proofpoint.

Guide d'achat de solutions de prévention des fuites de données

Ce guide d'achat met en évidence les fonctionnalités les plus importantes d'une solution moderne de protection des informations. Il fait la synthèse des connaissances acquises par Proofpoint au cours de l'élaboration de programmes efficaces de prévention des fuites de données (DLP) pour des entreprises de toutes tailles à travers le monde et dans tous les secteurs. Ce guide pratique vous aidera, que vous ayez décidé de vous lancer dans l'aventure de la prévention des fuites de données ou que vous souhaitiez moderniser vos systèmes DLP existants.

Sécurité centrée sur les personnes

Pour protéger les données contre les menaces uniques et courantes, vous avez besoin d'une plate-forme qui prend en charge un modèle de sécurité centré sur les personnes, à savoir une plate-forme offrant une visibilité complète sur les interactions des utilisateurs avec les données sensibles et le suivi des comportements à risque. Vous bénéficiez ainsi d'informations contextuelles importantes sur leur intention au moment de la perte ou du vol des données, ou de leur comportement apparemment suspect.

Grâce à une solution centrée sur les personnes, vous pouvez rapidement évaluer les risques de fuites de données via la messagerie, les endpoints et les applications cloud telles que Microsoft 365, Google Workspace et Salesforce. Ces renseignements vous permettent d'intervenir rapidement et de prendre les mesures nécessaires pour prévenir toute fuite de données.

Éléments incontournables d'une solution DLP moderne

Si vous souhaitez gérer les fuites de données et bloquer les menaces internes, vous devez être en mesure de détecter, d'analyser, de prévenir et de neutraliser les incidents. Pour limiter vos risques, toutes ces opérations doivent être coordonnées.

Surveillance

Pour protéger les données, vous ne pouvez pas vous concentrer uniquement sur le contenu. Vous avez besoin d'une visibilité sur les interactions des utilisateurs avec les données. Lorsque vous surveillez les activités de données de tous les utilisateurs via les endpoints, la messagerie, le cloud et le Web, vous obtenez un aperçu global et des informations contextualisées.

85 %

des entreprises ont été victimes d'au moins une fuite de données en 2023

50 %

des adultes actifs ayant changé d'emploi au cours des deux dernières années ont admis avoir emporté des données avec eux

Détection

Vous avez besoin d'une solution capable de détecter, en temps réel ou quasi réel, les actions dangereuses d'un utilisateur ou l'exposition potentielle de données, même si celles-ci ne se transforment pas en véritable incident. Les fonctionnalités de détection doivent trouver le meilleur compromis entre alertes opportunes et exploitables et risque de baisse de vigilance engendrée par la multiplication des alertes.

Analyse

Il s'agit de la capacité à analyser les tendances des comportements des utilisateurs et à traquer les menaces, ce qui n'est possible que si la solution DLP combine les activités des utilisateurs sur divers canaux. Vous pourrez ainsi détecter tout comportement à risque d'un utilisateur. Même si ce processus peut être automatisé, il est essentiel de faire appel à des analystes à même d'inspecter les données de manière approfondie.

Intervention

Il est important d'enquêter et d'intervenir rapidement et efficacement en cas d'incident. Plus il faut de temps pour neutraliser une menace interne, plus elle peut faire de dégâts sur le plan des résultats financiers et de la réputation. Une solution DLP moderne peut automatiquement appliquer des règles et neutraliser des menaces. L'automatisation protège vos données les plus précieuses et accroît l'efficacité de votre équipe de sécurité.

Prévention

Il s'agit de la capacité à empêcher un utilisateur d'enfreindre volontairement ou non les règles de sécurité de votre entreprise. Pour ce faire, vous devez former les utilisateurs, envoyer des rappels en temps réel et bloquer les activités de certains utilisateurs si nécessaire.

3 principaux scénarios de fuite de données

Voici trois scénarios courants de fuite de données. Tous sont imputables à une intervention humaine. Une plate-forme de protection des informations centrée sur les personnes doit pouvoir identifier :

- Les utilisateurs qui font preuve de négligence à l'égard des données sensibles
- Les utilisateurs négligents qui exposent des données sensibles en utilisant des applications d'IA générative
- Les utilisateurs internes malveillants qui cherchent à nuire à l'entreprise

1 : utilisateurs négligents et erreurs courantes

Selon le rapport Data Loss Landscape 2024 de Proofpoint, les utilisateurs négligents sont la principale cause de fuites de données. Ces utilisateurs n'ont pas l'intention de provoquer une fuite de données. Ils souhaitent simplement faire leur travail le plus efficacement possible. En revanche, leurs erreurs peuvent avoir de graves conséquences : perturbation des activités, atteinte à la réputation, position concurrentielle fragilisée, infractions et amendes réglementaires, actions en justice, etc.

3,5 Mds $ Dépenses totales estimées pour la prévention des fuites de données dans le monde d'ici 2025[1]

77 JOURS sont nécessaires pour éliminer les menaces internes[2]

85 % des entreprises sont ciblées par des attaques dans le cloud[3]

56 % des incidents sont dus à la négligence des utilisateurs[4]

Voici quelques exemples d'actions à risque de ces utilisateurs :

- Envoi d'emails au mauvais destinataire, avec ou sans pièce jointe
- Consultation de sites de phishing
- Installation de logiciels non autorisés
- Partage public de fichiers et données sensibles
- Envoi par email de données personnelles à un compte de messagerie personnel
- Enregistrement de données sensibles de l'entreprise sur des terminaux personnels

Protection contre la négligence

Un système de protection des informations efficace centré sur les personnes bloque les activités à risque. Il offre également aux utilisateurs négligents un accompagnement qui leur permet d'identifier et de modifier leurs comportements à risque.

Éléments indispensables :

- **Classification.** Vérifiez que la messagerie, les données et les contenus font l'objet d'une surveillance continue à la fois manuelle et par l'intelligence artificielle (IA) pour identifier et classer les utilisateurs à risque. Lorsqu'un utilisateur est considéré à haut risque, le système lui attribue un score de risque pour protéger les données en conséquence.
- **Détection.** Le système doit surveiller la messagerie, les documents et les données en évaluant en permanence les risques de non-conformité. Étant donné que les contenus sont en mouvement sur plusieurs canaux (endpoints, messagerie, cloud et Web), ils doivent être analysés de manière à vérifier que ce mouvement ou partage n'enfreint pas les règles de votre entreprise. Dès lors qu'une infraction est détectée dans la messagerie, le système doit permettre aux équipes de sécurité de bloquer l'email ou de le suivre en vue d'une investigation ultérieure.
- **Prévention.** Il convient d'empêcher les utilisateurs d'exfiltrer des données sensibles sur tous les canaux et terminaux : emails envoyés au mauvais destinataire avec ou sans pièce jointe, clés USB, chargements Web, synchronisation cloud, impression, etc. S'ils commettent une erreur, ils doivent recevoir instantanément un message d'avertissement contextuel leur permettant de la corriger et de prévenir la fuite de données en temps réel sans intervention de l'administrateur. Si nécessaire, les utilisateurs peuvent fournir une justification d'accès aux données. L'équipe de sécurité peut alors autoriser ou refuser cette demande.

1 The Radicati Group, « Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2025 » (Prévisions du chiffre d'affaires du marché de la prévention des fuites de données à l'échelle mondiale de 2019 à 2025), mai 2022.
2 Ponemon Institute, « 2022 Cost of Insider Threats Global Report » (Rapport 2022 sur le coût des menaces internes à l'échelle mondiale), février 2022.
3 Assaf Friedman et Itir Clarke (Proofpoint), « How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps » (Utilisation de comptes compromis par les cybercriminels pour créer et distribuer des applications OAuth), mai 2021.
4 Ponemon Institute, « 2022 Cost of Insider Threats Global Report » (Rapport 2022 sur le coût des menaces internes à l'échelle mondiale), février 2022.

2 : utilisateurs négligents et applications d'IA générative

En dépit du gain de productivité que procurent aux utilisateurs les outils d'IA générative tels que ChatGPT, ils sont souvent à l'origine de fuites de données. Pour éviter les fuites de données sans nuire à la productivité, vous devez mettre en place des mesures robustes de protection des données. Le problème, c'est que vous ne pouvez pas appliquer de règles d'utilisation acceptable pour l'IA générative si vous ne comprenez pas vos contenus et la manière dont vos collaborateurs interagissent avec eux.

Protection contre l'utilisation négligente de l'IA générative

Des mesures robustes de protection des données sont indispensables pour éviter les fuites de données sensibles par le biais d'outils d'IA générative. Vous ne pouvez pas bloquer complètement l'accès aux outils d'IA générative. Il est important de permettre aux utilisateurs d'accéder à ces outils pour accroître leur productivité et stimuler l'innovation.

Pour que vos collaborateurs puissent utiliser des outils d'IA générative sans mettre vos données en danger, vous devez adopter une approche de la prévention des fuites de données centrée sur les personnes. Une solution basée sur cette approche autorise et empêche de façon très précise les collaborateurs d'utiliser des outils d'IA générative selon leur comportement et contributions, même si les données ont été manipulées et sont passées par plusieurs canaux.

Éléments indispensables :

- **Identification des contenus sensibles.** Un système qui sait identifier les contenus à protéger, peut bloquer plus efficacement les fuites de données. Adoptez des méthodes avancées d'identification et de classification des contenus, comme la reconnaissance optique des caractères, la correspondance exacte des données et la correspondance de documents indexés.
- **Surveillance des utilisateurs.** Vous devez savoir qui utilise des outils d'IA générative dans votre environnement et les méthodes employées. Le système doit être en mesure de détecter, de bloquer et de signaler différents types d'actions des utilisateurs, notamment le chargement de fichiers de code source et le collage de propriété intellectuelle de l'entreprise.
- **Gestion proactive des risques.** Grâce à la création et à l'enregistrement d'explorations personnalisées, vos équipes peuvent traquer régulièrement les exfiltrations de données et autres activités à risque associées aux outils d'IA générative.

3 : utilisateurs malveillants

Les utilisateurs malveillants sont dangereux car ils sont les mieux placés pour voler des données sensibles. Les collaborateurs quittant l'entreprise constituent le type d'utilisateurs internes le plus à risque. Sur une période de neuf mois en 2023, 87 % des exfiltrations de fichiers suspectes via des locataires cloud utilisant la plate-forme Proofpoint Information Protection ont été causées par des collaborateurs quittant l'entreprise. Ces utilisateurs estiment souvent avoir le droit de conserver des informations compte tenu du temps qu'ils ont consacré à leurs projets.

Si les utilisateurs internes malveillants sont si dangereux, c'est qu'ils peuvent attendre leur heure et exploiter leur accès à privilèges pour mettre la main sur des données précieuses et exploiter des failles de sécurité. En outre, les entreprises aggravent leur cas en permettant à leurs collaborateurs de consulter et de stocker des données sur leurs terminaux personnels, ce qui facilite le vol de données sensibles.

Un système centré sur les personnes surveille certains utilisateurs de plus près que d'autres et applique des contrôles d'accès plus stricts aux utilisateurs les plus à risque.

Protection contre les utilisateurs malveillants

Un système centré sur les personnes surveille certains utilisateurs de plus près que d'autres, applique des contrôles d'accès plus stricts aux utilisateurs les plus à risque et bloque de façon proactive les activités malveillantes en se basant sur des facteurs de risque tels qu'une démission ou un licenciement.

Éléments indispensables :

- **Visibilité.** La visibilité sur les endpoints, la messagerie, le cloud et le Web offre un aperçu global et des informations contextualisées sur l'activité d'un utilisateur. Des données télémétriques sur les interactions des utilisateurs avec les données et les systèmes doivent être collectées, par exemple en cas de changement de nom d'un fichier sensible ou de son chargement sur un site Web non autorisé ou dans un dossier de synchronisation cloud. Si un utilisateur installe ou exécute des applications non autorisées, ces activités doivent également être surveillées. L'équipe de sécurité doit être en mesure d'identifier en temps réel la personne à l'origine du déclenchement d'une alerte.
- **Investigations.** Vous avez besoin d'une bibliothèque d'alertes complète pour les scénarios les plus courants (fraude au temps de travail, exfiltration de données, contournement des contrôles de sécurité). Cela vous permettra d'être rapidement opérationnel. L'équipe de sécurité doit recevoir des alertes avec des métadonnées détaillées et des captures d'écran des activités des utilisateurs. Une vue chronologique contextualisée des événements aide les équipes chargées des investigations à comprendre les tenants et aboutissants (« qui, quoi, quand, où ») des activités des utilisateurs.
- **Architecture moderne.** Une plate-forme native au cloud peut prendre en charge des centaines de milliers d'utilisateurs. Si elle est dotée de fonctionnalités telles que des contrôles d'accès basés sur des attributs, le masquage et l'anonymisation des données, ainsi que la prise en charge des centres de données multirégions, elle vous permettra de répondre aux exigences en matière d'emplacement et de confidentialité des données. De même, un système moderne complètera votre système de sécurité du fait de sa facilité d'intégration à divers outils, notamment :
  - Orchestration, automatisation et réponse aux incidents de sécurité (SOAR)
  - Gestion des événements et des incidents de sécurité (SIEM)
  - Réponse aux incidents
  - Gestion des tickets

Fonctionnalités requises

Maintenant que vous connaissez la protection apportée par des systèmes DLP modernes centrés sur les personnes, examinons plus en détail les fonctionnalités indispensables. On distingue trois catégories :

- Détection et prévention des risques de fuites de données
- Analyse et réponse aux incidents
- Déploiement et mise en œuvre

Détection et prévention des risques de fuites de données

Lorsque les équipes de sécurité disposent de renseignements sur le comportement des utilisateurs et les contenus sensibles, elles peuvent gérer les risques liés aux données de façon appropriée et ciblée.

BESOINS DES CLIENTS	FONCTIONNALITÉS REQUISES
Détection des contenus sensibles	Détection et analyse des données sensibles dans la messagerie, sur les endpoints, dans le cloud et sur le Web
	Fonctionnalité intégrée de classification des données sensibles en fonction du contexte métier
	Classification des données optimisée par l'IA grâce à de grands modèles de langage (LLM)
	Méthodes avancées d'identification : • Reconnaissance optique des caractères (OCR) • Correspondance exacte des données (EDM) • Correspondance de documents indexés (IDM)
	Règles prédéfinies pour détecter les données sensibles, notamment : • Code PII • Norme PCI, loi SOX, loi GLBA, termes relevant du délit d'initié définis par la SEC • Code PHI, loi HIPAA, CIM-9, CIM-11, Code national américain des médicaments • RGPD, UK-DPA, EU-DEPD, PIPEDA
	Capacité à définir des règles de lecture et d'application des étiquettes de confidentialité de Microsoft Information Protection (MIP) pour identifier les données métier critiques

BESOINS DES CLIENTS	FONCTIONNALITÉS REQUISES
Surveillance du comportement des utilisateurs	Approche centrée sur les personnes permettant aux analystes d'intervenir rapidement grâce aux informations suivantes : • Intention des utilisateurs • Modèles d'accès aux données • Modèles d'accès aux applications
	Capacité à surveiller les interactions des utilisateurs avec les données au niveau des endpoints managés et non managés, ainsi que le cloud : • Changement de noms de fichiers • Modification de l'extension de fichiers • Chargement et téléchargement Web • Copie sur une clé USB • Synchronisation de partages cloud • Ouverture de documents • Activité suspecte sur des fichiers
	Surveillance de l'utilisation de sites Web et d'applications : • Chargement, collage ou saisie de contenu sur des sites d'IA générative • Téléchargement et installation d'outils de piratage ou de sauvegarde de données
	Surveillance des comportements des utilisateurs internes les plus à risque pour déterminer leur intention et limiter les risques, comme la manipulation du registre Windows pour éliminer des contrôles
	Surveillance proactive des utilisateurs à risque par de simples captures d'écran en cas de déclenchement d'une alerte afin de garantir la confidentialité
	Accompagnement des utilisateurs et demande de justification en cas d'accès à des données sensibles au lieu d'un blocage pouvant impacter leur productivité (messagerie, endpoints, cloud, Web)
Prévention des fuites de données	Formation de sensibilisation à la sécurité informatique permettant de changer les comportements des utilisateurs en leur expliquant comment éviter les risques de cybersécurité et protéger les données sensibles
	Prévention de l'exfiltration de données sensibles depuis des endpoints managés, notamment : • Copie de fichiers sur une clé USB non autorisée • Chargement de fichiers vers un dossier cloud personnel • Impression de documents sensibles • Collage de contenus sensibles depuis le Presse-papiers • Partages réseau
	Contrôle du partage étendu de fichiers dans des applications cloud et limitation automatique des autorisations de partage de fichiers
	Sécurisation de l'accès à des fichiers sensibles dans des applications cloud approuvées par l'équipe informatique depuis des terminaux non managés
	Détection et prévention automatiques de l'envoi d'emails au mauvais destinataire, avec ou sans pièce jointe
	Détection et prévention automatiques de l'envoi d'emails au bon destinataire, mais avec une pièce jointe erronée
	Prévention du partage de données sensibles pas encore prédéfinies à des comptes de messagerie personnels et d'autres comptes non autorisés

Analyse et réponse aux incidents

Les équipes de sécurité doivent être en mesure de résoudre rapidement les incidents sur tous les canaux. L'objectif est de limiter l'exposition des données et de garantir ainsi la confidentialité.

BESOINS DES CLIENTS	FONCTIONNALITÉS REQUISES
Résolution des incidents couvrant tous les canaux	Console unifiée couvrant tous les canaux (messagerie, endpoints et cloud) et effectuant les opérations suivantes : • Tri des alertes • Investigations • Explorations personnalisées • Intervention
	Analyses couvrant tous les canaux et indiquant : • Les activités des utilisateurs au fil du temps • Les activités liées aux fichiers au fil du temps (création, modification, partage)
	Fonctionnalités d'exploration proactive qui offrent une visibilité en temps réel sur le comportement des utilisateurs à risque
	Intégration avec la plate-forme SIEM de votre entreprise permettant le tri des workflows avec vos outils existants
	Capacité à détecter et à neutraliser automatiquement les risques de fuites de données liés à des utilisateurs compromis par les moyens suivants : • Fermeture de sessions • Réinitialisation de mots de passe • Correction des risques • Identification de l'impact
Confidentialité	Flexibilité des contrôles d'accès vous assurant que les analystes ne voient les données que si cela est absolument nécessaire
	Anonymisation des informations d'identification des utilisateurs et masquage des contenus sensibles afin de protéger les données et d'éliminer les biais de la part des analystes

Déploiement et mise en œuvre

Une fois que vous aurez choisi la solution DLP la mieux adaptée à votre entreprise, il vous faudra la déployer. Pour que le processus de mise en œuvre soit fluide, vous devez choisir les bons partenaires pour vous accompagner tout au long du déploiement de votre stratégie DLP.

BESOINS DES CLIENTS	FONCTIONNALITÉS REQUISES
Déploiement	Solution native au cloud pouvant être déployée rapidement
	Solution hautement évolutive pouvant facilement être étendue à des centaines de milliers d'utilisateurs par locataire
	Solution facile à gérer nécessitant une maintenance et une alimentation minimales grâce à une communication claire sur les mises à jour et à une assistance du fournisseur en cas de besoin
	Centralisation des règles et de l'administration répondant aux exigences multirégions en matière d'emplacement des données
	Plate-forme flexible qui s'intègre avec votre écosystème de sécurité, notamment les solutions suivantes : • Microsoft • Okta et Sailpoint • CrowdStrike • Splunk et Service Now • Zscaler et Citrix ShareFile
	Agent d'endpoint léger en mode utilisateur qui : • Renforce la visibilité sur les menaces internes potentielles • Améliore la productivité des utilisateurs • Élimine les problèmes de stabilité • N'entre pas en conflit avec d'autres solutions
Mise en œuvre	Services professionnels qui peuvent vous aider à accélérer le déploiement grâce à une équipe d'experts chevronnés qui adapte votre système à vos besoins La mise en œuvre d'une solution DLP s'effectue en plusieurs étapes : • Collecte des exigences • Conception • Personnalisation de la solution • Test et ajustement • Formation des administrateurs et utilisateurs • Documentation
DLP managée	Quelle que soit la taille de l'entreprise, une offre de DLP managée doit être envisagée. Grâce aux services managés, vous bénéficiez de l'aide d'experts chevronnés, disponibles en permanence, qui se chargent de la conception, du déploiement et de la cogestion de votre programme.

EN SAVOIR PLUS

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

1207-013-03-01 7/24

proofpoint.