proofpoint.

FICHE SOLUTION

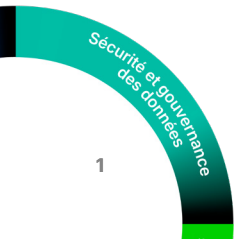
Proofpoint Insider Threat Management

Protégez votre entreprise contre les utilisateurs internes à risque

Principaux avantages

- Défense contre les préjudices financiers et les atteintes à la marque causés par des collaborateurs négligents, malveillants et compromis
- Détection proactive des comportements à risque grâce à une visibilité granulaire sur les indicateurs comportementaux
- Accélération des investigations grâce à des preuves irréfutables
- Collaboration efficace avec les RH, le département juridique et autres parties prenantes
- Protection de la vie privée des utilisateurs finaux et objectivité garantie lors des investigations
- Rentabilisation rapide grâce à un déploiement aisé et à un agent d'endpoint léger

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.



Les effectifs modernes et distribués travaillent de n'importe où. Les collaborateurs, les prestataires et les tiers n'ont jamais eu accès à autant de données, que ce soit sur leurs terminaux, dans la messagerie ou dans le cloud. Les changements organisationnels, tels que les fusions et acquisitions, les cessions et les restructurations, suscitent une incertitude qui peut déclencher des menaces internes. Les tensions géopolitiques et économiques, quant à elles, favorisent le cyberespionnage mené par des utilisateurs internes.

Ces dynamiques augmentent les risques de menaces internes pouvant entraîner le vol de secrets commerciaux et de propriété intellectuelle, la fraude, l'espionnage et le sabotage des systèmes. Toutes ces menaces peuvent infliger des dommages matériels, financiers, réputationnels et stratégiques à une entreprise. Pour traiter efficacement les risques internes, les équipes de sécurité ont besoin d'informations contextuelles sur les comportements à risque.

Proofpoint Insider Threat Management (ITM) offre une visibilité complète sur les utilisateurs internes négligents, malveillants et compromis. Il aide les équipes de sécurité à identifier les comportements à risque et à enquêter efficacement sur les incidents d'origine interne. Proofpoint ITM offre une approche centrée sur les personnes en fournissant des informations granulaires sur le comportement et les intentions des utilisateurs. Il vous permet de définir des règles, de trier les alertes, de traquer les menaces et de répondre aux incidents à partir d'une console centralisée. Grâce à des preuves numériques, vous pouvez enquêter rapidement et efficacement sur les violations d'origine interne. Plus un incident est résolu rapidement, moins les dégâts seront importants pour votre entreprise, votre marque et vos résultats financiers.

Réduisez les risques de sécurité de façon proactive

Visibilité complète sur les risques liés aux utilisateurs

Les menaces internes peuvent venir de n'importe où et survenir à tout moment. Cela en fait l'une des principales préoccupations en matière de cybersécurité des responsables de la sécurité des systèmes d'information (RSSI) à l'échelle mondiale. En utilisant Proofpoint Human Risk Explorer (HRE) avec Proofpoint ITM, vous pouvez consulter la notation des signaux de risque corrélés afin d'identifier et de réduire les risques émergents de façon proactive. Proofpoint HRE offre une compréhension complète des risques liés aux utilisateurs en analysant plusieurs dimensions au même endroit. Celles-ci incluent les vulnérabilités, les comportements, l'exposition aux attaques, la gestion des données sensibles, la sensibilisation à la sécurité et l'identité des collaborateurs.

Proofpoint HRE utilise également des informations basées sur des données pour formuler des recommandations. Par exemple, si un utilisateur adopte un comportement à risque, par exemple s'il télécharge d'importants volumes d'informations sensibles, vous pouvez intervenir immédiatement en appliquant des contrôles de sécurité plus stricts, en attribuant des formations ciblées ou en renforçant la surveillance. En vous concentrant d'abord sur les utilisateurs à haut risque, vous pouvez réduire considérablement les risques d'incidents et améliorer votre niveau de sécurité global.

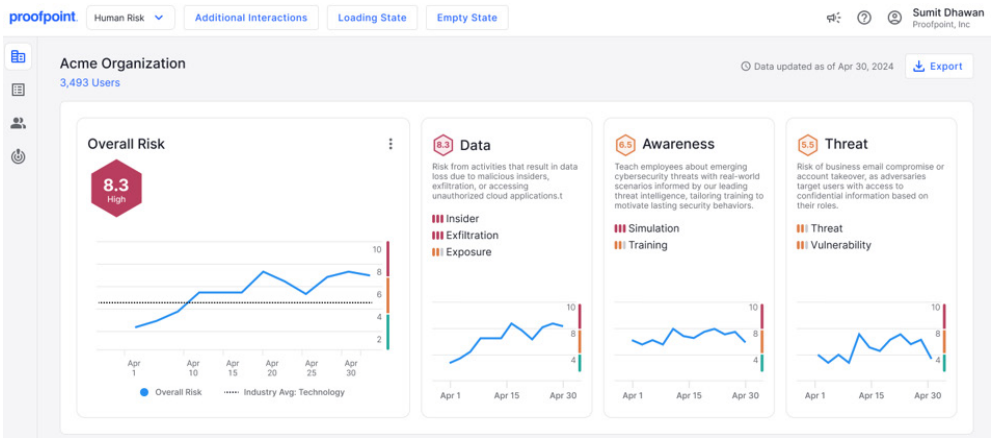


Figure 1. En utilisant Proofpoint Human Risk Explorer, vous pouvez facilement comprendre le risque global pour votre entreprise et le comparer à celui d'autres acteurs du secteur. Vous pouvez également obtenir des informations sur les risques associés aux utilisateurs internes, à l'exfiltration de données et à l'exposition de données.

Approche adaptative basée sur les risques

Pour atténuer les risques internes, la plupart des entreprises identifient les groupes à risque courants. Il s'agit d'individus ou d'équipes dont les rôles, les comportements ou les circonstances laissent penser qu'ils pourraient représenter un risque accru pour l'intégrité des systèmes et des données. Les groupes à risque courants incluent les collaborateurs qui s'apprêtent à quitter l'entreprise, les nouvelles recrues, les utilisateurs disposant d'un accès à privilèges, les cadres dirigeants, les prestataires, les utilisateurs qui se laissent piéger et bien d'autres encore.

Mais qu'en est-il des utilisateurs à risque inconnus ? La plupart des entreprises n'ont pas besoin de collecter en permanence des données télémétriques sur toutes les activités de tous les utilisateurs. À la place, Proofpoint propose une approche adaptative axée sur les risques. Les règles statiques et manuelles laissent la place à des règles qui s'ajustent automatiquement en temps réel, en fonction du comportement des utilisateurs.

Avec une approche adaptative, les règles dynamiques ajustent la surveillance des utilisateurs en fonction des comportements, et non selon des caractéristiques de risque prédéterminées. Par exemple, supposons qu'un utilisateur ne fait partie d'aucun groupe à risque. Lorsque cet utilisateur commence à copier des données sensibles sur une clé USB, Proofpoint ITM génère une alerte, ce qui déclenche une surveillance renforcée. Les règles de surveillance renforcée capturent des métadonnées détaillées et des captures d'écran pendant une période spécifiée. La surveillance n'a lieu que lorsqu'elle est nécessaire, ce qui assure la confidentialité et rationalise les alertes pour les analystes en sécurité. Avec une approche adaptative basée sur les risques, vous gagnez du temps et améliorez la précision de la détection.

Agent d'endpoint extrêmement stable et flexible

Pour offrir une approche adaptative basée sur les risques, Proofpoint utilise un seul agent d'endpoint léger qui prévient les fuites de données et fournit des informations approfondies sur le comportement des utilisateurs. Vous pouvez ajuster la quantité et les types de données collectés pour chaque utilisateur ou groupe d'utilisateurs. Cela vous aide à détecter les menaces à un stade précoce ainsi qu'à enquêter sur les alertes et y répondre efficacement, avec des coûts de traitement et de stockage moindres. L'agent en mode utilisateur de Proofpoint n'entre pas en conflit avec d'autres solutions et ne nécessite pas une importante puissance de traitement, ce qui garantit la stabilité, la productivité des utilisateurs et les performances.

Obtenez des informations en temps réel sur les comportements à risque

Visibilité granulaire sur les utilisateurs à risque

Pour vous aider à détecter les comportements à risque, Proofpoint offre une vue détaillée des mouvements de données sur les endpoints. Cela comprend les utilisateurs qui essaient de déplacer des données

sensibles, notamment via le chargement sur des sites Web non autorisés ou la copie dans des dossiers de synchronisation cloud. Cela inclut également les utilisateurs qui manipulent les types de fichiers (par exemple en modifiant les extensions de fichiers) ou qui renomment des fichiers contenant des données sensibles. Ces activités peuvent être le signe que les utilisateurs effacent les traces de leurs méfaits. Associées à un contexte supplémentaire, comme un collaborateur donnant son préavis et partant chez un concurrent, ces activités peuvent mettre en évidence un utilisateur à haut risque nécessitant des investigations plus approfondies.

Proofpoint offre également une visibilité sur l'utilisation des applications et la navigation Web. Les signaux de comportement à risque incluent l'installation et l'exécution d'outils non autorisés, la réalisation d'activités d'administration de la sécurité, la manipulation des contrôles de sécurité ou le téléchargement de logiciels malveillants. Proofpoint fournit des informations détaillées pour vous aider à comprendre tous les tenants et aboutissants (« qui, quoi, où et quand ») des activités à risque. Grâce au contexte et aux informations, vous pouvez mieux discerner les intentions des utilisateurs lorsque des comportements inhabituels se produisent.

Analyse du contenu et classification des données

Les données sensibles sont les plus exposées lorsqu'elles sont partagées ou transférées. Proofpoint analyse les données en mouvement et interprète les étiquettes de classification — comme Microsoft Information Protection (MIP) — pour s'assurer que les bonnes règles sont appliquées.

En tirant parti de vos investissements existants en matière de classification des données, vous pouvez identifier les informations métier sensibles, telles que les éléments de propriété intellectuelle, sans créer de workflow distinct pour les équipes de sécurité et les utilisateurs finaux. Toutefois, dans les cas où la classification des données ne permet pas d'identifier les données réglementées et les données clients de manière fiable, vous pouvez tirer parti des détecteurs de pointe de Proofpoint, y compris de la correspondance exacte des données (EDM) pour les données structurées et la correspondance des documents indexés (IDM) pour le contenu non structuré tel que la propriété intellectuelle. Ces méthodes avancées améliorent la précision de la détection et protègent vos informations les plus critiques.

MOUVEMENTS DE DONNÉES	**COMPORTEMENTS**
Alertes liées aux interactions avec les données et aux exfiltrations, 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/endpoint	Alertes liées aux comportements, notamment : • Dissimulation d'informations • Accès non autorisé • Contournement de 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 non autorisées d'administrateurs de bases de données (DBA) • Préparation d'une attaque • Sabotage informatique • Élévation de privilèges • Usurpation d'identité • Activités GIT suspectes • Utilisation inacceptable

Moteur de règles flexible et bibliothèque d'alertes

Avec Proofpoint ITM, vous pouvez créer de nouvelles règles et de nouveaux déclencheurs adaptés à votre environnement, ou ajuster nos scénarios de menaces prédéfinis. Vous pouvez modifier ces scénarios par groupes d'utilisateurs, applications, date/heure et degré de sensibilité, étiquettes de classification, sources et destinations, vecteurs de mouvement et types de données.

Proofpoint ITM comprend également des bibliothèques d'alertes prêtes à l'emploi qui facilitent la configuration et réduisent le délai de rentabilisation. Elles peuvent vous alerter des mouvements de données à risque ou des interactions suspectes sur les endpoints. Proofpoint peut en outre détecter un éventail plus large de comportements internes à risque. La bibliothèque de menaces internes comprend plus de 150 règles basées sur les directives du CERT et des recherches comportementales, ce qui vous offre un moyen simple et rapide de détecter les comportements à risque.

Prévention de l'exfiltration non autorisée de données à partir des endpoints

La détection des utilisateurs à risque et des mouvements de données suspects ne suffit pas toujours. Vous devez également bloquer les fuites de données en temps réel. Notre solution vous permet de prévenir les interactions contraires aux règles des utilisateurs avec des données sensibles : transfert de données vers et depuis des clés USB, synchronisation de fichiers avec des dossiers cloud, chargement sur le Web, copier-coller, impression et copie vers des terminaux mobiles, des cartes SD, des partages réseau, etc. Vous pouvez également empêcher les utilisateurs d'envoyer des données sensibles via des sites d'IA générative.

Vous pouvez personnaliser la prévention en fonction des utilisateurs, des groupes d'utilisateurs, des groupes d'endpoints, des noms de processus, de la clé USB, du numéro de série USB, du fournisseur USB, des étiquettes de classification des données, de l'URL source et des résultats de l'analyse du contenu.

Simplifiez et accélérez les investigations

Console unifiée

Proofpoint vous aide à optimiser la réponse aux incidents d'origine interne et les investigations. Pour bénéficier d'une visibilité multicanale, vous pouvez collecter des données télémétriques à partir des endpoints, de la messagerie et du cloud de manière centralisée. Cette console unifiée, appelée Data Security Workbench, propose des visualisations claires pour vous aider à surveiller les activités, à mettre en corrélation les alertes, à gérer les investigations, à traquer les menaces et à coordonner la réponse aux incidents. Cette vue centralisée vous permet de réduire vos coûts d'exploitation.

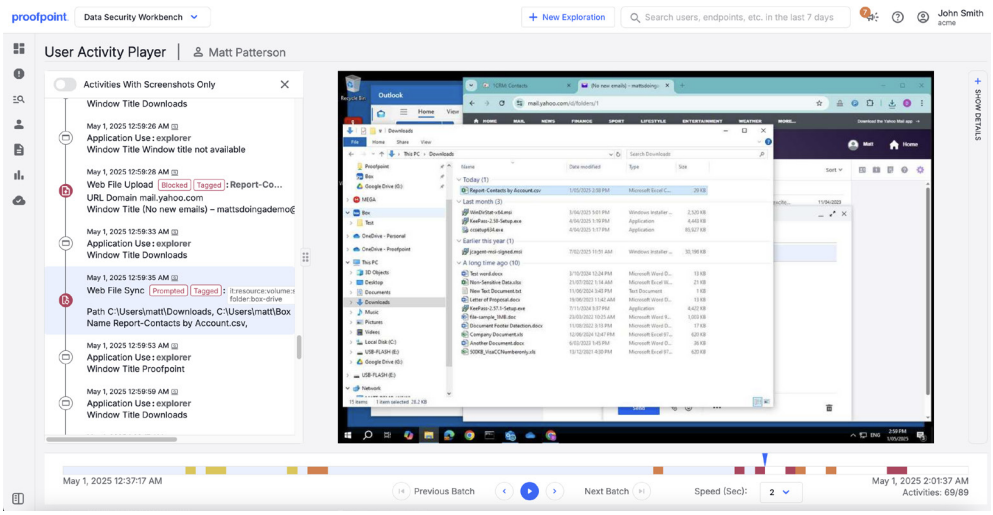


Figure 2. À partir du Data Security Workbench, vous pouvez voir ce qui s'est passé avant, pendant et après un incident d'origine interne grâce à une vue chronologique. Vous pouvez facilement consulter des captures d'écran pour obtenir du contexte supplémentaire et des preuves numériques.

Les puissantes fonctionnalités de recherche et de filtrage de Proofpoint 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. Vous pouvez accélérer les investigations grâce à la recherche assistée par l'IA utilisant des invites en langage naturel. Comme pour nos fonctionnalités de détection, vous pouvez adapter l'un des modèles d'exploration des menaces prêts à l'emploi ou créer le vôtre.

Tri des alertes

L'investigation et la résolution des alertes de sécurité causées par des utilisateurs internes ne sont pas toujours faciles. Ce processus peut être long et coûteux. De plus, ces opérations impliquent souvent d'autres départements non techniques comme les RH, la conformité, le département juridique et les chefs de service.

Avec Proofpoint, vous pouvez analyser chaque alerte de manière approfondie. Vous pouvez consulter les métadonnées et des informations contextualisées grâce à des vues chronologiques. Les équipes de sécurité peuvent identifier les événements qui doivent faire l'objet d'investigations plus poussées et ceux qu'elles peuvent clôturer immédiatement. Les informations contextualisées recueillies avant, pendant et après un incident d'origine interne fournissent du contexte sur les intentions d'un utilisateur. Il est essentiel de comprendre si un utilisateur est négligent, malveillant ou compromis pour décider des prochaines étapes.

Le workflow et les fonctionnalités de partage d'informations 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 exportations incluent des captures d'écran et des informations contextuelles. Cela peut aider les équipes non techniques, comme les RH et le département juridique, à interpréter les données à des fins d'investigation numérique et à prendre des décisions éclairées.

Captures d'écran pour la collecte de preuves numériques

Une image vaut parfois mille mots. Proofpoint peut prendre des captures d'écran de l'activité des utilisateurs.

Les RH, le département 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.

Si vous disposez d'une infrastructure de sécurité complexe, vous devrez peut-être conserver une seule source de vérité pour l'ensemble des systèmes, et donc conserver des captures d'écran, des extraits ou des fichiers à des fins d'investigation dans vos propres espaces de stockage. Proofpoint vous simplifie la tâche grâce à des exportations de données automatiques vers les espaces de stockage AWS S3, Microsoft Azure ou Google Cloud Platform qui vous appartiennent et que vous exploitez.

Trouvez le juste équilibre entre confidentialité et contrôles de sécurité

Un programme efficace de gestion des risques internes permet de trouver le juste équilibre entre la protection de la vie privée des utilisateurs et la sécurité des données, conformément aux réglementations en matière de confidentialité des données. Proofpoint adopte une approche de confidentialité dès la conception qui intègre la confidentialité au processus de conception du produit. Cela vous aide à protéger les droits des collaborateurs, à respecter les lois sur la confidentialité et à éviter les biais lors des investigations.

Emplacement et stockage des données

Proofpoint propose des centres de données dans plusieurs régions afin de vous aider à répondre aux exigences en matière d'emplacement et de confidentialité des données. Nous disposons actuellement de centres de données aux États-Unis, au Canada, en Europe, aux Émirats arabes unis, en Australie et au Japon.

Vous pouvez contrôler le stockage des données des endpoints grâce à des groupements d'endpoints. Chaque groupement peut être relié à un centre de données à des fins de stockage. Les clients peuvent ainsi séparer facilement les données d'un point de vue géographique.

Contrôles d'accès basés sur des attributs

Pour répondre aux exigences en matière de confidentialité, vous avez besoin de flexibilité et de contrôle sur l'accès aux données.

Avec Proofpoint, vous pouvez vous assurer que les analystes en sécurité ne voient que les données dont ils ont besoin. Par exemple, vous pouvez octroyer à un analyste un accès limité aux données d'un utilisateur spécifique ou limiter la durée pendant laquelle il peut accéder à ces données.

Anonymisation et masquage des données

L'anonymisation des informations personnelles garantit la protection de la vie privée des utilisateurs et élimine les biais lors des investigations. Proofpoint anonymise les données utilisateur qu'il collecte et ne stocke pas les noms complets ni les identifiants collaborateur des utilisateurs qui déclenchent des alertes. À la place, les analystes enquêtent sur les alertes en se basant sur des identifiants uniques et anonymisés. Lorsque l'identité d'un utilisateur doit être connue, l'analyste en sécurité peut demander la désanonymisation des données, laquelle peut être accordée par un administrateur.

Le masquage des données permet également de préserver leur confidentialité. Vous pouvez masquer des données sensibles telles que des données médicales protégées et des données personnelles.

Cela rend les données non identifiables dans l'interface utilisateur. Seules les personnes qui ont besoin d'accéder aux données peuvent les voir dans leur intégralité.

Améliorez l'agilité avec une approche moderne

Mise à l'échelle simple et rapide

Proofpoint est une solution native au cloud qui peut être facilement mise à l'échelle et qui s'adapte à l'évolution de vos besoins métier. Elle peut prendre en charge des centaines de milliers d'utilisateurs par locataire. De plus, elle se déploie rapidement et est facile à gérer. Cela garantit une rentabilisation rapide. Par ailleurs, Proofpoint s'intègre sans problème à votre écosystème existant grâce à une approche axée une API. Les webhooks facilitent l'ingestion des alertes par votre système de gestion des événements et des informations de sécurité (SIEM) et vos outils d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR), ce qui vous permet d'identifier et de trier rapidement les incidents.

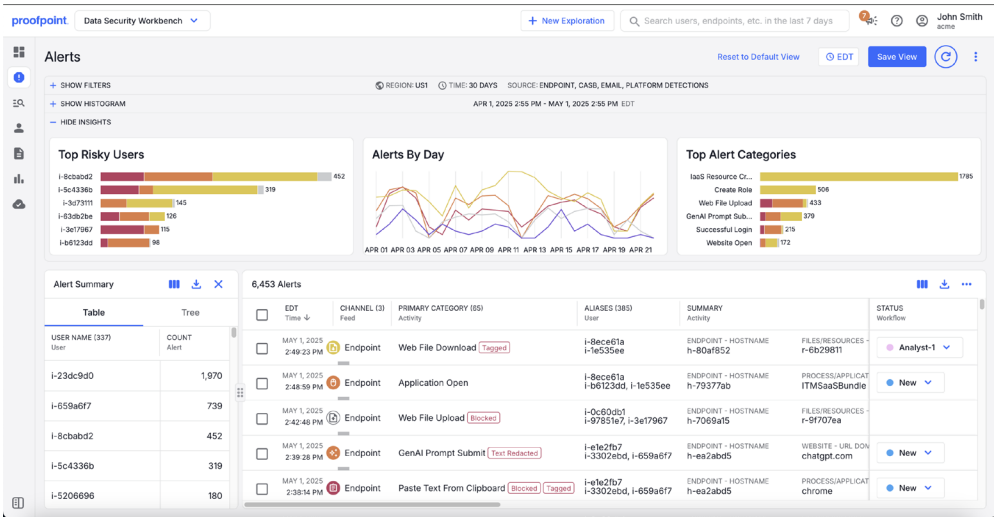


Figure 3. L'anonymisation protège l'identité des utilisateurs et contribue à garantir la confidentialité tout en éliminant les biais lors des investigations.

Prise en charge des changements à l'échelle de l'entreprise

Les changements organisationnels peuvent susciter le doute et l'incertitude, ce qui crée un environnement idéal pour les menaces internes. Les fusions et acquisitions, les licenciements imminents ou de nouvelles technologies telles que l'IA générative peuvent transformer les risques internes en menaces internes. Les équipes de gestion des risques internes ont besoin de visibilité et de contrôles pour prendre en charge les changements lorsqu'ils se produisent. À cette fin, Proofpoint leur offre une approche adaptative et basée sur les risques qui permet une détection et une prévention proactives.

Création et développement de votre programme

Un programme efficace de gestion des risques internes est une combinaison de personnes, de processus et de technologies. Proofpoint peut devenir votre partenaire de confiance pour garantir le succès de votre programme de gestion des risques internes. Nos services Premium fournissent l'expertise dont vous avez besoin pour optimiser votre programme, tirer parti de vos investissements technologiques et garantir l'adhésion et l'engagement des parties prenantes. Les services Advisory fournissent des conseils stratégiques et des services continus pendant que vous créez et améliorez votre programme. Les services Applied vous aident à optimiser votre investissement technologique, à soutenir vos opérations continues et à développer votre programme de gestion des risques internes.

proofpoint.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →