Acronis

DOCUMENTO TÉCNICO

Cómo lanzar y escalar los servicios de DLP: una guía para MSP

A pesar del aumento del nivel de concienciación, y de la abundancia de protocolos y normativas de seguridad, las empresas de todos los tamaños llevan años sin conseguir dar una respuesta al riesgo de fuga de datos. De hecho, este riesgo va en aumento. Según el informe 2021 Year End Report: Data Breach QuickView, de Risk Based Security, ese año se filtraron más de 22 000 millones de registros, con lo cual 2021 ocupa la segunda posición desde 2005 en cuanto a cantidad de datos confidenciales comprometidos. La inmensa mayoría de estos registros quedaron expuestos debido a fugas de datos. Una fuga de datos, también conocida como filtración, se define como una violación de la seguridad en la que se divulgan datos confidenciales, sensibles o protegidos, ya sea de forma accidental o deliberada, a un entorno no fiable o a usuarios no autorizados, internos o externos a la organización.

Pero ¿qué provoca las fugas de datos? Hay dos causas principales:

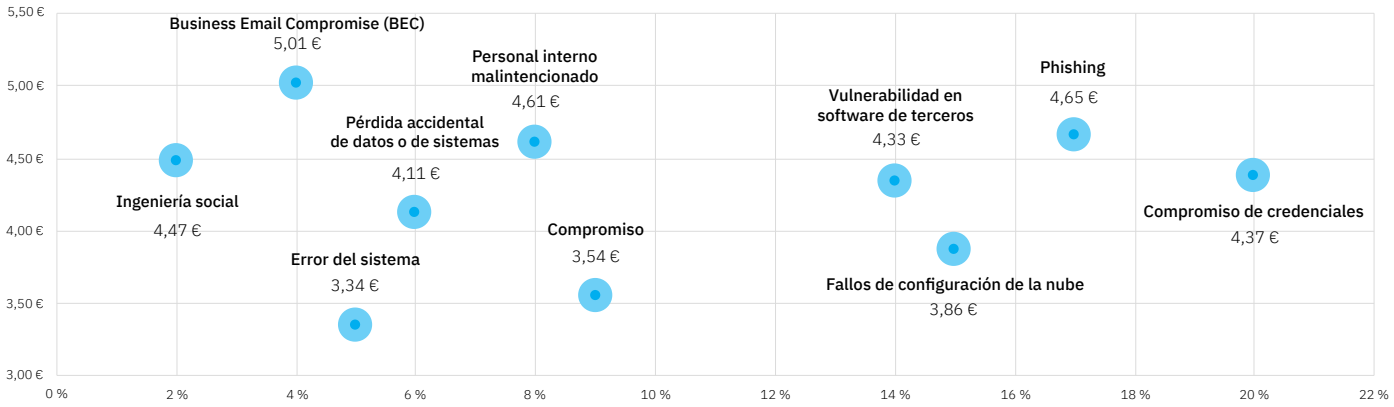
1. Ciberamenazas externas

Tal y como define el marco MITRE ATT&CK, la fuga de datos se encuentra entre las últimas tácticas que aplican los ciberdelincuentes durante un ataque. En más del 80 % de los casos los atacantes tienen motivaciones financieras, según el informe Verizon 2022 Data Breach Investigation Report.

Por eso, en la mayoría de los ataques, los datos confidenciales son el principal objetivo. Una vez que los ciberdelincuentes consiguen acceso al entorno corporativo, pueden intentar filtrar los datos a través de numerosos canales. El aumento de complejidad de los ataques y de la capacidad del atacante para sortear las capas de seguridad, incrementa enormemente el riesgo para los datos de las empresas.

2. Riesgos internos

Si bien el antimalware y otras tecnologías de seguridad de endpoints pueden detectar y detener los ataques externos, ganan fuerza otros riesgos para los datos de las empresas: los que se originan en el interior. Un caso habitual es cuando los usuarios transmiten de forma inadvertida datos a personas no autorizadas (por correo electrónico, por ejemplo). Esto puede deberse a errores accidentales de los empleados, a fallos de configuración de las tecnologías o bien a la existencia de personal interno malintencionado. Todo ello supone una seria amenaza para las empresas que puede generar violaciones de datos de graves consecuencias financieras.



Hay que destacar que, aunque algunas organizaciones subestiman el impacto de los riesgos internos, según el informe de Ponemon Institute sobre el coste de las fugas de datos de 2021, aproximadamente un tercio de las violaciones de datos cuentan con la participación de personal interno.

¿Qué impacto tienen las fugas de datos en las empresas?

Las fugas de datos presentan un riesgo grave para las empresas. La filtración de datos confidenciales a partes no autorizadas puede dar lugar a:

- **Incumplimiento de normativas**. El almacenamiento, el acceso y la protección de los datos sensibles, como los de identificación personal (PII) de empleados y clientes, la información médica protegida (PHI) o los detalles de los titulares de tarjetas bancarias, están sujetos al estricto cumplimiento de las normativas locales e internacionales (RGPD, CCPA, HIPAA, PCI-DSS, etc). Algunas de estas normativas, como el RGPD, incluso exigen que los incidentes se denuncien en un plazo concreto. En caso de retraso en la comunicación de una fuga de datos recogida en las normativas, las empresas se enfrentan al pago de cuantiosas multas e incluso a la pérdida de sus certificados de conformidad.
- **Daños financieros**. Una vez que se filtran los datos, además de las sanciones administrativas que deberán afrontar los clientes MSP, los proveedores de servicios también se exponen al riesgo de sufrir daños financieros como resultado de su responsabilidad en cuanto a la seguridad de los clientes, lo que puede generar litigios legales. Además, la filtración de secretos comerciales o propiedad intelectual podría provocar otras pérdidas financieras para las empresas e incluso desestabilizar su posición de mercado.
- **Riesgos para la reputación**. Aparecer en las noticias sobre fugas de datos puede ser embarazoso y dañar la imagen de las empresas. Esto no solo puede provocar la pérdida de clientela para sus clientes, sino también ser un obstáculo para alianzas en curso y mermar sus posibilidades de adquirir nuevos clientes en el futuro. La fuga de datos de sus clientes también puede afectar a su reputación y a su negocio.

¿Qué es la prevención de pérdida de datos?

La **prevención de pérdida de datos**, en inglés, Data Loss Prevention o DLP, es una categoría de soluciones de seguridad con una larga trayectoria, que representa a los sistemas de tecnologías de seguridad de la información integrados que detectan y previenen el empleo, transmisión y almacenamiento no autorizados de datos confidenciales o sensibles.

Para ello, las soluciones de DLP aplican una combinación de controles del flujo de datos y métodos de análisis de contenido. Este tipo de tecnologías implementan directivas de administración y uso de datos aceptables para la empresa con el fin de evitar que se filtren datos confidenciales a destinatarios no autorizados (ya sean externos o internos).

Aunque la protección de los datos se asocia principalmente con la copia de seguridad y la recuperación ante desastres, hay otras tecnologías esenciales, como las de DLP, certificación y cifrado, que garantizan la seguridad de la información confidencial frente a una variedad de amenazas más amplia, como la fuga de datos.

DLP es la única tecnología capaz de proporcionar visibilidad y control de los datos confidenciales que se transfieren y almacenan en una organización, con el objetivo de prevenir su filtración a entidades no autorizadas.

Estados de los datos y cómo los protegen las diferentes soluciones de DLP funcionales

Los datos pueden residir en una organización en **tres estados** diferentes:

- **Datos en uso:** son los utilizados/transferidos en canales locales (p. ej., periféricos, almacenamiento extraíble) o a través de aplicaciones en los endpoints. Un ejemplo de estos datos serían los archivos que se transfieren desde un ordenador endpoint a una unidad USB.
- **Datos en tránsito:** este término se refiere a los datos que se mueven o transfieren entre sistemas informáticos. Por ejemplo, los datos que se transfieren desde el almacenamiento de archivos local hasta la nube, o bien desde un ordenador hasta otro endpoint a través de la mensajería instantánea o el correo electrónico.
- **Datos en reposo:** este término describe los datos que están almacenados localmente o en una red y a los que en este momento no se acceden o no se están transfiriendo. Un ejemplo serían los datos almacenados en recursos compartidos de la red o en servidores locales.

Es importante destacar que los datos cambian con frecuencia y continuamente de estado, aunque algunos permanecen en un solo estado durante todo el ciclo de vida del endpoint. Entender los distintos estados de los datos, sus características concretas y sus diferencias puede ayudar a los clientes a gestionarlos de manera más segura y a protegerlos contra fugas.

Hay tres tipos de DLP "funcionales" dedicados a cada uno de los tres estados de los datos:

- **DLP para datos en uso**
- **DLP para datos en tránsito**
- **DLP para datos en reposo**

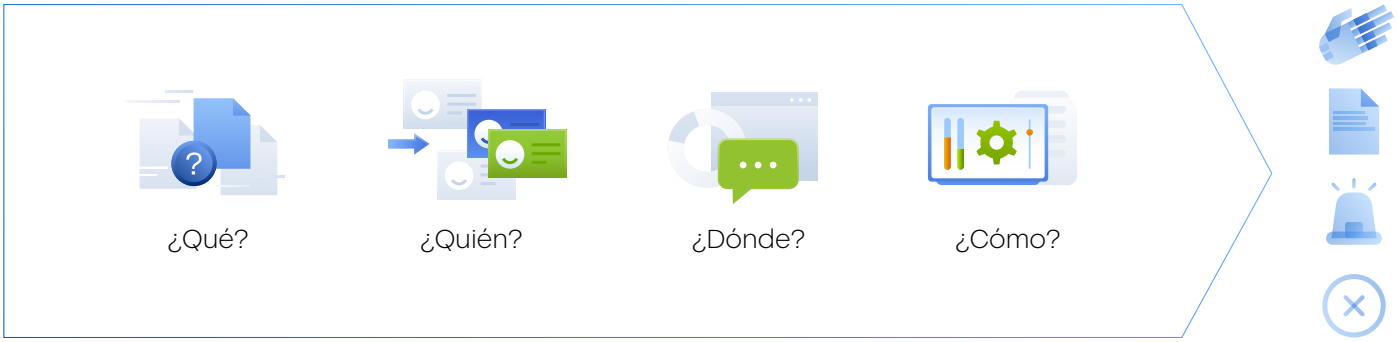
Si bien existen otras tecnologías que abordan distintos riesgos para los datos (accesibilidad, privacidad, etc.), como la administración de identidades y el cifrado, la prevención de pérdida de datos (DLP) es la única capaz de proteger los datos en varios estados, con el firme propósito de prevenir las fugas de datos y, al mismo tiempo, proporcionar visibilidad de los flujos de datos.

Controles de DLP: contenido frente a contexto

Cada flujo de datos de una organización tiene su contexto y su contenido. El contexto se refiere a factores de entorno, como los usuarios que participan en el flujo de la información, los canales utilizados, la dirección del flujo, etc. El contenido describe el tipo o categoría concretos de información que se transfiere; por ejemplo, historias médicas de pacientes, información de identificación personal de empleados, etc.

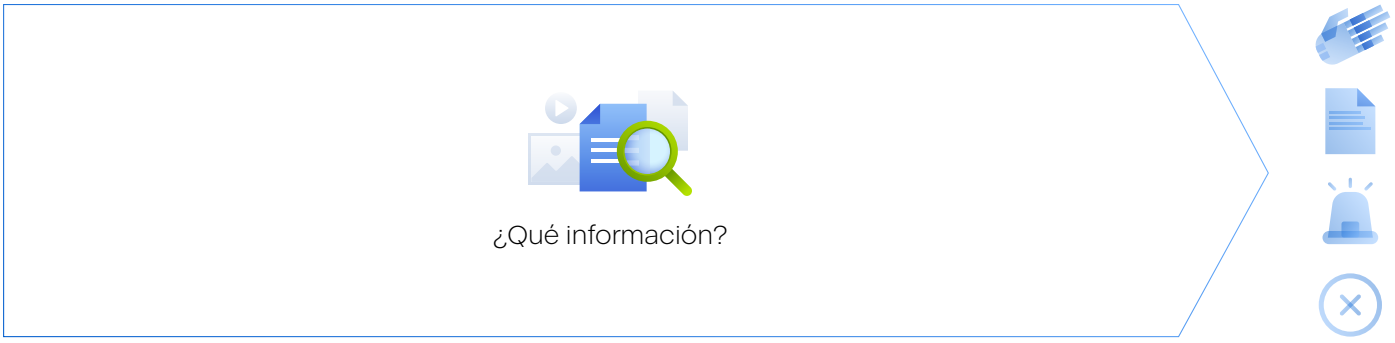
Una solución de DLP eficaz debe implementar en los flujos de datos controles basados en el contexto y en el contenido:

- **Controles de DLP basados en el contexto**: control de las operaciones de transferencia de datos según el contexto de la operación utilizando atributos tales como los usuarios involucrados, los canales utilizados, la dirección de los datos que se transfieren, el destino, la hora, etc.



Ejemplo: directivas que permiten la copia de datos (qué) realizada por usuarios (quién) en dispositivos USB cifrados (dónde) y el bloqueo de la copia de datos en dispositivos USB no cifrados.

- **Controles de DLP basados en el contenido**: el control más exhaustivo sobre los flujos de datos se basa en el tipo y nivel de sensibilidad de la información (el contenido) que se transfiere.

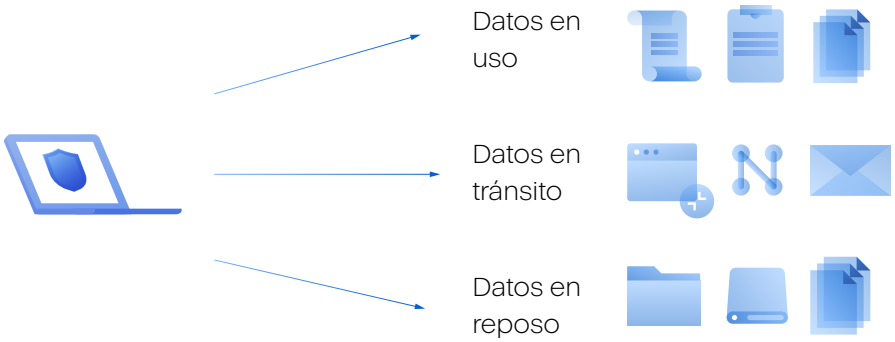


Ejemplo: se prohíbe la copia de documentos que contengan información médica (qué información) en cualquier dispositivo USB.

Tipos de arquitecturas DLP

Hay tres tipos principales de DLP basados en su método de despliegue y funcionamiento:

- **DLP en endpoints** : soluciones que usan agentes de DLP en endpoints y evitan la fuga de datos en uso, en tránsito y en reposo desde dichos ordenadores, con independencia de si se utilizan en la red corporativa o en Internet.



- **DLP en la red o la nube** : soluciones que solo tienen componentes residentes en la red, como gateways de DLP físicos o virtuales y servidores que protegen los datos en tránsito o en reposo en los ordenadores de la red corporativa, evitando la fuga de datos a destinatarios no autorizados y a destinos fuera de la red de la empresa.

- **Arquitecturas DLP híbridas** : soluciones que utilizan tanto componentes de DLP de red como de endpoints para realizar todas las funciones de las dos arquitecturas.

Hay que recordar que las soluciones de DLP de red no pueden proteger los datos en uso debido a su arquitectura y controlan únicamente las fugas de datos a destinatarios no autorizados fuera de la red corporativa, mientras que las soluciones de DLP híbridas protegen los datos en todos los estados y previenen las fugas a destinos no autorizados, ya sea dentro o fuera de la empresa.

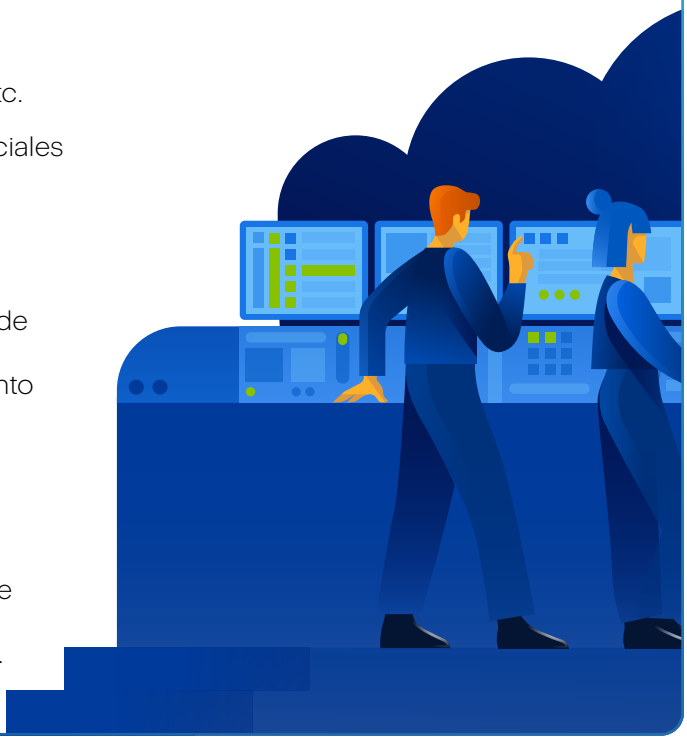
En lo que respecta a esta guía, nos centraremos en el lanzamiento, uso y escalada de un servicio de DLP basado en la arquitectura DLP para endpoints.

Por qué necesitan los clientes DLP

Según el informe de Ponemon Institute sobre el coste de las fugas de datos de 2021, el coste total medio de una fuga de datos a nivel mundial es de 4,24 millones de dólares, lo que implica un aumento del 10 % respecto a 2020. Al aumento de las fugas de datos, hay que sumar que el tiempo medio para identificar y contener un incidente es de 287 días, lo que da idea del enorme riesgo para los clientes hasta que se consigue contener la fuga. Estos riesgos pueden dar lugar a daños financieros, en la reputación y otros derivados del incumplimiento de normativas.

Así ayuda un servicio de DLP a reducir los riesgos para los clientes:

- **Ayuda a garantizar el cumplimiento** de normativas y a proteger la información regulada: información de identificación personal (RGPD, CCPA), datos médicos (HIPAA), información de tarjetas de pago (PCI DSS), etc.
- **Protege** la propiedad intelectual y los secretos comerciales de los clientes.
- **Minimiza el riesgo** de filtración de datos por malware y ataques a través de ingeniería social.
- **Refuerza la seguridad para el teletrabajo** y el empleo de dispositivos personales en el trabajo (BYOD), y evita la transferencia de datos confidenciales a almacenamiento privado en la nube.
- **Previene la fuga de datos** provocada por empleados debido a errores accidentales, negligencia o falta de ética profesional.
- **Facilita una rápida respuesta** en caso de incidentes de fuga de datos y agiliza las investigaciones posteriores, gracias a la visibilidad continua de los eventos de DLP.



Flujo de prestación de servicios de DLP

Antes de entrar en detalle sobre cómo lanzar, utilizar y escalar un servicio de DLP, es importante subrayar que, debido a sus características concretas, los servicios de DLP tienen un flujo determinado que incluye los pasos siguientes:

- **Despliegue del agente de DLP :** decidir qué endpoints deben aprovisionarse con los servicios de DLP con el fin de garantizar una completa protección de los datos de la empresa y desplegar los agentes de DLP en estos endpoints son los primeros pasos del proceso de prestación del servicio. Tenga en cuenta que se recomienda aprovisionar agentes de DLP para todas las cargas de trabajo en las que se crean, almacenan o utilizan datos confidenciales. Si estas cargas de trabajo no están protegidas, pueden crear brechas en la protección del sistema de seguridad de TI de la empresa.

- **Creación de directivas de DLP:** otro paso inicial es crear las directivas de DLP que garantizan el uso y la gestión adecuadas de los datos para prevenir incidentes de fuga. Tenga en cuenta que, en función de la tecnología de DLP que se utilice, es posible que este paso deba realizarse antes del despliegue. **Es importante subrayar** que las directivas de DLP no son universales —son específicas para cada cliente—, ya que cada organización tiene procesos internos diferentes, está sujeta al cumplimiento de distintas normativas y tiene necesidades de acceso y uso compartido de datos específicas. Debido a estas diferencias, las soluciones de DLP tradicionales que requieren la administración manual de directivas presentan a los proveedores de servicios inconvenientes en cuanto a complejidad y coste para implementar los servicios de DLP.
- **Validación de directivas de DLP**: un paso importante tras la creación de las directivas de DLP es validarlas con los clientes para asegurarse de que se ajustan a los requisitos de la empresa. Los MSP no pueden adquirir ese conocimiento detallado de las particularidades empresariales de cada cliente. Cuanto más compleja y "técnica" sea la representación visual de la directiva, más tiempo y experiencia necesitarán los clientes para validarla.
- **Implementación y administración de directivas de DLP:** tras validar las directivas de DLP con el cliente, se pueden implementar para comenzar a proteger los datos confidenciales de la empresa contra fugas de datos. No olvide que las tecnologías de DLP controlan los flujos de datos sensibles de una empresa, bloqueando los que no están autorizados. Sin embargo, las empresas evolucionan constantemente, se introducen nuevos procesos, surgen nuevas normativas de protección de datos y las antiguas pueden cambiar. Por lo tanto, las directivas de DLP que se crearon inicialmente deben ajustarse continuamente para satisfacer las distintas cambiantes necesidades de la empresa, con el fin de garantizar que no se bloqueen flujos de datos esenciales y, al mismo tiempo, se impidan todos los intentos de fuga de datos. Esto se consigue con la configuración manual de las directivas o bien utilizando métodos automáticos de adaptación de directivas.
- **Comunicación del valor del servicio de DLP:** informar continuamente de las transferencias de datos confidenciales bloqueadas y de las acciones de usuarios finales relacionadas con DLP para demostrar el valor de los servicios de DLP ayuda a mejorar la retención de clientes e ilustra cómo se reduce el riesgo ante clientes que no son conscientes de sus problemas de fuga de datos.

Problemas de las soluciones DLP actuales para los MSP

El mercado de soluciones de DLP es maduro, orientado a grandes empresas y copado por actores consolidados. El acceso para otros participantes del mercado general (proveedores de servicios y sus clientes del sector de las pymes) es difícil, debido a la necesidad de conocer continuamente y en detalle las particularidades de la empresa para adaptar convenientemente los controles de DLP, cumplir las normativas y garantizar la protección de los datos, tal y como exige el uso de este tipo de tecnologías. Todo esto ha provocado que el sector de la DLP se centre fundamentalmente en grandes empresas que pueden permitirse el alto coste de profesionales dedicados a la gestión de DLP.

Estos son los principales retos para los MSP en cuanto a implementación y ejecución de un servicio de DLP:

- **Poner en práctica un servicio de DLP es caro y complejo**. Las soluciones de DLP tradicionales requieren procesos manuales complejos para la creación inicial de las directivas y los ajustes posteriores, por lo que, si se tiene en cuenta el tiempo y el esfuerzo necesarios para implementar las soluciones de DLP en los clientes, el servicio resulta demasiado caro. Además, debido a esta complejidad, es preciso contratar a expertos en DLP, lo que es mucho más difícil y costoso que cuando se trata de especialistas en seguridad general de TI.

- **Una DLP eficaz requiere directivas específicas para el cliente**. Como hemos indicado antes, los procesos empresariales y el nivel de sensibilidad de los datos de cada empresa son diferentes y cambian continuamente, lo que exige ajustes continuos de las directivas de DLP. Sin embargo, los MSP carecen de este conocimiento de los procesos empresariales de cada cliente y son incapaces de adquirirlo y mantenerlo continuamente. Esto es un obstáculo que supone un problema de escalabilidad para los MSP que utilizan tecnologías de DLP tradicionales.
- **Las directivas de DLP que no se configuran correctamente pueden interrumpir la actividad empresarial**. Por una parte, no es difícil cometer fallos al crear y configurar las directivas de DLP, debido a su complejidad y granularidad. Por el otro, las tecnologías de DLP bloquean los flujos de datos no autorizados. La combinación de esta complejidad con las funciones de prevención de DLP puede interrumpir los procesos esenciales de la empresa bloqueando por error flujos de datos que son necesarios para el negocio si las directivas de DLP no están bien configuradas o si hay nuevos procesos empresariales que no se han asignado como corresponde a dichas directivas.
- **Los empleados son el eslabón más débil de los clientes**. No es solo que los MSP y sus clientes apenas tengan acceso a las tecnologías DLP; las principales causas de las fugas de datos son los errores humanos y los ataques externos contra los empleados. Aunque los proveedores de servicios puedan limitar el riesgo de amenazas externas con otras capas de protección de endpoints, ellos serán los responsables si los usuarios proporcionan sin saberlo datos confidenciales y con ello provocan una fuga de datos.
- **Los clientes pueden desconocer el problema de la fuga de datos**. Debido a la tradicional dificultad para acceder a la tecnología de DLP, es posible que los clientes no sean conscientes del problema de la fuga de datos. Lanzar un servicio de DLP implica que los proveedores deberán formar a sus clientes sobre los riesgos de fuga de datos a los que se enfrentan e informarles de que la tecnología de prevención de fuga de datos (DLP) es la única capaz de responder ante estos riesgos que representan amenazas importantes para organizaciones de todos los tamaños.

Las nuevas tendencias y tecnologías disponibles en el mercado, como la creación, ampliación y supervisión automáticas de las directivas basadas en el comportamiento, ayudan a superar las dificultades de las reglas de DLP que cambian rápidamente para adaptarse a la continua evolución de los procedimientos empresariales, además de a los requisitos de las normativas. Estas nuevas capacidades están democratizando el mercado de la DLP y facilitando su acceso a los proveedores de servicios y a sus clientes. Este es el momento perfecto para plantearse la ampliación de su cartera incorporando servicios de DLP.

Planificación y lanzamiento de un servicio de DLP

El primer paso para planificar y lanzar un servicio de DLP es verificar si los clientes realmente lo necesitan.

Los clientes necesitarán un servicio de DLP para reducir el riesgo de fuga de datos si cumplen algunas o todas las condiciones siguientes:

- Crean, almacenan o trabajan en sus cargas de trabajo con datos confidenciales, sometidos al cumplimiento de normativas.
- Poseen secretos comerciales o propiedad intelectual que debe protegerse para evitar filtraciones.
- Operan en sectores muy regulados.
- Han sufrido una fuga de datos y desean proteger su entorno y reducir los riesgos.
- Tienen o necesitan certificados de cumplimiento de normativas.
- Pagan o están planteándose adquirir un ciberseguro para reducir su responsabilidad civil.
- Carecen de personal de seguridad dedicado.

Además, los clientes de los siguientes sectores han demostrado siempre un mayor interés en la DLP:

- Banca y servicios financieros
- Atención sanitaria
- Sector legal
- TI y telecomunicaciones
- Sector público y Administración
- Industria
- Minoristas y logística
- Educación
- Energía

En caso de que tenga clientes que cumplen estas condiciones o que operan en los sectores mencionados, ha llegado el momento de que se plantee añadir la DLP a su cartera de servicios para satisfacer sus mayores necesidades de reducción de riesgos de fuga de datos y garantizar el cumplimiento de las normativas.

Planificación de los servicios y estimación de costes

Los tres principales factores que determinan el precio de su servicio son los costes de personal, los costes del producto y el margen que desea conseguir. Así afectan estos factores a su precio:

- **Costes laborales:** la complejidad de la solución elegida determinará el tiempo que sus técnicos de servicio dedicarán al aprovisionamiento y la gestión del servicio, así como el nivel de experiencia en seguridad de TI requerido.
- **Costes del producto:** las soluciones de DLP, que tradicionalmente han utilizado grandes empresas, conllevan un alto coste, por lo que es posible que las pequeñas y medianas empresas no se las puedan permitir. Si sus clientes son fundamentalmente pymes, debe elegir una solución que no suba demasiado el precio del servicio para ellas.
- **Margen deseado:** el MSP medio obtiene un margen bruto de hasta el 50 % en ventas de servicios remotos, con el modelo de ingresos recurrentes.

Un servicio de DLP con el paquete Acronis Advanced DLP

Acronis ofrece DLP basada en comportamientos que crea automáticamente y mantiene continuamente la coherencia con las directivas específicas para el cliente, sin necesidad de emplear meses en el despliegue, contratar a equipos o poseer un doctorado en derecho sobre la privacidad para entenderla.

Con el paquete Acronis Advanced DLP, puede proporcionar a los clientes protección contra fuga de datos para los datos en movimiento y los datos en uso, con un nivel de simplicidad extraordinario, lo que le permite:

- **Disfrutar de nuevas oportunidades de rentabilización**, gracias a la ampliación de su cartera para atraer a más clientes e incrementar las ganancias por cliente con servicios de DLP que antes solo estaban disponibles para las grandes empresas.
- **Minimizar los esfuerzos para obtener valor**, al añadir DLP fácilmente a su oferta, sin incrementar la complejidad de la administración, los costes ni el personal.
- **Mitigar los riesgos de seguridad para los clientes** previniendo las fugas de datos confidenciales.
- **Reforzar el cumplimiento de normativas para los clientes**, con plantillas prediseñadas de clasificación de datos según los marcos regulatorios habituales, como el RGPD, o la ley HIPAA y el estándar PCI DSS.
- **Simplificar el aprovisionamiento y la administración del servicio**, automatizando el aprovisionamiento del servicio de DLP, la configuración inicial de las directivas y su posterior ajuste.
- **Facilitar directivas de DLP específicas para cada cliente a cualquier escala**, adaptando las directivas de DLP a las circunstancias particulares de cada empresa a medida que cambian, con tecnología basada en comportamientos. A partir de ahí, se realiza una sencilla validación de las directivas con los clientes antes de su implementación.
- **Reaccionar más rápidamente a los eventos de DLP** y simplificar las operaciones del servicio de DLP, el mantenimiento de directivas, las auditorías de seguridad de TI y las investigaciones de incidentes con alertas de seguridad y registros de auditoría centralizados y basados en directivas.

Paquete Acronis Advanced DLP

El paquete Acronis Advanced DLP Cyber Protect Cloud ayuda a sus clientes a dormir tranquilos sabiendo que sus datos confidenciales están protegidos frente a las filtraciones a terceros no autorizados. Su exclusiva tecnología basada en el comportamiento permite crear directivas de DLP y ampliarlas continuamente conforme a las particularidades de cada cliente, además de facilitar el lanzamiento del servicio con una simplicidad nunca antes vista y un esfuerzo mínimo para rentabilizarlo.

Acronis

Encontrará más información en www.acronis.com