Proofpoint Endpoint Data Loss Prevention et Proofpoint Insider Threat Management

Protection centrée sur les personnes au niveau de l'endpoint

PRINCIPAUX AVANTAGES

- Réduction du risque de fuite de données sensibles et de menaces internes
- Simplification de la réponse aux fuites de données et aux violations des règles
- Réduction du délai de rentabilisation des programmes de prévention des menaces internes et des fuites de données

Les fuites de données ne se produisent pas par magie. Ce sont les utilisateurs qui les déclenchent.

C'est pourquoi Proofpoint Endpoint Data Loss Prevention et Proofpoint Insider Threat Management adoptent une approche centrée sur les personnes de la gestion des menaces internes et de la prévention des fuites de données au niveau de l'endpoint. Ils aident les équipes informatiques et de cybersécurité modernes à accomplir les tâches suivantes :

- Identifier les comportements à risque et les mouvements de données suspects
- Détecter et prévenir les incidents de sécurité d'origine interne et les fuites de données à partir des endpoints
- Accélérer la réponse aux incidents imputables aux utilisateurs

Vous devez pouvoir analyser et bloquer rapidement toute fuite de données ou tout incident de sécurité d'origine interne. Plus un incident est résolu rapidement, moins les dégâts seront importants pour votre entreprise, votre marque et vos résultats financiers.

Quand chaque seconde compte, la visibilité, la détection et le contexte sont essentiels. Les outils de prévention des fuites de données (DLP) d'ancienne génération offrent une visibilité limitée sur les incidents imputables aux utilisateurs. Ils passent à côté des signes critiques d'exfiltration non approuvée de données et d'autres violations des règles. Par ailleurs, ils ne fournissent pas les informations nécessaires (« qui, quoi, où, quand et pourquoi ») pour distinguer les alertes et les événements suspects des activités métier normales.

Notre plate-forme intègre Proofpoint Insider Threat Management (ITM) et Proofpoint Endpoint DLP. Avec leur architecture moderne, légère et partagée, nos solutions permettent de gérer les comportements à risque au niveau de l'endpoint grâce aux fonctionnalités suivantes :

- **Visibilité et contexte** sur les activités des utilisateurs et les mouvements de données
- **Détection** et signalement **en temps réel** des comportements à risque et des mouvements de données suspects
- **Prévention des exfiltrations de données** à risque **à partir de l'endpoint**
- **Accélération de la réponse aux incidents** et **des investigations**
- **Simplification du déploiement** grâce à un système de back-end exclusivement SaaS et à une architecture d'agent léger

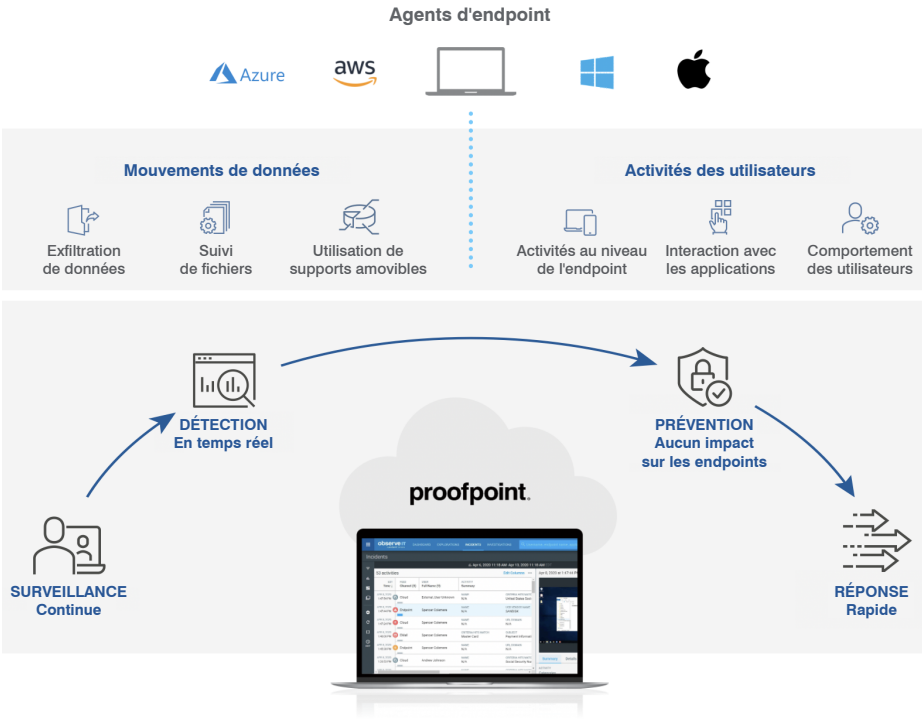


Plate-forme intégrant Proofpoint Endpoint DLP et Proofpoint ITM

Visibilité et contexte sur les activités des utilisateurs et les mouvements de données

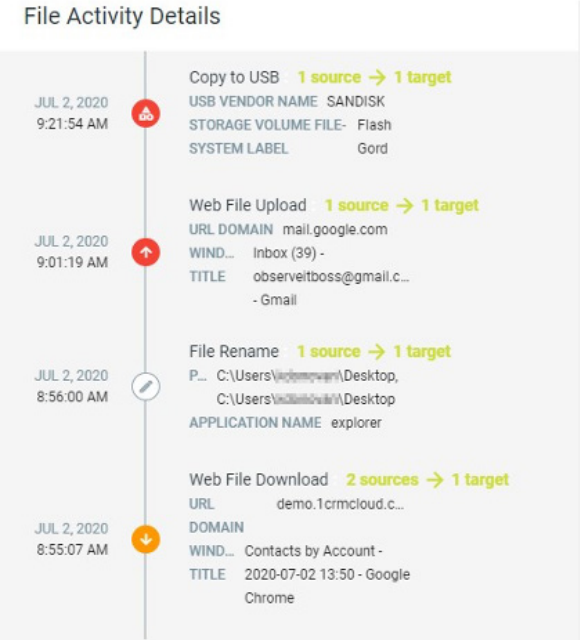
Il est essentiel de comprendre le contexte des activités numériques des utilisateurs pour évaluer les risques. Mais l'analyse des fichiers journaux peut prendre beaucoup de temps et ne fournit généralement pas les informations dont vos experts en investigation numérique ont besoin pour intervenir.

Visibilité avec Proofpoint Endpoint DLP

La plate-forme collecte des informations sur la façon dont les utilisateurs interagissent avec les données sur leurs endpoints. Elle ne se contente pas d'alerter les équipes informatiques et de sécurité en cas de mouvements de données suspects. Elle fournit également des informations contextuelles grâce à une vue chronologique montrant comment les utilisateurs accèdent aux fichiers et aux données, les déplacent et les manipulent. Les équipes de sécurité peuvent ainsi mettre rapidement en corrélation les éléments suivants :

- Interaction des utilisateurs avec les fichiers et les données (couper, copier, coller, renommer, déplacer, etc.)
- Nom, extension et taille des fichiers
- Étiquettes pour la classification des données (s'appuyant sur les étiquettes Microsoft Information Protection)
- Suivi des fichiers et des données (origine, emplacement intermédiaire, destination, etc.)
- Canal d'exfiltration (nom de domaine et URL si les données ont été déplacées via un canal Web, etc.)
- Contenu du presse-papiers du système d'exploitation

Cette approche centrée sur les personnes permet de réduire le délai de rentabilisation et de renforcer la protection en temps réel, contrairement aux outils DLP pour endpoints traditionnels, qui présentent peu d'intérêt tant que le contenu n'a pas été inspecté et classé. Qui plus est, ces outils ne fournissent aucune visibilité sur les mouvements de données, sauf si une action déclenche une alerte. Vous passerez donc à côté de mouvements de données en apparence inoffensifs qui, en contexte, présentent des signes critiques de malveillance.



Contexte sur les mouvements de fichiers et de données, depuis l'origine jusqu'à la destination

Visibilité avec Proofpoint ITM

Pour comprendre le contexte des incidents imputables aux utilisateurs, vous devez bénéficier d'une visibilité sur l'ensemble de leurs activités, y compris sur les mouvements de données. C'est la raison pour laquelle Proofpoint ITM offre une visibilité plus complète sur les activités au niveau de l'endpoint. En plus des mouvements de données capturés par Proofpoint Endpoint DLP, Proofpoint ITM vous fournit les informations suivantes :

- Comment les utilisateurs accèdent aux applications Web, aux supports amovibles, aux serveurs, aux applications virtuelles et aux postes de travail, et comment ils les utilisent
- L'utilisation de la souris et du clavier au niveau de l'endpoint
- Des instantanés des activités au niveau de l'endpoint.

Ensemble, ces éléments permettent de comprendre tous les tenants et aboutissants (« qui, quoi, où, quand et pourquoi ») des activités à risque. Grâce à ces informations contextuelles, vous pouvez mieux cerner les intentions des utilisateurs en cas de fuite de données ou de violation des règles.

Contexte des menaces

Visualiser le contexte des menaces ciblant des groupes d'utilisateurs spécifiques peut vous aider à mieux gérer les risques liés aux utilisateurs. Notre plate-forme vous permet de créer des listes de surveillance d'utilisateurs en fonction de critères tels que les suivants :

- Sensibilité du rôle de l'utilisateur et des données avec lesquelles il interagit
- Vulnérabilité de l'utilisateur au phishing et à d'autres techniques d'ingénierie sociale
- Emplacement de l'utilisateur
- Modifications des fonctions de l'utilisateur
- Autres facteurs RH et juridiques

Détection en temps réel des comportements à risque et des mouvements de données suspects

Bibliothèque d'alertes

Proofpoint ITM et Proofpoint Endpoint DLP intègrent des bibliothèques d'alertes prédéfinies qui facilitent la configuration et réduisent le délai de rentabilisation. Les règles d'alerte reposent sur des modèles de menaces créés en partenariat avec des universitaires et des experts gouvernementaux, ainsi que sur les bonnes pratiques de nos clients. Proofpoint Endpoint DLP et Proofpoint ITM peuvent tous deux vous alerter en cas d'interactions et de mouvements de données suspects au niveau de l'endpoint. En outre, Proofpoint ITM peut détecter un éventail plus large de menaces internes.

Bibliothèque d'alertes Proofpoint Endpoint DLP et Proofpoint ITM

Proofpoint Endpoint DLP

Mouvements de données

Plus de 40 alertes concernant les interactions avec les données et leur exfiltration, notamment :

- Chargement de fichiers sur le Web
- Copie de fichiers sur des clés USB
- Copie de fichiers dans un dossier de synchronisation cloud local
- Impression de fichiers
- Copier-coller de fichiers/dossiers/texte
- Activités exécutées sur des fichiers (changement de nom, copie, déplacement, suppression, etc.)
- Suivi de fichiers (Web vers USB, Web vers Web, etc.)
- Téléchargement de fichiers depuis le Web
- Envoi d'un fichier en pièce jointe à un email
- Téléchargement d'un fichier à partir d'un email

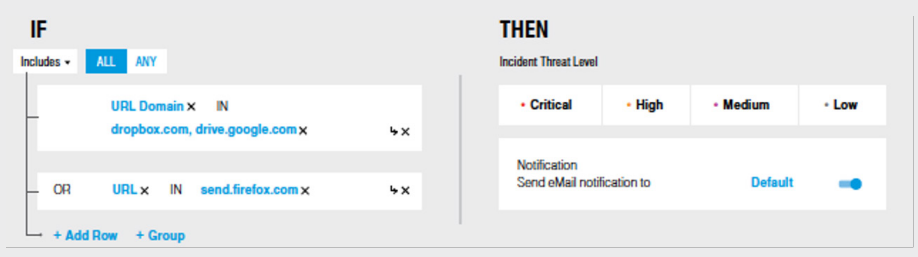
Activités des utilisateurs

Plus de 100 alertes concernant un large éventail d'activités réalisées par les utilisateurs au niveau de l'endpoint, notamment :

- Masquage d'informations
- Accès non autorisé
- Contournement des contrôles de sécurité
- Négligence
- Création d'une porte dérobée (backdoor)
- Violation de droits d'auteur
- Outils de communication non autorisés
- Tâches d'administration non autorisées
- Activités DBA non autorisées
- Préparation d'une attaque
- Sabotage informatique
- Élévation de privilèges
- Usurpation d'identité
- Activités GIT suspectes
- Utilisation inacceptable

Moteur de règles flexible

Vous pouvez créer des règles et des déclencheurs adaptés à votre environnement grâce à notre créateur de règles basé sur la logique booléenne. Pour la création de règles, vous pouvez partir de zéro ou de scénarios de menaces prédéfinis. Les règles de prévention des fuites de données peuvent se concentrer sur les mouvements de données sensibles en s'appuyant sur les étiquettes Microsoft Information Protection. Par rapport aux systèmes de détection basés sur les anomalies, cette approche permet d'éviter une baisse de la vigilance due à un volume élevé d'alertes.



Configuration d'une alerte à l'aide d'instructions simples et flexibles de type si-alors

Traque des menaces par pointer-cliquer

Nos puissantes fonctionnalités de filtrage et de recherche vous aident à traquer les menaces de manière proactive grâce à des explorations de données personnalisées. Vous pouvez rechercher les activités et les comportements à risque qui s'appliquent à votre entreprise ou vous familiariser avec les nouveaux risques.

Traque des comportements potentiellement dangereux ou sortant de l'ordinaire

Prévention de l'exfiltration non autorisée de données à partir de l'endpoint

Détecter les comportements à risque des utilisateurs et les mouvements de données suspects n'est pas toujours suffisant. Vous devez également les bloquer. Notre plate-forme vous permet de créer des règles afin d'empêcher les mouvements de données contraires aux règles et les interactions avec des données sensibles, notamment :

- Transfert vers des périphériques USB
- Synchronisation de fichiers avec d'autres terminaux et le cloud
- Partage de fichiers
- Couper, copier et coller
- Chargement Web

De plus, lorsque vous utilisez Proofpoint Endpoint DLP avec les autres produits de la suite Enterprise DLP, vous pouvez étendre les fonctionnalités de prévention des fuites de données à la messagerie et aux applications cloud.

Prise en charge de la réponse aux incidents et des investigations

L'investigation et la résolution des alertes de sécurité causées par des utilisateurs internes peuvent constituer un processus long et coûteux. De plus, elles impliquent souvent des départements non techniques comme les RH, la conformité, le service juridique et les chefs de service.

Notre plate-forme rationalise ces efforts transversaux grâce à trois fonctionnalités puissantes :

- Visualisations intuitives et faciles à comprendre des données
- Captures d'écran des activités des utilisateurs
- Exportation et partage de rapports en toute simplicité pour des workflows plus fluides

Captures d'écran

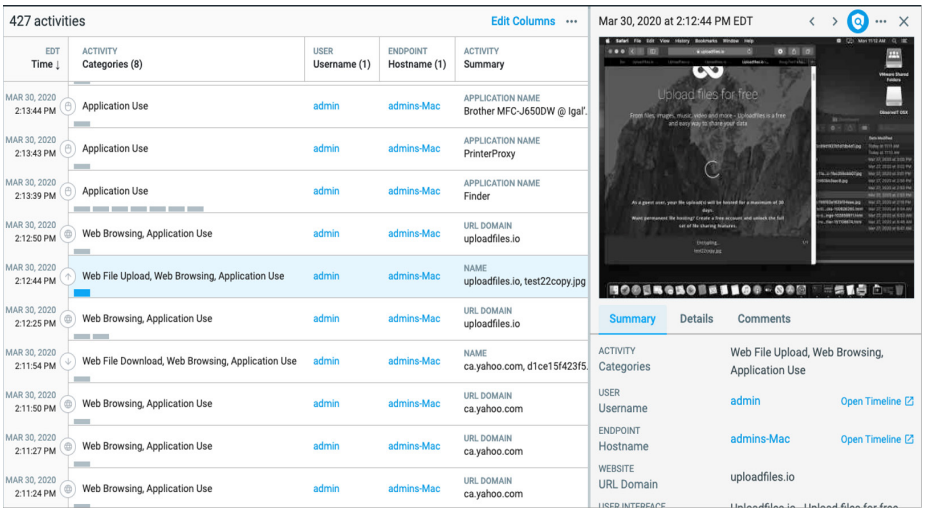
En matière d'investigations sur la sécurité et les fuites de données, une image vaut parfois mille mots. Proofpoint ITM permet d'effectuer des captures d'écran des activités des utilisateurs. Les RH, le service juridique et les chefs de service disposent ainsi de preuves claires et irréfutables des comportements malveillants ou négligents en vue de prendre des décisions éclairées.

Tri des alertes

Nos visualisations de données fournissent des informations contextuelles sur les incidents imputables aux utilisateurs d'une manière que même les équipes non techniques peuvent comprendre. La vue chronologique permet de mettre en corrélation alertes et incidents, et une puissante fonctionnalité de recherche aide les équipes à extraire rapidement les données pertinentes. Notre plate-forme permet aux équipes de sécurité d'identifier rapidement les événements qui doivent faire l'objet d'investigations plus poussées et ceux qu'ils peuvent clôturer immédiatement.

Workflow d'investigation

Le workflow de base et les fonctionnalités de partage d'informations intégrés à la plate-forme permettent de rationaliser la collaboration transversale. Vous pouvez exporter des enregistrements des activités à risque pour plusieurs événements dans des fichiers de format courant, tels que des PDF. Ces rapports incluent des captures d'écran et des informations contextuelles.



Vue chronologique des activités de l'utilisateur avec capture d'écran de l'endpoint

Simplification du déploiement grâce à une distribution exclusivement SaaS et à une architecture d'agent léger

Notre architecture moderne et native au cloud est conçue dans une optique d'évolutivité, de facilité d'utilisation, de sécurité et d'extensibilité. Pour Proofpoint Endpoint DLP, l'agent capture les mouvements de données. Pour Proofpoint ITM, l'agent collecte les mouvements de données et les activités des utilisateurs.

Évolutivité adaptée aux entreprises internationales

La plate-forme repose sur une infrastructure cloud publique hautement redondante et évolutive. Elle permet la surveillance de milliers, voire de centaines de milliers, d'utilisateurs.

Sécurité et protection des données dès la conception

Grâce à nos intégrations SAML et OAuth, vous pouvez authentifier les utilisateurs de la plate-forme à l'aide de leurs identifiants de connexion Microsoft 365, Okta Identity Cloud, Google Cloud IAM et d'autres fournisseurs. Vous pouvez octroyer aux utilisateurs des droits d'accès aux ressources de la plate-forme au moyen d'une combinaison de contrôles d'accès granulaires basés sur des attributs (ABAC), notamment :

- Utilisateur
- Ressource
- Activité à visualiser
- Environnement

La confidentialité est une composante essentielle de tout programme de gestion des menaces internes. La gestion avancée des règles vous permet de définir des règles de surveillance, des listes d'exclusion de données et des listes d'exclusion d'utilisateurs. Vous pouvez organiser les groupes par utilisateur, application, fichier et endpoint. Voici des exemples de groupes courants :

- Par région géographique (pour se conformer aux réglementations régionales en matière de protection des données)
- Par service (pour séparer les installations distantes, comme les magasins, des bureaux)

Architecture d'agent léger

Notre plate-forme utilise un agent d'endpoint léger qui intercepte uniquement les transactions qui enfreignent les règles de prévention. Sinon, la plupart des données télémétriques sont collectées en mode utilisateur. L'agent ne gêne pas les utilisateurs et n'entre pas en conflit avec les autres outils de sécurité au niveau du noyau. Grâce à notre agent, vous bénéficiez d'une visibilité indépendante des applications sur les activités des utilisateurs au niveau de l'endpoint.

Intégration aisée au sein d'environnements de sécurité complexes

L'architecture axée sur les API de notre plate-forme est pilotée par des microservices. Les webhooks intégrés à notre plate-forme permettent à vos outils SIEM et SOAR d'absorber les alertes Proofpoint Endpoint DLP et Proofpoint ITM, ce qui vous permet d'identifier et de trier les incidents plus rapidement.

Il est possible que les entreprises disposant d'une infrastructure de sécurité complexe doivent conserver une seule source de vérité pour l'ensemble des systèmes. Nous facilitons ce processus grâce à des exportations automatiques des données Proofpoint Endpoint DLP et Proofpoint ITM vers les espaces de stockage AWS S3 qui vous appartiennent et que vous exploitez.

Fonctionnement de Proofpoint Endpoint DLP et de Proofpoint ITM

La gestion des menaces internes et la prévention des fuites de données au niveau de l'endpoint sont essentielles dans l'environnement concurrentiel actuel. Toutefois, la plupart des entreprises n'ont pas besoin de collecter en permanence des données télémétriques sur toutes les activités de tous les utilisateurs.

Nous recommandons plutôt une approche plus adaptative et basée sur les risques. Vous bénéficierez ainsi d'informations sur certaines activités pour tous les utilisateurs et sur toutes les activités de certains utilisateurs (ceux qui présentent le risque le plus élevé). Ces utilisateurs peuvent inclure des collaborateurs figurant sur une liste de surveillance, des utilisateurs à haut niveau de privilèges, des sous-traitants et des utilisateurs ciblés tels que des dirigeants.

Notre plate-forme vous offre cette flexibilité. À l'aide d'un seul jeu de règles et du même agent d'endpoint, vous pouvez :

- limiter la collecte d'informations aux mouvements de données sensibles grâce à Proofpoint Endpoint DLP ;
- inclure des informations contextuelles sur les utilisateurs présentant un risque élevé avec Proofpoint Insider Threat Management.

Grâce à un simple changement de configuration des règles, vous pouvez ajuster la quantité et le type de données que vous collectez pour chaque utilisateur ou groupe d'utilisateurs. Cette approche adaptative vous aide à analyser les alertes et à y répondre plus efficacement, sans collecter une quantité astronomique de données.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : proofpoint.com/fr.

proofpoint.

0212-001-01-01 12/2020