proofpoint.

Contrôles d'accès et de confidentialité pour Proofpoint Information Protection

Respectez les exigences de conformité tout en protégeant les droits des collaborateurs et en éliminant les biais

Principaux avantages

- Conservation de la confiance des collaborateurs
- Protection des informations métier stratégiques
- Conformité aux lois en matière de confidentialité
- Prévention des biais lors des investigations

Préserver la confidentialité des données est une tâche de plus en plus importante et complexe. L'accélération de la transformation numérique, la généralisation du travail hybride et la prolifération des applications cloud ont rendu la sécurisation des données sensibles encore plus difficile. À mesure que les entreprises continuent à amasser des volumes croissants de données, leur valeur perçue augmente. Malheureusement, cette valeur accrue s'accompagne également d'un risque de fuite et de vol de données, y compris par des utilisateurs internes.

Malgré les difficultés grandissantes, les entreprises ne peuvent pas se permettre de faire des erreurs. Les entreprises du monde entier sont soumises à une pression croissante pour se conformer aux lois strictes en matière de confidentialité des données, qui imposent la prise de mesures robustes de sécurité et de confidentialité des données. Les non-conformités peuvent être coûteuses ; les lourdes amendes et les pertes de marchés sont monnaie courante. Selon plus d'un tiers des professionnels de la sécurité, les amendes et les infractions réglementaires sont une conséquence des fuites de données[1].

Proofpoint propose une suite complète de solutions conçues pour renforcer la sécurité des données et gérer les menaces internes, tout en assurant la conformité aux réglementations en matière de confidentialité des données. La gamme de solutions Proofpoint Information Protection met en œuvre des contrôles d'accès et de confidentialité robustes. Elle limite la visibilité aux seules personnes qui en ont vraiment besoin et préserve l'anonymat des utilisateurs en assurant la confidentialité des données d'identification. De ce fait, Proofpoint renforce la sécurité des données et contribue à éliminer les biais lors de vos investigations. Vous bénéficiez ainsi d'une approche équilibrée de la sécurité des informations.

Approche axée sur la confidentialité

Proofpoint Information Protection repose sur des principes de confidentialité dès la conception. Cette méthodologie suit une approche proactive de la protection des données. Elle place la confidentialité en première ligne de la conception des systèmes pour garantir que les systèmes informatiques, l'infrastructure et les processus métier intègrent dès le début la confidentialité en tant qu'élément central. Cette approche place la visibilité, la transparence et la centricité utilisateur au cœur de sa conception.

1 Rapport Data Loss Landscape 2024 de Proofpoint

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.

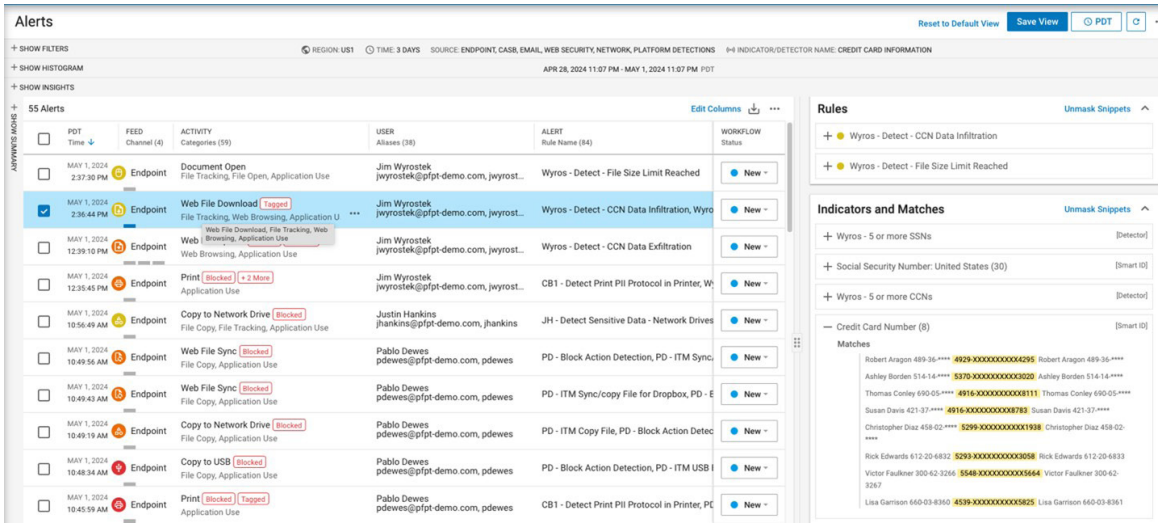

Figure 1. Masquage des numéros de carte de crédit dans Proofpoint Information Protection

Gérez l'emplacement et le stockage des données

Proofpoint place des centres de données régionaux de manière stratégique aux États-Unis, au Canada, en Europe, en Australie et au Japon pour satisfaire les exigences en matière de confidentialité et d'emplacement des données. Vous bénéficiez d'un contrôle total sur l'emplacement de stockage de vos données dans tous ces centres de données.

Pour gérer le stockage des données des endpoints, Proofpoint vous permet de créer des groupements d'endpoints. Chaque groupement peut être associé à un centre de données spécifique, ce qui vous permet de séparer facilement les données d'un point de vue géographique. Par exemple, un groupement aux États-Unis peut gérer les données des endpoints des États-Unis, qui sont envoyées au centre de données des États-Unis.

Assurez la confidentialité grâce à des contrôles d'accès basés sur des attributs

Les contrôles d'accès basés sur des attributs de Proofpoint Information Protection offrent un moyen flexible et efficace de gérer l'accès aux données. Ils permettent de s'assurer que les analystes en sécurité ne disposent d'une visibilité sur les données que si cela est absolument nécessaire.

Par exemple, vous pouvez définir des règles granulaires et attribuer un accès de façon à ce qu'un analyste en sécurité basé aux États-Unis ne puisse voir que les données des États-Unis, et non les données provenant d'Europe ou de la région Asie-Pacifique. Ce niveau de contrôle d'accès spécifique réduit considérablement le risque d'exposition inutile des données. Et lorsqu'un analyste a besoin d'accéder aux données d'un utilisateur spécifique dans le cadre d'investigations, l'administrateur système peut également limiter cet accès dans le temps, c'est-à-dire définir la durée pendant laquelle l'analyste peut accéder à ces données.

Assurez la confidentialité des données grâce au masquage des extraits

Proofpoint Information Protection propose une fonctionnalité de masquage des données pour assurer leur confidentialité. Le masquage des données dissimule les données d'investigation numérique sensibles, telles que les données médicales protégées et les données personnelles dans la console, afin que ces informations ne soient pas identifiables. Cette approche garantit que seules les personnes qui ont besoin d'accéder aux données peuvent les consulter dans leur forme complète et non masquée.

Les administrateurs système peuvent définir les identifiants de données qu'ils souhaitent masquer. Ils peuvent par exemple décider de n'afficher que les quatre derniers chiffres d'un numéro de carte de crédit et masquer tout le reste. Ils peuvent également décider du type et de la quantité de données auxquels les utilisateurs peuvent accéder en fonction de leur rôle. Par exemple, ils peuvent spécifier que seuls les analystes autorisés peuvent voir des extraits de données sensibles.

Protégez les données des utilisateurs grâce à l'anonymisation

Proofpoint Information Protection protège également les données des utilisateurs grâce à l'anonymisation, ce qui vous permet de masquer l'identité d'un utilisateur. Vous pouvez anonymiser le nom d'utilisateur, le nom d'hôte, l'adresse IP, les informations de localisation et les noms de fichiers.

L'anonymisation garantit que seuls les analystes en sécurité autorisés peuvent consulter les données d'identification des utilisateurs surveillés. Ce processus contribue également à éliminer les biais lors des investigations. Imaginez le scénario suivant : un dirigeant vient d'enfreindre une règle de l'entreprise. Si son identité était connue, l'incident pourrait être traité différemment ou un analyste en sécurité pourrait fermer les yeux sur l'infraction.

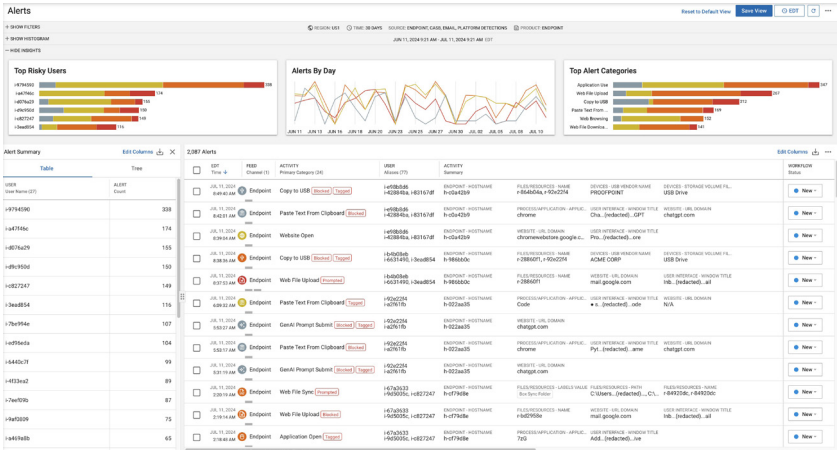

Figure 2. Aperçu des données anonymisées des utilisateurs dans Proofpoint Information Protection

Lorsque l'identité d'un utilisateur doit être connue plus en aval au cours d'investigations, l'analyste en sécurité peut demander la désanonymisation des données, laquelle peut être accordée par un administrateur.

Trouvez le juste équilibre entre sécurité et confidentialité des données

Dans toute entreprise, il est important de trouver le juste équilibre entre sécurité et confidentialité des données. Pour y parvenir, gardez les principes suivants en tête :

- **Surveillez les principaux canaux de fuite de données.** Concentrez vos efforts de protection des données sur les méthodes de travail. La plupart des fuites et des expositions de données passent par la messagerie, des applications cloud et des clés USB.
- **Soyez clair et transparent.** Assurez-vous que vos collaborateurs connaissent les règles de l'entreprise en matière de sécurité et de confidentialité des données. Expliquez-leur clairement ce que vous surveillez. Vous instaurerez ainsi un climat de confiance.
- **Formez les utilisateurs aux notifications automatisées.** Lorsqu'un utilisateur enfreint les règles de l'entreprise, une notification peut être générée automatiquement pour l'en informer. L'envoi d'une notification automatisée permet d'avertir l'utilisateur de son comportement à risque tout en éliminant la honte et l'émotion associées à un entretien avec son responsable ou les RH.
- **Faites des choix.** Vous n'avez pas besoin de collecter des données sur tout et tout le monde. Déterminez quelles données sont importantes et ce que vous avez vraiment besoin de savoir sur les activités des collaborateurs.
- **Contrôlez l'accès aux données.** Bien que les administrateurs de la sécurité, les analystes, le service juridique et les RH puissent bénéficier d'un accès illimité aux données concernant les collaborateurs, ce n'est pas toujours une bonne chose pour la confidentialité. Assurez-vous donc d'utiliser les contrôles d'accès fournis par les outils DLP et ITM.

Garantissez la confidentialité des données avec Proofpoint

Les solutions Proofpoint Information Protection telles que Data Loss Prevention et Insider Threat Management permettent d'assurer le plus haut niveau de protection des données tout en garantissant la conformité aux réglementations en matière de confidentialité des données. Elles contribuent également à éliminer les biais lors de vos investigations. Proofpoint Information Protection tient compte des contenus et des comportements afin que vous puissiez identifier les données sensibles ou réglementées ainsi que signaler les activités à risque et les intentions malveillantes – le tout à partir d'une console centralisée qui offre une visibilité sur l'ensemble des canaux, dont les endpoints, la messagerie, le cloud et le Web.

Proofpoint Managed Information Protection réunit les personnes, les processus et les technologies appropriés. Vous pouvez ainsi concevoir, mettre en œuvre et développer votre programme afin d'optimiser la protection et de garantir la confidentialité des données.

EN SAVOIR PLUS

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