Le DLP (Prévention contre la perte de données) et la transformation digitale

INTRODUCTION

L'ère actuelle du numérique a engendré une quantité de données sans précédent. La plupart de ces données sont considérées comme sensibles. Citons par exemple les informations personnelles sur les clients et les employés, les données financières et la propriété intellectuelle que les entreprises doivent protéger. Autrefois, ces informations étaient imprimées sur du papier et conservées dans un classeur verrouillé. Aujourd'hui, ces séries de zéros et de uns d'une grande valeur transitent d'un endroit à l'autre et sont plus vulnérables que jamais.

La nécessité de protéger ces données est donc incontestable. Elles constituent un élément vital de chaque organisation et comprennent des informations qui doivent être protégées. Certains types de données sont donc réglementés et les entreprises s'exposent à de lourdes sanctions si elles les gèrent mal. Il n'est donc pas étonnant que ces données soient également prisées sur le dark net. Un seul numéro de carte de crédit avec une adresse peut en effet coûter jusqu'à cinq dollars, et c'est bien le type d'informations dont de nombreuses bases de données regorgent. Pour toutes ces raisons, les organisations ont la responsabilité de mettre en œuvre des solutions complètes de prévention contre la perte de données (DLP).

POURQUOI LE DLP?

Une solution DLP est un ensemble de technologies et de processus qui surveille et inspecte les données sur le réseau d'une entreprise pour garantir que les données sensibles ne sont ni perdues ni volées. Un outil DLP doit toujours être au cœur de l'effort de protection des données d'une organisation qui rassemble les responsables de l'entreprise et de l'informatique pour déterminer quelles données peuvent être qualifiées de "sensibles" et convenir de la façon dont elles doivent être traitées et de ce qui constituerait une violation. Ces directives peuvent ensuite être traduites en un ensemble de règles dans un outil DLP. Les solutions DLP répondent à trois défis organisationnels majeurs: la conformité réglementaire, la protection contre la perte de données et la visibilité.

1

Conformité réglementaire:

Selon Gartner[1], la conformité réglementaire est loin en tête dans la liste des usages du DLP les plus courants. Elle est référencée dans 75% de tous les déploiements DLP enregistrés. Depuis mai 2018, le RGPD, le règlement général européen sur la protection des données, a mis les solutions DLP au centre de l'attention des spécialistes de la protection des données dans les organisations en dehors des industries réglementées, qui ont toujours été tenues de mettre en place certaines mesures pour protéger les renseignements personnels (PII) et les informations médicales protégées (PHI). Bien que les réglementations n'exigent pas explic-itement l'utilisation d'une solution DLP, les exigences de protection des données présentent souvent le concept de DLP comme pouvant aider à la conformité.

On dirait du DLP...

Département des services financiers de l'État de New York (NYDFS) — Le règlement 23 NYCRR 500 fait allusion à l'utilisation d'un DLP de données en transit sans être explicite:

Article 500.15 (a)

"(...) chaque entité concernée doit mettre en œuvre des contrôles, y compris le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, qu'elles soient en transit sur des réseaux externes ou au repos."

[1] Market Guide for Enterprise Data Loss Prevention (Guide du marché pour le DLP):
https://www.gartner.com/en/documents/3890116/market-guide-for-enterprise-data-loss-prevention

POURQUOI LE DLP?

2 Protection contre la perte de données

Les raisons pour lesquelles les informations sensibles ne sont pas exposées à des tiers non autorisés vont bien au-delà de la simple conformité. Elles sont fréquemment ciblées par des vols. Un bon indicateur de leur valeur est la volonté qu'ont les acteurs malveillants de payer sur le dark web un prix beaucoup plus élevé pour des données illégales telles que des abonnements à des récompenses et des numéros de programme de fidélité, que pour des numéros de sécurité sociale américains[2].

Bien que les organisations soient incitées à se conformer pour éviter des amendes ou des restrictions à leurs opérations commerciales, la perte de données comporte des risques financiers et de réputation beaucoup plus grands, tels que la perte de clients, le remboursement de "points" d'adhésion perdus entraînant des dommages à l'image de marque, ou même des conséquences judiciaires.

Selon l'étude Cost of a Data Breach (Coût d'une violation des données) menée en 2019 par Ponemon[3] , 30% des organisations subiront une violation dans les prochains deux ans, avec comme conséquence en moyenne:

un coût de 3,9 M$ **25.000 Enregistrements perdus**

Les secteurs soumis à la conformité réglementaire comme les soins de santé et les services financiers subissent des infractions plus coûteuses. Le coût moyen par information volée s'élevait à:

429$ soins de santé

210$ Services financiers

150$ tous les secteurs

Les solutions DLP sont particulièrement importantes pour éviter les pertes accidentelles de données dues à l'erreur humaine, comme le partage involontaire de données sensibles avec des tiers par envoi des fichiers ou sur les réseaux sociaux, ou à la défaillance des processus informatiques ou professionnels [4]. Le rapport Protected Health Information Data Breach de Verizon (2018) indique qu'en dépit des réglementations strictes appliquées au traitement des informations médicales, la perte accidentelle de données est particulièrement élevée dans le secteur des soins de santé où elle représente 57,5%[5] des cas de divulgation involontaire de données. Verizon fait également remarquer qu'il s'agit du seul secteur dans lequel les acteurs internes de l'organisation représentent une menace de perte de données plus importante que les acteurs externes malveillants

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/;
https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/#gref

[3] [4] Ponemon 2019 Data Breach:
https://databreachcalculator.mybluemix.net/

[5] Protected Health Information Data Breach Report:
http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

POURQUOI LE DLP?

3 Visibilité des données

La transformation digitale met les organisations et en particulier les responsable de la sécurité informatique face à des défis liés à la visibilité sur l'utilisation des données de leurs réseaux. Avec l'augmentation de la quantité des données, du nombre de propriétaires de données et encore plus du nombre d'endroits où les données sont stockées, il est difficile d'identifier toutes les informations sensibles et de mettre en place des mesures pour les protéger. Après tout, vous ne pouvez protéger que ce que vous pouvez voir. Trois tendances importantes rendent la visibilité plus difficile pour les organisations: l'adoption du cloud, la mobilité des utilisateurs et le chiffrement.

L'adoption du cloud oblige les organisations à maîtriser toutes les données stockées non seulement dans le data center, mais également dans toute l'organisation. Avant de migrer vos données vers le cloud, vous devez savoir de quelles données vous disposez.

Les employés ne sont plus liés à leur bureau, ce qui signifie qu'ils accèdent désormais à leurs applications et fichiers de travail à peu près n'importe où et à tout moment. Ces **utilisateurs mobiles** peuvent accéder aux données et stocker des fichiers en dehors du data center, hors de la vue de leur organisation.

De plus en plus d'organisations tentent de protéger leurs données au moyen de techniques de **chiffrement.** Toutefois, les systèmes de sécurité basés sur le matériel ne peuvent pas vérifier le contenu des fichiers cryptés. Les organisations perdent ainsi leur visibilité sur ces informations.

POURQUOI LE DLP?

Les données transitent à travers plusieurs canaux

Dans le monde numérique d'aujourd'hui, les données circulent plus librement que jamais. Elles peuvent à tout moment se trouver sur l'un des trois canaux suivants: dans un terminal, au repos ou en transit. Chaque canal dans lequel les données sont stockées ou transitent nécessite un ensemble différent d'outils ou de techniques de prévention contre les pertes de données. Les solutions DLP sont segmentées en fonction des trois canaux qu'elles protègent:

Données au niveau du endpoint: les solutions DLP au niveau du terminal sont basées sur des agents et surveillent les données en cours de traitement au niveau du terminal. Leur fonctionnement varie, mais inclut généralement des restrictions d'impression, de copier/coller entre les applications, et de téléchargement sur un support de stockage portable tel que l'USB.

Données au repos: Toutes les données stockées sur des serveurs de fichiers, des bases de données ou un stockage cloud sont considérées comme étant au repos. Les DLP appliqués aux données au repos analysent tout le contenu du dépôt pour détecter les informations sensibles.

Données en transit: également appelées DLP Web ou DLP réseau, les solutions appliquées aux données en transit inspectent tout le trafic allant d'un point A à un point B sur le Web (Internet) ou par e-mail. Il peut par exemple s'agir de données déplacées du stockage cloud vers un endpoint.

La transformation numérique a modifié le comportement des utilisateurs et les modèles de trafic, ce qui a affecté les endpoints et les canaux de données au repos. Alors que de plus en plus de données migrent vers le cloud, les solutions de données au repos perdent de leur pertinence car leurs fonctionnalités peuvent être essentiellement remplacées par des solutions CASB (Cloud Access Security Provider). En outre, il reste moins de données et peu d'applications sur les terminaux, ce qui donne plus d'importance à la sécurisation des données qui circulent entre les terminaux, les applications cloud et le stockage avec une **solution de** données en transit.

POURQUOI LE DLP N'A-T-IL PAS TENU SA PROMESSE?

Le marché du DLP est en évolution

Les solutions DLP sont en place depuis 15 ans et le marché est mature. Il y a eu si peu de différence entre les solutions DLP d'entreprise concurrentes que le grand cabinet d'analystes Gartner a envoyé à la retraite son Magic Quadrant pour la DLP d'entreprise. À la place, Gartner se focalise sur un guide du marché qui met en évidence l'importance d'une stratégie globale de protection de données et fournit des instructions quant à l'utilisation de solutions DLP intégrées.

En comparaison avec **les solutions DLP d'entreprise** qui fournissent généralement une variété de produits (agents, appliances physiques et virtuelles) à travers tous les canaux, **les solutions DLP intégrées** sont nativement fournies par des technologies telles que les passerelles web sécurisées, les systèmes de gestion de contenu, le chiffrement du courrier électronique ou la technologie CASB, et ont par conséquent une portée plus limitée.

Les solutions DLP d'entreprise sont notoirement complexes et coûteuses. Les organisations qui achètent une DLP d'entreprise finissent souvent par n'utiliser qu'un petit sous-ensemble de ses capacités et ne s'occupent que des cas d'utilisation de base qui pourraient être résolus avec une solution DLP intégrée qui évite à l'organisation une installation et une intégration coûteuses et longues.

Selon les estimations de Gartner,

> "D'ici 2021, 90% d'organisations mettront en œuvre au moins une forme de DLP intégrée, une augmentation par rapport à 50% aujourd'hui." [6]

Toutefois, DLP d'entreprise et DLP intégrée ne sont pas mutuellement exclusives. Les organisations qui ont déjà investi dans de tels produits devraient travailler avec leur infrastructure existante. Néanmoins, toute organisation devrait envisager d'ajouter un DLP intégré pour répondre à d'autres cas d'utilisation qui comblent les lacunes de sa stratégie de protection des données existantes qui auraient émergé à la suite de la transformation numérique.

[6]Comment choisir entre les approches DLP d'entreprise et DLP intégrée
https://www.gartner.com/doc/3757464?ref=mrktg-srch

POURQUOI LE DLP N'A PAS RÉALISÉ SA PROMESSE

La prévention des pertes de données est une initiative à l'échelle de l'organisation, et non un outil informatique

Bien qu'il s'agisse d'une solution mature, les organisations continuent de signaler des problèmes dans leurs déploiements DLP, la plupart provenant d'une mauvaise planification et à d'autres problèmes organisationnels.

La plupart des organisations pensent à tort que le DLP devrait être implémenté et géré à long terme uniquement par le service de sécurité informatique. Une fois les règles du DLP établies, la responsabilité de la solution DLP devrait être transférée aux opérations commerciales. En outre, ceux qui déploient des solutions DLP doivent obtenir l'adhésion de la haute direction, afin de redonner de la visibilité aux unités commerciales ou aux équipes de gestion des risques de l'entreprise.

Pour éviter d'avoir à chercher des sponsors supplémentaires ainsi que des précédents pour justifier le projet, ce qui ajoute inévitablement des exigences et de la complexité aux déploiements, les équipes doivent s'assurer de l'adhésion interne et lier les projets DLP à des initiatives ou des objectifs spécifiques.

EXIGENCES DU CLOUD DLP

À mesure que les organisations migrent vers le cloud, leur sécurité devrait également y migrer. Mais, le simple fait de reconfigurer une pile matérielle traditionnelle pour le cloud est inefficace et ne fournit pas les protections et les services d'une solution conçue pour le cloud. Cela vaut également pour le DLP. Pour relever les défis en matière de protection des données qui sont apparus avec la transformation numérique et surmonter les lacunes du DLP traditionnel, une solution DLP basée sur le cloud nécessite les trois éléments suivants:

1. **Protection identique pour tous les utilisateurs sur le réseau ou en dehors**
   Avec les solutions DLP traditionnelles ancrées dans le data center, le niveau de visibilité et de protection dépend de l'endroit où se trouvent vos utilisateurs. Les utilisateurs distants peuvent contourner l'inspection lorsqu'ils sont hors réseau, se connectant directement aux applications cloud et contournant le VPN ainsi que toutes les mesures de protection des données. Pour assurer une protection complète des données, une solution DLP devrait offrir une protection identique à tous les utilisateurs indépendamment de leur emplacement, qu'ils soient au bureau, dans un salon d'aéroport ou à domicile.

2. **Inspection du trafic chiffré**
   Plus de 70% du trafic moderne utilisant le chiffrement, il incombe aux organisations d'inspecter ce trafic. Cependant, le chiffrement ayant été créé à l'origine comme mesure de sécurité, les solutions de sécurité traditionnelles n'inspectent pas nativement ce trafic. Par conséquent, les organisations ont tendance à n'inspecter qu'une infime portion de leur trafic crypté — et à quoi sert une solution DLP si elle ne voit, peut-être, que 30% du trafic total? Renforcer votre niveau de sécurité en ajoutant des appliances SSL n'est probablement ni faisable financièrement, ni acceptable en termes de complexité informatique. La seule façon d'obtenir une visibilité sur le trafic crypté est d'utiliser une solution DLP qui inspecte nativement le SSL.

3. **Évolutivité élastique pour l'inspection inline**
   L'extraordinaire croissance du trafic Internet exige une constante mise à jour des solutions DLP traditionnelles basées sur des appliances, car leur capacité finie d'inspection est rapidement épuisée. Pour tenter de surmonter la complexité et le coût de cette entreprise, de nombreuses organisations résistent dès le départ au déploiement d'une solution DLP inline. Malheureusement, cela ne permet aux organisations de contrôler les dommages qu'après que leurs données aient été compromises. Une solution cloud permet une capacité d'inspection élastiquement modulable qui peut empêcher la perte de données en inspectant tout le trafic inline — avant que les données ne soient compromises.

ZSCALER CLOUD DLP

Une partie de Zscaler Internet Access

Zscaler Internet Access™ (ZIA™) est une passerelle Internet et Web sécurisée fournie en tant que service à partir du cloud. La ZIA se situe entre vos utilisateurs et Internet, inspectant chaque octet de trafic inline à travers de multiples techniques de sécurité, même au sein du trafic SSL, assurant une protection totale contre les menaces internet. Cette plate-forme cloud spécialement conçue inclut le Cloud Sandbox, le firewall de nouvelle génération, la visibilité et le contrôle des applications cloud, ainsi que le Cloud DLP.

Vue d'ensemble du Cloud DLP

Zscaler Cloud DLP offre une protection complète des données avec une inspection complète du contexte et du contenu pour toutes les données en transit, ainsi que des fonctionnalités avancées, notamment Exact Data Match, l'apprentissage automatique et les politiques granulaires pour une protection optimale.

Zscaler Cloud DLP remplit les trois conditions

Zscaler Cloud DLP fournit le même niveau de sécurité à tous vos utilisateurs en faisant migrer vos données de sécurité vers le cloud. Zscaler se situe entre vos utilisateurs et les applications auxquelles ils se connectent. La politique Cloud DLP suit les utilisateurs là où ils travaillent – sur réseau ou en dehors – fournissant en tout temps et à tous les utilisateurs le même niveau de protection.

Il permet également une inspection complète du trafic crypté. Environ 70% du trafic sortant est crypté et n'est donc pas soumis à l'inspection par les solutions DLP traditionnelles. Avec Zscaler, il n'y a aucune contrainte de capacité pour permettre l'interception SSL à grande échelle. Zscaler est un proxy par sa conception, effectuant l'inspection SSL sur tout le trafic sans subir les limites d'inspection des appliances.

En outre, Zscaler est conçu pour fonctionner inline, de sorte qu'il peut bloquer les informations sensibles avant qu'elles ne quittent votre réseau — au lieu de simplement contrôler les dégâts après que les données ont été compromises. L'architecture de sécurité Zscaler a été conçue dès le départ dans le cloud et le service est basé sur l'utilisateur, et non sur la capacité, ce qui permet à votre inspection Cloud DLP d'évoluer de manière élastique avec des performances garanties par des SLA.

CONCLUSION

Le DLP doit être considéré comme un processus de sécurité bien défini, renforcé par une technologie de support bien gérée. Cependant, même à ce stade avancé de maturité de la solution DLP, les organisations continuent de lutter avec les déploiements DLP. Cela est principalement dû à une mauvaise représentation des solutions DLP en interne dans le contexte d'un programme de sécurité. En outre, nombreux sont ceux qui, sur le marché, surestiment la simplicité des déploiements, le niveau de précision immédiate dans l'identification du contenu et la visibilité, et le contrôle de toutes les applications.

Avec l'augmentation des menaces et le nombre de plus en plus croissant de réglementations liées à la protection des données, les organisations doivent combler les failles de sécurité causées par le cloud et la mobilité. Par le passé, il se serait agi d'ajouter plus d'appliances à une pile de sécurité déjà complexe. Zscaler offre un meilleur moyen. Avec Zscaler Cloud DLP, vous pouvez combler les lacunes de protection des données, quel que soit l'endroit où les utilisateurs se connectent et où les applications sont hébergées, sans appliances coûteuses et complexes.

À propos de Zscaler

Zscaler permet aux entreprises de transformer en toute sécurité leurs réseaux et leurs applications pour s'adapter à la prédominance mobile et cloud du monde actuel. Zscaler connecte les utilisateurs aux applications et aux services cloud, quels que soient le périphérique utilisé, l'emplacement de l'utilisateur ou le type de réseau; tout en offrant une sécurité sans faille et une expérience utilisateur conviviale. Et le tout, sans appliances de passerelle coûteuses et complexes.

zscaler™