proofpoint

RAPPORT

État des lieux des fuites de données en 2024

Regard sur les collaborateurs quittant l'entreprise, les cybercriminels déterminés et les emails détournés à travers le monde

proofpoint.com/fr

INTRODUCTION

Bienvenue dans la première édition de notre rapport sur l'état des lieux des fuites de données. Dans ce rapport, nous nous intéresserons à l'état actuel de la prévention des fuites de données (DLP) et des menaces internes dans 12 pays et 17 secteurs d'activité. Il s'agit d'une nouvelle catégorie de rapports pour Proofpoint. Nous pensons qu'elle fait écho à notre principe fondamental, à savoir que les personnes constituent une variable critique de la sécurité des données.

Chaque année, une poignée de vulnérabilités et d'attaques « zero-day » font les gros titres et donnent des maux de tête aux équipes de sécurité. Au-delà de ces problèmes techniques, la plupart des analystes reconnaissent que les fuites de données sont généralement imputables à des utilisateurs plutôt qu'à des vulnérabilités système et à des erreurs de configuration. La cause sous-jacente de ces incidents peut être une simple négligence, le vol d'identifiants de connexion par un cybercriminel ou, dans les cas les plus extrêmes, l'exploitation d'un accès à privilèges par un utilisateur interne malveillant en vue de voler des données précieuses et des éléments de propriété intellectuelle.

Pour ne rien arranger, plusieurs facteurs macroéconomiques affectent les entreprises de toutes tailles. Les workflows cloud ont changé la façon dont les données sont stockées, consultées et synchronisées. Le travail hybride a multiplié le nombre d'environnements qui utilisent des données sensibles. L'IA générative absorbe des tâches courantes et des données confidentielles. Enfin, les cybercriminels ingénieux ne cessent d'innover afin de tirer parti des défauts de vigilance et ont recours à des technologies émergentes pour perfectionner leurs techniques.

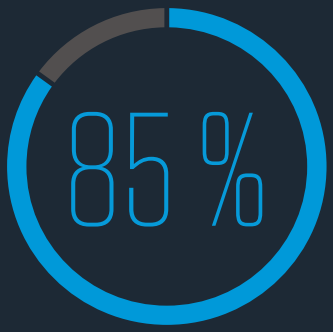
Compte tenu de tous ces problèmes, il est naturel de se demander si les approches DLP actuelles sont à la hauteur des enjeux du moment. Pour répondre à cette question, nous avons interrogé 600 professionnels de la sécurité concernant l'état actuel de la DLP à travers le monde. Nous avons complété ces réponses par des données issues de notre plate-forme Proofpoint Information Protection pour refléter l'ampleur des défis que les entreprises doivent relever pour lutter contre les fuites de données et les menaces internes.

SOMMAIRE

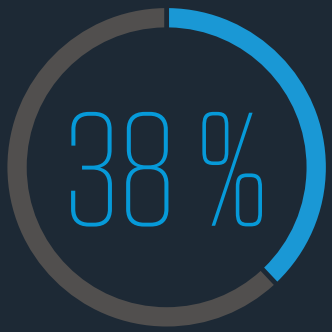
PRINCIPALES OBSERVATIONS

Les « utilisateurs négligents » ont été la cause la plus citée de fuites de données.

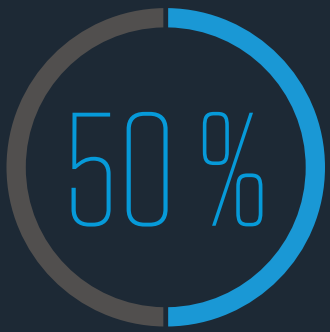
L'IA générative est le sujet de préoccupation qui connaît la croissance la plus rapide.



des entreprises ont été victimes d'au moins une fuite de données au cours de l'année écoulée.

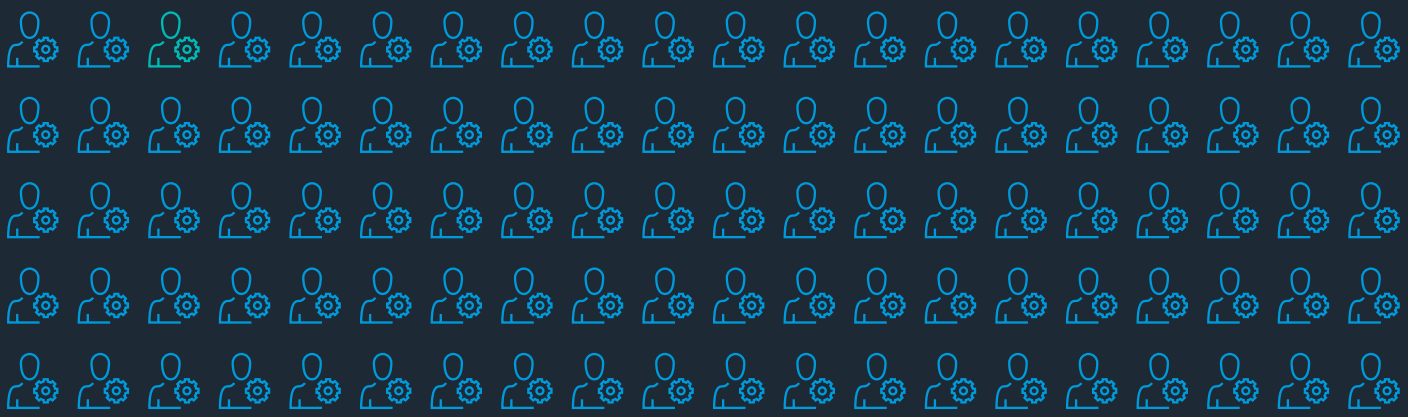


Seulement 38 % des entreprises disposent d'un programme DLP « mature ».



Les fuites de données sont perturbatrices : plus de 50 % des sondés ont fait part de perturbations des activités.

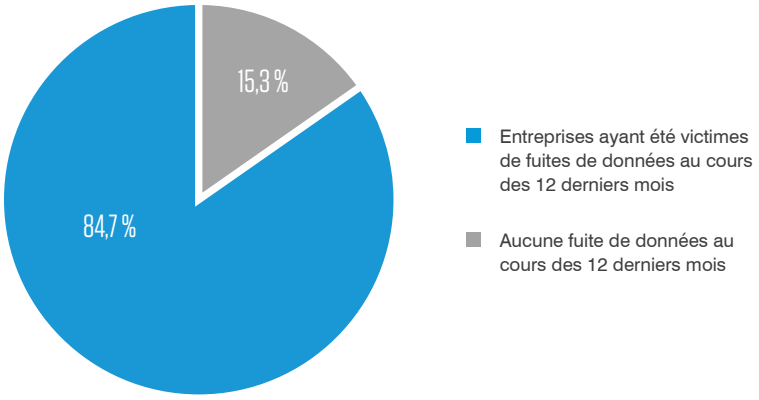
1 % des utilisateurs sont responsables de 88 % des fuites de données.



Les fuites de données sont un problème humain

La grande majorité (85 %) des entreprises interrogées dans le cadre de notre enquête ont été victimes d'au moins une fuite de données au cours de l'année écoulée, ce qui montre l'ampleur qu'a pris le problème. Le nombre moyen d'incidents par entreprise était légèrement supérieur à 15, soit plus d'un incident par mois. Si ces observations ne sont pas surprenantes compte tenu de la transition vers le travail hybride, de l'adoption accélérée du cloud et de l'importante rotation du personnel, elles donnent à réfléchir et illustrent l'ampleur du problème. En effet, 10 % des sondés ont signalé plus de 30 incidents distincts chacun. Les pays anglophones ont enregistré des taux globaux légèrement inférieurs. Même dans le pays affichant le pourcentage le plus faible, à savoir le Royaume-Uni, 73 % des sondés ont signalé au moins un incident au cours des 12 derniers mois.

Entreprises victimes de fuites de données



La prévalence des fuites de données dans tous les pays et secteurs d'activité soulève une question évidente : quelle est la cause de tous ces incidents ? Notre enquête apporte une réponse étonnante : les « utilisateurs négligents » (y compris les collaborateurs généraux, les professionnels de l'informatique et les sous-traitants/fournisseurs) ont été cités par plus de 70 % des sondés. Voici quelques exemples de négligence :

- Emails détournés
- Consultation de sites de phishing
- Installation de logiciels non autorisés
- Partage public de fichiers sensibles
- Envoi par email de données personnelles à un compte de messagerie personnel
- Toute autre exposition involontaire de systèmes ou données par un utilisateur

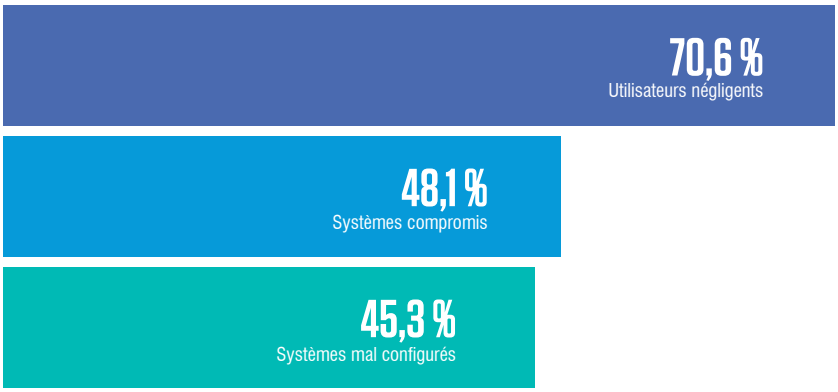
QU'EST-CE QU'UN UTILISATEUR NÉGLIGENT ?

Les fuites de données ne sont pas toujours le fruit d'une activité délibérément malveillante. Des erreurs sont parfois commises. Bien entendu, que la porte ait été enfoncée par un cybercriminel ou laissée ouverte par un collaborateur négligent, les conséquences des fuites de données peuvent être graves.

En février 2023, près de 14 000 collaborateurs du **NHS de Liverpool au Royaume-Uni** ont découvert que leurs données personnelles avaient été partagées avec des centaines de responsables du NHS et 24 personnes en dehors de l'organisation. Dans une lettre d'excuses adressée aux victimes, le PDG du trust a expliqué qu'une feuille de calcul comportant un onglet caché avait été jointe à un email. Bien que cet onglet ne soit pas visible pour les destinataires, les noms, les dates de naissance et même les salaires des collaborateurs étaient exposés. Malgré les mesures prises rapidement par l'organisation pour arranger les choses, des données personnelles avaient été partagées — une violation manifeste du RGPD.

Les causes techniques arrivent ensuite, sous la forme de systèmes compromis (48 %) et mal configurés (45 %), le manque de temps et de ressources ajoutant un facteur humain non négligeable à ces problèmes.

Principales causes des fuites de données



Le message des professionnels est clair : les fuites de données sont un problème causé par l'interaction entre les personnes et les machines. En ce qui concerne les personnes, il est possible de limiter les futurs incidents grâce à l'envoi d'informations contextuelles aux utilisateurs et à des formations ciblées de sensibilisation à la cybersécurité.

20 % des sondés ont affirmé qu'un collaborateur ou un sous-traitant malveillant était à l'origine de l'incident dont ils ont été victimes. Si ce chiffre est nettement inférieur au pourcentage de sondés attribuant les fuites de données à un utilisateur négligent, les conséquences peuvent être bien plus dévastatrices. Les utilisateurs malveillants sont motivés par leur profit personnel et cherchent à porter atteinte aux données, systèmes et réseaux d'une entreprise, par exemple via l'utilisation inappropriée d'applications, le sabotage de systèmes ou des campagnes d'espionnage industriel. Les collaborateurs quittant l'entreprise qui manifestent un comportement malveillant entrent également dans cette catégorie. Les incidents imputables à des utilisateurs internes malveillants peuvent également entraîner des litiges potentiellement coûteux.

Grâce aux données de la plate-forme Proofpoint Information Protection, nous avons examiné de plus près le facteur humain des fuites de données. Il s'avère que seul un très petit nombre d'utilisateurs sont responsables des alertes DLP. En effet, dans la plupart des entreprises, seulement 1 % des utilisateurs sont responsables de 88 % des alertes. Si cela pourrait signifier que le risque est contenu, la réalité n'est pas aussi simple. Dans les entreprises modernes, qui connaissent des recrutements, des départs et des changements de poste réguliers, et où les circonstances évoluent constamment, l'identité de ce 1 % d'utilisateurs change probablement d'un mois à l'autre. Et les 12 % d'alertes restants posent toujours un risque majeur, d'autant plus que les utilisateurs internes peuvent prendre leur temps pour voler des données, en exfiltrant périodiquement des documents importants pour échapper à toute détection. Même s'il est rassurant de constater que la cible est limitée, les équipes de sécurité doivent rester vigilantes pour garder une longueur d'avance sur cette cohorte d'utilisateurs à risque.

1 %

des utilisateurs sont responsables de 88 % des fuites de données. L'identité de ce 1 % d'utilisateurs change probablement d'un mois à l'autre.

Un tiers des utilisateurs

ont envoyé un ou deux emails au mauvais destinataire.

84 %

des emails détournés contenaient des pièces jointes l'année dernière.

Les emails détournés sont l'une des manifestations les plus courantes de la négligence des utilisateurs. La plupart des webmails et des clients de messagerie natifs proposant le remplissage automatique des adresses, il est facile pour les utilisateurs pressés de commettre des erreurs. Selon les données 2023 de Tessian, entreprise rachetée par Proofpoint à l'automne dernier, le problème est généralisé. Environ un tiers des utilisateurs ont envoyé environ deux emails par an au mauvais destinataire. Cela signifie qu'une entreprise de 5 000 collaborateurs peut s'attendre à faire face à près de 3 400 emails détournés chaque année.

Les conséquences de l'envoi d'un email au mauvais destinataire peuvent être dévastatrices. Un email détourné contenant des informations sensibles est l'une des formes les plus simples de fuite de données. Une fois le message envoyé, l'entreprise s'en remet à la bonne volonté des destinataires pour que la compromission ne s'aggrave pas.

Et même si le destinataire coopère (ou prête attention au texte standard en pied de page de l'email), il peut toujours y avoir des répercussions réglementaires. Un email détourné contenant des données de collaborateurs, de clients ou de patients peut donner lieu à une amende substantielle en vertu du RGPD et d'autres cadres légaux. Et bien entendu, même si aucune donnée sensible n'est concernée, le fait d'envoyer un email à la mauvaise personne, de répondre à tous ou d'utiliser la copie carbone au lieu de la copie carbone invisible peut causer de l'embarras et une atteinte à la réputation.

En plus d'envoyer un email au mauvais destinataire, un utilisateur négligent envoie parfois les mauvaises informations à la bonne personne, que ce soit dans le corps de l'email ou sous forme de pièce jointe. Les systèmes de protection de la messagerie de base peuvent avertir les utilisateurs lorsque l'adresse d'un destinataire appartient à un autre domaine. Toutefois, seules des solutions avancées peuvent détecter et avertir les utilisateurs de la présence d'informations sensibles dans des fichiers joints ou le corps d'un email. D'après les données de Tessian, dans 81 % des entreprises, au moins un utilisateur a envoyé la mauvaise pièce jointe dans un email l'année dernière.

Évaluation des conséquences

La forte incidence des fuites de données mise en lumière par notre enquête s'accompagne d'une incidence presque égale de conséquences négatives. Plus de 90 % des entreprises ayant été victimes d'au moins un incident ont signalé des répercussions négatives. Plus de la moitié des sondés ont fait état de perturbations des activités, et près de 40 % ont déclaré que la réputation de leur entreprise avait été entachée. Il convient de noter que ces conséquences ne s'excluent pas mutuellement. Par exemple, une fuite de données peut entraîner une atteinte à la réputation conduisant à la perte de revenus.

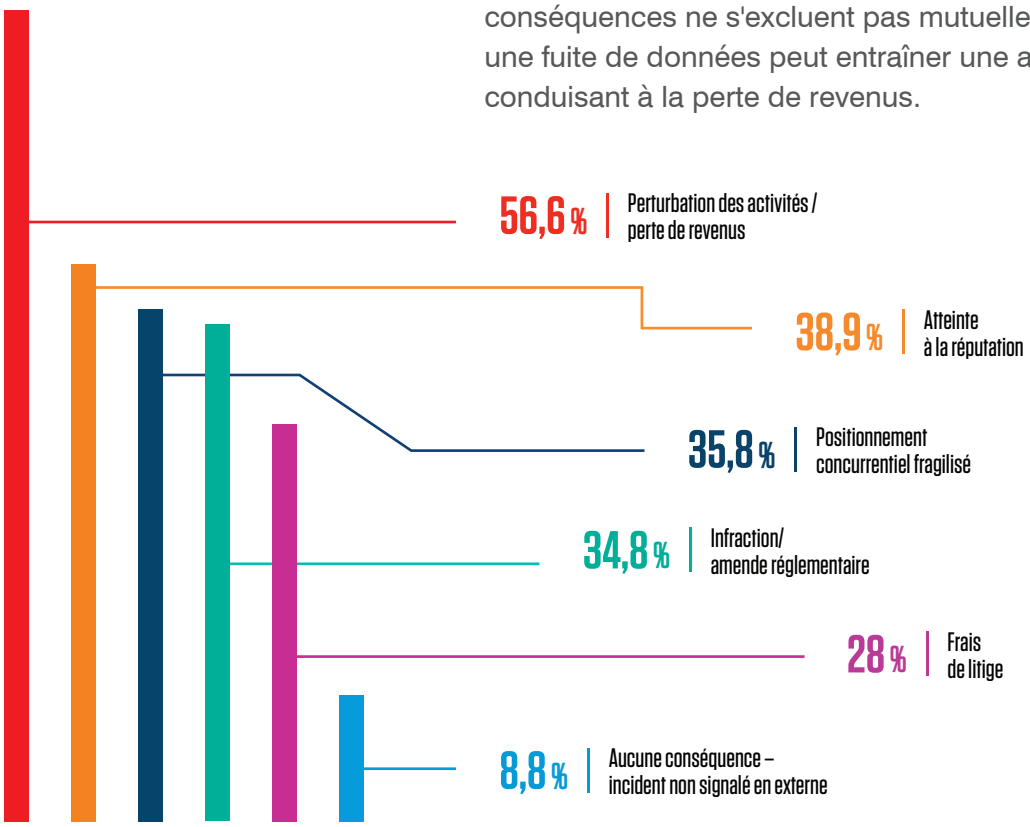


Figure 1. Conséquences des fuites de données

La probabilité de conséquences négatives était également répartie équitablement entre les différents pays et secteurs d'activité. Plus de 97 % des sondés sud-coréens et singapouriens ont affirmé avoir subi des retombées négatives suite à une fuite de données. 96 % des sondés du secteur de la vente au détail ont répondu la même chose. Plus de 80 % des sondés, tous pays et secteurs d'activité confondus, ayant signalé des conséquences négatives, il s'agit clairement d'un problème majeur et universel.

Quant aux 9 % qui ont indiqué n'avoir subi aucune conséquence, étant donné que leur incident n'a pas été signalé, ces sondés ressentent peut-être un faux sentiment de sécurité. Même si un incident n'est pas signalé sur le moment, rien ne garantit que des informations ne finiront pas par faire surface. Le préjudice porté à la réputation peut s'aggraver s'il semble qu'une entreprise a essayé de dissimuler les faits ou de fuir ses responsabilités. Avec la multiplication des réglementations, les entreprises n'auront peut-être bientôt plus le choix.

> 80 %

Plus de 80 % des sondés, tous pays et secteurs d'activité confondus, ont fait état de conséquences négatives.

Collaborateurs quittant l'entreprise et cybercriminels déterminés

Le paysage moderne des menaces confronte les équipes de sécurité à des défis provenant de tous les horizons. La rotation du personnel, le travail hybride, la migration vers le cloud, l'IA générative et l'évolution des techniques d'attaque sont autant de menaces pour la sécurité des données.

Les ressources étant dispersées entre tous ces domaines, une évaluation précise des risques devient un aspect critique d'une réponse efficace. Dans le cadre de notre enquête, nous avons demandé aux participants d'identifier les utilisateurs qui présentent le plus grand risque de fuites de données. Les collaborateurs ayant accès à des données sensibles, comme les professionnels des RH, les équipes financières et le personnel de support client, ont été la réponse la plus fréquente, citée par 63 % des sondés à travers le monde. Ces collaborateurs ont souvent accès à des données sensibles, comme des données personnelles et des informations financières, ou, dans le cas des équipes RH, aux salaires, aux performances et aux dossiers de congés médicaux. Le rôle d'un collaborateur peut également en faire une cible de choix pour les cybercriminels externes, qui espèrent voler ses identifiants de connexion via un email de phishing ou l'inciter à partager des éléments de propriété intellectuelle.

Seuls les sondés aux États-Unis ont cité les utilisateurs informatiques disposant d'un accès à privilèges comme le groupe le plus à risque. Les sondés des secteurs de la fabrication et des technologies ont également été une majorité à citer les utilisateurs informatiques. Cela peut indiquer que ces sondés ont davantage conscience que les utilisateurs informatiques peuvent manipuler ou détruire des données ainsi que les voler.

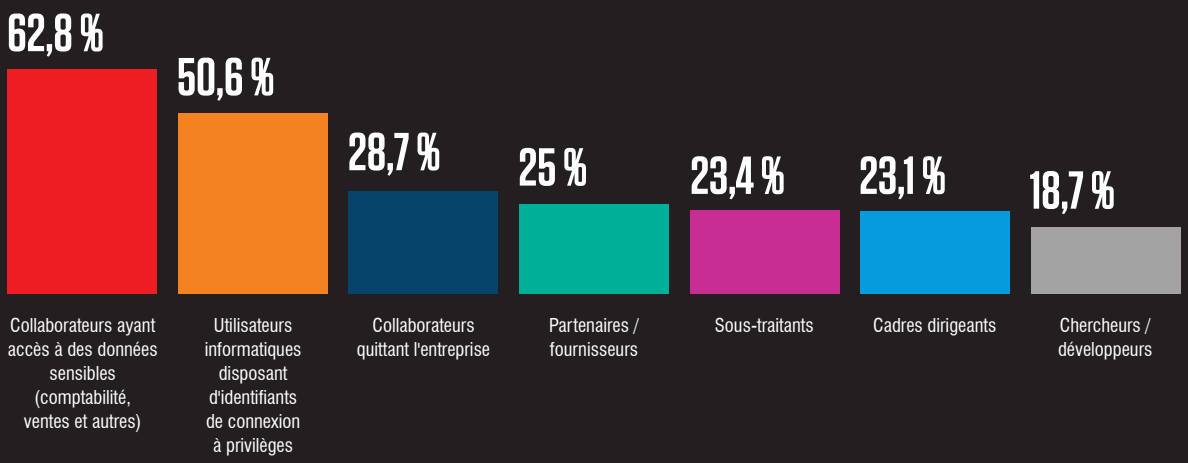
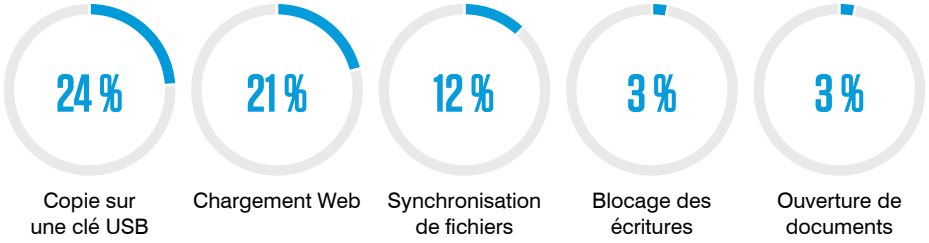


Figure 2. Utilisateurs qui présentent le plus grand risque de fuites de données

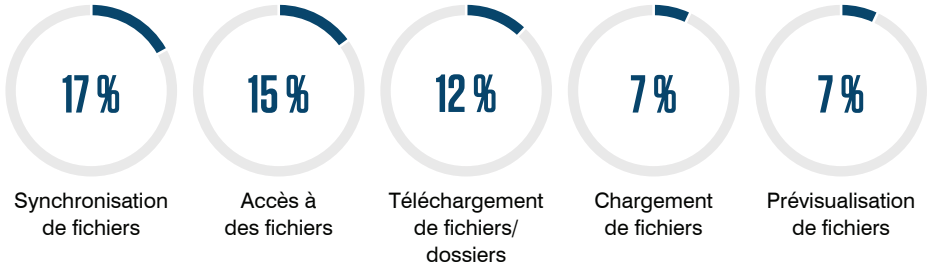
Alerte !

La menace posée par les utilisateurs négligents, compromis ou malveillants se reflète dans les types d'alertes déclenchées sur la plate-forme Proofpoint Information Protection. Près de la moitié des alertes sur les endpoints étaient causées par la copie de fichiers sur une clé USB ou par leur chargement sur le Web. Les principaux incidents cloud sont répartis de façon plus uniforme, le top 5 étant constitué de différentes opérations de chargement et de consultation de fichiers.

Catégories d'incidents sur les endpoints



Catégories d'incidents cloud



QU'EST-CE QU'UN UTILISATEUR MALVEILLANT ?

Bien qu'il puisse être réconfortant de s'imaginer que les cybercriminels sont des personnages éloignés, la menace vient parfois de l'intérieur. En réalité, les menaces internes peuvent être encore plus dangereuses que les attaques externes. Les utilisateurs internes malveillants peuvent attendre leur heure en exploitant un accès à privilèges pour mettre la main sur des données précieuses et exploiter des failles de la sécurité.

En décembre 2020, **Nickolas Sharp, collaborateur d'Ubiquiti**, a volé plusieurs gigaoctets de données confidentielles appartenant à l'entreprise. Il a utilisé le service VPN Surfshark pour dissimuler ses activités et son identité. Il s'est également servi de ses identifiants de connexion administrateur pour effacer les traces d'intrusion dans les journaux de serveur de l'entreprise. Peu de temps après, en janvier 2021, Ubiquiti a annoncé publiquement la compromission. Heureusement pour Nickolas Sharp, il faisait partie de l'équipe chargée d'enquêter sur l'incident. Dans le même temps, il poursuivait son action sournoise en coulisses. Il s'est fait passer pour un cyberpirate anonyme pour exiger d'Ubiquiti le paiement de 50 bitcoins (environ 1,9 million de dollars à l'époque) en échange des fichiers volés et d'informations sur la vulnérabilité exploitée. Ubiquiti a refusé de payer la rançon. En réponse, Nickolas Sharp a divulgué une partie des fichiers sur une plate-forme publique.

Deux mois plus tard, le FBI a perquisitionné son domicile et a saisi certains de ses terminaux. Imperturbable, Nickolas Sharp a contacté les médias en se faisant passer pour un lanceur d'alerte. Il a prétendu que l'entreprise minimisait la compromission. Lorsque la fausse nouvelle est sortie au grand jour, l'action d'Ubiquiti a perdu 20 % en une seule journée. Malgré le revers essuyé, Nickolas Sharp n'a pas renoncé à son plan pour faire fortune rapidement. Pour finir, c'est un bug technique qui a entraîné sa chute. Il s'avère que pendant le vol de données d'origine, son VPN a subi une panne temporaire, exposant l'adresse IP de son domicile. En mai 2023, Nickolas Sharp a été condamné à six ans de prison.

La prévalence des alertes USB n'est peut-être pas surprenante, car il s'agit de la catégorie la plus courante d'alertes configurées par des administrateurs à l'aide de nos produits. Outre les activités associées à des fichiers, les modifications apportées à Active Directory occupent la quatrième place et attestent du risque considérable que les menaces internes et externes font peser sur les réseaux. En cinquième place figure l'utilisation de sites d'IA générative. Bien que cette alerte n'ait pas été déclenchée assez souvent pour se classer parmi les plus courantes, sa présence sur la liste des alertes configurées montre à quel point les professionnels de la sécurité prennent au sérieux ce nouveau risque pour la sécurité des données.

Règles d'alerte les plus configurées pour la DLP et les menaces internes

- Copie sur une clé USB
- Exfiltration par chargement Web
- Exfiltration vers un dossier de synchronisation cloud
- Modifications apportées à Active Directory
- Utilisation de sites d'IA générative

La présence de l'IA générative mérite d'être soulignée, car elle n'est disponible que depuis cette année. Le risque que des utilisateurs saisissent des données sensibles dans des systèmes tels que Grammarly, ChatGPT, Bing Chat et Google Bard augmente chaque jour, car ces outils sont de plus en plus utiles et performants. Mais avec une faible transparence sur la façon dont les données soumises sont stockées et utilisées, et encore moins de clarté quant à la manière dont elles peuvent être retirées ou supprimées en cas d'envoi par erreur, ces systèmes représentent clairement un nouveau canal à risque via lequel des fuites de données peuvent se produire. Si certaines entreprises ont complètement banni l'utilisation des sites d'IA générative, d'autres reconnaissent les gains de productivité qu'ils peuvent offrir et ont décidé d'en surveiller l'utilisation.

La question délicate des départs

Les professionnels de la sécurité considèrent les collaborateurs quittant l'entreprise comme la troisième catégorie d'utilisateurs la plus à risque — un risque d'autant plus grand si ces collaborateurs avaient accès à des données sensibles ou à privilèges dans le cadre de leurs fonctions. Les collaborateurs sur le point de quitter l'entreprise estiment souvent avoir le droit de conserver des informations à leur départ, compte tenu du temps et des efforts qu'ils ont consacrés à une initiative, un produit ou un projet. Ces informations peuvent également leur donner un avantage dans leur nouveau poste.

Selon les données de notre plate-forme, cette préoccupation est justifiée. Sur une période de neuf mois, 87 % des exfiltrations de fichiers suspectes via des locataires cloud utilisant Proofpoint ont été causées par des collaborateurs quittant l'entreprise. Ce volume anormalement élevé peut indiquer qu'un collaborateur rassemble des fichiers et des données avant de quitter l'entreprise. Autoriser les collaborateurs à accéder à des données et à les stocker sur leurs terminaux personnels peut offrir un gain de productivité aux entreprises, mais il est facile de comprendre à quel point cette politique peut rapidement engendrer des risques de fuites de données.

Risques liés au cloud

Près de 38 % des sondés ont indiqué que la prolifération des applications cloud/SaaS est un défi pour leurs programmes DLP. Maintenant que de nombreuses entreprises ont adopté des solutions cloud en raison de la transition vers le travail hybride et de la transformation numérique, ces banques de données constituent une cible de choix pour les cybercriminels.

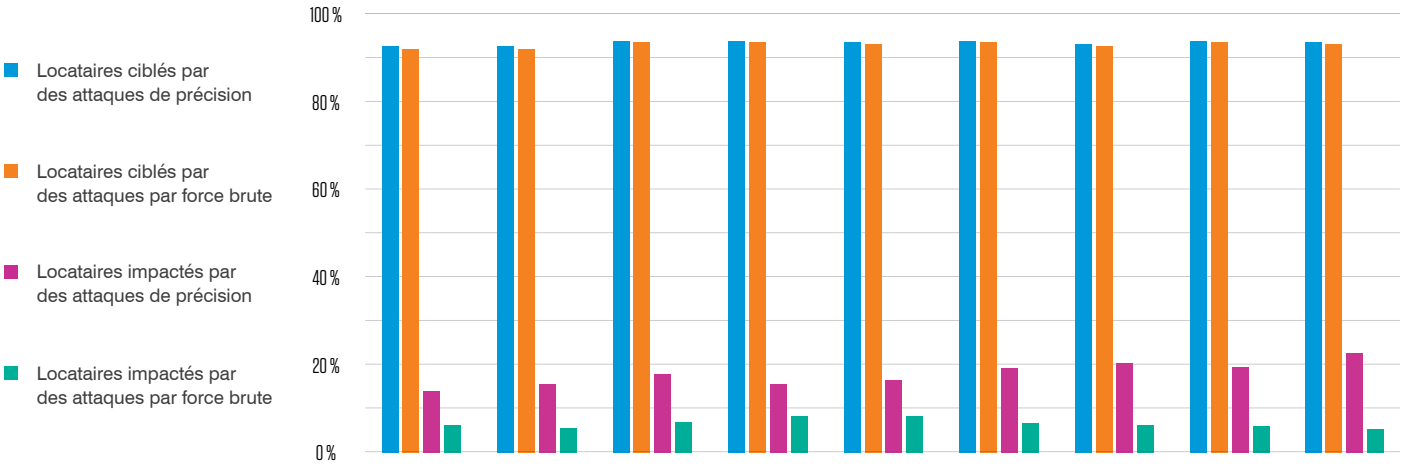


Figure 3. Vecteurs d'attaque au fil du temps

Le risque qui pèse sur les locataires cloud est confirmé par les données sur les menaces de notre plate-forme. Entre janvier et septembre 2023, 96 % des locataires cloud surveillés ont été ciblés par des attaques par force brute. Lors d'une attaque par force brute, des cybercriminels tentent d'obtenir un accès en devinant des mots de passe ou par d'autres moyens automatisés. Plus inquiétant encore, sur la même période, 96 % des locataires ont été visés par des attaques de précision, comme des tentatives de phishing ciblées. Bon nombre de ces attaques plus sophistiquées ont été fructueuses : 54 % des locataires ont été compromis au moins une fois par ce biais, alors que seulement 20 % d'entre eux l'ont été via des méthodes par force brute.

Cette grande différence d'efficacité peut s'expliquer par l'utilisation de l'ingénierie sociale et de kit d'outils sophistiqués qui permettent aux cybercriminels de contourner des mécanismes de sécurité avancés tels que l'authentification multifacteur (MFA). Tous types d'attaques confondus, les cybercriminels externes ont enregistré un taux de succès global de 58 % lorsqu'ils essayaient d'infiltrer des locataires cloud, ce qui montre qu'ils savent que les fuites de données sont centrées sur les personnes et qu'ils cherchent à exploiter les vulnérabilités des utilisateurs.

QU'EST-CE QU'UN UTILISATEUR COMPROMIS ?

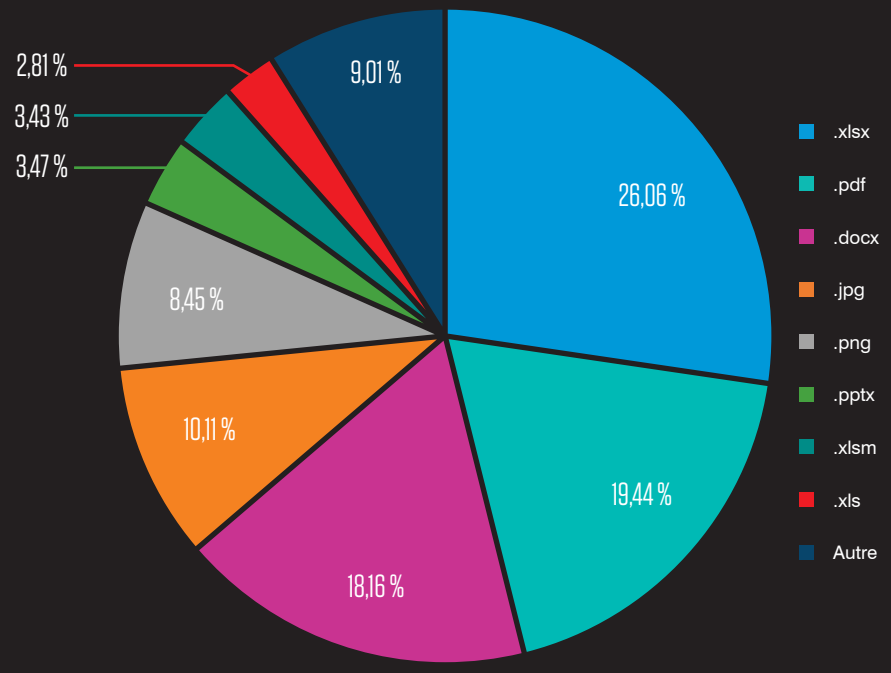
Les vulnérabilités « zero-day » ont beau faire les gros titres, si les cybercriminels les plus actifs se concentrent sur les personnes plutôt que les systèmes, ce n'est pas pour rien. Les collaborateurs des départements financier, informatique, des ressources humaines et du support client peuvent avoir accès à une foule de données précieuses. La compromission de l'identité d'un collaborateur à privilèges élevés peut permettre à un cybercriminel de se déplacer latéralement sur l'ensemble du réseau, de voler des données et de distribuer un ransomware, lequel se livre désormais souvent à des activités de chiffrement et d'exfiltration des données (technique appelée « double extorsion »).

En 2022, LastPass, un des gestionnaires de mots de passe les plus populaires au monde, a subi une violation de données majeure découlant de la compromission d'un seul utilisateur. Tout a commencé en août 2022, lorsque LastPass a révélé qu'une personne non autorisée avait obtenu un accès à son environnement de développement par le biais de l'ordinateur personnel d'un ingénieur compromis. Pendant l'attaque, un enregistreur de frappe a été installé et du code source a été volé. Mais ce n'est pas tout. Au cours des deux mois suivants, le cybercriminel a accédé à d'autres informations, y compris aux identifiants de connexion de collaborateurs et à des clés de déchiffrement. Grâce à ces identifiants de connexion valides, le cyberpirate a pu échapper à toute détection pendant plusieurs mois. Les clés volées lui ont ensuite permis de déchiffrer des volumes de stockage au sein des buckets Amazon S3 de l'entreprise. Une fois infiltré, le cybercriminel a alors exporté un large éventail de données, y compris des coffres-forts de mots de passe clients. En partant d'un seul utilisateur compromis, une attaque a pu être déployée et a fini par ébranler la confiance dans la gestion des mots de passe en tant que bonne pratique de sécurité.

Lorsqu'un locataire cloud est compromis, les cybercriminels commencent souvent par explorer les fichiers stockés et autres données. 30 % des locataires compromis ont subi une exfiltration de données ou une manipulation de fichiers post-compromission. Les documents aux formats .docx, .xlsx et .pdf sont ceux qui ont présenté les plus hauts niveaux d'activités suspectes. Le fait que le format de fichier .docx soit le plus prévalent peut indiquer un intérêt moindre pour les données hautement structurées et réglementées figurant souvent dans les fichiers .xlsx. Les cyberpirates savent que des données d'entreprise précieuses sont désormais capturées dans des documents moins structurés, raison pour laquelle ils s'y intéressent.

Par exemple, dans un récent incident analysé par Proofpoint, les cybercriminels ont accédé à plusieurs applications de connexion, dont le portail Azure et Microsoft 365 SharePoint Online, pour compromettre un compte. Ils ont chargé, modifié, prévisualisé ou téléchargé 45 fichiers sensibles. Lors d'un incident similaire, un cyberpirate a exfiltré quatre fichiers Excel contenant le terme « salaires » dans leur nom.

Répartition des formats de fichier dans les activités suspectes liées aux fichiers



Les espaces de travail cloud sont eux aussi de plus en plus menacés par des applications OAuth malveillantes ou exploitées. Tout comme les malwares traditionnels, une application OAuth malveillante peut permettre à des cybercriminels de faire ce qu'ils souhaitent sur un locataire infecté. Nos données indiquent que 11 % des locataires cloud ont été affectés par des applications OAuth malveillantes persistantes. Mais la menace ne se limite pas à des applications malveillantes spécifiques. Les applications cloud légitimes sont désormais fréquemment exploitées par des cybercriminels qui cherchent à obtenir un accès persistant à un locataire après une compromission. En effet, une application OAuth reste autorisée jusqu'à ce que son accès soit révoqué. Nous avons découvert que plus de 15 % des entreprises compromises ont subi ce type d'exploitation d'applications autorisées après une compromission initiale.

La maturation n'a pas pour seul objectif la conformité

De nombreux programmes DLP ont été élaborés pour répondre aux réglementations légales. Mais selon les sondés, les réglementations et la conformité ne sont plus les principaux facteurs de motivation. Il semble qu'à mesure que ces initiatives gagnent en maturité, l'accent soit mis sur la protection de la vie privée des clients et des collaborateurs, car plus de 50 % des sondés la citent comme principal facteur de motivation derrière leur programme DLP. Si cela est sans doute en partie lié aux nouvelles réglementations sur la confidentialité introduites aux niveaux local et international, il semble y avoir un réel désir de ne pas se limiter au minimum légal.

Figure 4. Principaux facteurs de motivation derrière les programmes DLP

Il existe toutefois des cas particuliers, surtout en Europe, où des lois strictes en matière de protection des données, comme le règlement général sur la protection des données (RGPD), sont en vigueur. Les sondés français et britanniques ont déclaré que la conformité aux réglementations externes était leur principale source de motivation pour la DLP. Par ailleurs, les sondés espagnols et brésiliens ont été les moins nombreux à citer les réglementations comme principal facteur (environ 18 % pour chaque pays). Les sondés allemands ont également mentionné la réduction des coûts associés aux fuites de données et la protection de la propriété intellectuelle comme leurs deuxième et troisième sources de motivation après la confidentialité. En Corée du Sud, la conformité interne était le principal facteur, la conformité externe arrivant en deuxième place.

Les réglementations étaient la principale motivation citée par les sondés du secteur des finances — ce qui n'a rien de surprenant, compte tenu du niveau de supervision auquel ces entreprises sont généralement soumises. Les sondés du secteur de la santé et des administrations publiques ont également cité les réglementations comme étant leur deuxième source de motivation.

La situation se complique lorsque nous nous intéressons aux catégories de données que les sondés considèrent comme les plus importantes à protéger. Les données d'entreprise précieuses arrivent en première position, suivies de près par les informations des clients. Le secteur de la santé constitue un cas particulier, les données médicales protégées étant citées par 60 % de ces sondés.

Figure 5. Préoccupation pour la protection des données, par type

NIVEAUX DE MATURITÉ DE LA DLP

Émergent : entreprises disposant d'un programme DLP limité ou sans programme DLP formel. Elles peuvent utiliser des solutions isolées dotées de fonctionnalités DLP (CASB, IPS, SWG, SEG).

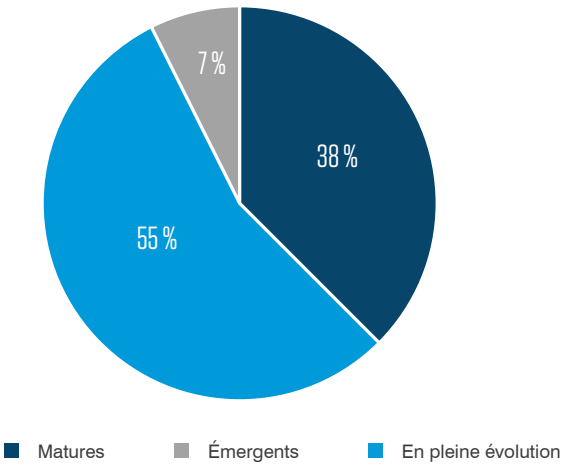
En pleine évolution : entreprises disposant d'un programme DLP formel sur certains canaux DLP, utilisé principalement à des fins d'audit et de génération de rapports.

Mature : entreprises disposant d'un programme DLP formel sur les principaux canaux DLP avec des fonctionnalités de classification ainsi qu'une prévention et une correction automatisées.

L'accent mis sur les « données d'entreprise précieuses » — une catégorie vague qui inclut les contrats, les listes de prix et les accords de fusion-acquisition — pourrait refléter la maturité croissante des plates-formes DLP ainsi qu'une évolution des priorités. Les systèmes DLP ont initialement été conçus pour protéger les données hautement structurées, comme les informations de paiement, les numéros d'identification des citoyens et les comptes utilisateur. Mais bon nombre d'entre eux sont désormais suffisamment flexibles pour surveiller et protéger des données dans des domaines non statiques, où les informations circulent librement dans le cadre des activités quotidiennes. Les solutions DLP innovantes se sont adaptées à l'augmentation de la diversité et du volume de données engendrée par la transformation numérique. Par exemple, les catégories non conventionnelles comme le code source et les conceptions CAD pourraient désormais représenter la propriété intellectuelle la plus précieuse d'une entreprise.

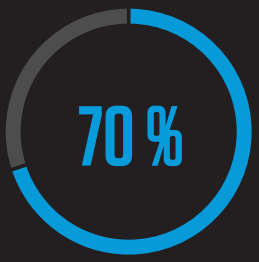
Mais alors qu'il ne fait aucun doute que les programmes et technologies DLP gagnent en maturité, seul un peu plus d'un tiers des sondés ont indiqué que leur programme était totalement « mature ». La majorité des sondés ont affirmé que leur programme était « en pleine évolution » — nous pouvons donc nous attendre à ce que l'équilibre entre facteurs de motivation et hiérarchisation des données continue à évoluer à mesure que les niveaux globaux de maturité augmentent.

État de la maturité des programmes DLP à travers le monde



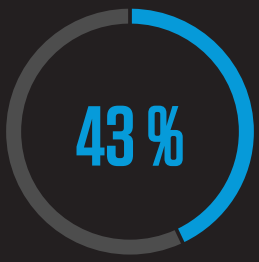
Le regard tourné vers l'avenir : meilleure visibilité, expertise approfondie

Face à la maturation des programmes DLP, les sondés sont largement d'accord sur les principaux défis actuels. Près de 70 % mentionnent la visibilité sur les données sensibles, la modification des comportements des utilisateurs et la protection contre les menaces externes comme les fonctionnalités les plus importantes de leur programme DLP. Toutefois, 43 % affirment qu'il s'agit d'un domaine qui requiert encore des améliorations. Compte tenu de la dispersion des effectifs modernes (augmentant l'accès aux données via la messagerie, les endpoints, le Web et le cloud) et de la sophistication des cybercriminels, il n'est pas surprenant que la visibilité soit considérée comme la fonctionnalité DLP la plus importante. La visibilité sur plusieurs canaux fournit aux équipes de sécurité le contexte dont elles ont besoin pour réagir de façon appropriée face à un utilisateur négligent, malveillant ou compromis.



mentionnent la visibilité sur les données sensibles, la modification des comportements des utilisateurs et la protection contre les menaces externes comme les fonctionnalités les plus importantes de leur programme DLP

mais



affirment qu'il s'agit d'un domaine qui requiert encore des améliorations.

En termes de ressources, la plupart des sondés ont indiqué qu'ils étaient satisfaits du niveau d'investissement et de soutien de la direction en faveur de leur programme DLP. Cela peut sembler étonnant compte tenu de la lutte interminable entre les cybercriminels et les équipes de sécurité, mais cela confirme que la sécurité des données est devenue un problème concernant la direction et que les hauts responsables ont conscience de la nécessité de protéger les ressources stratégiques de l'entreprise. Face aux nombreux incidents d'envergure qui font les gros titres à travers le monde, de nombreux cadres dirigeants et membres de conseil d'administration font tout pour éviter de subir le même sort que d'autres entreprises de leur secteur.

70 %

des sondés ont mentionné la visibilité sur les données sensibles, la modification des comportements des utilisateurs et la protection contre les menaces externes comme les fonctionnalités DLP les plus importantes pour prémunir leur entreprise contre les fuites de données.

Toutefois, la situation est quelque peu différente pour les sondés qui considèrent leur programme DLP comme « émergent ». Ils sont davantage susceptibles de mentionner un besoin constant de budgets plus importants et d'outils plus performants pour améliorer la visibilité sur tous les canaux. Il est possible que ces sondés utilisent toujours des outils limités à un seul canal, ce qui ne leur offre pas une vue d'ensemble des fuites de données et des menaces internes potentielles.

Outre une meilleure visibilité, les autres améliorations nécessaires selon la plupart des sondés sont une intégration plus étroite avec l'écosystème informatique/de sécurité et un personnel plus qualifié. Le secteur de la sécurité est extrêmement fragmenté, avec de nombreuses solutions isolées pour remédier à des faiblesses spécifiques. Le développement de nouvelles solutions fait émerger des fonctionnalités inédites, mais alourdit également la charge de travail des équipes de sécurité, qui doivent s'assurer que tout fonctionne parfaitement. Dans le cas contraire, elles risquent de perdre un temps précieux à basculer entre différents outils.

Les sondés qui ont qualifié leur programme de « mature » ont également exprimé un désir grandissant de disposer d'outils basés sur l'IA. Compte tenu de la pénurie actuelle de professionnels de la sécurité qualifiés, l'IA a le potentiel de renforcer la productivité des analystes tout en réduisant le risque de surmenage.

Conclusion

Plus de 90 % des personnes interrogées dans le cadre de notre enquête ont indiqué que leur entreprise était en train d'investir dans des solutions DLP — une bonne nouvelle pour les clients, les collaborateurs et les parties prenantes. Toutefois, seulement 41 % d'entre elles étaient « tout à fait d'accord » pour dire que leurs investissements étaient adéquats.

Seulement 41 %

des sondés sont « tout à fait d'accord » pour dire que leur niveau actuel d'investissement dans des outils et une expertise DLP est adéquat.

Face à l'adoption généralisée du cloud, du travail hybride et d'innovations de workflow comme l'IA générative par les entreprises, les solutions DLP doivent suivre le mouvement. Chaque menace interne et fuite de données est unique et peut causer des dommages considérables. C'est pourquoi la détection, l'analyse et la neutralisation de chacune d'entre elles requièrent une approche qui reconnaît les fuites de données comme un problème humain et qui offre une visibilité sur les comportements des utilisateurs, les contenus et les menaces, et ce sur divers canaux : cloud, endpoints, messagerie, Web, etc. Qu'un programme DLP soit mature, en pleine évolution ou émergent, les équipes de sécurité doivent mettre en place des processus pour :

- Surveiller les personnes ayant accès à des données sensibles ou disposant de privilèges administrateur
- Mettre en place un processus d'évaluation de la sécurité pour les collaborateurs quittant l'entreprise
- Implémenter des règles DLP pour les méthodes courantes d'exfiltration de données, comme les emails, la copie sur une clé USB, le chargement Web, la synchronisation de fichiers dans le cloud et le partage étendu de fichiers dans le cloud
- Identifier et protéger les ressources et données stratégiques grâce à la classification des données
- Examiner régulièrement le programme DLP, en gardant à l'esprit que l'adoption de l'IA générative et d'autres avancées technologiques sont susceptibles de modifier les comportements des utilisateurs

En plus de cette liste de contrôle, le passage du niveau « émergent » au niveau ultérieur requiert un investissement dans une plate-forme DLP spécialisée dotée d'une architecture moderne et axée sur le cloud. En offrant une visibilité sur les utilisateurs et les données pour chaque incident, une plate-forme DLP robuste fournit un contexte essentiel permettant aux équipes de sécurité de savoir comment réagir. Vous pouvez ainsi couvrir l'éventail complet de scénarios de fuites de données centrées sur les personnes, qu'il s'agisse de déjouer des menaces externes ou d'identifier les utilisateurs malveillants, négligents et compromis dans vos rangs.

Méthodologie

Données internes de Proofpoint

Les données ont été extraites de la plate-forme Proofpoint Information Protection entre janvier et septembre 2023 et de déploiements Tessian sélectionnés aléatoirement entre janvier et décembre 2023.

Données de l'enquête

Proofpoint s'est associé à CyberEdge, une entreprise de recherche en cybersécurité, pour développer l'instrument d'enquête en 15 questions, le localiser dans des langues autres que l'anglais, héberger l'enquête, permettre aux participants d'y répondre et analyser les résultats. Les sondés sont des professionnels de la sécurité informatique employés par une organisation commerciale, à but non lucratif ou gouvernementale comptant au minimum 1 000 collaborateurs.

Les participants à l'enquête sont issus de 12 pays et 17 secteurs d'activité. La taille de l'échantillon étant de 600 participants, la marge d'erreur de l'enquête à l'échelle mondiale (avec un niveau de confiance standard de 95 %) s'élève à 4 %. Tous les résultats associés à des pays et à des secteurs d'activité spécifiques doivent être considérés comme anecdotiques, car leurs tailles d'échantillon sont beaucoup plus petites. Proofpoint recommande de tenir uniquement compte des données mondiales pour prendre des décisions avisées.

À propos de CyberEdge

Fondée en 2012, CyberEdge est la plus grande entreprise de recherche, de marketing et de publication au service de la communauté des éditeurs de solutions de cybersécurité. Elle travaille avec près d'un éditeur de solutions de sécurité établi sur six.

Le célèbre rapport Cyberthreat Defense Report (CDR) de CyberEdge et d'autres rapports d'enquête soutenus par un ou plusieurs sponsors ont été primés à de nombreuses reprises et cités par des médias d'affaires et technologiques comme The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading et CISO Magazine.

CyberEdge est réputée pour fournir les données de recherche, les rapports d'enquête, les rapports d'analyse, les livres blancs et les ouvrages et eBooks personnalisés les plus qualitatifs du secteur de la cybersécurité. La profondeur de son expertise en cybersécurité et l'étendue de ses services sont inégalées.

Pour en savoir plus sur CyberEdge, consultez le site **www.cyber-edge.com**.

À propos de Proofpoint, Inc.

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 85 % 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.

0407-001-03-01 01/24