WHITEPAPER

ETES VOUS EN TRAIN DE PROFITER AU MAXIMUM DE VOTRE STRATEGIE DE CLASSIFICATION ?

COMENT AUTOMATISER LA PROTECTION DES DONNEES CLASSIFIEES

INTEGRATION DE SEALPATH AVEC LES OUTILS DE CLASSIFICATION

Dans les organisations, de plus en plus de documentation est gérée et stockée en format numérique sur les serveurs de fichiers, les gestionnaires de documents, les ordinateurs et appareils d'utilisateurs, etc. Une bonne partie de cette documentation est sensible et peut comprendre, selon l'industrie, la propriété intellectuelle, les données personnelles des clients, des partenaires, des employés ou des renseignements financiers tels que les données de carte de crédit.

Plus nous stockons d'informations, plus le risque de ne pas être contrôlé augmente et que les personnes sensibles ou soumises à des règlements sur la protection des données sont divulguées et peuvent causer un incident grave de perte de données. Le risque augmente également en augmentant le nombre d'emplacements où nous pouvons l'avoir comme (serveurs, mobiles, ordinateurs portables, etc.) et en utilisant de plus en plus de moyens de communication (email, systèmes de partage de nuages, soumissions de fichiers, outils Slack, Microsoft Teams, etc.).

FONCTIONNEMENT D'UN OUTIL DE CLASSIFICATION DE L'INFORMATION

L'un des objectifs des solutions de classification de l'information est d'identifier la valeur commerciale dans les données structurées au moment de la création du contenu, ou une fois qu'elles sont stockées. Ils permettent de séparer les informations qui sont publiques ou moins pertinentes pour l'entreprise de ce très sensible et dont la filtration ou la perte peut causer des problèmes à la documentation.

Les solutions de classification divisent l'information en groupes ou catégories prédéfinis qui partagent un risque commun. Ces groupes doivent avoir des contrôles de sécurité et des contraintes connexes. Plus de restrictions ou de contrôles, plus la documentation pour l'entreprise est sensible et précieuse. Les outils de classification favorisent une culture de protection qui sensibilisent les utilisateurs au niveau de sensibilité des données qu'ils gèrent (en mettant des marques visuelles indiquant que ce qui est géré est confidentiel, l'utilisation interne, etc.).

ÉTAPES D'UNE STRATÉGIE DE CLASSIFICATION DE L'INFORMATION

Une stratégie de classification des données passe par ces différentes étapes :

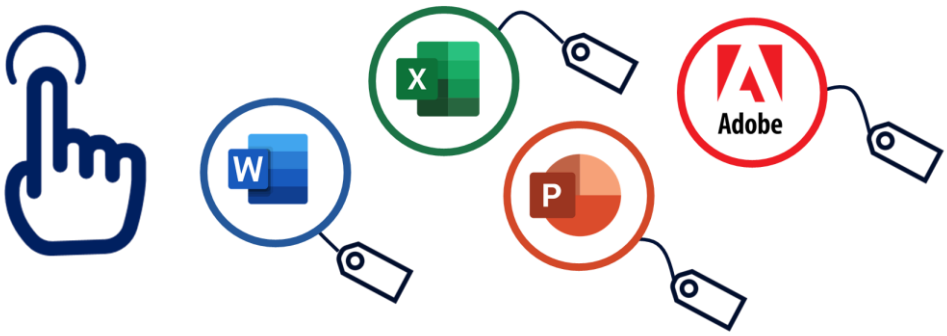
- **Définir les niveaux de classification pour les informations d'entreprise :** Parmi les plus couramment utilisés, ci-dessus : *Public, Internal Use, Confidential and Restricted* or *Top Secret*. Vous pouvez également créer des sous-catégories : Données financières, données personnelles, etc.

- **Découvrez où se trouvent les données d'organisation sensibles :** ici, vous pouvez lire des outils « Data Discovery » ou DLP qui identifient où nous stockons des documents avec certains contenus (mots clés, données financières, etc.).

- **Classification des données :** Cela peut se faire au moyen d'outils manuels, ce qui amène les utilisateurs à classer les données, ou des outils automatiques plus sujets aux faux positifs (par exemple, un DLP).

FONCTIONNEMENT DES OUTILS DE CLASSIFICATION

Les outils de classification modifient les métadonnées des fichiers Office, des fichiers PDF, etc. pour les étiqueter avec un certain niveau de classification (confidentiel, etc.). Grâce à des plugins dans Office, Outlook, ces métadonnées sont interprétées pour montrer visuellement aux utilisateurs le niveau de classification qui a été appliqué à un document donné.



EST-IL VRAIMENT EFFICACE DE CLASSER L'INFORMATION PAR ELLE-MÊME ?

Les outils de classification sont un moyen d'atteindre enfin un objectif : prévenir ou minimiser les fuites d'informations. Le moyen est d'étiqueter pour sensibiliser l'utilisateur à l'importance des données qu'il gère, mais la fin est perdue si les mécanismes de contrôle et de protection ne sont pas inclus pour empêcher la perte de ces données précédemment classifiées.

À lui seul, un outil de classification ne protège pas ou n'empêche pas l'accès à celui-ci lorsque les informations gérées sont sensibles. Ils exigent des technologies **IRM (Information Rights Management) / E-DRM (Enterprise Digital Rights Management)** telles que SealPath ou **DLP (Data Leak Prevention)** pour prévenir ou minimiser la perte d'informations sensibles.

Nous pouvons trier des informations sensibles pendant des années et les faire bien cataloguer, ou utiliser les outils de découverte des données pour nous dire quel type de données nous avons dans l'organisation ou dans quels dépôts nous avons des données financières, personnelles, etc. Nous pouvons investir dans des processus complexes pour déterminer comment classer certaines informations en fonction du risque, mais tous ces efforts seront à moitié cuits s'il n'y a finalement pas de stratégie efficace de protection de l'information par le biais de solutions DLP ou DLP.

COMMENT SEALPATH S'INTÈGRE-T-IL AUX SOLUTIONS DE CLASSIFICATION DE L'INFORMATION ?

Comme nous l'avons vu, lorsqu'un utilisateur classe un document au moyen d'une solution de classification, le document modifie les métadonnées de fichiers pour enregistrer le niveau de classification sélectionné. C'est le cas à la fois des solutions de classification manuelle et des solutions de classification automatiques basées sur le DLP.

SealPath est en mesure d'accéder aux métadonnées des fichiers et d'interpréter le niveau de classification. Cela est vrai, tant dans les documents consultés par les utilisateurs que dans les documents stockés sur les serveurs de fichiers, ou les gestionnaires de documents.

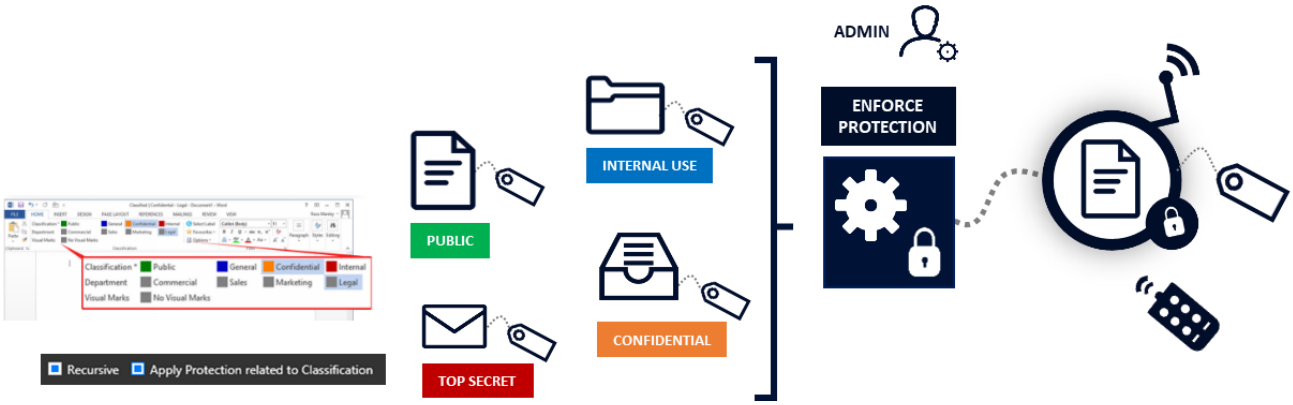
L'administrateur SealPath par l'intermédiaire du *SealPath Metadata Classifier Manager* vous permet de rejoindre les stratégies de protection SealPath avec des balises de classification. De cette façon, vous pouvez, par exemple, marquer "Utilisation interne" une stratégie de protection SealPath où seuls les utilisateurs internes du domaine ont accès à la vue et à la modification de la documentation.

Une fois que l'étiquette de classification et la politique de protection de SealPath sont liées, les fichiers classés avec ces balises seront automatiquement protégés dans les situations suivantes :

- Lorsqu'un utilisateur classe le document, par exemple étiqueté « Utilisation interne », le document est protégé au moment de la fermeture par SealPath avec la politique de protection assignée par

l'administrateur. L'utilisateur n'a qu'à classer le document et SealPath effectue automatiquement une protection pour celui-ci.

- Lors de la surveillance avec SealPath pour les serveurs de fichiers certains dossiers sur un serveur de fichiers, ou sur un ordinateur utilisateur, si un document classifié étiqueté "Utilisation interne" est détecté, il sera automatiquement protégé. Dans ce cas, nous devons avoir configuré SealPath pour les serveurs de fichiers pour protéger en fonction des niveaux de classification et non sur une politique de protection particulière.



QUELS AVANTAGES BÉNÉFICIEZ-VOUS DE CETTE INTÉGRATION ?

SealPath apporte les avantages suivants pour les organisations qui ont investi ou investissent leur efforts pour que l'information soit bien cataloguée :

- Atteindre l'objectif ultime d'une stratégie de classification, la protection des données afin de minimiser la perte d'information, car nous serons en mesure d'appliquer des contrôles de sécurité restrictifs sur les types d'informations qui sont particulièrement sensibles.

- Automatiser la protection en fonction du niveau de classification sans avoir à intervenir l'utilisateur pour protéger le document. L'utilisateur n'a qu'à classer le document.

- Tirer le meilleur parti des outils de classification non seulement manuel, où l'utilisateur est celui qui classe la documentation, mais automatique où, par exemple, un DLP étiquette la documentation avec un certain niveau dans le processus de découverte de informations sensibles.

- Laissez les documents les plus sensibles voyager avec une protection persistante pour vous accompagner où que vous voyiez, même si vous avez quitté le périmètre de l'entreprise. Le DLP sera également en mesure d'appliquer des règles pour empêcher les informations classées comme confidentielles de partir, mais si nous ne voulons pas gérer des règles complexes dans le DLP, sujettes à de faux positifs, nous saurons toujours qu'une fois que l'information est protégée par SealPath sera sous le contrôle de l'entreprise.

- Vérifier l'utilisation d'informations sensibles où que vous voyiez : Savoir qui a accédé, si quelqu'un a essayé d'y accéder sans autorisation, etc.

- Révoquez l'accès au document à certaines personnes internes ou externes à l'organisation lorsque vous en avez besoin et en temps réel. Le fichier peut toujours être classé de la même manière, mais vous pouvez décider en temps réel qui peut accéder et qui ne peut pas.

- Gérer la protection de grands volumes d'informations sur les serveurs de fichiers qui ont déjà été classés manuellement ou automatiquement. SealPath pour les serveurs de fichiers traversera ces dépôts et protégera les fichiers si le niveau de sensibilité de l'information est élevé.

INTÉGRATION AVEC TOUS LES OUTILS DE CLASSIFICATION MANUELS OU AUTOMATIQUES

SealPath a une approche "agnostique" avec les outils de classification existants sur le marché étant en mesure de s'intégrer avec *Boldon James, Titus, Microsoft AIP, Tukan IT, Janus,* etc. Bien qu'avec certains d'entre eux, il fonctionne sur la base d'API, être en mesure d'interpréter les métadonnées des fichiers peuvent automatiquement protéger les informations classifiées par ces outils.

D'autre part, il permet également l'intégration avec des outils de tri automatiques qui fonctionnent avec des métadonnées de fichiers telles que *McAfee DLP*. Aussi avec d'autres DLP tels que *ForcePoint* ou *Symantec* qui, bien qu'ils ne modifient pas les métadonnées des fichiers, permettent d'appliquer des mesures d'assainissement en raison d'une violation d'une politique de sécurité (par exemple. Détecter les données de carte de crédit sur certains documents).

En bref, avec une stratégie de protection basée sur les métadonnées, SealPath permet une intégration facile avec n'importe quel outil de classification permettant aux organisations d'empêcher efficacement les organisations de divulguer des données d'information classés comme sensibles.

Si vous avez des informations classifiées ou certaines métadonnées que vous souhaitez protéger, SealPath est la solution idéale pour configurer l'accès aux données sensibles.

Avec SealPath, vous pouvez appliquer des contrôles efficaces à vos données pour atténuer les fuites d'informations potentielles à l'intérieur et à l'extérieur de votre organisation. Pour en savoir plus, rendez-vous sur www.sealpath.com ou envoyez un courrier à sales@sealpath.com.