Lista de comprobación:
Cinco signos que indican que debe añadir DLP a sus servicios como MSP

¿Por qué deben los proveedores de servicios interesarse por la prevención de pérdida de datos (DLP)?

Durante años, las empresas han tenido escaso éxito protegiendo sus datos confidenciales frente al acceso no autorizado y las filtraciones causadas por ataques externos o riesgos internos, como las configuraciones incorrectas de tecnologías y los errores humanos. Todo ello les ha acarreado graves consecuencias, entre ellas titulares incómodos, pérdida de confianza de clientes y partners, quebrantos patrimoniales y sanciones por el incumplimiento de las normativas.

Con el aumento de las tecnologías de prevención de pérdida de datos (DLP) basadas en el comportamiento, ahora los MSP pueden lanzar y gestionar servicios de DLP rentables con el mínimo esfuerzo para reducir los riesgos de fuga de datos de sus clientes.

Es el momento de aprovechar esta tendencia y asegurar que sus clientes duerman tranquilos sabiendo que sus datos están protegidos y que siempre cumplen las normativas.

"El 80 % de las empresas internacionales cree probable sufrir una violación de los datos de sus clientes en los próximos 12 meses".

Fuente: Cyber Risk Index Report, 2021, Ponemon Institute

Vea cuáles son los cinco signos que indican que debe añadir DLP a sus servicios

1 Los empleados de sus clientes acceden a datos sensibles (por ejemplo, datos sujetos a normativas) desde sus endpoints

Da igual que sus clientes almacenen sus datos confidenciales en la nube, si los empleados acceden a ellos desde su estación de trabajo, pueden filtrarse fácilmente a través de sus dispositivos periféricos o canales de red, como el correo electrónico y las mensajerías instantáneas.

Según el informe Verizon Data Breach Investigation Report de 2022, más del 80 % de las violaciones de datos tienen motivación económica. Por esta razón, los datos que persiguen los ataques son datos de gran valor, como los que están sujetos a normativas, los secretos comerciales o la propiedad intelectual, ya que pueden generar pingües beneficios.

Si los empleados de sus clientes crean, almacenan o trabajan con este tipo de datos en sus endpoints, es preciso impedir que se filtren a terceros no autorizados para mantener a los clientes a salvo de los graves riesgos económicos, normativos y reputacionales que conlleva una fuga.

2 Está buscando nuevas fuentes de ingresos para ampliar sus servicios

Según el informe Acronis Pulse of the MSP 2021, los MSP prevén que su principal fuente de ingresos durante los próximos años procederá de la ciberseguridad. Sin embargo, dado que la mayoría de los proveedores de servicios ofrecen alguna forma de servicios de seguridad gestionados, la competencia se está convirtiendo en un reto importante en el sector.

Gracias al auge de las tecnologías de DLP basadas en el comportamiento, ahora puede diferenciar su cartera de productos con servicios de DLP que antes no estaban disponibles para MSP ni para pequeñas empresas a causa de su gran complejidad, los costes de la prestación del servicio y su largo plazo de rentabilización, ya que exigen adaptar las directivas a los cambiantes procesos empresariales propios de cada cliente.

Las tecnologías de DLP basadas en el comportamiento le permiten encontrar nuevas fuentes de ingresos ofreciendo un servicio de DLP atractivo para empresas de todos los tamaños, que reduce el riesgo de que los datos de sus clientes acaben en manos de terceros no autorizados.

3 Tiene clientes en sectores muy regulados (por ejemplo, atención sanitaria, servicios bancarios y financieros, Administración pública, etc.)

Si sus clientes trabajan o almacenan información de identificación personal (PII), información médica protegida (PHI), datos de titulares de tarjetas o cualquier otro tipo de datos confidenciales en sectores altamente regulados, necesitarán un nivel de protección de datos que vaya más allá de la mera copia de seguridad.

La mayoría de las normativas, como el RGPD, la HIPAA y el estándar PCI-DSS, exigen denunciar violaciones y fugas de datos en un plazo estricto y pueden imponer importantes multas a los clientes si se producen fugas de datos confidenciales.

Las soluciones de prevención de pérdida de datos son la única tecnología capaz de supervisar los flujos de datos internos de una organización, impedir fugas y, a la vez, mejorar la visibilidad y facilitar la investigación de los incidentes de pérdida de datos.

4 Tiene clientes más expuestos al riesgo de ataque y fuga de datos

Siempre ha habido sectores más vulnerables a los riesgos de ciberseguridad, sectores que, como además almacenan datos confidenciales de valor, se convierten en apreciados objetivos para los ciberdelincuentes. Entre ellos figuran los de educación, atención sanitaria y otros sectores públicos donde la accesibilidad a los datos es una necesidad, pero donde al mismo tiempo se precisa una protección eficaz para que la información no se filtre a terceros no autorizados.

Las tecnologías de DLP basadas en el comportamiento permiten ofrecer un servicio de DLP enormemente competitivo para, por un precio asequible, proteger a estas organizaciones frente a los riesgos de incumplimiento normativo y fuga de datos.

5 Tiene clientes que consideran contratar o ya han contratado un ciberseguro para reducir responsabilidades

Admitámoslo: los ciberseguros están en auge en el sector de la ciberseguridad en los últimos años. Los clientes recurren a las compañías de ciberseguros para limitar la responsabilidad de su empresa en caso de que se produzca una violación de datos.

El coste de un ciberseguro depende de varios factores, como la renta anual de la empresa, el sector, el tipo y el volumen de datos almacenados, y el nivel de seguridad. Considere la posibilidad de añadir una solución de DLP a su oferta de servicios para cubrir los requisitos de protección de datos de los ciberseguros y reducir así su coste para sus clientes.

Advanced DLP

El paquete Advanced DLP para Acronis 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