DLP ou IRM ?

Quelle solution choisir pour protéger mes données sensibles ?

Chaque organisation génère et gère, dans une mesure plus ou moins grande, des informations sensibles stockées dans différents emplacements : ordinateurs des utilisateurs, gestionnaires de documents, stockage en nuage, serveurs de fichiers, etc.

D'une part, les organisations doivent prévenir les menaces internes : informations extraites par les employés qui quittent l'organisation, perte d'informations par le biais de fournisseurs ou de la chaîne logistique, etc. De nombreuses organisations pensent que ce problème concerne uniquement les grandes agences gouvernementales et autres entités gérant plusieurs informations, mais ce type de fuite est un problème plus grave que ne le pensent la plupart des entreprises, mais aussi l'un des types de fuites générant plus de coûts pour les organisations, selon le Ponemon Institute.

En outre, les organisations sont soumises à des réglementations en matière de protection des données telles que le règlement UE-GDPR, le PCI dans le secteur financier, etc. Souffrir d'une fuite de données ou enfreindre l'une de ces réglementations peut être très coûteux pour une organisation, comme l'a démontré les récents cas de British Airways (183 M £) et de Marriott (99 M £) qui ont entraîné la perte/le vol de données de millions d'utilisateurs.

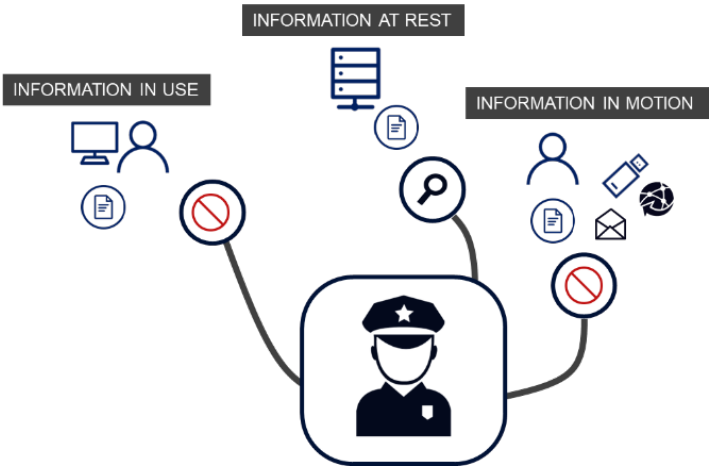
Face à ce problème, de nombreux RSSI ou DSI doivent choisir les technologies à utiliser pour éviter ou atténuer une éventuelle fuite de données sensibles. Deux des technologies généralement prises en compte sont la prévention de la perte de données (Context-Aware Data Loss Prevention) et la gestion des droits de l'information (IRM).

Cet article explique comment les deux technologies peuvent aider à prévenir les fuites de données, exposent leurs différences et démontrent comment elles peuvent se compléter.

DLP – DATA LOSS PREVENTION / DATA LEAK PREVENTION

Une solution DLP permet de prévenir la fuite ou la perte de données sensibles de différentes manières. D'une part, lorsque les données sont en stockage, en analysant les serveurs de fichiers, les points de terminaison, etc., et en localisant ou en classant les données sensibles. Également en transit, lorsque la documentation ou des données sensibles sont acheminées sur le réseau, vers des périphériques amovibles, etc. Enfin, lorsque les données sont en cours d'utilisation, elles contrôlent si un utilisateur du réseau d'entreprise y a accès ou non. Habituellement, les pirates essaient de trouver des données personnelles, financières, de propriété intellectuelle, de données et autres sur la base de dictionnaires préétablis.

Une DLP agit comme un "policier" situé à la sortie du réseau, sur les ports de l'ordinateur qui vérifie ce qui tente de quitter et qui tente de l'extraire du réseau.



Bien qu'il s'agisse d'une technologie extrêmement puissante, elle doit surmonter d'importants problèmes de protection des données sensibles :

- Comment peut-il déterminer efficacement ce qui peut partir et ce qui ne peut pas ?
- Est-il possible de "fermer" efficacement tous les points de sortie possibles des données de l'entreprise ou de les contrôler ?
- Puis-je contrôler tous les types de périphériques de l'entreprise, y compris les téléphones mobiles, le cloud, etc. ?
- Et si quelque chose quittait le réseau et échappait au contrôle de ce « policier » ? Puis-je restreindre l'accès ?

Les solutions DLP traditionnelles ne peuvent qu'examiner ce qui essaie de partir et décider de le laisser ou non. C'est un processus binaire. Cependant, les situations quotidiennes ne sont pas « binaires ». En effet, il est très difficile pour un professionnel de l'informatique de définir des politiques décrivant les exigences en matière de données quittant l'organisation de manière efficace sans générer un certain nombre de « faux positifs ». Si les données ou les informations ne sont pas classées, il est difficile de répondre efficacement.

C'est pourquoi, dans de nombreux cas, il est d'abord nécessaire de classer ou de cataloguer les données, en indiquant au DLP les référentiels à analyser et en déterminant ce qui est confidentiel et ce qui ne l'est pas. Cela nécessite que le service informatique déploie des efforts considérables lors de la configuration, de la classification et de la gestion des règles du DLP afin de les affiner suffisamment et de générer le nombre minimum de faux positifs. Cependant, il est important de garder à l'esprit qu'il est difficile pour un service informatique de déterminer ce qui est confidentiel et ce qui ne l'est pas. Les utilisateurs qui travaillent quotidiennement avec ces données sont ceux qui savent vraiment ce qui est important et qui doivent être protégés et ce qui ne l'est pas.

D'autre part, une autre question se pose : que se passe-t-il avec les documents une fois qu'ils ont été distribués ? En effet, une fois que les données sont en dehors de l'organisation, rien n'empêche les destinataires de les transmettre à des utilisateurs non autorisés, de les sauvegarder sur des clés USB, etc. Cela s'applique également aux appareils mobiles, où l'approche de la protection tend à être "tout ou rien". Les entreprises délèguent souvent le contrôle des données sur les appareils mobiles aux applications MDM afin d'empêcher que certaines données ne soient ouvertes en dehors d'applications d'entreprise ou contrôlées.

En exigeant une gestion affinée des stratégies et de la classification, les entreprises commencent généralement par une phase de « surveillance » afin de détecter le type de données quittant le réseau, avant de passer à une phase de « blocage ». Si la stratégie est affinée, le contrôle des données sortantes sera efficace et les processus de blocage ne généreront pas de faux positifs. Sinon, le bruit généré dans l'organisation en raison du blocage de données qui devraient être accessibles ou être envoyées peut être important.

Pour résumer, les outils DLP sont très puissants et peuvent classer, surveiller et bloquer la sortie des données sensibles du réseau, mais les efforts nécessaires pour les mettre en œuvre, les affiner et éviter les faux positifs ne doivent pas être sous-estimés. Enfin, bien qu'ils protègent le « périmètre » du réseau, les données peuvent être transférées n'importe où.

IRM – INFORMATION RIGHTS MANAGEMENT

Cette technologie, dans le cadre de Data-Centric Security, permet d'appliquer une forme de protection aux fichiers qui accompagnent les fichiers, où qu'ils soient. Il est également connu sous le nom de E-DRM (Gestion des droits numériques d'entreprise) ou EIP & C (Protection et contrôle de l'information d'entreprise). Il permet de contrôler qui accède aux fichiers, quand ils le font, et si les fichiers sont à l'intérieur ou à l'extérieur de l'organisation. Les autorisations peuvent également être restreintes sur les documents (lire, éditer, imprimer, copier et coller, etc.). Vous pouvez révoquer l'accès aux fichiers en temps réel si vous ne souhaitez pas que certaines personnes y accèdent à nouveau.

Lorsque vous envoyez un document à une tierce personne, il peut avoir été imprimé en 3 minutes, envoyé à 5 autres personnes qui à leur tour l'ont envoyé à 10 autres et y ont apporté des modifications. Nous ne possédons le document qu'au moment de le créer, mais une fois partagé, le document cesse d'avoir un propriétaire et le destinataire peut en faire ce qu'il veut. C'est l'un des problèmes que cette technologie essaie de résoudre : garantir qu'un utilisateur continue d'être le propriétaire des données, quelle que soit la personne avec laquelle elles ont été partagées.

Tenant compte de la difficulté de déterminer le périmètre du réseau d'entreprise, l'IRM applique une couche de protection aux données pouvant être contrôlées même si elles ne font plus partie du réseau, que ce soit sur le Cloud, sur un appareil mobile, etc...

Si les données parviennent à une personne qui, à votre avis, ne devrait pas y avoir accès, vous pouvez révoquer l'accès à distance. Vous pouvez également définir des dates d'expiration pour les documents, accorder plus ou moins d'autorisations aux utilisateurs, et ce, en temps réel (avant ou ils ne pouvaient que lire, ou restreignez les autorisations en lecture seule si nous ne voulons pas qu'elles soient éditées ou imprimées).

Un des avantages de ce type de solution est la facilité avec laquelle elle peut être mise en œuvre. En effet, elle est rapidement et facilement utilisable. En effet, vous pouvez utiliser l'IRM efficacement dès le premier jour : vous pouvez rapidement chiffrer et contrôler les données sensibles que l'entreprise gère en interne ou avec des tiers.

L'un des principaux défis de cette technologie est de faciliter son utilisation par les utilisateurs qui peuvent ainsi gérer des données protégées presque comme s'il s'agissait de données non protégées mais aussi de la rendre compatible avec les applications que les utilisateurs utilisent régulièrement, telles que Office, Adobe, AutoCAD ou avec les référentiels d'informations habituellement utilisés par les entreprises : serveurs de fichiers, SharePoint, applications Office 365 Cloud, G-Suite. , Boîte, etc.

Un autre défi des solutions IRM est la protection automatique : c'est-à-dire la protection des données indépendamment de la décision de l'utilisateur de le faire. Dans ce cas, la protection automatique des dossiers sur les serveurs de fichiers ou des gestionnaires de documents est particulièrement utile.

À cet égard également, l'intégration à un outil DLP peut être très utile et offrir la combinaison parfaite.

COMMENT L'IRM COMPLÈTE LA DLP ?

Comme mentionné, l'administrateur peut établir des règles pour identifier les informations sensibles à l'aide de l'outil DLP. Une fois détecté, en stockage, en transit ou en cours d'utilisation, l'administrateur peut appliquer une action corrective telle que la création d'un journal, le blocage de l'accès, la suppression du fichier, etc.

Grâce à l'intégration à l'IRM, la solution DLP peut établir la protection automatique du fichier en tant qu'action corrective à l'aide d'une stratégie de protection IRM. Par exemple, si un nœud final ou un dossier réseau est numérisé et que des données de carte de crédit, des informations personnelles, etc. sont détectées dans les documents, le DLP peut s'assurer que ces données soient automatiquement protégés par une stratégie d'«utilisation interne», de sorte que seules les personnes en contact avec le domaine ou certains départements peuvent y accéder.

Quels sont les avantages ?

- Les documents sensibles peuvent se protéger sans recourir à l'action de l'utilisateur.
- Ceux-ci seront protégés, qu'ils soient transférés à l'intérieur ou à l'extérieur du réseau d'entreprise.
- Vous pouvez surveiller leur accès indépendamment de l'endroit où ils se trouvent.
- Vous pouvez révoquer l'accès aux données sensibles même si elles se trouvent en dehors de l'organisation.

SealPath peut protéger les informations facilement et efficacement en s'intégrant aux principales solutions DLP du marché telles que ForcePoint, McAfee ou Symantec, ce qui facilite ainsi la protection des données sensibles dans l'organisation et son contrôle, où qu'elles se trouvent.

SealPath se concentre sur la création de la meilleure expérience utilisateur, en s'intégrant aux outils de travail normaux de l'utilisateur, en proposant un produit spécialement conçu pour les grandes entreprises et intégré à une multitude de systèmes d'entreprise, tels que DLP, SIEM, Office 365, SharePoint, G-Suite et Alfresco, OneDrive, etc.

Souhaitez-vous voir une démonstration de l'intégration de SealPath avec les DLP ? **Contactez-nous ici**.