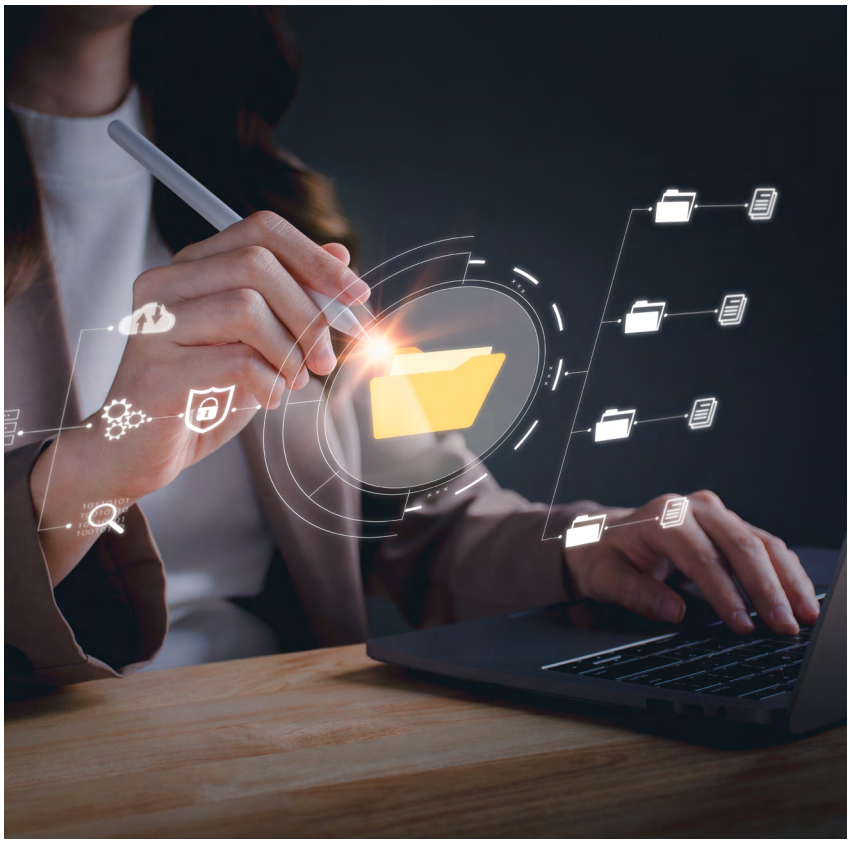
# Plateforme complète de sécurité des données

Grâce à sa plateforme de sécurité centrée sur les données, Varonis réduit au maximum le risque et l'impact des ransomwares, cryptoactivités et autres – de manière hautement automatisée.

De nos jours, toutes les entreprises doivent s'attendre à des cyberattaques. L'objectif des cybercriminels est généralement de voler des données ou de les crypter et de les vendre sur le darknet ou de les restituer contre une rançon. La taille de l'entreprise et le secteur d'activité ne jouent aucun rôle: celui qui détient des données sensibles intéresse les cybercriminels, peu importe que l'entreprise soit connue ou inconnue, grande ou petite, privée ou publique. Il suffit qu'une entreprise possède des données sensibles pour que quelqu'un veuille les récupérer.



**Le périmètre de sécurité perd de sa pertinence**

Les solutions de cybersécurité se concentrent traditionnellement sur la protection du périmètre de sécurité et la défense contre les attaques. Tous les systèmes sont basés sur le même principe: il y a un utilisateur et un profil d'utilisateur et les autorisations qui leur sont associées. À l'époque des modes de travail hybrides, des terminaux mobiles et des services cloud, cela devient de plus en plus difficile à gérer. Les collaborateurs ont en moyenne accès à 17 millions de fichiers dès leur premier jour de travail.
Peu importe qu'ils en aient réellement besoin ou qu'ils en bénéficient simplement par défaut en raison de leur position ou du groupe d'utilisateurs.
Le périmètre de sécurité de plus en plus large et les nombreuses autorisations non nécessaires ont pour effet de gonfler massivement le «blast radius» (celui-ci décrit combien de données sont immédiatement disponibles pour un attaquant) et donc le risque lié aux données: il suffit d'un seul des centaines de vecteurs d'attaque potentiels, d'un utilisateur compromis, pour qu'un pirate ait accès à des millions de fichiers. Celui-ci peut ainsi, souvent sans se faire remarquer, extraire les données au fil des semaines et des mois, voire finalement les crypter.

**Priorité aux données**

La plateforme de sécurité des données de Varonis adopte une approche radicalement différente: la portée des cyberattaques est fortement réduite par la détection, l'analyse et la classification automatisées de toutes les données ainsi que par la réduction adéquate des droits d'accès. Sur la base de centaines de modèles différents et du machine learning, la plateforme est en mesure de classer de manière autonome environ 95 % des données. Les 5 % restants sont évalués et classés individuellement par les entreprises en collaboration avec Varonis.

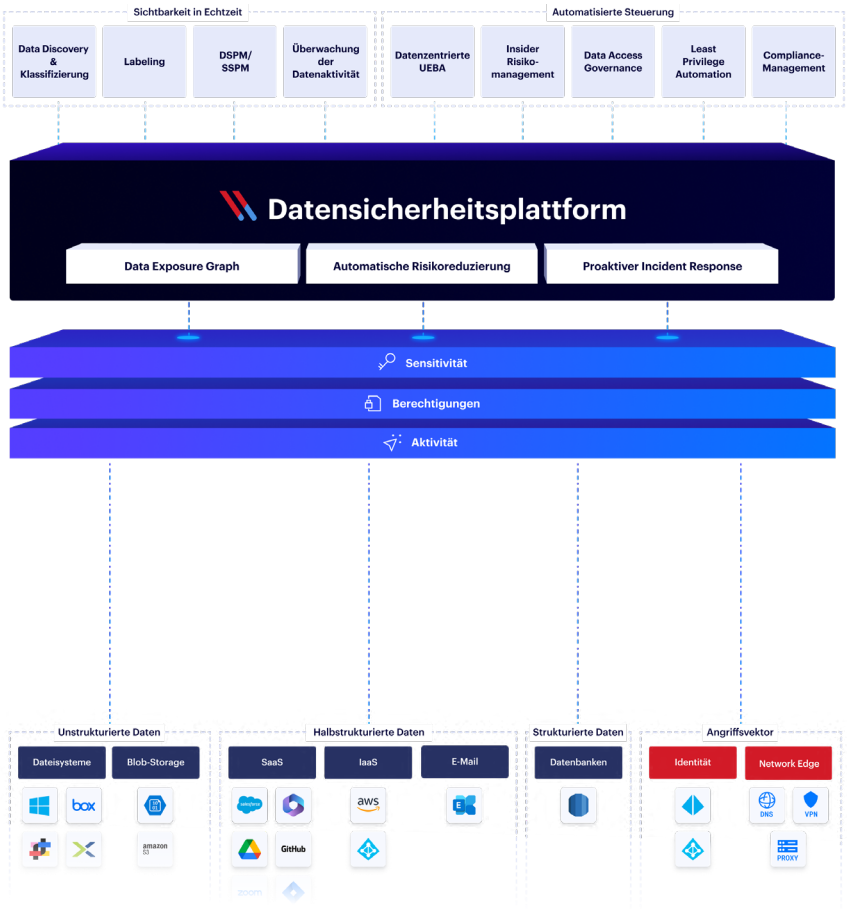
La classification est suivie d'une analyse des activités d'accès. Sur cette base, la plateforme de sécurité des données →

peut émettre des recommandations pour limiter les droits d'accès – en appliquant une procédure de sandbox, généralement sans que les utilisateurs ne s'en rendent compte. Ainsi, les utilisateurs et les groupes qui ne travaillent pas directement avec un fichier n'ont plus qu'un accès en lecture, ce qui empêche le cryptage. En outre, la plateforme utilise l'authentification et la télémétrie du périmètre, vérifie en permanence les activités d'accès aux fichiers pour détecter les opérations suspectes et, si nécessaire, déclenche automatiquement des contre-mesures – par exemple, en isolant un utilisateur en cas d'activité de cryptage ou de copie anormalement élevée. Une classification et, le cas échéant, une reclassification des fichiers ont lieu à chaque nouvel enregistrement – indépendamment des classifications effectuées auparavant. Ainsi, il est garanti que les fichiers peuvent toujours être évalués correctement. La plateforme de sécurité des données de Varonis regroupe les fonctionnalités d'une douzaine de solutions de sécurité, allant de la gestion de la posture de sécurité des données à la prévention des ransomwares, en passant par la classification automatique des autorisations et des données, le tout sur une seule console de gestion, avec toujours les données en priorité.

**Point de départ: analyse des risques liés aux données**

Au lieu d'une preuve de concept, Varonis propose aux entreprises intéressées une analyse gratuite des risques liés aux données qui fournit un aperçu complet des données sensibles existantes, des droits d'accès, des comportements inhabituels des utilisateurs ainsi que des données et comptes utilisateurs éventuellement inutiles. Cela permet de déterminer les risques existants pour les données. Dans la pratique, on découvre très souvent des faits choquants, tels que des mots de passe Kerberos jamais modifiés depuis des décennies.

Celui qui choisit la plateforme de sécurité des données de Varonis bénéficie en plus d'une équipe de réponse aux incidents qui surveille quotidiennement et de manière proactive les anomalies, informe les clients en cas d'incidents et prend ou propose des mesures appropriées. À cela s'ajoute une évaluation trimestrielle des activités, au cours de laquelle la valeur ajoutée obtenue et les éventuelles adaptations nécessaires sont discutées.




**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
- Ajustement entièrement automatisé des autorisations au sein du système de fichiers
- Remédiation des liens dans les environnements Microsoft 365
- Visualisation prioritaire en temps réel de la situation en matière de sécurité et de conformité des données dans des tableaux de bord compréhensibles et des rapports générés automatiquement.
- Regroupement des fonctionnalités de nombreuses solutions de sécurité en une seule interface de gestion
- Equipe de réponse proactive en cas d'incidents
- Business review inclus par trimestre

BOLL
IT Security Distribution

**BOLL Engineering SA**
En Budron H15
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch