Acronis

LIVRE BLANC

Lancement et montée en charge de services DLP – Guide pour les MSP

Depuis des années, les entreprises de toutes tailles peinent à lutter contre les fuites de données, en dépit de la sensibilisation accrue à la cybersécurité et de la prolifération des protocoles de sécurité et des réglementations. Ces attaques sont même en plein essor : selon le rapport « 2021 Year End Report: Data Breach QuickView » de Risk Based Security, plus de 22 milliards d'enregistrements ont été exposés. 2021 est ainsi la deuxième année pendant laquelle le nombre de données confidentielles compromises a été le plus élevé depuis 2005. La grande majorité de ces enregistrements ont été exposés en raison d'une fuite de données, à savoir une faille de sécurité qui se traduit par la divulgation accidentelle ou délibérée de données confidentielles, sensibles ou protégées à un environnement non fiable ou à des utilisateurs internes ou externes non autorisés d'une entreprise.

Quelle est l'origine d'une fuite de données ? On distingue deux causes principales :

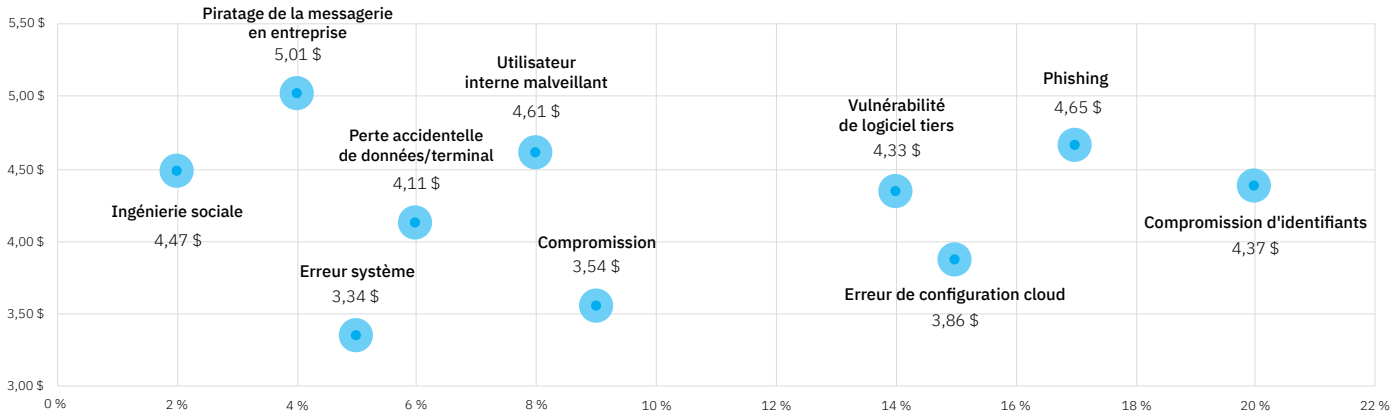
1. Cybermenaces externes

Selon l'infrastructure MITRE ATT&CK, l'exfiltration de données fait partie des tactiques les plus récentes utilisées par les cybercriminels pendant une attaque. L'appât du gain est, dans plus de 80 % des violations de données, la motivation des cybercriminels, selon le rapport Verizon 2022 Data Breach Investigation Report.

C'est pourquoi les données sensibles constituent la cible privilégiée de la majorité des attaques. Une fois que le cybercriminel est parvenu à s'introduire dans l'environnement de l'entreprise, il peut exfiltrer des données via de nombreux canaux. Compte tenu de la complexité croissante des attaques et de leur capacité à franchir les niveaux de sécurité, le risque de fuite de données pour les entreprises augmente de façon exponentielle.

2. Risques internes

Si les protections antimalware et autres technologies de sécurité des terminaux parviennent à détecter et à neutraliser les attaques externes, d'autres risques d'origine interne menacent les données des entreprises. Un utilisateur final peut divulguer involontairement des données à des parties non autorisées (p. ex. en transférant un e-mail). Qu'il s'agisse d'erreurs accidentelles de collaborateurs, d'erreurs de configuration informatique ou d'utilisateurs internes malveillants, la menace pour les entreprises est grave et peut donner lieu à des compromissions de données coûteuses.



Et bien que certaines entreprises sous-estiment l'impact des risques internes, le rapport « 2021 Cost of Data Breach Report » du Ponemon Institute indique clairement que près d'un tiers des compromissions de données sont imputables à des utilisateurs internes malveillants.

Quel est l'impact d'une fuite de données pour une entreprise ?

Les fuites de données sont une menace grave pour les entreprises. Voici les conséquences de l'exfiltration de données sensibles à des parties non autorisées :

- **Non-conformité aux réglementations** – Le stockage, la consultation et la protection des données sensibles (informations d'identification personnelle de collaborateurs et de clients, données médicales protégées ou données de titulaires de cartes) sont rigoureusement soumis à des réglementations locales et internationales (RGPD, CCPA, HIPAA, PCI DSS, etc.). Certaines de ces réglementations, comme le RGPD, exigent même le signalement des compromissions dans un délai strict. En cas de non-respect de ce délai, les entreprises s'exposent à de lourdes amendes, voire à la perte de leurs certifications de conformité.
- **Pertes financières** – En cas de fuite de données, en plus des amendes réglementaires dont les clients MSP sont passibles, les fournisseurs de services peuvent subir des pertes financières du fait de leur responsabilité à l'égard de la sécurité de leurs clients, voire faire l'objet de poursuites judiciaires. De plus, l'exfiltration de secrets commerciaux ou d'éléments de propriété intellectuelle peut être à l'origine de pertes financières supplémentaires, voire de pertes de parts de marché.
- **Dégradation de l'image de marque** – La médiatisation embarrassante d'une compromission de données peut avoir de lourdes conséquences pour l'entreprise : augmentation du taux d'attrition de vos clients, impact négatif sur leurs partenariats existants et sur leur capacité à attirer de nouveaux clients. Une fuite de données chez vos clients peut également nuire à votre réputation et à votre activité.

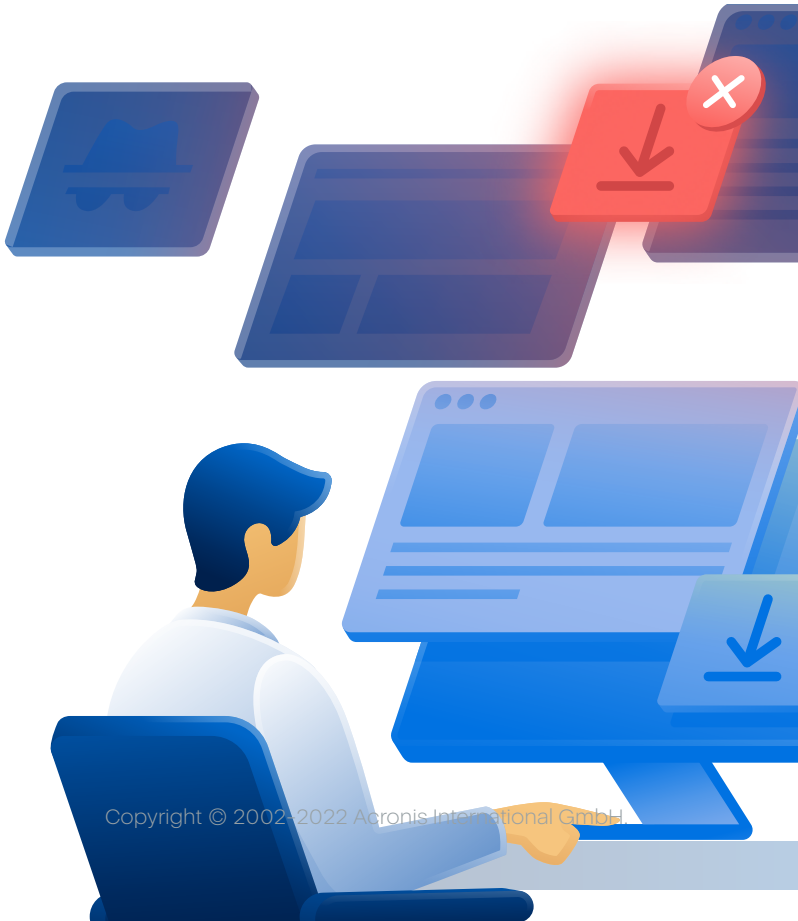
Qu'est-ce que la prévention de la perte de données ?

La prévention de la perte de données (DLP) désigne une catégorie de solutions de sécurité établies de longue date et basées sur des technologies intégrées de protection des informations qui détectent et préviennent l'utilisation, la transmission et le stockage non autorisés de données confidentielles et sensibles.

Les solutions DLP appliquent, pour ce faire, une combinaison de contrôles des flux de données et de méthodes d'analyse du contenu. Ces technologies appliquent des règles d'utilisation et de traitement des données acceptables au sein de l'entreprise afin de prévenir l'exfiltration de données sensibles vers des destinataires non autorisés (internes et externes).

Si la protection des données est principalement associée à la sauvegarde et à la reprise d'activité après sinistre, d'autres technologies essentielles, comme la DLP, la notarisation et le chiffrement, protègent les informations sensibles contre un large éventail de menaces, y compris la fuite de données.

La DLP est la seule technologie capable d'offrir visibilité et contrôle sur les données sensibles en circulation et stockées dans une entreprise afin de prévenir toute fuite vers des entités non autorisées.



États des données et protection DLP fonctionnelle associée

Les données stockées dans une entreprise peuvent présenter **trois principaux états** :

- **Données en cours d'utilisation :** données consultées ou transférées sur des canaux locaux (p. ex. périphériques et supports de stockage amovibles) ou via des applications sur des ordinateurs, comme les fichiers transférés entre un ordinateur et un lecteur USB.
- **Données en transit :** données déplacées ou transférées entre différents systèmes informatiques, comme les données transférées entre un stockage local et un stockage cloud, ou entre deux terminaux via une application de messagerie instantanée ou par e-mail.
- **Données au repos :** données stockées localement ou sur un réseau et qui ne font l'objet d'aucune consultation ni d'aucun transfert, comme les données stockées dans des partages réseau ou sur des serveurs sur site.

Il est important de souligner que les données changent fréquemment et continuellement d'état. Il existe cependant des données qui conservent le même état tout au long du cycle de vie d'un terminal. Comprendre les différents états des données, leurs spécificités et leurs différences peut aider les clients à traiter leurs données d'entreprise de façon plus sécurisée et à les protéger contre les fuites.

On distingue trois principaux types de solutions DLP « fonctionnelles » dédiées à la protection de chacun des états des données :

- **DLP des données en cours d'utilisation**
- **DLP des données en transit**
- **DLP des données au repos**

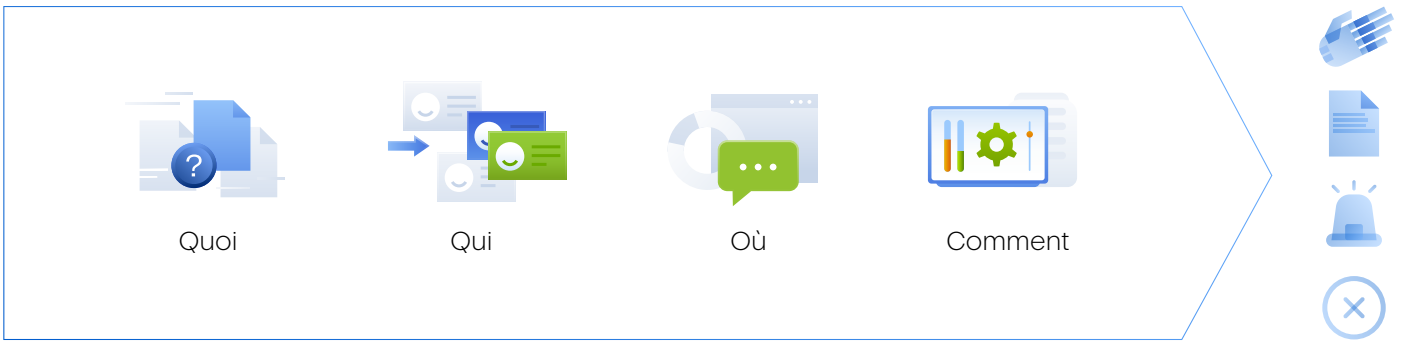
Il existe d'autres technologies permettant de limiter différents risques pour les données (p. ex. accessibilité et confidentialité), comme la gestion des identités ou le chiffrement. En revanche, la DLP est la seule technologie capable de protéger les données quel que soit leur état avec pour seul objectif la prévention des fuites de données et la visibilité sur les flux de données.

Contrôles DLP : contenu et contexte

Dans une entreprise, chaque flux de données est associé à un contexte et à un contenu. Le contexte désigne les facteurs environnementaux, tels que les utilisateurs intervenant dans un flux de données, les canaux utilisés, la direction du flux, etc. Le contenu désigne quant à lui le type/la catégorie des informations transférées (dossiers médicaux de patients, informations d'identification personnelle de collaborateurs, etc.).

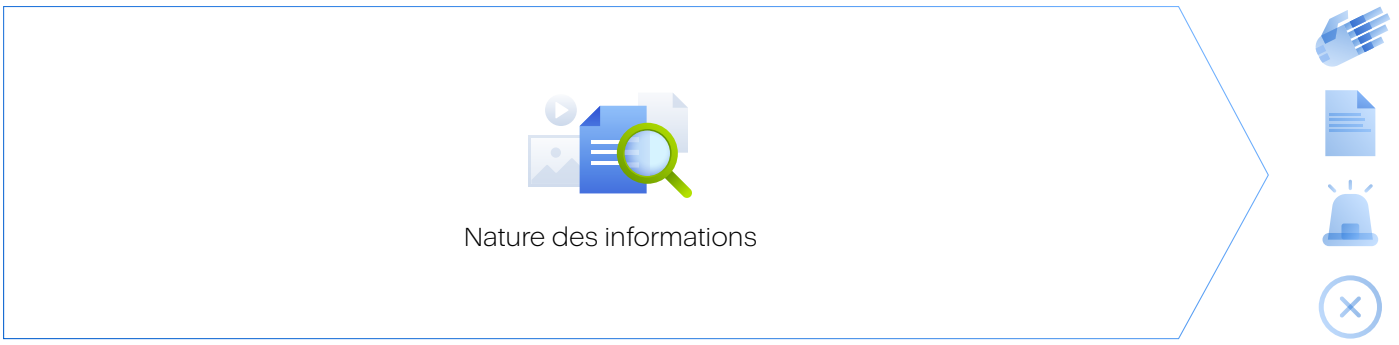
Une solution DLP efficace doit mettre en place des contrôles sur les flux de données en fonction du contexte et du contenu :

- **Contrôles DLP sensibles au contexte** : contrôle des opérations de transfert de données tenant compte du contexte et s'appuyant sur des attributs tels que les utilisateurs concernés, les canaux utilisés, la direction du flux, la destination et l'heure



Exemple : règles qui autorisent les utilisateurs (qui) à copier des données (quoi) sur des périphériques USB chiffrés (où), mais qui empêchent leur copie sur des périphériques USB non chiffrés

- **Contrôles DLP sensibles au contenu** : contrôle plus approfondi des flux de données tenant compte du type et de la sensibilité des informations (contenu) transférées

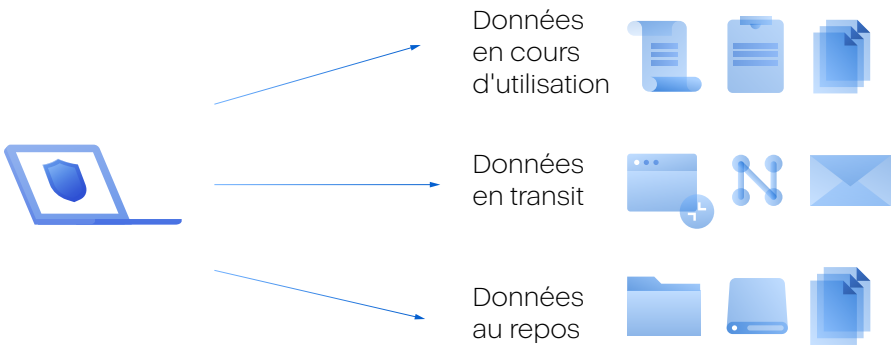


Exemple : règles qui interdisent la copie sur périphérique USB de tout document contenant des informations protégées par la loi HIPAA (nature des informations)

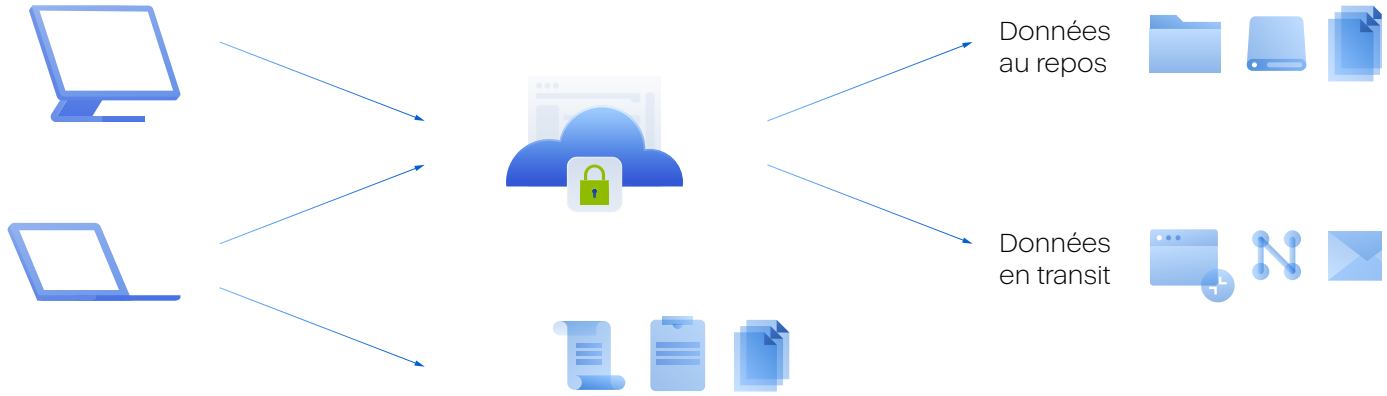
Types d'architectures DLP

On distingue trois principaux types d'architectures DLP en fonction de leur mode de déploiement et de fonctionnement :

- **DLP pour terminaux** : solutions utilisant des agents DLP sur des ordinateurs et empêchant toute fuite de données en cours d'utilisation, en transit et au repos depuis ces ordinateurs, qu'ils soient connectés au réseau d'entreprise ou à Internet



- **DLP pour réseau/cloud** : solutions ne comprenant que des composants réseau, y compris des passerelles et serveurs DLP matériels/virtuels qui protègent les données en transit ou au repos stockées sur les ordinateurs connectés au réseau d'entreprise, empêchant ainsi toute fuite de données vers des destinataires non autorisés et des destinations extérieures au réseau d'entreprise



- **DLP hybrides** : solutions qui utilisent des composants DLP pour réseau et terminaux afin d'exécuter toutes les fonctions des architectures DLP associées

Il convient de rappeler que les DLP pour réseau, du fait de leur architecture, ne protègent pas les données en cours d'utilisation et contrôlent uniquement les fuites de données vers des parties non autorisées extérieures au réseau d'entreprise. Les DLP pour terminaux et hybrides protègent toutes les données, quel que soit leur état, et empêchent les fuites vers des parties non autorisées internes et externes.

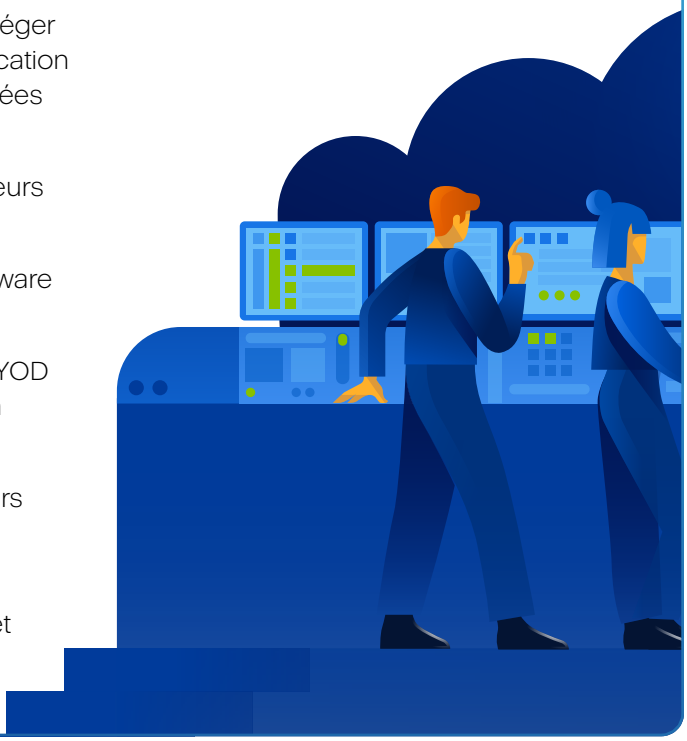
Dans ce guide, nous nous concentrerons sur le lancement, l'exécution et la montée en charge d'un service DLP basé sur l'architecture DLP pour terminaux.

Intérêt d'une solution DLP pour les clients

Selon le rapport « 2021 Cost of Data Breach Report » du Ponemon Institute, le coût total moyen d'une compromission de données est de 4,24 millions de dollars, soit une augmentation de 10 % par rapport à 2020. Parallèlement, il faut actuellement en moyenne 287 jours pour identifier et contenir une compromission, période pendant laquelle vos clients sont exposés à d'importants risques pouvant engendrer des pertes financières, une dégradation de l'image de marque et des coûts de mise en conformité.

Pour contribuer à réduire les risques pour vos clients grâce à un service DLP, vous devez :

- **Les aider à se conformer aux réglementations** et à protéger les informations réglementées — informations d'identification personnelle (RGPD, CCPA), données médicales protégées (HIPAA), données de carte de paiement (PCI DSS), etc.
- **Protéger** leurs éléments de propriété intellectuelle et leurs secrets commerciaux
- **Réduire le risque** d'exfiltration de données par un malware et d'attaques d'ingénierie sociale
- **Renforcer la sécurité des pratiques de télétravail** et BYOD et empêcher le transfert de données sensibles vers un stockage cloud privé
- **Prévenir les fuites de données** imputables à des erreurs accidentelles, des négligences ou des manquements commis par les collaborateurs
- **Réduire le délai de résolution** des fuites de données et accélérer les investigations après une compromission grâce à une visibilité continue sur les événements DLP



Déroulement de la prestation d'un service DLP

Avant d'entrer dans les détails du lancement, de l'exécution et de la montée en charge d'un service DLP, il est important de souligner que compte tenu de ses spécificités, la prestation d'un service DLP s'effectue selon les étapes suivantes :

- **Déploiement d'agents DLP :** pour démarrer le processus de prestation de votre service, il convient d'identifier les terminaux sur lesquels provisionner des services DLP afin d'assurer la protection des données de l'entreprise et de déployer des agents DLP sur ces terminaux. N'oubliez pas qu'il est recommandé de provisionner des agents DLP sur toutes les ressources dans lesquelles des données sensibles sont créées, stockées ou utilisées. En l'absence de protection de ces ressources, le système de sécurité informatique de l'entreprise présente des failles pouvant l'exposer à des fuites de données.

- **Création de stratégies DLP :** cette étape initiale permet de prévenir les fuites de données grâce à des règles appropriées en matière d'utilisation et de traitement des données. Selon la technologie DLP utilisée, cette étape peut précéder le déploiement. **Il est important de souligner** que les stratégies DLP ne sont pas universelles, mais spécifiques à chaque client, du fait des différences entre les processus internes, les réglementations applicables et les besoins en matière d'accès aux données et de partage de données de chaque entreprise. Compte tenu des spécificités de la création de stratégies DLP, les solutions DLP traditionnelles nécessitant une gestion manuelle des stratégies sont trop complexes et coûteuses pour convenir à des fournisseurs de services mettant en place des services DLP.
- **Validation des stratégies DLP :** une fois les stratégies DLP initiales créées, il convient de les valider avec les clients afin de veiller à ce qu'elles soient adaptées à leurs exigences métier. En effet, les MSP ne sont pas en mesure d'acquérir une compréhension suffisamment approfondie des spécificités de l'activité de chacun de leurs clients. Plus la représentation visuelle de la stratégie est complexe et technique, plus il faudra de temps et de compétences au client pour la valider.
- **Application et gestion des stratégies DLP :** une fois les stratégies DLP validées par le client, vous pouvez les appliquer et commencer ainsi à protéger les données métier sensibles contre les fuites. N'oubliez pas que les technologies DLP contrôlent les flux de données sensibles d'une entreprise et bloquent les flux non autorisés. À mesure du développement de l'entreprise, de l'introduction de nouveaux processus, de la publication de nouvelles réglementations et de la modification des réglementations existantes, les stratégies DLP initiales doivent être adaptées à l'évolution continue des besoins afin de veiller à ne pas bloquer de nouveaux flux de données essentiels tout en assurant la prévention des fuites de données. Pour ce faire, des méthodes d'ajustement adaptatif manuelles ou automatiques doivent être utilisées.
- **Reporting sur la valeur ajoutée du service DLP :** un reporting continu sur les transferts de données sensibles bloqués et les actions dédiées des utilisateurs finaux démontre la valeur ajoutée des services DLP, améliore le taux de fidélisation des clients et met en évidence les fuites de données bloquées dont ils ignoraient l'existence.

Difficultés posées aux MSP par les solutions DLP actuelles

La prévention des fuites de données (DLP) est un marché mature ciblant les entreprises où opèrent des acteurs établis de longue date et sur lequel le marché au sens plus large — comme les fournisseurs de services et leurs clients PME — a du mal à s'implanter. En effet, l'utilisation de ces technologies requiert une compréhension approfondie et continue et la mise en correspondance des spécificités métier avec les contrôles DLP, ainsi que la maîtrise des réglementations et des exigences en matière de conformité des données. C'est pourquoi le secteur de la DLP se concentre principalement sur les grandes entreprises qui peuvent se permettre d'avoir des spécialistes en interne dédiés à la gestion DLP.

Voici les principales difficultés posées aux MSP par l'implémentation et l'exécution d'un service DLP :

- **L'exécution d'un service DLP est coûteuse et complexe** : avec les solutions DLP traditionnelles, la création de stratégies initiales et les ajustements ultérieurs sont des opérations manuelles complexes qui ralentissent et renchérissent l'implémentation d'un service DLP efficace. De plus, cette complexité nécessite le recrutement d'experts en la matière, tâche encore plus difficile et coûteuse que l'embauche de spécialistes en sécurité informatique.

- **Un service DLP efficace nécessite des stratégies spécifiques à chaque client** : comme évoqué précédemment, les processus métier et la sensibilité des données sont différents dans chaque entreprise et évoluent en permanence, ce qui oblige à ajuster continuellement les stratégies DLP en fonction des spécificités métier. Toutefois, les MSP ne disposent pas des ressources nécessaires pour acquérir et actualiser en continu de telles informations sur les processus métier de chaque client, ce qui est un obstacle à l'évolutivité des MSP utilisant des technologies DLP traditionnelles.
- **La continuité des activités est menacée par la mauvaise configuration des stratégies DLP** : d'une part, la création et la configuration manuelles de stratégies DLP sont sujettes aux erreurs en raison de la complexité et de la granularité des systèmes. D'autre part, les technologies DLP bloquent tout flux de données non autorisé. Cette complexité, combinée aux fonctionnalités DLP, risque de perturber des processus métier essentiels en bloquant par erreur des flux de données nécessaires si les stratégies DLP sont mal configurées ou si les nouveaux processus métier ne sont pas systématiquement mis en correspondance avec ces stratégies.
- **Les collaborateurs sont le maillon faible des clients** : peu importe que les technologies DLP soient difficilement accessibles aux MSP et à leurs clients, les erreurs humaines et les attaques externes ciblant les collaborateurs sont les principales causes de fuites de données. Même si les fournisseurs de services sont en mesure de limiter le risque de menaces externes en rajoutant des niveaux de protection des terminaux, ils seront tenus responsables si des utilisateurs divulguent involontairement des données sensibles, provoquant ainsi une compromission de données.
- **Les clients peuvent ne pas être conscients des fuites de données** : en raison de l'accès historiquement difficile à la technologie DLP, les clients peuvent ne pas avoir conscience du risque de fuite de données. Pour lancer un service DLP, un fournisseur de services va devoir sensibiliser ses clients aux risques de fuite de données auxquels ils sont exposés et leur démontrer que la DLP est la seule technologie capable de limiter ces risques majeurs pour les entreprises de toutes tailles.

Les nouvelles tendances et technologies du marché — comme la création, le renforcement et la surveillance automatiques des stratégies basées sur les comportements — permettent de résoudre les problèmes liés à l'adaptation rapide des règles DLP en fonction de l'évolution constante des procédures métier, ainsi que des obligations réglementaires. Ces nouvelles fonctionnalités contribuent à la démocratisation du marché de la DLP, le rendant accessible aux fournisseurs de services et à leurs clients. C'est le moment idéal pour compléter votre gamme avec des services DLP.

Planification et lancement d'un service DLP

La première étape de la planification et du lancement d'un service DLP consiste à s'assurer que vos clients en ont réellement besoin.

Un client a besoin d'un service DLP pour réduire le risque de fuite de données s'il répond à tout ou partie des critères suivants :

- Il crée, stocke ou traite sur ses ressources des données sensibles soumises à des réglementations.
- Il possède des secrets commerciaux ou des éléments de propriété intellectuelle devant être protégés contre les fuites.
- Il exerce ses activités dans des secteurs très réglementés.
- Il a été victime d'une compromission de données et souhaite protéger son environnement et réduire les risques.
- Il dispose/a besoin de certifications de conformité.
- Il a souscrit/envisage de souscrire une cyberassurance afin de limiter sa responsabilité.
- Il ne dispose pas d'une équipe de sécurité dédiée et de l'expertise nécessaire.

De plus, les clients des secteurs suivants ont toujours fait preuve d'un intérêt accru pour la DLP :

- Services bancaires et financiers
- Santé
- Services juridiques
- Informatique et télécommunications
- Administrations et secteur public
- Fabrication
- Retail et logistique
- Éducation
- Énergie

Si certains de vos clients répondent à ces critères ou exercent leurs activités dans les secteurs susmentionnés, c'est le moment idéal d'envisager l'ajout d'un service DLP à vos offres. Vous pourrez ainsi mieux répondre à leurs besoins croissants en matière de prévention des risques de fuite de données et de renforcement de la conformité réglementaire.

Planification de votre service et évaluation des coûts

Les trois principaux facteurs déterminant le prix de votre service sont les coûts de main-d'œuvre, les coûts de la solution et la marge souhaitée. Voici l'impact de chacun d'eux sur votre devis :

- **Coûts de main-d'œuvre :** la complexité de la solution choisie détermine le temps que consacreront les techniciens de maintenance au provisionnement et à la gestion du service, ainsi que le niveau requis de leur expertise en sécurité informatique.
- **Coûts de la solution :** les solutions DLP, historiquement réservées aux grandes entreprises, entraînent des coûts élevés que ne peuvent supporter les PME. Si vos clients sont principalement des PME, vous devez choisir une solution qui limite le coût du service.
- **Marge souhaitée :** en moyenne, un MSP génère une marge brute d'environ 50 % sur les services fournis à distance lorsqu'ils sont vendus selon le modèle de revenus récurrents.

Exécution d'un service DLP avec le pack Acronis Advanced DLP

Acronis propose un service DLP basé sur les comportements qui peut être déployé rapidement, qui crée automatiquement et assure en continu la cohérence des stratégies spécifiques à chaque client et qui ne nécessite aucune équipe pour sa maintenance, ni un doctorat en droit sur la protection de la vie privée pour son utilisation.

Avec le pack Acronis Advanced DLP, vous pouvez offrir à vos clients une protection DLP complète et d'une simplicité inédite pour les données en transit et en cours d'utilisation, qui vous permettra de :

- **Débloquer de nouvelles opportunités d'accroissement de la rentabilité** grâce à l'extension de votre gamme qui vous aidera à attirer de nouveaux clients et à augmenter vos revenus par client avec des services DLP jusque-là réservés aux grandes entreprises
- **Réduire les efforts de valorisation** en ajoutant facilement un service DLP à votre activité sans accroître la complexité de gestion, les coûts ni les effectifs
- **Réduire les risques de sécurité pour les clients** grâce à la prévention des fuites de données sensibles
- **Renforcer la conformité réglementaire des clients** grâce à des modèles de classification des données prêts à l'emploi pour les réglementations en vigueur (RGPD, HIPAA, PCI DSS, etc.)
- **Simplifier le provisionnement et la gestion du service** en automatisant le provisionnement du service DLP, la configuration initiale des stratégies et les ajustements ultérieurs
- **Assurer la personnalisation des stratégies DLP à tous les niveaux** en ajustant automatiquement les stratégies DLP en fonction de l'évolution des spécificités métier grâce à une technologie basée sur les comportements, simplifiant ainsi la validation des stratégies par les clients avant leur application
- **Améliorer la réactivité en cas d'événement DLP** et simplifier les opérations, la maintenance des stratégies, les audits de sécurité informatique et les investigations consécutives aux incidents grâce à la centralisation axée sur les stratégies de la consignation des audits et des alertes de sécurité

Pack Acronis Advanced DLP

Le pack 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, tout en limitant vos efforts.

Acronis

Découvrez nos solutions sur www.acronis.com