VARONIS

2025

RAPPORT SUR L'ÉTAT DE LA SÉCURITÉ DES DONNÉES

MESURER L'IMPACT DE L'IA SUR LES RISQUES LIÉS AUX DONNÉES

Enseignements tirés de 1 000 environnements informatiques réels

RÉSULTATS CLÉS

L'adoption de l'IA dépasse les mesures de sécurité.

Bien que l'IA puisse favoriser le progrès, elle peut également accélérer les risques. Dans notre étude de 1 000 organisations, nous avons découvert des problèmes alarmants en matière de sécurité des données :

90 % **des entreprises ont exposé des données sensibles dans le cloud.**

Les données critiques non verrouillées peuvent être révélées par l'IA. Les données d'entraînement de l'IA exposées sont vulnérables aux fuites de données et à l'empoisonnement des modèles.

88 % **ont des utilisateurs fantômes activés mais obsolètes.**

Ces comptes restent activés et donnent accès aux applications et aux données. Les utilisateurs fantômes peuvent permettre aux hackers de mener des opérations de reconnaissance ou d'exfiltrer des données sans déclencher d'alarme.

98 % **ont des applications non vérifiées, dont des IA non autorisées.**

Le Shadow AI augmente le risque d'exposition et de fuite de données. Les attaquants peuvent utiliser des applications non vérifiées pour les exfiltrer.

99 % **des entreprises ont des données sensibles dangereusement exposées aux outils d'IA.**

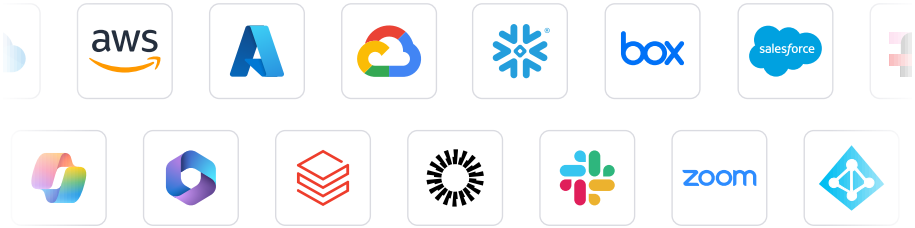
À PROPOS DE CE RAPPORT

Méthodologie

Varonis a analysé les risques de sécurité des données dans un large éventail de secteurs et de zones géographiques :

- 1 000 entreprises
- Près de 10 milliards de ressources cloud (objets, fichiers, rapports, pièces jointes, etc.)
- Plus de 20 pétaoctets de données — environ 20 téraoctets par organisation

Applications et services IaaS et SaaS examinés :



Pays inclus :

États-Unis, Canada, Allemagne, France, Belgique, Pays-Bas, Suède, Suisse, Royaume-Uni, Espagne, Italie, Brésil, Australie, Inde, etc.

Analyse firmographique

Ce rapport analyse les données de différents secteurs :

- Santé/biotechnologie/pharmaceutique
- Finances
- Gouvernement/secteur public
- Assurance et services professionnels
- Fabrication
- Éducation
- Technologie
- Consommation/commerce de détail
- Et d'autres...

TABLE DES MATIÈRES

LE SHADOW AI :
UNE MENACE LATENTE POUR LA SÉCURITÉ DES DONNÉES

Le Shadow AI, qui désigne les applications d'IA générative non autorisées, représente une menace de taille pour la sécurité des données. Ces outils peuvent contourner la gouvernance d'entreprise et la supervision informatique, et par conséquent, entraîner des fuites de données.

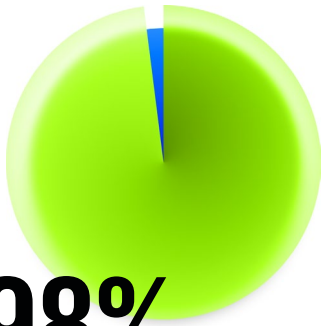
Les employés peuvent accidentellement divulguer des données sensibles ou confidentielles en utilisant le Shadow AI. Si ces applications ne respectent pas le GDPR, la loi HIPAA et d'autres réglementations, les entreprises s'exposent à des amendes.

Les applications obsolètes présentent toujours des risques après la dernière connexion d'un utilisateur. Les applications OAuth obsolètes, qui n'ont pas été utilisées ou consultées depuis des semaines voire des mois, permettent toujours d'accéder à des données sensibles.

En 2025, des millions d'utilisateurs ont téléchargé DeepSeek.

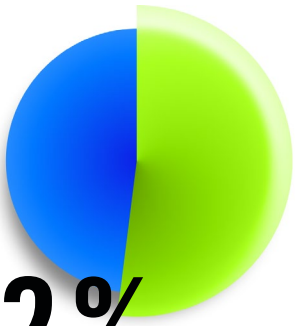
Les employés qui ont téléchargé DeepSeek ont mis en danger les données de leur entreprise. Une **base de données DeepSeek non sécurisée** a exposé un million de lignes de flux de logs contenant l'historique des discussions, des clés secrètes, des informations sur le backend et d'autres données extrêmement sensibles. Les entreprises doivent donc examiner et sécuriser toutes les applications d'IA.

MALGRÉ LES RISQUES, NOTRE ANALYSE A RÉVÉLÉ CE QUI SUIT :



98%

des entreprises ont des employés qui utilisent des applications non autorisées, dont le Shadow AI. En moyenne, une entreprise possède **1 200** applications non officielles.



52 %

des employés utilisent des applications OAuth à haut risque

1 sur 4

les applications OAuth non vérifiées (200 sur 800) dans une entreprise moyenne sont à haut risque

PROJECTEUR :

RISQUES LIÉS AUX DONNÉES MICROSOFT 365 COPILOT

Si les applications non autorisées peuvent accroître le risque de fuite de données, même celles autorisées peuvent menacer les données sensibles.

Microsoft 365 Copilot s'intègre parfaitement aux données d'une entreprise pour accroître la productivité. Mais il engendre également des risques pour la sécurité. Copilot peut afficher toutes les données accessibles, et donc potentiellement exposer des informations critiques.

Une prompt de Copilot suffit pour exposer les données. Prenons l'exemple d'une compagnie d'assurance de 2 000 employés : si chacun d'entre eux saisit 20 prompts par jour, cinq jours par semaine, l'entreprise a plus de 200 000 chances de voir des données sensibles exposées hebdomadairement.

NOUS AVONS TROUVÉ :

90 %
des entreprises ont des fichiers sensibles accessibles à tous les employés via M365 Copilot

+ de 25 000
dossiers sensibles sont exposés à tous les employés en moyenne

6 %
des entreprises ont des fichiers sensibles accessibles sur Internet

Le labeling des fichiers, qui garantit que les données sont catégorisées, gérées et protégées contre toute utilisation abusive de l'IA, est essentiel pour la gouvernance des données.

Le data labeling permet d'appliquer les contrôles tels que la prévention des pertes de données et le chiffrement. Il soutient également les exigences de conformité réglementaire en montrant que les données sont traitées conformément aux normes et politiques juridiques. Pour être efficace, il doit être automatisé et continu.

Malgré l'importance du labeling, seule une entreprise sur dix avait des fichiers comportant un label.

PROJECTEUR :

RISQUE LIÉ AUX DONNÉES SALESFORCE AGENTFORCE

Les organisations Salesforce contiennent de nombreuses données sensibles (données à caractère personnel, PCI, informations financières, etc). Les administrateurs supervisent généralement le CRM. Ils s'occupent de tous les aspects, de la gestion des utilisateurs aux paramètres de sécurité. Cependant, cela signifie généralement que les équipes informatiques et de sécurité ne sont pas toujours informées. Cela peut entraîner des lacunes de sécurité.

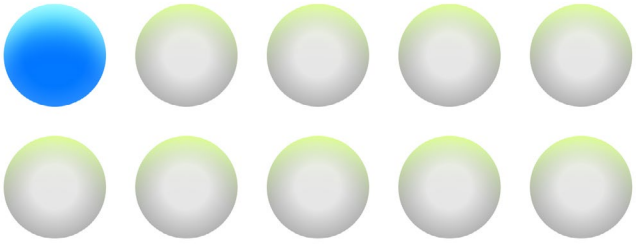
Salesforce Agentforce peut amplifier ces lacunes si les données sont exposées. En effet, les agents peuvent révéler des informations sensibles non protégées par le biais de prompts en langage naturel, ce qui peut entraîner un accès non autorisé aux données et une utilisation abusive.

Nous avons identifié un nombre inquiétant d'utilisateurs et de comptes de service qui peuvent facilement accéder à toutes les données Salesforce via un agent Agentforce et exporter ces données. Donner à n'importe quel utilisateur l'autorisation nécessaire pour télécharger toutes les données Salesforce laisse présager une catastrophe.

100 %

des entreprises ont au moins un compte capable d'exporter toutes les données

1 sur 10 comptes peuvent librement exporter toutes les données Salesforce

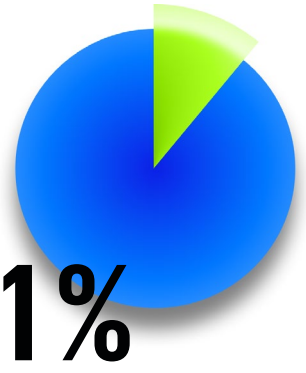


Notre analyse a révélé un nombre étonnamment élevé d'utilisateurs qui disposent d'autorisations administratives étendues. Permettre à de nombreux utilisateurs d'installer des applications tierces, de définir la sécurité au niveau des champs et de manipuler les autorisations augmente le risque d'exposition des données critiques dans Salesforce et de mouvements latéraux.

Une entreprise de taille moyenne qui compte 1 000 employés dispose de 110 utilisateurs ayant l'autorisation de créer et d'accorder des autorisations, et de personnaliser des applications. Si une menace avancée persistante (APT) compromet un seul compte utilisateur de Salesforce, elle peut accorder l'accès à d'autres attaquants ou vendre des identifiants hautement privilégiés sur le dark Web.

De nombreux utilisateurs peuvent également créer des liens publics. Les liens ouverts peuvent involontairement permettre aux applications d'IA, comme ChatGPT, de parcourir les données internes de votre entreprise pour répondre aux prompts et donner à des personnes non autorisées l'accès à des données sensibles de l'entreprise et des clients.

Lorsque les utilisateurs disposent d'une autorisation, partager des liens publics est chose aisée. Si l'un de ces utilisateurs est compromis, un hacker peut créer et utiliser ces liens pour voler des données sensibles.



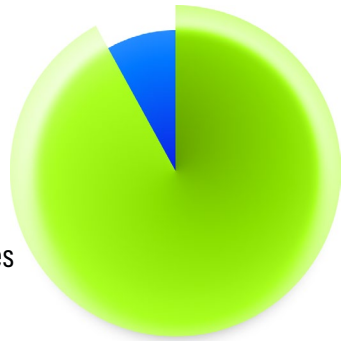
11 %

Part d'utilisateurs qui peuvent accorder des autorisations et installer des applications personnalisées

NOUS AVONS CONSTATÉ QU'UN NOMBRE ALARMANT D'UTILISATEURS PEUVENT CRÉER DES LIENS DE PARTAGE :

92 %

des entreprises autorisent les utilisateurs à créer des liens publics



de ces entreprises,

3 689

les utilisateurs peuvent créer des liens publics

EMPOISONNEMENT DES MODÈLES ET RISQUES POUR LES DONNÉES D'ENTRAÎNEMENT DE L'IA

Alors que de plus en plus d'entreprises développent leurs propres processus et produits d'IA, les données utilisées pour les entraîner sont exposées à des risques de fuites et d'attaques. Dans la mesure où les données d'entraînement sont stockées dans plusieurs clouds ou IaaS, il peut être difficile de gérer les autorisations de manière uniforme dans tous les environnements.

Les modèles entraînés sur des données sensibles peuvent exposer par inadvertance des informations confidentielles. Les données d'entraînement exposées peuvent conduire à un accès non autorisé et une utilisation abusive, et ainsi compromettre l'intégrité et la sécurité des systèmes d'IA.

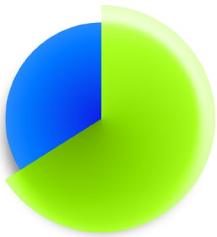
Compte tenu des gros volumes d'informations sensibles et des nombreux utilisateurs à gérer, la sécurité des données dans le cloud peut s'avérer complexe à grande échelle. Notre analyse a montré que les données cloud, y compris les données non masquées et les compartiments exposés, sont largement surexposées et sous-protégées.

NOUS AVONS TROUVÉ :

9 sur 10

entreprises ont exposé des données sensibles dans le cloud

66 %



des entreprises ont des données cloud exposées à des utilisateurs anonymes

Le chiffrement des données protège les données utilisées pour entraîner les LLM en les convertissant dans un format sécurisé auquel seules les personnes autorisées qui disposent d'une clé de déchiffrement peuvent accéder. Grâce à cette méthode, les informations sensibles restent confidentielles et ne sont pas exposées à des utilisateurs non autorisés. Le chiffrement permet également d'éviter les fuites de données pendant le processus d'entraînement, de la collecte des données au prétraitement, puis à l'entraînement des modèles.

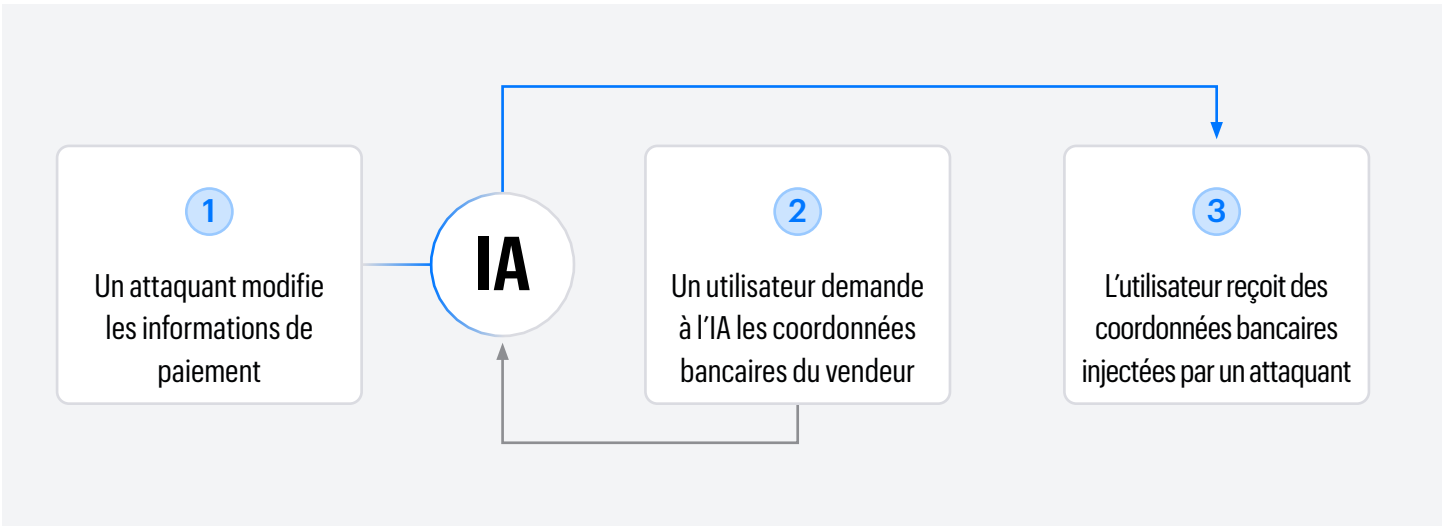
NOUS AVONS TROUVÉ :

2 000 stockages d'objets non chiffrés dans une entreprise moyenne

1 500 bases de données non chiffrées dans une entreprise moyenne

Autre risque majeur : l'empoisonnement des modèles. Il s'agit de manipuler les données d'entraînement pour corrompre les performances d'un modèle d'IA. Ce type d'attaque se produit lorsqu'un utilisateur malveillant accède aux ressources cloud du modèle, telles que les conteneurs, les comptes de stockage et les bases de données, et peut écrire ou modifier ces ressources sans déclencher d'alarme.

L'empoisonnement des modèles peut entraîner des conséquences dramatiques. Imaginons qu'un attaquant modifie les informations de paiement utilisées dans un modèle. Sans le savoir, l'entreprise le déploie. Lorsqu'un utilisateur demande les coordonnées bancaires du vendeur, il reçoit les coordonnées bancaires injectées par le pirate.



Ces attaques peuvent également se produire accidentellement. Imaginons qu'un analyste dans une entreprise médicale entraîne par inadvertance un modèle sur des données incorrectes. Sans données précises, les médecins et le personnel soignant peuvent prendre de mauvaises décisions pour leurs patients. Si l'empoisonnement du modèle n'est pas détecté suffisamment tôt, il sera difficile de le repérer en surveillant les performances du modèle.

DES FANTÔMES DANS LA MACHINE :

EXPLOITATION DE LA SURFACE D'EXPOSITION

Une fois dans votre environnement, les attaquants cherchent à s'implanter et à s'étendre. Les comptes utilisateur obsolètes, ou « utilisateurs fantômes », sont des comptes actifs d'anciens employés ou sous-traitants. Ces comptes restent activés et donnent accès aux applications et aux données. Ils offrent ainsi la possibilité aux hackers de mener des opérations de reconnaissance ou d'exfiltrer des données sans déclencher d'alarme.

La gestion des identités actives est essentielle, en particulier en ce qui concerne le déploiement d'agents d'IA. Si une seule identité est compromise, les hackers peuvent se déplacer latéralement, utiliser l'IA pour trouver des informations sensibles ou installer des logiciels malveillants. Avec des audits réguliers et des solutions éprouvées de gestion des identités, seules les identités nécessaires restent actives et chacune d'entre elles dispose d'un accès approprié.

88 %

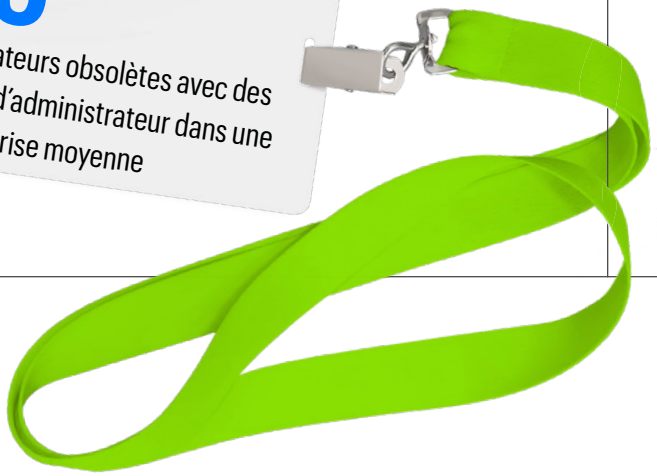
des entreprises ont des utilisateurs fantômes obsolètes mais activés (en moyenne, 15 000 par entreprise)

176 000

identités externes inactives dans une entreprise moyenne

10

utilisateurs obsolètes avec des rôles d'administrateur dans une entreprise moyenne

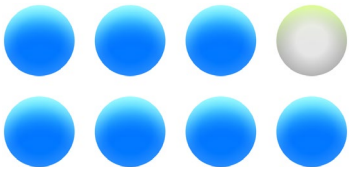


>31 000

autorisations obsolètes dans une organisation moyenne

Les parties prenantes internes qui disposent d'un accès légitime peuvent, par inadvertance ou dans une mauvaise intention, exposer des données sensibles. Le renforcement des protocoles de gestion des identités peut contribuer à atténuer ces risques en s'assurant que seuls les utilisateurs autorisés ont accès aux systèmes et données critiques.

NOUS AVONS TROUVÉ :



7 sur 8 entreprises ont des données sensibles exposées à ***chaque*** utilisateur

IDENTITÉS CLOUD :
PROLIFÉRATION ET COMPLEXITÉ

Les groupes, les adhésions et les rôles peuvent se développer au fil du temps. Un seul utilisateur peut cumuler des dizaines de rôles et d'adhésions à des groupes. Parallèlement, les équipes informatiques et de sécurité en sous-effectif ont souvent du mal à révoquer les adhésions inutilisées ou superflues lorsque les utilisateurs changent de poste ou quittent l'entreprise.

Notre analyse montre que les entreprises ont pris du retard dans la gestion des autorisations et la sécurisation des identités, en particulier les identités non humaines telles que les API et les comptes de service. Une mauvaise gestion des identifiants et des privilèges excessifs entraînent des accès non autorisés et des fuites de données.

La gestion des identités et des droits dans le cloud peut impliquer des milliers d'autorisations et de rôles. Elle nécessite un travail constant pour garder une longueur d'avance sur les cybercriminels. L'environnement AWS à lui seul dispose de **plus de 18 000 autorisations possibles de gestion des identités et des accès** à gérer.

NOTRE ANALYSE DES ORGANISATIONS UTILISANT AWS A MONTRÉ :

20 224 politiques gérées dans le compte AWS moyen

3 087 politiques de droits d'accès excessifs dans le compte AWS moyen

PAS DE MFA :
UNE FAILLE DE SÉCURITÉ MAJEURE

L'absence de MFA facilite la tâche des hackers. En effet, les comptes peuvent être la cible d'attaques par pulvérisation de mots de passe, de credential stuffing et de phishing. Sans MFA, l'accès non autorisé aux comptes est simplifié et risque d'entraîner une fuite de données. La MFA n'est efficace que lorsqu'elle est activée et appliquée.

La plus grande fuite de données de 2024, qui a entraîné la **perte de 190 millions de dossiers médicaux,** a été attribuée à l'absence de MFA. Par conséquent, **les modifications proposées** à la loi HIPAA imposent actuellement la mise en œuvre de cette méthode.

NOUS AVONS TROUVÉ :

1 sur 7

entreprise sur sept n'utilise pas ou n'applique pas la MFA dans ses environnements SaaS et multicloud

1 800

utilisateurs ont des mots de passe qui n'expirent pas dans une entreprise moyenne

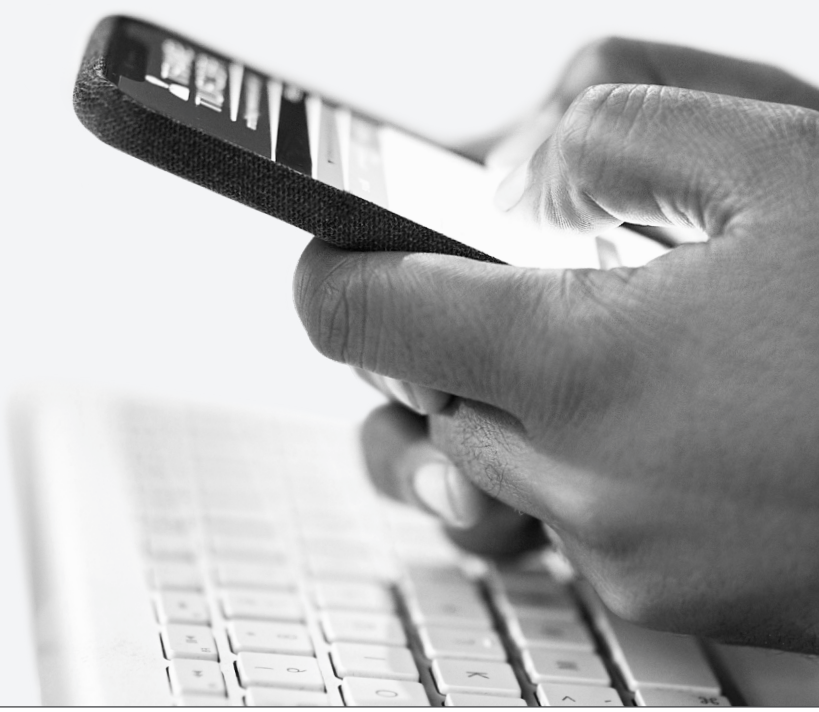
5

administrateurs globaux ont des mots de passe qui n'expirent jamais dans une entreprise moyenne

En l'absence de contrôles d'authentification adaptés, les attaquants se contentent de se connecter avec des identifiants volés et accèdent aux outils d'IA pour rapidement identifier vos données les plus précieuses.

La campagne qui a ciblé Snowflake en 2024 illustre parfaitement la raison pour laquelle toutes les entreprises devraient appliquer la MFA par défaut.

Les hackers **ont utilisé des identifiants volés** et ont exploité l'absence de MFA pour accéder à plusieurs environnements clients avant d'exposer leurs données sur le dark Web. Les enquêtes ont révélé qu'ils ont accédé aux comptes Snowflake via des identifiants compromis d'un sous-traitant tiers.



La MFA à elle seule n'est pas une solution miracle.

Varonis Threat Labs a révélé comment les cybercriminels peuvent contourner la MFA à l'aide de cookies de navigateur volés. En utilisant des extensions de navigateur malveillantes et des scripts d'automatisation personnalisés, ils peuvent extraire et réutiliser les cookies d'authentification pour se faire passer pour des utilisateurs. Ils n'ont pas besoin d'identifiants et sont tout aussi efficaces.

La preuve de concept **« Cookie Bite »** accorde un accès non autorisé aux applications M365 pour une reconnaissance et une augmentation de privilèges supplémentaires. La recherche montre que ces techniques s'appliquent également à de nombreuses autres plateformes et services cloud.

L'ÉTAT DE LA SÉCURITÉ DES DONNÉES

LA MENACE DE L'IA EST IMMINENTE

Ce n'est plus à démontrer : l'IA est une bombe à retardement de la stratégie de sécurité des données des entreprises.

L'IA présente de nouveaux risques pour les données. Par conséquent, les entreprises doivent s'empresser de sécuriser leurs informations critiques.

1. Réduisez votre rayon d'exposition.

Partez du principe que des fuites de données se produiront. Réduisez de manière proactive les dommages qu'un attaquant peut causer avec une seule identité volée. Essayez de réduire votre rayon d'exposition en surveillant continuellement les données et en remédiant aux problèmes, en verrouillant les autorisations et les accès pour empêcher les attaques basées sur l'identité, et en surveillant les Copilotes, les Chatbots et les Agents d'IA pour prévenir l'exploitation et l'utilisation abusive.

2. Dans la mesure où elles alimentent cette technologie, sécuriser les données revient à sécuriser l'IA.

Pour prévenir les risques et les fuites de données associés, surveillez en permanence vos données, automatisez la gouvernance des accès et la gestion de la posture, et utilisez la détection proactive des menaces. Une approche holistique de la sécurité des données garantit la sécurité de l'IA.

3. Utilisez l'IA à bon escient.

C'est un puissant outil de protection. Les équipes informatiques et de sécurité peuvent exploiter l'IA et l'automatisation comme suit :

- Identifiez, classifiez et ajoutez un label avec précision aux données sensibles dans de grands ensembles de données, en veillant à ce qu'aucune information critique ne soit exposée ou menacée
- Corrigez les vulnérabilités et faites office d'analyste SOC de première ligne
- Repérez les menaces internes et les comportements anormaux qui indiquent une attaque

VARONIS

SÉCURITÉ UNIFIÉE DES DONNÉES. RÉSULTATS AUTOMATISÉS.

COLLABOREZ AVEC LE LEADER DE LA SÉCURITÉ DES DONNÉES.

La Plateforme de sécurité des données de Varonis a été désignée **leader du secteur et plateforme préférée des clients** par un cabinet d'analyse de premier plan et a été élue choix des clients par Gartner® Peer Insights™ **et classée n° 1 des DSPM.**

Demandez votre évaluation gratuite des risques sur vos données.

Découvrez comment Varonis accélère vos progrès et atténue vos risques.

Accès à la plateforme Varonis

Bénéficiez gratuitement d'un accès complet à la plateforme Varonis de sécurité des données pendant toute la durée de votre évaluation.

Analyste de réponse aux incidents dédié

Nos experts surveilleront vos données pendant votre évaluation et vous contacteront s'ils observent quelque chose d'alarmant.

Rapport de résultats clés

Un résumé détaillé des risques liés à la sécurité de vos données que vous pouvez conserver, même si vous ne devenez pas client.

Obtenir votre évaluation