L'APPRENTISSAGE FACILE

Édition spéciale Netskope

Prévention moderne des pertes de données (DLP)

pour les nuls
A Wiley Brand

Découvrez les techniques modernes de DLP

Utilisez les principes Zero Trust pour protéger les données lorsqu'elles sont en mouvement

Améliorez la sécurité dans le cloud

Proposé par

netskope

Carmine Clementelli

À propos de Netskope

Netskope, un leader mondial du SASE (Secure Access Service Edge), réinvente la sécurité dans le cloud, celle des données et des réseaux pour aider les entreprises à appliquer les principes Zero Trust et à protéger leurs données de manière optimale. Grâce à sa plateforme rapide et conviviale, Netskope offre un accès sécurisé et en temps réel aux utilisateurs, aux appareils et aux données, où qu'ils se trouvent. Avec Netskope, les clients bénéficient d'une réduction des risques, d'une amélioration des performances et d'une visibilité inégalée sur l'activité de toutes les applications cloud, web et privées. Netskope et son réseau NewEdge sont réputés pour leur capacité à relever les défis liés aux menaces en constante évolution, aux nouveaux risques, aux changements technologiques, organisationnels et réseau, ainsi qu'aux exigences réglementaires. Cette entreprise compte parmi sa clientèle plus de 25 entreprises figurant dans le classement Fortune 100. Pour découvrir comment Netskope accompagne ses clients tout au long de leur parcours SASE, visitez le site netskope.com.

Nous souhaitons exprimer notre gratitude envers toutes les personnes qui ont contribué à la réalisation de ce livre, en collaboration avec l'auteur :

Chez Netskope : Amanda Anderson, Chad Berndtson, Jason Clark, Scott Hogrefe, Kathy Jacobsen, Naveen Palavalli, Stephenie Pang, Lauren Polito, Carolyn Robinson, Neil Thacker

Chez Evolved Media : David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Prévention moderne des pertes de données (DLP)

Édition spéciale Netskope

par Carmine Clementelli

pour les nuls®

Prévention moderne des pertes de données (DLP) pour les Nuls®, édition spéciale Netskope

Publié par
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-20766-4 (pbk) ; ISBN 978-1-394-20767-1 (ebk)

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre *pour les Nuls* destiné à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis, par téléphone au 877-409-4177, par e-mail à info@dummies.biz, ou consulter notre site www.wiley.com/go/custompub. Pour obtenir des informations sur la licence de la marque *pour les Nuls* pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Rédacteur projet : Elizabeth Kuball

Rédacteur chargé des acquisitions : Traci Martin

Responsable éditorial : Rev Mengle

Responsable de compte client : Jeremith Coward

Éditeur de la production : Mohammed Zafar Ali

Assistance spéciale : Nicole Sholly

Introduction

La protection des données en tant que concept de cybersécurité n'a rien de nouveau, mais les exigences imposées aux systèmes de protection des données existants ont radicalement changé au cours de la dernière décennie. Autrefois, les experts en sécurité étaient persuadés que les informations précieuses qu'ils sauvegardaient étaient stockées en toute sécurité dans des datacenters hautement sécurisés. Cependant, la transformation numérique implique que les entreprises, qu'elles soient grandes ou petites, transfèrent leurs données vers le cloud et sur des sites répartis géographiquement. Désormais, vos données sont accessibles partout où se trouvent les utilisateurs. Votre entreprise peut partager des connexions numériques avec un grand nombre de tierces parties : fournisseurs, partenaires et sous-traitants.. Ces scénarios offrent à la fois des opportunités commerciales sans précédent (bonne nouvelle) et des défis en matière de sécurité, notamment en ce qui concerne la protection des données (mauvaise nouvelle).

Les violations qui aboutissent peuvent avoir des conséquences dévastatrices pour une entreprise. Les risques liés aux initiés (qu'ils soient malveillants ou négligents) sont aussi dangereux pour votre entreprise que les attaques d'acteurs extérieurs qui font la une des journaux. Tous menacent d'exposer des informations sensibles. La protection des données est devenue essentielle pour garantir la conformité de votre entreprise aux réglementations spécifiques de votre secteur et aux lois sur la confidentialité des données. Ces réglementations définissent clairement les responsabilités de votre entreprise et prévoient des sanctions sévères en cas de non-respect.

Les entreprises doivent adopter une nouvelle approche et appliquer des politiques de protection des données de manière uniforme, quel que soit l'endroit où se trouvent leurs données. Idéalement, la protection des données soutient les objectifs de l'entreprise tout en la protégeant. Mais la gestion des politiques de protection des données et des outils nécessaires à leur mise en œuvre peut s'avérer complexe et coûteuse. Les entreprises ont besoin de solutions de protection des données qui simplifient l'application des politiques tout en garantissant leur efficacité. Une nouvelle génération de solutions de prévention des pertes de données (DLP) en mode cloud offre une alternative prometteuse. Les organisations doivent opter pour une solution cloud moins complexe, hautement évolutive et plus rentable, tout en protégeant idéalement les données avec une plus grande fiabilité et une meilleure précision, et en réduisant au minimum les risques d'accès non autorisé ou d'usage inapproprié. Aujourd'hui, il est possible de trouver cet équilibre délicat en suivant des conseils judicieux.

À propos de ce livre

Ce livre est conçu pour vous aider à prendre des décisions informées concernant la stratégie de protection des données de votre organisation. Il fournit des informations précieuses sur l'évaluation de votre stratégie actuelle et l'identification de nouvelles solutions de protection des données qui répondent le mieux à vos besoins, en mettant en œuvre les principes Zero Trust pour une sécurité contextuelle et cohérente. En expliquant le fonctionnement des systèmes DLP modernes en mode cloud, ce livre élimine les artifices marketing pour identifier les caractéristiques et les capacités nécessaires pour protéger de manière fiable vos données, où qu'elles soient utilisées.

Quelques suppositions idiotes

Ce livre part du principe que vous avez une compréhension élémentaire de la manière dont les entreprises ont adopté le cloud pour gagner en flexibilité et mieux se préparer à la transition numérique. Il présume aussi que vous êtes ici pour trouver la combinaison idéale d'innovations technologiques et de processus afin de protéger vos données sensibles, quels que soient leur emplacement et leur parcours dans votre environnement informatique.

Icônes utilisées dans ce livre

Nous utilisons des icônes pour attirer l'attention du lecteur sur des informations importantes. Voici leur signification :

CONSEIL

Tout le contenu en regard de l'icône *Conseil* est un raccourci pour faciliter une tâche spécifique.

RAPPEL

L'icône Rappel signale les faits qu'il est particulièrement important de connaître.

JARGON TECHNIQUE

Lorsque nous proposons des informations très techniques que vous pouvez ignorer sans risque, nous utilisons l'icône *Jargon technique*.

ATTENTION

Tenez bien compte de tout ce qui se trouve en regard de l'icône Attention pour vous épargner des maux de tête.

Au-delà de ce livre

Bien que ce livre regorge d'informations, si vous vous retrouvez à la fin à vous demander « Où puis-je en savoir plus ? », rendez-vous sur `www.netskope.com`.

DANS CE CHAPITRE

- **Comprendre où les données sensibles sont stockées et comment elles sont contrôlées**
- **En quoi consiste réellement la protection des données**
- **En savoir plus la prévention des pertes de données (DLP)**
- **Découvrir pourquoi la DLP traditionnelle n'est plus une solution viable**
- **Passer à une stratégie « cloud first » avec une solution DLP moderne**
- **Dissiper les mythes courants sur la DLP**

Chapitre 1
Les données sensibles sont partout et de plus en plus difficiles à trouver

En général, lorsqu'on parle de données sensibles, on fait référence à des informations de nature confidentielle ou personnelle. Ce qui est sensible varie grandement selon que l'on considère les données du point de vue de l'entreprise ou du point de vue de la personne.

Guide rapide des données sensibles

Vous remarquerez peut-être que la plupart des données qualifiées de sensibles existent sous une forme ou une autre depuis des années ou des décennies, voire plus longtemps :

- **Données/informations personnelles :** p. ex. numéro de sécurité sociale, numéro de carte bancaire, numéro de permis de conduire, données médicales et adresse du domicile

- La propriété intellectuelle (PI) : p. ex. conceptions de produits, nouvelles inventions, brevets et code source
- Les informations confidentielles et les secrets commerciaux : p. ex. plans financiers, contrats, déclarations fiscales, informations sur les fusions et acquisitions, documents de lancement de produits comme les communiqués de presse

Ce qui est nouveau, c'est que le paysage commercial moderne a complètement changé la façon dont les données sont partagées et malheureusement exposées. De nombreuses entreprises, en particulier depuis l'apparition de la pandémie de COVID-19, adoptent désormais un environnement de travail hybride.

Presque tous les types de données sensibles sont créés, stockés et déplacés numériquement. Les données circulent vers et depuis les services cloud, les réseaux d'entreprise et tout autre emplacement où les utilisateurs peuvent y accéder. Dans le même temps, de plus en plus d'applications stockent et partagent ces données sur plusieurs plateformes, les rendant accessibles à partir de pratiquement n'importe quel appareil et à distance. Le volume, la variété et la vitesse des données augmentant de manière exponentielle, il devient alors difficile d'identifier et de protéger les informations sensibles. L'énorme volume de données disponibles fait que les mesures de sécurité traditionnelles peinent à faire face aux nouvelles menaces qui ne cessent d'apparaître.

Un raz-de-marée de données

D'ici 2025, selon IDC, le monde sera submergé par pas moins de 181 zettaoctets de données ! Une grande partie de ces données sera créée et stockée directement dans le cloud, augmentant d'année en année. Parmi les défis auxquels se heurtent les systèmes de protection des données et leurs opérateurs, on peut citer :

- **Trop de catégories de données sensibles :** l'augmentation des réglementations et des lois sur la confidentialité des données, qui protègent un plus grand nombre d'individus et de types d'informations à l'échelle mondiale, est à l'origine d'une croissance massive des catégories de données sensibles. Il s'agit notamment d'informations permettant d'identifier une personne, telles que sa localisation, ses informations financières et médicales, ses préférences personnelles, ses croyances religieuses et son orientation sexuelle. Les données sensibles comprennent des éléments tels que les numéros d'identification nationaux, les cartes bancaires, le code source, les dessins, les plans financiers, les comptes bancaires, les contrats, les formulaires fiscaux, les mots de passe, les informations sur les fusions et acquisitions, les informations de santé protégées (PHI), les e-mails confidentiels, le sexe et la religion.

Il existe des catégories de données sensibles qui diffèrent d'un pays à l'autre, dans des langues locales, et qui sont spécifiques à chaque pays.

- **Trop de formats et de types de données :** PDF, images graphiques (JPG, PNG et BMP), fichiers compressés et encapsulés (ZIP, RAR et ISO), pièces jointes, messages Slack, chats, formulaires en ligne, captures d'écran, feuilles de calcul, conception assistée par ordinateur (CAO), posts sur les réseaux sociaux, fichiers texte, présentations et e-mails.
- **Trop de contexte :** le contexte doit prévaloir lors de la prise de décision concernant la manière dont les données sensibles doivent être consultées, utilisées, transférées et partagées en toute sécurité. Le contexte permet de définir ce qu'est une action risquée concernant des données sensibles et ce qui devrait être considéré comme une violation ou une tentative de violation, en prenant en compte divers facteurs tels que : l'identité des acteurs, le lieu, la nature de l'action, la méthode employée, les motivations, le moment, les personnes concernées, et d'autres aspects pertinents.

Face à l'afflux de données obscures, les systèmes de sécurité existants sont obligés de faire preuve de prudence, multipliant ainsi les tâches administratives. Pourquoi ? Les équipes de sécurité chargées des réponses en cas d'incident sont confrontées à des montagnes de faux positifs, dont la plupart doivent être évalués manuellement par un personnel déjà surchargé.

La protection des données, c'est bien plus que de simples données

Les entreprises ont besoin de nouvelles stratégies automatisées capables d'identifier, de surveiller et de protéger efficacement leurs précieuses données. Dans le même temps, l'univers dans lequel évolue la protection des données ne cesse de présenter de nouveaux défis, exacerbant ainsi le problème de la sécurité. Ces nouveaux défis sont notamment les suivants :

- **Davantage de risques de cybersécurité :** les entreprises sont plus vulnérables que jamais aux violations de données. Ces vulnérabilités peuvent être à la fois intentionnelles et non intentionnelles. Le comportement inapproprié des initiés, tels que les collaborateurs commettant des actes de vol ou une mauvaise manipulation (oups !), est l'un des moyens par lesquels les informations sensibles d'une entreprise peuvent être exploitées. 82 % des infractions liées aux données impliquent un facteur humain, notamment :
  - *Les initiés malveillants :* par exemple, un collaborateur mécontent peut prendre des captures d'écran d'un document de travail crucial, transférer ces données vers un service de stockage en ligne

personnel via une application SaaS (Software as a Service, logiciel en mode service), ou les envoyer via une adresse e-mail personnelle plutôt que professionnelle (c'est-à-dire en utilisant un compte Gmail personnel au lieu d'un compte Gmail professionnel).

- *Une exposition involontaire :* par exemple, un collaborateur qui envoie par inadvertance trop d'informations à un fournisseur ou qui partage trop de données sur un dossier OneDrive par simple négligence. Tous ces facteurs contribuent largement aux violations de données.

De même, les attaques externes et les tentatives de piratage exposent les secrets de l'entreprise à des risques de rançon, de divulgation publique ou de révélation à des organisations concurrentes.

- **Le cloud, y compris les solutions SaaS et IaaS (infrastructure en mode service) du cloud public :** l'adoption des applications SaaS, en particulier, augmente à un rythme effréné. Selon des études récentes, l'entreprise moyenne utilise plus de 2 400 applications cloud, dont 97 % sont considérées comme *Shadow IT* (non approuvé par le service informatique, inconnue de lui ou invisible à ses yeux). Cela pose des problèmes techniques et de sécurité, car les données peuvent être stockées et partagées par un grand nombre d'applications SaaS, se déplacer sur les réseaux de l'entreprise et les appareils managés, et être facilement accessibles par les collaborateurs et même par des utilisateurs externes se connectant à partir de sites distants avec des appareils non managés. Les applications cloud peuvent rapidement devenir un vecteur d'attaque important, si elles ne sont pas correctement surveillées et managées. Les entreprises doivent prendre des mesures pour améliorer leurs solutions de protection des données afin de se prémunir contre ces menaces.
- **Le travail hybride :** l'essor du travail en mode hybride modifie la manière dont les entreprises stockent leurs données sensibles et y accèdent. Les choses ont radicalement changé depuis l'époque où les entreprises conservaient leurs informations les plus stratégiques dans un datacenter privé qu'elles contrôlaient. Les accords de travail en mode hybride ont engendré une nouvelle ère où les informations sensibles sont largement diffusées dans des espaces situés en dehors du périmètre de l'entreprise, échappant ainsi à sa surveillance et à son contrôle. De nos jours, les données sont réparties dans divers environnements, tant numériques que physiques, notamment les datacenters, le siège social de l'entreprise, les filiales, les bureaux à domicile et les appareils (professionnels et personnels) des utilisateurs en télétravail.
- **Les nouvelles exigences en matière de conformité :** la conformité a toujours été une préoccupation majeure. Toutefois, face à l'augmentation des réglementations imposées aux entreprises et à l'évolution de la législation concernant la confidentialité des données, qui

s'accompagne de sanctions financières et de poursuites judiciaires de plus en plus sévères, les organisations de toutes envergures ressentent une pression croissante pour garantir le respect des normes de conformité et assurer la sécurité de leurs données sensibles. Les entreprises doivent prendre des mesures pour se conformer aux réglementations sectorielles telles que la norme de sécurité des données de l'industrie des cartes de paiement (PCI-DSS), la loi Informatique et Liberté et le code de la santé publique, tout en veillant à respecter les lois et réglementations applicables en matière de confidentialité des données, entre autres le règlement général sur la protection des données (RGPD) et la loi sur la protection du consommateur (DDADUE), pour n'en nommer que quelques-unes. Dans le monde entier, beaucoup de pays sont régis par des législations visant à protéger la vie privée, y compris des nations telles que le Brésil, Singapour, le Japon et le Royaume-Uni. Aujourd'hui plus que jamais, les entreprises doivent montrer qu'elles prennent les mesures nécessaires pour protéger les informations personnelles de leurs clients et se conformer à toutes les politiques législatives pertinentes, sous peine de se voir infliger de lourdes sanctions.

- **Des talents rares et coûteux :** les compétences spécialisées et qualifiées nécessaires à la mise en œuvre de programmes complexes de protection des données sont rares. Les technologies de protection des données requièrent une supervision habile pour faire face aux nombreux incidents déclenchés par le système. Ce problème s'aggrave lorsque les systèmes de protection des données existants surveillent les services cloud comme les applications SaaS (ce pour quoi ils n'ont pas été conçus à l'origine), ce qui entraîne une augmentation du nombre de faux positifs et, par conséquent, un surcroît de travail pour l'équipe. En raison des compétences spécialisées exigées, ces experts en informatique bénéficient de salaires élevés, ce qui peut représenter une charge considérable pour les entreprises, qu'ils soient maintenus en poste et rémunérés, ou qu'ils décident de partir lorsqu'ils sont surchargés et doivent être remplacés.

Qu'est-ce que la DLP et quelle est son utilité ?

Les technologies de sécurité dédiées à la prévention des pertes de données (DLP) sont des systèmes développés pour détecter et protéger automatiquement le stockage, la circulation et l'exploitation des informations sensibles en tout point au sein des réseaux, des utilisateurs et des services d'une organisation. La technologie est déployée afin d'identifier un large éventail de données sensibles, incluant les informations personnelles des clients et des collaborateurs, les documents financiers ainsi que la propriété intellectuelle. La DLP surveille la manière dont ces données sont consultées et utilisées, afin de prévenir les fuites, l'exposition

accidentelle et le vol. Elle permet aux entreprises de réduire les risques de violation de données et de contrôler leurs fichiers pour éviter la publication accidentelle d'informations confidentielles. Face à un paysage de conformité de plus en plus rigoureux et étendu, la DLP s'est désormais imposée comme une mesure de sécurité cruciale pour les entreprises, leur permettant de se prémunir contre les violations de données onéreuses et de satisfaire aux exigences législatives en matière de conformité.

Pourquoi la DLP traditionnelle est aujourd'hui terriblement inadaptée

Les solutions DLP traditionnelles sont utilisées pour la protection des données depuis plus de dix ans. Au fil du temps, la DLP traditionnelle a accumulé une réputation négative, car elle est perçue comme difficile à mettre en place et à gérer, coûteuse, avec des limitations dans son champ d'application, une précision réduite et une couverture incomplète pour répondre aux besoins du travail moderne où les employés peuvent travailler à distance depuis n'importe où dans le monde. Les solutions DLP ont été développées afin d'assurer une protection optimale des données dans les datacenters et l'infrastructure informatique de l'entreprise. L'adaptation de ces solutions aux changements apportés par l'ère du cloud computing a été difficile. Alors que la DLP traditionnelle peut être efficace dans les tâches pour lesquelles elle a été conçue, elle ne convient pas à la sécurisation des données dans le cloud ou à leur transfert entre plusieurs clouds, ce qui est devenu un besoin courant des entreprises. Par ailleurs, son modèle basé sur le périmètre ne peut pas suivre les données qui sont dispersées sur plusieurs sites et dans de multiples applications.

Les inconvénients des anciennes solutions DLP

Les systèmes DLP existants, constitués de plusieurs composants logiciels et matériels, peuvent être difficiles à installer et à gérer. Leur configuration peut être complexe et impliquer un coût élevé, difficilement gérable pour les entreprises disposant de ressources informatiques ou budgétaires limitées. La couverture des entreprises multi-sites est également un défi majeur et coûteux, car il est souvent nécessaire de répliquer l'architecture DLP sur site dans chaque filiale, ce qui peut représenter des coûts supplémentaires importants. Même dans ce cas, l'approche ne répond pas aux exigences cruciales de l'ère moderne, telles que la collaboration à distance, l'intégration du cloud et la souplesse des politiques « apportez votre propre appareil » (BYOD).

Les anciennes technologies DLP nécessitent également de longues mises à jour logicielles et des ajustements continus qui entraînent des interruptions d'activité qu'il est impossible d'ignorer. En raison de ces

perturbations, les entreprises ont tendance à éviter les mises à jour, ce qui peut les amener à accumuler des retards de plusieurs mois, voire de plusieurs années, sur les versions de DLP. Par conséquent, elles se privent des dernières protections disponibles pour faire face aux exigences actuelles en matière de données, de conformité et de gestion des risques.

L'absence de mises à jour et de correctifs pour un système DLP peut engendrer divers problèmes indésirables pour toute organisation, tels que des failles de sécurité, des violations de données et une protection insuffisante des informations. Ceci peut compromettre la sécurité des informations confidentielles et entraver la capacité d'une organisation à se conformer aux réglementations relatives à la protection des données. De plus, la complexité intrinsèque de la DLP traditionnelle entraîne fréquemment des pratiques de protection des données incohérentes et excessivement spécifiques, conduisant ainsi à une utilisation inefficace des ressources et du temps.

ATTENTION

Pour certaines entreprises, les perturbations causées par leur ancien système de protection des données sont jugées si critiques qu'elles passent en mode de « surveillance uniquement » pour leur système DLP. Cela signifie que le système se limite à surveiller les activités sans appliquer de politique de protection des données. Utiliser votre DLP sans appliquer de politique, c'est comme posséder un coffre-fort que vous laissez ouvert, en espérant sincèrement que personne ne s'échappera avec votre argent, vos bijoux et vos documents précieux.

L'énigme des faux positifs

Les systèmes DLP actuels, en plus d'exiger des déploiements et des processus complexes, requièrent également un investissement considérable en ressources et en efforts humains pour assurer une surveillance et des ajustements continus et efficaces. J'ai précédemment mentionné la pression générée par les faux positifs sur les équipes en charge de la sécurité, mais cette problématique vaut la peine qu'on s'y attarde.

Le nombre d'incidents nécessitant une correction manuelle a tellement augmenté que l'équipe chargée de la gestion des incidents se retrouve désormais dans l'incapacité d'analyser la totalité de ces incidents, sans même parler de les résoudre efficacement. Les équipes de réponse aux incidents sont souvent confrontées à un volume élevé d'alertes qui présentent deux problèmes majeurs : elles manquent de contexte pour évaluer leur niveau de risque et sont souvent reçues avec un certain retard après la survenue de l'incident. Par conséquent, les équipes doivent analyser des événements passés et, même en contactant les collaborateurs impliqués, ces derniers ont souvent du mal à se souvenir des détails spécifiques de l'incident. Ces alertes, qui peuvent s'élever à des milliers, voire à des centaines de milliers par jour, proviennent d'une multitude de sources variées. Vu l'ampleur des événements, les équipes responsables

de la sécurité se retrouvent tout simplement dans l'incapacité d'examiner toutes ces alertes ; en fait, elles doivent en ignorer un grand nombre pour pouvoir faire face à la charge de travail.

La répartition et le déplacement des données vers de multiples emplacements en dehors du réseau de l'entreprise jouent un rôle important dans cette problématique. Les solutions DLP traditionnelles ne sont pas équipées pour gérer efficacement la diversité et le volume croissants des données ni pour fournir une détection améliorée grâce à l'apprentissage automatique. De plus, elles ne répondent pas aux exigences des cas d'usage modernes en termes de partage de données et de prise en compte du contexte. Les politiques rigides mises en place par ces solutions ne parviennent pas à s'adapter de manière efficace à l'évolution des risques et des contextes spécifiques à chaque entreprise : par exemple, les personnes manipulant les données, leurs méthodes d'utilisation, l'environnement et l'instance d'application, ainsi que l'évaluation de la sécurité de leurs comportements et la destination finale des données.

Afin de remédier à certains de ces problèmes, des outils d'automatisation et d'orchestration de la cybersécurité, tels que l'analyse du comportement des utilisateurs et des entités (UEBA), ont été incorporés. Ces outils permettent de prendre en compte de manière plus précise les alertes et de les corriger plus rapidement. Or, si le système DLP manque de précision, ne tient pas compte du contexte de l'entreprise, n'est pas conscient des risques et présente de nombreuses lacunes, les modèles UEBA ne pourront pas fonctionner correctement.

Afin de garantir une protection optimale des données sensibles, il est essentiel d'intégrer et d'automatiser un système DLP qui permette une surveillance et une vérification constantes de l'identité des individus et des appareils autorisés, de leur comportement, de leur collaboration et du partage d'informations externes, des applications utilisées et des risques associés, ainsi que d'autres éléments contextuels variés. L'approche basée sur le principe de Zero Trust (voir le chapitre 3) offre la possibilité d'établir des recommandations détaillées concernant les politiques et les règles de gestion des incidents, qui s'ajustent en fonction des variations des conditions de risque et du contexte spécifique dans lequel les données sont exploitées. Une telle approche ne limite en rien les pratiques commerciales modernes, mais les rend possibles en garantissant la sécurité.

Les solutions DLP traditionnelles ne prennent pas en compte les aspects stratégiques du cloud

Les anciens systèmes DLP ont été conçus selon un modèle de sécurité basé sur le périmètre, qui suppose que toutes les données sont stockées au sein du réseau de l'entreprise et des environnements managés. À l'ère

du cloud, où les données sont stockées dans de multiples emplacements cloud et accessibles par des utilisateurs et des appareils situés en dehors du réseau de l'entreprise, ce modèle est trop limité. De plus, les systèmes DLP ne sont pas conçus pour s'intégrer aux services et infrastructures cloud utilisés actuellement. Cela rend difficile, voire impossible, une protection complète des données dans le cloud.

L'intégration de technologies complémentaires, telles que les agents de sécurité d'accès au cloud (CASB) et les passerelles web sécurisées (SWG) fournies en mode cloud, à un système DLP déployé localement, peut offrir une protection renforcée pour les référentiels cloud. Cependant, cela ne résoudra pas les limitations fondamentales du système existant. Les équipes sont également confrontées à des consoles de gestion disjointes et à des politiques de protection des données non harmonisées – qui sont des effets indésirables courants lors de l'intégration de CASB et de SWG à un système DLP existant.

En d'autres termes, l'intégration de technologies supplémentaires à une approche DLP dépassée ne la rend pas adaptée au cloud et ne fait qu'ajouter à la complexité. Un système DLP doit être en mesure de s'adapter aux normes en perpétuelle évolution de la sécurité du cloud grâce à des politiques dynamiques et des capacités d'évaluation des risques en temps réel. Ceci permet aux entreprises de garantir la protection de leurs collaborateurs, clients et données. Les solutions DLP traditionnelles sont déployées localement. Point final.

RAPPEL

Pour assurer la protection des données dans le cloud, la DLP traditionnelle doit s'intégrer de manière harmonieuse aux solutions de sécurité spécifiques du cloud. Les données stockées dans le cloud requièrent une sécurité native au cloud.

JARGON TECHNIQUE

Dans la plupart des entreprises aujourd'hui, deux solutions de sécurité dans le cloud sont généralement associées à la DLP traditionnelle : les CASB pour le trafic des applications cloud et les SWG pour le trafic web des télétravailleurs et des filiales. Ces solutions sont conçues pour le cloud, mais leurs capacités de protection des données sont généralement limitées. Ce faisant, on espère que l'intégration de ces solutions permettrait d'offrir à la DLP traditionnelle une visibilité accrue dans le cloud, ce qui est indispensable pour étendre ses fonctionnalités du site vers le cloud et localiser des données sensibles au-delà des limites du datacenter. Malheureusement, l'intégration s'est avérée particulièrement difficile en raison des redirections du trafic réseau nécessaires, qui reposent sur le protocole ICAP (Internet Content Adaptation Protocol) extrêmement complexe. Heureusement, ce sujet dépasse le cadre de cet ouvrage.

Même lorsque l'intégration est réalisée, l'approche ne s'avère pas durable. D'une part, les CASB utilisent des interfaces de programmation

d'applications (API) pour se connecter aux applications cloud de l'entreprise telles que Microsoft 365, Salesforce, Slack, Zoom, Teams, Google Workspace, Amazon Web Services (AWS) et Box. Ces API améliorent le système DLP existant en fournissant une meilleure visibilité dans ces applications cloud. Par exemple, si des données sensibles sont stockées dans Salesforce, la DLP peut les analyser et les protéger. Les CASB utilisent également une détection en temps réel pour analyser les transferts de données dans des milliers d'applications SaaS.

Il est également difficile de consolider les politiques de protection des données entre les systèmes sur site et les systèmes cloud. Par exemple, les CASB ne peuvent souvent pas reproduire les mêmes politiques que les systèmes DLP traditionnels. Étant donné que ces technologies ne possèdent pas les mêmes fonctionnalités, les politiques et les consoles de gestion deviennent fragmentées et désynchronisées.

Le problème avec cette architecture réside dans le fait que l'intégration d'un système DLP sur site via un CASB avec une application dans le cloud introduit également une *latence* supplémentaire. La latence signifie que même si votre système DLP traditionnel détecte une violation de données dans le cloud, il peut s'écouler plusieurs minutes, voire des heures ou plus, avant de pouvoir mettre en place une réponse adéquate. Imaginez le scénario suivant : la violation a eu lieu, elle a été détectée, mais vous ne l'avez pas arrêtée à temps (ce qui signifie que vos données sont compromises !).

Finalement, associer les technologies DLP traditionnelles aux technologies cloud revient à tenter de fusionner deux éléments distincts. Le premier est un service cloud (CASB), tandis que le second est un déploiement massif de matériel et de logiciels sur site (système DLP traditionnel). Le résultat est délicat, facilement sujet aux vulnérabilités, entraînant ainsi latence et complexité. L'optimisation et la maintenance seront difficiles. L'idéal serait de se débarrasser de cette complexité en simplifiant et en rationalisant l'ensemble, ce qui permettrait de réduire les risques de problèmes.

L'attachement à l'infrastructure locale et le manque de ressources pour une montée en puissance rapide et rentable entravent considérablement l'efficacité de la DLP traditionnelle dans les environnements cloud. Cette approche n'est tout simplement plus viable.

RAPPEL

Afin d'assurer l'efficacité de la DLP, il est essentiel de concentrer les efforts non plus sur le périmètre extérieur de l'ensemble de données, mais plutôt sur les données elles-mêmes, ainsi que sur leur localisation et la manière dont elles sont transférées. Les entreprises doivent désormais délaisser les stratégies DLP traditionnelles pour assurer une protection efficace de leurs informations au sein du cloud.

La DLP à l'ère du cloud

La transformation numérique a révolutionné la manière dont les organisations fournissent des services à la clientèle et développent des produits et des services. Elle a également eu un impact considérable sur la manière dont les données sont sécurisées. Les entreprises, qu'elles soient grandes ou petites, comptent énormément sur la technologie du cloud pour stimuler leur croissance et leur expansion. Par conséquent, les stratégies de sécurité doivent s'adapter à ces évolutions. L'architecture DLP doit s'adapter à l'expansion continue des équipes hybrides en adoptant une approche « cloud first ». Cela permet d'étendre la portée, d'optimiser l'efficacité et la capacité d'évolution, de bénéficier de ressources informatiques performantes et de mettre en place des mesures de prévention des risques plus efficaces. Avec une refonte du modèle de DLP, les entreprises modernes pourront réussir dans un environnement de travail hybride se préparer à l'avenir. La modernisation de la DLP au sein de votre entreprise est un projet d'envergure. Toutefois, étant donné l'évolution constante des risques et les avancées des solutions de DLP adaptées au cloud, il est judicieux d'envisager cette démarche dès maintenant.

Avec la DLP dans le cloud, il n'y a rien de compliqué à déployer, il vous suffit simplement d'activer un service cloud. Vous n'avez pas à gérer de nombreux composants et logiciels nécessitant des mises à jour et une gestion manuelle. Plus besoin de gérer les bases de données DLP ou d'embaucher des experts en bases de données. Vos serveurs DLP ne deviendront plus obsolètes et vous n'aurez plus à les remplacer. Et plus aucun proxy à actualiser.

Les plateformes de protection des données cloud sont spécifiquement conçues pour s'intégrer facilement aux services de sécurité, de réseau, d'infrastructure et de cloud, tout en consolidant de manière harmonieuse les risques et le contexte organisationnel provenant d'autres mécanismes de contrôle. La surveillance des données et les algorithmes de détection sont plus performants dans le cloud, où l'accès à des ressources extensibles à l'infini permet de réduire la charge sur votre infrastructure informatique, tout en suivant le rythme des nouveaux cas d'usage et le nombre d'appareils en constante augmentation. Vous n'êtes plus limité par une infrastructure sur site, ce qui signifie que vos utilisateurs sont couverts où qu'ils aillent.

En outre, grâce à une architecture cloud indépendante de votre infrastructure et de votre planning, votre système DLP reste constamment à jour, avec des mises à jour en temps réel disponibles partout. Cette approche s'avère être un outil bien plus efficace pour protéger les données précieuses de votre organisation.

Briser les mythes

En ce qui concerne la DLP dans le cloud, il est bien connu que le marché est rempli de termes tendance, de promesses exagérées et de jargon technique, ce qui peut entraîner une confusion et une désorientation face aux nombreuses options disponibles. Mais en réalité, toutes les solutions DLP ne se sont pas égales. Dans cet ouvrage, je vous accompagne pour faire la distinction entre les faits et le discours marketing lors de votre sélection, en vous proposant un guide détaillé des caractéristiques et fonctionnalités essentielles de chaque solution.

Prenons maintenant un peu de recul pour démystifier quelques idées courantes liées à la protection des données dans le cloud. Ainsi, vous serez en mesure de distinguer le vrai du faux et de prendre une décision informée parfaitement adaptée aux besoins de votre entreprise.

Mythe : la DLP dernier cri est la meilleure DLP

Réalité : lorsqu'il s'agit de programmes de protection des données, il ne faut rien laisser au hasard. Non seulement le programme doit comporter suffisamment de fonctions pour garantir la sécurité, mais vous devez également vous appuyer sur un fournisseur dédié et compétent qui a une expérience reconnue dans le domaine de la prévention des pertes de données (DLP). Les solutions traditionnelles n'ont peut-être pas été élaborées spécifiquement pour le cloud, mais elles apportent néanmoins des indications sur la maturité de la plupart des solutions DLP cloud.

La solution de protection des données la plus fiable a bénéficié d'une longue période de maturation et a développé de nouvelles fonctionnalités au fur et à mesure. Si vous envisagez d'investir dans un programme complet de protection des données, veillez à ce que votre fournisseur puisse répondre à tous vos besoins, de la prise en charge du cloud à la maturité des fonctionnalités, afin de garantir une sécurité maximale des données. Il ne faut pas confondre la solution la plus récente avec la meilleure.

Mythe : l'ancien système DLP manquait de précision

Réalité : les anciens systèmes DLP ont été élaborés par des éditeurs qui ont investi une décennie ou plus dans le développement d'algorithmes et de stratégies rigoureuses visant à détecter et prévenir le transfert non autorisé d'informations confidentielles.

La précision n'est pas le véritable problème. Le vrai problème, comme je l'ai mentionné plus haut dans ce chapitre, ce sont les faux positifs. Ceux-ci peuvent conduire à une situation dangereuse où les menaces

réelles passent inaperçues et où des données sensibles sont accidentellement divulguées. Cela conduit également à une augmentation de la taille des équipes de réponse aux incidents hautement qualifiées (et donc coûteuses) pour faire face à un volume croissant d'incidents. Dans le chapitre 2, j'explique pourquoi les systèmes DLP doivent être précis et exacts pour maintenir la confiance.

Mythe : en ce qui concerne la DLP, il est nécessaire de se satisfaire d'un niveau de performance « suffisamment bon »

Réalité : lorsqu'il s'agit de s'assurer de la sécurité de vos données, ne faites pas d'économie. Envisagez-vous d'utiliser une solution cloud qui promet une sécurité « suffisamment bonne » ? Réfléchissez-y à deux fois. Vous risquez de vous retrouver avec un ensemble de fonctionnalités limité ou focalisé uniquement sur les vecteurs d'attaque et les catégories de données les plus superficielles, vous exposant ainsi à des risques d'activités malveillantes, de faux positifs et d'identification inexacte.

Investissez plutôt dans un système DLP moderne, en mode cloud, qui offre une précision élevée dans la détection des données, propose des couches de sécurité supplémentaires et assure une protection complète contre les menaces potentielles pesant sur vos données d'entreprise ou autres documents confidentiels. Ne prenez pas de risques avec les données de votre entreprise ; veillez à investir dans le bon système DLP pour une sécurité et des performances optimales.

Mythe : la DLP cloud est moins performante que la DLP traditionnelle

Réalité : actuellement, de nombreux systèmes DLP cloud utilisent moins de 100 identifiants de données (voir chapitre 2) et n'analysent que quelques types de fichiers, ce qui signifie qu'ils ne détectent pratiquement rien. Cela s'explique par le manque de maturité de la technologie. Contrairement aux systèmes DLP développés et utilisés depuis une dizaine d'années, ces nouveaux systèmes ont été conçus pour répondre à de nouveaux cas d'usage ce spécifiques, tels que des applications cloud particulières, et ne protègent qu'un nombre restreint de types de fichiers courants. Le manque d'orientation générale adéquate implique qu'ils ne disposent pas encore de la précision requise pour équilibrer de manière efficace la protection des données et les exigences de l'entreprise, entraînant ainsi des tensions persistantes entre les deux parties. La technologie DLP en mode cloud devrait être supérieure à la DLP traditionnelle en raison de sa capacité à s'adapter massivement et à grande échelle. On pourrait penser qu'avec une plus grande échelle, il serait possible de résoudre les problèmes de faux positifs et d'améliorer la précision.

ATTENTION

En matière de protection des données, l'expérience compte. Bien que les nouvelles options puissent paraître attrayantes sur le papier ou à première vue, les solutions DLP établies offrent un niveau de sécurité et de compréhension plus approfondi, étant donné qu'elles ont été développées et perfectionnées au fil du temps. Optez pour un éditeur qui a fait ses preuves et testez vous-même plusieurs systèmes pour avoir l'esprit tranquille lors de la protection de vos données essentielles.

Mythe : un ensemble de systèmes de protection des données est tout aussi efficace qu'une solution complète et intégrée de protection des données

Réalité : dans le domaine de la protection des données, il peut sembler logique de mettre en place des initiatives et des programmes de sécurité regroupant plusieurs produits et services DLP distincts provenant de différents éditeurs. Après tout, les services DLP peuvent déjà être intégrés à certaines applications SaaS, à des services de cloud public, à des pare-feu et à des solutions SWG. Mais tôt ou tard, ces programmes de protection des données multiservices seront inévitablement insuffisants. En unifiant des systèmes disparates qui n'ont pas été conçus conjointement, la solution risque de fournir une compréhension limitée du contexte et des risques de l'entreprise. De plus, les experts de la protection des données se retrouveront face à des politiques disjointes et à des consoles multiples. En réalité, la portée de chaque service DLP intégré est généralement restreinte à des environnements et à des canaux spécifiques, se concentrant par exemple exclusivement sur le trafic web ou sur des points de contrôle spécifiques tels qu'une ou plusieurs applications SaaS. Cela rendra vos données vulnérables dès qu'elles seront rendues publiques.

Pour assurer une protection optimale pour vous et votre organisation, optez pour des solutions entièrement intégrées offrant une couverture exhaustive des données. Celles-ci doivent couvrir l'ensemble des domaines de risques potentiels, y compris les services cloud, les infrastructures sur site, les services de messagerie et les terminaux, tout en garantissant une protection complète à travers divers types de données et de contrôles.

DANS CE CHAPITRE

- **Découvrir les défis traditionnels auxquels la prévention des pertes de données (DLP) est confrontée**
- **Se préparer à s'adapter à d'éventuels changements et à une croissance future**
- **Connaître les réalités et les limites de la DLP en mode cloud**
- **Comprendre comment la DLP renforce l'efficacité des autres outils de sécurité**

Chapitre 2
Protéger l'ensemble de l'entreprise dans le cloud

Pourquoi est-il important que les systèmes de protection des données d'une organisation protègent l'ensemble de l'entreprise, y compris ses applications cloud ? Parce que la perte de données ou l'accès non autorisé à celles-ci peut avoir de graves conséquences pour une organisation et ses parties prenantes. Cette approche peut sembler évidente, mais dans la pratique, de nombreuses forces entravent la réalisation de cet objectif. Dans ce chapitre, j'explique pourquoi une protection complète des données dans l'ensemble de l'entreprise est un processus pouvant avoir des bénéfices immédiats tout en offrant des avantages stratégiques à long terme.

Entreprises sans frontières

Il y a dix ans, le concept d'entreprise était largement défini par les limites physiques d'un bâtiment ou d'un site. Généralement, les collaborateurs, les équipements et les ressources étaient situés à l'intérieur de ces murs. Or, la définition de l'entreprise a évolué au fil du temps pour refléter la nature changeante du monde des affaires et de la technologie, et l'entreprise n'est plus limitée à un emplacement physique.

Vu le développement du télétravail, des données précieuses sont susceptibles de transiter sur les appareils et les réseaux domestiques de vos collaborateurs. Avec l'essor des services cloud, vos données peuvent être

disséminées à différents emplacements de cette infrastructure, notamment dans des applications SaaS (Software as a Service) comme Microsoft 365 et Salesforce, ainsi que dans des conversations en ligne sur des applications de collaboration comme Slack et Microsoft Teams (voir figure 2-1). Le périmètre de l'entreprise comprend désormais les nombreux appareils que les collaborateurs utilisent pour se connecter aux ressources de l'entreprise, ainsi que les milliers d'applications cloud approuvées ou non qui peuvent être utilisées au sein de l'entreprise.

ATTENTION

Si vous ne savez pas où se trouvent vos données sensibles, vous ne pourrez pas les protéger. Si vous savez que des données sensibles existent quelque part, mais que vous ne connaissez pas leur emplacement ni leur destination, vous ne pourrez pas les protéger non plus.

RAPPEL

Afin de garantir la détection et la protection de toutes les données sensibles, indépendamment de leur localisation ou de leur destination, il est crucial d'adopter une approche globale en matière de détection et de protection des données sensibles. Cela implique d'éliminer toutes les lacunes en termes de couverture et les éventuels « angles morts » où les données seraient susceptibles d'être divulguées ou exposées involontairement sans que vous en soyez conscient.

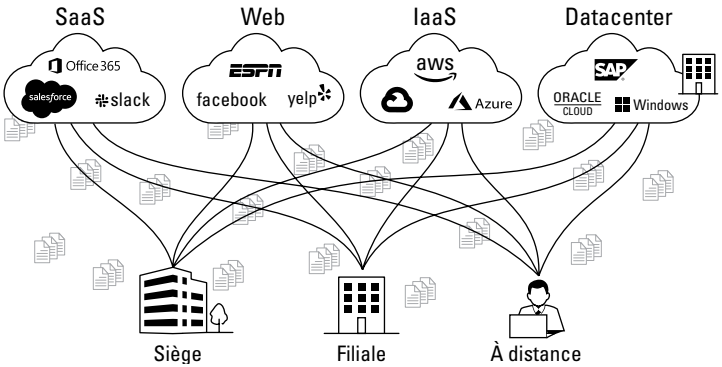

FIGURE 2-1 : Dans l'entreprise moderne hautement distribuée, les données résident et circulent dans de nombreux nouveaux environnements.

Le défi que la DLP doit relever au fur et à mesure de son évolution

Comme je l'ai expliqué au chapitre 1, les systèmes DLP ont été principalement axés sur la protection des données stockées *dans* un datacenter d'entreprise. Aujourd'hui, il est important de protéger les données partout où elles se trouvent, que ce soit dans le cloud, sur des appareils distants, dans le réseau de l'entreprise ou sur des sites extérieurs. Cela signifie que les

anciens systèmes DLP, qui ont été conçus pour protéger les données au sein de l'entreprise, ne sont plus suffisants.

RAPPEL

Même s'il est nécessaire d'identifier tous les emplacements où les données résident et circulent, une approche axée sur la protection des données elles-mêmes plutôt que sur leurs origines et leurs emplacements peut offrir des avantages considérables en termes de flexibilité et d'efficacité. C'est un peu comme une équipe de basketball qui passe d'une défense de zone à une défense individuelle. Comme je l'explique plus en détail par la suite, en adoptant cette approche globale, vous pouvez protéger vos données sensibles et éviter qu'elles ne tombent entre de mauvaises mains.

Lorsque vous remplacez un ancien système DLP, il est essentiel que la nouvelle solution offre à votre entreprise une couverture complète à la fois des canaux cloud et des canaux traditionnels sur site. Même les solutions DLP en mode cloud les plus modernes ont été conçues pour couvrir uniquement des canaux spécifiques sur site. Elles peuvent protéger un réseau, un ensemble d'appareils ou des applications particulières, mais elles ne sont pas en mesure de couvrir l'ensemble des cas d'usage modernes.

Afin de garantir une protection totale de l'entreprise, il est nécessaire que la solution DLP choisie assure la sécurité de toutes les transmissions de données, quel que soit l'emplacement ou l'appareil d'origine et de destination. Il s'agit de prendre en compte tous les appareils, qu'ils soient managés ou non, utilisés par les utilisateurs à l'intérieur et à l'extérieur du réseau de l'entreprise, y compris dans les applications SaaS, les solutions IaaS (infrastructure en mode service), le courrier électronique, les applications privées et les appareils. Cela nécessite une solution DLP complète et flexible, capable s'adapter aux besoins en constante évolution d'une entreprise hautement distribuée.

Dans les sections suivantes, j'examine les éléments clés à prendre en compte lors de la conception d'une solution DLP pour la nouvelle entreprise sans frontières.

Évolutivité et pérennité

Il n'y a pas si longtemps, les entreprises utilisaient peu d'applications SaaS, mais, petit à petit, le nombre d'applications de ce type utilisées par leurs collaborateurs a considérablement augmenté. Aujourd'hui, il n'est pas rare que les entreprises utilisent des centaines d'applications SaaS approuvées, et leurs collaborateurs pourraient bien utiliser des milliers d'autres applications sans qu'elles le sachent, ce qui serait préoccupant.

CONSEIL

L'évolutivité implique non seulement de satisfaire les besoins actuels, mais également de se préparer à des changements potentiels et à une expansion future. Il est crucial d'adopter une approche tournée vers l'avenir afin de concevoir des solutions flexibles et adaptables qui puissent répondre à une charge de travail en constante augmentation ou à une

expansion continue, tout en préservant les performances et les fonctionnalités. L'évolutivité vous permet de garantir que vos systèmes demeurent performants et productifs même en cas de modifications imprévues.

Mais l'évolutivité ne consiste pas seulement à s'adapter à de nouveaux environnements et à couvrir de nouveaux emplacements pour les données. Elle consiste également à gérer la vitesse, la variété et le volume croissants des données. La quantité de données générées et collectées aujourd'hui est sans précédent. Grâce à la popularité croissante des applications de collaboration et des outils en ligne, les données peuvent désormais prendre la forme de discussions sur des plateformes telles que Slack, Teams et Zoom, ainsi que sur des applications de messagerie électronique dans le cloud telle que Gmail. Elles peuvent également se présenter sous la forme d'images, telles que des photos et des captures d'écran. Les gens ont autant tendance à faire des captures d'écran d'informations importantes qu'à les coller dans un document. L'évolutivité consiste à protéger tous les formats de données et tous ces cas d'usage, y compris ceux qui n'ont pas encore été développés.

RAPPEL

La section « La DLP moderne en action », plus loin dans ce chapitre, explique plus en détail le fonctionnement des systèmes DLP. Pour l'instant, gardez à l'esprit que la fonctionnalité de base d'un système DLP est de détecter les données sensibles et de les protéger.

Comment la DLP est passée du statut d'héroïne à celui d'enfant à problèmes

Au fur et à mesure que les organisations adoptaient des applications cloud et s'étendaient à de nouveaux sites, le déploiement de systèmes DLP traditionnels devenait de plus en plus difficile à gérer. Ces systèmes étaient conçus pour être installés et gérés sur site, ce qui signifiait qu'il fallait les dupliquer et les installer dans chaque nouveau site et nouvelle filiale. Cela a ajouté un degré de complexité important et nécessité beaucoup de ressources, notamment en termes de matériel, de maintenance et de personnel. En outre, un niveau de complexité supplémentaire est venu s'y ajouter avec la tendance croissante au télétravail, puisque les collaborateurs ont commencé à accéder à des données sensibles à partir d'une variété d'appareils et de lieux différents. Dans ces conditions, il était difficile pour les organisations de gérer efficacement leurs systèmes DLP, avec pour conséquences une augmentation des coûts et des risques potentiels pour la sécurité.

Avez-vous déjà retardé la mise à jour de votre smartphone ou de votre ordinateur portable par crainte que cela ne perturbe une application souvent utilisée ou ne crée un problème gênant ? Multipliez ce chiffre par des milliers, et imaginez que vous ayez à mettre à jour des logiciels de DLP existants dans de multiples serveurs et filiales, ainsi que sur des milliers d'appareils utilisés par des collaborateurs. Il n'est donc pas étonnant que

certains clients préfèrent utiliser d'anciennes versions de leur logiciel DLP, car cela nécessite moins d'efforts que de procéder à une mise à jour.

ATTENTION

Si les mises à jour ne sont pas effectuées régulièrement, cela laisse les données vulnérables et augmente les risques de non-conformité et d'atteinte à la protection des données.

La DLP doit travailler plus intelligemment, et non plus durement

Les systèmes DLP traditionnels analysent tous les formulaires de données et identifient les informations sensibles à protéger. Ils partent du principe que seules les données sensibles doivent être protégées, car la protection des données non sensibles peut avoir un impact négatif sur la productivité. Par exemple, il est certes important d'empêcher que certaines données sensibles soient partagées par courrier électronique avec des tiers, mais il n'est pas nécessaire de protéger, voire de retarder toutes les communications par courrier électronique avec des tiers, car cela peut entraver la communication et la collaboration et générer trop d'alertes pour l'équipe chargée de gérer les incidents. De plus, il est possible que les collaborateurs soient autorisés à utiliser les ressources de leur entreprise pour des activités personnelles, comme le partage de photos sur les réseaux sociaux, à condition que le contenu ne soit pas confidentiel et ne révèle pas de secrets professionnels. Les systèmes DLP traditionnels étant constitués de composants logiciels et matériels, l'analyse de l'ensemble du trafic web et de tous les dépôts de fichiers, ainsi que la recherche de tous les types de données sensibles, nécessitent le déploiement de serveurs et de modules de détection supplémentaires, et de bases de données plus importantes.

En raison de leur déploiement sur site, les systèmes DLP traditionnels s'appuient sur des ressources informatiques matérielles qui sont nécessairement limitées. Par exemple, les logiciels DLP installés sur les ordinateurs du personnel sont conçus de manière restrictive, limitant leurs capacités de détection des données, en ayant recours à des moteurs de détection de base qui sont moins exigeants en termes de ressources. Par conséquent, même s'ils peuvent détecter certaines données sensibles sur les appareils, ils ne sont pas en mesure d'utiliser des méthodes de détection avancées, ce qui peut entraîner la non-détection d'une quantité importante de données sensibles. Par exemple, la DLP traditionnelle n'est pas en mesure d'utiliser des technologies avancées, telles que l'apprentissage automatique (ML) et la correspondance exacte des données, qui nécessitent des ressources de traitement importantes (comme décrit dans la section suivante). La solution DLP en mode cloud bascule les activités gourmandes en ressources vers le cloud tout en continuant à les appliquer sur l'appareil. L'évolutivité de cette approche représente une avancée considérable, permettant à la DLP de détecter des empreintes de données telles que des noms spécifiques, des numéros de sécurité sociale et d'autres informations sensibles associées à des individus.

RAPPEL

Grâce à l'évolutivité infinie offerte par le cloud, il est possible d'optimiser ces capacités de détection, en permettant ainsi aux systèmes DLP de se concentrer sur les données les plus importantes et de les protéger contre tout accès non autorisé.

Le besoin de précision

L'un des mythes les plus répandus, dont je parle au chapitre 1 , est celui de l'inexactitude de la DLP traditionnelle. Or, la précision n'est pas le véritable problème, ou du moins pas la principale préoccupation. Le principal problème est celui des faux positifs (également abordés au chapitre 1), qui sont principalement dus à l'absence de contexte. Effectivement, avec la prolifération des données sur plusieurs appareils et applications en dehors du périmètre de l'organisation, plus la complexité croissante de la détection des données sensibles due à la diversité exponentielle des types de données, les anciens systèmes DLP n'ont pas été en mesure de s'adapter et leur précision s'est amoindrie. Cependant, le problème principal réside dans le fait que les solutions DLP traditionnelles ont souvent été trop restrictives, signalant ou bloquant des actions bénéfiques sans prendre en compte le contexte métier ou le niveau de risque associé. Dans un monde où la collaboration est essentielle à la nouvelle façon de mener une entreprise, le nombre de ces fausses alertes est devenu excessif.

Il est important que la DLP ne crée pas de friction pour l'entreprise et ne perturbe pas le flux de données nécessaires aux opérations métiers légitimes. Prenons le cas d'un collaborateur qui souhaite envoyer un fichier à un sous-traitant de confiance, impliqué dans un projet. Dans une telle situation, il faut que la solution DLP ne bloque pas cette transmission. Dans l'idéal, la solution DLP doit permettre aux équipes d'intervention d'être plus efficaces en amplifiant les incidents légitimes de perte potentielle de données et en filtrant le bruit généré par les faux positifs.

L'exactitude et la précision n'étaient pas les principaux problèmes des systèmes DLP traditionnels, mais elles le sont pour les solutions DLP cloud les moins avancées. Il existe deux aspects :

- En raison de l'imprécision de la détection des données, il est possible de détecter et de protéger inutilement une quantité excessive de données qui ne sont pas sensibles – des données faussement identifiées comme étant sensibles alors qu'elles ne le sont pas – et éventuellement d'interrompre des communications commerciales légitimes.
- Les méthodes de détection pour identifier de manière précise les données qui sont réellement sensibles peuvent manquer, ce qui peut laisser des données sensibles exposées. Par exemple, si le système n'est pas en mesure d'identifier certains formats et types de fichiers tels que des images ou des fichiers compressés, ainsi que des informations spécifiques comme les numéros de passeport, les données médicales,

les numéros d'acheminement internationaux et les identifiants nationaux propres à un pays.

RAPPEL

Pour maintenir la confiance, il est essentiel que les systèmes DLP soient précis et exacts. Ils doivent signaler et bloquer uniquement les transferts de données réellement malveillants, en évitant la génération excessive de faux positifs.

Ingrédient clé n° 1 : identificateurs de données

Les *identificateurs de données* sont utilisés pour localiser des informations sensibles telles que les numéros de sécurité sociale ou de carte bancaire, en se basant sur un contenu décrit de manière générique, comme les expressions régulières (ou *regex*) : cet outil puissant permet à la DLP d'identifier automatiquement des types de données spécifiques en utilisant des termes, des expressions et des modèles naturels et couramment utilisés (par exemple, « rechercher un nombre à neuf chiffres »). Il existe une réponse possible : c'est un numéro de sécurité sociale. Mais comment pouvez-vous en être certain ?

Les identificateurs de données utilisent des règles spéciales basées sur le nombre de chiffres, des motifs textuels, des séquences, des séparations et des mots clés de proximité (comme le numéro de sécurité sociale [SSN], le mot de passe [pwd], le numéro de carte bancaire [CCN], et ainsi de suite) pour reconnaître ces numéros et les conserver en toute sécurité. Voici quelques points importants à garder à l'esprit concernant les identificateurs de données :

- Il est essentiel d'avoir des milliers d'identificateurs de données prédéfinis, ainsi que la possibilité de les personnaliser en fonction de votre activité, afin de garantir la sécurité de vos informations et de respecter les règles de gouvernance. En outre, la possibilité de modifier ou de créer des identificateurs de données personnalisés est essentielle, car chaque organisation peut avoir des informations sensibles spécifiques qui nécessitent une protection adéquate.
- Les identificateurs de données doivent prendre en charge des milliers de types de fichiers (Word, XLS, JPG, PNG, PDF, CSV, ZIP, RAR, etc.), de formats et de catégories (image, analyse, archive et compression, feuille de calcul, audio, vidéo, base de données, etc.) (voir le chapitre 1).
- Vous devez prendre en charge une vaste gamme de numéros d'identification spécifiques à chaque pays, tels que les informations bancaires internationales, les adresses, les codes postaux, les numéros d'identification nationaux, les numéros de passeport et les indicatifs téléphoniques. De plus, il est nécessaire de respecter les profils de conformité réglementaire et de protection de la vie privée afin de garantir que la solution DLP puisse répondre aux exigences de gouvernance les plus récentes.

CONSEIL

Pour être efficace, votre système DLP a besoin de milliers d'identificateurs de données. Ainsi, il pourra signaler avec précision les informations potentiellement sensibles où qu'elles se trouvent, dans tous les États, régions et pays.

Ingrédient clé n° 2 : correspondance exacte des données (EDM)

L'EDM est un moyen de trouver des informations structurées spécifiques à partir de sources telles que des feuilles de calcul et des bases de données. L'EDM permet à une solution DLP de créer des empreintes numériques et d'indexer les dossiers confidentiels des clients et des collaborateurs. Cela facilite l'identification d'une personne à partir de son nom complet, de son numéro de sécurité sociale, de son adresse et d'autres numéros d'identification. L'EDM peut également servir à trouver des documents financiers qui identifient les actifs d'une personne, tels que les numéros de cartes de paiement ou de comptes bancaires. Elle peut même être utilisée pour les informations de santé et les bases de données d'identification et de tarification des produits. Grâce à l'EDM, une solution DLP peut indexer ces informations et les retrouver là où elles sont censées se trouver. Pour que l'EDM soit efficace et précise, elle doit faire correspondre différents éléments de données indexées et combiner les champs de données d'un enregistrement particulier. Elle doit également être en mesure d'indexer des milliards d'enregistrements afin de soutenir les organisations en pleine croissance, leurs bases de données en expansion et la quantité toujours croissante d'informations qu'elles génèrent. C'est pourquoi l'échelle de traitement est importante pour l'EDM.

Ingrédient clé n° 3 : capacités avancées de détection des données

Les organisations ont besoin d'un système DLP capable de détecter avec précision les informations sensibles, compte tenu de la grande variété de types de données et de modes de transfert disponibles. Les *capacités de détection avancées* sont diverses. En voici quelques exemples :

- **Reconnaissance optique de caractères (OCR) et reconnaissance d'images basée sur l'intelligence artificielle (IA) :** ces fonctionnalités sont de plus en plus importantes pour la protection des données. De nos jours, on capture très facilement des images de documents, de formulaires, de cartes d'identité, de tableaux blancs et d'autres types d'images. Par exemple, on prend souvent des captures d'écran ou des photos instantanées afin de saisir rapidement des informations et de les communiquer à un collègue. Grâce à l'OCR, une solution DLP peut extraire le texte d'une image, puis appliquer une classification des données basée sur les politiques de détection en vigueur.

- **Intelligence artificielle (IA) et apprentissage automatique (ML) :** en utilisant des techniques de détection avancées, l'IA et le ML peuvent classifier les images en reconnaissant différents types de fichiers et de documents courants tels que les cartes bancaires, les formulaires fiscaux, les accords de non-divulgation (NDA), les formulaires de fusion et d'acquisition (M&A), ainsi que les brevets. Tout ceci peut être fait sans avoir besoin d'extraire le contenu de ces documents. Ces méthodes peuvent détecter des éléments de contenu flous, froissés ou endommagés, même lorsque les informations sont difficiles à lire clairement. En effet, les algorithmes sont entraînés pour reconnaître des modèles et des attributs particuliers propres à chaque document, tels que la présentation, les styles de polices et les couleurs utilisées. En outre, ils peuvent également tenir compte du contexte dans lequel le document est utilisé. Grâce à cette fonctionnalité, l'IA est capable de classer de manière précise les documents, même dans des conditions difficiles telles que des images de faible qualité ou des documents endommagés.
- **Création d'une empreinte numérique des dossiers et des documents :** cette technique est essentielle pour les organisations qui souhaitent garantir la sécurité et la confidentialité de leurs documents stratégiques et de leurs fichiers hautement sensibles. En indexant l'ensemble d'un document et en détectant les copies exactes ou partielles de son contenu, les entreprises peuvent prévenir la fuite et la duplication non autorisées de leurs informations confidentielles (telles que les documents de fusion et d'acquisition, les informations préalables à une mise sur le marché, les dessins techniques ou les données relatives aux investisseurs). Cette technique est particulièrement utile pour détecter les copies de fichiers sensibles dans des environnements et des canaux de transmission à risque, tels que les e-mails sortants et les téléchargements d'e-mails vers des instances d'applications personnelles.

Les solutions DLP traditionnelles, dans leur formule uniquement sur site, ont apporté quelques réponses par le passé, mais elles ne peuvent plus suivre la cadence. Elles n'ont tout simplement pas la puissance de calcul ni l'évolutivité nécessaire.

Ingrédient clé n° 4 : beaucoup de contexte et un modèle de protection des données Zero Trust

Telles les vagues de l'océan qui sont en perpétuel mouvement et changent constamment, les utilisateurs, les réseaux, les applications, les données et les règles de gouvernance au sein d'une entreprise sont également en constante évolution. Pour garder une longueur d'avance sur les risques potentiels, un système DLP et une stratégie connexe doivent être capables de s'adapter et de réagir rapidement et efficacement aux changements constants dans le paysage des données. Ils doivent, en d'autres termes,

comprendre le contexte. Cette souplesse permet au système DLP de protéger efficacement les données sensibles, de minimiser les risques de violation des données et d'assurer la conformité aux réglementations en vigueur sans nuire à la productivité des utilisateurs ni à la continuité de l'activité.

Pour atteindre cette subtilité et cette flexibilité, une plateforme de protection des données en mode cloud doit être intégrée à l'infrastructure de sécurité et de réseau globale de l'entreprise. Cette plateforme DLP doit également collecter en continu des informations provenant de diverses sources telles que la gestion de l'identité, l'analyse comportementale, les logs du réseau, les outils de sécurité cloud, l'analyse des menaces, la sécurité du réseau, les mesures de sécurité SaaS et cloud, les indices de confiance natifs cloud des agents de sécurité d'accès au cloud (CASB), ainsi que les mesures de sécurité des appareils. Ces informations peuvent être utilisées de manière précise pour identifier les circonstances spécifiques de l'accès d'un utilisateur aux données sensibles, évaluer le contexte professionnel et les risques potentiels associés à une telle action, et par conséquent, déterminer le niveau d'accès approprié et la réponse adéquate en matière de protection des données. Toutes ces opérations sont effectuées en utilisant plusieurs facteurs, notamment l'identité, la localisation et le comportement d'une personne, la sécurité de son appareil, la fiabilité du réseau, la réputation de l'application utilisée, la destination finale d'un transfert de données, et ainsi de suite.

CONSEIL

En tenant compte des risques et du contexte, une plateforme de protection des données peut s'adapter en permanence et offrir une efficacité élevée, ainsi qu'une réponse précise aux incidents.

Le chapitre 3 traite du concept Zero Trust et de son rôle central dans l'efficacité des solutions DLP. Pour l'instant, gardez à l'esprit que le principe de Zero Trust est une stratégie de sécurité essentielle qui suppose que tous les utilisateurs, appareils et réseaux présents dans l'environnement d'une organisation peuvent potentiellement représenter une menace et doivent donc être traités avec méfiance en permanence.

Cela signifie que tous les accès aux ressources et aux systèmes sont soumis à des contrôles et à des vérifications rigoureux, que l'utilisateur ou l'appareil se trouve à l'intérieur ou à l'extérieur du périmètre du réseau. Le contexte est le moteur d'une stratégie Zero Trust, car il permet au système DLP de choisir en connaissance de cause quand autoriser ou non les activités liées aux données.

RAPPEL

La différence entre un simple *outil* de protection des données et une véritable *plateforme* de protection des données réside dans sa capacité à travailler en collaboration avec des solutions de sécurité intégrées et des technologies de protection des données complémentaires.

La DLP moderne en action

La DLP occupe une position centrale au sein de l'infrastructure de sécurité informatique d'une entreprise, et elle permet d'améliorer l'efficacité des autres outils de sécurité. Elle remplit plusieurs fonctions essentielles, dont les suivantes :

- **La DLP identifie les données sensibles, quels que soient leur emplacement et leur parcours, par exemple :**
  - Les *données en mouvement*, c'est-à-dire les données qui traversent l'Internet, les réseaux, les applications et les appareils (comme les chargements et les téléchargements).
  - Les *données au repos*, c'est-à-dire les données stockées. Il peut s'agir d'un stockage dans vos applications privées, d'une application SaaS adoptée par l'entreprise – par exemple lorsque les données des clients sont stockées dans Salesforce – ou de documents à usage interne stockés et partagés sur Microsoft OneDrive ou Microsoft SharePoint.
  - Les *données en cours d'utilisation*, c'est-à-dire les données qui sont activement utilisées dans le cadre d'une collaboration, comme le transfert vers une clé USB, les activités liées à l'impression ou l'envoi de données par fax. (Envoie-t-on encore des fax ?)
- **La DLP surveille l'environnement des données** pour détecter les personnes qui accèdent aux données et ce qu'elles font avec celles-ci. En surveillant les actions, la solution DLP est capable de repérer des incidents tels que le partage non autorisé d'informations confidentielles, qui pourraient constituer une violation de la politique de l'entreprise. Elle peut ensuite prendre les mesures nécessaires pour remédier à ces situations. Ainsi, il est possible de garantir que les données sensibles ne sont pas consultées ou utilisées sans les privilèges appropriés, selon qu'il s'agit de collaborateurs ou de personnes externes, d'appareils professionnels ou d'appareils personnels. De plus, cela permet de s'assurer que toute utilisation non autorisée ou suspecte, telle que des téléchargements massifs de fichiers, est détectée rapidement et que toute violation potentielle de la sécurité est identifiée et corrigée dans les plus brefs délais.
- **La DLP prend automatiquement des mesures pour appliquer les politiques**, par exemple en arrêtant le flux de données, en chiffrant les données, en mettant en quarantaine les informations confidentielles ou en ne partageant pas les données sur une application SaaS. Par exemple, si un collaborateur utilise OneDrive pour partager intentionnellement ou accidentellement un fichier contenant des informations confidentielles avec des utilisateurs externes, la solution DLP peut automatiquement annuler le partage du fichier pour empêcher sa divulgation non autorisée.

- **La DLP permet d'accompagner les utilisateurs** en les informant automatiquement des violations et de leurs causes, tout en leur apprenant des pratiques sûres en matière de traitement des données. La notification permet également d'informer instantanément les utilisateurs sur les politiques de sécurité, réduisant ainsi la nécessité pour les équipes chargées de répondre aux incidents de trier manuellement les problèmes. Une bonne solution DLP doit également être en mesure de notifier les utilisateurs instantanément, sans délai, et de faire remonter les notifications jusqu'aux responsables, à l'équipe de réponse aux incidents de cybersécuritéou aux RH si nécessaire.

C'est le moment de changer votre solution DLP

La DLP traditionnelle a été une solution de sécurité fiable pendant des années, et il n'est pas étonnant que tant de professionnels en soient encore fans. Après tout, comme je l'ai indiqué précédemment, ces systèmes ont été largement développés au cours de la dernière décennie pour assurer la protection des réseaux sur site contre les menaces prévalentes avant l'avènement du cloud.

Les fournisseurs traditionnels de DLP ont tenté de combler le fossé entre leurs systèmes et les exigences des entreprises modernes, axées sur le cloud, en utilisant des technologies cloud telles que les passerelles web sécurisées (SWG) et des solutions CASB à l'aide de l'intégration du protocole ICAP (Internet Content Adaptation Protocol)

ATTENTION

Malheureusement, la plupart des systèmes DLP traditionnels ne sont pas spécifiquement conçus pour gérer les scénarios d'utilisation dans le cloud et le travail hybride. Ces scénarios requièrent une intégration de services cloud et des fonctionnalités spécifiques, ce qui n'est pas aisément pris en charge par les systèmes DLP traditionnels. Par conséquent, cela peut entraîner des problèmes de compatibilité et des performances insatisfaisantes.

Ces diverses limitations, ainsi que d'autres, abordées dans les chapitres précédents, ont rendu la DLP traditionnelle impopulaire, conduisant de nombreuses organisations à abandonner complètement ces outils. À mesure que les organisations transfèrent de plus en plus leurs données vers le cloud, il devient de plus en plus nécessaire d'avoir des systèmes DLP cloud capables de reconnaître les contextes changeants et les risques associés à la gestion des données. Ces systèmes doivent être faciles à déployer, à étendre et à faire évoluer, et être capables de couvrir à la fois les cas d'usage traditionnels et modernes. Étant accessibles via le cloud, ces systèmes sont constamment mis à jour, ce qui leur permet d'améliorer la protection au fur et à mesure que le contexte et les risques de l'entreprise évoluent.

DANS CE CHAPITRE

- **Découvrir comment une sécurité des données dépassée peut nuire à votre entreprise**
- **Découvrir les types de contextes de données et assurer le bon déroulement des activités de l'entreprise**
- **S'adapter à l'évolution des risques pour protéger vos données**
- **Veiller à ce que les nouveaux cas d'usage des entreprises puissent se mettre en place en toute sécurité**
- **Évaluer le contexte métier, les risques et le comportement des utilisateurs pour assurer la sécurité de vos données à l'avenir**

Chapitre 3
Le rôle du Zero Trust dans la DLP moderne

Les principes Zero Trust sont extrêmement importants dans le domaine de la sécurité aujourd'hui, pour la DLP et d'autres technologies. Une stratégie Zero Trust part du principe que tous les utilisateurs et appareils, même ceux qui se trouvent à l'intérieur du réseau de l'organisation, peuvent être dangereux et ne sont pas dignes de confiance. Cela signifie que l'identification personnelle et l'appartenance à une organisation ne suffisent pas pour accéder automatiquement aux données et aux systèmes sensibles. Pour obtenir l'accès, il est nécessaire de passer par une authentification rigoureuse, une vérification des mesures de sécurité et une évaluation constante du contexte de risque. Le Zero Trust ne doit pas être un obstacle à la productivité, mais au contraire, il doit permettre une utilisation sécurisée des données sensibles tout en soutenant les pratiques métiers modernes. Il doit être capable de s'adapter automatiquement aux évolutions des conditions de risque tout en garantissant la sécurité.

Ce concept évalue continuellement la fiabilité de chaque utilisateur, appareil et environnement d'exploitation avant d'accorder l'accès à des données sensibles ou à certaines utilisations de ces données sensibles. Même lorsque l'accès a déjà été accordé à un collaborateur, il est important de l'évaluer avec soin en vérifiant son identité, en contrôlant son appareil et sa connexion réseau, en évaluant les risques liés aux applications

auxquelles il accède, et en surveillant son comportement afin de s'assurer qu'il *reste* digne de confiance. S'il commence à avoir un comportement suspect ou à manifester des signes de négligence, tels que le partage excessif de données, le système réagit en prenant des mesures pour limiter ses actions, par exemple en réduisant ses privilèges. Cette approche vise à assurer la protection des données sensibles en minimisant les risques de perte de données. Elle garantit également que seules les personnes dignes de confiance ont accès à ces données et sont autorisées à les partager avec d'autres personnes de confiance.

Le concept de Zero Trust a été élaboré pour établir un environnement sécurisé et contrôlé pour l'accès et le transfert des données, ce qui réduit le risque de violation des données et protège les données sensibles contre tout accès non autorisé. À cette fin, le Zero Trust met en place des contrôles d'accès rigoureux et effectue une surveillance et une vérification continues des actions des utilisateurs, des risques contextuels et du comportement. Dans le contexte de la prévention des pertes de données (DLP), l'adoption d'un modèle de sécurité Zero Trust permet de réduire les risques de violation des données, d'améliorer la précision des mesures de protection et d'optimiser les cycles de réponse aux incidents en tenant compte du contexte et des risques spécifiques à l'organisation. En permettant exclusivement un accès sécurisé et une utilisation appropriée des données sensibles par des utilisateurs autorisés, et en empêchant toute tentative malveillante, suspecte, négligente ou risquée d'accéder à ces données ou de les transférer, les organisations peuvent renforcer la protection de leurs actifs.

Les risques d'une sécurité dépassée

Les systèmes DLP ont été créés pour empêcher les informations sensibles de quitter une entreprise. Les versions traditionnelles se concentrent sur un nombre restreint de scénarios courants de perte des données. Leur objectif principal est d'identifier les données sensibles et de les maintenir au sein de l'organisation en adoptant une approche basée sur le périmètre, tout en mettant l'accent sur le contrôle du flux de données entrant et sortant du réseau de l'organisation.

En appliquant une approche dite de *confiance implicite*, la DLP traditionnelle se concentre sur la détection et la réponse aux violations de données préalablement définies. Cependant, cette approche ne prend pas en compte le contexte des utilisateurs, leurs motivations professionnelles, ni les risques associés à une action spécifique.

À titre d'exemple, un système DLP traditionnel peut effectuer une recherche de numéros de sécurité sociale et bloquer toute tentative d'envoi de ces numéros en dehors du périmètre de l'entreprise. Dans un autre scénario, il peut stopper systématiquement le téléchargement de données

sensibles vers une application SaaS sans faire de distinction entre une instance approuvée de cette application SaaS, telle que Microsoft Teams, et une instance personnelle de la même application. Cette approche, qui peut sembler sûre, est en fait assez rigide et ne permet pas de prendre en compte les utilisateurs, les appareils, les réseaux, les applications et les destinations qui pourraient révéler une activité approuvée. La confiance implicite est un frein à la communication facile et à la circulation des données qui sont nécessaires au développement d'une entreprise moderne.

ATTENTION

Étant donné qu'un système DLP traditionnel ne réévalue pas en permanence le contexte et les risques métiers, il ne peut pas prendre des décisions informées concernant la protection des données, ce qui peut entraîner des interruptions inutiles des activités de l'entreprise.

Avec des politiques peu contraignantes, l'approche de confiance implicite permet d'accéder aux données sensibles sans effectuer une vérification continue de l'identité et de la fiabilité de l'utilisateur ou de l'appareil. C'est problématique, puisque cela expose l'organisation à des vulnérabilités potentielles en ce qui concerne la manipulation indésirable de ses données sensibles. Une fois que ces données quittent le périmètre, elles échappent au contrôle de la sécurité de l'organisation.

Cette situation constitue un problème majeur à l'ère du cloud. Des données sensibles sont utilisées et partagées en dehors du périmètre de l'entreprise, même pour les fonctions internes les plus courantes. Par exemple, les applications et services cloud courants tels que Dropbox et Google Drive permettent aux employés d'accéder à des données sensibles, de les partager et de collaborer à l'intérieur et à l'extérieur de l'environnement de l'entreprise. Cependant, les systèmes DLP traditionnels qui reposent sur la confiance implicite risqueraient de perturber une collaboration légitime ou de laisser échapper négligemment des données vers l'extérieur, exposant ainsi l'organisation à des menaces potentielles.

La protection des données Zero Trust consiste à autoriser l'utilisation et le partage de données sensibles uniquement lorsque les conditions de sécurité sont constamment vérifiées. Grâce à elle, les données sensibles peuvent être échangées et partagées entre les utilisateurs, les appareils et stockées dans différents services cloud. Cette approche garantit que les conditions de sécurité sont constamment vérifiées, notamment l'authentification de l'utilisateur, la sécurité de l'appareil, du réseau et de l'application, ainsi que le suivi du comportement de l'utilisateur au fil du temps. La protection des données Zero Trust s'applique spécifiquement aux données sensibles et garantit que toutes les conditions de sécurité sont remplies à tout moment, ce qui permet de travailler de manière hybride, dans le cloud et dans des cas d'usage modernes de l'entreprise.

RAPPEL

Un système DLP moderne basé sur le cloud et s'appuyant sur les principes Zero Trust assure une surveillance et un contrôle des données à chaque point de connexion et d'accès souhaité par les utilisateurs de l'entreprise.

Il garantit également la sécurité des données stockées et transférées dans les référentiels d'applications cloud et les environnements sur site.

Les approches de sécurité traditionnelles qui reposent sur l'utilisation de multiples produits et une confiance implicite présentent un autre inconvénient majeur : elles sont hautement fragmentées. Elles n'appliquent qu'un seul contrôle de sécurité à la fois, sans intégrer l'ensemble des contrôles et sans partager les informations relatives aux risques. Les divers contrôles de sécurité sont donc séparés les uns des autres et ne sont pas intégrés au sein d'une plateforme de sécurité cohérente, créant ainsi des lacunes dans votre stratégie globale de sécurité. Pour protéger pleinement vos données, vous avez besoin de plusieurs contrôles de sécurité fonctionnant ensemble et partageant des informations entre eux.

L'approche Zero Trust adopte une perspective plus globale et dynamique en matière de protection des données. Elle tient compte du contexte de l'utilisateur, de l'appareil, du réseau et d'autres facteurs pertinents afin de prendre des décisions plus informées en matière de protection des données. Cette approche permet d'intégrer la DLP à d'autres contrôles de sécurité et outils de productivité, tout en assurant une surveillance et une adaptation constantes face à l'évolution des menaces, des risques et des conditions propres à l'entreprise.

Globalement, les organisations qui font implicitement confiance à la DLP supposent, à tort, que leurs utilisateurs sont dignes de confiance, qu'ils respectent les mesures de sécurité et qu'ils ne mettront jamais en péril des données sensibles. En fait, sans contexte de sécurité, une application restrictive des politiques DLP peut souvent entraîner une perturbation des processus métiers légitimes. En revanche, lorsque la DLP est basée sur des principes Zero Trust, elle assure une surveillance et un contrôle étroits sur la manière dont les données sont utilisées à tout moment, ce qui permet de prévenir de manière adaptative les violations de la politique de protection des données.

Un système DLP basé sur la confiance implicite protégerait un numéro de carte bancaire en permettant aux utilisateurs autorisés d'accéder aux données sensibles, tandis qu'il refuserait l'accès aux utilisateurs non autorisés. Cela suppose qu'il est possible de faire confiance aux utilisateurs autorisés pour manipuler les données de manière sécurisée et ne pas les utiliser de façon abusive.

Contrairement aux systèmes DLP traditionnels basés sur la confiance implicite, un système DLP basé sur les principes Zero Trust ne repose pas sur l'hypothèse d'une confiance aveugle envers les utilisateurs. Au contraire, il protège les données sensibles, telles que les numéros de cartes bancaires, en exigeant que tous les utilisateurs se soumettent à un processus d'authentification avant d'accéder à ces données, quel que soit leur niveau d'autorisation. Il peut s'agir d'une authentification multifacteur,

qui nécessite à la fois un mot de passe et un code à usage unique envoyé à un appareil mobile.

Le système évalue également en permanence les risques liés aux appareils, aux utilisateurs, aux données et aux applications. Il effectue des vérifications pour s'assurer que les appareils sont fiables et sécurisés, que les applications et leurs instances (qu'elles soient professionnelles ou personnelles) sont sécurisées et conformes, que le réseau est sécurisé et fiable, que les données sont partagées avec des destinations et des destinataires dignes de confiance, et que le comportement de l'utilisateur est conforme. Ces conditions sont vérifiées en permanence et le système adapte sa réponse/protection en conséquence. En outre, le système surveille et enregistre l'accès des utilisateurs aux données sensibles, en signalant aux administrateurs tout comportement suspect ou toute violation potentielle, et en formant les utilisateurs aux bonnes pratiques d'utilisation sécurisée des données en cas de non-respect des politiques de l'entreprise. Cette approche diminue le risque d'accès non autorisé aux données sensibles en vérifiant l'identité de chaque utilisateur avant de lui accorder l'accès. De plus, elle réduit progressivement les risques pour les données sensibles en éduquant les utilisateurs en temps réel.

Le contexte permet à votre DLP de dire oui à une activité métier importante

Le concept de Zero Trust permet aux systèmes de protection des données de prendre des décisions avisées concernant l'autorisation ou la restriction de certaines activités. Pour ce faire, il prend en compte plusieurs facteurs ou contextes, tels que l'identité de l'utilisateur, l'appareil utilisé, la fiabilité de l'application et le contexte des données concernées. (L'approche Zero Trust définit le contexte avec l'aide d'autres solutions, que j'aborde dans la section « La DLP ne doit pas être utilisée de façon isolée »). En prenant en compte tous ces contextes, l'application des principes Zero Trust permet d'évaluer de manière plus précise si une activité spécifique est bénéfique et essentielle pour l'entreprise, et si elle peut être approuvée. Cela permet de garantir la protection des données et de minimiser le risque de failles de sécurité ou d'autres menaces, tout en permettant à l'entreprise de continuer à fonctionner normalement.

La liste suivante définit les types de contexte utilisés dans l'approche Zero Trust :

- **Contexte de l'utilisateur :** c.-à-d. qui fait une action et qui est le destinataire d'une action. Ces informations permettent de déterminer si le comportement d'un utilisateur est approprié ou si quelque chose ne va pas. Prenons par exemple le cas d'un utilisateur qui transfère subitement une quantité de données bien supérieure à la normale, se

connecte à partir d'emplacements inhabituels ou adopte un comportement étrange par rapport à ses habitudes précédentes. Ces indicateurs peuvent signaler un comportement à risque ou malveillant. Il en va de même si un utilisateur accède à des données sensibles ou les utilise et/ou les envoie à des applications personnelles. En analysant l'identité et le comportement d'un utilisateur, il est possible d'ajuster les privilèges de manière à garantir la protection des données sensibles. Ainsi, seuls les utilisateurs autorisés peuvent y accéder, les partager avec des destinataires autorisés et les transférer vers des destinations sécurisées.

- **Contexte de l'appareil :** c.-à-d. l'appareil qui tente d'accéder à vos données. Vous devez vérifier si l'appareil est à usage personnel ou professionnel, s'il présente des mesures de sécurité adéquates et s'il est régulièrement mis à jour avec les correctifs nécessaires. Vous pouvez également tenir compte de facteurs environnants, tels que la fiabilité de l'emplacement à partir duquel l'appareil se connecte, dans l'évaluation de la sécurité. En prenant en compte tous ces éléments, il est possible de déterminer le niveau approprié de privilèges pour l'appareil en fonction du niveau de confiance et de risque associé. Même si un utilisateur est généralement fiable, son appareil peut néanmoins être compromis ou présenter un risque de sécurité. Le contexte de l'appareil est donc essentiel pour déterminer les privilèges à accorder.
- **Contexte de l'application :** c.-à-d. la réputation et la fiabilité de l'application utilisée pour accéder aux données ou les traiter. Ceci est important, car si une application a une mauvaise réputation ou n'est pas digne de confiance, elle peut présenter un risque pour la sécurité des données utilisées. Les systèmes de protection des données peuvent s'appuyer sur d'autres systèmes tels qu'un agent de sécurité d'accès au cloud (CASB) pour recueillir des informations sur les attributs de conformité et de risque de l'application. Ainsi, le système peut déterminer si l'application présente un risque, par exemple si elle enfreint le règlement général sur la protection des données (RGPD) en surexposant potentiellement des données sensibles.

  Un utilisateur peut avoir accès à plusieurs instances d'une application cloud, ce qui nécessite un contrôle plus précis des données sensibles afin d'éviter tout partage accidentel avec des comptes personnels. Les applications de communication collaborative telles que Slack et Microsoft Teams peuvent également présenter un risque si les canaux de ces applications incluent à la fois des utilisateurs internes et externes. Dans ce cas, le système doit être en mesure de les distinguer afin d'éviter toute fuite de données. Gardez tout cela à l'esprit pour vous assurer que les applications que vous utilisez sont réputées et dignes de confiance et pour protéger vos données contre les risques potentiels.
- **Contexte des données :** c.-à-d. le degré de sensibilité d'une donnée spécifique, son format, sa taille et d'autres facteurs. À quel endroit vos données sont utilisées et la légitimité de cette utilisation. Il est utile de

savoir quel type de données est consulté ou déplacé et si elles ont leur place là où elles sont utilisées. L'accès à des données sensibles ou leur transfert vers un emplacement non autorisé nécessite des mesures pour éviter leur fuite ou une violation. Le contexte des données est essentiel pour s'assurer que les données sont traitées de manière appropriée et qu'elles ne sont accessibles qu'aux utilisateurs autorisés, dans des lieux autorisés, en fonction de leur niveau de sensibilité. Il permet de déterminer si une activité est nécessaire à l'entreprise et si le risque en vaut la peine.

ATTENTION

La plupart des solutions DLP, et pas seulement les solutions DLP traditionnelles, posent problème pour la gestion de votre entreprise, car elles ne recueillent pas suffisamment d'informations sur votre activité et les risques auxquels elle est exposée. La plupart des solutions DLP forcent votre organisation à s'appuyer sur les équipes de réponse aux incidents pour prendre des décisions manuelles sur les actions à entreprendre. Cette approche est frustrante, inefficace et coûteuse.

Avec une approche Zero Trust, ces problèmes sont considérablement réduits, voire éliminés. Un système DLP moderne, basé sur les principes Zero Trust, tient compte de tous les risques associés aux utilisateurs, aux appareils, aux données, aux réseaux et aux applications. De cette manière, le système acquiert une meilleure compréhension des risques et peut prendre automatiquement les décisions appropriées pour protéger vos données, en se basant sur des politiques dynamiques de protection des données adaptées aux besoins spécifiques de votre entreprise. Le Zero Trust vous permet d'assurer la sécurité de vos données et le bon fonctionnement de votre entreprise.

La DLP ne doit pas être utilisée de façon isolée

Les contrôles de données sont présents à la fois dans les systèmes traditionnels et dans les nouvelles solutions DLP. La DLP est en fait conçue pour identifier les données sensibles et les protéger. Le problème de la plupart de ces contrôles de données réside dans le fait qu'ils manquent de contexte. La DLP doit faire partie d'une plateforme plus large, basée sur les principes Zero Trust, qui utilise tout le contexte disponible pour prendre des décisions avisées. La DLP nécessite la collaboration et l'intégration avec d'autres solutions afin de recueillir tous les éléments contextuels nécessaires, tels que le contexte de l'utilisateur, le contexte de l'appareil, le contexte de l'application et le contexte des données. C'est pourquoi un système basé sur les principes Zero Trust est conçu pour être intégré et se concentre sur les contrôles contextuels des données, plutôt que de faire aveuglément confiance à toute connexion. C'est une approche qui permet de s'adapter à l'évolution des risques et de protéger automatiquement vos données en adoptant la réponse la plus appropriée à chaque fois.

CONSEIL

Dans le contexte de la protection des données Zero Trust, il est important de privilégier des contrôles consolidés où chaque contrôle partage des informations et fonctionne de manière transparente en collaboration avec d'autres outils pour assurer la protection de vos données. Prenons l'exemple de Netskope Intelligent Security Service Edge (SSE) qui intègre directement les principes Zero Trust et permet le partage des informations et du contexte entre les différents contrôles, y compris la DLP qui joue un rôle central. Cette intégration facilite grandement et rend plus efficace la protection de vos données.

Netskope Intelligent SSE enrichit sa plateforme DLP très complète en y intégrant plusieurs autres solutions de sécurité. Parmi les plus importantes, on peut citer :

- **Passerelle web sécurisée (SWG) :** une SWG est une solution de sécurité qui agit comme un intermédiaire entre les utilisateurs et Internet, assurant des connexions web sécurisées et offrant une protection contre les menaces en ligne. Par l'intermédiaire d'une SWG, la solution DLP de Netskope s'assure que les données sensibles ne sont pas exposées à des fuites via un trafic web non fiable et potentiellement risqué, y compris le trafic chiffré. Elle détecte et surveille les données sensibles de l'entreprise et les protège contre les fuites et l'exposition sur toutes les connexions web, qu'il s'agisse de connexions depuis le domicile des télétravailleurs, les filiales ou les réseaux Wi-Fi publics.
- **CASB :** la solution DLP de Netskope, associée à un CASB, détecte, surveille et protège les données sensibles dans les applications SaaS (Software as a Service), l'IaaS (Infrastructure as a Service), les réseaux d'entreprise et les filiales, les services de messagerie électronique, ainsi que les appareils du personnel mobile et des collaborateurs. Ce service centralisé et hébergé dans le cloud met en œuvre des politiques de protection des données unifiées partout où des données sensibles sont stockées, utilisées ou transférées. Il couvre à la fois les données en mouvement et les données au repos. Il prend en charge une vaste gamme d'applications SaaS, couvrant des milliers d'entre elles, et dispose d'une connaissance approfondie des données transmises entre des instances d'applications personnelles (par exemple, entre les versions professionnelles et personnelles de OneDrive) ainsi que des applications considérées comme étant à risque. Il analyse des milliers de types de fichiers différents, ainsi que des messages et des communications asynchrones via les applications de collaboration et les services de messagerie électronique. Les politiques de protection des données, de conformité et de confidentialité des données sont appliquées de manière uniforme dans les services cloud publics et se synchronisent automatiquement dans l'ensemble de la plateforme DLP.
- **Gestion des mesures de sécurité SaaS (SSPM) et gestion des mesures de sécurité dans le cloud (CSPM) :** ces technologies

permettent de gérer la sécurité et la conformité des environnements SaaS et des services cloud publics, assurant ainsi une protection adéquate. Elles effectuent une surveillance et une évaluation continues du niveau de sécurité, identifient les risques ainsi que les mauvaises configurations, et fournissent des informations et des recommandations exploitables. Grâce à des capacités de correction automatisées, les problèmes identifiés peuvent être résolus en temps réel.

- **Logiciel de protection des appareils :** Netskope Endpoint DLP est une solution qui détecte, surveille et protège les données sensibles sur les appareils de vos collaborateurs La solution étant intégrée dans le client unique Netskope, il n'est pas nécessaire de déployer un agent distinct. Netskope Endpoint DLP optimise l'utilisation des ressources tout en offrant une gamme complète de fonctionnalités, telles que des classificateurs basés sur l'apprentissage automatique (ML), la reconnaissance optique des caractères (OCR), l'empreinte numérique des fichiers, la correspondance exacte des données (EDM) et bien d'autres fonctionnalités. En tirant parti de la solution DLP en mode cloud et des informations provenant de l'ensemble de la plateforme DLP, il est possible d'éviter l'analyse redondante des données provenant du cloud, ce qui se traduit par une expérience utilisateur fluide et des résultats plus efficaces en termes de protection des données.
- **Analyse du comportement des utilisateurs et des entités (UEBA) :** ce contrôle de sécurité évalue en permanence le comportement des utilisateurs afin d'identifier toute activité inhabituelle ou potentiellement risquée. Dans le passé, l'UEBA était souvent considéré comme un contrôle de sécurité indépendant, mais pour être réellement efficace, celui-ci doit être intégré à la DLP. En analysant les journaux des violations de la DLP et en signalant les comportements à risque pour une évaluation plus approfondie, l'UEBA peut fournir des informations pour des ajustements ultérieurs de la politique et contribuer à la sécurité de vos données.
- **Gestion des identités et des accès (IAM) :** l'IAM est la pratique qui consiste à gérer et à contrôler l'accès aux ressources sur la base de l'identité des utilisateurs. Elle intègre des technologies telles que l'authentification multifacteur, l'authentification unique et les listes de contrôle d'accès. Netskope s'intègre à de nombreux fournisseurs IAM pour garantir que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques et pour empêcher les accès non autorisés. L'IAM est un élément essentiel de la stratégie de sécurité Zero Trust de toute organisation, car elle contribue à protéger les ressources et à garantir le respect des politiques et des réglementations en matière de sécurité.
- **Protection du courrier électronique :** Netskope propose une solution DLP très complète pour les messageries électroniques telles que Microsoft 365 et Gmail, et pour les données en mouvement et au

repos. La solution protège les e-mails sensibles sortants en temps réel grâce à un proxy SMTP et à une plateforme webmail. Elle permet également de faire la distinction entre les données sensibles envoyées via un compte de messagerie personnel et celles envoyées via un compte professionnel ou des services de messagerie privés.

- **Accès Zero Trust au réseau (ZTNA) :** la solution Netskope de prévention des pertes de données (DLP), fournie via Netskope Private Access (NPA), une solution d'accès à distance, offre une protection contre la perte et l'exfiltration de données sur des ressources privées, que ce soit dans le datacenter ou dans des environnements de cloud public. Elle garantit la sécurité des données lors de l'accès via un navigateur à des applications privées, peu importe l'emplacement à partir duquel les utilisateurs se connectent.

En regroupant ces composants fondamentaux au sein d'une seule plateforme intégrée, la plateforme SSE de Netskope offre une solution de sécurité complète qui permet de protéger votre organisation contre une variété étendue de menaces.

Mettre en œuvre les principes Zero Trust avec la DLP

RAPPEL

L'objectif de la protection des données Zero Trust n'est pas d'empêcher les données sensibles de quitter l'entreprise. Elle vise également à permettre aux entreprises modernes de mettre en œuvre des cas d'usage tout en maintenant un équilibre entre sécurité et risques.

Cela implique une prise en charge des utilisateurs dispersés dans différents endroits et de favoriser la collaboration, tout en garantissant la sécurité de vos données. La protection des données Zero Trust permet de travailler de manière flexible depuis n'importe où, avec un accès aux ressources nécessaires et une collaboration sécurisée avec des membres de son équipe et des partenaires externes, sans craindre les fuites de données. En utilisant une solution unifiée comme Netskope SSE, vous pouvez protéger vos données et bénéficier de tous les avantages offerts par les flux de données d'entreprise modernes. Voici quelques exemples concrets de son fonctionnement :

- Imaginez-vous en train de travailler sur votre ordinateur portable, connecté au réseau de votre entreprise à l'aide de Netskope SSE. Vous accédez à certains documents commerciaux importants et commencez à travailler dessus. Mais vous essayez alors accidentellement d'enregistrer une copie des documents sur votre compte de stockage cloud personnel plutôt que sur l'instance de cette même application de stockage cloud autorisée par votre entreprise.

  Grâce à la DLP basée sur les principes Zero Trust, le système reconnaît que vous essayez d'envoyer des données sensibles vers une instance

d'application personnelle, et il empêche l'enregistrement de ces données. Au lieu de cela, le système affiche une notification de coaching pour l'utilisateur, une fenêtre contextuelle qui vous informe immédiatement de la violation et vous rappelle l'emplacement correct pour enregistrer les documents. Ainsi, vous pouvez travailler de n'importe où, tout en ayant accès à toutes les ressources dont vous avez besoin sans craindre d'envoyer accidentellement des données sensibles à un endroit où elles n'ont pas leur place. Les notifications de coaching permettent de sensibiliser les utilisateurs aux bonnes pratiques et aux politiques de l'entreprise, ce qui réduit progressivement le risque de perte de données et limite la nécessité d'une formation fastidieuse tout au long de l'année.

- Imaginons que vous collaboriez avec des partenaires externes sur un projet et que vous souhaitiez partager certains documents avec eux. Grâce à la DLP basée sur les principes Zero Trust, le système vérifie la réputation et la fiabilité de l'application que vous utilisez pour partager des documents, ainsi que votre identité et votre comportement, l'appareil utilisé et la destination de la transmission.
- Si vous utilisez une application de stockage cloud personnelle dont le niveau de sécurité est différent de celui de l'application de votre entreprise, le système pourra vous empêcher de partager les données via cette application. Il pourra vous suggérer d'utiliser une autre application ou d'envoyer les documents via un canal sécurisé. La DLP vérifiera également la destination de la transmission, par exemple si le destinataire est un utilisateur externe ou un collaborateur et si la destination est sûre. La DLP peut vous envoyer une notification vous demandant de confirmer le partage des données sensibles avec le destinataire externe et peut même vous demander de justifier votre action. Vous pouvez ainsi collaborer en toute confiance, en sachant que vos données sont protégées et que seuls les utilisateurs autorisés peuvent y accéder.

Approche Zero Trust adaptative

L'approche Zero Trust adaptative consiste à reconnaître que les choses changent avec le temps. Cela signifie que la protection des données Zero Trust doit évaluer en permanence le contexte de l'entreprise, les risques et le comportement des utilisateurs afin de garantir la sécurité des données.

Pour illustrer ce point, imaginez un videur dans une boîte de nuit. Un soir, alors qu'il se trouve à la porte, un groupe de personnes s'approche. Le videur vérifie leurs cartes d'identité et tout semble correct, il laisse donc entrer le groupe. Mais au fur et à mesure que la nuit avance, le videur commence à remarquer un comportement étrange chez l'un des membres du groupe. Peut-être agit-il de manière agressive ou essaie-t-il d'accéder à des zones du club où il n'est pas censé se rendre ? Grâce à l'approche Zero

Trust adaptative, notre videur reconnaît ce changement de comportement et prend des mesures pour protéger les autres personnes et le club. Il peut surveiller de plus près cette personne pour s'assurer qu'elle ne cause pas de problèmes, voire lui demander de quitter les lieux. De cette façon, vous pouvez assurer la sécurité des autres personnes et de votre club, même si le comportement d'une personne change.

Passons en revue ces situations courantes auxquelles votre entreprise pourrait être confrontée :

- **Le comportement de quelqu'un change.** Vous avez un collaborateur de confiance qui a toujours eu accès à certaines données sensibles de l'entreprise. Un jour, peut-être après une évaluation de ses performances, il commence à se comporter différemment. Il accède à et télécharge plus de données sensibles que d'habitude, ou se connecte à partir d'emplacements inhabituels. Avec l'approche Zero Trust adaptative, le système reconnaît ce changement de comportement et ajuste les privilèges du collaborateur en conséquence. Par exemple, le système peut restreindre son accès à des données spécifiques ou avertir l'équipe de sécurité pour une évaluation plus approfondie. De cette façon, vous pouvez protéger les données même si le comportement d'un collaborateur de confiance change.
- **La réputation et la fiabilité des applications changent.** Les applications évoluent au fil du temps ; non seulement leur fonctionnalité, mais aussi leur réputation, leurs mesures de sécurité et leur fiabilité peuvent changer. Par exemple, une application de stockage cloud qui était considérée comme sûre peut présenter une nouvelle vulnérabilité ou une mauvaise configuration qui affecte sa fiabilité. Avec l'approche Zero Trust adaptative, la solution évalue en permanence le niveau de risque de l'application et ajuste les privilèges si nécessaire. Vous pouvez ainsi protéger vos données même si la fiabilité d'une application change.
- **Des appareils sont compromis.** Les appareils peuvent devenir plus vulnérables ou même être compromis sans que l'utilisateur s'en rende compte. Par exemple, un ordinateur portable considéré comme sûr peut être infecté par un logiciel malveillant ou voir ses paramètres de sécurité modifiés à l'insu de l'utilisateur. Avec l'approche Zero Trust adaptative, le système évalue en permanence le niveau de sécurité de l'appareil et ajuste les privilèges si nécessaire. De cette façon, vous pouvez protéger vos données même si un appareil est compromis.
- **Changements dans le flux de données.** Le flux de données peut changer en raison des modifications apportées aux règles de conformité à différents niveaux. Par exemple, un flux de données peut être considéré comme acceptable, mais si la destination devient non conforme ou dangereuse, la réglementation peut quand même exiger que l'organisation protège le flux de données. C'est le cas du RGPD, qui

stipule que certaines données privées ne peuvent pas être autorisées à quitter l'UE à moins que cela soit approprié ou qu'un accord de transfert valide soit en place. Avec l'approche Zero Trust adaptative, le système évalue en permanence les risques et ajuste les privilèges en fonction des besoins. Vous pouvez ainsi protéger vos données même si les règles changent.

- **Le rôle ou le statut d'un utilisateur change.** Les utilisateurs qui donnent leur préavis peuvent encore avoir accès à des données sensibles pendant la période précédant leur départ. Avec l'approche Zero Trust adaptative, le système évalue en permanence les risques encourus et ajuste les privilèges si nécessaire. Par exemple, le système peut limiter l'accès d'un utilisateur à des données spécifiques ou alerter l'équipe chargée de la sécurité lorsqu'une action nécessite une évaluation plus approfondie.

CONSEIL

L'approche Zero Trust adaptative évalue l'utilisation des données sous autant d'angles que possible afin d'ajuster les privilèges, de protéger les données sensibles et la réputation de l'entreprise, tout en favorisant l'activité commerciale.

Cette approche permet de renforcer la protection tout en améliorant la productivité des données et des personnes. Elle met en œuvre une politique de protection des données dynamique et adaptative, en évaluant en permanence les risques et en ajustant les privilèges en fonction des besoins. Cela représente un changement significatif par rapport à l'approche habituelle des systèmes DLP, qu'ils soient traditionnels ou récents, qui se basent sur une confiance implicite unique, entraînant ainsi de nombreux faux positifs et une certaine lassitude en matière de gestion des incidents. Avec une approche aussi lourde, l'équipe chargée de répondre aux incidents se retrouve dans l'obligation d'évaluer manuellement chaque incident pour déterminer s'il s'agit d'une véritable violation, puis de contacter l'utilisateur responsable, souvent longtemps après que l'action initiale a été effectuée et oubliée par ce dernier. L'équipe doit alors déchiffrer l'ensemble du flux de données, un processus long et fastidieux. L'approche Zero Trust adaptative fournit un modèle de protection continue, ce qui facilite grandement la sécurité des données et le bon fonctionnement de l'entreprise.

Protection des données Zero Trust et adaptative par Netskope

Le déploiement par Netskope de la protection adaptative Zero Trust des données repose sur le contexte. En analysant le trafic entre les utilisateurs, les appareils, les applications, les réseaux et les destinations, Netskope vous offre une meilleure visibilité sur les activités au sein de votre organisation. Le système peut ainsi exercer un contrôle précis sur l'accès aux données, ce qui vous permet de protéger vos données sensibles sans entraver les activités de votre entreprise.

Imaginons par exemple qu'un utilisateur tente d'accéder à des données sensibles de l'entreprise à partir d'un appareil personnel. Avec Netskope, le processus commence par la détection précise des données sensibles. En outre, en tenant compte de divers facteurs contextuels, la réponse à l'incident devient plus précise et plus efficace, ce qui réduit la nécessité d'un triage manuel et la charge de travail des équipes chargées de la sécurité. Le système évalue le niveau de sécurité de l'appareil, l'identité de l'utilisateur et son comportement pour déterminer si l'accès doit être accordé.

Parmi les autres facteurs pris en compte, citons le type de connexion et l'emplacement du réseau, les vulnérabilités potentielles, les informations disponibles sur les menaces, etc. Les risques liés à une application et sa réputation sont pris en compte par le Netskope Cloud Confidence Index (CCI), une base de données de près de 60 000 applications (en constante évolution) évaluées par Netskope selon une cinquantaine de critères basés sur le risque. Ces critères mesurent l'aptitude d'une application à être utilisée en entreprise, en tenant compte de sa sécurité, de son auditabilité et de sa capacité à assurer la continuité de l'activité de l'entreprise.

Si l'appareil est jugé risqué ou si le comportement de l'utilisateur est considéré inhabituel, l'accès sera restreint ou l'équipe chargée de la sécurité sera avertie pour une évaluation plus approfondie. Si l'appareil est sécurisé et que le comportement de l'utilisateur est normal, l'accès sera accordé.

CONSEIL

La protection des données par Netskope repose sur sa solution SSE, qui fait partie intégrante de la plateforme SASE (Secure Access Service Edge) globale de Netskope. Cette solution de sécurité convergente et native cloud rassemble les technologies de sécurité essentielles que j'ai décrites précédemment en une plateforme unique et intégrée. Ainsi, Netskope simplifie la gestion de votre sécurité à partir d'une solution unique. Netskope SSE est une solution native cloud, ce qui signifie qu'elle peut évoluer rapidement et efficacement pour répondre aux besoins de votre organisation. Elle est également conçue pour être très flexible, afin que vous puissiez la personnaliser pour répondre à vos besoins spécifiques en matière de sécurité.

De par sa conception, Netskope SSE part du principe que la sécurité ne se résume pas à l'application d'une politique. Il est également important de former les employés et de les encourager à manipuler les données en toute sécurité. C'est pourquoi la solution préserve la capacité de l'utilisateur à prendre des décisions tout en assurant la sécurité de vos données. Par exemple, en cas de violation, Netskope SSE peut orienter les employés vers une formation sur la manière de traiter les données sensibles, poser des questions pour évaluer le contexte de manière plus approfondie, ou fournir des conseils et de bonnes pratiques pour travailler à domicile en toute sécurité. En adoptant une approche globale pour la protection des données, Netskope peut vous aider à créer une culture de la sécurité au sein de votre organisation.

DANS CE CHAPITRE

- **Comparer des solutions DLP modernes et traditionnelles**
- **La sécurité partout où vous accédez à des données**
- **Utiliser des politiques et des contrôles d'accès unifiés**
- **Évaluer les avantages et les facteurs de différenciation de la DLP fournie par Netskope**

Chapitre 4
Pourquoi utiliser Netskope pour une DLP moderne ?

Les responsables de la sécurité des systèmes d'information (RSSI) et les équipes en charge de la sécurité de l'information se trouvent souvent face à un choix difficile : privilégier des solutions de prévention des pertes de données (DLP) avancées, mais complexes et coûteuses, ou opter pour des solutions cloud faciles à déployer, mais susceptibles de ne pas offrir la profondeur et l'étendue nécessaires à leurs besoins ? Une fois que vous aurez parcouru ce chapitre et découvert les principaux avantages de toutes les solutions DLP en mode cloud, vous serez en mesure de répondre :

- **Elles peuvent fournir une couverture complète.** Une solution DLP en mode cloud peut assurer la protection de vos données, peu importe leur lieu de stockage, leur mode de transfert ou les moyens d'accès qui y sont associés.
- **Elles peuvent fournir une couverture pour les environnements cloud.** Applications SaaS, services cloud publics pour l'IaaS et accès au web, quel que soit l'endroit d'où vos utilisateurs se connectent dans l'entreprise hybride moderne.
- **Elles éliminent la nécessité de mettre en place une infrastructure supplémentaire, car elles peuvent être déployées rapidement et facilement en tant que services cloud.**

- **Elles protègent vos données sensibles sans peser sur votre réseau et vos ressources.** Un système DLP en mode cloud peut offrir une capacité maximale pour prendre en charge tous les algorithmes d'analyse et de détection de données dont vous avez besoin.
- **Elles sont plus faciles à intégrer à un large éventail d'outils de sécurité.**
- **Elles offrent une meilleure visibilité des données transférées et stockées en dehors des locaux de l'entreprise.**
- **Elles sont plus faciles à maintenir et à mettre à jour en temps réel, et offrent la possibilité d'évoluer plus rapidement et plus facilement qu'avec les anciens modèles déployés dans les locaux de l'entreprise.**

Après avoir lu ce chapitre, vous aurez acquis une compréhension approfondie de la manière dont ces avantages peuvent s'appliquer à votre organisation. Vous serez ainsi bien préparé pour prendre une décision informée quant à la solution de DLP en mode cloud qui convient le mieux à votre entreprise. Tout au long du processus, nous vous fournirons des informations détaillées sur les caractéristiques distinctives de la plateforme Netskope.

Différencier les différentes options disponibles en matière de DLP en mode cloud

Les solutions DLP modernes doivent être hébergées dans le cloud. Il existe deux types de solutions dans ce domaine. La DLP native cloud est généralement intégrée dans les plateformes d'infrastructure en mode service (IaaS) et les applications logicielles en mode service (SaaS) des fournisseurs de services cloud. Les solutions DLP cloud font généralement partie d'un service ou d'un produit de sécurité comme une passerelle web sécurisée (SWG), un pare-feu de nouvelle génération (NGFW) ou un agent de sécurité d'accès au cloud (CASB).

Type 1 : la DLP Netskope comparée à des solutions ponctuelles cloud natives

La solution DLP de Netskope offre un certain nombre d'avantages par rapport à des solutions ponctuelles natives cloud plus limitées. L'un des principaux avantages de cette solution est sa large couverture grâce à un moteur de stratégie DLP professionnel unique, assurant ainsi la protection des données sensibles dans divers formats, canaux de communication et environnements : applications SaaS, services IaaS, applications privées, services de messagerie, partage de fichiers et transactions web, peu importe l'emplacement de vos utilisateurs. La solution DLP de Netskope inclut également une protection des appareils, ce qui est important pour

s'assurer que toutes vos données sensibles sont protégées, même sur des dispositifs situés dans des lieux distants qui peuvent ou non être connectés au cloud par le biais d'un réseau spécifique. Le moteur de stratégie DLP unique réduit la complexité et simplifie grandement la gestion en éliminant la nécessité de gérer des règles de stratégie DLP distinctes pour chaque canal et service cloud.

La solution DLP de Netskope se distingue également par sa précision de détection supérieure. Grâce à une analyse complète de tous les types de fichiers et formats de données, l'utilisation d'une variété d'algorithmes de détection de données et de l'apprentissage automatique pour comprendre différentes informations et documents, ainsi que leur contexte spécifique, cette solution DLP est capable d'identifier et de classer précisément les données sensibles, même si ces données sont stockées et transférées dans des structures, langues ou formats différents, ou intégrées dans des images. Cette capacité est cruciale, car elle garantit qu'aucune donnée sensible n'est accidentellement divulguée ou exposée, ce qui pourrait avoir des conséquences graves pour une organisation. De plus, cela permet au système de générer des événements réels liés à la sécurité des données plutôt que de produire des faux positifs.

Enfin, la solution DLP de Netskope intègre un contexte Zero Trust, ce qui signifie qu'elle est conçue pour fonctionner dans un puissant cadre de sécurité Zero Trust. Cette fonctionnalité est essentielle, car elle garantit un contrôle et une surveillance rigoureux de tous les accès aux données sensibles, dans le contexte approprié en termes de risques. Ainsi, le risque d'accès non autorisé, de surexposition ou de fuites de données indésirables est considérablement réduit.

Aujourd'hui, de nombreux fournisseurs de services cloud (CSP) et vendeurs de SaaS proposent des capacités natives DLP dans leurs plateformes. Les organisations qui adoptent une stratégie « cloud first » ou qui débutent leur parcours de protection des données ont souvent recours à ces solutions cloud facilement accessibles. Bien qu'elles soient conçues pour répondre à des cas d'usage spécifiques de protection des données dans le cloud, ces solutions peuvent présenter une couverture limitée et ne pas être aussi exhaustives que les solutions DLP traditionnelles.

ATTENTION

Certaines entreprises optent initialement pour des solutions DLP natives cloud, car elles peuvent être rapides et faciles à mettre en œuvre. Cependant, il est crucial d'adopter ces solutions avec une vision claire, en sachant qu'elles pourraient ne pas suffire à répondre à tous vos besoins en matière de protection des données. Dans certains cas, les organisations peuvent se retrouver contraintes d'adopter plusieurs solutions DLP déconnectées et cloisonnées pour couvrir d'autres cas d'usage, ce qui peut entraîner une fragmentation de la stratégie de protection des données et une efficacité potentielle réduite.

Type 2 : toutes les solutions DLP en mode cloud ne se valent pas

Lorsqu'il s'agit de choisir une solution DLP cloud, il est important de prendre en compte le fait que de nombreuses solutions récentes sur le marché présentent des lacunes significatives :

- Elles peuvent offrir une couverture étendue, mais ne disposent pas de l'envergure technologique et des fonctionnalités nécessaires pour protéger les données sensibles de votre organisation de manière efficace et précise dans tous les cas d'usage modernes.
- Elles peuvent proposer des méthodologies et fonctionnalités innovantes pour certains cas d'usage et formats de données spécifiques, sans pourtant offrir une couverture suffisante pour protéger de manière exhaustive les données sensibles de votre organisation.

ATTENTION

Bien que certaines solutions DLP cloud plus récentes puissent bénéficier d'une bonne stratégie marketing, elles ne sont pas aussi sophistiquées et avancées que les solutions DLP traditionnelles qu'elles prétendent remplacer.

Il est essentiel de mener des recherches approfondies et de comparer les différentes solutions DLP afin de choisir celle qui répondra efficacement aux besoins de votre organisation. Lors de cette évaluation, prenez en compte des facteurs tels que la maturité et la sophistication des capacités de détection des données (par exemple, combien de types de fichiers sont analysés et le nombre d'identificateurs de données utilisés, y compris les types de données spécifiques à différents pays), la couverture des différents canaux, la capacité d'adaptation aux risques et aux environnements en constante évolution, ainsi que le niveau d'intégration et de personnalisation offert par la solution.

Si vous envisagez d'utiliser une solution DLP cloud, vous vous demandez peut-être quel type de solution convient le mieux à vos besoins spécifiques. Examinons plus en détail les éléments à prendre en compte :

- **Étendue de la couverture :** les solutions DLP intégrées sont généralement incluses dans une solution SWG, CASB ou NGFW, et font souvent partie d'une solution d'accès réseau Zero Trust (ZTNA). Ces solutions sont fournies via le cloud et typiquement intégrées dans un service de sécurité réseau. Ces solutions présentent des limitations, telles que l'absence de protection des données pour les e-mails sortants, les appareils et un large éventail d'applications SaaS, y compris leurs instances spécifiques (par exemple, les comptes d'entreprise par rapport aux comptes personnels).
- **Limites des solutions :** il convient de noter que ces solutions peuvent ne pas couvrir tous les cas d'usage modernes et traditionnels, tels que

la collaboration cloud avec des utilisateurs externes, les transferts de données via des adresses e-mail personnelles ou des brouillons de courrier, les transferts de fichiers via des clés USB, les captures d'écran et les photos de documents sensibles, les nouveaux modèles de conformité, les données dans des langues et formats étrangers, etc. De plus, leurs capacités de détection peuvent être moins avancées. En outre, leurs capacités en matière d'apprentissage automatique et d'IA ne sont pas toujours suffisantes.

- **Précision de la détection des données sensibles :** de nombreuses solutions DLP cloud récentes ne parviennent pas à détecter de manière précise et granulaire les données sensibles. Elles se limitent souvent à l'analyse d'un nombre restreint de types de fichiers et ne disposent pas de la gamme complète d'identificateurs de données dont bénéficient les solutions plus avancées. Bien que ces solutions puissent attirer l'attention en se concentrant sur une ou deux fonctionnalités tape-à-l'œil, elles ne parviennent pas à assurer une protection complète des données.

  En revanche, une solution avancée proposera des milliers d'identificateurs de données prédéfinis, couvrant un large éventail d'informations personnelles identifiables (passeports, comptes bancaires, informations bancaires internationales, cartes d'identité nationale, données financières, données médicales, données biométriques, informations spécifiques à un secteur), ainsi que des langues localisées et des identifiants personnalisables. Elle offrira également une vaste sélection de profils de politiques prédéfinis pour répondre aux différents cas d'usage et aux exigences de conformité, tels que le règlement général sur la protection des données (RGPD), la norme de sécurité des données de l'industrie des cartes de paiement (PCI-DSS), la loi Informatique et Liberté, et le code de la santé publique, pour n'en citer que quelques-uns.

- **Intégration dans une plateforme :** une solution DLP cloud efficace doit être étroitement intégrée à une plateforme de sécurité globale afin de protéger efficacement les données sensibles dans tous les contextes de risque pertinents, qu'il s'agisse d'utilisateurs, d'appareils, de réseaux, d'applications, de comportements ou de destinations. Une solution DLP bien intégrée tire parti des informations provenant d'autres points de contrôle tels que l'analyse comportementale des utilisateurs, les passerelles web sécurisées de nouvelle génération, les agents de sécurité d'accès au cloud (CASB), l'accès Zero Trust au réseau (ZTNA) et la gestion des mesures de sécurité pour comprendre de manière exhaustive la situation d'une organisation et les risques associés à chaque interaction avec des données sensibles. Cela implique de connaître les instances spécifiques des applications SaaS et des appareils utilisés, de faire la distinction entre les identités des utilisateurs des comptes de messagerie personnels et professionnels, les destinataires du partage des données, et bien plus encore. Ce niveau d'intégration permet une

approche plus précise et granulaire de la détection et de la protection des données sensibles.

CONSEIL

Toutes les solutions de protection des données ne se valent pas, et nombre d'entre elles ne sont pas suffisamment avancées et sophistiquées pour remplacer efficacement les solutions traditionnelles. Certains fournisseurs peuvent proposer une solution DLP en complément de leurs formules de base, mais sans l'étendue et la profondeur nécessaires, ces solutions risquent de ne pas offrir le niveau de protection dont les organisations ont besoin. Toute solution envisagée doit être testée pour s'assurer qu'elle prend en charge tous les types et volumes de données nécessaires aujourd'hui et qu'elle couvre tous les points de sortie des données sur site et dans le cloud sans compromis.

Évaluez soigneusement les capacités des différentes solutions DLP et choisissez celle qui répondra aux besoins de votre organisation, aujourd'hui et demain. Pour réussir dans cette démarche, il est essentiel de s'appuyer sur un ensemble de fonctionnalités avancées fournies par un spécialiste du domaine. Se fier uniquement aux principes de base peut entraîner des imprécisions, une détection partielle et un grand nombre de faux positifs.

Grâce à une décennie d'innovation constante et à un engagement sans faille envers la protection des données, Netskope s'est imposée comme un leader du secteur par rapport à d'autres fournisseurs de services SASE (Secure Access Service Edge) et SSE (Security Service Edge). Dans les prochaines sections, nous examinerons de près les caractéristiques et les capacités qui font la différence de la solution DLP de Netskope.

Comment la solution DLP de Netskope assure votre sécurité

La solution DLP de Netskope offre une protection complète et intégrée dans le cloud pour vos données, couvrant tous les canaux essentiels tels que les infrastructures cloud, les réseaux, les e-mails, les appareils et les utilisateurs, où qu'ils se trouvent. Cette solution a été spécialement conçue pour prendre en compte les risques et le contexte, garantissant ainsi la sécurité de vos données, quel que soit leur emplacement.

La solution DLP de Netskope est *entièrement intégrée* à la plateforme Netskope SSE, comme décrit dans le chapitre 3, et est fournie dans le cadre d'une solution SASE complète. De ce fait, vous bénéficiez d'une plateforme de sécurité cloud intégrée et native qui élimine les zones d'ombre, garantit la cohérence, améliore les performances, tout en réduisant les coûts et la complexité.

La solution DLP de Netskope offre une couverture complète de tous les canaux et transferts de données, comme illustré dans la figure 4-1,

garantissant ainsi la protection constante de vos informations sensibles. Elle couvre :

- près de 60 000 applications SaaS (les nouvelles applications étant classées de manière dynamique), et chaque instance de ces applications ;
- tous les principaux fournisseurs d'IaaS, y compris Amazon Web Services (AWS), Google cloud et Microsoft Azure ;
- les applications privées dans le datacenter ou hébergées dans le cloud public ;
- vos réseaux d'entreprise et vos filiales ;
- votre personnel nomade ;
- tous les services de messagerie, sur site et dans le cloud, y compris les plateformes webmail ; et
- tous les appareils de vos employés, sur site et hors site.

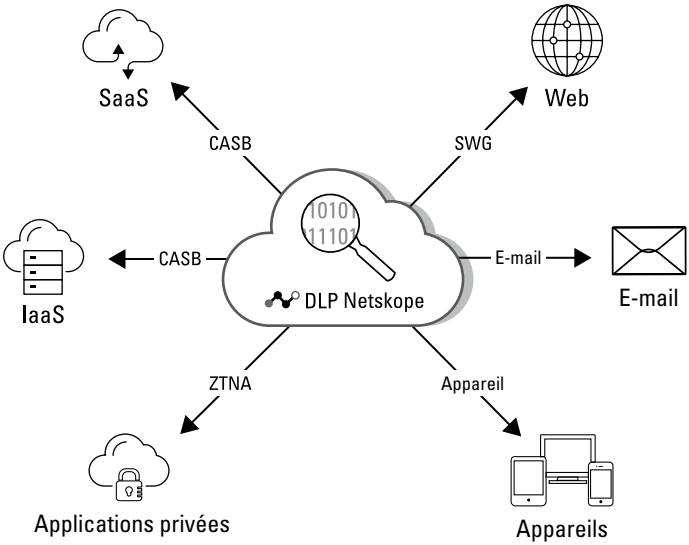

FIGURE 4-1 : La solution DLP de Netskope couvre vos données, où qu'elles se trouvent.

Principaux facteurs de différenciation

Il existe un mythe selon lequel les solutions DLP traditionnelles manquent de précision, mais en réalité, le problème le plus préoccupant est celui des faux positifs, qui nécessite une plus grande précision pour être résolu. Nous abordons cette question plus en détail dans le chapitre 2, où nous présentons et expliquons également les éléments clés qui peuvent aider les

systèmes DLP à atteindre une plus grande précision. Dans cette section, nous décrivons comment Netskope a transformé ces éléments clés en facteurs de différenciation, offrant ainsi une solution DLP moderne qui peut être personnalisée et automatisée pour répondre aux besoins spécifiques de votre entreprise.

Couverture complète de tous les canaux essentiels avec des stratégies unifiées

La protection et le suivi des données sensibles qui circulent en dehors des locaux traditionnels de l'entreprise deviennent de plus en plus complexes, avec un risque accru d'exposition intentionnelle ou accidentelle. La solution DLP cloud de Netskope est conçue pour détecter, surveiller et protéger les données sensibles en mouvement, au repos et en cours d'utilisation dans l'ensemble de l'écosystème de l'entreprise. Cela inclut les applications SaaS, les services de cloud public (IaaS), les réseaux d'entreprise et les filiales, le personnel en déplacement, les services de messagerie électronique et les appareils des employés.

Elle propose des stratégies de protection des données unifiées pour tous les emplacements où les données sont stockées, utilisées ou transférées, grâce à un service cloud centralisé.

Une seule console, dotée d'un contrôle d'accès basé sur les rôles, permet aux professionnels de gérer les configurations des stratégies, la surveillance, les rapports et la réponse aux incidents pour tous les canaux, le tout depuis un seul écran.

Détection et protection supérieures des données sensibles

Les identificateurs de données jouent un rôle crucial pour aider une solution DLP à identifier les données sensibles en fonction de différentes caractéristiques telles que des mots clés descriptifs, des expressions régulières, le nombre de chiffres, les caractères spéciaux, des modèles, l'analyse de proximité, etc. Lorsque vous recherchez une solution DLP, il est important de vérifier qu'elle dispose des capacités d'identification nécessaires pour couvrir tous vos cas d'usage actuels et futurs. Une bonne solution DLP doit être en mesure de fournir plusieurs milliers d'identifiants prédéfinis pour rechercher et identifier avec précision la plus grande variété et les moindres variations de données sensibles. Cela est particulièrement important pour les entreprises internationales qui ont besoin d'identifiants pour plusieurs pays. Netskope propose toutes ces fonctionnalités en utilisant des techniques d'apprentissage automatique et offre la possibilité de personnaliser précisément les identifiants et les modèles de stratégie, garantissant ainsi une détection précise et complète des données sensibles.

CONSEIL

Ne vous limitez pas aux seuls identifiants de données dont vous avez besoin actuellement. Il vous faut une solution prête pour l'avenir et capable de prendre en charge de nouveaux types de données, applications et réglementations qui pourraient émerger. Recherchez une solution qui propose des milliers d'identifiants de données prédéfinis ainsi que des modèles de stratégies conformes à des réglementations telles que le RGPD et la loi Informatique et Liberté. Il est également important d'avoir la possibilité de créer et de modifier des identifiants de données personnalisés pour répondre à vos besoins spécifiques.

Il existe une multitude de types de fichiers différents susceptibles de contenir des informations sensibles, tels que les fichiers compressés (ZIP, RAR, ISO, etc.), les présentations, les e-mails, les images (BMP, JPG, PNG, etc.), les feuilles de calcul, les fichiers de conception assistée par ordinateur (CAO), les messages sur les réseaux sociaux, les formulaires en ligne, les messages de conversation instantanée, ainsi que diverses pièces jointes et graphiques. La gestion de tous ces types de données peut être complexe, c'est pourquoi il est important de choisir une solution DLP capable de les gérer tous de manière efficace.

L'échelle de la correspondance exacte des données (EDM) est un aspect essentiel à considérer, surtout si vous êtes une grande entreprise – ou si vous prévoyez de le devenir un jour. La solution DLP doit pouvoir traiter facilement des millions, voire des milliards d'enregistrements. Les solutions DLP cloud modernes, telles que celle de Netskope, peuvent tirer parti du cloud pour effectuer des analyses d'empreintes de données à grande échelle, même sur les appareils, sans ralentir d'autres processus essentiels. De cette manière, l'ensemble des données personnelles des employés, des clients et des partenaires, et de bien d'autres acteurs, seront entièrement protégées.

PATRON, RÉDUISONS LA SURFACE D'ATTAQUE

CONSEIL

Pour protéger efficacement leurs données sensibles contre les cybermenaces, les organisations doivent combler leurs lacunes en matière de protection. La *surface d'attaque* fait référence au nombre total de vulnérabilités ou de points d'entrée potentiels que les pirates informatiques peuvent exploiter, ainsi que ceux que les initiés peuvent utiliser intentionnellement ou malicieusement. En réduisant la surface d'attaque, il devient plus difficile pour les pirates de découvrir et d'exploiter les faiblesses. En comblant les lacunes existantes dans la protection, le risque d'une attaque réussie et d'une exposition accidentelle de l'organisation est

suite

suite

considérablement réduit. Il est essentiel de s'assurer que l'ensemble des appareils, applications et réseaux sont correctement sécurisés afin d'éliminer toute vulnérabilité pouvant faciliter l'exposition aux risques.

Afin d'assurer une protection renforcée de vos données sensibles, il est important de rechercher dans votre solution DLP des capacités de détection avancées telles que la reconnaissance optique de caractères (OCR), l'intelligence artificielle (IA), l'apprentissage automatique, les empreintes de fichiers et les stratégies Zero Trust. Toutes ces fonctionnalités sont incluses dans la solution DLP de Netskope, comme nous l'expliquons plus en détail dans le chapitre 2.

La solution DLP de Netskope est capable d'identifier précisément les données sensibles, même si elles sont stockées dans des formats modernes non structurés tels que des images (captures d'écran et photos) ou dans différentes langues. Grâce à ses classificateurs d'apprentissage automatique sophistiqués, la solution peut reconnaître des informations sensibles dans des images telles que des permis de conduire, des cartes bancaires, des pièces d'identité, des contrats, des brevets, des documents de fusion et d'acquisition, et des chèques, même si ces images sont floues, déformées ou endommagées. Elle assure une protection proactive des informations sensibles, vous permettant de lui faire confiance pour garantir la sécurité de vos données dans l'environnement en constante évolution du cloud. De plus, elle allège la charge de travail de vos équipes chargées de la sécurité, car la solution identifie et protège automatiquement les données sensibles.

La solution DLP de Netskope propose une gamme d'outils de classification avancés basés sur l'apprentissage automatique, qui comprennent des milliers d'identificateurs de données. Elle est capable d'analyser plus de 1 600 types de fichiers différents en utilisant des politiques de détection contextuelles, une correspondance exacte des données hautement évolutive, une empreinte numérique des documents structurés et non structurés, une classification précise des images basée sur l'apprentissage automatique, une reconnaissance optique avancée des caractères (OCR), ainsi que des classificateurs de données basés sur l'intelligence artificielle et l'apprentissage automatique pour la découverte et l'identification des données.

Protection des données en fonction du contexte et des risques

La protection efficace des données repose sur le contexte. En surveillant le trafic entre les utilisateurs et les applications, il est possible d'exercer un contrôle précis et de permettre ou d'empêcher l'utilisation risquée de

données sensibles en fonction de plusieurs facteurs tels que l'identité de l'utilisateur, son intention et le contexte de son action. Cette approche centrée sur les données est essentielle pour gérer les risques dans les entreprises modernes et hybrides.

Avec la solution DLP de Netskope, la lassitude liée à la réponse aux incidents et les interruptions d'activité font partie du passé. En effet, cette solution va au-delà de l'approche statique de la découverte des informations sensibles et de la réponse à des politiques de violation prédéfinies. Elle tient compte du contexte organisationnel et des risques de sécurité pour mettre en place de manière dynamique la protection appropriée en fonction des conditions changeantes.

La solution DLP de Netskope est intégrée de manière native à la solution complète Netskope Security Service Edge (SSE). Cette plateforme de sécurité cloud native entièrement intégrée consolide les technologies de sécurité telles que les services SWG, CASB et UEBA sur une plateforme cloud native unifiée et intégrée. Cette approche permet d'éliminer les angles morts en matière de sécurité, d'assurer la cohérence des stratégies et de réduire considérablement les coûts et la complexité. La plateforme est continuellement alimentée en informations sur le comportement des utilisateurs, leur géolocalisation, les mesures de sécurité, les risques liés aux appareils, les risques et la réputation des applications, ainsi que les instances d'applications personnelles, etc. Ces informations permettent à la solution DLP d'adapter sa réponse aux véritables incidents de sécurité des données, réduisant ainsi les faux positifs, la nécessité de trier les incidents et les interruptions d'activité.

En optant pour une solution unique de protection des données SASE basée sur les principes Zero Trust et des contrôles avancés de protection des données, vous pouvez améliorer la visibilité et réduire les risques sur tous les vecteurs clés. La plateforme intégrée offre aussi une simplification de la classification des données, de la définition des stratégies et de la gestion des incidents grâce à l'utilisation de l'apprentissage automatique, de rapports détaillés et d'analyses avancées. De plus, grâce à des stratégies flexibles et contextuelles, ainsi qu'à un agent léger, vous pouvez améliorer l'agilité de l'utilisateur final et réduire les frictions.

RAPPEL

Pour garantir le succès de votre programme de protection des données, il est essentiel de former vos employés et de promouvoir des pratiques sûres dans le traitement des données. La solution DLP de Netskope propose des programmes d'accompagnement et de sensibilisation des utilisateurs en temps réel. La solution s'intègre également aux principaux systèmes de gestion de la formation et offre un portail personnalisable dédié aux utilisateurs finaux, leur permettant d'accéder à des ressources de formation en libre-service sur la protection des données.

Travailler plus intelligemment avec la DLP

La solution DLP de Netskope est entièrement basée sur le cloud, ce qui signifie qu'elle ne nécessite pas de composants sur site. Elle offre une protection en continu et actualisée automatiquement, éliminant ainsi la nécessité de procéder à des mises à jour logicielles manuelles, comme c'est le cas avec les solutions DLP traditionnelles.

Grâce à des politiques de protection des données unifiées, à une console unique et à un contrôle d'accès basé sur les rôles (RBAC), la gestion des configurations des politiques, la surveillance, la création de rapports et la réponse aux incidents sont désormais simples et intuitives.

Auparavant, les entreprises devaient développer des stratégies distinctes pour chaque canal de communication, comme le web, le courrier électronique et chaque application individuelle. Cela nécessitait des ressources considérables et prenait beaucoup de temps. Avec la solution DLP de Netskope, vous disposez d'un service cloud unifié et centralisé qui vous permet de définir une stratégie globale pour votre entreprise. Cette stratégie est ensuite automatiquement synchronisée sur tous les canaux. Ainsi, vous pouvez définir votre stratégie une seule fois et vous n'avez pas besoin de l'ajuster continuellement pour la reproduire et la maintenir dans différents environnements.

CONSEIL

Les solutions DLP traditionnelles exigeaient un nombre important d'administrateurs système pour configurer et gérer les politiques. Cependant, compte tenu de la pénurie actuelle de talents, il est essentiel de choisir une solution qui soit plus facile à gérer et à administrer.

Une interface utilisateur centralisée et une console de gestion unifiée sont également essentielles pour apporter une réponse efficace aux incidents. Il peut être frustrant et chronophage d'avoir des consoles distinctes pour les outils sur site et les outils basés sur le cloud. Malheureusement, certaines nouvelles solutions DLP utilisent toujours une approche multiconsoles, ce qui peut compliquer encore les choses. Avec la solution DLP de Netskope, toutes les violations sont regroupées en un seul endroit, la détection des données sensibles et la réponse aux incidents sont cohérentes et en temps réel, ce qui vous permet de réagir rapidement et efficacement aux menaces potentielles.

CONSEIL

Une interface utilisateur centralisée et une console de gestion unifiée facilitent le suivi de tous les éléments et rationalisent le processus de réponse aux incidents.

Chapitre **5**

Dix conseils pour une transition réussie vers une solution DLP moderne en mode cloud

Remplacer les solutions de sécurité traditionnelles établies de longue date, telles que la prévention des pertes de données (DLP), peut sembler décourageant. Votre infrastructure actuelle est le résultat de processus complexes et interdépendants qui se soutiennent mutuellement. Comme un château de cartes, chaque élément est lié aux autres, et retirer l'un d'entre eux pourrait compromettre l'ensemble de la structure.

Ne vous découragez pas ! L'innovation de la transformation numérique en vaut la peine. Le changement ne se fera pas du jour au lendemain. Procédez par étapes progressives, tirez parti de vos investissements actuels de manière judicieuse, et vous serez en bonne voie pour mettre en place une solution complète de protection des données qui sécurise vos informations sensibles sur toutes les plateformes, qu'elles soient sur site ou dans le cloud.

- **Évaluez vos besoins en matière de protection des données.** Prenez le temps d'examiner en détail l'environnement technologique actuel de votre organisation. Analysez et comprenez quelles données nécessitent une protection, quels services et référentiels sont utilisés pour stocker et traiter les informations sensibles, et comment ces services sont utilisés par les équipes et collaborateurs. Impliquez votre équipe en charge de la sécurité pour identifier et évaluer spécifiquement toutes les applications de l'entreprise, les services de messagerie, les outils de collaboration, les réseaux, les pratiques de travail hybrides des utilisateurs, les dispositifs de connexion et les processus métiers. Cette analyse vous permettra de cartographier les flux de données et de déterminer comment les informations sont partagées entre les employés ou avec des parties externes.

  
  CONSEIL

  Ne vous limitez pas à l'équipe en charge de la sécurité. Le responsable des données de votre entreprise, le personnel juridique et les membres de l'équipe des ressources humaines sont parmi les autres parties prenantes qui peuvent vous donner un aperçu de la manière dont votre entreprise utilise les données.

  Procédez à une analyse approfondie de toutes les catégories de données stockées et des transactions impliquant la circulation des données sur les réseaux. Déterminez quelle priorité doit être accordée à la protection des différents types de données au sein de votre organisation. Cette étape peut être particulièrement bénéfique pour les organisations qui ont des besoins en conformité réglementaire ou qui rencontrent des problèmes d'efficacité avec leurs systèmes DLP traditionnels. Elle permettra d'identifier rapidement les domaines à améliorer et facilitera le déploiement d'une nouvelle solution DLP plus adaptée à vos besoins.

- **Identifiez et atténuez les risques les plus élevés.** Lorsque vous envisagez de migrer vers une solution de protection des données en mode cloud, il est important de prendre en compte les domaines de votre environnement technologique actuel présentant les risques les plus élevés. Cela inclut le partage involontaire de données, l'exfiltration malveillante et d'autres menaces de cybersécurité liées aux applications SaaS, à la messagerie électronique et à l'infrastructure en mode service (IaaS) dans le cloud. La solution CASB (Cloud Access Security Broker) de Netskope, leader du marché, intègre une solution DLP centrale pour assurer la sécurité des données et ce, pour les applications cloud approuvées ou non par l'entreprise (car il est erroné de penser que vous n'en avez pas).
- **Choisissez judicieusement votre fournisseur de protection des données.** Assurez-vous de sélectionner un fournisseur qui répondra aux besoins actuels et futurs de votre entreprise, quel que soit l'environnement dans lequel vous évoluez. La solution DLP de Netskope se

distingue en offrant une couverture complète pour tous les besoins liés au cloud et au-delà. Cela comprend la protection des données au repos, en transit et en cours d'utilisation dans les environnements cloud et sur site, ainsi que la DLP pour les appareils, les e-mails, les réseaux, le web, le SaaS et l'IaaS, et les applications privées. Grâce à cette couverture complète de tous les mouvements de données modernes, les entreprises bénéficient d'une visibilité maximale sur l'ensemble de leur système, y compris les sites non fiables. Lors de l'évaluation des solutions, il est essentiel de considérer l'étendue des capacités offertes, telles que le nombre et les types de fichiers analysés, la compréhension possible des formats d'image et la couverture des différentes catégories de données sensibles, y compris les identificateurs internationaux et spécifiques à un pays. Il est également important de prendre en compte la capacité du système à exploiter le contexte des risques pour prendre des décisions automatisées et informées afin de répondre de manière adaptative aux incidents lors de l'utilisation de données sensibles. Bref, évitez une approche superficielle de la protection des données qui pourrait engendrer plus de problèmes que de solutions.

- **Protégez vos services de messagerie et vos applications de collaboration.** Découvrez la puissance de la protection des e-mails et des logiciels SaaS hébergée dans le cloud avec la solution DLP de Netskope. Elle offre une protection complète pour toutes les informations sensibles de votre entreprise, y compris les e-mails sortants sensibles et les communications asynchrones via des applications de collaboration SaaS telles que Slack et Teams. Grâce aux interfaces de programmation d'applications (API), à la protection en ligne en temps réel et à la prise en compte des instances de messagerie personnelle et de logiciels SaaS par rapport aux instances professionnelles des mêmes services, vous pouvez avoir la certitude que vos données d'entreprise sont sécurisées dans toutes les circonstances. Que ce soit pour la collaboration interne ou avec des partenaires externes, Netskope vous offre une tranquillité d'esprit pour la sécurité de vos données.
- **Protégez votre messagerie électronique hébergée dans le cloud.** Découvrez la puissance de la protection du courrier électronique dans le cloud avec la solution DLP de Netskope. Celle-ci offre une protection complète pour toutes les informations sensibles de votre entreprise en les protégeant contre les attaques malveillantes et le partage involontaire de données. Grâce aux interfaces de programmation d'applications (API), à la protection en temps réel en ligne et à la prise en compte des instances de courrier électronique personnelles, vous pouvez avoir l'assurance que vos données professionnelles sont sécurisées dans toutes les situations. Avec l'aide de Netskope, vous pouvez migrer votre service de messagerie vers le cloud en gardant l'esprit tranquille.

- **Sécurisez les données en mouvement.** Les données transférées entre différents lieux, connexions, services et appareils, tels que les réseaux domestiques, les bureaux d'entreprise, les filiales, les appareils professionnels et personnels, peuvent être difficiles à gérer et à sécuriser. Les solutions DLP traditionnelles basées sur un proxy ne suffisent pas toujours à protéger les données en mouvement. C'est là que le service DLP unifié de Netskope entre en jeu. Intégré à la plateforme intelligente SSE (Security Service Edge) de Netskope, il est conçu pour sécuriser les données sensibles, peu importe où vos collaborateurs travaillent. Avec cette solution, vous bénéficierez d'une sécurité optimale pour vos transactions de données, en appliquant les principes Zero Trust et en exploitant tout le contexte de risque disponible, sans les contraintes matérielles complexes. Grâce à l'innovante solution DLP de Netskope, vous pouvez garder l'esprit tranquille en sachant que vos données sont sécurisées en tout temps et en tout lieu.
- **Protégez les données sur les appareils de vos collaborateurs.** Même avec la migration croissante des données vers le cloud, il est essentiel de prévenir la perte ou le vol de fichiers sensibles, qu'ils soient stockés sur des appareils connectés à un réseau d'entreprise ou non. Que ces données sensibles soient créées localement sur un appareil ou téléchargées à partir du cloud, la solution DLP de Netskope est là pour vous aider. Cette solution légère pour les appareils offre toutes les fonctionnalités avancées de la DLP, telles que les classificateurs basés sur l'apprentissage automatique, la reconnaissance optique des caractères (OCR), l'empreinte numérique des fichiers, la correspondance exacte des données (EDM), et bien plus encore. De plus, elle utilise efficacement les ressources en tirant parti du cloud. Elle prend en charge une variété de cas d'usage, y compris la détection des données transférées via des périphériques USB, et fournit des stratégies de contrôle des périphériques pour garantir la sécurité de vos données sensibles, peu importe où se trouvent vos employés et à partir de quel appareil ils sont connectés.
- **Restez fidèle à ce qui fonctionne lorsque vous planifiez l'avenir.** Si vous avez récemment investi dans des capacités de protection des données (DLP) avec un fournisseur de services cloud ou un fournisseur de logiciels en mode service (SaaS), il peut être judicieux de continuer à utiliser ces services à court terme. Par exemple, si un fournisseur SaaS protège déjà efficacement vos applications de bureau, il n'est pas nécessaire de changer immédiatement de solution. Cependant, veillez à ne pas vous retrouver avec de nombreuses stratégies spécifiques et déconnectées les unes des autres. Si vous souhaitez étendre la protection des données à plusieurs clouds et applications SaaS, vous risquez de vous retrouver avec plusieurs consoles et stratégies différentes. La solution DLP de Netskope propose une approche plus simple : une

console unique avec des stratégies cohérentes qui peuvent protéger vos données, indépendamment de l'endroit où elles sont stockées ou consultées.

- **Profitez d'une protection complète des données.** La solution DLP de Netskope constitue une approche plus moderne et plus efficace que jamais de la protection des données. Elle utilise des technologies de détection avancées telles que l'apprentissage automatique, l'empreinte numérique des données et la reconnaissance d'images à grande échelle, même sur les appareils, grâce à la puissance de calcul fournie par le cloud. Avec sa console unique et des stratégies unifiées, elle simplifie la gestion des besoins de protection des données dans toute l'organisation. La solution DLP de Netskope tire parti de la collecte et de l'analyse de renseignements sur les risques et de données contextuelles sur les utilisateurs, les appareils, les données, les réseaux, les clouds et les comportements pour évaluer chaque interaction avec des données sensibles. Cela permet d'adapter dynamiquement la réponse à chaque violation spécifique de la stratégie. Cette nouvelle approche favorise une collaboration sécurisée et des pratiques modernes de partage des données, sans entraver la productivité. De plus, elle réduit les faux positifs et améliore la précision de la protection des données. La solution DLP de Netskope est intégrée nativement à la plateforme globale Netskope SSE, assurant une identification continue des risques pour l'entreprise, des comportements et des vulnérabilités en matière de sécurité. Ainsi, les entreprises bénéficient d'une intégration complète de la solution DLP Netskope à Netskope SSE, garantissant une visibilité constante sur les risques, les comportements et les vulnérabilités en matière de sécurité.
- **Préservez les connaissances de vos collaborateurs.** La transition vers une nouvelle solution DLP en mode cloud peut sembler complexe, mais elle ne doit pas être source de stress. Profitez de l'expertise des personnes qui ont géré votre système DLP existant, telles que les administrateurs des politiques de sécuritéet l'équipe d'intervention en cas d'incident. Leur expérience peut vous aider à reproduire les meilleures pratiques lors de la transition vers une solution cloud, ainsi qu'à répondre aux exigences technologiques en matière de conformité, en produisant des profils de politiques, et à développer de nouveaux processus pour gérer les incidents. La solution DLP de Netskope réduit la charge de travail de votre équipe DLP, permettant ainsi à vos équipes en charge de la sécurité de consacrer moins de temps à la gestion de problèmes frustrants et davantage de ressources à des initiatives proactives en vue d'assurer la sécurité de votre entreprise.
- **Privilégiez l'expérience aux beaux discours marketing.** La réussite nécessite plus que des compétences techniques. Que ce soit pour développer des indicateurs pour la direction générale ou fournir des

conseils et des actions au personnel, il est important de prendre en compte de nombreux aspects. Veillez à solliciter l'aide des équipes d'assistance de votre fournisseur afin d'organiser votre parcours et d'exploiter pleinement la valeur de votre entreprise, pour vous assurer que l'effort en vaut la peine.

La sécurité prête à toute épreuve

Protection des données

Netskope, leader mondial du SASE, redéfinit la sécurité du cloud, des données et des réseaux afin d'aider les entreprises à appliquer les principes du zero trust pour protéger leurs données. Rapide et facile à utiliser, la plateforme Netskope offre un accès optimisé et une sécurité en temps réel pour les utilisateurs, leurs appareils et les données, peu importe où ils se trouvent. Netskope aide ses clients à réduire les risques, à augmenter la productivité et à bénéficier d'une visibilité sans précédent sur l'activité des applications cloud, web et privées. Des milliers de clients, dont plus de 25 du classement Fortune 100, font confiance à Netskope et à son puissant réseau NewEdge pour faire face à l'évolution des menaces, aux nouveaux risques, aux changements technologiques, aux changements organisationnels et de réseau, ainsi qu'aux contraintes réglementaires. Pour savoir comment Netskope aide ses clients à être prêts à toute épreuve au cours de leur parcours SASE, rendez-vous **sur netskope.com/fr**.

netskope

Préparez-vous à un avenir « cloud first » en utilisant une technologie DLP moderne

Avec l'adoption rapide du cloud et l'évolution des modes de travail, les méthodes traditionnelles de protection des données ne sont plus adaptées. La sécurité des données doit désormais garantir une protection cohérente, quel que soit l'emplacement des données et des utilisateurs. Une solution DLP moderne doit être conçue spécifiquement pour les cas d'usage dans le cloud, plutôt que d'être simplement adaptée à cette technologie. Elle doit appliquer des principes Zero Trust, simplifier la complexité et offrir une application uniforme des politiques de sécurité, en toute circonstance.

À l'intérieur…

- Évaluez votre approche en matière de protection des données
- Protégez les données et soutenez les objectifs de l'entreprise
- Découvrez le fonctionnement de la DLP moderne
- Minimisez l'accès non autorisé aux données
- Simplifiez les politiques de sécurité tout en garantissant leur efficacité
- Déplacez en toute sécurité des données vers les applications cloud et entre celles-ci

Carmine Clementelli est un leader technologique et un expert en cybersécurité spécialisé dans la sécurité des données, la sécurité dans le cloud, les principes Zero Trust et les services de sécurité en périphérie (SSE) chez Netskope. Il possède une vaste expérience, ayant travaillé chez Palo Alto Networks, Symantec et d'autres organisations internationales, et est reconnu en tant qu'auteur, conférencier et conseiller depuis de nombreuses années.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-394-20766-4

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.