proofpoint.

FICHE TECHNIQUE

Proofpoint Communications Insights for Insider Threat Management

Informations sur les risques liés aux utilisateurs pour une détection proactive

Principaux avantages

- Identification des signaux d'alerte précoces avant que des actions nuisibles ne se produisent
- Visibilité complète sur l'intention et le comportement des utilisateurs
- Accélération de la prise de décisions grâce à des résumés générés par l'IA et à des informations contextuelles
- Intervention proactive permettant de prévenir de nouveaux dommages et de prendre des mesures appropriées
- Protection de la vie privée des collaborateurs en générant des alertes extrêmement fiables sans exposer l'intégralité des communications

Les menaces internes commencent par une intention

Les menaces internes commencent rarement par une action — elles commencent par une intention. Pourtant, la plupart des programmes de gestion des risques internes s'appuient principalement sur des signaux comportementaux. Ils détectent les violations de règles seulement après qu'une activité à risque s'est produite. Cependant, des signaux d'alerte critiques (tels que le ressentiment, la coercition, les griefs ou l'intention malveillante) apparaissent souvent en premier dans les communications professionnelles quotidiennes. Celles-ci incluent les emails, la messagerie et les plates-formes de collaboration.

Sans visibilité sur les signaux de communication, les équipes de sécurité ne disposent pas du contexte complet nécessaire pour anticiper les risques internes. Résultat : la détection est retardée et les investigations sont réactives. Les équipes manquent des opportunités d'intervenir avant que des données sensibles ne soient exposées ou que des dommages ne soient causés aux systèmes et réseaux.

Pourquoi adopter Proofpoint Communications Insights for ITM

Proofpoint Communications Insights for Insider Threat Management fournit un contexte plus approfondi sur l'intention des utilisateurs en analysant les communications professionnelles à la recherche d'indicateurs de comportements malveillants ou à risque. En fusionnant les informations sur les communications avec l'activité des utilisateurs sur l'endpoint, la solution aide les équipes de gestion des risques internes à détecter les menaces potentielles plus tôt. Il est important que les équipes comprennent non seulement ce que les utilisateurs font, mais aussi ce qu'ils pourraient penser ou planifier.

Une compréhension holistique des motivations et des actions permet une intervention plus rapide et proactive avant que des dommages ne surviennent. Vous obtenez ainsi un programme de gestion des risques internes plus mature qui réduit l'exposition, améliore le temps de réponse et favorise la conformité.

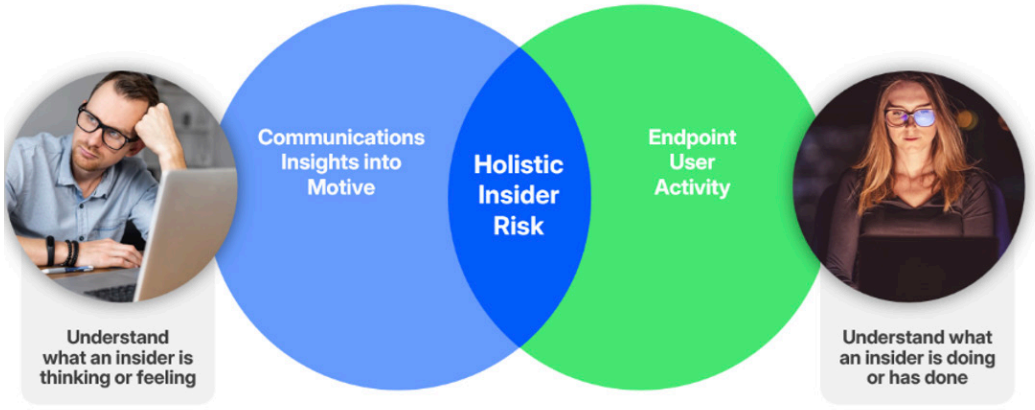

Figure 1. Proofpoint Communications Insights for ITM combine des informations sur les communications des utilisateurs et leur activité sur les endpoints.

Fonctionnement de Proofpoint Communications Insights for ITM

Proofpoint Communications Insights for ITM peut surveiller les communications des utilisateurs dans Microsoft 365 et Google Workspace. La surveillance de Microsoft 365 inclut Copilot, Mail, OneDrive, SharePoint, Teams et Viva Engage. La surveillance de Google Workspace inclut les emails, la voix, les SMS, les enregistrements d'appels et Google Chat.

L'analyse des risques liés aux communications des utilisateurs pilotée par l'IA identifie des indicateurs alignés sur le modèle Insider Threat Matrix™, un cadre industriel ouvert et public pour détecter et prévenir les menaces internes. Cette analyse identifie le sentiment des utilisateurs, y compris des états nuancés tels que le ressentiment, le mécontentement ou la coercition. L'analyse des communications des utilisateurs par l'IA est prise en charge pour plus de 100 langues et dialectes.

Lorsque Proofpoint Communications Insights for ITM identifie des communications d'utilisateurs comme à risque, une alerte est envoyée à Data Security Workbench, la console unifiée de Proofpoint Insider Threat Management. De là, les analystes en sécurité peuvent examiner des résumés générés par l'IA qui mettent en évidence des intentions potentiellement préoccupantes. Les analystes peuvent voir l'ensemble des conversations des utilisateurs uniquement lorsque cela est nécessaire. Cela garantit un accès contrôlé aux données sensibles et protège la vie privée des utilisateurs.

La solution conserve les communications des utilisateurs pendant 90 jours.

Détection proactive des risques internes

Proofpoint Communications Insights for ITM permet aux équipes de sécurité de passer d'investigations réactives à une détection proactive des menaces internes. Il unifie la motivation et le comportement dans une vue unique et exploitable des risques.

La combinaison d'une analyse des communications pilotée par l'IA et des données télémétriques sur les endpoints de Proofpoint ITM donne aux équipes de sécurité un aperçu de l'intention et du comportement des utilisateurs. Le contexte plus approfondi permet des investigations plus rapides et plus fiables. Les fonctionnalités de détection améliorées protègent la vie privée des collaborateurs.

Avec Proofpoint Communications Insights for ITM, vous pouvez profiter d'une détection proactive des risques internes avec :

- **Identification précoce des risques** – Obtenez une visibilité sur l'intention des utilisateurs grâce à une capture continue et à une analyse intelligente des communications professionnelles. Détectez les menaces potentielles plus tôt et avec plus de précision.
- **Informations sur le « pourquoi »** – Comprenez pourquoi les risques se produisent en ajoutant un contexte et une intention humains aux signaux techniques.
- **Accélération des investigations** – Grâce à une visibilité sur les signaux de communication et le comportement des endpoints, obtenez un contexte plus approfondi pour des investigations plus rapides.
- **Détection améliorée** – Libérez les analystes en sécurité de l'examen des communications non intentionnelles. Concentrez-vous sur des alertes extrêmement fiables, réduisant la charge opérationnelle.
- **Contrôles de la confidentialité** – Protégez la vie privée des utilisateurs en ne faisant remonter les risques que sous forme d'alertes, sans afficher l'intégralité des communications des utilisateurs.

proofpoint.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →