VARONIS

LIVRE BLANC

3 façons d'améliorer la prévention des pertes de données avec Varonis

Table des matières

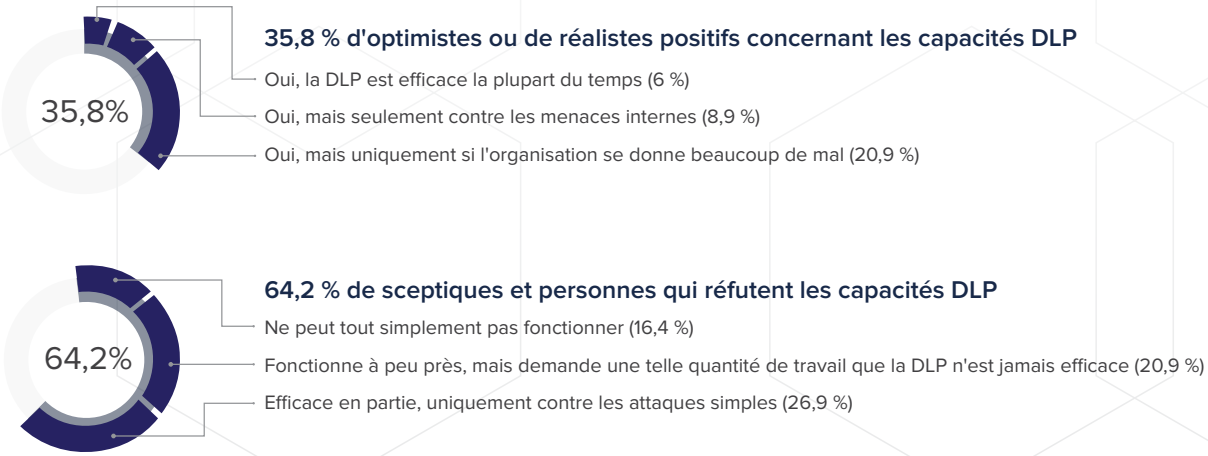
Présentation

La prévention des pertes de données (DLP) a longtemps été considérée comme une des principales technologies à utiliser pour limiter la perte de propriété intellectuelle, de données médicales, de données financières et d'informations permettant d'identifier une personne. Toutefois, les professionnels de l'informatique qui déploient des systèmes de DLP en grande entreprise ont souvent des difficultés à dépasser le stade des phases initiales de découverte et de surveillance des flux de données. Par conséquent, ils ne profitent jamais des avantages apportés par une analyse plus approfondie des données ou de l'application de protections appropriées des données.[1]

Dans une enquête récente, Anton Chuvakin, analyste chez Gartner a demandé à des informaticiens si « la technologie DLP peut être efficace contre les « méchants » (à savoir toute personne malintentionnée, qu'elle vienne de l'intérieur ou de l'extérieur de l'entreprise) qui menacent l'organisation ».

Les deux tiers des personnes qui ont répondu à l'enquête sont sceptiques, indiquant que la DLP « ne peut tout simplement pas fonctionner », « fonctionne à peu près, mais trop inefficace », ou « fonctionne uniquement dans le cas de menaces simples ».

LA TECHNOLOGIE DE PRÉVENTION DES PERTES DE DONNÉES (DLP) PEUT-ELLE ÊTRE EFFICACE CONTRE LES « MÉCHANTS » QUI MENACENT VOTRE ORGANISATION ?



Brian Reed. « It's Time to Redefine Data Loss Prevention ». https://www.gartner.com/doc/3803465/time-redefine-data-loss-prevention (accès le 14 février 2018)

Le Directeur de la sécurité des informations (DSI/CISO) d'une société d'assurance a fourni un point de vue plus descriptif en déclarant récemment : « Nous sommes arrivés à la conclusion que la DLP est davantage un concept qu'un outil ».

Le vice-président des services technologiques d'une entreprise de services financiers a déclaré pour sa part : « La nôtre [DLP] ne vaut pas le coup. Je ne suis même pas certain qu'un système de qualité présente un intérêt. »

Pourquoi les équipes de cybersécurité sont-elles si nombreuses à rejeter la DLP ?

L'absence d'intelligence exploitable est une des raisons. Lors de la mise en œuvre d'une DLP, il n'est pas rare de recevoir des dizaines de milliers d'« alertes » portant sur des fichiers sensibles. Par où commencer ? Comment définir des priorités ? Parmi cette masse phénoménale d'incidents, lequel présente un risque important justifiant votre attention totale et immédiate ?

Et le problème ne s'arrête pas là. Sélectionnez un incident / une alerte au hasard : les fichiers sensibles concernés ont peut-être été chiffrés et mis en quarantaine automatiquement, mais après ? Qui possède les connaissances et l'autorité nécessaires pour décider des contrôles d'accès adéquats ? Qui empêchons-nous maintenant de travailler ? Comment et pourquoi les fichiers ont-ils été placés ici au départ ?

En elles-mêmes, les solutions de DLP apportent très peu de contexte sur l'utilisation des données, les droits et la propriété. Par conséquent, le service informatique a du mal à corriger les problèmes de manière durable. Le service informatique à lui seul n'est pas qualifié pour prendre des décisions sur l'accessibilité et l'utilisation autorisée. Même si c'était le cas, prendre de telles décisions pour chaque fichier n'est pas réaliste.

La DLP n'apporte pas le contexte nécessaire concernant les données : qui possède un accès, qui accède réellement aux données, où sont-elles surexposées et comment les verrouiller de manière sécurisée. Sans ce contexte, il est presque impossible de définir des priorités parmi les opérations de limitation des risques. C'est la raison pour laquelle de nombreuses organisations perçoivent la DLP comme une fonction intégrée plutôt que comme un produit.

Ces limitations compliquent également la tâche lorsqu'il s'agit de respecter des réglementations telles que le GDPR appliqué en UE, qui exigent non seulement de savoir où se trouvent les données à caractère personnel, mais aussi si elles sont en permanence accessibles uniquement aux bonnes personnes, si toutes les utilisations sont surveillées et si les abus sont signalés.

Alors, si vous ne pouvez plus appuyer votre stratégie de sécurité des données sur la DLP, sur quoi va-t-elle reposer ?

Les entreprises complètent déjà leur stratégie DLP en déployant des produits d'audit et de protection centrés sur les données (DCAP) à grande échelle incluant une fonctionnalité DLP ou intégrant DLP et DCAP. Les analystes de la sécurité considèrent maintenant la DLP comme un élément d'une solution plus complète et conseillent d'évoluer vers une plate-forme unifiée incluant découverte des données, gestion des droits, analyse de la sécurité, gouvernance de l'accès aux données, etc.

Dans ce livre blanc, nous aborderons les trois capacités de la Plate-forme de sécurité des données Varonis qui vous aideront à aller au-delà de la prévention des pertes de données pour bénéficier d'une protection complète des données.

- Identification des données sensibles
- Visibilité et gestion des droits à 360°
- Détection avancée des menaces

1 Identification des données sensibles

Les organisations doivent déterminer où se trouvent leurs données sensibles afin d'évaluer les risques, surveiller les menaces et corriger les droits en priorité là où le besoin est le plus urgent.

Le Moteur de classification des données de Varonis - Data Classification Engine (DCE) - classe les données confidentielles conservées dans OneDrive, SharePoint Online et dans des dépôts de données sur site tels que serveurs de fichiers Windows, appareils NAS, UNIX et SharePoint. Data Classification Engine combine une puissante capacité de correspondance de contenus selon un schéma, des expressions régulières (RegEx) et la mise en correspondance à partir de dictionnaires dynamiques à actualisation automatique.

L'analyse préalable et a posteriori des négatifs et la vérification algorithmique garantissent un faible taux de faux positifs.

Si nécessaire, Data Classification Engine peut utiliser les métadonnées de classification de produits tiers déjà déployés (notamment de produits DLP). Varonis affiche en natif les informations tierces parties sur la sensibilité et les combine à ses propres métadonnées, apportant ainsi des capacités exploitables de protection et de gestion des données. Les informations de classification peuvent également être importées automatiquement dans la plate-forme Varonis par le biais de fichiers CSV de manière planifiée.

La piste d'audit des accès aux fichiers fournie par DatAdvantage permet à Data Classification Engine de procéder à une véritable analyse incrémentale. Grâce aux connaissances en temps réel obtenues sur les créations et modifications de fichiers, seules les nouvelles données sont classées et les performances obtenues sont bien supérieures à celles des produits traditionnels.

DCE intègre un large éventail de packs de conformité adaptés à des réglementations telles que GDPR, HIPAA, SOX, PCI-DSS, etc...

Il permet en outre de créer des règles personnalisées, de procéder à des vérifications algorithmiques, d'ajouter des indicateurs manuels et même d'automatiser la mise en quarantaine ou la suppression des contenus sensibles non conformes à la politique.

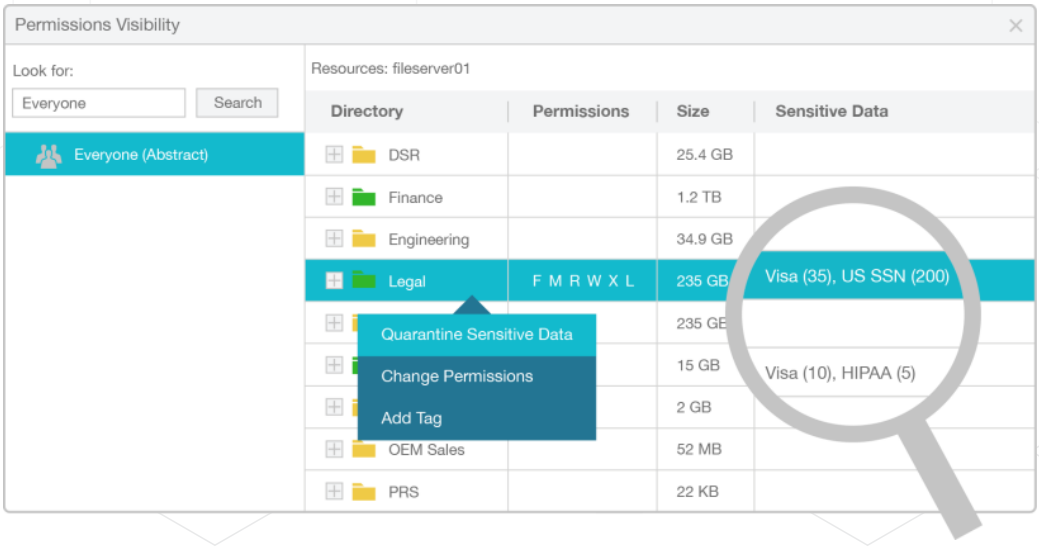
> *Varonis Data Classification Engine nous a aidés à gagner en efficacité tout en nous apportant de précieuses informations sur des domaines spécifiques où il était vraiment important d'améliorer notre visibilité. Je sais avec certitude où se trouvent nos informations de carte de crédit et chacun des numéros de sécurité sociale.*
>
> -Ian Aguilar, directeur technique de Campbell Global

2 Visibilité et gestion des droits à 360°

Trouver les informations sensibles n'est que le début. Pour limiter les risques de manière durable, nous avions aussi besoin de connaître les emplacements concentrant un nombre important de données sensibles surexposées afin de définir des priorités dans nos interventions et de mettre en place un plan d'action.

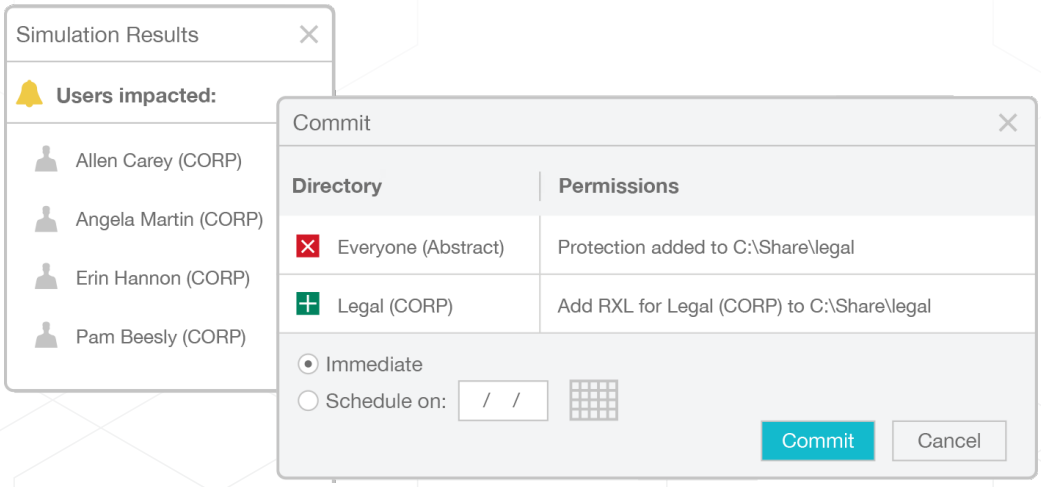
Il peut être extrêmement difficile, voire impossible, de déterminer à quels dossiers, sites SharePoint et messageries un utilisateur ou un groupe peut accéder. Il est encore plus difficile de trouver les données exposées à des risques, d'identifier les dossiers et objets sensibles qui ont été partagés avec l'extérieur, et de corriger les droits qui n'ont plus de raison d'être. La technologie DLP n'a pas été conçue pour résoudre ce problème.

Le Moteur de classification des données de Varonis s'inscrit dans la Plate-forme de sécurité des données Varonis, une solution de plus grande envergure. De ce fait, la sensibilité des données est combinée à des métadonnées de droits, ce qui permet d'établir un plan de remédiation exploitable. Prouvez aux auditeurs que vous ne vous contentez pas de surveiller les données réglementées, mais que vous les protégez de manière préventive en supprimant les accès inutiles en vous basant sur les schémas d'utilisation réels des données.



Varonis vous apporte une vue complète de l'accès aux données conservées dans les référentiels cloud et sur site. Quelques secondes suffisent à l'équipe informatique pour visualiser ou obtenir un rapport sur l'accès potentiel de tout utilisateur ou groupe Active Directory, Azure AD ou d'un système local, localiser les données confidentielles surexposées et identifier les droits excessifs.

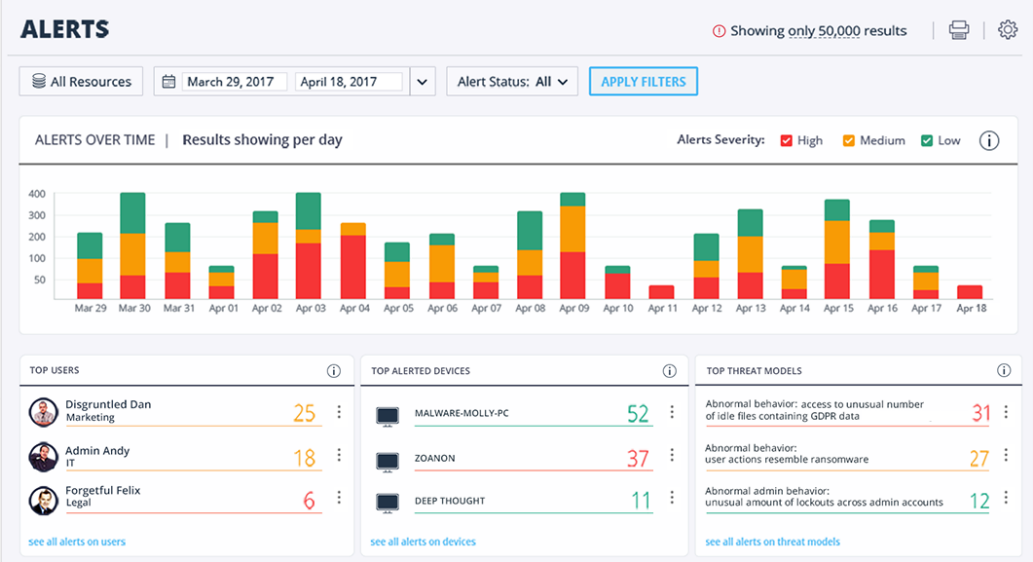
Un puissant moteur de validation permet de simuler dans un bac à sable les modifications apportées au contrôle d'accès et de les valider lorsqu'elles donnent satisfaction. Inutile de comprendre toutes les particularités des modèles de droits cloud et sur site : Varonis gère les accès aux données dans une seule et même interface récapitulative et réduit systématiquement la surface exposée aux attaques



3 Détection avancée des menaces

Varonis analyse l'activité et le comportement des utilisateurs dans les environnements hybrides et détermine le comportement de référence de chaque compte. Sa Plate-forme de sécurité des données analyse les événements d'accès aux données dans leur contexte en tenant compte de la sensibilité des données, des droits et des métadonnées Active Directory, résultant en des alertes exactes et un nombre réduit de faux positifs.

DatAlert vous aide à répondre avec assurance à la question « Mes données sont-elles en sécurité ? » grâce des services continus de surveillance et d'envoi d'alertes concernant vos données et systèmes centraux. Varonis est la seule solution à combiner classification des données, et gouvernance des accès , avec une analyse de la sécurité pour apporter à nos modèles de menace un contexte plus riche et des alertes plus précises.



Avec plus de 100 modèles de menaces, Varonis émet des alertes en cas d'activité suspecte dans la messagerie, de menace interne ou de comportement de ransomware connu. Les équipes de sécurité ont la possibilité d'utiliser le tableau de bord DatAlert ou d'envoyer des alertes à un système intégré de gestion des événements et informations de sécurité (SIEM).

Récapitulatif

À elles seules, les solutions de prévention des pertes de données (DLP) ne fournissent pas suffisamment de contexte pour apporter une réponse systématique et durable aux problèmes fondamentaux de la gestion et de la protection des données : des personnes ont accès à des données alors qu'elles ne devraient pas et n'en ont pas besoin, et leur utilisation des données n'est pas surveillée.

La connaissance du contexte de l'entreprise est un problème qui relève du domaine de l'audit et de la protection centrés sur les données, et non de la prévention des pertes de données. Lorsque les contrôles d'accès sont optimisés, l'utilisation des données est surveillée, les abus sont signalés et le risque de perte de données diminue considérablement.

Si elles souhaitent optimiser leur sécurité, les entreprises devront utiliser des technologies complémentaires pour remplacer ou renforcer de façon notable les solutions DLP en place.

> "Varonis est une solution fantastique"

Gartner peerinsights™

En savoir plus sur les résultats obtenus par les clients →

ABOUT VARONIS

Varonis est un pionnier de la sécurité et de l'analyse des données, spécialisé dans les logiciels de sécurité des données, la gouvernance, la conformité, la classification et l'analyse. Varonis détecte les menaces internes et les cyberattaques en analysant l'activité effectuée sur les fichiers et les comportements des utilisateurs. Il prévient les catastrophes en verrouillant les données sensibles et maintient un état sécurisé grâce à l'automatisation.

Nous aidons des milliers de clients à éviter les fuites de données.

NASA · ING · Nasdaq · CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 · DELL EMC

TOYOTA · LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE · L'ORÉAL

Bénéficiez d'une évaluation personnalisée des risques

Évaluation des risques sur les données

Déterminez votre profil de risque, découvrez vos vulnérabilités et corrigez vos problèmes de sécurité réels.

info.varonis.com/express-assessment-fr

Démo en direct

Installez Varonis dans votre propre environnement et découvrez comment stopper le ransomware et protéger vos données.

info.varonis.com/trial-fr

VARONIS