Proofpoint Endpoint DLP et Proofpoint ITM

Bénéficiez d'une protection centrée sur les personnes contre les fuites de données et les menaces internes au niveau de l'endpoint

Produits

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

Principaux avantages

- Réduction du risque de fuite de données sensibles et de menaces internes
- Simplification de la réponse aux incidents d'origine interne et aux violations des règles
- Réduction du délai de rentabilisation des programmes de prévention des menaces internes et des fuites de données

Les effectifs modernes peuvent travailler de n'importe où. Les collaborateurs, les prestataires et les tiers n'ont jamais eu accès à autant de données, que ce soit sur leur ordinateur portable, dans la messagerie ou dans le cloud. Le risque de fuite de données atteint donc des niveaux records. Néanmoins, les fuites de données ne se produisent pas par magie. Ce sont les utilisateurs qui en sont à l'origine.

Les utilisateurs qui exfiltrent des données peuvent être classés dans trois catégories : utilisateurs négligents, utilisateurs malveillants et utilisateurs compromis. Pour mettre en place des règles appropriées, vous devez d'abord comprendre le contexte du comportement des utilisateurs. Vous pourrez ainsi mieux déterminer les mesures à prendre en cas d'incident d'origine interne.

Proofpoint Endpoint Data Loss Prevention (DLP) et Proofpoint Insider Threat Management (ITM) offrent une approche centrée sur les personnes de la gestion des menaces internes et de la prévention des fuites de données au niveau de l'endpoint.

Ils aident les équipes informatiques et de cybersécurité à accomplir les tâches suivantes :

- Identifier les comportements à risque et les mouvements de données sensibles suspects
- Détecter et prévenir les incidents de sécurité d'origine interne et les fuites de données à partir des endpoints
- Accélérer la réponse aux incidents imputables aux utilisateurs

Proofpoint Endpoint DLP prévient les fuites de données imputables aux utilisateurs quotidiens. Proofpoint ITM inclut la même protection, mais prévient également les menaces liées aux utilisateurs à risque en offrant une visibilité étendue sur les activités des utilisateurs. Les deux solutions font partie de la plate-forme Proofpoint Information Protection and Cloud Security. Cette plate-forme complète, contextualisée et native au cloud offre une visibilité et des informations sur tous les canaux. Elle 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. La plate-forme vous aide à bloquer les fuites de données et à enquêter sur les violations d'origine interne rapidement et efficacement. Plus un incident est résolu rapidement, moins les dégâts seront importants pour votre entreprise, votre marque et vos résultats financiers.

Surveillance des utilisateurs quotidiens et à risque

Flexibilité grâce à un agent d'endpoint unique

Dans l'environnement concurrentiel actuel, vous devez être capable de gérer les menaces internes et les fuites de données au niveau de l'endpoint. Toutefois, la plupart des entreprises n'ont pas besoin de collecter en permanence des données télémétriques sur toutes les activités de tous les utilisateurs. Nous recommandons plutôt une approche plus adaptative et basée sur les risques. Vous bénéficierez ainsi d'informations sur certaines activités pour tous les utilisateurs et sur toutes les activités des utilisateurs présentant le risque le plus élevé.

Pour répondre à ce besoin, Proofpoint a développé un agent d'endpoint léger qui prévient les fuites de données et offre une visibilité étendue sur les activités des utilisateurs. Grâce à un simple changement de configuration des règles, vous pouvez ajuster la quantité et les types de données que vous collectez pour chaque utilisateur ou groupe d'utilisateurs. Cette approche adaptative vous aide à analyser les alertes et à y répondre plus efficacement, sans nécessiter la collecte d'une quantité astronomique de données.

Les utilisateurs quotidiens sont généralement des utilisateurs professionnels lambda. Étant donné le faible risque qu'ils présentent, vous pouvez les surveiller avec Proofpoint Endpoint DLP pour obtenir des informations sur les mouvements de données et du contexte sur les activités des utilisateurs. Vous pouvez par exemple définir des règles afin de générer des alertes lorsqu'un utilisateur tente d'exfiltrer des données sensibles en les copiant sur une clé USB ou en les chargeant dans un dossier de synchronisation cloud.

Les utilisateurs à risque doivent faire l'objet d'une attention accrue. Il peut s'agir de collaborateurs qui quittent ou rejoignent l'entreprise, de prestataires tiers, de titulaires de comptes à privilèges et d'utilisateurs ciblés, comme des cadres dirigeants. Vous avez besoin d'informations détaillées pour comprendre leurs motivations et intentions. Leur surveillance doit tenir compte de leur comportement ou des circonstances. Proofpoint ITM collecte des données approfondies sur les activités de ces utilisateurs. Ces données peuvent fournir des informations contextuelles sur leurs intentions avant, pendant et après un incident.

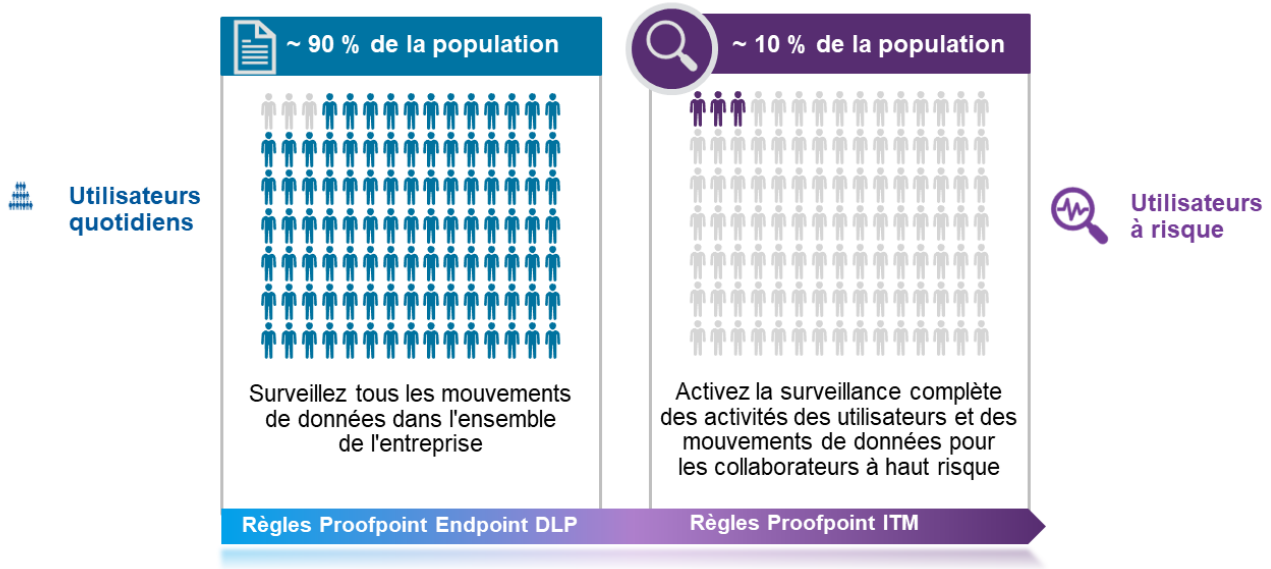

Figure 1. Agent d'endpoint léger offrant la flexibilité nécessaire pour surveiller les utilisateurs quotidiens et à risque

Les informations détaillées fournies par Proofpoint ITM permettent de comprendre tous les tenants et aboutissants (« qui, quoi, où et quand ») des activités à risque. Grâce à ces informations contextuelles, vous pouvez mieux cerner les intentions des utilisateurs en cas de fuite de données ou de violation des règles.

Listes de surveillance d'utilisateurs

Les listes de surveillance intelligentes vous aident à organiser et à hiérarchiser les utilisateurs selon leur tolérance aux risques en fonction de leur profil. Ces listes de surveillance peuvent être fondées sur des critères tels que le degré de sensibilité du rôle de l'utilisateur et les données auxquelles il accède. Elles peuvent également être basées sur la vulnérabilité de l'utilisateur au phishing et à d'autres menaces d'ingénierie sociale. Les critères peuvent également tenir compte de l'emplacement de l'utilisateur, de l'évolution de son poste et d'autres facteurs RH et juridiques.

Visibilité et contexte sur les activités des utilisateurs et les mouvements de données

Visibilité sur les utilisateurs quotidiens et à risque

Proofpoint Endpoint DLP et Proofpoint ITM offrent tous deux une visibilité sur les interactions des utilisateurs avec les données. En revanche, ils ne recueillent pas les mêmes types ni la même quantité de données.

Proofpoint Endpoint DLP collecte des données télémétriques sur les interactions des utilisateurs avec les données sur l'endpoint. Il consigne des actions telles que la manipulation des types de fichiers (le changement de l'extension d'un fichier, par exemple) ou la modification du nom de fichiers contenant des données sensibles. Il enregistre également les tentatives de déplacement de données sensibles, par exemple lorsque les utilisateurs les chargent sur un site Web non autorisé ou les copient dans un dossier de synchronisation cloud.

Proofpoint ITM offre une vue plus complète des activités des endpoints afin que vous puissiez surveiller les utilisateurs à risque. Il répertorie les interactions avec les données capturées par Proofpoint Endpoint DLP, offre une visibilité sur l'utilisation des applications et fournit des captures d'écran des activités au niveau de l'endpoint et des autres comportements à risque. De tels comportements peuvent inclure l'installation et l'exécution d'outils non autorisés ou la réalisation d'activités d'administration de la sécurité. Les informations détaillées fournies par Proofpoint ITM permettent de comprendre tous les tenants et aboutissants (« qui, quoi, où et quand ») des activités à risque. Grâce à ces informations contextuelles, vous pouvez mieux cerner les intentions des utilisateurs en cas de fuite de données ou de violation des règles.

L'approche centrée sur les personnes de Proofpoint offre une visibilité sur les interactions de vos utilisateurs avec les données sensibles plus complète que celle fournie par les outils DLP pour endpoints traditionnels. En effet, ces derniers ne fournissent aucune visibilité sur les mouvements de données, sauf si une action déclenche une alerte. Ils n'établissent pas non plus de lien entre les utilisateurs et les actions. En raison de ces lacunes, vous pourriez passer à côté de mouvements de données en apparence inoffensifs qui, en contexte, sont révélateurs de comportements à risque.

Analyse du contenu et classification des données

Vous pouvez identifier les données sensibles en mouvement, lorsqu'elles sont les plus vulnérables, grâce à l'analyse du contenu en mouvement et à la lecture des étiquettes de classification des données, comme celles de Microsoft Information Protection.

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. 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 de détecteurs de contenu éprouvés et de pointe issus de Proofpoint Cloud App Security Broker (CASB) et Proofpoint Email DLP. En outre, Proofpoint Intelligent Classification and Protection (anciennement Dathena) vous permet d'identifier et de classifier automatiquement les données en temps réel grâce à l'intelligence artificielle.

Vous pouvez configurer des règles d'analyse du contenu pour détecter et prévenir les comportements à risque. Une alerte est générée dès lors qu'un comportement enfreint les règles, de sorte que vous disposez d'informations exploitables en temps réel. Les activités des utilisateurs à risque déclenchent l'analyse du contenu. Ces activités peuvent inclure le chargement ou le téléchargement Web, la copie sur une clé USB, la synchronisation de partages cloud et l'ouverture de documents.

Détection en temps réel des comportements à risque et des mouvements de données suspects

Moteur de règles flexible

Vous pouvez créer des règles et des déclencheurs adaptés à votre environnement à partir de zéro, ou ajuster nos scénarios de menaces prédéfinis. Vous pouvez modifier les 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. Pour assurer la cohérence et vous faire gagner du temps, les règles définies pour Proofpoint ITM peuvent être appliquées à d'autres canaux, comme la messagerie, le cloud et le Web, via l'outil de gestion des règles unifié de la plate-forme.

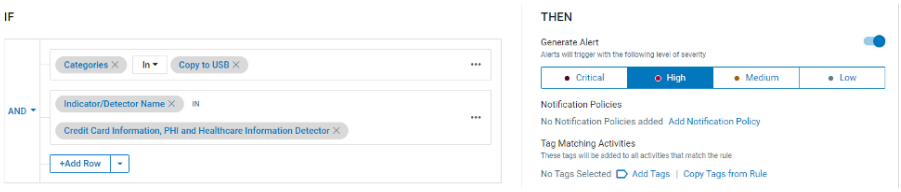

Figure 2. Configuration d'alertes à l'aide d'instructions simples de type si-alors

Bibliothèque d'alertes

Proofpoint Endpoint DLP et Proofpoint ITM intègrent des bibliothèques d'alertes prêtes à l'emploi, qui facilitent la configuration et réduisent le délai de rentabilisation. Proofpoint Endpoint DLP et Proofpoint ITM peuvent tous deux vous alerter en cas d'interactions et de mouvements de données suspects au niveau de l'endpoint. Proofpoint ITM peut en outre détecter un éventail plus large de menaces internes.

Bibliothèque d'alertes Proofpoint Endpoint DLP et Proofpoint ITM

MOUVEMENTS DE DONNÉES

Plus de 40 alertes concernant les interactions avec les données et leur exfiltration, 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
- Activités exécutées sur des fichiers (changement de nom, 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

ACTIVITÉS DES UTILISATEURS (PROOFPOINT ITM UNIQUEMENT)

Plus de 100 alertes concernant un large éventail d'activités réalisées par les utilisateurs au niveau de l'endpoint, notamment :

- Masquage 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
- Tâche d'administration non autorisée
- 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

Bien souvent, les utilisateurs ignorent que leur comportement est dangereux. Mais vous pouvez activer les notifications pour les former.

Prévention de l'exfiltration non autorisée de données à partir de l'endpoint

La détection des utilisateurs à risque et des mouvements de données suspects ne suffit pas toujours. Vous devez également bloquer activement les fuites de données en temps réel. Notre plate-forme vous permet de prévenir les interactions contraires aux règles des utilisateurs avec des données sensibles.

Par exemple :

- Transfert vers et depuis des clés USB
- Synchronisation de fichiers avec des dossiers cloud
- Chargement sur des sites Web non autorisés
- Impression de fichiers

Personnalisez 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. Vous pouvez étendre les fonctionnalités DLP à la messagerie, au cloud et aux applications Web avec les autres composants de la plate-forme Proofpoint Information Protection and Cloud Security.

Formation des utilisateurs aux comportements à risque

Bien souvent, les utilisateurs n'ont pas conscience que leur comportement est dangereux. Vous pouvez activer les notifications pour les former. Par exemple, lorsque des utilisateurs tentent de déplacer des fichiers sensibles, ils recevront une notification indiquant que cette action enfreint les règles de l'entreprise. Ils devront ensuite fournir une justification. Un lien vers les règles de l'entreprise peut être ajouté à la notification. L'envoi de notifications aux collaborateurs concernant leur comportement permet de préserver leur productivité tout en renforçant les contrôles de sécurité. Les notifications peuvent être personnalisées en fonction du niveau de risque, de la fonction ou de l'emplacement d'un utilisateur.

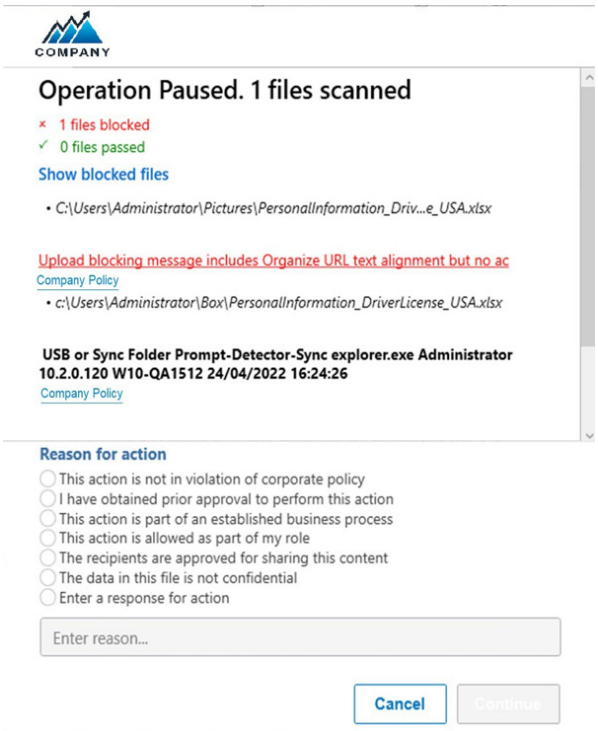

Figure 3. Envoi d'une notification aux utilisateurs finaux présentant un comportement à risque et demande de justification

Accélération de la réponse aux incidents et des investigations

Console unifiée

Proofpoint Endpoint DLP et Proofpoint ITM tirent parti de la plate-forme Proofpoint Information Protection and Cloud Security. Cela vous permet d'optimiser la réponse aux incidents d'origine interne et les investigations. La plate-forme collecte des données télémétriques à partir des endpoints, de la messagerie et du cloud pour offrir une visibilité multicanale de manière centralisée. Sa console unifiée propose des visualisations intuitives 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.

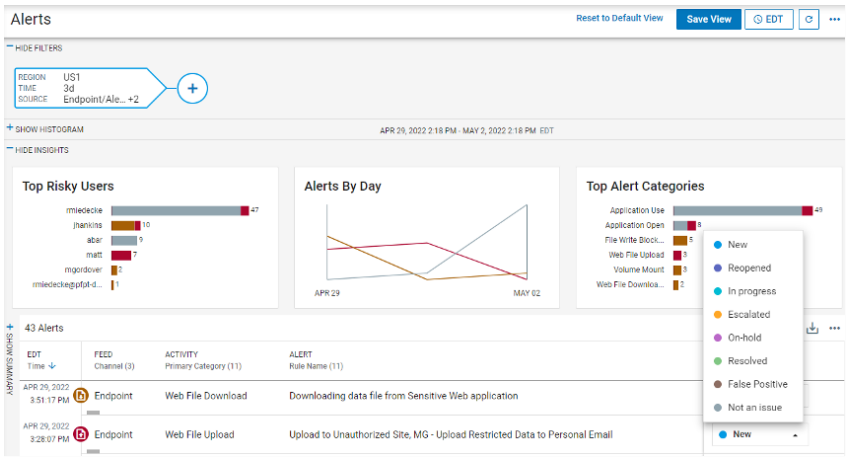

Figure 4. Affichage de l'ensemble des incidents et alertes au sein d'une console unifiée

Traque des menaces par pointer-cliquer

Nos puissantes fonctionnalités de recherche et de filtrage 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. 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.

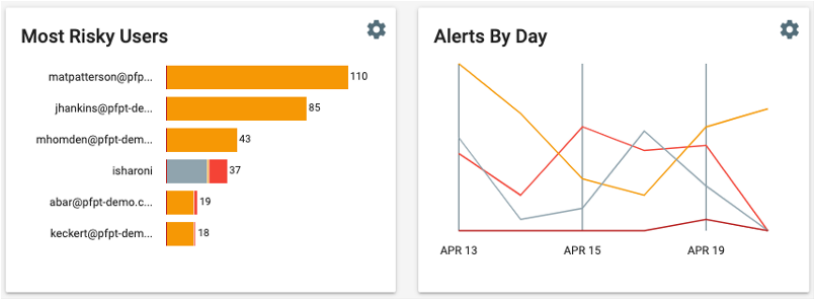

Figure 5. Traque des comportements potentiellement dangereux ou inhabituels

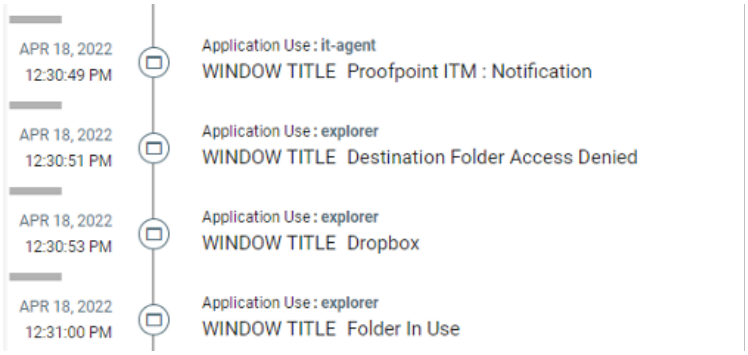

Figure 6. Vue chronologique fournissant un historique des interactions de l'utilisateur avec les données

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 des départements non techniques comme les RH, la conformité, le service juridique et les chefs de service.

Avec Proofpoint Endpoint DLP et Proofpoint ITM, vous pouvez analyser chaque alerte de façon approfondie. Ces solutions vous permettent de voir les métadonnées et d'obtenir des informations contextualisées grâce à des vues chronologiques. Les équipes de sécurité peuvent identifier rapidement les événements qui doivent faire l'objet d'investigations plus poussées et ceux qu'elles peuvent clôturer immédiatement. Des balises peuvent être utilisées pour regrouper et classifier les alertes afin de favoriser la coordination.

Le workflow de base 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. Grâce à Proofpoint ITM, ces exportations au format PDF à partir de la plate-forme incluent des captures d'écran et des informations contextuelles. Cela peut aider les équipes non techniques, comme les RH et le service juridique, à interpréter les données à des fins d'investigation numérique.

Captures d'écran pour les utilisateurs à risque

Une image vaut parfois mille mots. Proofpoint ITM permet d'effectuer des captures d'écran des activités des utilisateurs. Les RH, le service 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.

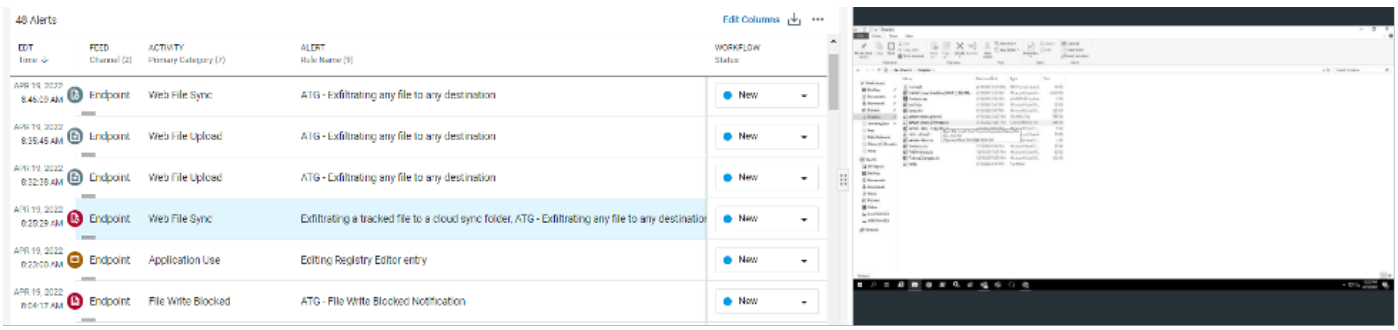

Figure 7. Vue chronologique des activités de l'utilisateur avec capture d'écran de l'endpoint

Intégration aisée au sein d'environnements de sécurité complexes

La plate-forme Proofpoint Information Protection and Cloud Security est pilotée par des microservices. Les webhooks intégrés à notre plate-forme permettent à vos outils SIEM et SOAR d'absorber les alertes Proofpoint Endpoint DLP et Proofpoint ITM, ce qui vous permet d'identifier et de trier rapidement les incidents.

Il est possible que les entreprises disposant d'une infrastructure de sécurité complexe doivent conserver une seule source de vérité pour l'ensemble des systèmes. Nous facilitons ce processus grâce à des exportations automatiques des données Proofpoint Endpoint DLP et Proofpoint ITM vers les espaces de stockage AWS S3 qui vous appartiennent et que vous exploitez.

Réponse aux besoins en matière de confidentialité et de conformité

Gestion de l'emplacement et du stockage des données

Nous prenons en charge les centres de données multirégions pour la plate-forme Proofpoint Information Protection and Cloud Security, 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, en Europe, en Australie et au Japon.

Vous pouvez contrôler le stockage des données des endpoints grâce à un groupement 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. Par exemple, les données des endpoints aux États-Unis peuvent être gérées par un groupement aux États-Unis, qui est envoyé au centre de données des États-Unis.

Confidentialité garantie grâce aux 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 Endpoint DLP et Proofpoint ITM, vous pouvez facilement gérer l'accès afin de vous assurer que les analystes en sécurité ne voient 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 en Europe ne puisse voir que les données européennes, et non les données des États-Unis ou de la région Asie-Pacifique. Vous bénéficiez de la flexibilité nécessaire pour 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.

Visibilité et contexte multicanaux

Proofpoint Endpoint DLP et Proofpoint ITM tirent parti de la puissance de la plate-forme Proofpoint Information Protection and Cloud Security. Ces solutions adoptent une approche centrée sur les personnes du contenu, des comportements et des menaces pour bloquer les fuites de données et enquêter sur les menaces. Grâce à une console unifiée, vous pouvez bénéficier d'une visibilité et d'informations contextualisées sur plusieurs canaux, dont les endpoints, le cloud, la messagerie et le Web.

Vous pouvez définir des règles, traquer les menaces ainsi qu'analyser les alertes et y répondre, quel que soit le canal, à partir d'une même interface. Vous n'avez pas besoin de basculer d'un outil à un autre pour réaliser chaque tâche. Vous pouvez également analyser les métadonnées des alertes de manière approfondie. Cela vous aidera à comprendre ce qui s'est passé avant, pendant et après un incident. La solution native au cloud peut également être déployée rapidement, afin de réduire le délai de rentabilisation.

Travaillez plus efficacement, gagnez un temps précieux et réduisez les perturbations des activités dues aux fuites de données et aux menaces internes grâce à la visibilité et au contexte fournis par la plate-forme Proofpoint Information Protection and Cloud Security.

EN SAVOIR PLUS

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

À PROPOS DE 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 risques 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 75 % des entreprises de l'index 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 les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.