Rôle d'une solution DLP moderne dans la conformité au RGPD

En vigueur depuis 2018, le Règlement général sur la protection des données (RGPD) offre aux Européens davantage de contrôle sur la collecte et la gestion de leurs données personnelles, notamment au vu des avancées technologiques de ces vingt dernières années. Ce texte de référence accorde entre autres, aux citoyens de l'Union, le droit d'accéder, de rectifier et d'effacer (« droit à l'oubli numérique ») les informations détenues à leur sujet, ainsi que le droit à la portabilité des données.

Les dispositions qui y sont énoncées s'appliquent à toute entreprise qui contrôle ou traite les données personnelles de résidents de l'Union européenne. Juridiquement parlant, le terme de « données personnelles » couvre un champ relativement vaste. Il désigne en règle générale les données qui : identifient ou peuvent être utilisées pour contacter une personne (par exemple, le nom, l'adresse e-mail, la date de naissance, le numéro de téléphone ou l'ID utilisateur…) ; identifient un appareil individuel (comme une adresse IP) ; reflètent ou bien représentent le comportement ou l'activité d'une personne (par exemple, sa localisation). Le RGPD concerne les entreprises basées dans l'UE ainsi que les organisations établies hors de l'Union, dès lors que ces dernières offrent des biens ou des services aux résidents de l'UE ou qu'elles suivent le comportement de ces personnes au sein de l'Union européenne. En bref, tous les prestataires de services traitant les données à caractère personnel de résidents de l'UE sont tenus de respecter cette réglementation.

Les entreprises soumises au RGPD doivent donc implémenter les processus et les outils de sécurité adéquats afin de gérer, protéger et connaître à tout moment l'emplacement des données réglementées. Tout défaut de conformité peut entraîner de lourdes sanctions, nuire à la réputation de la marque, voire aboutir à des poursuites judiciaires.

Alors que de nombreux pays adoptent des réglementations de plus en plus draconiennes en la matière, la protection et la confidentialité des données s'imposent clairement comme une initiative stratégique incontournable pour les entreprises. Mais faute d'un plan d'action suffisamment clair, la plupart d'entre elles peinent encore à mettre en œuvre les mesures nécessaires. De même, étant donné la diversité des informations sensibles et le nombre croissant de sites qui composent les structures distribuées d'aujourd'hui, une mise en conformité manuelle relève de la gageure. Les entreprises ont donc tout intérêt à investir dès à présent dans des technologies qui leur permettront d'être présentes sur tous les fronts : bonnes pratiques de sécurité et de gestion des risques, visibilité sur l'utilisation et l'emplacement des données, détection des compromissions et planification de la réponse à incident.

Protection des données : une mission de plus en plus complexe

D'un côté, le RGPD donne aux entreprises l'élan dont elles ont besoin pour renforcer la confidentialité et la sécurité des données à caractère personnel (DCP). De l'autre, l'implémentation d'un cadre de protection structuré reste une tâche ardue, surtout si l'on considère la diversité des DCP pouvant être collectées et le nombre croissant des lieux de circulation et d'accès à ces informations.

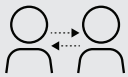
Du reste, l'adoption du cloud et la généralisation du télétravail ajoutent encore un degré de complexité. Les données personnelles et les informations sensibles qui évoluent dans les nouveaux confins de la datasphère (applications SaaS, clouds privés ou publics, etc.) sont plus que jamais soumises aux risques d'exposition. Enfin, l'évolution inattendue des modes de travail a vu émerger une pléthore de sites distants qui augmentent considérablement les risques de fuite ou d'exposition dus à des erreurs humaines ou des négligences internes.

Une stratégie en trois temps

Dans ce contexte, la mise en conformité des stratégies de protection des données représente un véritable défi pour les RSSI. Nous pensons qu'il convient d'aborder ce processus en prenant appui sur ces trois volets essentiels :

1. **Identification du contenu à protéger**. Il s'agit ici des données à caractère personnel pouvant permettre d'identifier tout résident de l'UE.
2. **Mise en œuvre des mécanismes préventifs**. Les entreprises doivent protéger les données personnelles sensibles et réglementées contre les menaces externes, les acteurs internes, mais aussi contre les expositions accidentelles dues à la négligence de certains utilisateurs. Dans certains cas, les fuites et les compromissions avérées sont soumises à une obligation de notification aux autorités de tutelle ou individus concernés. Tout défaut de divulgation ou non-respect des délais impartis peut alors aboutir à des sanctions supplémentaires, des recours collectifs ainsi qu'à l'indemnisation des victimes, sans oublier le préjudice en termes d'image.
3. **Application des mesures de sécurité**. Le RGPD permet aux clients d'accéder aux données personnelles que les entreprises collectent à leur sujet. Hormis dans certains cas spécifiques, ils peuvent également en réclamer la suppression, ce qui oblige les entreprises à connaître – à tout moment – l'emplacement précis de ces informations. Nos conseils : munissez vos équipes d'outils dédiés au suivi des DCP sur l'ensemble des vecteurs de communication, implémentez des règles d'accès Zero Trust obéissant au principe du moindre privilège et déployez des mesures de protection fortes.

Recommandations



Dialoguez avec vos dirigeants ; faites des points réguliers sur les progrès de votre programme de sécurité en matière de confidentialité des données

Identifiez et relevez vos principaux défis de sécurité et de confidentialité

Recensez les DCP que vous détenez et vérifiez qu'elles sont utilisées dans le respect de la réglementation

Déterminez les technologies capables de faciliter votre mise en conformité

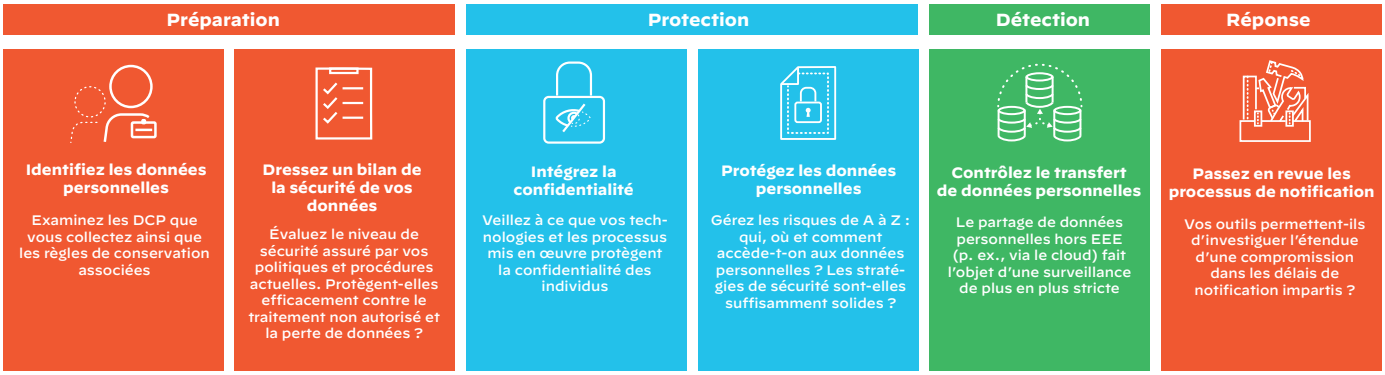


Figure 1 : Quatre étapes pour relever les défis du RGPD

Une approche intégrale de la sécurité et de la confidentialité des données

La conformité RGPD exige une stratégie de sécurité exhaustive et consolidée. Celle-ci doit couvrir l'ensemble des réseaux – sur site, dans le cloud ainsi que les utilisateurs distants – tout en vous permettant de répondre efficacement à ces quatre enjeux primordiaux :

- Identification et suivi des DCP (où qu'elles se trouvent)
- Protection des données et restrictions d'accès aux seules personnes autorisées
- Prévention des fuites et des compromissions
- Réponse et remédiation rapides des incidents

Les données personnelles sensibles sont susceptibles d'être stockées, partagées et transmises de toute part, qu'il s'agisse des équipements IT de vos collaborateurs ou des applications SaaS auxquelles ils ont accès. En plus de votre propre cloud privé (data center), les plateformes cloud publiques stockent et échangent également ce type d'informations sensibles. Côté transmission, les données peuvent circuler via différents vecteurs de communication : trafic web chiffré et non chiffré, e-mails, applications de partage de fichiers, stockage dans le cloud public, appareils mobiles et plus encore. Ces multiples canaux de données au repos et en transit nous amènent à votre premier défi : **comment identifier et suivre à tout moment l'ensemble des données à caractère personnel ?**

Malgré toute leur bonne volonté, la négligence des utilisateurs constitue l'un des premiers facteurs de perte de données personnelles. Exposition d'informations sensibles via des applications SaaS non approuvées, partage excessif dans des référentiels cloud, envoi à des tiers non autorisés... les causes peuvent être nombreuses. Ces menaces internes représentent donc votre deuxième problématique : **comment limiter l'exposition des données et en restreindre l'accès aux seuls utilisateurs autorisés ?**

Les fuites de données et les compromissions de sécurité peuvent semer le chaos dans une entreprise, avec une onde de choc aux effets potentiellement durables. La plupart des menaces externes sont véhiculées par des campagnes de phishing ou des attaques par malware, ce qui implique le plus souvent le téléchargement de fichiers sur le web. En d'autres termes, ces leaks sont le fait d'un comportement ou d'une action du dépositaire des données. Les DCP doivent être protégées en continu, même lorsque vous êtes tenu de les partager pour des raisons professionnelles avec un partenaire ou un fournisseur. Ce qui soulève la question suivante : **comment bloquer ou prévenir les fuites ou les compromissions de données personnelles lorsque celles-ci circulent à l'extérieur de votre réseau ?**

Le RGPD impose également des obligations de notification lorsque des données à caractère personnel sont compromises. Voici donc un autre enjeu de taille : **comment organiser la réponse à incident, les investigations et les actions de remédiation afin de neutraliser les effets d'une compromission dans les délais impartis ?**

Une solution DLP innovante au service de votre conformité au RGPD

Les technologies DLP modernes sont spécialement conçues pour automatiser la détection, le suivi et la protection des données sensibles sur l'ensemble de votre environnement. Grâce à des règles prédéfinies et personnalisables, ainsi que des conditions contextuelles alignées sur les exigences réglementaires, les équipes peuvent découvrir et recenser les DCP en toute simplicité. Prêtes à l'emploi, des politiques spécifiques au RGPD ainsi qu'à d'autres règlements sur la protection des données facilitent la configuration et réduisent le nombre de paramétrages manuels.

En offrant une visibilité sur l'ensemble du réseau et du trafic – y compris les télétravailleurs, les référentiels cloud ainsi que les applications approuvées ou non – les solutions DLP avancées éliminent les angles morts et les problèmes de Shadow IT. Les entreprises peuvent contrôler facilement la façon dont les données sensibles sont utilisées, ainsi que les individus qui y ont accès. Associées à des stratégies d'authentification, de gouvernance des données et de gestion des droits d'accès, ces technologies permettent d'appliquer le principe du moindre privilège et de sécuriser le partage de données avec des tiers. Les systèmes DLP de dernière génération proposent également des actions de remédiation pour répondre à toute infraction aux politiques en place. Ils peuvent par exemple alerter automatiquement les utilisateurs, bloquer les transferts de données non sécurisés, corriger et chiffrer les informations, ou encore limiter le partage de données confidentielles ouvertement exposées via des applications SaaS.

Vu la rigueur du cadre réglementaire européen, les entreprises ont tout intérêt à investir dans des technologies visant à faciliter et accélérer la mise en conformité de leurs initiatives de protection et de confidentialité des données. **À cette fin, elles peuvent compter sur l'efficacité de technologies DLP évolutives.**

Devenus excessivement complexes, les produits DLP traditionnels ne font pas le poids, tant ils sont enracinés dans des infrastructures sur site difficiles et coûteuses à faire évoluer. Quant aux nouvelles offres intégrées, elles restent trop limitées en matière de couverture. À l'heure de la dématérialisation et de la transformation des réseaux, l'adoption d'une solution DLP moderne, implémentée en mode cloud, constitue votre meilleure garantie pour répondre aux enjeux de protection des données. D'ailleurs, près de 40 % des professionnels interrogés dans le cadre d'une étude ESG estiment que leurs contrôles de sécurité réseau auront basculé vers le cloud d'ici les deux prochaines années[1]. Les solutions DLP de dernière génération sont déployées sur une architecture cloud-native. Elles offrent ainsi des atouts majeurs sur l'ensemble des points de contrôle (sur site et dans le cloud), avec des gains notables en matière d'efficience, d'efficacité opérationnelle, d'échelle et de coût.

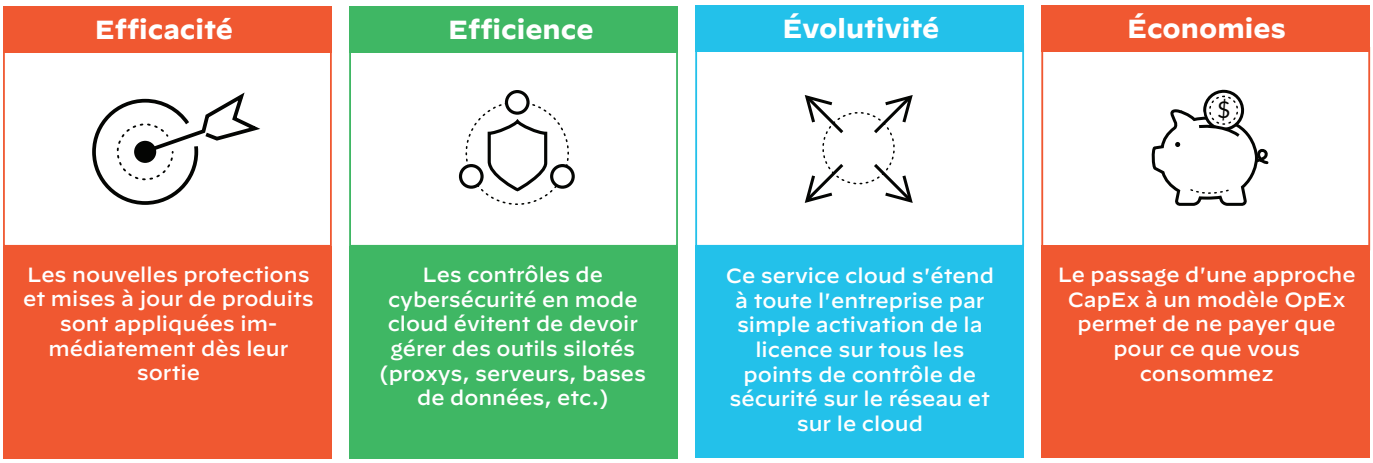


Figure 2 : Principaux avantages d'une solution DLP cloud moderne

Enterprise DLP de Palo Alto Networks

Enterprise DLP, la solution dédiée signée Palo Alto Networks, répond efficacement aux enjeux de la protection des données de toute l'entreprise au sein d'environnements distribués et pilotés depuis le cloud. Grâce à ses fonctionnalités automatiques de détection, de suivi et de protection des données à caractère personnel, cette solution cloud corrige les lacunes des systèmes de protection traditionnels.

Dès le départ, Enterprise DLP propose des règles de détection contextualisées, précises et personnalisables, déjà alignées sur les exigences fondamentales du RGPD. Ces politiques prêtes à l'emploi simplifient le processus de configuration et accélèrent les paramétrages manuels.

En tant que solution DLP cloud le plus complet du marché, notre solution fournit une visibilité sur l'ensemble du réseau et du trafic – y compris les télétravailleurs, les sites distants, les logiciels, les infrastructures et les plateformes sous forme de services (SaaS, IaaS et PaaS) – afin d'éliminer les angles morts ainsi que les problèmes de Shadow IT. Les politiques RGPD organisationnelles sont définies en central, puis synchronisées automatiquement sur l'ensemble des environnements où le service est activé (dans le cloud et sur site). L'homogénéité est donc assurée sur l'intégralité de vos infrastructures, pour l'ensemble de vos utilisateurs, et s'adapte au rythme de développement de l'entreprise : fini les cycles de création de politiques inutiles.

Enterprise DLP s'intègre nativement à tous nos pare-feu nouvelle génération pilotés par machine learning (NGFW physiques, virtuels et cloud) ainsi qu'à la suite de produits de sécurité cloud Prisma®. Vos données sensibles sont donc constamment protégées sur les réseaux physiques et virtuels, dans le cloud (SaaS au repos, SaaS inline et IaaS cloud-native), pour chaque utilisateur et chaque type de connexion (sur le campus, depuis une filiale ou en télétravail). Grâce à ses politiques prédéfinies et personnalisables, notre solution identifie automatiquement les données entrant dans le cadre du RGPD. Elle surveille la façon dont ces informations sont utilisées et transférées sur des environnements sécurisés ou des sites non conformes, tout en les protégeant contre la perte et le vol.

1. « Transitioning Network Security Controls to the Cloud » ESG, août 2020, https://www.esg-global.com/research/esg-research-report-transitioning-network-security-controls-to-the-cloud.

Enterprise DLP de Palo Alto Networks est un service facile à déployer, à utiliser et à maintenir, qui ne requiert l'ajout d'aucun logiciel, proxy, serveur ou connecteur cloud, ni de base de données ou de ressources IT. Au final, vous bénéficiez d'une solution économique qui vous permettra de diviser votre coût total de possession (TCO) par au moins trois par rapport aux technologies DLP traditionnelles.

Différents outils sont disponibles pour aider votre entreprise à respecter les exigences de confidentialité des données. Toutefois, une technologie isolée ne peut à elle seule lutter contre l'évolution croissante des cybermenaces. Afin de protéger efficacement vos réseaux, terminaux, infrastructures cloud et les différents utilisateurs qui s'y connectent, nous vous conseillons d'adopter une approche multicouche de la sécurité.

Conclusion

À l'heure où la protection des données est soumise à des réglementations de plus en plus strictes, l'adoption d'une solution DLP cloud innovante vous permettra de répondre à vos obligations via une approche à la fois complète et unifiée. Pour plus d'informations, rendez-vous sur notre site web.

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr