Sécurité data first, not last

Plateforme de sécurité centrée sur les données avec classification automatisée et automatisation complète

Varonis a été fondée en 2005 par le CEO Yaki Faitelson. L'entreprise, dont le siège est à New York, emploie actuellement près de 2000 personnes et compte 8000 entreprises à travers le monde parmi ses clients. Le spécialiste de la sécurité des données est fortement ancré dans le monde des grandes entreprises. Mais la plateforme de sécurité des données en mode SaaS de Varonis est aussi parfaitement adaptée aux entreprises de taille moyenne.

Contrairement à d'autres fournisseurs de solutions de sécurité des données, Varonis ne traite pas le périmètre de sécurité mais les données elles-mêmes. Sur la base d'une classification continue et automatisée de toutes les données non structurées et des activités d'accès, la plateforme Varonis gère les droits d'accès et limite l'accès à ceux pour qui celà est réellement nécessaire. De plus, les clients bénéficient de précieux services inclus, dont l'accès à toute une équipe chargée de répondre aux questions sur les incidents et une session de revue trimestrielle des activités – toujours en collaboration avec Varonis, le partenaire de sécurité concerné et les spécialistes de la sécurité du client final.

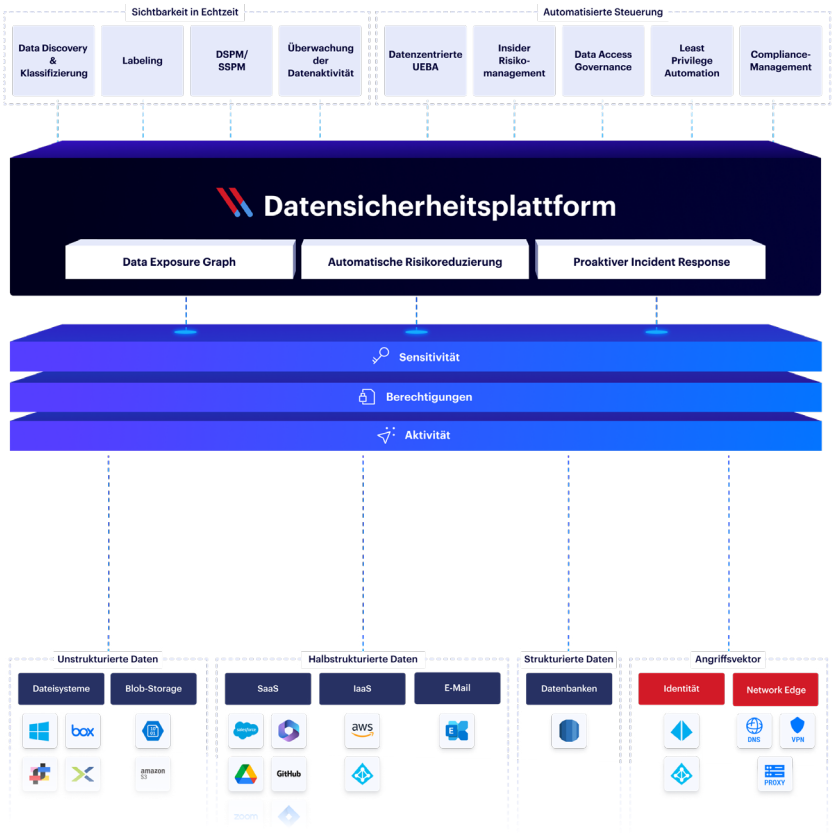
Plateforme de sécurité des données Varonis: les points forts

- Plateforme de sécurité cloud-native centrée sur les données
- Solution SaaS pour les grandes et moyennes entreprises
- Classification automatisée des données
- Remédiation des autorisations et des configurations erronées
- Aperçu en temps réel de la sécurité et de la conformité des données
- Regroupement des fonctionnalités de douze solutions de sécurité
- Équipe proactive de réponse aux incidents
- Revue d'entreprise par trimestre incluse
- Définition et mise en œuvre d'un plan opérationnel

Une sécurité complète centrée sur les données

Les cybercriminels visent toujours les données pour les voler ou les rendre inutilisables et pour demander une rançon. Avec sa plateforme de sécurité centrée sur les données, Varonis réduit au maximum le risque et l'impact des ransomwares et du vol de données – de manière entièrement automatisée et avec une charge de travail réduite pour les clients.

Les solutions de sécurité conventionnelles protègent le périmètre de sécurité et protègent contre les attaques – une tâche de plus en plus difficile à l'heure des services dans le cloud et des formes de travail hybrides. À cela s'ajoute le fait que les collaborateurs d'une entreprise ont en moyenne un accès illimité à quelques 17 millions de fichiers – indépendamment du fait qu'ils en aient réellement besoin. Ainsi, les autorisations sont généralement liées à la fonction et au poste. Pour les attaquants, c'est du pain béni: pour compromettre les données, les pirates n'ont besoin que d'un vecteur ou d'un point faible pour obtenir un accès à une grande partie des données de l'entreprise. L'utilisateur est souvent le point faible, car les systèmes de sécurité courants peuvent être facilement déjoués.

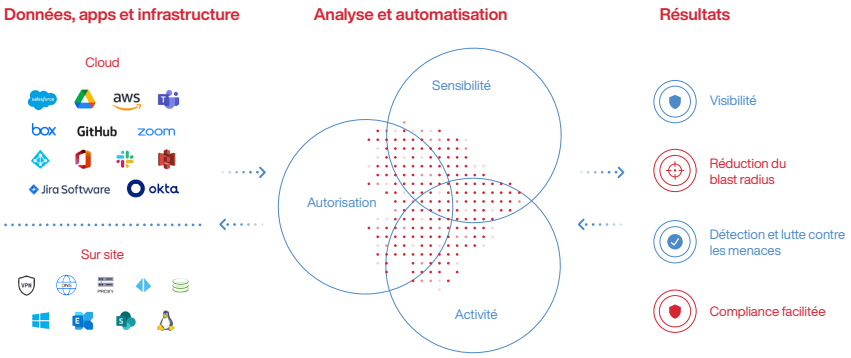


Des données au centre de la cybersécurité

La plateforme de sécurité des données de Varonis procède différemment: en analysant et en classant automatiquement toutes les données et en surveillant les activités d'accès, elle utilise le machine learning pour déterminer les risques liés aux données en se basant sur des centaines de patterns différents et sur les contenus sensibles/critiques. La plateforme peut adapter automatiquement les autorisations et émettre des recommandations, puis vérifier leur plausibilité dans un processus de sandbox avant de les activer: les utilisateurs ont uniquement accès aux fichiers avec lesquels ils travaillent réellement. En général, les utilisateurs ne remarquent pas ces ajustements.

Flyer du fabricant
Plateforme de sécurité des données Varonis

En outre, la plateforme utilise la télémétrie d'authentification et du périmètre, surveille en permanence les activités d'accès pour détecter les processus suspects et est en mesure de déclencher automatiquement des contre-mesures. Le risque lié aux données est ainsi considérablement réduit. La portée d'une attaque de ransomware, par exemple, est nettement limitée, car les utilisateurs et les groupes qui ne travaillent pas directement avec un fichier ont seulement un accès en lecture, voire plus du tout.
Une activité de cryptographie est stoppée sur la base de valeurs seuils recommandées et le chiffrement des serveurs de fichiers ou des mémoires dans le cloud est rendu impossible.
La plateforme cloud-native de sécurité des données de Varonis combine également les fonctionnalités d'une douzaine de solutions de sécurité sur une console de gestion commune – toujours centrée sur les données:



3 alerts

Cameron Hubbard accessed an anomalous number of account records

Insider threat indication

Cameron Hubbard
chubbard@company.com

inactive entity | orphaned user | no mfa

- Gestion de la posture en matière de sécurité des données
- Détection et classification automatisées des données
- Audit de l'activité des données
- Analyse du comportement utilisateur basée sur les données (UEBA)
- Identification des autorisations rompues et correction automatisée de l'autorisation (broken ACL)
- Gouvernance de l'accès aux données
- Gestion de la conformité
- Intégration dans les stratégies et solutions de prévention des pertes de données existantes
- Protection d'Active Directory / Azure AD
- Gestion des risques internes
- Prévention des ransomwares

À cela s'ajoutent des prestations incluses attractives de Varonis. Il s'agit notamment des services suivants:

- Sur demande, une analyse gratuite des risques liés aux données est effectuée, avec pour résultat un aperçu complet des données sensibles existantes, des droits d'accès et des comportements inhabituels des utilisateurs.
- Les clients ont la possibilité d'organiser régulièrement des «office hours». Ces «office hours» aident les administrateurs à utiliser la plateforme Varonis de manière plus efficace et les soutiennent activement dans la réalisation de leurs objectifs.
- L'équipe proactive de réponse aux incidents vérifie quotidiennement l'état de l'environnement et informe les administrateurs locaux en cas d'anomalies.
- La valeur ajoutée obtenue est présentée lors d'une session de revue trimestrielle des affaires et les incidents survenus ainsi que les adaptations nécessaires qui en découlent sont régulièrement discutés avec le client et son partenaire de sécurité.

BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 (0)56 437 60 60 / sales@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 (0)21 533 01 60 / vente@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / D-89081 Ulm / Telefon +49 (0)731 85 07 48 23 / info@boll-europe.com / www.boll-europe.com
BOLL Europe GmbH . Wienerbergstrasse 9 / A-1100 Wien / Telefon +43 (0)664 46 48 580 / info@boll-europe.at / www.boll-europe.at