VARONIS

ANALYSE DE SÉCURITÉ DE MICROSOFT 365 COPILOT

GARANTIR LA SÉCURITÉ DE COPILOT AVANT, PENDANT ET APRÈS LE DÉPLOIEMENT

VARONIS + Microsoft

Nasdaq Market Activity News + Insights Solutions About Nasdaq+

Varonis Accelerates Secure Adoption of Microsoft Copilot for Microsoft 365

PUBLISHED
JAN 23, 2024 9:00AM EST

Integration lays the foundation for secure and compliant deployment of Microsoft Copilot for Microsoft 365

NEW YORK, Jan. 23, 2024 (GLOBE NEWSWIRE) -- Varonis Systems, Inc. (Nasdaq: VRNS), a leader in data security, today announced a strategic collaboration with Microsoft to help companies safely harness the power of AI. The integration helps joint customers continually assess and improve their Microsoft 365 data security posture before, during, and after they deploy Microsoft Copilot for Microsoft 365.

« L'intégration de Varonis fournit aux clients les contrôles de sécurité et de conformité supplémentaires nécessaires pour adopter rapidement et en toute confiance Microsoft Copilot pour M365. »

ANAT GIL

Responsable des partenaires,
Microsoft Europe

PRÉPARATION POUR COPILOT EN 10 JOURS

Varonis a réduit l'exposition à Copilot de 99,8 % en 10 jours pour une entreprise financière.
Aucun impact sur l'entreprise grâce à 20 politiques d'automatisation pour verrouiller environ un million de fichiers.

992 000 Fichiers

Point de départ

Environ un million de fichiers de l'entreprise sur SharePoint, Teams et OneDrive. Varonis a rapidement classifié 120 000 fichiers sensibles.

57 000 fichiers exposés

Identifiez les risques liés à Copilot

A utilisé Varonis pour identifier les informations médicales protégées (PHI), les données à caractère personnel (PII) et les informations d'identification susceptibles d'être exposées via Copilot.

99,8 % de réduction du rayon d'exposition

Différence de 10 jours

A éliminé automatiquement environ 2 000 liens de partage et a adapté l'accès à 57 000 fichiers grâce aux politiques de Varonis

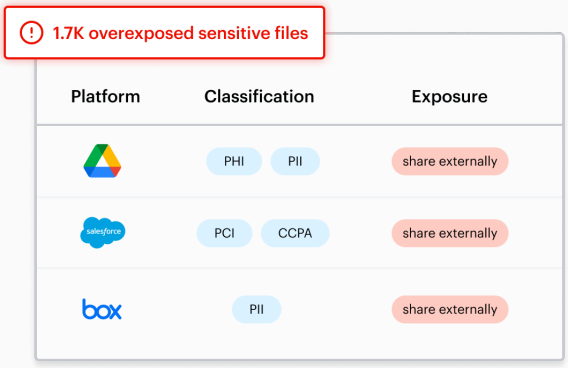
0 ticket relatif à des plaintes

Zéro impact sur le client

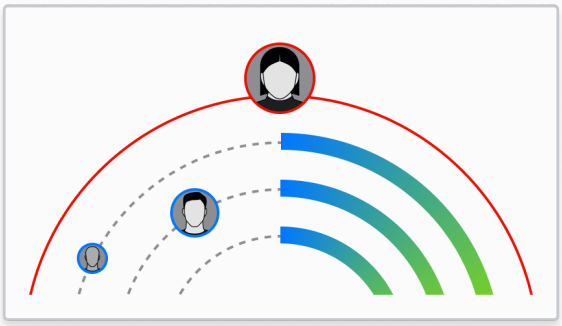
A informé de manière proactive les administrateurs M365 du plan de remédiation. L'équipe n'a reçu aucune plainte.

ANALYSE DE SÉCURITÉ MICROSOFT 365 COPILOT

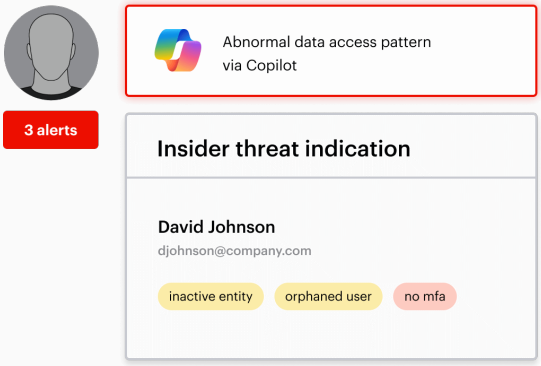
Classifier et assigner un label aux données créées par Copilot.



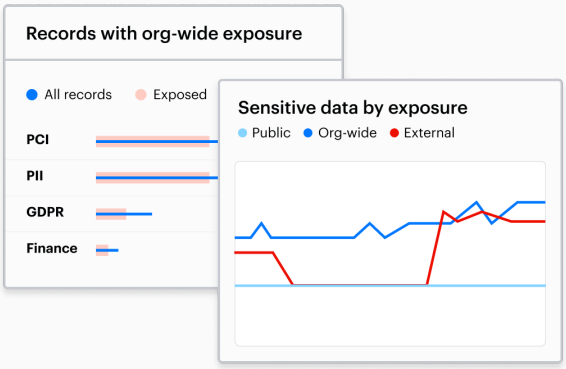
Réduire le rayon d'exposition de Copilot.



Surveiller l'activité de Copilot en temps réel.

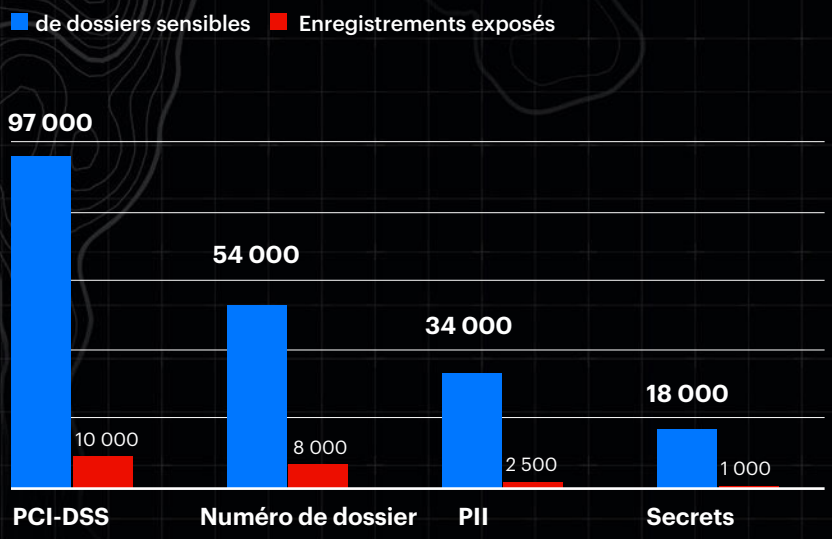


Activer les contrôles DLP en aval.



QUELLES DONNÉES SENSIBLES SONT EXPOSÉES À COPILOT ?

Les tableaux de bord de posture Copilot vous aident à évaluer la sécurité du déploiement.

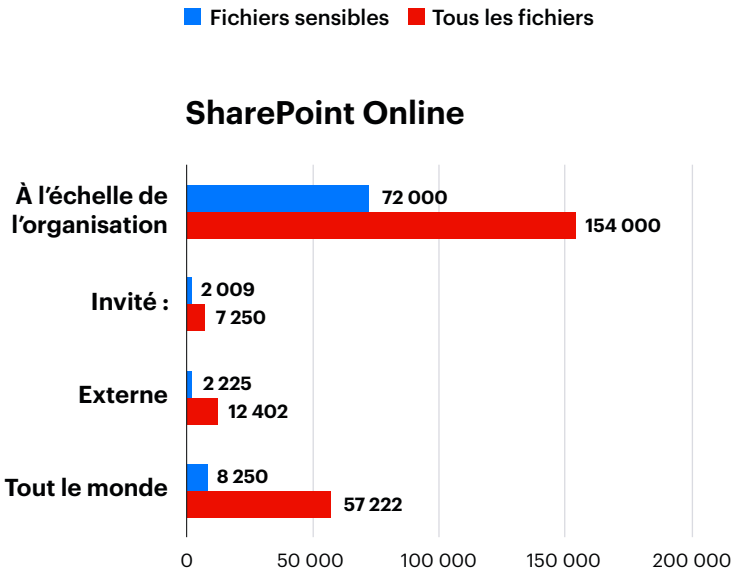


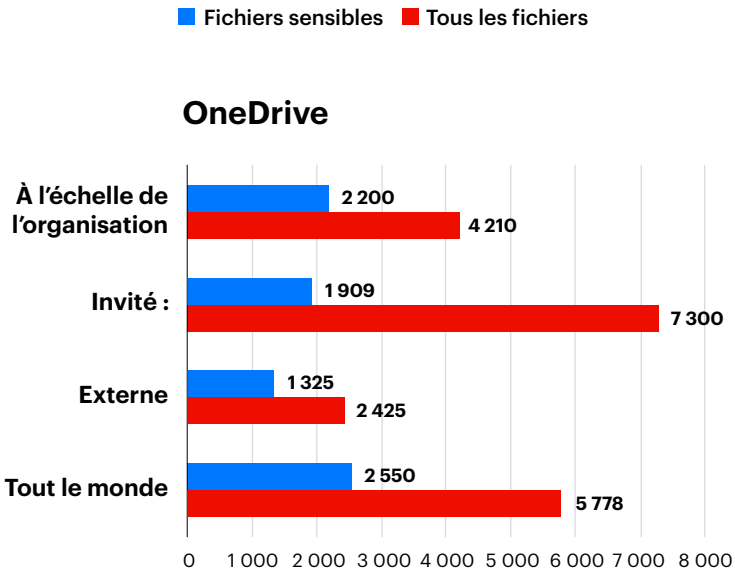
203K de dossiers sensibles

1,5K Enregistrements sensibles exposés en externe

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

Exposition des données Copilot par niveau

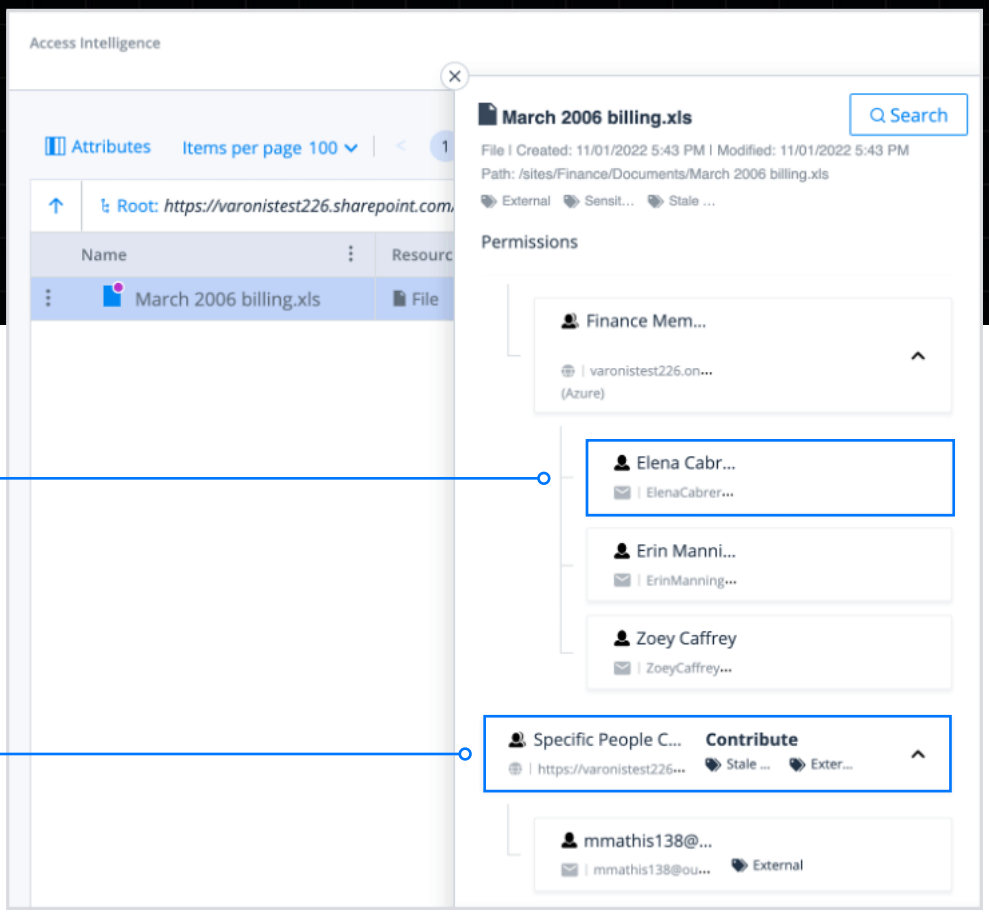




COMMENT COPILOT A-T-IL ACCÈS AUX DONNÉES SENSIBLES ?

Varonis vous montre exactement comment Copilot peut accéder à des données sensibles par n'importe quelle méthode afin que vous puissiez résoudre les problèmes avant le déploiement.

+ Permissions directes
+ Appartenance à des groupes (Teams, Azure, SharePoint, etc.)
+ Autorisations des invités
+ Liens ouverts à tout le monde
+ Liens à l'échelle de l'entreprise
+ Liens d'utilisateurs spécifiques



Elena ne fait pas partie du service Finance, mais a rejoint le groupe via Teams.

Elle ne devrait pas avoir accès aux données de facturation.

Elena a partagé ce fichier avec un compte de messagerie personnel.

Quels fichiers sensibles ont le mauvais labeling ?

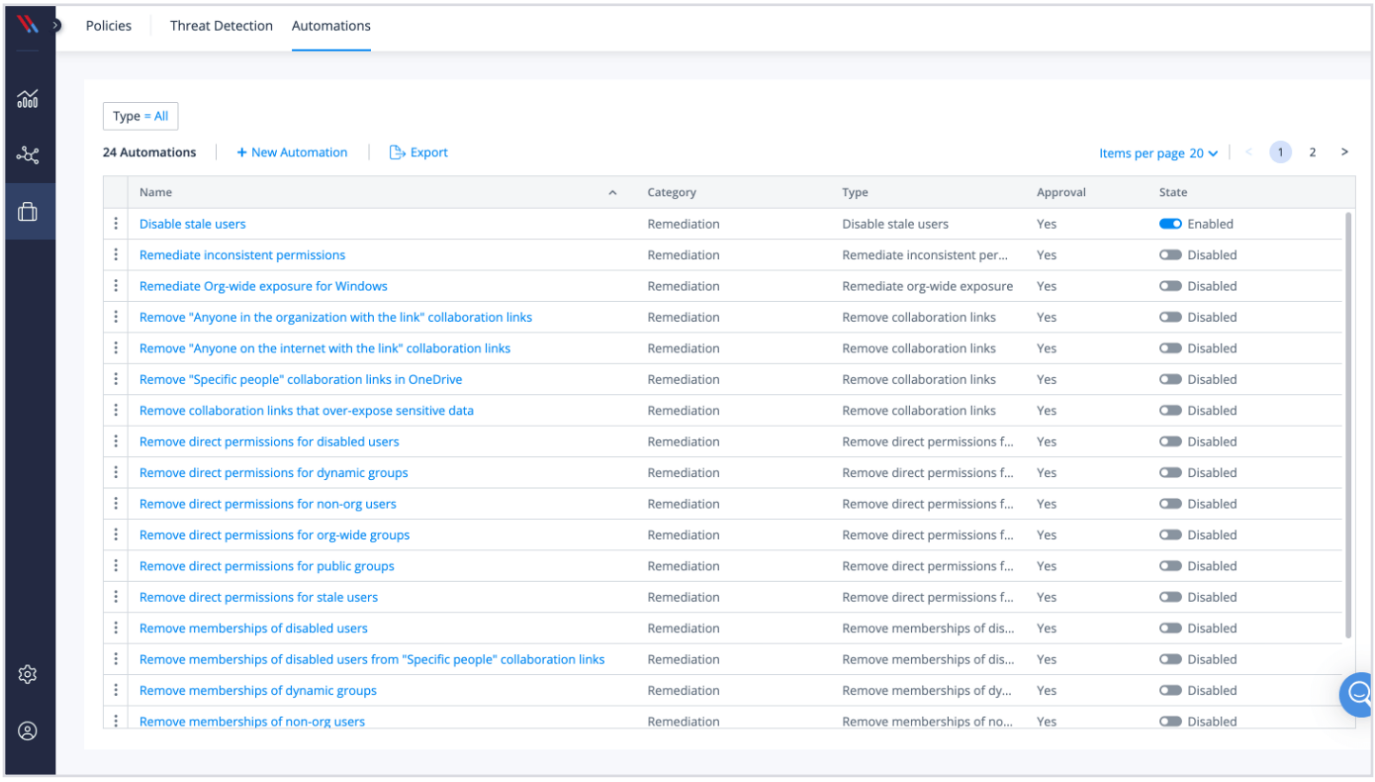
La sécurité de Copilot repose en grande partie sur des labels MPIP précis. Varonis peut les trouver et les corriger.

Nous avons trouvé plus de 27 000 fichiers sensibles sans label. Copilot ne les considère pas comme sensibles.

Drag here to set row groups

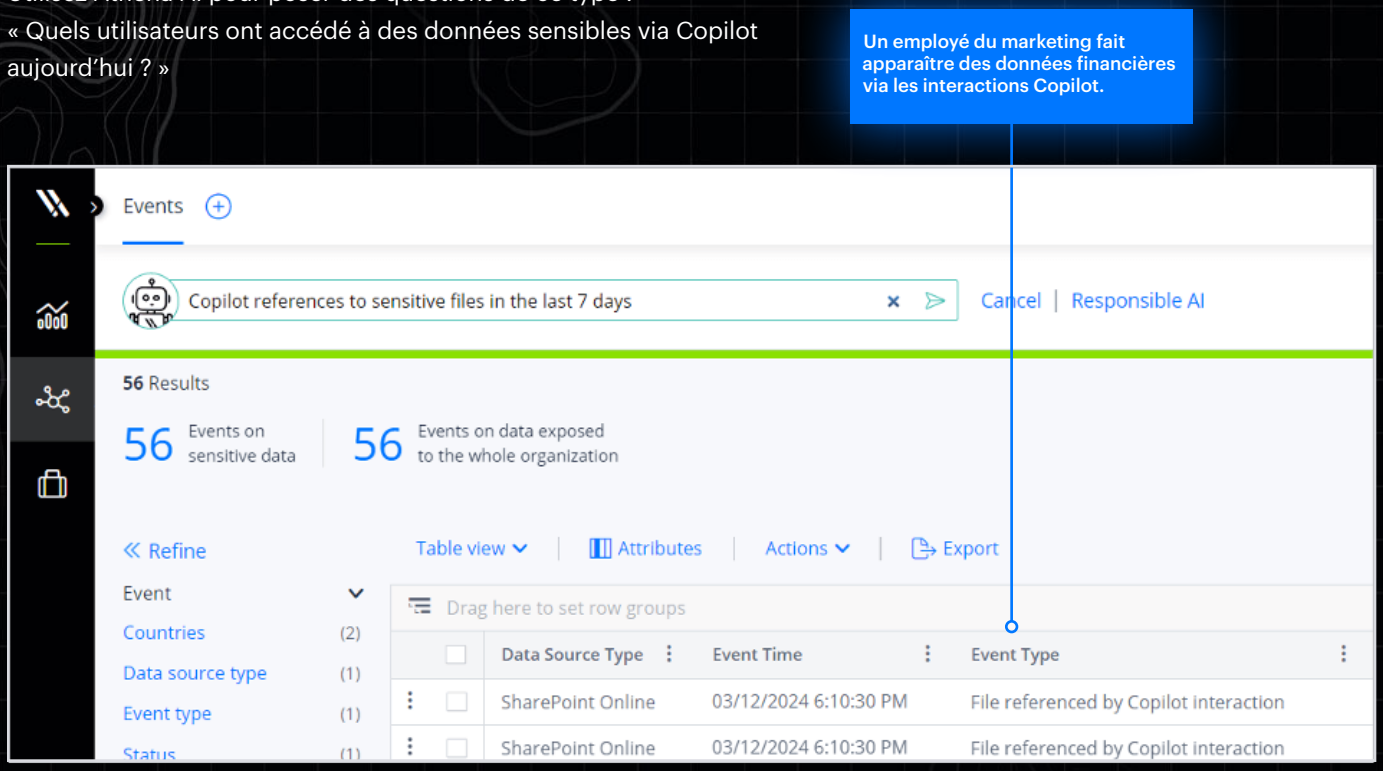
Path	Classification Results	Classification Labels	Name
C:\Share\Finance	US PII (0/43),HIPAA PHI Data - 2.0 US (0/...	GDPR Regulated Data (0/1)	Finance
C:\Share\Finance\Controllers	US PII (0/29),HIPAA PHI Data - 2.0 US (0/...		Controllers
C:\Share\Finance\Controllers\Finance repor...	US PII (2/7),HIPAA PHI Data - 2.0 US (12/...		Q1 2006
C:\Share\Finance\Controllers\Finance repor...	US PII (2/2),HIPAA PHI Data - 2.0 US (10/...		Inventory
C:\Share\Finance\Controllers\Finance repor...	US PII (3/3),HIPAA PHI Data - 2.0 US (15/...		Revenues
C:\Share\Finance\Controllers\Finance repor...	US PII (20/20),HIPAA PHI Data - 2.0 US (8...		SEC
C:\Share\Finance\data	Passwords (1/2),GDPR Greece (1/1),UK D...	GDPR Regulated Data (1/1)	data
C:\Share\Finance\DEMO94	Passwords (3/3),PCI Data Security Stand...		DEMO94
C:\Share\Finance\data\KolNet	Passwords (1/1),UK Data Protection Act ...		KolNet
C:\Share\Finance\Economics\Costing	[Preview] Document Passwords - 2.0 (6/...		Costing
C:\Share\Finance\Economics\Budget\2006\...	[Preview] Document Passwords - 2.0 (2/...		Final

Activez les stratégies d'automatisation Copilot pour que M365 soit prêt à être déployé en quelques jours.



QUI ACCÈDE AUX DONNÉES SENSIBLES VIA LES PROMPTS COPILOT ?

Utilisez Athena AI pour poser des questions de ce type :
« Quels utilisateurs ont accédé à des données sensibles via Copilot aujourd'hui ? »



Qui abuse de Copilot ?

- Détecter les interactions inappropriées ou risquées
- Détecter le partage d'informations confidentielles
- Suivre les fichiers consultés et les labels pertinents
- Appliquer des labels en réponse à des alertes

3 alerts

Abnormal data access pattern via Copilot

Insider threat indication

David Johnson
djohnson@company.com

inactive entity | orphaned user | no mfa

PLAN DE DÉPLOIEMENT DE COPILOT : **ÉTAPE PAR ÉTAPE**

Avant le déploiement de Copilot

- Déployer Varonis
- Effectuer les analyses initiales
- Ajouter et corriger des labels de confidentialité
- Remédier à une exposition à haut risque
- Vérifier l'accès aux données critiques
- Activez la DLP en aval avec Purview

Après le déploiement de Copilot

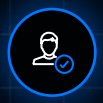
- Surveillez l'utilisation de Copilot et alertez en cas de comportement suspect et d'accès à des données sensibles
- Automatiser les politiques de contrôle d'accès
- Automatisez les politiques de DLP et de cycle de vie des données

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 liés aux 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 de 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 dès aujourd'hui sur **Varonis.fr.**

Approuvé par des milliers de clients

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