proofpoint.

FICHE SOLUTION

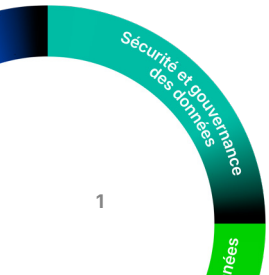
Proofpoint Data Loss Prevention

Transformez votre programme et votre architecture de sécurité des données.

Principaux avantages

- Prévention des fuites de données au niveau de la messagerie, du cloud et des endpoints
- Accélération de la résolution des incidents, avec tri des alertes DLP, investigations et réponse
- Déploiement rapide, évolution automatique et maintenance simplifiée
- Respect des exigences nationales/régionales en matière de confidentialité des données

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.



De nos jours, les collaborateurs peuvent mettre les données en péril de bien des façons. Ils sont de plus en plus nombreux à avoir recours à des outils de productivité non approuvés tels que l'IA générative. Ils utilisent également leurs terminaux personnels pour accéder aux applications cloud de leur entreprise. Les équipes de sécurité des données ont du mal à tenir la cadence, car on leur demande d'en faire plus avec moins pour assurer la confidentialité des données. Par ailleurs, les conséquences des compromissions de données sont de plus en plus dévastatrices, que ce soit sur le plan des pertes financières, de l'atteinte à la réputation et des non-conformités réglementaires. Les entreprises ont besoin d'une meilleure visibilité sur leurs données au niveau de la messagerie, du cloud et des endpoints, ainsi que sur le comportement de leurs utilisateurs. Malheureusement, les outils de prévention des fuites de données (DLP) d'ancienne génération ne répondent pas à ces besoins. Pire encore, ils sont souvent cloisonnés, coûteux et difficiles à gérer et à faire évoluer.

Les solutions Proofpoint Data Loss Prevention (DLP) vous permettent de transformer votre programme et votre architecture de sécurité des données. Nos solutions favorisent une approche adaptative de la DLP. Vous pouvez ainsi prévenir plus efficacement les fuites de données d'origine humaine au niveau de la messagerie, du cloud et des endpoints.

Proofpoint identifie avec précision les contenus sensibles et offre une visibilité étendue sur le comportement des utilisateurs. Une console unifiée vous aide à gérer les alertes et à enquêter sur les incidents sur tous les canaux. À l'aide d'analyses puissantes, vous pouvez évaluer rapidement les risques qui pèsent sur les données, parvenir à des verdicts très fiables et prendre des mesures appropriées. Nos solutions reposent sur une architecture native au cloud offrant des contrôles modernes de la confidentialité et un agent extrêmement stable. Elles évoluent automatiquement et sont faciles à déployer et à gérer.

Réduisez les risques pour la sécurité des données au niveau de la messagerie, du cloud et des endpoints

Visibilité étendue sur le comportement des utilisateurs

Proofpoint surveille la façon dont vos collaborateurs interagissent avec les données au niveau de la messagerie, des endpoints managés et non managés et des applications cloud telles que Microsoft 365, Google Workspace et Salesforce. Nous fournissons des informations sur les intentions des utilisateurs qui vous aident à répondre de manière appropriée aux risques qui pèsent sur les données. Nous détectons et prévenons également l'exfiltration de données sensibles, notamment via la copie de fichiers sur une clé USB non autorisée ou leur chargement dans un dossier cloud personnel.

Par le biais d'intégrations avec LDAP et Active Directory, Proofpoint vous aide à définir et à appliquer de façon dynamique des règles granulaires de chiffrement des emails. Nous collectons aussi des données télémétriques sur les comportements suivants :

- **Manipulation de fichiers** – comme le changement de nom de fichiers contenant des données sensibles ou la modification de leur extension
- **Utilisation de sites Web et d'applications** – comme le téléchargement de sauvegardes de données ou d'outils de piratage depuis le Web et leur installation
- **Comportements dangereux des utilisateurs les plus à risque** – comme la manipulation du registre Windows pour désactiver des contrôles de sécurité

© 2025 Proofpoint, Inc.

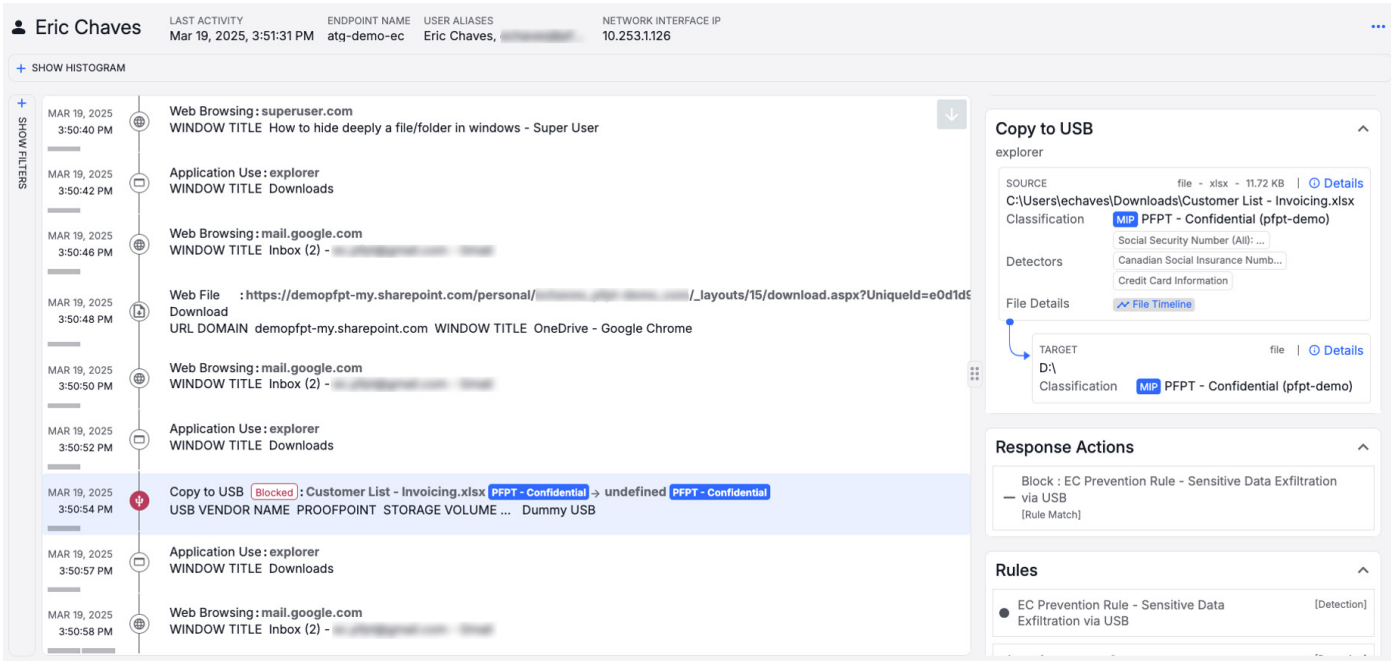


Figure 1. Sur cette capture d'écran de la console Data Security Workbench, un utilisateur visite un site Web intitulé « How to hide deeply a file/folder in Windows » (Comment dissimuler un fichier/dossier en profondeur sous Windows). L'utilisateur télécharge ensuite un fichier à partir du lecteur SharePoint de l'entreprise. Enfin, il copie un fichier confidentiel intitulé « Customer List – invoicing.xlsx » (Liste de clients – facturation.xlsx) sur une clé USB. La chronologie des activités de l'utilisateur et l'identification d'un contenu sensible indiquent à un analyste que l'utilisateur essaie de contourner les règles de l'entreprise et que des investigations plus poussées sont nécessaires.

Identification précise des contenus

Proofpoint emploie des méthodes avancées d'identification des contenus pour protéger vos données. Par exemple, dans le cloud, la correspondance exacte des données et la reconnaissance optique des caractères (OCR) peuvent détecter les numéros de dossier médical sur les images. Cela peut aider un établissement de santé, par exemple, à réduire les faux positifs et les faux négatifs.

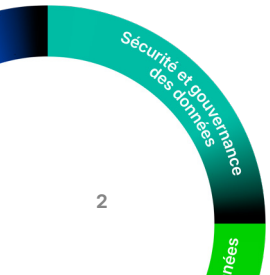
Vous pouvez créer des règles DLP intégrant des classificateurs basés sur de grands modèles de langage (LLM). Cela vous permettra de protéger les contenus sensibles récemment développés sans classification préalable — un véritable gain de temps. Et en combinant classificateurs LLM et correspondance de modèles, vous pourrez réduire les faux positifs.

Les alertes LLM facilitent la catégorisation des documents. Par exemple, si la mise en correspondance de modèles de numéros de sécurité sociale déclenche une alerte, Proofpoint pourra déterminer si le document en question est une déclaration d'impôt, un formulaire patient ou une demande de crédit, ce qui accélérera le tri et les investigations.

Application adaptative des règles

Grâce aux renseignements sur le comportement des utilisateurs et sur le mouvement des données sensibles, vous pouvez répondre aux risques pesant sur les données avec plus de précision. Proofpoint prévient les fuites de données sensibles via des invites d'IA générative. Nos solutions apprennent aux utilisateurs à modifier leur comportement, favorisant ainsi une utilisation acceptable de l'IA. Elles corrigent automatiquement le partage étendu de fichiers dans des applications cloud. Elles demandent également aux utilisateurs de fournir une justification lorsqu'ils copient des données sensibles dans un dossier cloud ou sur un lecteur réseau.

Les règles adaptatives vous permettent de surveiller les utilisateurs à haut risque de plus près. Vous bénéficiez ainsi d'un contexte approfondi et d'une meilleure compréhension des intentions de vos utilisateurs. Plutôt que d'ajuster manuellement les règles, vous pouvez automatiser la réponse aux comportements à risque. Ces règles dynamiques vous permettent de collecter des métadonnées supplémentaires et des preuves visuelles des activités des utilisateurs lorsqu'une alerte est générée. Grâce à une visibilité accrue et à des informations exploitables, vous accélérez le processus d'investigation et réduisez votre coût total de possession.



© 2025 Proofpoint, Inc.

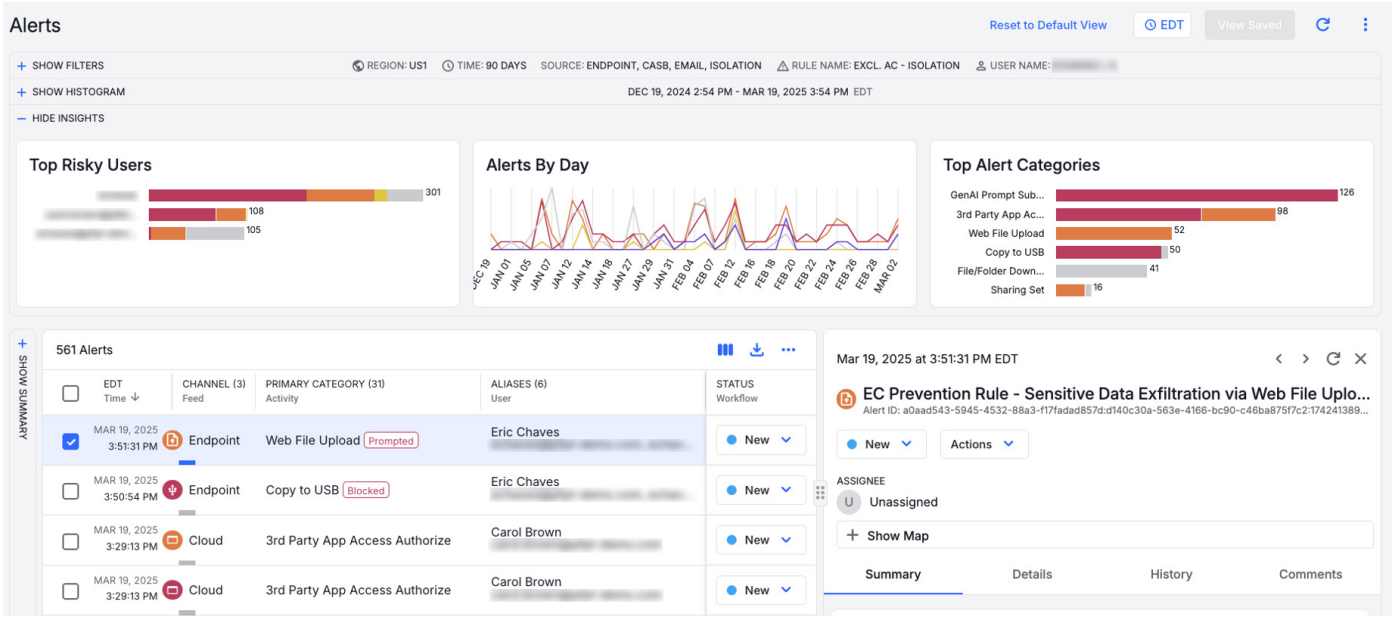


Figure 2. La console Data Security Workbench rationalise la gestion des alertes au niveau de la messagerie, du cloud et des endpoints, pour que vous n'ayez pas à jongler entre plusieurs consoles. Dans cet exemple, un analyste a filtré les alertes pour un utilisateur spécifique. La console montre que l'utilisateur a chargé des données sensibles sur son compte de messagerie d'entreprise, puis qu'il a essayé de copier un fichier sur une clé USB avant d'être bloqué.

Réduisez les coûts opérationnels et accélérez la résolution des incidents

Opérations DLP efficaces sur tous les canaux

Les équipes de sécurité qui utilisent des outils DLP cloisonnés ou d'ancienne génération peuvent subir des délais d'investigation prolongés et passer à côté d'infractions aux règles. Pour vous offrir une visibilité multicanale complète sur les risques pesant sur les données de manière centralisée, Proofpoint collecte des données télémétriques au niveau des applications cloud, des endpoints et de la messagerie. Cela permet de rationaliser le tri des alertes sur tous les canaux et d'accélérer les investigations et la réponse aux incidents. La console Data Security Workbench fournit des analyses puissantes, des visualisations intuitives et des workflows efficaces qui vous aident à :

- Enquêter sur les interactions des utilisateurs avec les données au sein d'une vue chronologique afin de déterminer leurs intentions et leur niveau de risque (figure 1)
- Trier et mettre en corrélation les alertes (figure 2)
- Retracer le cycle de vie d'un fichier (création, modification, partage)
- Coordonner la réponse aux incidents
- Utiliser des rapports de synthèse prêts à l'emploi pour démontrer l'efficacité et la couverture ainsi que générer des rapports personnalisés à des fins d'audit
- Mettre en œuvre et gérer des règles DLP cohérentes et des contrôles administrateur pour l'accès aux données et la confidentialité de celles-ci sur tous les canaux

Sécurité proactive des données

La console Data Security Workbench dispose d'une fonctionnalité avancée de recherche et de filtrage. Elle vous aide à créer des explorations personnalisées afin que vous puissiez gérer les risques pesant sur les données de façon proactive. Vous pouvez rechercher les tentatives d'exfiltration de données et autres activités à risque, telles que l'utilisation d'applications d'IA générative non approuvées. La chronologie des activités des utilisateurs vous aide à comprendre les tenants et aboutissants (qui, quoi, où, quand et pourquoi) de chaque incident de sécurité.

© 2025 Proofpoint, Inc.

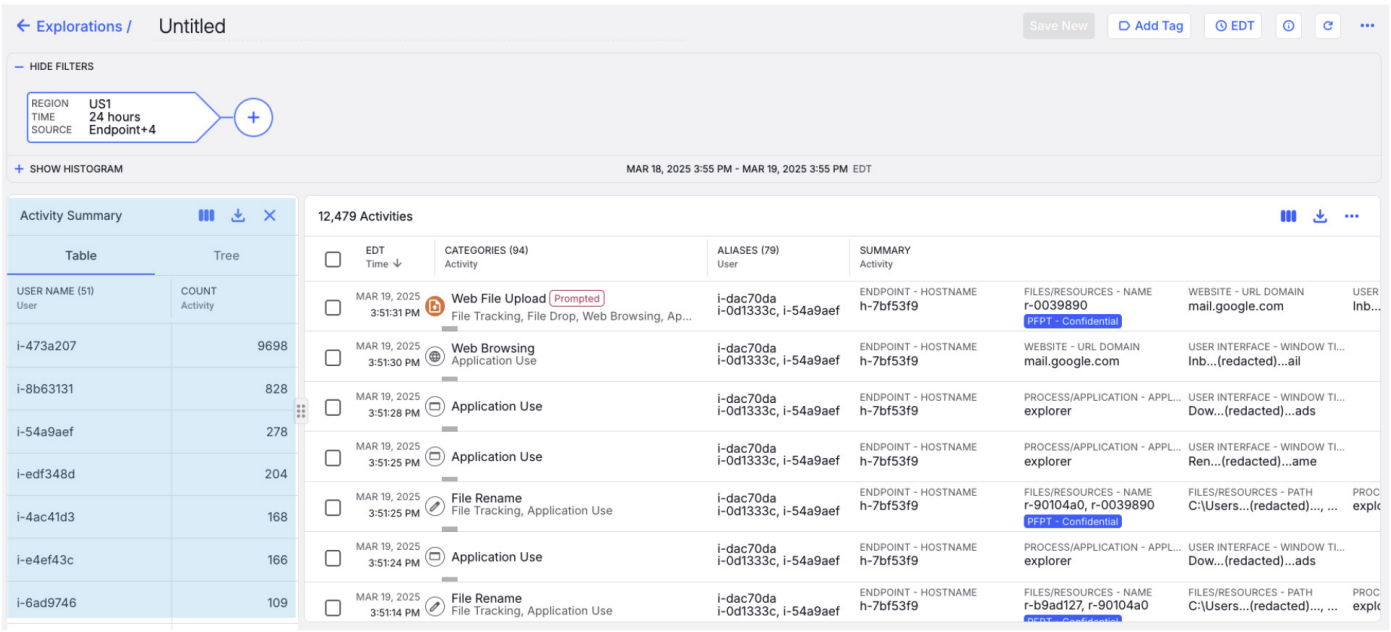


Figure 3. Comme on peut le voir sur la capture d'écran, la console anonymise les noms des utilisateurs. Cela protège la vie privée des utilisateurs faisant l'objet d'investigations et élimine les biais de la part des analystes.

Améliorez l'agilité avec une architecture moderne

Disponibles sous forme de services, nos solutions vous permettent de gagner un temps précieux. Elles se déploient rapidement, évoluent automatiquement et facilitent la maintenance. Elles sont modulaires et proposent des services partagés basés dans le cloud. Nos solutions multilocataires natives au cloud reposent sur une API et sont hautement évolutives. Elles peuvent prendre en charge des centaines de milliers d'utilisateurs par locataire. La plate-forme Proofpoint prend en charge des intégrations d'API avec des partenaires de l'écosystème comme Microsoft, Okta, Splunk et ServiceNow.

Contrôles granulaires de la confidentialité des données

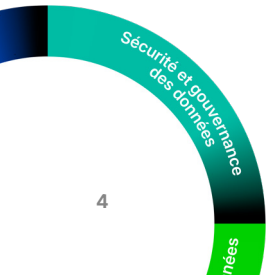
Bien que Proofpoint propose une console mondiale native au cloud, il peut stocker des données dans plusieurs régions. Vous pouvez utiliser des contrôles d'accès basés sur des attributs afin de gérer les alertes et les investigations pour l'ensemble des fonctions et des rôles régionaux. Vous pouvez également masquer les données sensibles et anonymiser les informations permettant d'identifier les utilisateurs (figure 3). Cela vous aidera à vous conformer aux exigences propres à chaque région du monde en matière d'emplacement et de confidentialité des données.

Agent d'endpoint extrêmement stable

Notre agent léger en mode utilisateur est stable et rapide à déployer. Il est capable de détecter les fuites de données et d'améliorer votre visibilité sur les menaces internes potentielles. En ajustant les règles sur la plate-forme, vous pouvez modifier le comportement de l'agent. Contrairement aux agents en mode noyau, l'agent Proofpoint offre une expérience utilisateur fiable. Vous réduisez ainsi le nombre de tickets d'assistance et permettez aux administrateurs de gagner du temps.

Délai de rentabilisation réduit grâce à notre expertise

La prévention des fuites de données n'est pas une mince affaire. Elle exige des connaissances techniques et des produits, ainsi qu'une compréhension approfondie de la gouvernance et de l'administration des données. Proofpoint peut devenir votre partenaire de confiance pour garantir le succès de votre programme DLP. Nos services Applied vous offrent l'expertise dont vous avez besoin pour optimiser votre investissement technologique, soutenir la continuité de vos opérations et faire évoluer votre stratégie de protection des données.



© 2025 Proofpoint, Inc.

Principales fonctionnalités des solutions Proofpoint DLP

Comparez nos solutions pour trouver la mieux adaptée à votre entreprise.

PRINCIPALES FONCTIONNALITÉS	PROOFPOINT DLP TRANSFORM	PROOFPOINT DLP TRANSFORM ADVANCED	MODULES COMPLÉ-MENTAIRES
Contexte détaillé sur les utilisateurs et les fichiers	✓	✓	
Traque des menaces pour une détection et des investigations proactives	✓	✓	
Agent unique en mode utilisateur pour la gestion des menaces internes et la DLP	✓	✓	
Détections DLP enrichies (RegEx, OCR, IDM, EDM) et classification MIP	✓	✓	
Surveillance et détection des mouvements des fichiers avec traçabilité des données	✓	✓	
API, proxys inverses et de transfert	✓	✓	
Détecteurs étendus d'applications cloud	✓	✓	
Gestion unifiée des alertes et configuration DLP	✓	✓	
Contrôles granulaires de la confidentialité des données et des accès	✓	✓	
Intégration à l'écosystème de sécurité (SIEM/SOAR/Teams)	✓	✓	
Détection et analyse des données sensibles dans les emails et les pièces jointes		✓	
Chiffrement dynamique des emails externes et internes		✓	
Analyse de l'empreinte numérique des documents sensibles dans les emails		✓	
Prévention optimisée par l'IA des fuites de données accidentelles et intentionnelles par email			✓
Identification et classification des banques de données			✓
Détection et correction des risques d'exposition dans les banques de données			✓
Capture visuelle des menaces internes			✓

proofpoint.

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs. ©Proofpoint, Inc. 2025

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →