Liste de contrôle : 5 raisons d'ajouter un service DLP à votre activité de MSP

Pourquoi les fournisseurs de services devraient-ils se préoccuper de la prévention de la perte de données (DLP) ?

Depuis des années, les entreprises peinent à protéger leurs données sensibles contre les accès non autorisés et l'exfiltration via des attaques externes ou des risques internes, tels que des problèmes de configuration informatique ou des erreurs humaines. Elles sont ainsi exposées à des conséquences fâcheuses : médiatisation embarrassante, perte de confiance des clients et des partenaires, chute du cours des actions et sanctions réglementaires.

Face à l'essor des technologies de prévention de la perte de données (DLP) basées sur les comportements, les MSP peuvent désormais lancer et gérer, en limitant les efforts de valorisation, des services DLP afin de réduire les risques de fuite de données pour leurs clients.

Il est temps de tirer parti de cette tendance et d'apporter à vos clients la tranquillité d'esprit dont ils ont besoin, sachant que leurs données sont protégées et que leur conformité réglementaire est inchangée.

« 80 % des entreprises internationales considèrent qu'elles seront probablement victimes d'une compromission affectant les données de leurs clients au cours des 12 prochains mois. »

Source : Cyber Risk Index Report, 2021, Ponemon Institute

5 raisons d'ajouter un service DLP à votre activité

1 Les collaborateurs de vos clients ont accès à des données sensibles depuis leurs terminaux (p. ex. données soumises à des réglementations)

Même si vos clients stockent leurs données sensibles dans le cloud, leurs collaborateurs peuvent y accéder depuis leurs postes de travail. Il existe donc un risque de fuite via des périphériques ou des canaux réseau, comme les e-mails et les messageries instantanées.

Selon le rapport « 2022 Data Breach Investigation Report » de Verizon, plus de 80 % des compromissions de données sont motivées par l'appât du gain. C'est pourquoi les attaques ciblent principalement les données de grande valeur, comme celles soumises à des réglementations, les secrets commerciaux ou les éléments de propriété intellectuelle.

Si les collaborateurs de vos clients créent, stockent ou traitent de telles données sur leurs terminaux, vous devez vérifier qu'ils bénéficient d'une protection contre les fuites vers des parties non autorisées, afin de leur éviter des pertes financières, des amendes réglementaires et une dégradation de l'image de marque.

2 Vous recherchez de nouvelles sources de revenus pour développer votre activité

Le rapport « Pulse of the MSP 2021 » d'Acronis montre que les MSP misent sur la cybersécurité comme principale source de revenus dans les années à venir. Mais comme la majorité des fournisseurs de services proposent des services de sécurité managés, la concurrence est un défi majeur dans ce secteur.

L'essor des technologies DLP basées sur les comportements vous permet de différencier vos offres avec des services DLP jusqu'alors inaccessibles aux MSP et aux petites entreprises compte tenu de leur complexité, du coût de leur prestation et de la lenteur du retour sur investissement dû à l'évolution constante des processus métier propres à chaque client.

Grâce aux technologies DLP basées sur les comportements, vous pouvez bénéficier de nouvelles sources de revenus et offrir un service DLP attractif aux entreprises de toutes tailles qui permettra d'éviter que les données des clients ne tombent entre les mains de parties non autorisées.

3 Certains de vos clients exercent leurs activités dans des secteurs très réglementés (santé, services bancaires et financiers, administrations, etc.)

Si vos clients traitent ou stockent des informations d'identification personnelle, des données médicales protégées de patients, des données de titulaires de cartes ou tout autre type de données sensibles dans des secteurs très réglementés, ils doivent disposer d'un niveau élevé de protection des données ne se limitant pas aux sauvegardes.

La majorité des réglementations — RGPD, HIPAA et PCI DSS — exigent le signalement des compromissions et des fuites de données dans un délai strict et peuvent imposer de lourdes amendes aux clients en cas de fuite de données sensibles.

Les solutions de prévention des pertes de données intègrent la seule technologie capable de surveiller les flux de données au sein d'une entreprise et de prévenir les fuites de données tout en offrant la visibilité sur les événements DLP et la capacité d'investigation associée.

4 Certains de vos clients sont plus vulnérables aux attaques et aux fuites de données

Les secteurs présentant d'importantes vulnérabilités de sécurité et stockant des données sensibles de valeur ont toujours représenté une cible de choix pour les cybercriminels. Parmi ces secteurs, on peut citer l'éducation, la santé et d'autres services publics dans lesquels l'accessibilité aux données est indispensable mais doit être contrôlée afin d'éviter toute fuite vers des parties non autorisées.

Les technologies DLP basées sur les comportements vous permettent de proposer un service DLP très compétitif à un prix abordable pour protéger ces entreprises contre les risques de non-conformité et de fuite de données.

5 Certains de vos clients ont souscrit ou envisagent de souscrire une cyberassurance afin de limiter leur responsabilité

Il faut bien l'admettre : ces dernières années, la cyberassurance est l'un des sujets les plus sensibles dans la communauté de la cybersécurité. Les clients souscrivent ces assurances pour limiter la responsabilité de leur entreprise en cas de compromissions de données.

Le coût d'une cyberassurance dépend de plusieurs facteurs, y compris du chiffre d'affaires annuel de l'entreprise, du type et du volume de données détenues, ainsi que du niveau de sécurité. L'ajout d'un service DLP à votre gamme permet de répondre aux critères de protection des données d'une cyberassurance et de réduire les coûts pour les clients.

Advanced DLP

Advanced DLP pour Acronis Cyber Protect Cloud apporte à vos clients la tranquillité d'esprit dont ils ont besoin, sachant que leurs données sensibles sont protégées contre toute fuite vers des parties non autorisées. Sa technologie exclusive basée sur les comportements permet de créer et de renforcer en continu des stratégies DLP en fonction des spécificités de chaque client et de lancer votre service avec une simplicité inédite et en limitant les efforts de valorisation.

Acronis

Découvrez nos solutions sur www.acronis.com