Lista de verificación: Cinco señales de que necesita agregar DLP a su práctica de MSP

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

Las empresas llevan años sin conseguir proteger con éxito los datos confidenciales del acceso no autorizado y la filtración a través de ataques externos o riesgos internos, como las configuraciones erróneas de TI y los errores humanos. Esto las ha dejado expuestas a consecuencias como titulares embarazosos, pérdida de confianza de clientes y partners, pérdidas de patrimonio y sanciones normativas.

Con el aumento de las tecnologías de prevención de pérdida de datos (DLP) basadas en el comportamiento, los proveedores de servicios gestionados (MSP) ahora pueden lanzar y administrar sin esfuerzo los servicios de DLP con el fin de reducir los riesgos de filtración de datos de los clientes.

Ahora es el momento de aprovechar esta tendencia y garantizar que sus clientes duerman mejor por la noche sabiendo que sus datos están protegidos y que el cumplimiento de las normativas está intacto.

> "El 80 % de las empresas mundiales declara que es probable que sufra una fuga de datos que afecte a los datos de los clientes en los próximos 12 meses".

Fuente: Cyber Risk Index Report, 2021, Ponemon Institute

Verifique las cinco señales que indican que necesita agregar DLP a su práctica

1 Los empleados de los clientes tienen acceso a datos confidenciales a través de sus endpoints (p. ej., datos sujetos a normativas)

No importa si sus clientes almacenan sus datos confidenciales en la nube o si acceden a ellos a través de las estaciones de trabajo de los empleados. Sea cual sea el caso, pueden filtrarse fácilmente a través de estos medios por los dispositivos periféricos o canales de red como el correo electrónico y la mensajería instantánea.

Más del 80 % de las fugas de datos tienen motivaciones financieras, se acuerdo con el informe Verizon Data Breach Investigation Report de 2022. Debido a esto, 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, que se pueden aprovechar para obtener beneficios económicos.

Si los empleados de los clientes crean, almacenan o trabajan con este tipo de datos en sus endpoints, debe asegurarse de que estén protegidos contra la filtración a partes no autorizadas para evitarles graves riesgos financieros, normativos y de la reputación.

2 Busca nuevas fuentes de ingresos para hacer crecer su práctica

En el informe Pulse of the MSP 2021 de Acronis, podemos ver que los MSP esperan que sus principales ingresos para los próximos años provengan de la ciberseguridad. Sin embargo, la mayoría de los proveedores de servicios ofrecen algún tipo de servicio de seguridad administrado, por lo que la competencia se está convirtiendo en un desafío principal para la industria.

El aumento de las tecnologías de DLP basadas en el comportamiento le permite diferenciar su cartera con servicios de DLP que antes no estaban disponibles para los MSP y las empresas más pequeñas, debido a la alta complejidad, los costos de provisión de servicios y la lentitud en la obtención de valor, debido a que exigen adaptar las directivas a los cambiantes procesos empresariales propios de cada cliente.

Con las tecnologías de DLP basadas en el comportamiento, puede encontrar nuevas fuentes de ingresos y brindar una atractiva oferta de servicios de DLP a empresas de todos los tamaños, reduciendo así los riesgos de que los datos de los clientes acaben en manos de destinatarios no autorizados.

3 Tiene clientes en industrias muy reguladas (p. ej., sanidad, servicios bancarios y financieros, el sector público)

En caso de que sus clientes almacenen o se manejen con información de identificación personal (PII), información de salud protegida (PHI), datos de titulares de tarjetas o cualquier otra forma de datos confidenciales en industrias muy reguladas, requerirán un nivel de protección de datos más alto que una simple copia de seguridad.

La mayoría de las normativas, como el RGPD, la HIPAA y el estándar PCI-DSS, exigen la notificación de las fugas y filtraciones de datos en un plazo estricto y podrían generar multas graves para los clientes en caso de filtración de datos confidenciales.

Las soluciones de prevención de pérdida de datos son la única tecnología capaz de supervisar los flujos de datos dentro de la empresa y evitar las filtraciones, mientras aumentan la visibilidad y facilitan la investigación de los casos de DLP.

4 Tiene clientes que son más propensos a sufrir ataques y riesgos de filtración de datos

Históricamente ha habido industrias con mayores vulnerabilidades de seguridad que también almacenan datos confidenciales valiosos, lo que las convierte en un objetivo de alto valor para los ciberataques. Entre los ejemplos de dichas industrias se incluyen los sectores de educación, sanidad y otros sectores públicos para los que se requiere la accesibilidad a los datos, pero, al mismo tiempo, se necesita una protección eficaz para evitar que se filtren a partes no autorizadas.

Las tecnologías de DLP basadas en el comportamiento le permiten ofrecer un servicio de DLP muy competitivo a un precio asequible para proteger a dichas empresas contra los riesgos de incumplimiento y de filtración de datos.

5 Tiene clientes que están considerando adquirir o que ya tienen un ciberseguro para reducir la responsabilidad

Reconozcámoslo: los ciberseguros son uno de los temas más candentes en el espacio de la ciberseguridad en los últimos años. Los clientes recurren a los ciberseguros para limitar la responsabilidad de sus empresas en caso de que se produzcan fugas de datos.

El costo de un ciberseguro depende de varios factores, como los ingresos anuales de la empresa, la industria, el tipo y la cantidad de datos que posee y el nivel de seguridad. Debería considerar la posibilidad de agregar la DLP a su pila de servicios para dar respuesta a los requisitos de protección de datos para el ciberseguro y minimizar el costo para los clientes.

Advanced DLP

Advanced DLP para Acronis Cyber Protect Cloud ayuda a sus clientes a dormir mejor por la noche sabiendo que sus datos confidenciales están protegidos contra filtraciones a partes no autorizadas. Su exclusiva tecnología basada en el comportamiento permite la creación y la ampliación continua de las políticas de DLP según las particularidades de cada cliente y facilita el lanzamiento de su servicio con una sencillez nunca vista y un esfuerzo mínimo.

Acronis

Encontrará más información en www.acronis.com