VARONIS

REMÉDIATION

ÉVALUATION DES RISQUES DES DONNÉES

Préparé pour Umbrella Corp

CONSTATS CRITIQUES

0 10 20 30 40 50 60 70

DATE DE CRÉATION : 07/08/2023

SOMMAIRE

TABLE DES MATIÈRES

« J'ai été impressionné de la rapidité avec laquelle Varonis a pu classifier les données et détecter les expositions potentielles des données pendant l'évaluation gratuite. Cela m'a vraiment ouvert les yeux. »

Michael Smith, DSI, HKS

POURQUOI UMBRELLA CORP A-T-ELLE LANCÉ UNE ÉVALUATION DES RISQUES LIÉS AUX DONNÉES AVEC VARONIS ?

Le conseil d'administration d'Umbrella Corp exige de pouvoir identifier, classifier et étiqueter/taguer toutes les données PII pour garantir la conformité de l'entreprise et l'efficacité de la DLP en aval. Le récent incident de ransomware vécu par Umbrella Corp met en évidence le besoin de surveiller les données. Sans action de sa part, Umbrella Corp s'expose à des amendes réglementaires et une exposition des données que la direction aimerait éviter.

Le Défi

Classifier les données sensibles et corriger les expositions est un vrai challenge.

Quantifier la posture de sécurité des données et transmettre la progression au conseil d'administration est indispensable.

La remédiation des données est difficile avec une petite équipe.

Il est nécessaire de surveiller l'utilisation des données et d'alerter sur les activités anormales.

Les sous-divisions fonctionnent indépendamment, il est donc nécessaire de mettre en place un programme unifié de sécurité des données.

Les audits de conformité sont manuels et incomplets.

PRÉSENTATION DE L'ÉVALUATION DES RISQUES D'UMBRELLA CORP

Sources de données connectées et chronologie de l'évaluation

Varonis peut se connecter à des dizaines de sources de données supplémentaires. La configuration prend quelques minutes.

Microsoft 365 | Active Directory + Azure AD | Salesforce | Partages de fichiers Windows | Google Workspace

Installation de la plateforme
1er juin 2023

Évaluation

Preuve de valeur
21 juin 2023

5,6 millions
ressources (fichiers/objets)

12 000
identités

805 000
événements (moyenne quotidienne)

2,4M
d'enregistrements sensibles classifiés (données de santé, de cartes bancaires ou secrets)

Remarque : seule une partie de l'environnement global de Umbrella Corp a été connectée pour la phase de POC.

CONSTATS CRITIQUES

Risques susceptibles d'entraîner une fuite de données

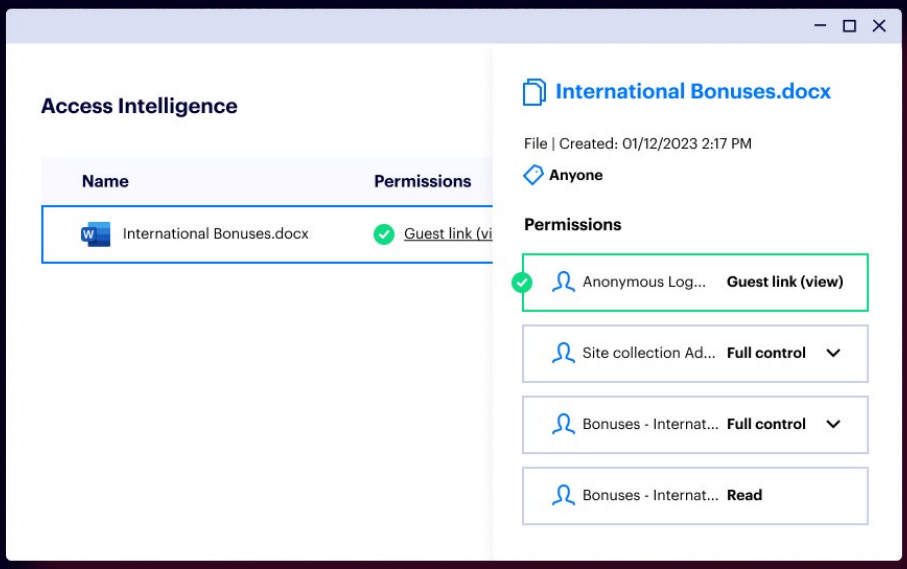
Voici les quatre principaux résultats que Varonis considère comme risques critiques pour la sécurité des données.

1. Rapports de salaires des RH partagés en public via des liens accessibles par « tout le monde »
2. 332 utilisateurs de Salesforce peuvent exporter des données sur la production.
3. Un utilisateur externe est un super administrateur dans Google Workspace.
4. Un assistant marketing a déclenché une alerte sur un accès anormal aux données.

Constat critique n° 1

Rapports de salaires des RH partagés en public via des liens accessibles par « tout le monde »

Melissa Donovan a accidentellement divulgué sur Internet les primes versées par l'entreprise.



Type de risque :
Exposition publique des données

Contrôle du NIST :
AC-3(9) : publication contrôlée

Système affecté :
Microsoft 365

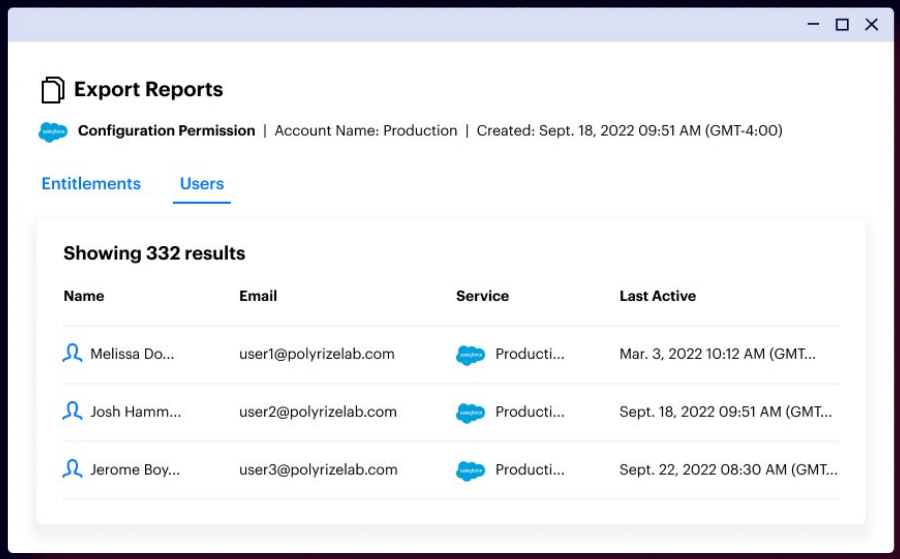
Observation :
le 12 janvier, Melissa Donovan, responsable des ressources humaines, a téléchargé International Bonsuses.docx sur le site Microsoft Teams de son équipe RH. L'analyse de classification de Varonis a identifié 231 instances de données à caractère personnel dans le fichier. En outre, nos logs indiquent qu'elle a créé le lien « Tout le monde » le 13 février, exposant ainsi le fichier sur Internet. Le lien a été consulté par des utilisateurs anonymes à partir de 27 adresses IP différentes dans le monde.

Recommandation :
révoquez immédiatement l'accès « Tout le monde » à ce fichier en désactivant le lien.
Désactivez la possibilité de partager publiquement.
Utilisez l'automatisation Varonis pour révoquer tout lien public vers des fichiers contenant des informations sensibles.

Constat critique n° 2

332 utilisateurs de Salesforce peuvent exporter des données sur la production.

Le profil « Ventes » standard accorde un droit d'exportation des fichiers. Cette autorisation est trop vaste et devrait être corrigée.



Type de risque :
Exposition des données sensibles

Contrôle NIST :
AC-2(7) : schémas basés sur les rôles

Système affecté :
Salesforce (production, sandbox, dev)

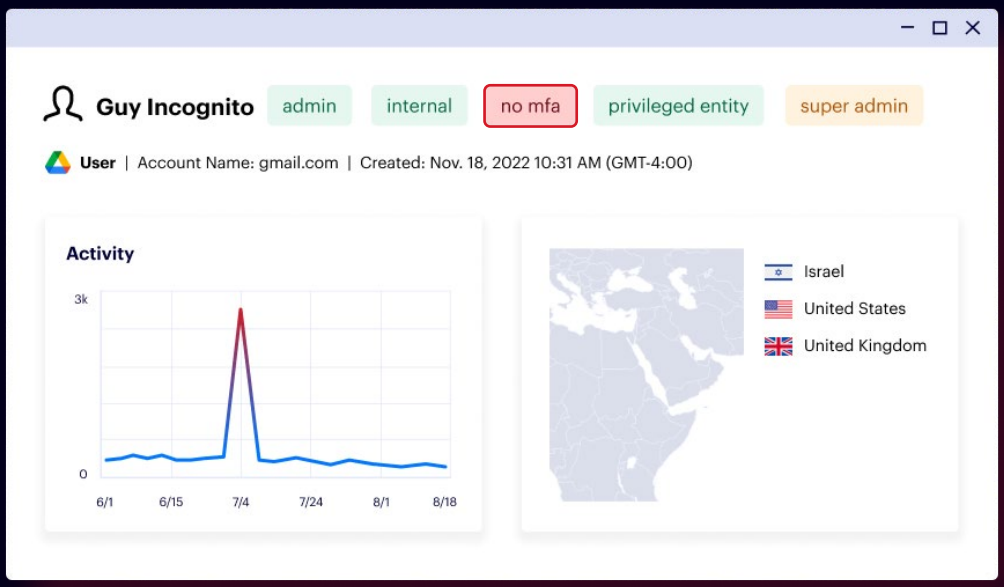
Observation :
Les analyses de Varonis ont permis d'identifier une combinaison toxique d'autorisations qui crée un risque élevé d'exfiltration de données : 332 commerciaux, via leur profil « Ventes », peuvent exporter toutes les données sur les prospects, les contacts, les opportunités et les comptes à partir de l'instance Salesforce de production d'Umbrella Corp.

Recommandation :
supprimez l'autorisation d'exportation des rapports du profil « Ventes » et de tout autre rôle non-administrateur. Passez en revue tous les profils et ensembles d'autorisations qui accordent des actions hautement privilégiées telles que l'exportation de rapports, la modification et la lecture de toutes les données.

Constat critique n°3

Un utilisateur externe est un super administrateur dans Google Workspace.

Guy Incognito est un super administrateur sans MFA. Son activité a fortement augmenté le 14 juillet, ce qui a déclenché une alerte.



Type de risque :
compte administrateur non sécurisé

Contrôle NIST :
AC-2(7) : comptes d'utilisateurs privilégiés

Système affecté :
Google Workspace

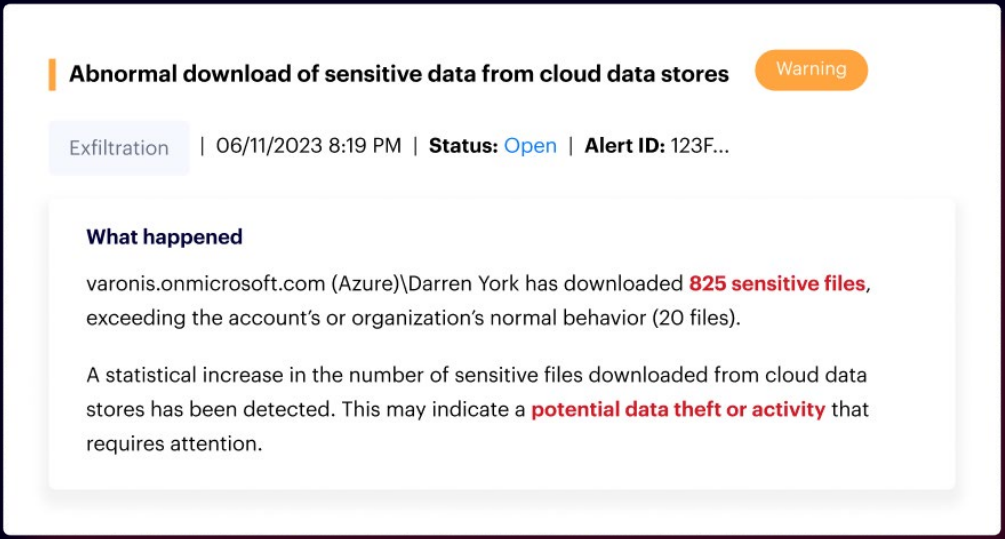
Observation :
Guy Incognito est un sous-traitant externe qui utilise un compte Gmail personnel pour accéder au compte Google Workspace d'Umbrella Corp. Cet utilisateur dispose de droits de super administrateur et n'a pas activé l'authentification multifacteur. Ce compte est considéré comme extrêmement risqué.

Recommandation :
Appliquez immédiatement l'authentification multifacteur sur le compte de Guy Incognito et ajoutez-le à une liste de surveillance dans Varonis. Passez en revue les 30 derniers jours d'activité de l'utilisateur, les droits d'administrateur et les identités associées. Déterminez si cet utilisateur externe a réellement besoin de droits de super administrateur.

Constat critique n° 4

Un assistant marketing a déclenché une alerte sur un accès anormal aux données.

Darren York ne devrait pas avoir accès aux données financières. Varonis UEBA a détecté un accès anormal.



Type de risque :
Comportement anormal des utilisateurs

Contrôle NIST :
AC-2(12) : surveillance des comptes pour une utilisation anormale

Système affecté :
Microsoft 365

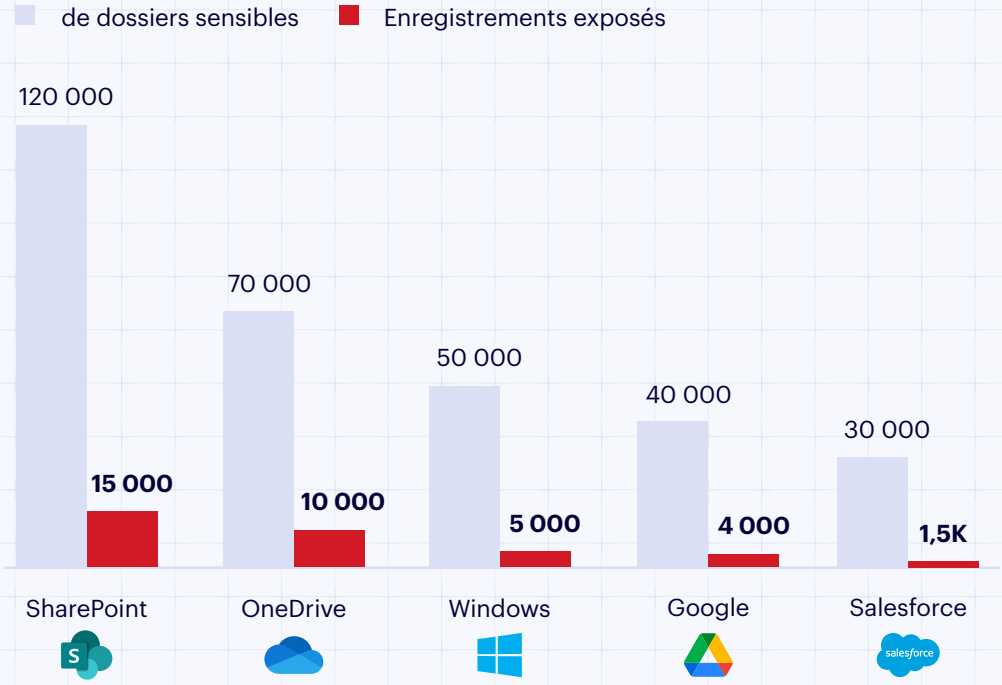
Observation :
Darren York, assistant marketing, a déclenché une alerte basée sur le comportement, car il a eu un comportement inhabituel au niveau de l'accès aux données. Varonis a détecté qu'il accédait à des fichiers contenant des données financières, ce qui est atypique pour son rôle.

Recommandation :
Utilisez Varonis pour lancer une requête afin de tout voir de l'activité de Darren au cours des 30 derniers jours. Assurez-vous que les autorisations relatives aux données contenant des dossiers financiers ne sont accessibles qu'aux employés qui en ont besoin.

POSTURE DE SÉCURITÉ DES DONNÉES

Les données sensibles d'Umbrella Corp sont réparties entre plusieurs services cloud et dépôts de données on-premise. Pour minimiser le risque de fuite de données, il est essentiel que l'entreprise dispose d'une visibilité et d'un contrôle en temps réel sur son patrimoine de données, qui évolue rapidement, avec une classification unifiée, la détection des menaces et l'application de politiques.

Où se trouvent les données les plus sensibles de Umbrella Corp et quel est leur degré de risque ?



Indicateurs de risques clés :

310 000 dossiers sensibles	**27 000** événements sur des données sensibles par jour
24 500 Enregistrements sensibles exposés à l'échelle de l'entreprise	**11 000** Enregistrements sensibles exposés en externe

Recherche et classification des données

Politiques de classification activées

Nous avons activé 85 règles intégrées et créé trois règles personnalisées lors de cette évaluation des risques. Les quatre principaux types de données en termes de volume sont présentés ci-dessous.

PCI-DSS

Conteneurs : 1 160
Objets : 12 421
Enregistrements : 89 924

Mots de passe :

Conteneurs : 160
Objets : 421
Enregistrements : 923

U.S. PII

Conteneurs : 2 620
Objets : 72 245
Enregistrements : 199 104

Numéros de dossiers

Conteneurs : 1 002
Objets : 92 420
Enregistrements : 799 922

Bibliothèque de politiques intégrée

PII	GDPR	Données d'identification	Financières	FÉDÉRAL
HIPAA PHI 2.0	RGPD Allemagne	Mots de passe :	PCI-DSS 2.0	ITAR
Colorado Privacy Act (CPA)	RGPD France	Clés privées	SOX	CONFIDENTIEL
NY SHIELD Act	RGPD Autriche	Certificats	GLBA	CUI

Plus des centaines de règles, modèles et dictionnaires supplémentaires

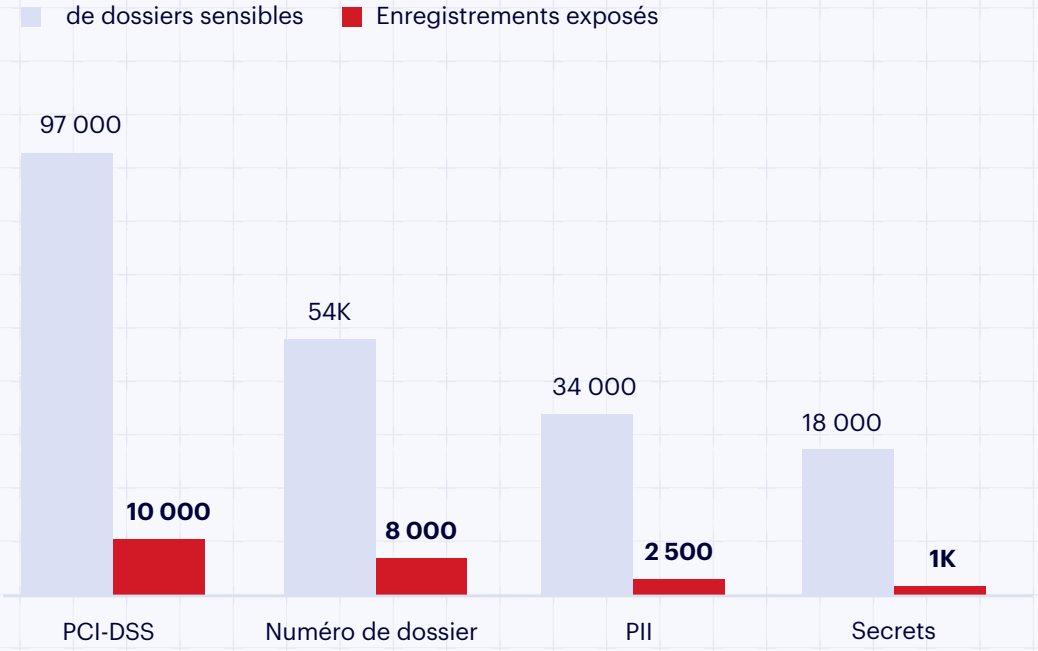
La puissance de la classification des données Varonis

- Véritable analyse incrémentielle pour une détection efficace et évolutive sur des ensembles de données volumineux
- Unification des politiques de classification pour tous les dépôts de données pris en charge
- Testé dans des environnements de plusieurs pétaoctets
- Plus de 400 règles conçues et testées par des experts disponibles et prêtes à l'emploi (et ce chiffre ne fait qu'augmenter)
- Portée et échantillonnage de l'analyse personnalisables

Exposition des données dans Microsoft 365

L'exposition des données dans M365 n'est pas propre à Umbrella Corp. En moyenne, une entreprise lambda dispose de plus de 40 millions d'autorisations uniques sur ses données multicloud et, selon Microsoft, plus de la moitié des autorisations présentent un risque élevé et peuvent causer des dommages catastrophiques en cas de mauvaise configuration.

Quels types de données réside dans M365 et quelle est l'exposition d'Umbrella Corp ?



Indicateurs de risques clés :

203K
dossiers sensibles

20K
Enregistrements sensibles exposés à l'échelle de l'entreprise

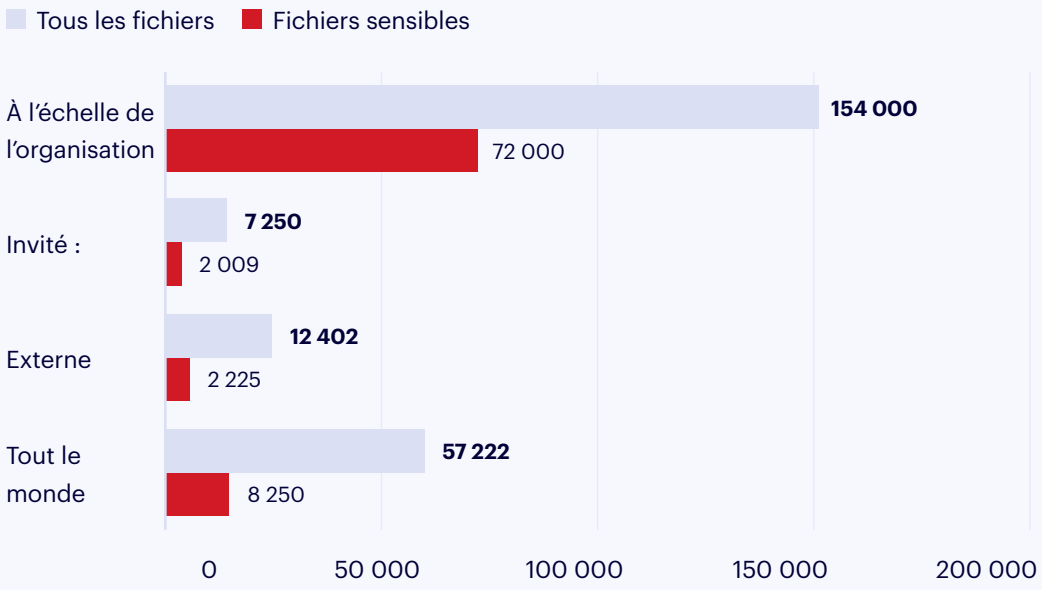
1,5K
Enregistrements sensibles exposés en externe

Risque de la collaboration

Niveaux d'exposition

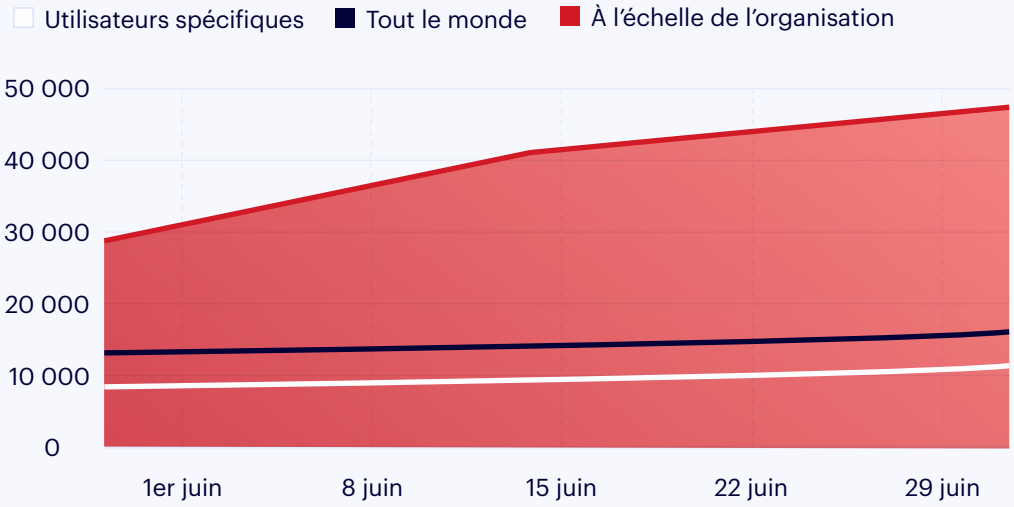
Partager des liens facilite la collaboration, mais ce processus peut exposer ces données à tous les membres de l'entreprise, aux utilisateurs invités ou à Internet. Umbrella Corp comporte un volume substantiel de données sensibles exposées en raison des liens dans SharePoint et OneDrive.

SharePoint Online et OneDrive



Croissance des liens partagés

Le rayon d'action d'Umbrella Corp augmente rapidement de semaine en semaine. Vous trouverez ci-dessous un graphique de la croissance des liens, par type, au cours de la période d'évaluation des risques.



Données exposées publiquement

Données exposées publiquement via des liens accessibles à « Tout le monde »

Vous trouverez ci-dessous un petit échantillon de fichiers sensibles accessibles à tous sur Internet. La piste d'audit Varonis indique le type de données dans le fichier (PCI, PHI, etc.), qui a partagé le lien, quand et si le fichier a été consulté via le lien.

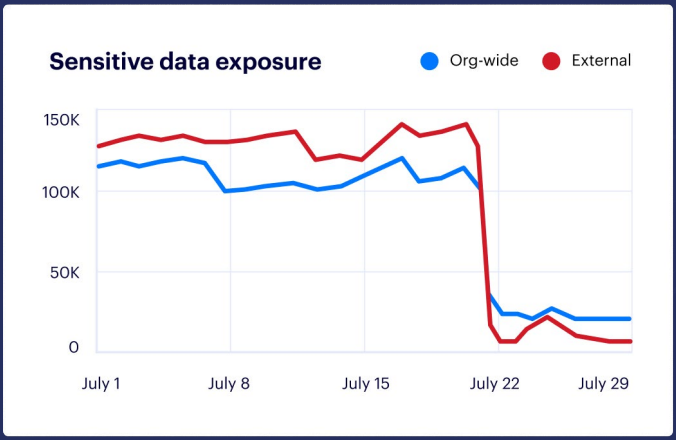
	File type	Name (resource)	Classification category	Total record
1		JV costs for Feb-Apr.xls	*Credentials (6)	28
		JV costs for Feb-Apr.xls	*Credentials (4)	22
		Transaction-English-06.xsl	*Credentials (4)	22
		GL Entry.ppt	*Credentials (4)	22
2		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx	*Financial (3)	21

1 Tableurs contenant des identifiants et informations de cartes bancaires

2 Contrats de travail contenant des données personnelles et des coordonnées bancaires

En combien de temps pouvons-nous remédier aux risques liés aux liens partagés ?

Un client standard de Varonis peut éliminer rapidement son exposition aux risques grâce à l'automatisation. Vous trouverez ci-dessous les résultats d'une grande institution financière qui a activé l'automatisation du principe de moindre privilège. Près de 100 % de l'exposition aux données externes et à l'échelle de l'entreprise a été éliminée en moins de 30 jours.



Les politiques d'automatisation maintiennent les risques à un faible niveau face à la croissance des données et à la collaboration continue. Grâce à la mise en œuvre automatique des politiques, les nouveaux risques sont éliminés dès leur apparition et le principe du moindre privilège est appliqué en permanence.

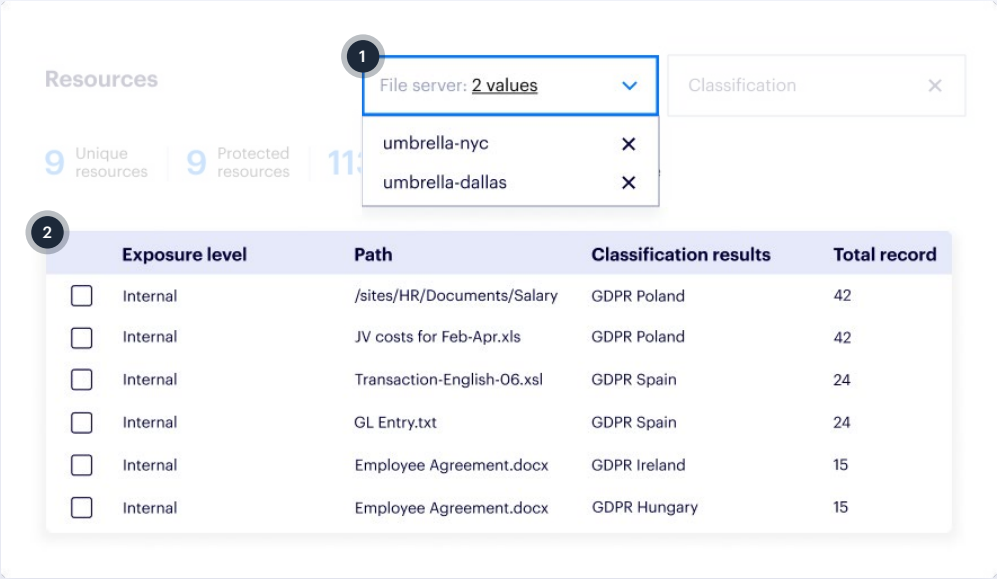
Données égarées et mal étiquetées

Données égarées : risque de non-conformité au RGPD

Varonis a détecté des enregistrements de données à caractère personnel de citoyens de l'UE dans un tenant M365 hébergé aux États-Unis. Les fichiers ont été téléchargés le 15 juillet par un compte de service nommé « ExportJob » qui semble être connecté à une tâche automatisée de Workato. Nous vous recommandons de migrer ces données vers le tenant d'Umbrella Corp basé dans l'UE et de modifier la tâche automatisée.

1 Tenants M365, basés aux États-Unis

2 Fichiers contenant des PII de citoyens de l'UE



Exposure level	Path	Classification results	Total record
Internal	/sites/HR/Documents/Salary	GDPR Poland	42
Internal	JV costs for Feb-Apr.xls	GDPR Poland	42
Internal	Transaction-English-06.xsl	GDPR Spain	24
Internal	GL Entry.txt	GDPR Spain	24
Internal	Employee Agreement.docx	GDPR Ireland	15
Internal	Employee Agreement.docx	GDPR Hungary	15

Fichiers mal étiquetés : écart d'application de la DLP

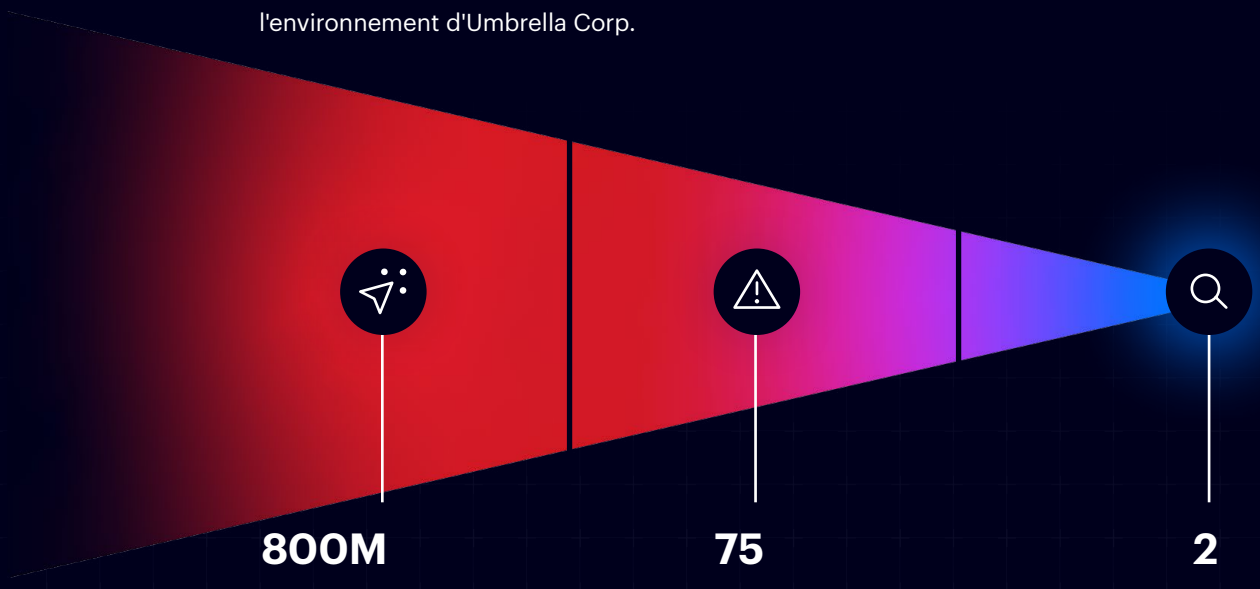
De nombreux fichiers ne contiennent pas d'étiquettes MIP ou ont des étiquettes obsolètes et incorrectes. Par conséquent, l'application du DLP en aval peut échouer, entraînant une fuite de données sensibles ou inversement, les utilisateurs ne peuvent pas partager des données non sensibles mal étiquetées.

Nous avons trouvé plus de 27 000 fichiers sensibles sans étiquette.

Path	Classification results	Classification labels	Name
C:\Share\Finance	US PII, HIPAA PHI Data	GDPR Regulated Data (0/1)	Finance
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Controllers
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Q1 2006
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Inventory
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Revenues
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		SEC

Détection des menaces et réponse

La surveillance en temps réel et la détection des menaces basée sur le comportement de Varonis ont été activées sur chaque système concerné. Au cours de la période d'évaluation, nos modèles d'IA ont été entraînés sur plus de 800 millions d'événements afin de connaître le comportement unique des utilisateurs et des appareils dans l'environnement d'Umbrella Corp.



800M

Des centaines de millions d'événements recueillis

Chaque événement est automatiquement enrichi et normalisé.

75

Des dizaines d'alertes déclenchées

En moyenne ~3 par jour

2

Quelques incidents ayant fait l'objet d'une enquête

L'IR de Varonis a repéré et fait remonter deux incidents.

UEBA centrée sur les données

Les événements sont enrichis par les données, l'utilisateur et l'appareil. Les analystes de sécurité peuvent lancer des requêtes telles que « Répertorier tous les événements d'accès aux données sensibles par des comptes privilégiés à partir d'appareils connectés depuis l'Allemagne ».

Identification du compte

Résolution de l'adresse IP à l'appareil

Opération par	Type de compte	Objet	Sensible ?	Adresse IP de l'appareil	Nom de l'appareil	Adresse IP externe	Géolocalisation
Amy Johnson	Exécutif	Client.xlsx	Oui	173.17.33.3	aj-03154	54.239.13.2	Canada

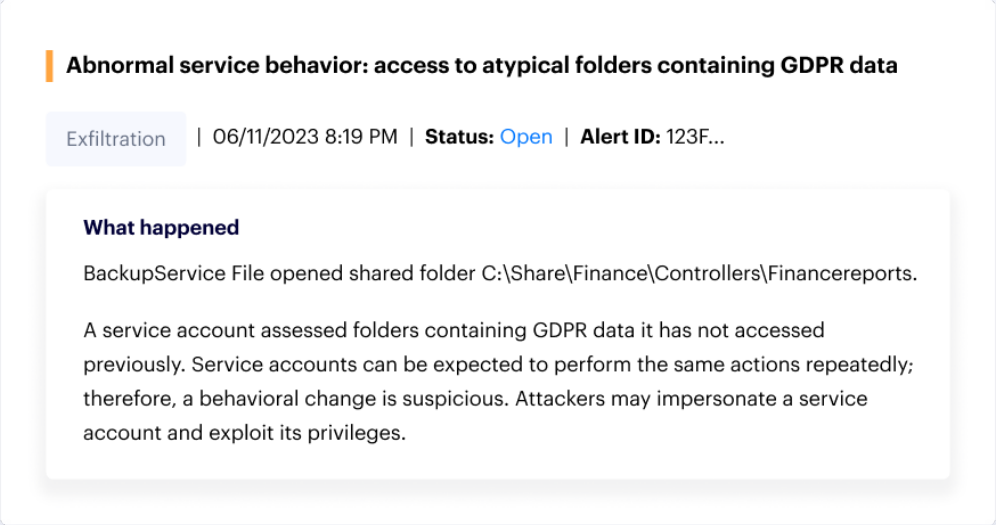
Sensibilité des fichiers

Géolocalisation

ANALYSE DES MENACES

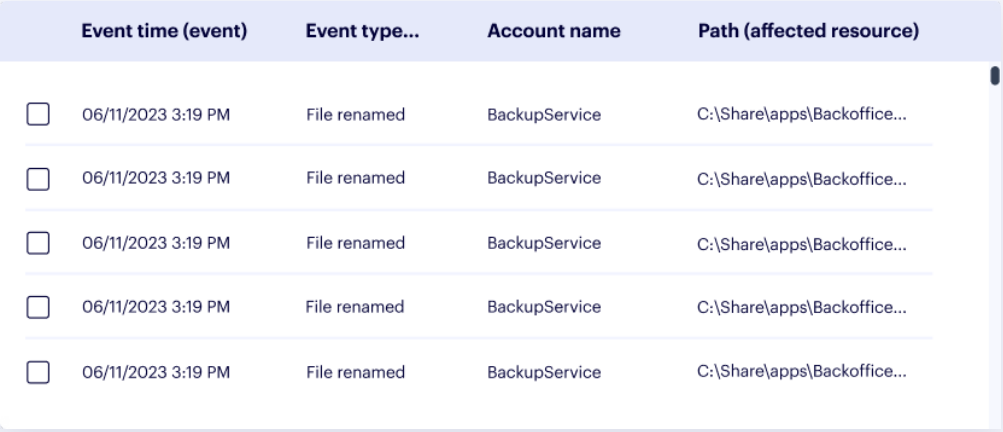
Rapport d'incident : compte de service compromis

Observation :
L'équipe de réponse aux incidents de Varonis a découvert qu'un compte de service de sauvegarde était compromis et a commencé à accéder aux données des utilisateurs.



Mesures d'atténuation :
L'IR Team de Varonis a trié et corrigé l'incident en quelques minutes. Le compte UC\BackupService a été immédiatement désactivé, les sessions actives ont été arrêtées et le mot de passe a été réinitialisé. Varonis a fourni un rapport d'enquête complet à l'équipe d'Umbrella Corp, avec analyse des causes premières et recommandations.

Analyse :
Le compte compromis a accédé à 142 fichiers. 82 étaient classés comme sensibles par Varonis.



Event time (event)	Event type...	Account name	Path (affected resource)
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...

RISQUE DE CONFIGURATION

Varonis analyse en permanence les configurations des systèmes des plateformes SaaS et IaaS d'Umbrella Corp afin de déterminer si certains paramètres présentent des risques ou si des configurations ne sont pas conformes à l'état souhaité.

21 erreurs de configuration découvertes

Salesforce a le plus d'erreurs de configurations (8).

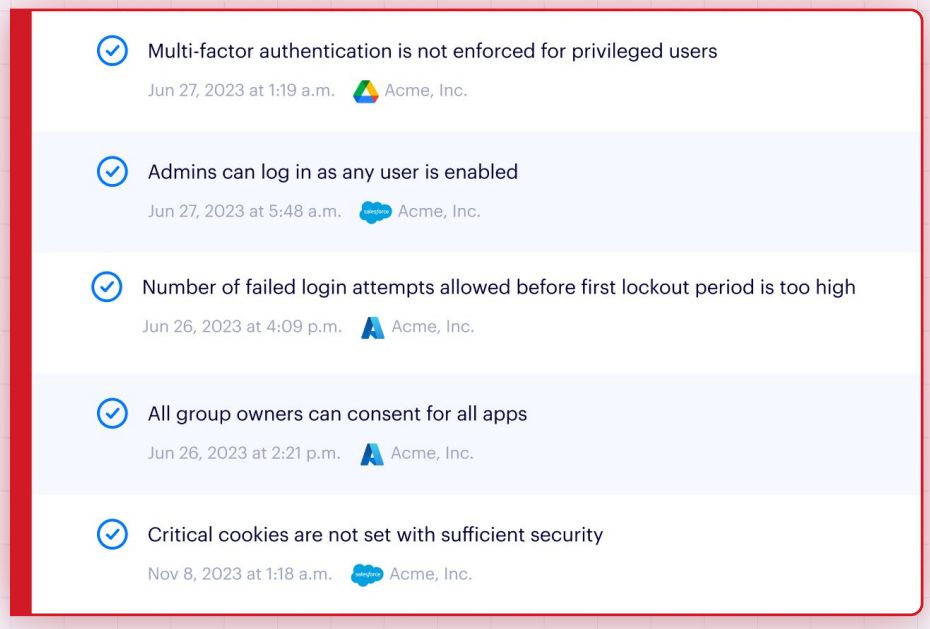
5 graves erreurs de configuration

M365 et Salesforce ont chacun 2 erreurs critiques de configuration.

4 ensembles de configurations à appliquer automatiquement

Varonis peut automatiquement appliquer des paramètres sécurisés.

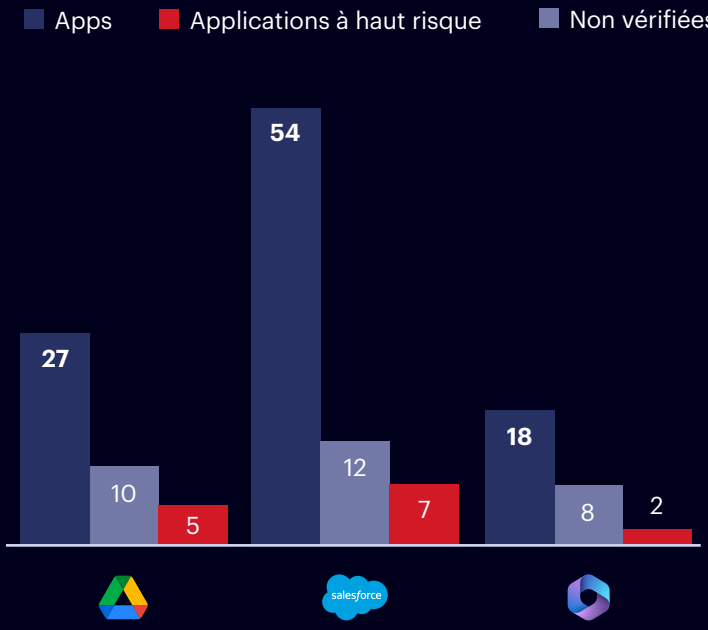
Vous trouverez ci-dessous un résumé des **cinq erreurs de configuration les plus graves** identifiées lors de l'évaluation. Vous trouverez toutes les informations et recommandations qui s'y rapportent dans l'interface utilisateur de Varonis.



Cliquez ici pour découvrir d'autres exemples de configurations SaaS et IaaS que Varonis peut surveiller.

RISQUE LIÉ AUX APPLICATIONS TIERCES

Nous avons identifié 36 applications tierces à risque, inactives ou non vérifiées.



99
Applications tierces installées

14
à haut risque avec un large accès aux données

22
Applications inactives

Voici le détail des quatre principales applications tierces, par nombre d'utilisateurs, intégrées aux plateformes SaaS surveillées par Varonis :

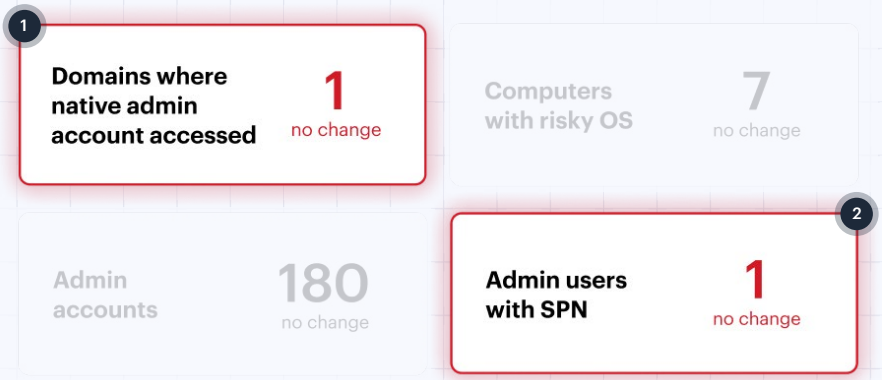
Google	Salesforce	Microsoft 365
miro	6sense	
dialpad	HubSpot	slack
Signeasy	INCENT	Trello
SUPERMETRICS	Power BI	Evernote

En outre, nous avons découvert 111 utilisateurs inactifs dont les affectations d'applications peuvent être révoquées dans l'interface utilisateur Varonis.

RISQUE LIÉ À L'IDENTITÉ

Posture de sécurité d'Active Directory

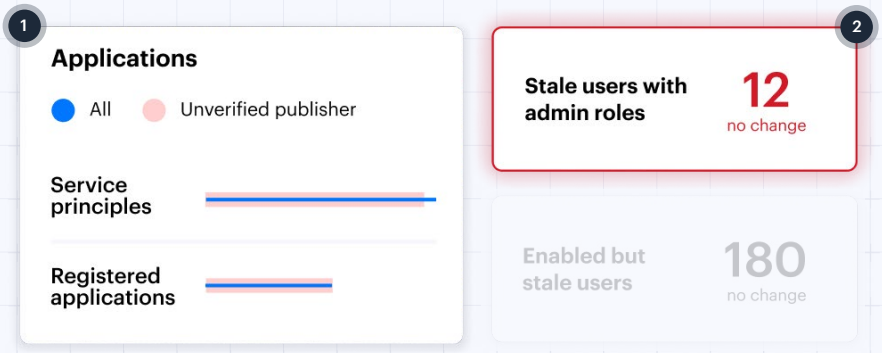
Varonis analyse les directory services cloud et on-premise d'Umbrella Corp et détecte des configurations faibles qui peuvent fournir des voies d'accès aux attaquants. Ces risques sont mis à jour en temps réel sur vos tableaux de bord Varonis et vous permettent de prioriser les actions de renforcement d'AD.



1. Il est rare que ce compte soit utilisé dans des circonstances normales. Cela peut signaler un piratage.
2. Vulnérabilité au piratage de mots de passe hors-ligne

Posture de sécurité d'Entra ID (Azure AD)

Varonis surveille et évalue en permanence la posture d'Entra ID. Les erreurs de configuration qui exposent vos données apparaissent dans vos tableaux de bord et rapports de risque.

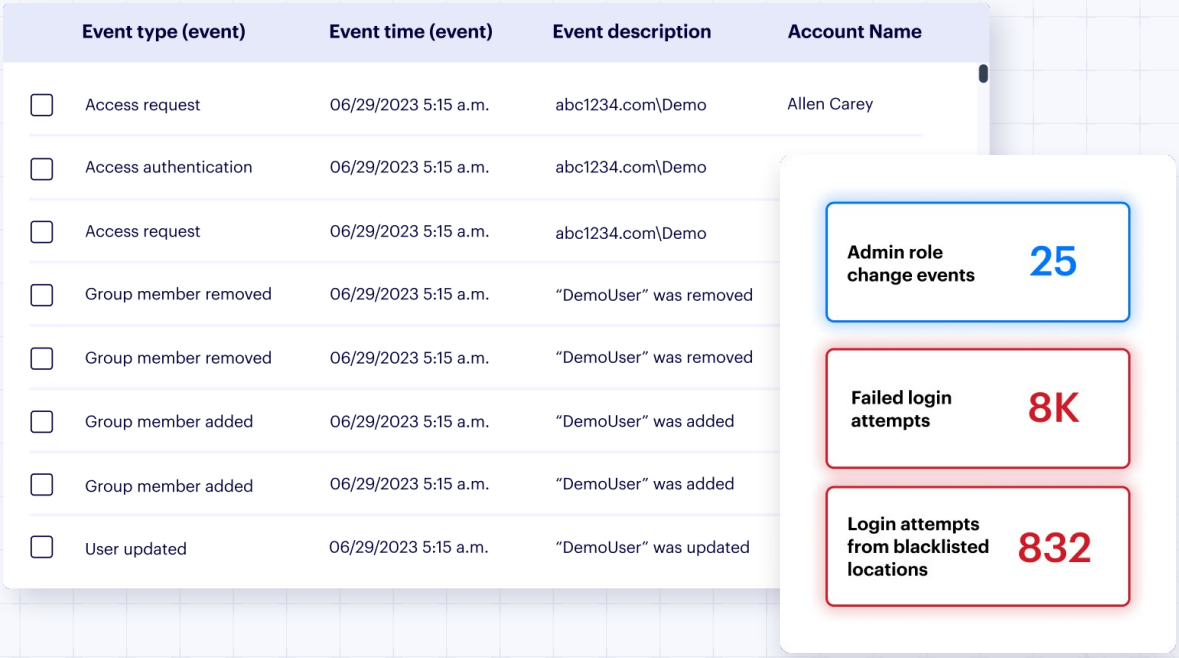


1. Vérifiez les autorisations et l'accès aux données des applications non vérifiées.
2. Ces comptes doivent être désactivés immédiatement.

Surveillance d'Active Directory

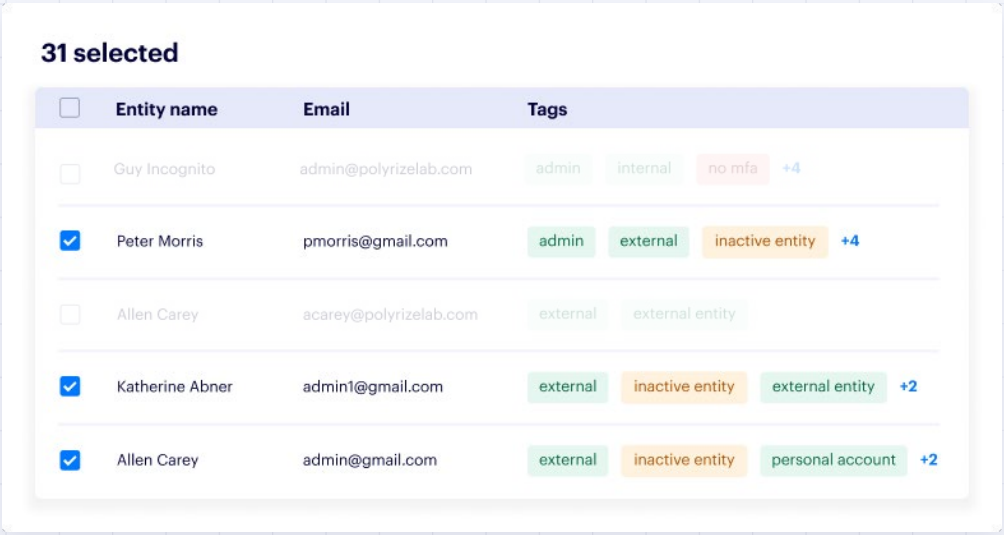
Varonis surveille les événements dans les directory services d'Umbrella Corp et établit une corrélation entre ces actions et les événements centrés sur les données collectées à partir des plateformes de collaboration et des dépôts de données.

Ces modifications ont été effectuées en dehors de la fenêtre de contrôle des modifications.



Event type (event)	Event time (event)	Event description	Account Name
Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	Allen Carey
Access authentication	06/29/2023 5:15 a.m.	abc1234.com\Demo	
Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	
Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
User updated	06/29/2023 5:15 a.m.	"DemoUser" was updated	

Utilisateurs externes risqués et comptes personnels



Les comptes utilisateur Gmail sont obsolètes mais ont accès à des données sensibles.

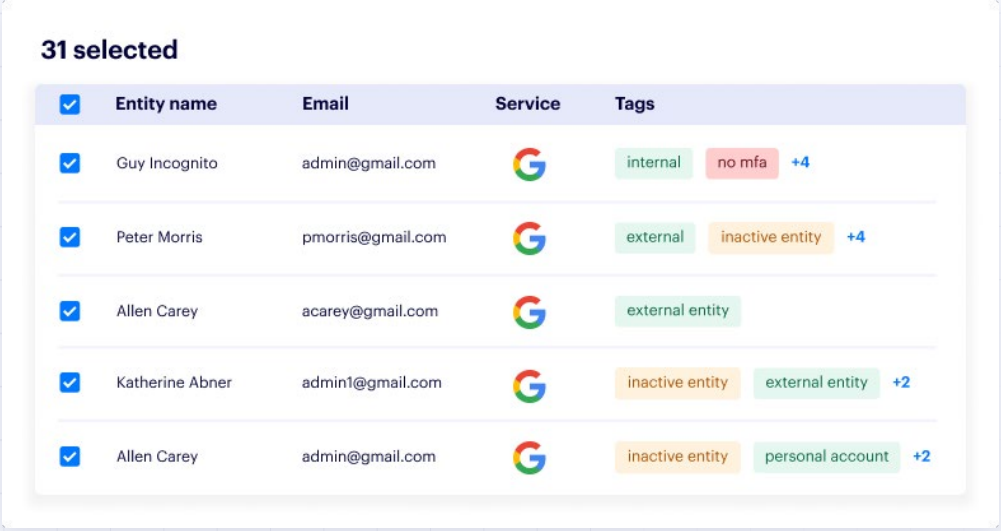
Cartographie des identités associées

Varonis identifie automatiquement les comptes associés à l'aide d'un algorithme exclusif. Guy Incognito est administrateur de Google Workspace et utilise un compte Gmail personnel sans authentification multifacteur. Il possède plusieurs identités dans l'environnement de Umbrella Corp.

Guy a plusieurs pseudos - un mélange de comptes professionnels et de comptes personnels.

Lacunes de départ : comptes inactifs

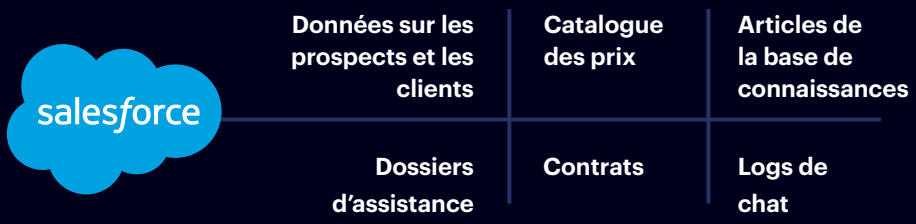
Varonis a identifié plus de 3 000 identités obsolètes dans les directory services d'Umbrella Corp et les référentiels de comptes locaux.



Sous-traitants en fin de contrat qui ont toujours accès à partir de leur compte Google personnel.

RISQUE DANS SALESFORCE

Salesforce héberge les données les plus précieuses d'une entreprise, mais ses structures d'autorisation complexes et son manque de visibilité sur les personnes autorisées à accéder à ces données l'exposent aux menaces internes et aux cybermenaces.



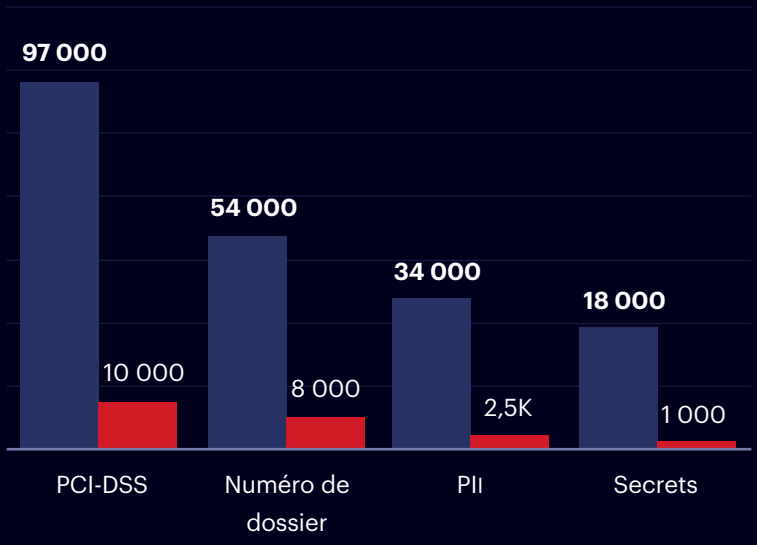
Portée de l'évaluation

Environnements	• Production • Sandbox	• Dév.
Data	• 234 240 enregistrements • 8 241 documents • 520 champs • 9 214 ressources sensibles	• 203 dossiers externes et partagés en public • 22 applications tierces surveillées
identités	• 2 012 utilisateurs internes • 425 utilisateurs externes • 124 sous-traitants	• 212 utilisateurs invités • 55 super administrateurs
Droits	• 89 profils • 52 profils privilégiés • 22 profils de communauté • 3 profils d'invités	• 55 ensembles d'autorisations • 27 groupes d'ensembles d'autorisations • 33 rôles
Les trois principaux domaines externes	gmail.com	hotmail.com Proton Mail protonmail.com

EXPOSITION DES DONNÉES DE SALESFORCE

SALESFORCE

Quel type de données réside dans Salesforce et quelle est l'exposition ?



203K
Objets avec au moins un enregistrement sensible

1,5K
Enregistrements sensibles exposés en externe

20K
Enregistrements sensibles exposés à l'échelle de l'entreprise

Risque d'exfiltration des données d'Umbrella Corp

Les droits indiqués ci-dessous doivent être considérés comme hautement privilégiés. S'ils sont accordés à un trop grand nombre d'utilisateurs, ils peuvent engendrer un risque élevé d'exposition et d'exfiltration des données.

235 droits avec l'option « Exporter des rapports » activée

L'option Exporter des rapports permet aux utilisateurs d'exporter des données directement à partir de Salesforce. Si nécessaire, cette autorisation devrait être appliquée aux ensembles d'autorisations.

124 droits avec l'option Afficher toutes les données ou Modifier toutes les données activée

Les utilisateurs disposant de cette autorisation peuvent consulter et modifier toutes les données au sein de l'entreprise.

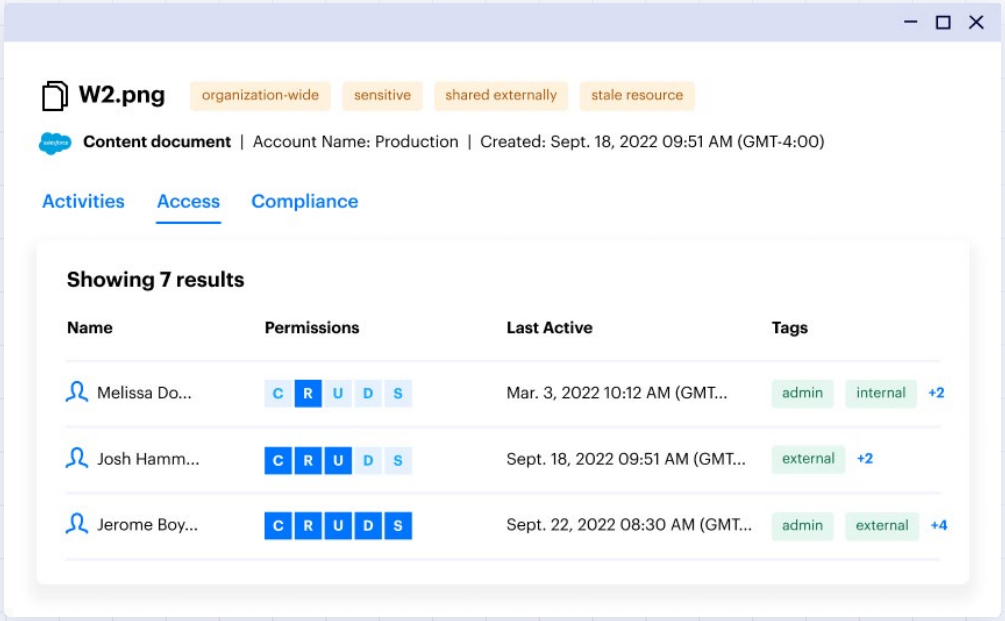
52 droits avec l'API activée

Permet aux utilisateurs de communiquer avec toutes les API Salesforce, d'exfiltrer des données ou d'effectuer d'autres actions.

Varonis fournit à Umbrella Corp une vue en temps réel des droits critiques et la possibilité de paramétrer rapidement les droits d'accès et d'appliquer le principe du moindre privilège. Nous vous recommandons également de configurer des alertes Varonis qui se déclenchent lorsque ces droits privilégiés changent.

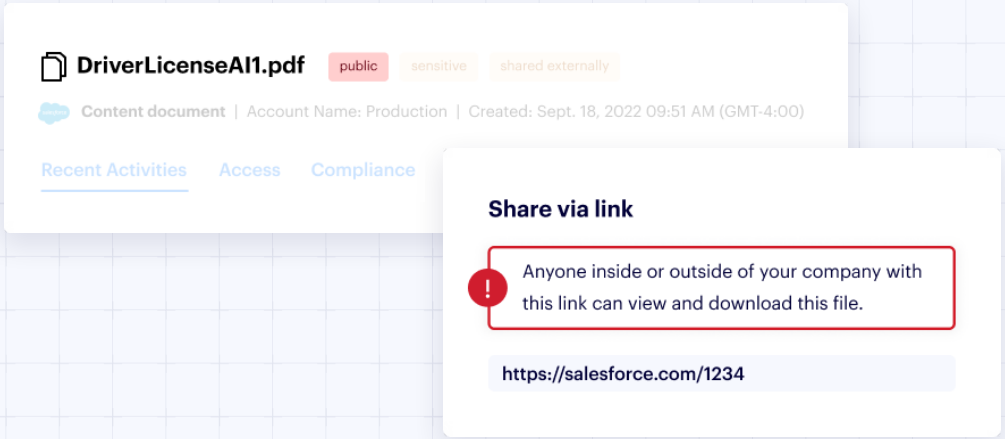
DONNÉES SENSIBLES PARTAGÉES EN EXTERNE

Les instances Salesforce d'Umbrella Corp autorisent l'accès des utilisateurs invités. Il existe également plusieurs comptes utilisateur qui agissent en tant que comptes de service pour des applications tierces. Varonis a détecté plus de 1 500 enregistrements sensibles exposés en externe, tels que la pièce jointe W2 ci-dessous.



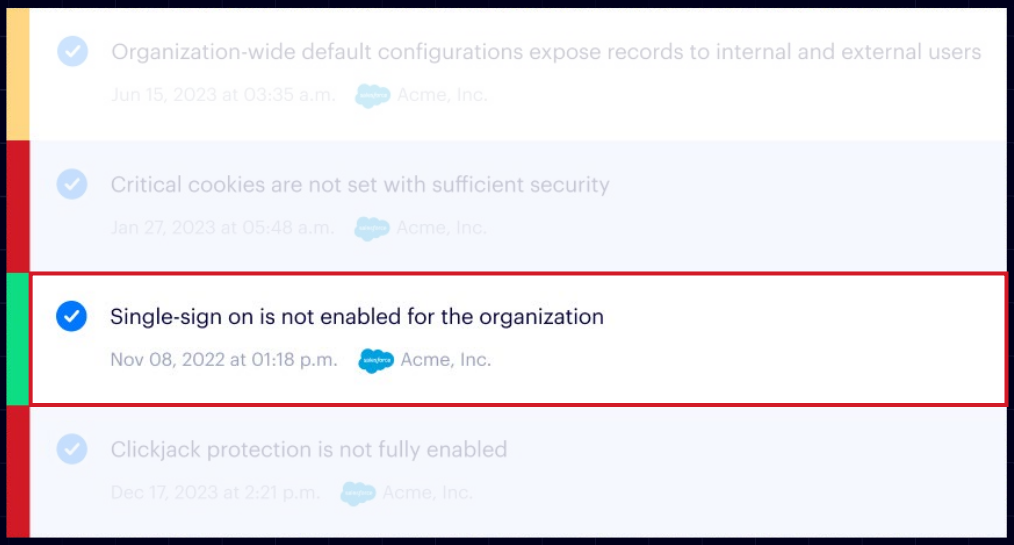
Les utilisateurs externes à l'entreprise peuvent accéder, mettre à jour ou supprimer les données PCI et PII dans votre instance Salesforce.

Outre l'exposition des données aux utilisateurs invités, aux sous-traitants et à d'autres tiers authentifiés, notre évaluation a également mis en évidence des données exposées sur Internet via des liens publics.



ERREURS DE CONFIGURATION SALESFORCE

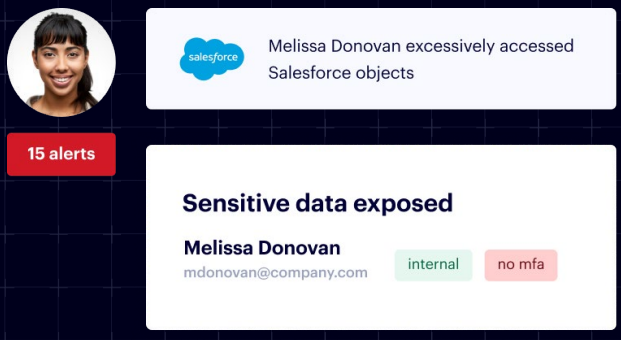
Varonis a détecté et corrigé quatre erreurs de configuration ou un problème de sécurité des valeurs par défaut à l'échelle de l'entreprise qui pourraient fournir un chemin d'attaque.



Les sous-traitants qui ne travaillent plus pour l'entreprise pouvaient accéder au compte sandbox alors que les comptes Okta avaient été supprimés.

Salesforce alerts

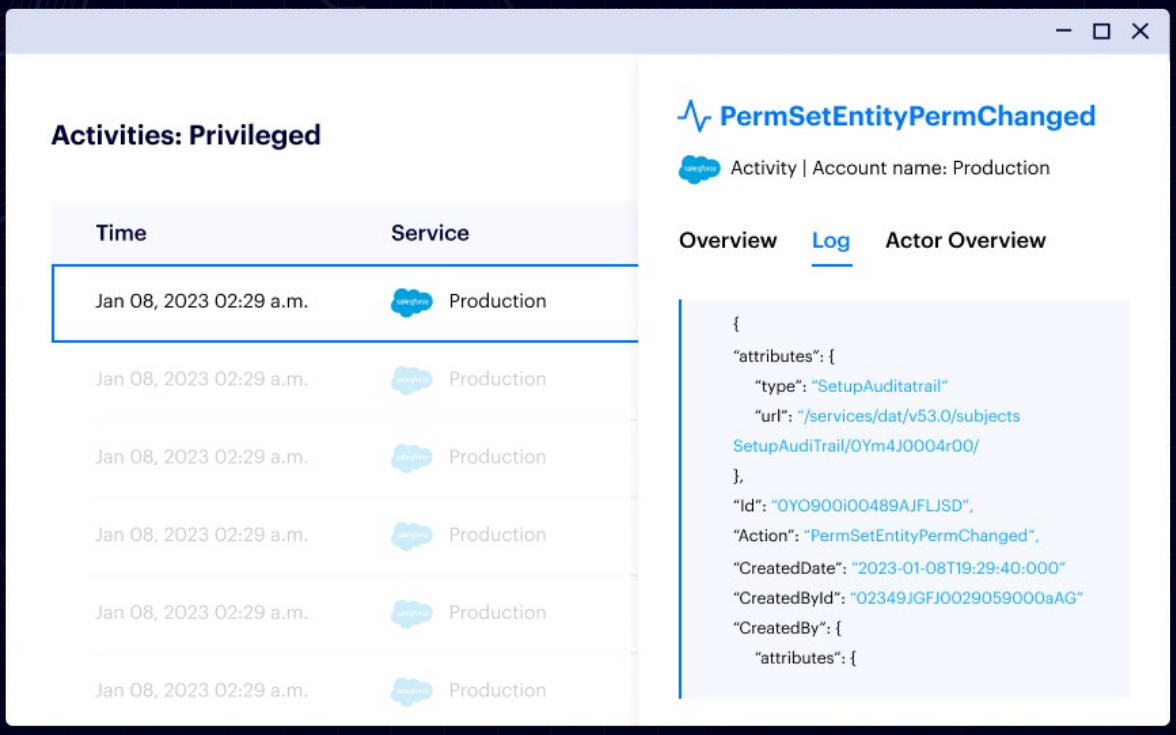
15 alertes ont été déclenchées et résolues par l'équipe de réponse aux incidents de Varonis, y compris un cas où la collaboratrice Melissa Donovan accédait à un nombre anormal d'enregistrements par rapport à d'habitude. Notre enquête a révélé que Melissa avait installé une extension de navigateur qui accédait rapidement aux URL des enregistrements Salesforce.



Melissa Donovan a eu un comportement inhabituel en accédant à des dossiers qu'elle n'a pas l'habitude de consulter.

Surveillance des modifications des admin

Josh Hammond a fait plusieurs modifications d'admin à l'environnement de production en dehors de la fenêtre de contrôle des modifications. Vous trouverez ci-dessous le journal détaillé des modifications.

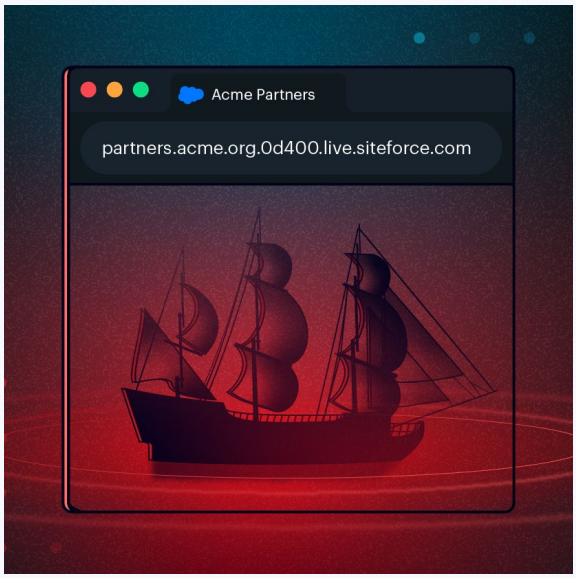


VARONIS
THREAT LABS

RECHERCHE SALESFORCE

Notre équipe recherche et divulgue les vulnérabilités et les configurations toxiques dans Salesforce.

Sites fantômes : vol de données provenant de communautés Commerce désactivées



Einstein's Wormhole : le bug qui permet de récupérer les informations des calendriers Outlook et Google à l'aide des utilisateurs invités de Salesforce

À propos du Varonis Threat Labs

Notre équipe de chercheurs en sécurité et de spécialistes des données compte parmi les meilleurs experts au monde en matière de cybersécurité. Forte de plusieurs décennies d'expérience dans les secteurs de l'armée, du renseignement et des entreprises, la Varonis Threat Lab recherche de manière préventive les vulnérabilités des applications que nos clients utilisent afin de trouver et de combler les lacunes avant qu'un attaquant ne les détecte. Toutes ces connaissances sont programmées dans notre plateforme pour vous aider à garder une longueur d'avance sur les hackers.

Consultez les dernières recherches : **www.varonis.com/blog/tag/threat-research**

RÉDUISEZ LES RISQUES SANS EN PRENDRE AUCUN.

Notre évaluation gratuite des risques ne prend que quelques minutes et apporte une valeur immédiate. En moins de 24 heures, vous disposerez d'une vue claire et basée sur les risques des données les plus importantes et d'un parcours clair vers la remédiation automatisée.

Accès complet à la plateforme Varonis SaaS

Bénéficiez d'un accès complet à notre plateforme de sécurité des données pendant toute la durée de votre évaluation et obtenez des informations exploitables sur vos données les plus critiques.

Analyste de réponse aux incidents dédié

Le fait d'être connecté à la plateforme de sécurité des données SaaS de Varonis signifie que nos experts surveillent vos alertes et vous contacteront s'ils détectent une activité anormale.

Rapport sur les résultats clés

Un résumé détaillé des risques liés à la sécurité de vos données et une présentation examinant les conclusions et les recommandations. Vous pouvez conserver ce rapport, même si vous ne devenez pas client.

Obtenez votre évaluation gratuite

Approuvé par des milliers de clients

ING · L'ORÉAL · NASA · BlueCross BlueShield · Nasdaq · Coca-Cola · TOYOTA · U.S.ARMY · Penguin Random House · E*TRADE

LEADER DE L'ENQUÊTE FORRESTER

Varonis nommé leader des plateformes de sécurité des données

« Varonis est la solution idéale pour les entreprises qui cherchent à visualiser précisément leurs données, exploiter les fonctionnalités de classification et bénéficier d'une remédiation automatisée pour l'accès aux données ».

Forrester Wave™ : Plateformes de sécurité des données, 1er trimestre 2023

LEADER SELON FORRESTER

0 10 20 30 40 50 60 70

VARONIS