# La nécessité de la DLP aujourd'hui – Un livre blanc Clearswift

**Ben Rothke, CISSP CISA**

**La DLP (Data Leak Prevention, ou Prévention contre la fuite de données en français) est une technologie puissante pouvant être utilisée pour combler les fissures du barrage établi contre les fuites de données qui affectent d'innombrables organisations dans le monde entier.**

**Bien que la DLP regroupe un grand nombre de fonctionnalités, qui nécessiteraient un document beaucoup plus long, Clearswift a le plaisir de vous offrir ce livre blanc comme introduction à la DLP, l'un des outils les plus importants et les plus performants du kit industriel de sécurité des informations.**

## Introduction

Quiconque a déjà essayé de remplacer une cartouche de toner pour imprimante laser dans une entreprise américaine sait combien cela peut s'avérer compliqué. Si vous avez la chance d'en trouver une dans le placard à fournitures, quelques signatures et tours de clé seront nécessaires pour extraire la cartouche des fins fonds du placard. Une fois la cartouche sortie, la porte du placard sera refermée et sécurisée.

Les entreprises pensent de toute évidence qu'il est dangereux de laisser des cartouches couteuses sans sécurité et à la portée d'employés qui pourraient les voler.

Pour une raison ou pour une autre, ces entreprises ne pensent pas pouvoir faire confiance à leurs employés les plus fiables en ce qui concerne les fournitures de bureau, ce qui les oblige à les stocker dans des pièces fermées à clé.

La vérité est que quelques brebis galeuses peuvent rapidement voler des milliers de dollars de fournitures de bureau et les entreprises ont donc réalisé l'importance de sécuriser ces dernières.

Pour des raisons similaires, les sociétés choisissent souvent d'étiqueter chaque chaise, table, ordinateur portable, micro-ondes, etc. Si ces objets étaient laissés sans sécurité et sans marque, le pire pourrait en effet arriver.

Cependant, les entreprises prennent souvent des pincettes pour sécuriser les téraoctets de données confidentielles et exclusives qui circulent sur leurs réseaux. Pourquoi les fournitures de bureau font-elles donc l'objet d'un plus haut niveau de sécurité que les données ?

Tout d'abord, prenez un instant pour réfléchir à la multitude de types de données différents qui circulent dans votre organisation et qui nécessitent des contrôles de sécurité des informations. Sans trop d'efforts, vous devriez pouvoir en identifier une dizaine en l'espace d'une minute. La liste ci-dessous n'est qu'un exemple des nombreux types de données pouvant se trouver dans votre organisation :

| | | | |
|---|---|---|---|
| Données financières/Feuilles de calcul | Données de prévision des ventes | Ressources humaines | R&D |
| Fusions & Acquisitions | Données légales | Données privées des clients | Numéros de cartes de crédit |
| Numéros de sécurité sociale | Coordonnées | Listes de clients | Stratégies marketing |

Pendant de nombreuses années, Sun Microsystems a considéré que le réseau était l'ordinateur. En partant de cette hypothèse, le réseau est donc les données, car celles-ci constituent le trésor de beaucoup d'organisations. Imaginez si 500 chaises de bureau portant des étiquettes d'identification étaient volées ; cela ne poserait pas de réel problème car elles sont assurées.

En revanche, le vol d'un gigaoctet de données dans une organisation provoque souvent des conséquences considérables, notamment :

- Une action collective en justice
- La honte publique
- Des dépenses pour récupérer
- La non-conformité (violation de la norme PCI DSS, des lois Sarbanes-Oxley, GLBA, EURO-SOX, HIPAA/HITECH, UK Data Protection Act, California Senate Bill SB 1386, et bien d'autres encore)
- La perte de confiance des clients
- Une diminution des avantages concurrentiels
- Une image de marque négative
- Des conséquences financières

C'est pourquoi de nombreuses organisations se tournent vers une solution de DLP pour les aider à maîtriser leurs bases de données apparemment incontrôlées.

## Pourquoi utiliser la DLP ?

Les raisons d'envisager une solution de DLP sont nombreuses. Gartner fait remarquer dans son étude *2010 Buyer's Guide to Content-Aware DLP*[1] que les solutions de DLP sensibles au contenu offrent un éventail considérable de fonctionnalités aux organisations. Leurs principales découvertes indiquent que la DLP :

- Aide les organisations à développer, à éduquer et à mettre en œuvre des pratiques commerciales efficaces concernant l'accès, la manipulation et la transmission des données confidentielles.
- Fournit une fonction de reporting et un flux de production permettant de soutenir la gestion des identités et des accès, les initiatives de conformité réglementaire, la protection de la propriété intellectuelle et la gestion de la conformité aux politiques de données.

À eux seuls, ces deux domaines sont déjà sources de difficultés pour la majorité des sociétés. Voici d'autres domaines dans lesquels la DLP présente des avantages significatifs :

- L'assistance aux organisations dans le développement, l'éducation et l'application de pratiques commerciales efficaces concernant l'accès, la manipulation et la transmission de données confidentielles.
- L'application dynamique de politiques basées sur la classification du contenu déterminé au moment d'une opération.
- Une détection précoce, et donc une mitigation plus rapide.

De nombreuses organisations considèrent les logiciels et les matériels de DLP comme la réponse à leurs problèmes de sécurité des informations. Comme je l'ai écrit dans *DLP – A security solution, not a security savior*[2], la DLP a franchi un cap décisif au cours des dernières années. Mais en quoi consiste exactement ce remède contre les problèmes de sécurité appelé *DLP* ? La DLP fait référence à un ensemble de solutions logicielles et matérielles qui identifient, contrôlent et protègent les données, principalement grâce à l'inspection du contenu et à des analyses de sécurité contextuelles.

L'un des principaux avantages d'une solution de DLP est qu'elle est capable de détecter et d'éviter les utilisations et les transmissions non autorisées d'informations confidentielles (selon des critères définis par l'organisation). La DLP semble être une

---

[1] http://www.gartner.com/DisplayDocument?id=1421941&ref=g_sitelink
[2] http://www.btsecurethinking.com/2009/12/dlp-%E2%80%93-a-security-solution-not-a-security-savior

solution de sécurité puissante pouvant être utilisée par toutes les organisations. Cependant, bien qu'il soit important de protéger les données, mettre en place une solution de DLP ne suffit pas.

Comme indiqué au début de ce livre blanc, beaucoup d'organisations sont davantage au courant du nombre de crayons dont elles disposent dans leur stock de fournitures que de la quantité de données qui circulent sur leurs réseaux. Les outils de DLP possèdent des fonctionnalités de découverte des données et peuvent analyser les référentiels de l'entreprise et identifier les informations stockées. Il est alors possible de décider si une donnée doit être intégrée au programme de protection. Les données peuvent également être indexées de manière à pouvoir identifier leur propriétaire.

Lorsque l'on s'intéresse aux fonctionnalités de découverte des données d'un produit, l'un des principaux éléments à étudier est le nombre de types de données différents qu'il est capable d'identifier. Pas moins d'une centaine de formats de fichiers différents sont en effet utilisés au sein des entreprises : des documents Microsoft Office, des fichiers multimédia, cryptés et zippés, des codes sources, et bien d'autres encore.

**Comment surviennent les fuites de données ?**

Des fuites de données peuvent survenir de centaines de manières différentes (dont beaucoup restent un mystère pour de nombreuses organisations). Le tableau suivant en fournit une liste non exhaustive :

| | | | |
|---|---|---|---|
| Erreurs d'inattention, souvent lors de la réalisation de tâches ordinaires et répétitives | Envoi accidentel d'un e-mail à un groupe de personnes au lieu d'un seul individu | Faute de frappe | Employé(e) mécontent(e) |
| Erreur lors de la sélection d'une pièce jointe | Manque d'attention dû à la précipitation pour respecter un délai | Pression prématurée du bouton « Envoyer » | Intention malveillante |
| Espionnage d'entreprise | Sous-traitants, partenaires commerciaux, contractants, etc. avec des pratiques de sécurité médiocres | Mauvais paramétrage du pare-feu | Perte de clé USB, carte mémoire, DVD etc. |
| Perte de smartphones | Perte de cassettes de sauvegarde | Terminaux de stockage de données mal aseptisés | Hameçonnage |

| | | | |
|---|---|---|---|
| Logiciel malveillant | Transmission non sécurisée de données personnellement identifiables ou secrètes | | |

## La solution : voir plus loin que la DLP

Il est important de remarquer que, lorsqu'elles envisagent une solution de DLP, de nombreuses sociétés sont beaucoup trop naïves et pensent que la DLP fonctionne en vase clos. Les entreprises pragmatiques n'approchent pas la chose de cette manière et s'assurent d'intégrer la DLP dans leur cadre global de sécurité des informations. L'utilisation de la DLP peut être comparée à l'un des rayons de la grande roue que constitue la sécurité des informations. En l'intégrant aux autres technologies et outils, notamment à la sensibilisation et à la formation des utilisateurs finaux, la DLP peut devenir l'un des maillons très solides de la chaîne de sécurité des informations.

## Un parcours en plusieurs étapes pour atteindre le paradis de la DLP

Mais comment mettre en pratique la théorie de la DLP ? Voici quelques-unes des étapes à respecter pour protéger vos données, si vous décidez de déployer une solution de DLP :

### Étape 1 – Définition du niveau de sécurité

Gardez à l'esprit que la DLP ne résoudra pas tous vos problèmes de sécurité des données et qu'elle n'en diminuera pas non plus les risques. La DLP n'est qu'une pièce du puzzle que représente la sécurité des informations.

### Étape 2 – Localiser les données pour les protéger

Chaque année, les sociétés cotées en bourse publient leurs rapports annuels. Dans la section du bilan, elles indiquent le montant de leurs liquidités. Ces entreprises se doivent de connaître précisément cette information ainsi que d'autres détails financiers importants.

Cependant, combien de ces sociétés sont en mesure de fournir un rapport annuel sur leurs données ? Les organisations ne devraient en effet pas non plus avoir de mal à répondre aux questions suivantes : *Combien de données sont stockées sur vos réseaux ? Quelle proportion de ces données est stockée à long terme ? Archivée ?* Une organisation sur 100 sera peut-être capable de fournir des renseignements sensés sur ses banques de données.

Le principal élément à considérer est qu'il y a beaucoup trop de données en circulation dont les sociétés n'ont pas connaissance. Il est en effet impossible de protéger des informations dont une organisation ignore l'existence, le lieu de stockage et la voie de transmission.

La première étape dans la protection des données consiste donc à identifier où se trouvent les données de l'entreprise. Un projet de découverte des données vous permettra de détecter toutes les informations présentes sur votre réseau. Notez cependant qu'il s'agit d'une initiative de longue haleine. Attendez-vous donc à ce que la localisation, la schématisation et la documentation de tous vos principaux emplacements de stockage de données prennent des semaines, voire des mois.

### Étape 3 – Classification des données

Toutes les données ne se valent pas. Vous aurez donc besoin de mettre en place un projet de classification des données pour comprendre ce qui doit être protégé et pourquoi. Détaillez les dangers qu'elles représentent pour la confidentialité et dressez une liste des scénarios de risques courants pouvant survenir suite à une fuite inappropriée des données.

Envisagez la sécurité comme l'assurance de vos données, or vous devez uniquement assurer les objets de valeur. La première étape d'une initiative de DLP consiste donc à définir quelles sont vos données précieuses et sensibles.

Quelle proportion de vos données sont secrètes ? Plus que vous ne le pensez. Selon Forrester[3], les secrets représentent deux-tiers de la valeur des portefeuilles d'informations des entreprises. Malgré l'augmentation des mandats auxquels les entreprises doivent faire face, les actifs de données surveillés ne sont pas les actifs les plus précieux des portefeuilles d'informations des entreprises. Les connaissances exclusives et les secrets professionnels sont en effet deux fois plus précieux que les données surveillées. Et comme le montrent les récentes attaques subies par les sociétés, les secrets sont les cibles des voleurs.

### Étape 4 – Stratégie DLP

Une solution de DLP ne peut être déployée en vase clos. Les organisations se doivent de développer une stratégie DLP formelle qui détaille les exigences et les besoins spécifiques aux niveaux technologique et commercial. De nombreux fournisseurs positionnent leurs solutions de DLP différemment ; il est donc important que vous documentiez chacune d'elles différemment. Il est également nécessaire que vous

[3] www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf

documentiez vos exigences et que vous ne vous contentiez pas de les projeter sur l'offre de produit.

L'une des erreurs commises par beaucoup trop d'organisations est de rentrer dans les menus détails de la DLP avant d'avoir développé une stratégie de DLP de haut niveau. Commencez par définir vos objectifs clés et, seulement après, approfondissez vos exigences.

Quand vous atteignez la phase des exigences, ne perdez pas de vue que la DLP n'est pas uniquement une solution informatique. Les organisations qui ont déployé la DLP avec succès se sont appuyées sur les observations de diverses entités de la compagnie.

Bien que cette liste ne soit pas exhaustive, assurez-vous d'inclure au moins ces services dans votre approche :

- Propriétaires de l'entreprise
- Service juridique
- Audit informatique
- Service financier
- Audit interne
- Sécurité des informations
- Opérations technologiques

Notez la présence du service juridique dans la liste ci-dessus. Pour beaucoup de professionnels de l'informatique, collaborer avec ce service est un concept qui leur est totalement étranger ; cela ne devrait pourtant pas être le cas. Étant donné que la DLP inclut le contrôle des données personnelles et exclusives de l'entreprise, le service juridique de votre société devra approuver le projet de DLP pour garantir que ce contrôle n'enfreint aucune loi ni exigence. Ce point est tout particulièrement important pour les entités de l'Union Européenne, car les directives européennes sur la protection des données peuvent facilement être enfreintes avec la DLP, si les sociétés ne font pas preuve de vigilance.

Parallèlement au développement de votre stratégie, prenez en considération que la DLP nécessite de fournir des efforts sur le long terme ; comprenez : des *années* et non pas des *mois.* La DLP n'est à l'évidence pas une technologie « plug and play ». Entre le moment où vous commencez à envisager une solution de DLP et le moment où celle-ci

est totalement déployée et optimisée, il vous faudra faire preuve de patience et de dévouement.

**Que faire quand le Directeur de l'information veut une solution de DLP fonctionnelle <u>maintenant</u>, et pas l'année prochaine ?**

Vous avez sans doute remarqué que le paragraphe précédent utilise les mots *années* et *DLP* dans la même phrase. Mais qu'en est-il de ces entreprises qui ne veulent pas d'une solution de DLP complète mais plutôt d'une solution intermédiaire qui puisse être mise en place et fonctionner rapidement ? Que faire quand le Directeur de l'information rechigne face au long délai de production et insiste pour que la solution de DLP soit opérationnelle *ce trimestre,* et non pas *l'année prochaine* ?

Les solutions Secure Web Gateway and Secure Email Gateway de Clearswift constituent un complément idéal pour ceux qui souhaitent bénéficier des fonctionnalités d'une solution de DLP sans investir trop de temps et d'efforts.

Les solutions Secure Gateway intègrent, en mode natif, des fonctionnalités de DLP de base et avancées, allant du cryptage des e-mails intégré aux capacités anti-pourriels/anti-logiciels malveillants, entre autres. Les solutions Gateway ont été adoptées aussi bien par de grandes sociétés que par des petites et moyennes entreprises (PME) ayant choisi de déployer une solution de DLP pour moins de 3 000 utilisateurs.

Les passerelles de sécurité du contenu peuvent être rapidement mises en place pour mettre un terme aux problèmes de fuite de données, et leur effet positif peut être constaté en l'espace de quelques heures seulement.

De nombreuses organisations préfèrent cette approche car elle peut être rapidement mise à exécution et qu'elle offre des résultats immédiats.

Pour les organisations qui souhaitent opter pour cette approche, la première étape consiste à identifier les données en transit *aujourd'hui*, afin que les fuites accidentelles (comme la transmission involontaire de documents confidentiels) puissent être non seulement détectées par les passerelles e-mail et Internet, mais aussi évitées.

Gartner écrit dans son rapport *2010 Content-Aware Data Loss Prevention FAQs* que les entreprises devraient « développer une stratégie sur deux à trois ans pour le déploiement de leurs capacités, du contrôle initial seul au blocage effectif ». Pour les entreprises qui ne souhaitent pas attendre deux ou trois ans, Clearswift Secure Web Gateway offre un sursis appréciable.

Le rapport Gartner indique également que les organisations peuvent trouver un équilibre entre la richesse des fonctionnalités de DLP et le coût, en définissant dès le début le type et l'étendue du problème qu'elles tentent de résoudre. À partir de là, vous pouvez ensuite définir à la fois les exigences professionnelles en matière de processus technologiques et d'assistance, ainsi que la tolérance des frais opérationnels qui seront probablement nécessaires après le déploiement.

Pour finir, de nombreuses initiatives de DLP sont immédiatement rejetées quand les organisations découvrent leur coût, qui est souvent exorbitant. Dans le rapport *Budgeting the Costs of Content-Aware DLP Solutions,* Gartner indique que le prix moyen d'une solution de DLP complète varie de 350 000 $ à 750 000 $. Les passerelles Clearswift Secure Gateway sont disponibles pour une fraction de ce prix.

Alors, pourquoi faut-il un an ou plus pour déployer intégralement une solution de DLP ? Cela est dû au fait que l'une des autres erreurs commises par les organisations est de tenter de conserver l'anarchie de leurs données et de la gérer telle quelle grâce à la DLP. Pour que la DLP soit opérationnelle, il est nécessaire de progresser par petites étapes au début, puis d'évoluer par la suite. De nombreux projets informatiques échouent à cause d'ambitions initiales trop importantes. Commencez donc petit, obtenez vos premières victoires et réussites, puis continuez à progresser.

Au début du projet, commencez par les données les plus critiques et les plus sensibles, telles que les données confidentielles, les ordinateurs portables et les terminaux mobiles. Une fois cet aspect réglé, attaquez-vous à d'autres systèmes et à ceux contenant moins de données cruciales. La plupart des organisations possèdent beaucoup trop de données pour pouvoir tout sécuriser d'un seul coup avec la DLP.

Puisque nous venons de mentionner les ordinateurs portables, remarquez que, bien qu'ils constituent d'excellents outils de productivité, ce sont également les instruments les plus utilisés dans le monde du vol et des fuites de données au monde. Leur niveau de commodité et d'accessibilité est en relation directe avec la quantité de données pouvant être compromise. Un fervent adversaire pourra en effet choisir de prendre pour cible l'ordinateur portable d'un cadre ou d'un dirigeant pour accéder au trésor de données qu'il contient.

Il est important de signaler que cette étape n'a rien à voir avec les fournisseurs, qui entrent en jeu à l'étape 5. Votre stratégie DLP « de grande écoute » devrait en effet être complète avant de vous engager auprès d'un fournisseur de DLP.

De nombreux projets de DLP perdent parfois des financements entre le stade de la stratégie et le stade du déploiement. Afin d'obtenir un meilleur soutien de la direction et une meilleure justification commerciale pour le projet, il pourrait s'avérer judicieux de déterminer le nombre de violations de la DLP. Présenter des chiffres à la direction, tels que le nombre de cartes bancaires ou de numéros de sécurité sociale mis en quarantaine, est un excellent moyen de prouver les mérites de la technologie de DLP.

Au final, pour ceux qui envisagent sérieusement d'adopter une stratégie DLP, le rapport Gartner *Develop an Enterprise Strategy for Data Loss Prevention*[4] contient beaucoup d'informations précieuses et peut donc être utilisé comme guide.

### Étape 5 – Sélection, test et déploiement du produit

Une fois les exigences documentées, l'étape suivante consiste à créer un pilote pour essayer plusieurs produits de DLP. Assurez-vous de tester plusieurs cas d'utilisation

[4] http://www.gartner.com/DisplayDocument?id=1383713

pour analyser le produit dans différents scénarios. Utilisez des mesures spécifiques et objectives pour garantir que les contrôles des valeurs sont testés et que vos résultats sont justes.

## Conclusion

D'un point de vue général, la DLP constitue une excellente technologie de sécurité, mais ce n'est pas pour autant une formule magique qui pourra sécuriser votre réseau comme par miracle. Les étapes indiquées ici ne sont qu'un échantillon de toutes celles que vous devrez suivre pour procéder à une installation formelle de la DLP dans votre entreprise. En envisageant la DLP selon cette approche tactique, vous pouvez être sûrs qu'elle empêchera réellement la perte de vos données.

Pour de nombreuses organisations, une solution de DLP de type entreprise peut paraître excessive. Étant donné les frais et les efforts que cela implique, beaucoup d'organisations trouvent plus judicieux sur le long terme de débuter par la solution Clearswift Secure Gateway, qui offre des avantages à court terme et un succès intermédiaire immédiat.

C'est après avoir complètement déployé des solutions Secure Web Gateway and Secure Email Gateway fonctionnelles que ces organisations décident d'envisager un progiciel de DLP complet.

## À propos de l'auteur…

Ben Rothke, CISSP, CISM, CISA est un consultant senior en sécurité travaillant à New York pour BT Professional Services. Il possède 15 années d'expérience professionnelle dans la sécurité et la confidentialité des systèmes d'information.

Ses domaines d'expertise sont la gestion et la mitigation des risques, les problèmes réglementaires en matière de sécurité et de confidentialité, la conception et la mise en place de la sécurité des systèmes, le cryptage, la cryptographie et le développement de politiques de sécurité, avec une spécialisation dans les services financiers et le secteur de l'aviation.

Auteur de *Computer Security - 20 Things Every Employee Should Know* (McGraw-Hill), Ben rédige également une critique littéraire mensuelle sur les livres traitant de sécurité pour le magazine *Security Management*. Il intervient aussi régulièrement lors de congrès professionnels, tels que les conférences CSI, RSA et MISTI, possède de nombreuses certifications professionnelles, et est membre d'ASIS, de la CSI, de la Society of Payment Security Professionals et d'InfraGard.