Proofpoint Insider Threat Management

Gestion des menaces internes centrée sur les personnes pour les entreprises modernes

PRINCIPAUX AVANTAGES

- Détection des activités internes à risque et prévention des fuites de données à partir de l'endpoint
- Simplification de la réponse aux menaces et fuites de données d'origine interne
- Réduction du délai de rentabilisation grâce à un déploiement SaaS hautement évolutif piloté par un système back-end moderne et natif au cloud
- Préservation de la productivité des utilisateurs grâce à un agent d'endpoint léger

PRINCIPAUX SCÉNARIOS D'UTILISATION DE PROOFPOINT ITM

- Identification des risques liés aux utilisateurs
- Prévention des fuites de données à partir de l'endpoint
- Accélération de la réponse aux incidents imputables aux utilisateurs
- Développement de programmes de gestion des menaces internes

Par son approche centrée sur les personnes, Proofpoint Insider Threat Management (ITM) protège votre entreprise contre les fuites de données, les actes malveillants et les atteintes à la marque imputables aux utilisateurs internes. Nous vous défendons contre la malveillance, la négligence ou le manque de connaissances des utilisateurs autorisés. Par ailleurs, nous mettons en corrélation les activités des utilisateurs et les mouvements de données, de façon à vous protéger contre les compromissions de données induites par des utilisateurs internes. Qui plus est, nous détectons en temps réel les comportements à risque pour vous fournir des preuves irréfutables concernant les actes malveillants.

Détection et prévention en temps réel des comportements à risque

Avec Proofpoint ITM, vous pouvez mettre en corrélation les comportements à risque au niveau des applications, des fichiers, des postes de travail, des serveurs et des environnements virtualisés en temps réel, et non une fois que l'incident s'est produit. Nous vous offrons une visibilité en temps réel vous permettant de mettre en corrélation, détecter et neutraliser les incidents dus à des menaces internes.

Scénarios de menaces réels et collaboratifs

Vous pouvez détecter en temps réel les comportements à risque, tels que :

- Exfiltration de données
- Déplacement latéral à risque de données
- Utilisation abusive de privilèges
- Utilisation inappropriée d'applications
- Accès non autorisé
- Actions accidentelles dangereuses

Notre créateur de règles basé sur la logique booléenne vous permet de créer facilement des règles et des déclencheurs adaptés à votre environnement. Il est possible de partir de zéro ou de scénarios de menaces prédéfinis. Notre large éventail de règles de détection des menaces internes s'appuie sur les connaissances du CERT de l'université Carnegie-Mellon, du NITFF, du NIST et de notre clientèle.

Traque des menaces par pointer-cliquer

La traque des menaces ne se limite pas aux dangers externes. Avec Proofpoint ITM, vous pouvez identifier les utilisateurs internes qui prennent des risques inutiles ou délibérés. Notre interface par pointer-cliquer permet d'explorer et de rechercher facilement et proactivement les comportements anormaux.

La traque des menaces simplifiée par pointer-cliquer vous offre les possibilités suivantes :

- Étudier les activités et les comportements à risque au sein de votre environnement
- Utiliser des groupes intelligents pour filtrer les milliers d'activités qui ne sont pas pertinentes et vous concentrer sur celles qui le sont
- Contextualiser les comportements anormaux grâce à une vue chronologique des activités et à des preuves basées sur des captures d'écran

Support pour la classification des données

Nos solutions s'intègrent à Microsoft Information Protection (MIP). Notre agent ITM lit les étiquettes de confidentialité en temps réel pendant que l'utilisateur interagit avec le fichier. Vous pouvez définir des règles de détection et de prévention en fonction de l'étiquette de confidentialité MIP du fichier, de son origine, de son type et de sa destination.

Prévention des fuites de données

Proofpoint ITM permet de prévenir l'exfiltration de données sensibles par le biais des canaux courants, notamment les périphériques USB tels que les dossiers de synchronisation locaux, les dispositifs de stockage réseau, les clés USB, les terminaux multimédias et les téléphones. La solution fonctionne même lorsque l'utilisateur est hors ligne.

Vous pouvez gérer les activités USB par utilisateur, groupe et hôte comme suit :

- Blocage de l'écriture de données sur les périphériques USB
- Mise sur liste d'autorisation de certains périphériques USB
- Blocage des fichiers correspondant à un modèle de nom de fichier
- Blocage de types de fichiers
- Blocage de sources de fichiers
- Application de règles de prévention globales

La suite Proofpoint Enterprise DLP peut étendre la protection à la messagerie et aux applications cloud.

Accélération de la réponse aux incidents

De nombreuses entreprises prennent des mesures contre les menaces internes suite à un événement de sécurité. La plupart d'entre elles estiment que les workflows génériques de leurs outils de sécurité existants ne sont pas efficaces contre les menaces internes. Les données internes sont sensibles et nécessitent une collaboration plus étroite avec les équipes qui ne sont pas en charge de la cybersécurité.

Contexte immédiat et preuves irréfutables

Nos workflows sont spécifiquement adaptés aux événements induits par des utilisateurs. Vous pouvez rechercher des événements de sécurité grâce à des mots-clés et à des filtres parmi toutes les métadonnées collectées et toutes les captures d'écran effectuées. En d'autres termes, vous n'avez pas besoin d'apprendre un tout nouveau langage de requête. Vous pouvez enregistrer les filtres pour une traque proactive des menaces ou pour référence ultérieure au cours d'une investigation.

À mesure que vous identifiez les alertes et les événements critiques liés aux investigations, vous pouvez les marquer et les catégoriser. Si vous avez besoin de partager des preuves, vous pouvez retrouver les alertes et les événements pertinents grâce à ces balises, puis les exporter dans des formats de fichier courants (PDF, par exemple). Ces rapports incluent des captures d'écran et des informations contextuelles sur les tenants et aboutissants des alertes et des événements (« qui, quoi, où et quand »). Cela facilite leur gestion par l'équipe de cybersécurité et leur compréhension par les équipes juridiques, de RH et de conformité, ainsi que par les analystes.

Avantages de l'architecture de Proofpoint ITM

Notre architecture cloud est conçue dans une optique d'évolutivité, de facilité d'utilisation, de sécurité et d'extensibilité. Elle utilise nos agents d'endpoint légers de pointe pour collecter des données sur les activités. Vous bénéficiez ainsi d'une visibilité inégalée et indépendante des applications sur les activités des utilisateurs au niveau des systèmes, sans que leur travail en soit perturbé.

Déploiement exclusivement SaaS

Proofpoint Endpoint DLP est une plate-forme SaaS moderne conçue dans une optique d'évolutivité, d'analyse, de sécurité, de confidentialité et d'extensibilité. Elle réduit le délai de configuration et les coûts en back-end, et simplifie la gestion continue pour les administrateurs en charge de la sécurité de toute l'entreprise. Vous bénéficiez ainsi d'une visibilité instantanée sur les mouvements de données.

Deux problèmes, une solution légère

Proofpoint Endpoint DLP et Proofpoint Insider Threat Management reposent sur le même agent léger et sur une architecture SaaS moderne. Lorsque les deux solutions sont utilisées conjointement, Proofpoint Endpoint DLP prévient les risques de fuites de données liés aux utilisateurs quotidiens, tandis que Proofpoint ITM étend cette protection à tous les comportements des utilisateurs malveillants et à plus haut risque.

EN SAVOIR PLUS

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