Sicherheit mit «Data first, not last»

Datenzentrierte Sicherheitsplattform mit automatisierter Klassifizierung und umfassender Automatisierung

Varonis wurde 2005 vom CEO Yaki Faitelson gegründet. Das Unternehmen mit Hauptsitz in New York beschäftigt aktuell rund 2000 Mitarbeitende und zählt weltweit gegen 8000 Unternehmen zu seinem Kundenkreis. Der Data-Security-Spezialist ist stark im Enterprise-Geschäft verankert. Doch die SaaS-basierte Data Security Platform von Varonis eignet sich auch optimal für mittelständische Unternehmen. Im Gegensatz zu anderen Anbietern von Datensicherheitslösungen setzt Varonis nicht beim Sicherheitsperimeter an, sondern bei den Daten selbst. Die Varonis-Plattform regelt auf Basis einer kontinuierlichen, automatisierten Klassifizierung aller unstrukturierten Daten und der Zugriffsaktivitäten die Zugriffsberechtigungen und schränkt den Zugriff auf das wirklich Notwendige ein.
Darüber hinaus erhalten Kunden wertvolle Services inklusive, darunter Zugang zu einem globalen und proaktiven Incident-Response-Team und eine vierteljährliche Business-Review-Session – stets gemeinsam mit Varonis, dem jeweiligen Security-Partner und den Sicherheitsspezialisten des Endkunden.

Varonis Data Security Platform: Die Highlights

- Cloudnative datenzentrierte Sicherheitsplattform
- SaaS-Lösung für grosse und mittelständische Unternehmen
- Automatisierte Datenklassifizierung
- Sanierung von Berechtigungen und Fehlkonfigurationen
- Echtzeitansicht der Datensicherheits- und Compliance-Lage
- Vereint Funktionalitäten von zwölf Sicherheitslösungen
- Globales, proaktives Incident-Response-Team
- Business-Review pro Quartal inklusive
- Definition und Umsetzung einer Operational Journey

Umfassende datenzentrierte Sicherheit

Cyberkriminelle haben es immer auf Daten abgesehen, um diese zu stehlen oder unbrauchbar zu machen und um Lösegeld zu fordern. Mit seiner datenzentrierten Sicherheitsplattform reduziert Varonis das Risiko und die Auswirkungen von Ransomware und Datenklau auf ein Minimum – voll automatisiert und mit geringem Arbeitsaufwand für die Kunden.

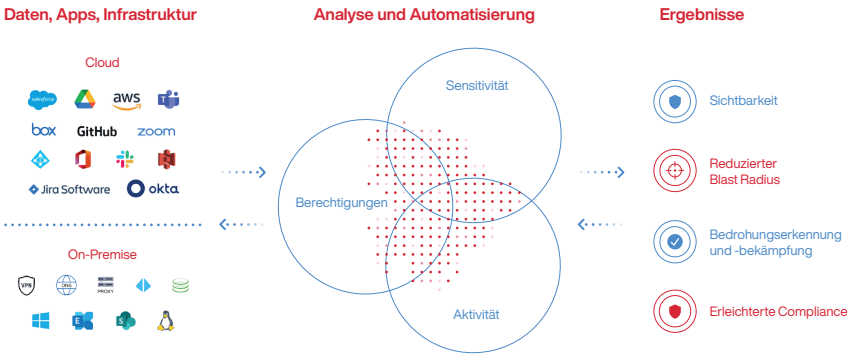
Herkömmliche Sicherheitslösungen schützen den Sicherheitsperimeter und wehren Angriffe ab – in Zeiten von Cloud-Diensten und hybriden Arbeitsformen ein zunehmend schwieriges Unterfangen. Hinzu kommt, dass die Mitarbeitenden eines Unternehmens durchschnittlich uneingeschränkten Zugriff auf rund 17 Millionen Dateien haben – unabhängig davon, ob sie dies wirklich benötigen. So sind Berechtigungen in der Regel mit der Funktion und der Position verknüpft. Für Angreifer ein gefundenes Fressen: Um Daten zu kompromittieren, benötigen Angreifer nur einen Vektor beziehungsweise eine Schwachstelle, um einen Zugang zu einem Grossteil der Unternehmensdaten zu erhalten. Der User ist hier häufig die Schwachstelle, da sich gängige Security-Systeme leicht umgehen lassen.

Daten im Zentrum der Cybersicherheit

Die Data Security Platform von Varonis geht anders vor: Durch automatisierte Analyse und Klassifizierung aller Daten sowie Überwachung der Zugriffsaktivitäten ermittelt sie mithilfe von Machine Learning anhand Hunderter verschiedener Patterns das Datenrisiko, basierend auf sensitiven/kritischen Inhalten. Die Plattform kann Berechtigungen automatisiert anpassen und Empfehlungen aussprechen und diese vor der Aktivierung in einem Sandbox-Verfahren auf Plausibilität prüfen: Benutzer erhalten nur auf jene Dateien Vollzugriff, mit denen sie tatsächlich arbeiten. Von diesen Anpassungen spüren die User im Allgemeinen nichts. Darüber hinaus nutzt die Plattform Authentifizierungs-

und Perimetertelemetrie, überwacht die Zugriffsaktivitäten kontinuierlich auf verdächtige Vorgänge und kann automatisch Gegenmassnahmen einleiten.

Dadurch reduziert sich das Datenrisiko massiv. Die Tragweite etwa einer Ransomware-Attacke wird deutlich eingeschränkt, weil zum Beispiel User und Gruppen, die nicht direkt mit einer Datei arbeiten, nur noch Lese- oder gar keinen Zugriff mehr erhalten.
Eine Kryptoaktivität wird, basierend auf empfohlenen Schwellenwerten, gestoppt, und eine Verschlüsselung der Fileserver beziehungsweise der Cloud-Speicher dadurch verhindert.
Die cloudnative Data Security Platform von Varonis kombiniert darüber hinaus die Funktionalität von einem Dutzend Sicherheitslösungen auf einer gemeinsamen Managementkonsole – immer stehen die Daten im Mittelpunkt. Es sind dies:



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

- Data Security Posture Management
- Automatisierte Datenermittlung und -klassifizierung
- Prüfung von Datenzugriffsaktivitäten
- Datenzentrierte und userbasierte Verhaltensanalyse (UEBA)
- Identifikation gebrochener Berechtigungen und automatisierte Korrektur der Berechtigung (broken ACL)
- Data Access Governance
- Compliance Management
- Integration in bestehende Data-Loss-Prevention-Strategien und -Lösungen
- Härtung von Active Directory/ Azure AD
- Insider-Risikomanagement
- Ransomware-Prävention

Hinzu kommen attraktive eingeschlossene Dienstleistungen von Varonis. Dazu gehören die folgenden Services:

- Auf Wunsch erfolgt eine kostenlose Datenrisikoanalyse mit dem Ergebnis einer umfassenden Übersicht über die vorhandenen sensiblen Daten, Zugriffsrechte und ungewöhnliches Benutzerverhalten.
- Kunden erhalten die Möglichkeit, regelmässige Office Hours durchzuführen. Die Office Hours helfen Administratoren, den Umgang mit der Varonis-Plattform effektiver zu gestalten, und unterstützen aktiv bei der Umsetzung der gesteckten Ziele.
- Das proaktive, global verfügbare Incident-Response-Team überprüft täglich den Zustand der Umgebung und informiert bei Auffälligkeiten die lokalen Administratoren.
- In einer vierteljährlichen Business-Review-Session wird erzielter Mehrwert dargestellt und aufgetretene Vorkommnisse und damit verbundene erforderliche Anpassungen gemeinsam mit dem Kunden und seinem Security-Partner regelmässig besprochen.