proofpoint.

FICHE SOLUTION

Proofpoint Enterprise DLP

Transformez votre programme et votre architecture de sécurité des données

Principaux avantages

- Prévention des fuites de données via la messagerie électronique, le cloud, les endpoints et les applications d'IA générative
- Accélération de la résolution des incidents, notamment du tri des alertes DLP, des investigations et de la réponse
- Déploiement rapide, évolution automatique et simplification de la maintenance
- Respect des exigences en matière de confidentialité des données aux États-Unis et dans d'autres régions

Les travailleurs d'aujourd'hui mettent en danger les données de multiples manières. Ils utilisent des terminaux personnels pour accéder aux applications cloud et partager des données via la messagerie électronique, des endpoints et des outils de collaboration. En outre, les outils d'IA générative non approuvés sont souvent à portée de clic du navigateur. Les équipes de sécurité travaillent plus dur pour protéger la vie privée, maintenir la conformité et soutenir l'adoption responsable de l'IA générative. Les compromissions ont désormais des conséquences croissantes sur le plan financier, de la réputation et des audits.

Les entreprises ont besoin d'une meilleure visibilité sur les données sensibles. Elles doivent également observer comment les utilisateurs gèrent ces données au niveau de la messagerie électronique, du cloud, des endpoints et des applications d'IA générative. Cependant, les outils de prévention des fuites de données (DLP) d'ancienne génération sont souvent cloisonnés, difficiles à faire évoluer et incohérents d'un canal à l'autre. Ils sont également incapables de faire face aux risques émergents liés à l'IA.

Proofpoint Enterprise DLP favorise une approche unifiée et adaptative de la prévention des fuites de données (DLP). Il contribue à prévenir les fuites de données causées par des personnes via la messagerie électronique, le cloud, les endpoints et les applications d'IA. Il aide également les équipes de sécurité à travailler plus efficacement.

Proofpoint identifie les contenus sensibles et montre comment les collaborateurs les utilisent. La console unifiée vous aide à gérer les alertes et à enquêter sur les incidents sur tous les canaux. Les analyses et la classification par IA aident les équipes à évaluer les risques liés aux données, à prendre de meilleures décisions et à agir rapidement. La solution fonctionne dans le cloud, évolue automatiquement et est facile à déployer et à gérer. Elle est également dotée de contrôles de confidentialité modernes et d'un agent extrêmement stable.

Réduisez les risques pour la sécurité des données sur tous les canaux

Une vision claire du comportement des utilisateurs

Proofpoint surveille comment les travailleurs utilisent les données au niveau de la messagerie électronique, des endpoints gérés et non gérés, des outils d'IA générative et des applications cloud (Microsoft 365, Google Workspace, Salesforce, etc.). Il révèle l'intention des utilisateurs et détecte et prévient les exfiltrations. Par exemple, la copie de fichiers sur une clé USB non autorisée, le chargement de fichiers sensibles dans un dossier cloud personnel ou le partage d'informations confidentielles via des invites d'IA.

Proofpoint aide les entreprises à adopter l'IA générative en toute sécurité. Il détecte, bloque et masque les données sensibles avant qu'elles ne soient partagées avec des applications d'IA approuvées ou non approuvées. Les équipes peuvent appliquer des règles dans les applications d'IA de navigateur et de bureau. Des mesures correctives intelligentes et des expériences utilisateur guidées aident les utilisateurs à rester productifs.

Proofpoint surveille et contrôle ce qui suit :

- Chargements de fichiers dans des applications d'IA
- Activités de copier-coller impliquant des données sensibles
- Invites d'IA contenant des informations réglementées ou propriétaires
- Pièces jointes sensibles partagées par le biais de la messagerie électronique et d'outils de collaboration cloud
- Comportements à risque des utilisateurs sur les endpoints et les services cloud

Proofpoint s'intègre à LDAP et à Active Directory. Vous pouvez utiliser les groupes de ces répertoires pour définir et appliquer dynamiquement des stratégies détaillées de chiffrement des emails. Notre solution suit les comportements tels que les suivants :

- **Modifications de fichiers**, comme le changement de nom de fichiers contenant des données sensibles ou la modification de leur extension
- **Utilisation inhabituelle de sites Web et d'applications**, y compris le téléchargement de sauvegardes de données ou d'outils de piratage
- **Actions dangereuses d'utilisateurs à haut risque**, y compris la manipulation du registre Windows pour désactiver les contrôles de sécurité

Identification précise des contenus et classification par IA

Proofpoint améliore la précision de détection avec plus de 110 classificateurs prêts à l'emploi pilotés par l'IA. Ceux-ci identifient les catégories de documents et ajoutent un contexte métier aux alertes DLP. Ils fonctionnent avec les technologies de correspondance de modèles, de correspondance exacte des données (EDM), de correspondance de documents indexés (IDM), de reconnaissance optique de caractères (OCR) et d'analyse de l'empreinte numérique. Cette combinaison réduit les faux positifs et améliore la protection sur tous les canaux.

La classification personnalisée autonome de Proofpoint utilise de grands modèles de langage (LLM) pour identifier les contenus sensibles de chaque entreprise, et cela sans ajustement manuel. Les équipes peuvent rapidement trouver et protéger les données propriétaires (code source, modèles financiers, documents techniques, dossiers clients, etc.). Cela simplifie la création de règles et réduit le délai de rentabilisation.

Les moteurs de détection partagés pilotés par l'IA offrent une protection cohérente sur tous les canaux DLP d'entreprise. Les entreprises peuvent détecter et classer les données personnelles, les données médicales protégées, les données du secteur des cartes de paiement, les identifiants de connexion, la propriété intellectuelle et les informations métier confidentielles. Les alertes enrichies par des LLM ajoutent du contexte afin que les équipes puissent enquêter et réagir plus rapidement.

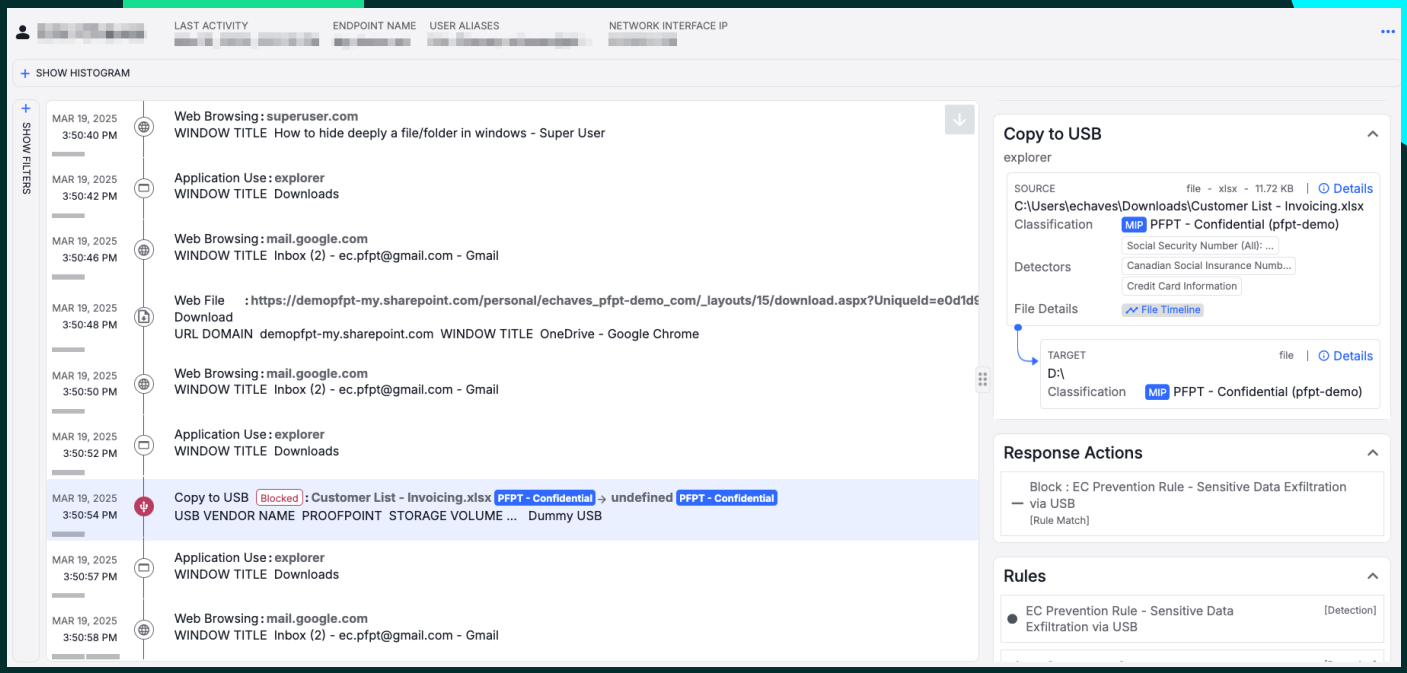

Figure 1. Cet exemple de Data Security Workbench montre une séquence à risque d'actions des utilisateurs. L'utilisateur recherche des moyens de cacher un fichier, télécharge un fichier sensible à partir de SharePoint et tente de le copier sur une clé USB.
Les actions et la chronologie associée laissent entrevoir un possible contournement des règles qui nécessite un examen plus approfondi.

Application adaptative des règles et correction guidée

Proofpoint propose une application partagée des règles sur tous les canaux DLP. Les équipes peuvent définir une seule fois les règles et les appliquer de manière cohérente.

Les règles adaptatives aident les équipes à surveiller les utilisateurs à haut risque, à comprendre leur intention et à automatiser les réponses. Lorsqu'une alerte apparaît, ces règles recueillent davantage de métadonnées et de preuves visuelles. Des informations plus claires aident les analystes à enquêter plus rapidement et à réduire le coût total de possession.

Proofpoint prévient également les fuites de données sensibles via des invites d'IA générative. Notre solution guide les utilisateurs vers une utilisation plus sûre de l'IA. Elle corrige automatiquement le partage étendu de fichiers dans les applications cloud. Elle demande également aux utilisateurs de justifier la copie de données sensibles dans un dossier cloud ou sur un lecteur réseau.

Réduisez les coûts opérationnels et accélérez la résolution des incidents

Opérations DLP efficaces sur tous les canaux

Les équipes utilisant des outils DLP cloisonnés et d'ancienne génération sont souvent confrontées à des investigations lentes, à une visibilité fragmentée et à des violations manquées des règles. Proofpoint centralise la détection, les règles et les contrôles de gouvernance sur tous les canaux DLP. Data Security Workbench centralise également la télémétrie et les alertes. Cela aide les équipes à trier, à enquêter et à réagir plus rapidement.

La console Data Security Workbench offre les avantages suivants :

- Vues chronologiques des interactions des utilisateurs avec des données sensibles (voir figure 1)
- Gestion unifiée des alertes et configuration de la DLP (voir figure 2)
- Investigations liées au niveau de la messagerie électronique, du cloud, des endpoints et des applications d'IA
- Suivi de la traçabilité des fichiers à mesure de leur création, de leur modification et de leur partage
- Traque des menaces pour détecter et enquêter plus tôt sur les risques
- Tableaux de bord pour les dirigeants et rapports d'audit

Sécurité proactive des données

Data Security Workbench vous permet de rechercher et de filtrer les risques liés aux données. Vous pouvez créer des vues personnalisées pour gérer ces risques avant qu'ils ne se développent. 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 utilisateurs montre qui a fait quoi, où, quand et pourquoi.

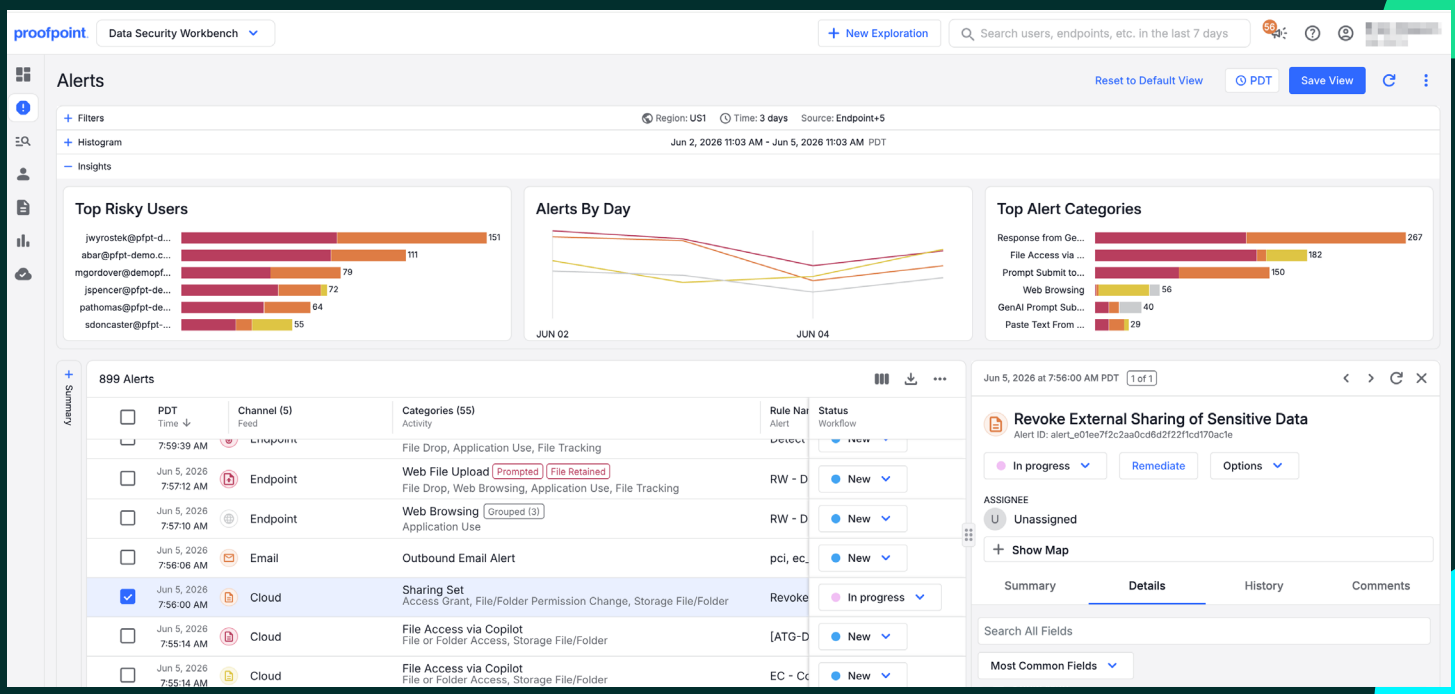

Figure 2. Dans Data Security Workbench, vous pouvez créer des explorations personnalisées des risques liés aux données.

Améliorez l'agilité avec une architecture moderne

Les solutions Proofpoint sont fournies sous forme de services, ce qui vous permet de gagner un temps précieux. Elles se déploient rapidement, évoluent automatiquement et simplifient la maintenance. Elles sont modulaires et utilisent des services cloud partagés. Nos solutions natives au cloud prennent en charge plusieurs locataires et API. Elles sont conçues pour évoluer. Elles peuvent prendre en charge des centaines de milliers d'utilisateurs par locataire. La plate-forme Proofpoint s'intègre à des partenaires tels que Microsoft, Okta, Splunk et ServiceNow.

Contrôles granulaires de la confidentialité des données

Proofpoint propose une console mondiale native au cloud et peut stocker des données dans plusieurs régions. Les contrôles d'accès basés sur des attributs limitent qui peut consulter les alertes et les investigations par rôle, fonction ou région. Le masquage des données et l'anonymisation des utilisateurs (voir figure 3) aident à respecter les règles régionales en matière de confidentialité et de résidence des données.

Agent d'endpoint extrêmement stable

Notre agent léger en mode utilisateur est stable et rapide à déployer. Il est unique dans la manière dont il détecte les fuites de données et les menaces internes potentielles. Vous pouvez modifier le comportement de l'agent en mettant à jour les règles sur la plate-forme. Contrairement aux agents en mode noyau, l'agent Proofpoint offre une expérience utilisateur fiable. Cela peut réduire le nombre de tickets d'assistance et faire gagner du temps aux administrateurs.

Délai de rentabilisation réduit grâce à notre expertise

La prévention des fuites de données nécessite une expertise technique et produit ainsi que de solides compétences en gouvernance des données. Les services Proofpoint Applied vous aident à tirer davantage parti de votre investissement, à soutenir des opérations continues et à faire évoluer votre programme de protection des données.

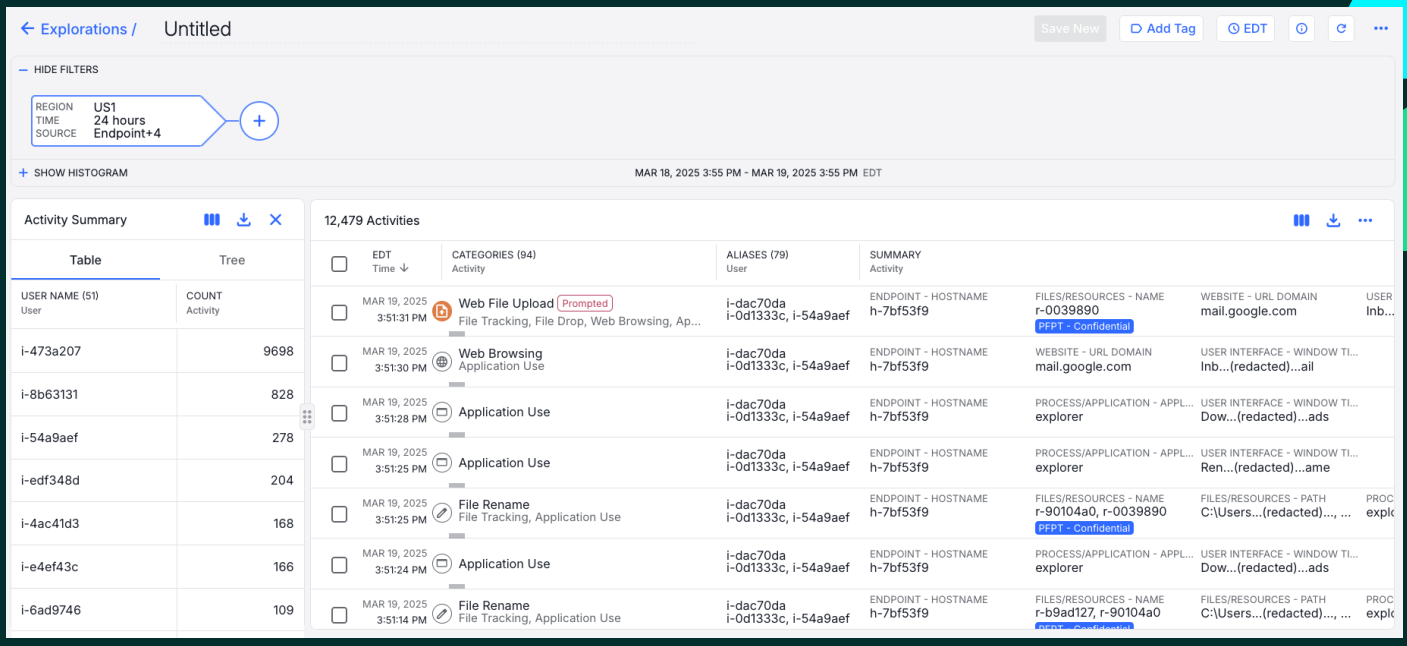

Figure 3. La console peut anonymiser les informations des utilisateurs lors d'investigations. Cela protège leur vie privée et aide à réduire le biais des analystes.

Principales fonctionnalités et capacités	Proofpoint DLP Transform niveau 1	Proofpoint DLP Transform niveau 2	Modules complémentaires
Contexte détaillé sur les utilisateurs et les fichiers	✓	✓	
Traque des menaces pour détecter et enquêter plus tôt	✓	✓	
Agent unique en mode utilisateur pour la gestion des menaces internes et la DLP	✓	✓	
Détecteurs DLP enrichis (RegEx, OCR, IDM, EDM) et classification MIP	✓	✓	
IA prête à l'emploi et classificateurs autonomes pilotés par l'IA	✓	✓	
Traçabilité des données pour surveiller et détecter les mouvements de fichiers	✓	✓	
API, proxys inverses et de transfert	✓	✓	
Détecteurs étendus d'applications cloud	✓	✓	
Gestion unifiée des alertes et configuration de la 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 ou 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			✓
Découverte et classification des banques de données			✓
Détection et atténuation de l'exposition aux risques dans les banques de données			✓
Capture visuelle des menaces internes			✓

En savoir plus

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

À propos de Proofpoint, Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et en toute confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr

Suivez-nous : LinkedIn

proofpoint.