos confidenciales. Esto es especialmente importante para las empresas globales que necesitan tener identificadores para varios países. Netskope ofrece todas esas funciones con el aprendizaje automático y la posibilidad de personalizar de forma granular los identificadores y las plantillas de políticas, además de garantizar la cobertura de todas sus necesidades de protección de datos.

CONSEJO

No se centres solo en los identificadores de datos que necesita ahora. Necesita una solución a prueba de futuro que pueda abarcar tipos de datos, aplicaciones y normativas aún por inventar. Busque una solución con miles de identificadores de datos predefinidos y plantillas de políticas para normativas de cumplimiento como el GDPR y la CCPA. Y no olvide la posibilidad de crear y modificar los identificadores de datos personalizados para adaptarlos a sus necesidades específicas.

Hay miles de tipos de archivos que pueden contener información confidencial, como los archivos comprimidos (ZIP, RAR, ISO, etc.), presentaciones, correos electrónicos, imágenes (BMP, JPG, PNG, etc.), hojas de cálculo, archivos de diseño asistido por ordenador (CAD), publicaciones en redes sociales, formularios en línea, mensajes de *chat*, archivos adjuntos y gráficos. Son muchos tipos diferentes de datos que hay que controlar, por lo que se necesita una solución DLP que pueda gestionarlos todos.

La escala de la coincidencia exacta de datos (EDM) es un aspecto fundamental a tener en cuenta, sobre todo si tiene una gran empresa (o planea tenerla algún día). La solución DLP debe ser capaz de procesar millones o incluso miles de millones de registros con facilidad; las soluciones modernas DLP basadas en la nube, como Netskope, pueden aprovechar la informática en la nube para realizar análisis de huellas digitales de datos a gran escala, incluso en *endpoints*, sin ralentizar otros procesos esenciales. De este modo, toda la recopilación de datos personales de empleados, clientes y socios, y mucho más, estará totalmente protegida.

CARIÑO, VAMOS A REDUCIR LA SUPERFICIE DE ATAQUE

CONSEJO

Las organizaciones que quieran proteger sus datos confidenciales de las amenazas cibernéticas deben eliminar cualquier brecha en la protección. La *superficie de ataque* es la cantidad total de vulnerabilidades potenciales o puntos de entrada que los atacantes podrían aprovechar y que las personas internas podrían utilizar de forma intencionada o maliciosa. Limitar la superficie de ataque puede hacer más difícil encontrar y explotar los puntos débiles. Cerrar cualquier brecha existente en la protección también puede reducir significativamente el riesgo de que una organización sufra un ataque con éxito y quede expuesta de forma accidental. Asegurarse de que todos los dispositivos, aplicaciones y redes están protegidos adecuadamente es esencial para eliminar cualquier resquicio que pueda facilitar una exposición de riesgo.

Para garantizar una mayor protección de sus datos sensibles, busca capacidades de detección avanzadas como reconocimiento óptico de caracteres (OCR), IA, aprendizaje automático, huellas digitales de archivos y estrategias *Zero Trust* en tu solución DLP. Todas ellas están incluidas en Netskope DLP (y hablamos de ellas con más detalle en el capítulo 2).

Netskope DLP puede identificar con precisión los datos confidenciales, incluso si están almacenados en formatos modernos no estructurados, como imágenes (capturas de pantalla y fotografías), o en diferentes idiomas. Gracias a sus sofisticados clasificadores de aprendizaje automático, la solución es capaz de discernir imágenes confidenciales, como permisos de conducir, tarjetas de crédito, documentos de identidad, contratos, patentes, documentos de fusiones y adquisiciones y cheques, incluso si dichas imágenes no son claras, están borrosas, distorsionadas y dañadas. Protege activamente la información confidencial, por lo que puede confiar en que mantendrá sus datos seguros en el mundo de la nube que está en constante evolución. Esto también reduce la carga de trabajo de sus equipos de seguridad al identificar y proteger automáticamente los datos confidenciales.

Netskope DLP cuenta con diversas herramientas avanzadas de clasificación basadas en aprendizaje automático, que incluyen miles de identificadores de datos. Escanea más de 1600 tipos de archivos diferentes con políticas de detección contextual, coincidencia exacta de datos sumamente ampliable, huella digital de documentos estructurados y no estructurados, clasificación precisa de imágenes basada en aprendizaje automático, OCR avanzado y clasificadores de datos por IA/aprendizaje automático para facilitar el descubrimiento y la identificación de los datos.

Protección de datos en función del contexto y del riesgo

La protección eficaz de los datos depende del contexto. Al supervisar el tráfico entre usuarios y aplicaciones, puede ejercer un control granular y permitir o impedir el uso arriesgado de los datos confidenciales en función de muchos factores, como quién es el usuario, qué intenta hacer y por qué lo hace. Este enfoque centrado en los datos es la mejor manera de gestionar el riesgo en las empresas híbridas actuales.

La fatiga de la respuesta ante incidentes y la interrupción del negocio son problemas del pasado con Netskope DLP. De hecho, la solución Netskope DLP va más allá del enfoque estático de descubrir información confidencial y responder a unas políticas de vulneración predefinidas, ya que tiene en cuenta el contexto de la organización y los riesgos de seguridad para activar dinámicamente la protección adecuada en función de los cambios en las condiciones.

Netskope DLP se integra de forma nativa en la completa solución Netskope Security Service Edge (SSE) de Netskope, una plataforma de seguridad nativa en la nube totalmente convergente que consolida tecnologías de seguridad, como SWG, CASB y UEBA, en una plataforma nativa en la nube unificada e integrada. Este enfoque elimina los puntos ciegos en materia de seguridad, aporta coherencia a las políticas y reduce drásticamente los costosy la complejidad. La plataforma conoce continuamente el comportamiento de los usuarios, su geolocalización, las posiciones de seguridad, los riesgos de los dispositivos, los riesgos y reputación de las aplicaciones, las instancias de aplicaciones personales, etc., y permite al DLP adaptar la respuesta a los incidentes a los verdaderos incidentes de seguridad de los datos, reduciendo los falsos positivos, la clasificación de incidentes y la interrupción del negocio.

Puede aumentar la visibilidad y la reducción de los riesgos en todos los vectores clave con una única solución convergente de protección de datos SASE basada en principios *Zero Trust* y controles avanzados de protección de datos. Además, puede simplificar la clasificación de datos, la definición de políticas y la gestión de incidentes con una plataforma convergente que utiliza el aprendizaje automático, informes enriquecidos y análisis avanzados. Y gracias a las políticas flexibles basadas en el contexto y a un agente ligero, puede mejorar la agilidad del usuario final y reducir la fricción.

RECUERDA

Para garantizar el éxito de su programa de protección de datos, debe formar a sus empleados y fomentar prácticas seguras para la manipulación de los datos. Para ello, Netskope DLP ofrece programas de formación y concienciación para los usuarios en tiempo real. También se

integra con los principales sistemas de gestión del aprendizaje y dispone de un portal de usuario final personalizable para la autoformación sobre protección de datos.

Trabaje de forma más inteligente con DLP

Netskope DLP se suministra desde la nube, por lo que no depende de componentes locales. También ofrece una protección siempre activa y actualizada, eliminando la necesidad de actualizaciones manuales de *software* que deben llevar a cabo las soluciones DLP heredadas.

Con las políticas unificadas de protección de datos y el control de acceso basado en funciones (RBAC) de una sola consola, gestionar las configuraciones de políticas, la supervisión, la elaboración de informes y la respuesta ante incidentes es pan comido.

En el pasado, las empresas tenían que crear distintas políticas para cada canal (por ejemplo, web, correo electrónico y cada aplicación individual), lo que consumía muchos recursos y tiempo. Netskope DLP es un servicio en la nube unificado y centralizado en el que puede definir una única política para su empresa y sincronizarla automáticamente en todos los canales. De este modo, puedes crear su política una vez y no tiene que replicarla ni perfeccionarla constantemente en diferentes lugares.

CONSEJO

Las soluciones DLP heredadas necesitaban muchos administradores de sistemas para crear y gestionar las políticas. La actual escasez de personal cualificado hace que sea importante elegir una solución que sea más fácil de gestionar.

Una interfaz de usuario (IU) centralizada y una consola de gestión unificada también son cruciales para lograr una respuesta eficaz y eficiente ante incidentes. Es posible que haya tenido consolas separadas para las herramientas locales y en la nube, lo que puede resultar confuso y ralentizar la gestión. Incluso hoy en día, algunos de los últimos proveedores de DLP siguen utilizando un método con varias consolas, lo que puede complicar aún más las cosas. Con Netskope DLP, recibe todas las infracciones en un solo lugar, la detección de datos confidenciales y la respuesta ante incidentes se proporcionan de forma coherente y en tiempo real, así puedes responder con rapidez y eficacia ante las posibles amenazas.

CONSEJO

Una IU centralizada y una consola de gestión unificada le permiten hacer un seguimiento de todo y agilizan el proceso de respuesta ante incidentes.

Capítulo 5
Diez claves para una transición exitosa a un DLP moderno en la nube

Sustituir implementaciones de seguridad heredadas y establecidas desde hace tiempo, como la prevención de pérdida de datos (DLP), puede parecer abrumador. Su iteración actual es el resultado de años de procesos complicados e interrelacionados. Como en un castillo de naipes, cada elemento está en contacto con los demás, pero si se quita uno, toda la estructura puede venirse abajo.

¡No se deje intimidar! Merece la pena aspirar a una transformación digital innovadora. Y el cambio no tiene por qué producirse de la noche a la mañana. De pequeños pasos y utilice sus inversiones actuales con prudencia para poder conseguir una solución integral de protección de datos que proteja la información confidencial en todas las plataformas, ya sean a nivel local o en la nube.

- **Evalúe sus necesidades de protección de datos.** Tómese su tiempo para evaluar a fondo el entorno tecnológico actual de tu organización. Identifique y trate de comprender qué datos deben protegerse, qué servicios y repositorios se utilizan para almacenar y procesar información confidencial, y cómo utilizan estos servicios los departamentos y las personas. Haga que su equipo de seguridad

identifique y evalúe específicamente todas las aplicaciones corporativas, servicios de correo electrónico, herramientas de colaboración, ubicaciones de red, prácticas de trabajo híbridas de los usuarios, dispositivos de conexión y procesos empresariales para trazar los flujos de datos y determinar cómo se comparten los datos entre los empleados o con terceros ajenos a la organización.

CONSEJO

No se limite al equipo de seguridad. El director de datos de su empresa, el personal jurídico y el personal de RR. HH. son algunas de las partes interesadas que pueden aportar información sobre cómo se utilizan los datos en su empresa.

Examine todas las categorías de datos almacenados y cualquier transacción que implique datos que se mueven a través de redes. Averigue qué prioridad debe darse a la protección de los distintos tipos de datos en su organización. Esta fase puede representar una victoria rápida para las organizaciones que necesitan apoyo para el cumplimiento de normativas o que requieren nuevas implementaciones de DLP debido a la ineficacia de los sistemas heredados.

- **Identifique y reduzca sus mayores riesgos.** Cuando se plantee la transición a una solución de protección de datos en la nube, determine qué áreas de su entorno tecnológico actual plantean los mayores riesgos. Piense en el intercambio involuntario de datos, la exfiltración maliciosa y otras amenazas cibernéticas basadas en la nube que están asociadas a las aplicaciones corporativas de *software* como servicio (SaaS), el correo electrónico en la nube y la infraestructura como servicio (IaaS). La solución de agente de seguridad para el acceso a la nube (CASB) de Netskope, líder del mercado, incorpora DLP como componente principal para proteger la seguridad de los datos, tanto de las aplicaciones en la nube autorizadas por la empresa como de las aplicaciones no autorizadas (se engañaría a ti mismo si cree que no las hay).
- **Elija bien a su proveedor de protección de datos.** Asegúrese de elegir un proveedor que satisfaga las necesidades de su empresa en todos los entornos actuales y en el futuro inmediato. Netskope DLP es el único proveedor que ofrece una protección completa para todas las necesidades de la nube y más allá. Esto incluye la protección de datos en reposo, en tránsito y en uso en nubes y entornos locales, DLP para *endpoints*, DLP para correo electrónico, DLP de red para web y correo electrónico, DLP para SaaS e IaaS, y DLP para aplicaciones privadas. Esta protección integral de todos los movimientos de datos actuales garantiza a las empresas la máxima visibilidad de todo su sistema y también de las ubicaciones no fiables. Evalúe cuidadosamente hasta dónde llegan las capacidades de cada solución,

por ejemplo, cuántos y qué tipos de archivos es capaz de escanear la solución, si puede comprender formatos de imagen y la protección de la más amplia variedad de datos confidenciales posible, incluidos los identificadores internacionales y específicos de cada país. Tenga en cuenta la capacidad del sistema para aprovechar al máximo el contexto de riesgo y de negocio y, por tanto, para tomar decisiones automatizadas e informadas de respuesta ante incidentes con cada uso de los datos confidenciales de forma adaptativa. Básicamente, asegúrese de no adoptar un enfoque superficial ante la protección de datos que cree más problemas que soluciones.

- **Proteja sus servicios de correo electrónico y sus aplicaciones de colaboración.** Descubra todo el poder de la protección del correo electrónico y SaaS basada en la nube con Netskope DLP. Esta solución DLP integral está diseñada para proteger toda la información confidencial de su empresa, incluidos los correos electrónicos confidenciales de salida y las comunicaciones asíncronas a través de aplicaciones de colaboración basadas en SaaS, como Slack y Teams. Con interfaces de programación de aplicaciones (API), protección en tiempo real en línea, protección para colaboraciones externas e incluso conocimiento de instancias, como correo electrónico e instancias SaaS personales frente a instancias corporativas de los mismos servicios, puedes estar seguro de quesus datos corporativos estarán protegidos pase lo que pase. Con la ayuda de Netskope, puede estar tranquilo en lo que respecta a la colaboración y las comunicaciones.
- **Proteja su correo electrónico basado en la nube.** Descubra todo el poder de la protección del correo electrónico basado en la nube con Netskope DLP. Esta completa solución DLP está diseñada para mantener segura toda la información confidencial de su empresa, protegiéndola contra ataques malintencionados y el intercambio involuntario de datos. Con interfaces de programación de aplicaciones (API), protección en línea en tiempo real e incluso protección de datos a través de instancias de correo electrónico personales, puede estar seguro de que sus datos corporativos estarán protegidos pase lo que pase. Con la ayuda de Netskope, estará tranquilo a la hora de migrar su servicio de correo electrónico a la nube.
- **Datos seguros en movimiento.** Los datos que se transfieren a través de distintas ubicaciones, conexiones, servicios y dispositivos (como redes domésticas, oficinas corporativas, sucursales, dispositivos corporativos y dispositivos personales) pueden ser difíciles de gestionar y proteger. Las soluciones DLP tradicionales conectadas a proxy no siempre proporcionan una protección suficiente cuando se trata de datos en movimiento. Netskope ofrece un servicio DLP unificado que se presta a través de toda la plataforma inteligente de

servicios de Netskope Security Service Edge (SSE), y está diseñado para proteger los datos confidenciales desde cualquier lugar en el que se encuentren trabajando los empleados. De este modo, dispondrá de la máxima seguridad para sus transacciones de datos, incluidas todas las ventajas de los principios *Zero Trust* y todo el contexto de riesgo disponible, y ninguna de las molestias derivadas de las configuraciones de *hardware* dudosas. Con la innovadora solución DLP de Netskope, puede garantizar la seguridad de sus datos en todo momento y en todo lugar.

- **Proteja los datos en los dispositivos endpoint de los empleados.** Aunque cada vez se almacenan más datos en la nube, todavía es importante asegurarse de que los archivos confidenciales no se pierdan ni sean robados en *endpoints* que pueden o no estar conectados a una red corporativa, o no estar conectados en absoluto. Tanto si los datos confidenciales se crean en el *endpoint* como si se descargan de la nube, Netskope DLP puede ayudar en este aspecto. Esta solución ligera para *endpoints* ofrece todas las funciones avanzadas de DLP como clasificadores basados en aprendizaje automático (AA), reconocimiento óptico de caracteres (OCR), huellas digitales de archivos, coincidencia exacta de datos (EDM), entre otras, con una utilización mínima de recursos porque aprovecha la nube. Permite una variedad de casos de uso (incluida la detección de datos transferidos a través de USB) y proporciona protección de los dispositivos USB y otras políticas de control de dispositivos para garantizar la seguridad de sus datos confidenciales independientemente del lugar desde el que se conectensus empleados.
- **Siga usando lo que funciona mientras planifica el futuro.** Si ha invertido recientemente en las capacidades de DLP de un proveedor de servicios en la nube o de SaaS, puede tener sentido seguir con ellos a corto plazo. Por ejemplo, si un proveedor de SaaS ya está haciendo un buen trabajo protegiendo sus aplicaciones de ofimática, no tienes por qué cambiar inmediatamente. Pero esté atento al punto en el que esté gestionando demasiadas políticas independientes y desconectadas. Si deseaampliar la protección de datos a varias nubes y aplicaciones SaaS, podría acabar lidiando con demasiadas consolas y políticas diferentes. Netskope DLP ofrece una solución más sencilla: una consola con políticas coherentes que pueden proteger sus datos independientemente de dónde se almacenen o del lugar desde el que se acceda a ellos.
- **Desbloquée la protección integral de datos.** Netskope DLP ofrece un enfoque actual ante la protección de datos, más eficiente y eficaz que nunca. Las tecnologías de detección avanzadas, como el AA, las huellas digitales de los datos y el reconocimiento de imágenes, se

utilizan con todo su potencial y a una escala sin precedentes, incluso en *endpoints*, ya que la capacidad informática se suministra desde la nube. La consola única con políticas unificadas simplifica la gestión de las necesidades de protección de datos de toda la organización. La recopilación y el análisis de información sobre riesgos e información contextual sobre usuarios, dispositivos, datos, redes, nubes y comportamientos permite a Netskope DLP evaluar cada interacción que se produzca con datos confidenciales y adaptar dinámicamente la respuesta a cada infracción específica de las políticas. Este nuevo enfoque favorece la colaboración segura y las prácticas actuales de intercambio de datos y no obstaculiza la productividad; además, reduce los falsos positivos y produce resultados más precisos en la protección de datos. Netskope DLP está integrado de forma nativa en la plataforma global Netskope SSE y, por tanto, siempre tiene conocimiento de los riesgos empresariales, los comportamientos y las vulnerabilidades de seguridad. Netskope DLP está totalmente integrado con Netskope SSE, por lo que las organizaciones siempre tienen conocimiento de los riesgos empresariales, los comportamientos y las vulnerabilidades de seguridad.

- **Conserve los conocimientos internos.** La transición a un nuevo DLP basado en la nube puede parecer abrumadora, pero no tiene por qué serlo. Aproveche la experiencia y los conocimientos de las personas que han mantenido su sistema DLP heredado, incluidos los administradores de políticas y el equipo de respuesta ante incidentes. Su experiencia puede ayudar a garantizar que se reproduzcan las mejores prácticas en la transición a un sistema basado en la nube. Esa experiencia también puede ayudar a su organización a cumplir las expectativas tecnológicas mediante la elaboración de perfiles de políticas de cumplimiento y el desarrollo de nuevos flujos de trabajo de corrección de incidentes. Netskope DLP ayuda a reducir las demandas que se exigen a su equipo de DLP, por lo que sus equipos de seguridad dedicarán menos tiempo a gestionar incidentes frustrantes y más tiempo a centrarse en iniciativas proactivas que mantengan la seguridad de la empresa.
- **Valore la madurez por encima de las modas.** El éxito requerirá algo más que conocimientos técnicos. Desde la elaboración de métricas para la alta dirección hasta las directrices y los elementos de acción para el personal, hay mucho que tener en cuenta. Asegúrese de apoyarse en los equipos de soporte de su proveedor para que te ayuden a estructurar su viaje y, en última instancia, a desbloquear el valor de la innovación de la empresa para que el viaje merezca verdaderamente la pena.

Security that's ready for anything

Data Protection

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, **visit netskope.com**.

netskope

Prepárese para un futuro en la nube con tecnología DLP moderna

La rápida adopción de la nube y la tendencia a trabajar desde cualquier lugar hacen que las técnicas de protección de datos que antes eran de vanguardia resulten ahora lamentablemente inadecuadas. Los esfuerzos en materia de seguridad de los datos deben proporcionar una protección coherente allá donde vayan los datos y las personas. La solución ideal para la prevención de pérdida de datos (DLP) actual debe crearse para la nube, no adaptarse a los casos de uso en la nube. Debe aplicar técnicas *Zero Trust*, reducir la complejidad y proporcionar una aplicación coherente de las políticas, en todas partes.

Al interior...

- Evalúe su enfoque ante la protección de datos
- Proteja los datos y respalda los objetivos empresariales
- Aprenda cómo funciona el DLP moderno
- Minimice el acceso no autorizado a los datos
- Simplifique las políticas de Mientras garantiza su eficacia su eficacia
- Mueva datos a la nube y entre aplicaciones en la nube de forma segura

netskope

Carmine Clementelli es experto en ciberseguridad y líder tecnológico en seguridad de datos, seguridad en la nube, Zero Trust y perímetro de servicio de seguridad (SSE) en Netskope. Tiene décadas de experiencia como autor, conferencista y asesor, anteriormente en Palo Alto Networks, Symantec y otras organizaciones internacionales.

Visite Dummies.com®
para ver vídeos, fotografías paso a paso, artículos con instrucciones o para comprar.

ISBN: 978-1-394-20764-0
Prohibida la venta

para dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.