Forcepoint | SECLORE

Présentation succincte

Seclore pour Forcepoint DLP

Le défi

- DLP peut empêcher les données sensibles de sortir de l'entreprise, ou bien les surveiller après qu'elles en soient sorties. En bloquant les données lors de leur sortie, les flux de productivité sont interrompus, tandis que la surveillance les envoie à l'extérieur sans protection et les laisse se défendre seules.

La Solution

- Ajout automatique de contrôles d'utilisation persistants et granulaires aux données découvertes.
- Attribution et révocation dynamiques et instantanées des autorisations de fichiers
- Attribution et révocation dynamiques et instantanées des autorisations de fichiers
- Sécurisation des données des terminaux, sur le réseau, ou dans le courriel.
- Récupérez des informations d'analyse de l'utilisation des données

Résultat

- Accélérez les déploiements DLP pour réduire les coûts et augmenter la rentabilité.
- Réduisez considérablement les faux positifs afin de diminuer les surcoûts administratifs.
- Autorisez une collaboration interne et externe ininterrompue
- Maintenez le contrôle et le suivi des données sensibles lorsqu'elles quittent l'organisation.
- Respectez les audits et la conformité réglementaire

Data Loss Prevention (DLP) permet de détecter les données sensibles et éviter qu'elles ne s'échappent de votre réseau. Cependant, que se passe-t-il après la découverte des données ? Que faire de tous ces incidents ? Comment sécuriser la collaboration avec des partenaires commerciaux externes ou des tiers, lorsque les courriels sont bloqués sur le terminal ou envoyés sans protection ? Comment protéger les fichiers partagés via le cloud, ou consultés par des prestataires externes sur des appareils mobiles ? Comment récupérer des données sensibles lorsqu'elles tombent dans de mauvaises mains ?

Seclore Rights Management et Forcepoint DLP

DLP peut inspecter le contenu des documents et y découvrir des données sensibles. En détectant les données sensibles, vous pouvez, à votre tour, ajouter automatiquement les contrôles d'utilisation (droits) appropriés aux documents et à l'interaction avec les données. En intégrant Seclore Rights Management, vous avez un contrôle total sur vos informations – y compris la capacité de révoquer entièrement l'accès – même au-delà du périmètre de votre entreprise. Dès que Forcepoint DLP découvre des données sensibles, Seclore peut les protéger instantanément avec les politiques d'utilisation appropriées. Les contrôles d'utilisation des données persistants et granulaires de Seclore résident avec le fichier, où qu'il aille, à l'intérieur ou à l'extérieur de l'entreprise, et protègent les données en cours d'utilisation (fichiers sur lesquels on travaille), en transit (envoyés par courriel) et au repos (tout format de fichier, tout appareil, tout système d'exploitation).

L'union fait la force

Seclore Rights Management vous aide à passer d'une posture de sécurité « réactive » à une posture « proactive » lorsque vous utilisez Forcepoint DLP. Traditionnellement, la protection DLP est configurée en mode « surveillance », fournissant des tableaux de bord, des rapports et des alertes, qui permettent un suivi des informations qui quittent l'entreprise. Le mode de surveillance est une application DLP standard. Toutefois, le problème de sécurité réside dans le fait que les données sensibles quittent l'entreprise. Si vos données sensibles tombent entre les mains d'un acteur nocif ou si vous devez les récupérer auprès d'un tiers, vous devez vous lancer à la poursuite de vos données sensibles. Avec Seclore, vous avez le contrôle en permanence.

Seclore Rights Management accélère également de manière significative le déploiement de Forcepoint DLP. Si vous n'êtes pas sûr de la règle à appliquer aux informations découvertes : bloquer, mettre en quarantaine, autoriser, etc., la protection automatique des informations avec Seclore peut devenir votre action par défaut. En outre, elle élimine les configurations en cours.

DLP Découvre

- → Analyse du contenu
  - Mot-clés
  - Modèles
  - Empreintes numériques
  - Reconnaissance optique de caractères (OCR)
- → Empêche les informations sensibles de quitter le périmètre de l'entreprise
- → Enregistre les incidents survenant dans l'entreprise

Rights Management Protège

- → Sécurise les contenus
  - Contrôles d'utilisation granulaires
  - Précise qui peut accéder à quoi, où, quand et comment.
  - Limite et révoque l'accès
  - Données en cours d'utilisation, en transit et statiques
- → Permet aux utilisateurs externes autorisés d'accéder à des informations sensibles
- → Suivi et audit des données à l'intérieur et à l'extérieur de l'entreprise.

En combinant Seclore RM et Forcepoint DLP, vous pouvez contrôler qui peut accéder au document, ce qu'il peut en faire, quand et à partir de quels ordinateurs ou appareils l'accès est autorisé. En ajoutant des contrôles d'utilisation persistants et centrés sur les données, le champ d'application de Forcepoint DLP peut être étendu aux documents qui transitent par des réseaux publics et partenaires, qui sont stockés sur le cloud ou sur des services de partage de fichiers, ou auxquels on accède sur des appareils mobiles.

Protection instantanée : Sur les terminaux, sur le réseau ou dans le cloud.

Les données sensibles découvertes lors des analyses de Forcepoint DLP – sur les terminaux, sur le réseau ou dans le cloud – peuvent être instantanément protégées par Seclore Rights Management. Par exemple, les politiques de protection Seclore peuvent être mises en relation avec la découverte de mots-clés sensibles ou d'expressions régulières (p. ex. les numéros de cartes de crédit). Les contrôles d'utilisation garantiront qu'aucun utilisateur en dehors du service concerné (et encore moins hors de l'organisation) ne pourra utiliser ce document, même s'il lui est envoyé. Avec Forcepoint DLP, la protection s'étend encore plus loin, tirant parti d'empreintes d'identité précises pour reconnaître les données sensibles où qu'elles résident, comme sur les serveurs de fichiers, ou lorsque ces données sensibles sont distribuées par les utilisateurs, ce qui aide les administrateurs à concentrer leur attention sur les utilisateurs et les comportements les plus risqués.

De plus, cette protection est quasi immédiate et totalement automatique. L'application automatisée des contrôles d'utilisation basés sur les politiques de découverte DLP n'entraîne aucune étape supplémentaire pour les employés, moins de coûts de formation et moins d'efforts de gestion des changements.

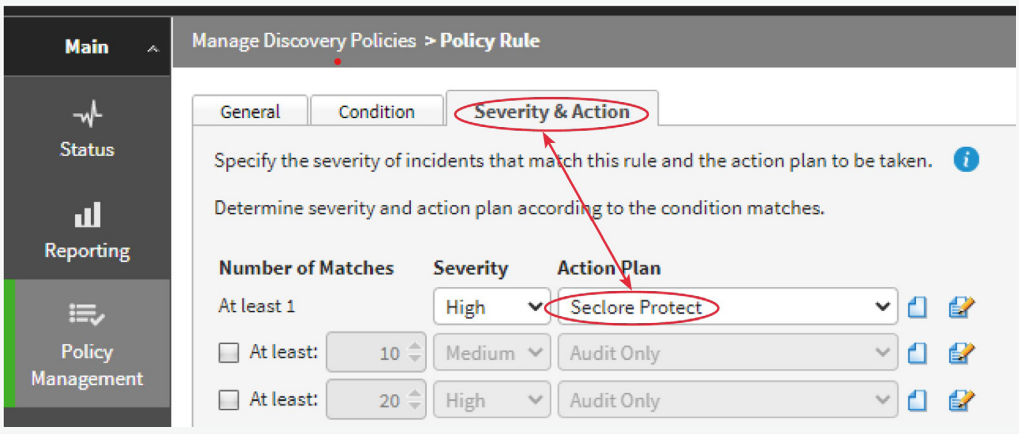

Figure 1 : Les résultats de la découverte sont automatiquement mis en relation avec la politique de protection.

Seclore Rights Management et Forcepoint DLP pour terminaux

Forcepoint DLP peut analyser les documents et découvrir les données confidentielles se trouvant sur les terminaux du réseau. Forcepoint DLP peut faire correspondre des mots-clés (p. ex. des projections de revenus), des modèles et des expressions régulières (p. ex. des numéros de cartes de crédit) et peut également examiner des répertoires spécifiques ou rechercher des documents de formats particuliers. Après la découverte, Seclore sécurise ces informations sensibles, en appliquant la politique Seclore pertinente pour empêcher leur fuite ou leur mauvaise utilisation, sur la base des définitions des politiques définies par l'administrateur de l'organisation. Avec Forcepoint DLP, vous pouvez étendre la portée des politiques réseau aux appareils hors réseau et appliquer des politiques au niveau des terminaux individuels, pour que les données soient protégées même avec les utilisateurs distants.

Avantages

- → Protection automatisée des informations sensibles, dans ou en dehors du réseau
- → Réduction de la dépendance vis-à-vis des utilisateurs pour la protection des données sensibles
- → Une protection qui reste avec le fichier – qu'il soit en stockage, en transit ou en cours d'utilisation

1 Un utilisateur sauvegarde ou copie un document contenant des données sensibles sur son ordinateur local.

2 Forcepoint DLP découvre des données sensibles sur un document du terminal – soit lors d'une analyse planifiée, soit lors d'une analyse en temps réel. En cas d'infraction à la politique, la politique d'utilisation pertinente de Seclore est d'application.

3 Chaque fois que le document est ouvert, où que ce soit dans le monde, la protection Seclore reste en vigueur. Toutes les opérations effectuées sur le document sont enregistrées et centralisées en temps réel.

Figure 2 : Découverte sur les terminaux

Seclore Rights Management et Forcepoint DLP Network

Forcepoint DLP analyse les documents sensibles résidant dans les serveurs de fichiers. Il est essentiel de protéger les données qui sont déplacées dans l'entreprise et hors de son périmètre. Avec DLP Network, sécurisez les données en cours d'utilisation en surveillant les flux de données via les canaux de communication tels que le courriel et le Web. Seclore étend la protection en sécurisant les informations sensibles pour éviter leur fuite ou une mauvaise utilisation.

1 Un utilisateur crée ou copie un document contenant des données sensibles...

2 ... et l'enregistre dans un dossier de partage réseau.

3 Forcepoint DLP découvre les données sensibles dans ce document, soit lors d'une analyse planifiée, soit lors d'une analyse en temps réel. En cas d'infraction à la politique, la politique d'utilisation pertinente de Seclore est d'application.

4 Chaque fois que le document est ouvert, où que ce soit dans le monde, la protection Seclore reste en vigueur. Toutes les opérations effectuées sur le document sont enregistrées et centralisées en temps réel.

Figure 3 : Découverte sur le réseau

Seclore Data Classification et Forcepoint DLP

Seclore Data Classification – par Boldon James – fonctionne avec Forcepoint DLP pour réduire les faux positifs lors de la découverte de données.

- → **Un utilisateur classe** un document Office, par exemple, en cliquant simplement sur une étiquette de classification qui se trouve dans le ruban Office.
- → **Forcepoint DLP marque** le document selon la classification choisie.
- → **Seclore Rights Management protège** le document avec la politique d'utilisation adéquate. Chaque fois que le document est ouvert, où que ce soit dans le monde, la protection Seclore reste en vigueur.
- → **La prise d'empreintes de Forcepoint** permet de découvrir quand des extraits du document sont copiés, collés ou modifiés, de sorte que l'exfiltration de données peut être détectée et empêchée.
- → Toutes les opérations effectuées sur le document sont enregistrées et centralisées en temps réel. Comme la classification du document est choisie par l'utilisateur, les **chances de faux positifs sont pratiquement nulles.**

Seclore Automatic Email Protection avec Forcepoint Email Security

DLP Email Security est le plus souvent exécuté en mode découverte, en raison du risque de faux positifs. Toute découverte d'un comportement anormal de l'utilisateur n'intervient qu'après coup. Pour les données qui doivent sortir du réseau à fins professionnelles, il n'y a pas d'autre choix que de laisser les courriels circuler sans aucune protection.

Seclore offre une solution simple et uniformisée à ces problèmes. Une fois que les courriels sont traités par DLP Email Gateway, la protection automatisée de Seclore Rights Management sécurise le courriel et ses pièces jointes avec la politique d'utilisation appropriée. Cela garantit que les destinataires ne peuvent pas utiliser le courriel à mauvais escient ou le détourner après l'avoir reçu et lu. Ainsi, une politique « Autoriser » avec DLP devient une politique « pour les 10 prochains jours » avec Seclore.

Grâce à la protection automatisée de Seclore Rights Management, la sécurité n'entrave pas la collaboration essentielle par courriel. Le partage des données peut se poursuivre, tout en préservant la sécurité et la conformité. Le tout de façon totalement transparente pour l'expéditeur et le destinataire du courriel.

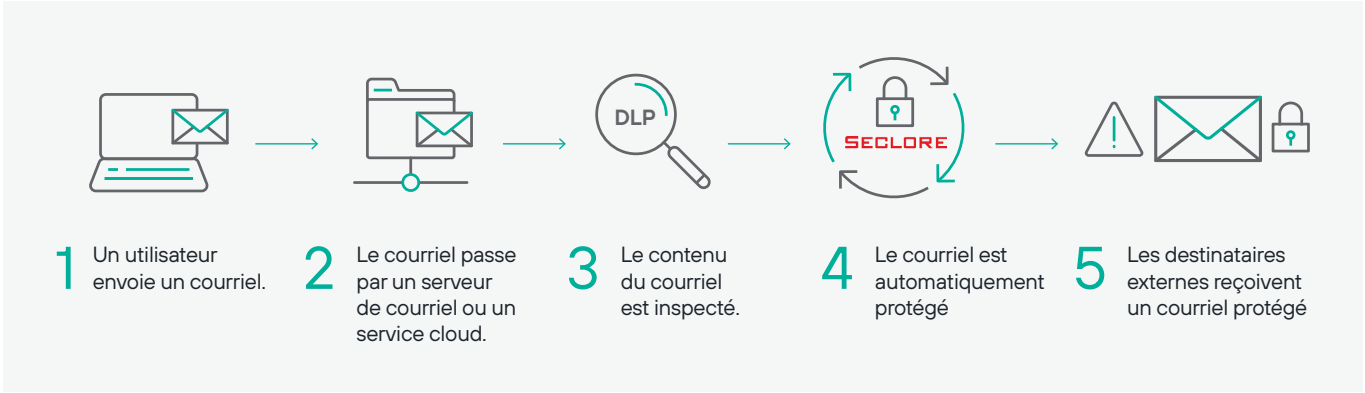

Figure 4 : Seclore et Forcepoint DLP

Secure Email Decryption pour Forcepoint DLP Content Discovery

L'un des défis posés aux systèmes DLP consiste à découvrir le contenu sensible des courriels et des pièces jointes cryptés, afin de décider si un courriel doit être partagé ou bloqué. Seclore Decrypter for Email résout ce problème en activant un accès sécurisé aux courriels et pièces jointes chiffrés par Seclore. Lorsque le courriel protégé est décrypté, Forcepoint DLP peut rechercher le contenu et les modèles sensibles et prendre les décisions appropriées (autoriser/bloquer/protéger). Decrypter for Email de Seclore fonctionne en conjonction avec Email Auto-Protector de Seclore pour automatiser la protection des courriels avant de les envoyer à l'extérieur de l'entreprise.

Les entreprises qui utilisent Seclore Rights Management et Forcepoint DLP peuvent désormais revendiquer leur conformité aux réglementations, car Forcepoint DLP peut découvrir, suivre et auditer tous les fichiers, qu'ils soient protégés ou non.

Avantages clés pour les activités

Protection automatique des données
L'intégration DLP-Digital Rights Management (DRM, la gestion des droits numériques) automatise l'ensemble du processus de classification, de protection, de contrôle de l'utilisation et d'audit. Le passage de la détection à la protection se fait de manière transparente. Le processus de protection DRM est totalement transparent pour l'utilisateur final.

Déploiements DLP plus rapides
La gestion des droits numériques peut être configurée comme règle de gestion par défaut de DLP, afin de tirer immédiatement profit de DLP dès son déploiement.

Sécurité et conformité au-delà du firewall
L'intégration DLP-DRM permet de sécuriser et d'auditer les données où qu'elles aillent : sur les réseaux des prestataires et des partenaires, sur les réseaux publics, dans le cloud ou sur les appareils mobiles.

Listes réduites d'incidents
DLP peut être configuré pour traiter les fichiers protégés par DRM comme étant sûrs – et ne pas générer d'alertes pour ces fichiers. Cela permet de réduire considérablement le volume de journalisation des incidents.

Formation minimale
Il n'y a quasiment aucune nécessité de formation des utilisateurs finaux, puisque la protection est automatique et qu'un document protégé s'ouvre dans l'application native comme tout autre document.

Agilité commerciale accrue
La possibilité de sécuriser les informations qui circulent au-delà du périmètre de l'entreprise résout un problème de conformité épineux, réduit considérablement les risques de sécurité et permet une adoption en toute sécurité des services de partage de fichiers, des politiques BYOD et du cloud computing.

Audit intégral et conformité réglementaire
L'intégration DLP-DRM active la conformité aux obligations réglementaires pour l'ensemble du cycle de vie des données non structurées, à l'intérieur comme à l'extérieur du réseau de l'entreprise.

Appliquer des politiques TI à des tiers
L'intégration DLP-DRM vous aide à faire appliquer votre régime de gouvernance des données et des politiques informatiques de l'entreprise aux sous-traitants, prestataires, partenaires et autres tiers.

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données. Son objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Nos solutions à facteur humain s'adaptent en temps réel à la façon selon laquelle les individus interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables protégeant des milliers de clients dans le monde entier.

forcepoint.com/contact

À propos de Seclore

Seclore propose la première plateforme de sécurité centrée sur les données et basée sur navigateur. Elle offre aux entreprises la possibilité d'utiliser les meilleures solutions du marché pour découvrir, identifier, protéger et contrôler l'utilisation des données où qu'elles aillent, à l'intérieur comme à l'extérieur du périmètre de l'entreprise. La possibilité d'automatiser le processus de sécurité centré sur les données permet aux organisations de protéger pleinement les informations avec un minimum de friction et de coûts. Plus de 2000 entreprises dans 29 pays utilisent Seclore pour atteindre leurs objectifs en matière de sécurité des données, de gouvernance et de conformité.

seclore.com/contact