VARONIS

GEGENMASSNAHMEN

DATENRISIKO-BEURTEILUNG

Vorbereitet für Umbrella Corp.

WICHTIGE ERKENNTNISSE

0 10 20 30 FÜR 40 50 60 70

ERSTELLUNGSDATUM: 8.7.23

INHALTSÜBERSICHT

„Ich war erstaunt, wie schnell Varonis während der kostenlosen Bewertung Daten klassifizieren und potenzielle Exposition von Daten aufdecken konnte. Es war wirklich erstaunlich.“

Michael Smith, CISO, HKS

WARUM HAT UMBRELLA CORP EINE DATEN-RISIKOBEWERTUNG VON VARONIS DATA RISK GESTARTET?

Die Umbrella Corp. hat auf Vorstandsebene die Auflage, alle PII zu ermitteln, zu klassifizieren und zu kennzeichnen, um die Einhaltung der Vorschriften und die Wirksamkeit der nachgelagerten DLP sicherzustellen. Der jüngste Ransomware-Vorfall der Umbrella Corp. unterstreicht die Notwendigkeit einer Datenüberwachung. Wenn sie nicht handeln, drohen ihnen Geldstrafen und eine Daten-Exposure, die für die Unternehmensleitung unangenehm ist.

Herausforderungen

Die Klassifizierung sensibler Daten und die Behebung von Gefährdungen ist eine Herausforderung.

Die Quantifizierung der Datensicherheit und die Darstellung der Fortschritte gegenüber dem Vorstand sind ein Muss.

Mit einem kleinen Team sind Datensanierungsbemühungen schwierig.

Es ist notwendig, die Datennutzung zu überwachen und bei abnormalen Aktivitäten zu alarmieren.

Untereinheiten arbeiten unabhängig voneinander – ein einheitliches Datensicherheitsprogramm ist erforderlich.

Compliance-Audits sind manuell und unvollständig.

ÜBERBLICK ÜBER DIE RISIKOBEWERTUNG VON UMBRELLA CORP

Verbundene Datenquellen und Zeitplan für die Bewertung

Varonis kann sich mit Dutzenden zusätzlicher Datenquellen verbinden. Die Einrichtung dauert nur wenige Minuten.

Microsoft 365 | Active Directory + Azure AD | Salesforce | Windows-Dateifreigabe | Google Workspace

Plattform-Installation
1. Juni 2023

Bewertung

Proof of Value
21. Juni 2023

5,6 M
Ressourcen (Dateien/Objekte)

12K
Identitäten

805K
Ereignisse (Tagesdurchschnitt)

2,4 M
sensible klassifizierte Datensätze (PHI, PCI, Geheimnisse)

Hinweis: Nur ein Teil der gesamten Umgebung von Umbrella Corp war für das Proof of Concept angeschlossen.

WICHTIGE ERKENNTNISSE

Risiken, die zu einem Datenleck führen könnten

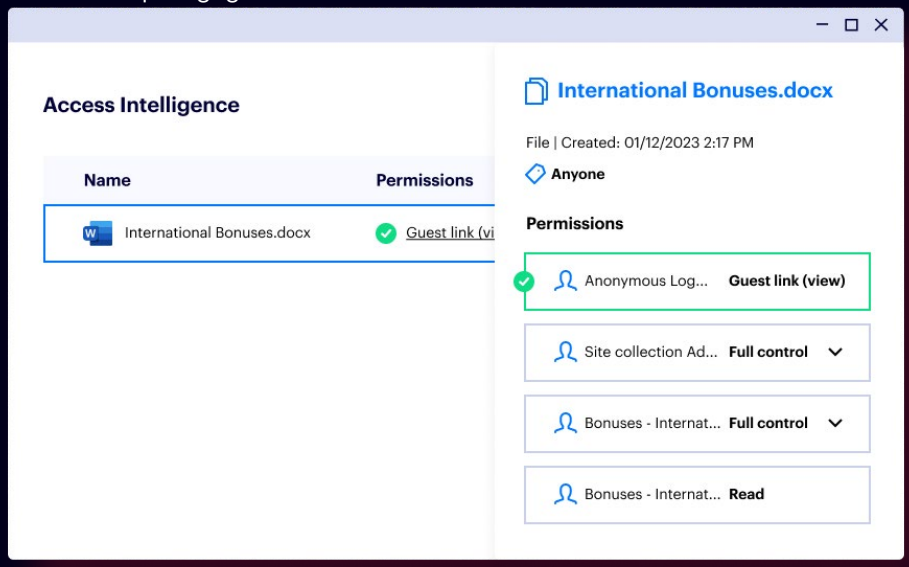
Nachfolgend sind die vier wichtigsten Erkenntnisse aufgeführt, die Varonis als kritisches Datensicherheitsrisiko ansieht.

1. HR-Vergütungsberichte, die über für jeden zugängliche Links öffentlich geteilt werden.
2. 332 Salesforce-Benutzer können Produktionsdaten exportieren.
3. Ein externer Nutzer ist ein Superadmin in Google Workspace.
4. Ein Marketingassistent hat einen Alert wegen ungewöhnlichen Datenzugriffs ausgelöst.

Wichtige Erkenntnis Nr. 1

HR-Vergütungsberichte, die öffentlich über für jeden zugängliche Links geteilt werden.

Melissa Donovan hat die Bonusinformationen des Unternehmens versehentlich im Internet preisgegeben.



Art des Risikos:
Preisgabe öffentlicher Daten

NIST-Kontrolle:
AC-3 (9): Kontrollierte Freigabe

Betroffenes System:
Microsoft 365

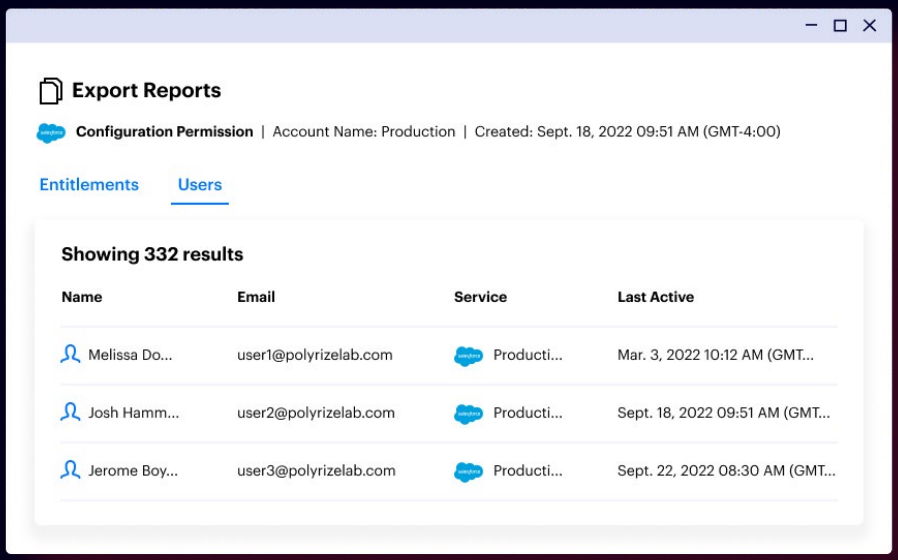
Beobachtung:
Melissa Donovan, eine HR-Geschäftspartnerin, hat am 12. Januar „International Bonuses.docx“ auf ihre HR-Teams-Website hochgeladen. Der Klassifizierungsscan von Varonis identifizierte 231 Fälle personenbezogener Daten in der Datei und unsere Protokolle zeigen, dass sie am 13. Februar den frei zugänglichen Link erstellt hat, wodurch die Datei im Internet zugänglich gemacht wird. Auf den Link haben anonyme Benutzer von 27 verschiedenen IP-Adressen weltweit zugegriffen.

Empfehlung:
Entziehen Sie sofort den freien Zugriff auf diese Datei, indem Sie den Link deaktivieren. Deaktivieren Sie die Möglichkeit, öffentlich zu teilen. Verwenden Sie die Varonis-Automatisierung, um alle öffentlichen Links zu Dateien mit vertraulichen Informationen zu widerrufen.

Wichtige Erkenntnis Nr. 2

332 Salesforce-Benutzer können Produktionsdaten exportieren.

Das reguläre Profil „Vertrieb“ gewährt Exportzugriff. Dies ist zu weit gefasst und sollte behoben werden.



Risikotyp:
Preisgabe sensibler Daten

NIST-Steuerung:
AC-2(7): rollenbasierte Schemata

Betroffenes System:
Salesforce (Produktion, Sandbox, Entwicklung)

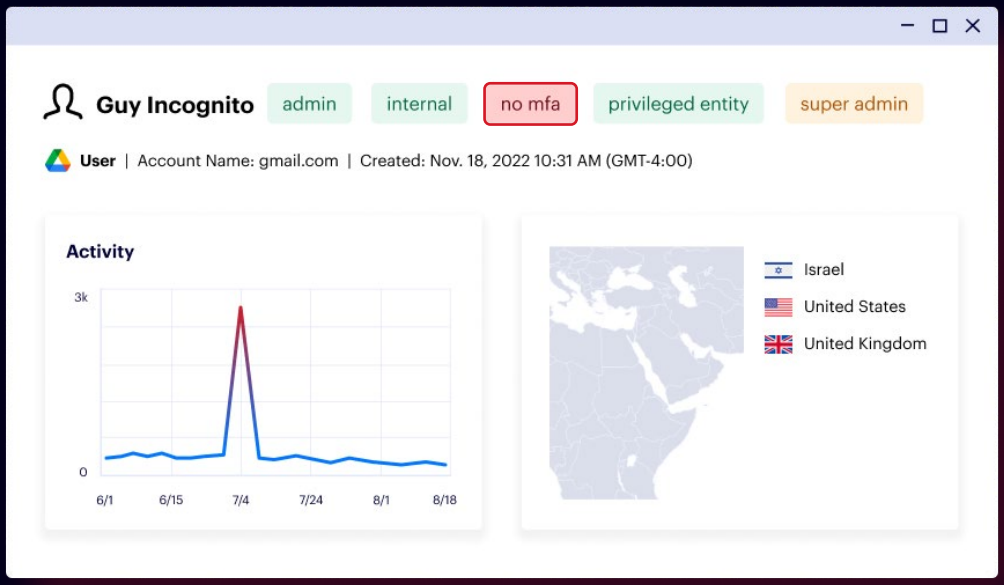
Beobachtung:
Varonis-Scans ergaben eine toxische Kombination von Berechtigungen, die ein ernstes Datenexfiltrationsrisiko darstellt – 332 Vertriebsmitarbeiter können über ihr „Vertrieb“-Profil alle Lead-, Kontakt-, Möglichkeiten- und Kontodaten aus der Salesforce-Produktionsinstanz von Umbrella Corp. exportieren.

Empfehlung:
Entfernen Sie die Berechtigung zum Exportieren von Berichten aus dem Profil „Vertrieb“ und jeder anderen Rolle, die kein Administrator ist. Überprüfen Sie alle Profile und Berechtigungssätze, die hochprivilegierte Aktionen gewähren – wie Bericht exportieren, alle Daten ändern und alle Daten lesen.

Wichtige Erkenntnis Nr. 3

Ein externer Benutzer ist ein Super-Admin in Google Workspace.

Guy Incognito ist ein Super-Admin ohne MFA. Seine Aktivität hat am 4. Juli stark zugenommen, was einen Alert ausgelöst hat.



Risikotyp:
Unsicheres Administratorkonto

NIST-Kontrolle:
AC-2(7): Privilegierte Benutzerkonten

Betroffenes System:
Google Workspace

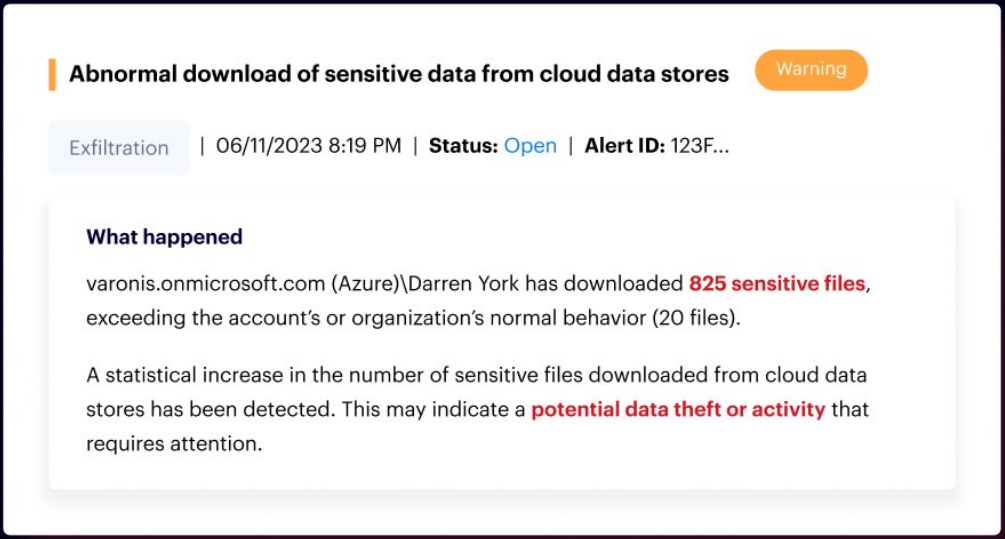
Beobachtung:
Guy Incognito ist ein externer Auftragnehmer, der ein persönliches Gmail-Konto für den Zugriff auf das Google-Workspace-Konto von Umbrella Corp verwendet. Dieser Benutzer hat Super-Admin-Rechte und hat keine MFA aktiviert. Dieses Konto gilt als extrem hohes Risiko.

Empfehlung:
Sofort MFA auf dem Konto von Guy Incognito erzwingen und zu einer Beobachtungsliste in Varonis hinzufügen. Überprüfen Sie die Aktivitäten, Berechtigungen und zugehörigen Identitäten des Benutzers in den letzten 30 Tagen. Entscheiden Sie, ob dieser externe Benutzer wirklich Super-Admin-Rechte benötigt.

Wichtige Erkenntnis Nr. 4

Ein Marketingassistent hat einen Alert wegen ungewöhnlichen Datenzugriffs ausgelöst.

Darren York sollte keinen Zugriff auf Finanzdaten haben. Varonis UEBA hat einen ungewöhnlichen Zugriff festgestellt.



Risikotyp:
Ungewöhnliches Benutzerverhalten

NIST-Kontrolle:
AC-2(12): Kontoüberwachung auf ungewöhnliche Aktivitäten

Betroffenes System:
Microsoft 365

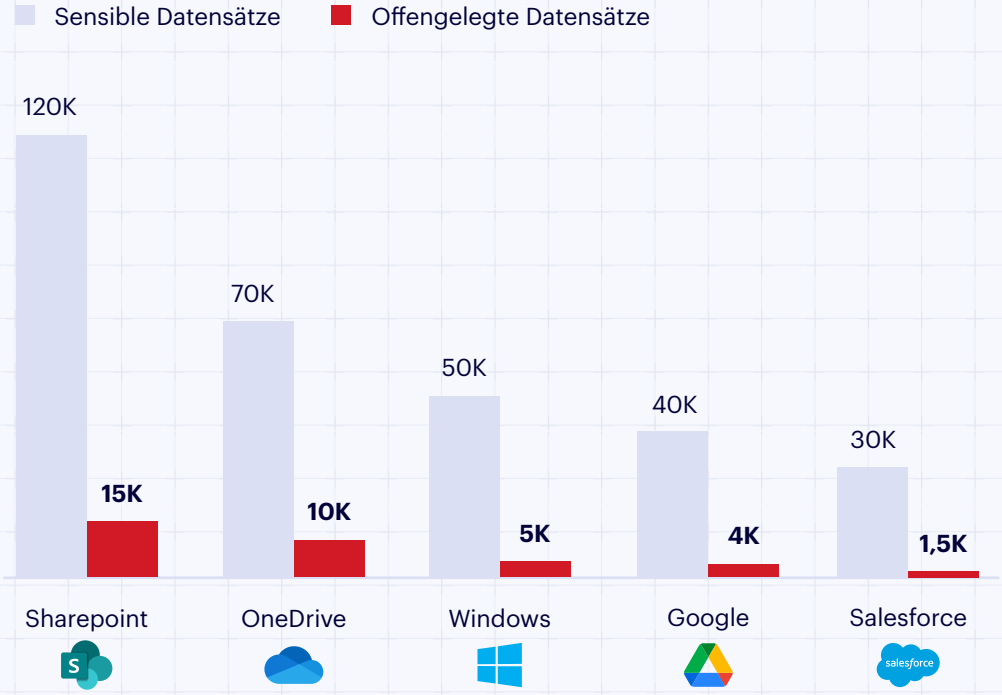
Beobachtung:
Der Marketingassistent Darren York löste eine verhaltensbasierte Warnung aus, indem er von seiner normalen Grundlinie der Datenzugriffsaktivität abwich. Varonis stellte fest, dass er auf Dateien mit Finanzdaten zugriff, was für seine Rolle untypisch ist.

Empfehlung:
Verwenden Sie Varonis, um eine Abfrage auszuführen, um alle von Aktivitäten von Darren in den letzten 30 Tagen zu sehen. Stellen Sie sicher, dass Berechtigungen für Daten, die Finanzunterlagen enthalten, nur Mitarbeitern zugänglich sind, die Zugriff benötigen.

MANAGEMENT DER DATENSICHERHEITSLAGE

Die sensiblen Daten von Umbrella Corp. sind über mehrere Cloud-Dienste und lokale Datenspeicher verteilt. Um das Risiko eines Datenlecks zu minimieren, ist es für das Unternehmen von entscheidender Bedeutung, in Echtzeit Einblick in und Kontrolle über seinen sich schnell verändernden Datenbestand zu haben – mit einheitlicher Klassifizierung, Bedrohungserkennung und Durchsetzung von Richtlinien.

Wo befinden sich die sensibelsten Daten von Umbrella Corp und wie viele davon sind gefährdet?



Wichtige Risikoindikatoren:

310K sensible Datensätze	**27K** Ereignisse mit sensiblen Daten pro Tag
24,5K Sensible Datensätze werden organisationsweit offengelegt	**11K** sensible Aufzeichnungen werden extern offengelegt

Datenermittlung und -klassifizierung

Klassifizierungsrichtlinien aktiviert

Wir haben 85 integrierte Regeln aktiviert und während dieser Risikobewertung drei benutzerdefinierte Regeln erstellt. Die vier wichtigsten Datentypen nach Volumen sind unten aufgeführt.

PCI-DSS

Container: 1.160
Objekte: 12.421
Datensätze: 89.924

Passwörter

Container: 160
Objekte: 421
Datensätze: 923

US-amerikanische PII

Container: 2.620
Objekte: 72.245
Datensätze: 199.104

Fallzahlen

Container: 1.002
Objekte: 92.420
Datensätze: 799.922

Integrierte Richtlinienbibliothek

PII	DSGVO	Anmeldeinformationen	Finanziell	Bundesebene
HIPAA PHI 2.0	DSGVO Deutschland	Passwörter	PCI-DSS 2.0	ITAR
Colorado Privacy Act	DSGVO Frankreich	Private Schlüssel	SOX	STRENG GEHEIM
NY SHIELD Act	DSGVO Österreich	Zertifikate	GLBA	CUI

Plus Hunderte weitere Regeln, Muster und Wörterbücher

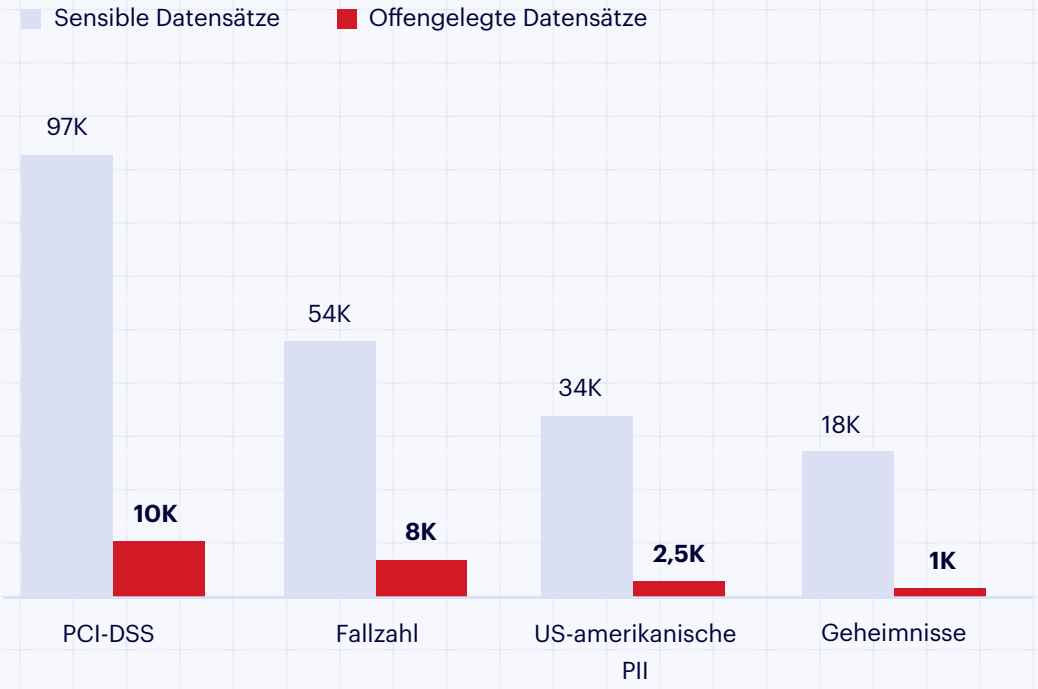
Die Leistungsfähigkeit der Varonis-Datenklassifizierung

- Echtes inkrementelles Scannen für effiziente und skalierbare Erkennung von riesigen Datensätzen
- Einheitliche Klassifizierungsrichtlinien für alle unterstützten Data Stores
- In Multi-Petabyte-Umgebungen getestet
- Über 400 von Experten erstellte und getestete Regeln sind sofort verfügbar (und es werden immer mehr).
- Anpassbare Scan-Umfänge und Probenahme

Daten-Exposure bei Microsoft 365

Die Exposure von Daten bei M365 betrifft nicht nur Umbrella Corp. Ein durchschnittliches Unternehmen verfügt über mehr als 40 Millionen eindeutige Berechtigungen für seine Multi-Cloud-Daten und laut Microsoft sind mehr als 50 % der Berechtigungen mit hohem Risiko verbunden und können bei falscher Konfiguration katastrophale Schäden anrichten.

Welche Art von Daten sind in M365 gespeichert und wie hoch ist die Exposure von Umbrella Corp.?



Wichtige Risikoindikatoren:

203K
sensible Datensätze

20K
Sensible Datensätze werden unternehmensweit offengelegt

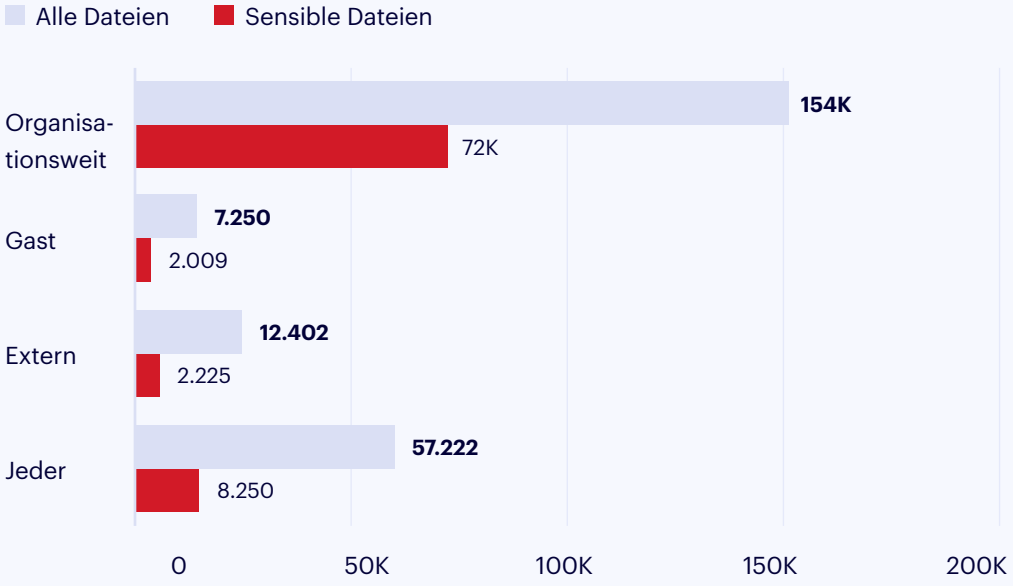
1,5K
sensible Aufzeichnungen werden extern offengelegt

Kollaborationsrisiko

Exposure-Level

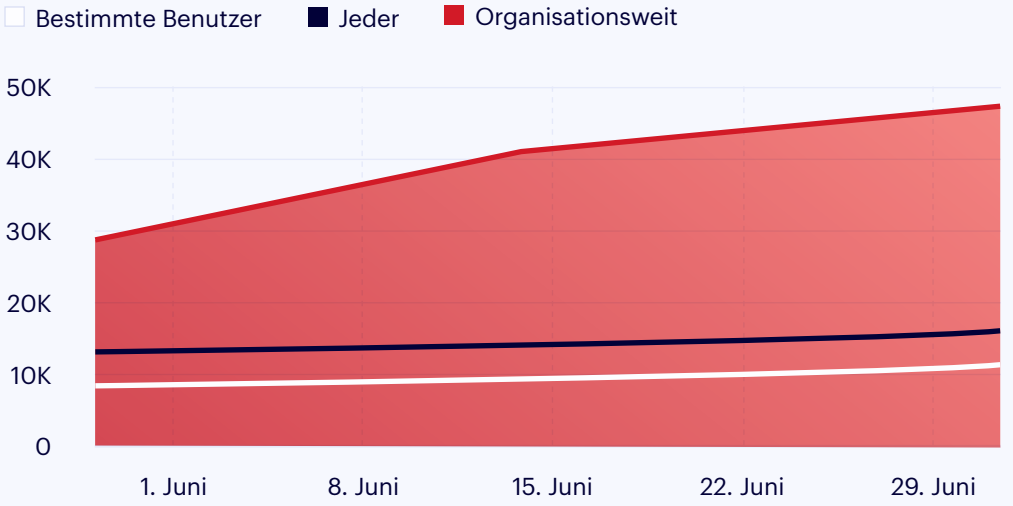
Das Teilen von Links ist hilfreich für die Zusammenarbeit, aber sie können diese Daten für jeden im Unternehmen, für Gastbenutzer oder für das Internet zugänglich machen. Die Umbrella Corp. ist aufgrund von Verknüpfungen in SharePoint und OneDrive in erheblichem Umfang sensiblen Daten ausgesetzt.

SharePoint Online und OneDrive



Wachstum von Freigabelinks

Der schädliche Radius von Umbrella Corp. wächst von Woche zu Woche explosionsartig. Nachfolgend finden Sie eine Grafik des Link-Wachstums nach Typ während des Risikobewertungszeitraums.



Daten öffentlich zugänglich gemacht

Daten, die über frei zugängliche Links öffentlich zugänglich gemacht werden

Nachfolgend finden Sie eine kleine Auswahl vertraulicher Dateien, auf die jeder im Internet zugreifen kann. Der Varonis-Audit-Trail zeigt die Art der Daten in der Datei (PCI, PHI usw.) an, wer den Link wann freigegeben hat und ob über den Link auf die Datei zugegriffen wurde.

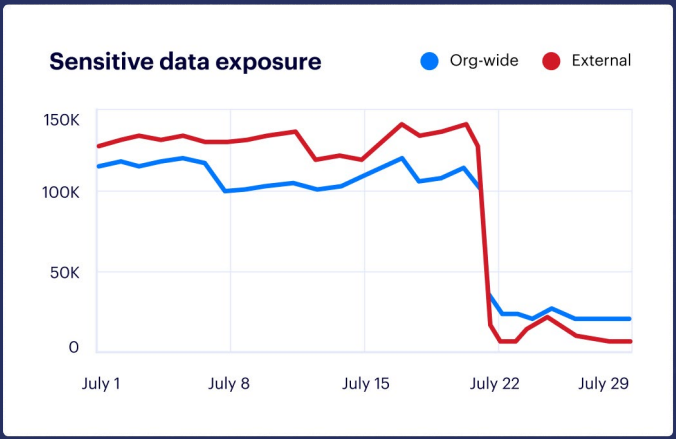
	File type	Name (resource)	Classification category	Total record
1		JV costs for Feb-Apr.xls	*Credentials (6)	28
		JV costs for Feb-Apr.xls	*Credentials (4)	22
		Transaction-English-06.xsl	*Credentials (4)	22
		GL Entry.ppt	*Credentials (4)	22
2		Employee Agreement.docx	*Financial (3)	21
		Employee Agreement.docx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

1 Tabellen mit Zugangs- und Kreditkartendaten

2 Arbeitsverträge mit personenbezogenen Daten und Bankkontoinformationen

Wie schnell können wir das Risiko geteilter Links beheben?

Ein typischer Varonis-Kunde kann Daten-Exposure durch Automatisierung schnell eliminieren. Im Folgenden sind die Ergebnisse eines großen Finanzinstituts aufgeführt, das eine Automatisierung des Least-Privilege-Prinzips aktiviert hat. Knapp 100 % der externen und unternehmensweiten Daten-Exposure wurde in weniger als 30 Tagen eliminiert.



Automatisierungsrichtlinien halten das Risiko angesichts des Datenwachstums und der kontinuierlichen Zusammenarbeit gering. Wenn Richtlinien so eingestellt sind, dass sie automatisch erzwungen werden, werden neue Risiken behoben, sobald sie auftreten, und das Least-Privilege-Prinzip wird kontinuierlich erzwungen.

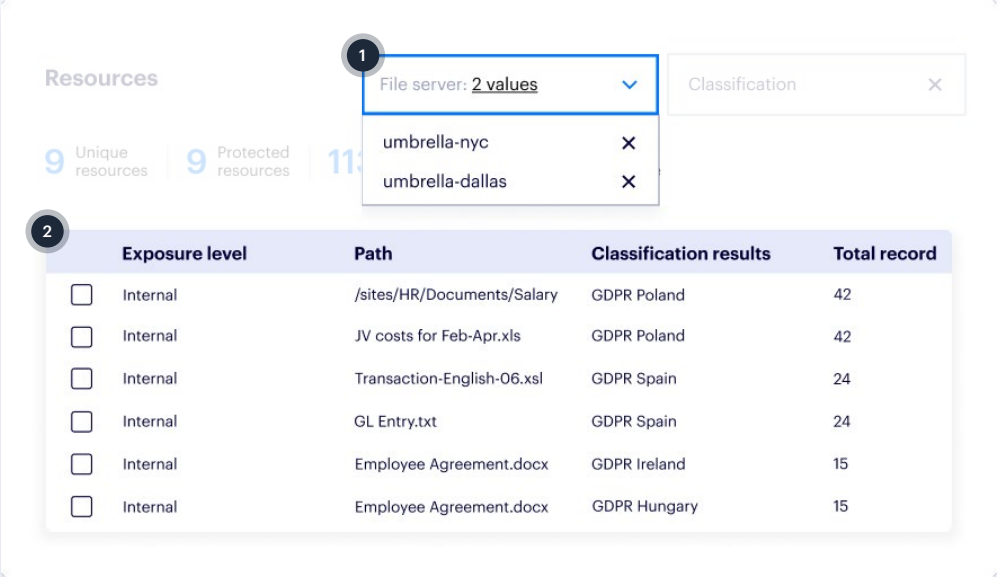
Falsch platzierte und falsch beschriftete Daten

Falsch platzierte Daten: Risiko für die DSGVO-Compliance

Varonis entdeckte personenbezogene Daten von EU-Bürgern auf einem in den USA gehosteten M365-Tenant. Die Dateien wurden am 15. Juli von einem Servicekonto namens „ExportJob“ hochgeladen, das anscheinend mit einer automatisierten Aufgabe von Workato verbunden ist. Wir empfehlen, diese Daten auf den in der EU ansässigen Tenant von Umbrella Corp zu migrieren und die automatisierte Aufgabe anzupassen.

1 M365-Tenant mit Sitz in den USA

2 Dateien mit personenbezogenen Daten von EU-Bürgern



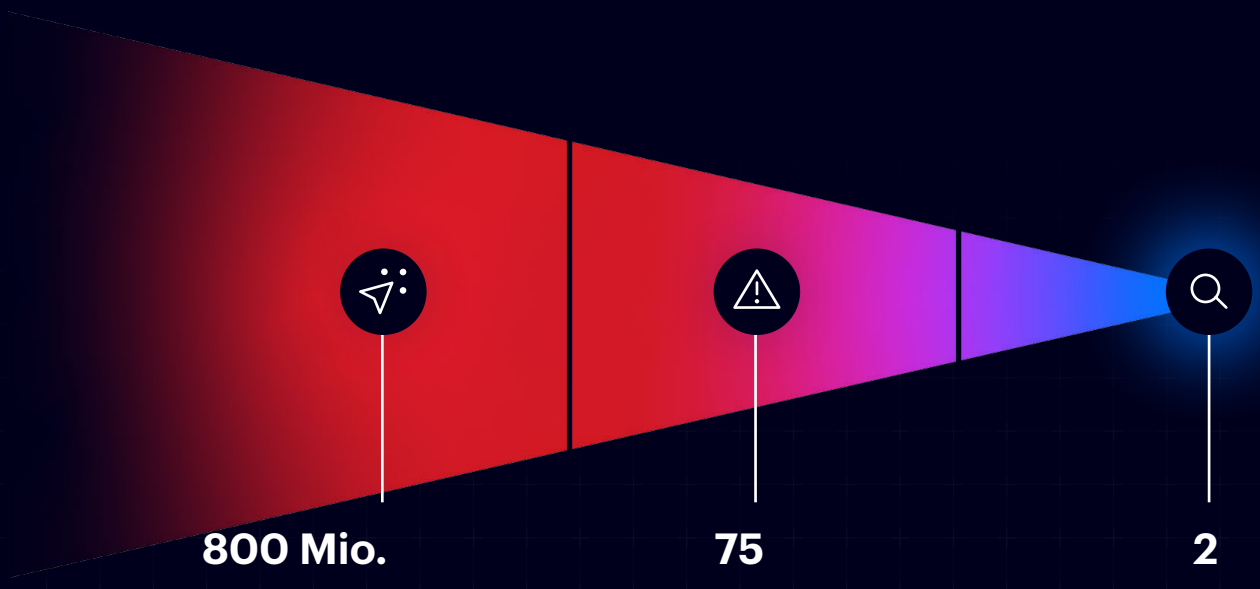
Falsch gekennzeichnete Dateien: DLP-Durchsetzungslücke

In vielen Dateien fehlen MIP-Label oder sie haben veraltete, falsch angebrachte Label. Infolgedessen kann die nachgelagerte DLP-Durchsetzung fehlschlagen, was zum Verlust sensibler Daten führen kann oder umgekehrt – Benutzer werden daran gehindert, nicht-sensible Daten, die falsch gekennzeichnet sind, weiterzugeben.

Wir haben mehr als 27.000 vertrauliche Dateien gefunden, denen kein Label zugewiesen wurde.

Bedrohungserkennung und -bekämpfung

Varonis-Echtzeitüberwachung und verhaltensbasierte Bedrohungserkennung wurden für jedes betroffene System aktiviert. Während des Bewertungszeitraums wurden unsere KI-Modelle anhand von mehr als 800 Millionen Ereignissen trainiert, um das einzigartige Verhalten von Benutzern und Geräten in der Umgebung von Umbrella Corp. zu lernen.



800 Mio.

Hunderte Millionen erfasster Ereignisse

Jedes Ereignis wird automatisch angereichert und normalisiert.

75

Dutzende Alerts ausgelöst

Durchschnittlich ~3 pro Tag

2

Eine Handvoll Vorfälle wurden untersucht

Varonis Proactive-Incident-Response hat zwei Vorfälle entdeckt und eskaliert.

Datenzentrierte UEBA

Ereignisse werden mit Daten, Benutzern und Gerätekontext angereichert. Sicherheitsanalysten können Abfragen wie die folgenden durchführen: „Listen Sie alle Ereignisse für den Zugriff auf sensible Daten durch privilegierte Konten von Geräten auf, die von Deutschland aus verbunden sind."

Erkennung von Konten

Zuordnung von IP zu Gerät

Operation durch	Kontotyp	Objekt	Vertraulich?	IP-Adresse des Geräts	Gerätename	Externe IP-Adresse	Geolocation
Amy Johnson	Führungskraft	Customer.xlsx	Ja	173.17.33.3	aj-03154	54.239.13.2	Kanada

Vertraulichkeit von Dateien

Geolocation

BEDROHUNGSANALYSE

Vorfallbericht: Kompromittiertes Servicekonto

Beobachtung:
Das Varonis IR-Team stellte fest, dass ein Backup-Servicekonto kompromittiert wurde und auf Benutzerdaten zugegriffen wurde.

Abnormal service behavior: access to atypical folders containing GDPR data

Exfiltration | 06/11/2023 8:19 PM | **Status:** Open | **Alert ID:** 123F...

What happened

BackupService File opened shared folder C:\Share\Finance\Controllers\Financereports.

A service account assessed folders containing GDPR data it has not accessed previously. Service accounts can be expected to perform the same actions repeatedly; therefore, a behavioral change is suspicious. Attackers may impersonate a service account and exploit its privileges.

Schadensbegrenzung:
Varonis IR hat den Vorfall innerhalb von wenigen Minuten untersucht und behoben. Das Konto UC\BackupService wurde sofort deaktiviert, aktive Sitzungen wurden beendet und das Passwort wurde zurückgesetzt. Varonis hat dem Team von Umbrella Corp einen vollständigen Untersuchungsbericht mit Ursachenanalysen und Empfehlungen vorgelegt.

Drilldown:
Auf 142 Dateien wurde vom gefährdeten Konto zugegriffen. 82 dieser Dateien wurden von Varonis als vertraulich eingestuft.

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...

KONFIGURATIONRISIKEN

Varonis scannt kontinuierlich die Systemkonfigurationen auf den SaaS- und IaaS-Plattformen von Umbrella Corp, um festzustellen, ob irgendwelche Einstellungen riskant sind oder ob Konfigurationen ihren gewünschten Status verloren haben.

21 Fehlkonfigurationen entdeckt

Salesforce hat die meisten Fehlkonfigurationen (8).

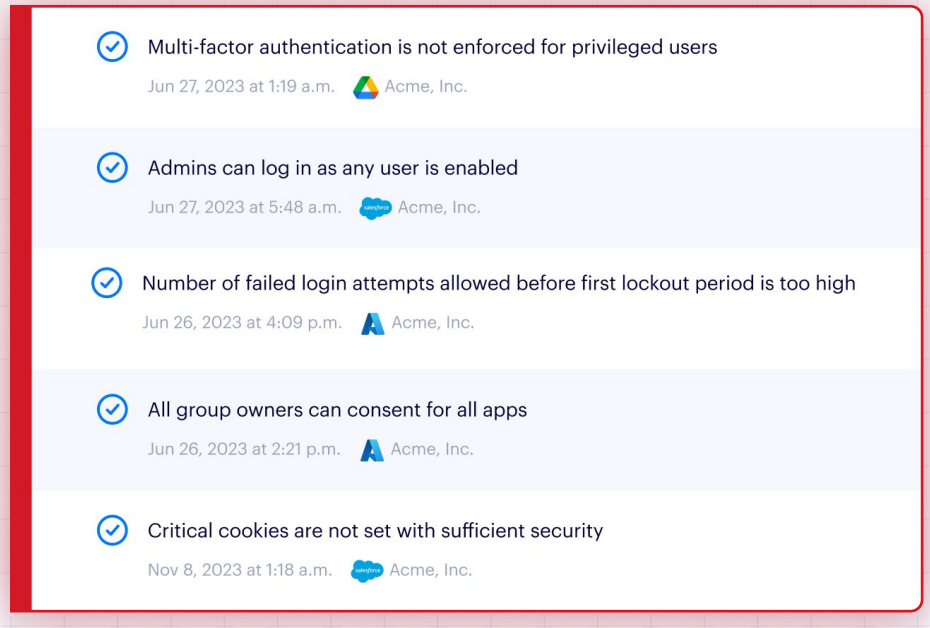
5 schwerwiegende Fehlkonfigurationen

M365 und Salesforce weisen jeweils zwei kritische Fehlkonfigurationen auf.

4 Konfigurationen mit automatischer Durchsetzung

Varonis kann automatisch sichere Einstellungen erzwingen.

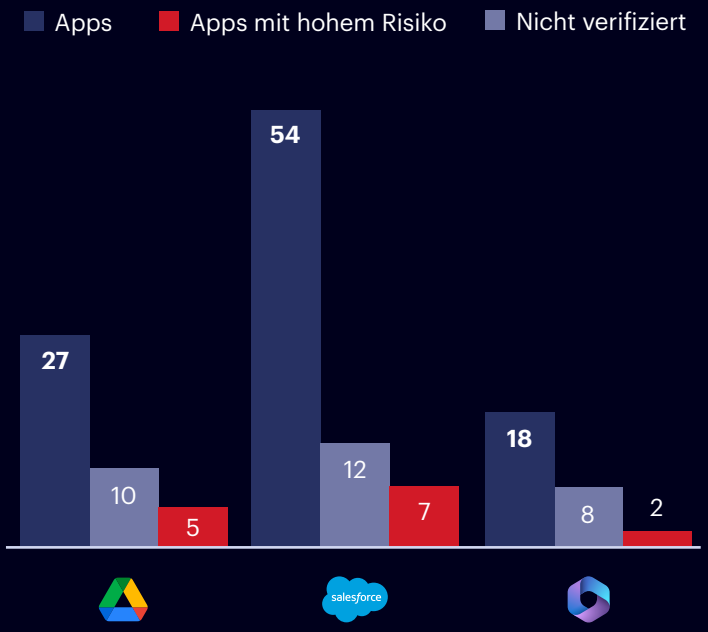
Im Folgenden finden Sie eine Zusammenfassung der fünf schwerwiegenden **Fehlkonfigurationen,** die bei der Bewertung entdeckt wurden. Vollständige Informationen und Empfehlungen für jeden einzelnen finden Sie in der Varonis-Benutzeroberfläche.



Klicken Sie hier, um weitere Beispiele für SaaS- und LaaS-Konfigurationen zu sehen, die Varonis überwachen kann.

RISIKO VON DRITTANBIETER-APPS

Wir haben 36 Apps von Drittanbietern identifiziert, die riskant, inaktiv oder nicht verifiziert sind.



99
Installierte Anwendungen von Drittanbietern

14
hohes Risiko mit umfassendem Datenzugriff

22
Inaktive Apps

Hier ist eine Aufschlüsselung der vier wichtigsten Drittanbieter-Apps nach Benutzeranzahl, die in die von Varonis überwachten SaaS-Plattformen integriert sind:

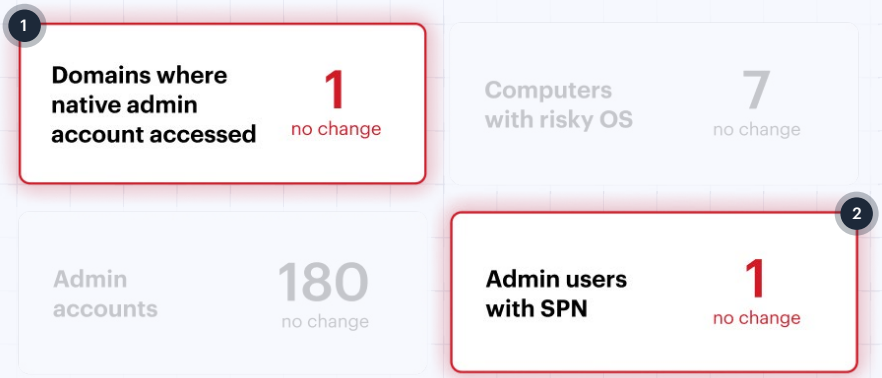
Google	Salesforce	Microsoft 365
miro	6sense	
dialpad	HubSpot	slack
Signeasy	INCENT	Trello
SUPERMETRICS	Power BI	Evernote

Darüber hinaus haben wir 111 inaktive Benutzer entdeckt, deren App-Zuweisungen direkt über die Varonis-Benutzeroberfläche widerrufen werden können.

IDENTITÄTSRISIKO

Sicherheitsstatus von Active Directory

Varonis scannt Umbrella Corps Cloud- und On-Premise-Directory Services und erkennt schwache Konfigurationen, die von Angreifern ausgenutzt werden können. Diese Risiken werden in Echtzeit auf Ihren Varonis-Dashboards aktualisiert und helfen dabei, AD Hardening-Bemühungen zu priorisieren.

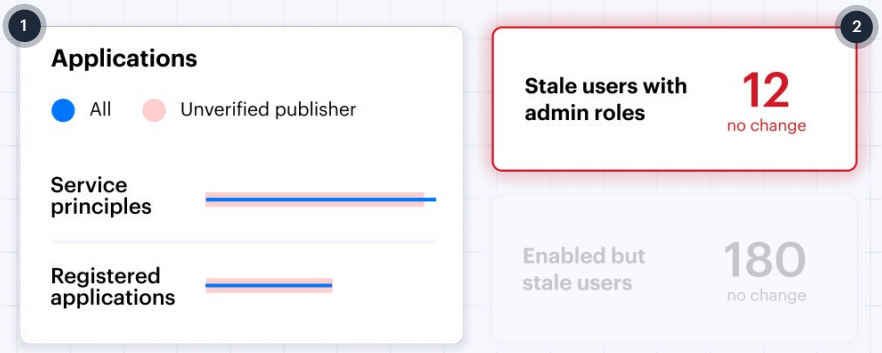


1 Es kommt selten vor, dass dieses Konto unter normalen Umständen verwendet wird. Dies könnte auf eine Kompromittierung hindeuten.

2 Anfällig für das Knacken von Offline-Passwörtern

Sicherheitsstatus von Entra ID (Azure AD).

Der Status von Entra ID wird von Varonis kontinuierlich überwacht und bewertet. Riskante Fehlkonfigurationen, die Ihre Daten gefährden, werden in Ihren Risiko-Dashboards und -Berichten angezeigt.



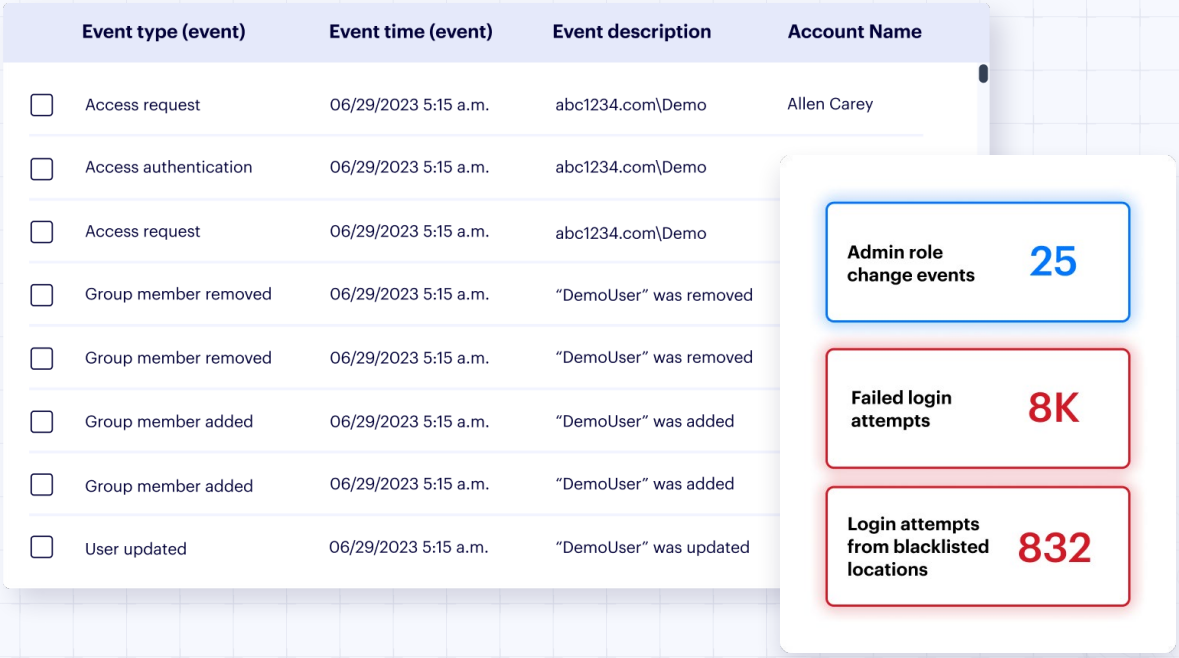
1 Überprüfen Sie die nicht verifizierte App-Berechtigung und den Datenzugriff.

2 Diese Konten sollten sofort deaktiviert werden.

Überwachung des Active Directory

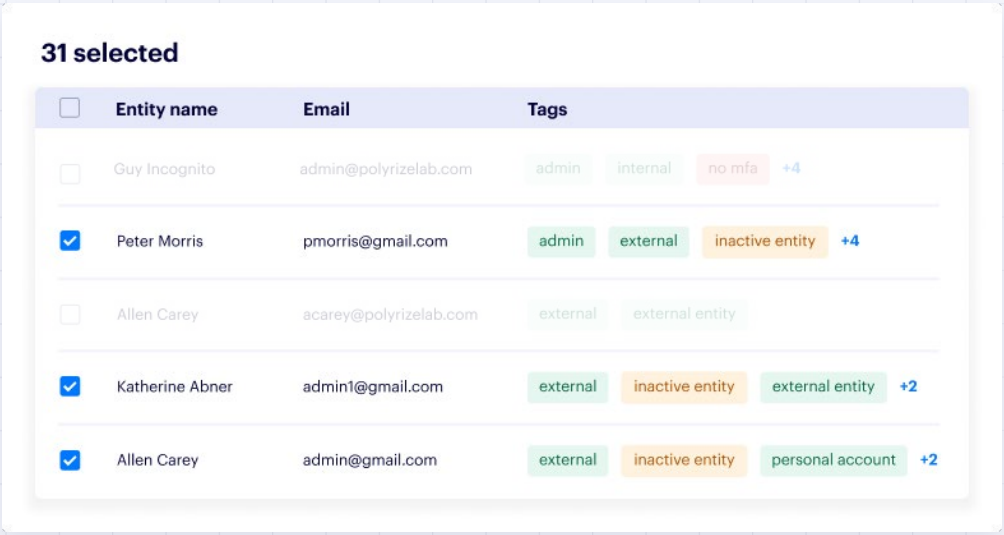
Varonis überwacht Ereignisse in den Directory Services von Umbrella Corp und korreliert diese Aktionen mit den datenzentrierten Ereignissen, die von Kollaborationsplattformen und Datenspeichern erfasst wurden.

Diese Änderungen wurden außerhalb des Fensters zur Änderungskontrolle vorgenommen.



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	

Riskante externe Benutzer und persönliche Konten



Gmail-Benutzerkonten sind veraltet, haben aber Zugriff auf vertrauliche Daten.

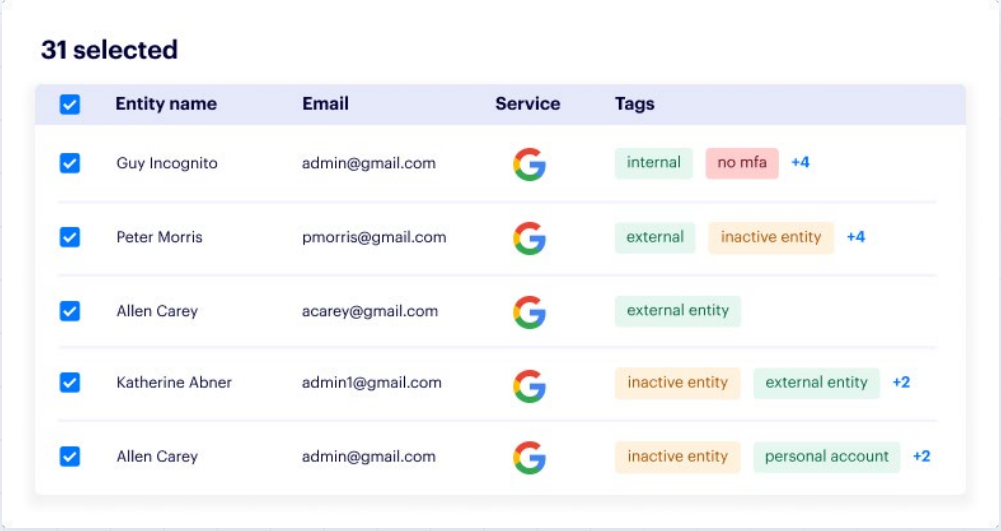
Verwandte Identitätszuordnung

Varonis identifiziert automatisch zugehörige Konten mithilfe eines proprietären Algorithmus. Guy Incognito ist ein Administratorbenutzer in Google Workspace, der ein persönliches Gmail-Konto ohne MFA verwendet. Er ist mit mehreren Identitäten in den Umgebungen der Umbrella Corp. verbunden.

Guy hat mehrere Aliase – eine Mischung aus Firmen- und Privatkonten.

Offboarding-Lücken: inaktive Konten

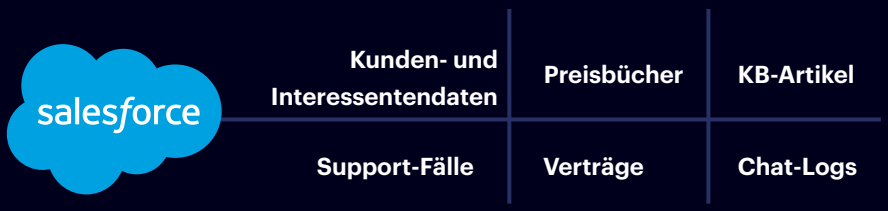
Varonis fand über 3.000 veraltete Identitäten in den Directory Services und lokalen Konto-Repositorys von Umbrella Corp.



Auftragnehmer behalten auch nach Ablauf der Verträge den Zugriff von ihren persönlichen Google-Konten aus.

SALESFORCE-RISIKO

Salesforce beherbergt die wertvollsten Daten eines Unternehmens, aber die komplexen Berechtigungsstrukturen und die mangelnde Übersicht darüber, wer auf diese Daten zugreifen kann, machen es zu einem Risiko für Insider- und Cyber-Bedrohungen.

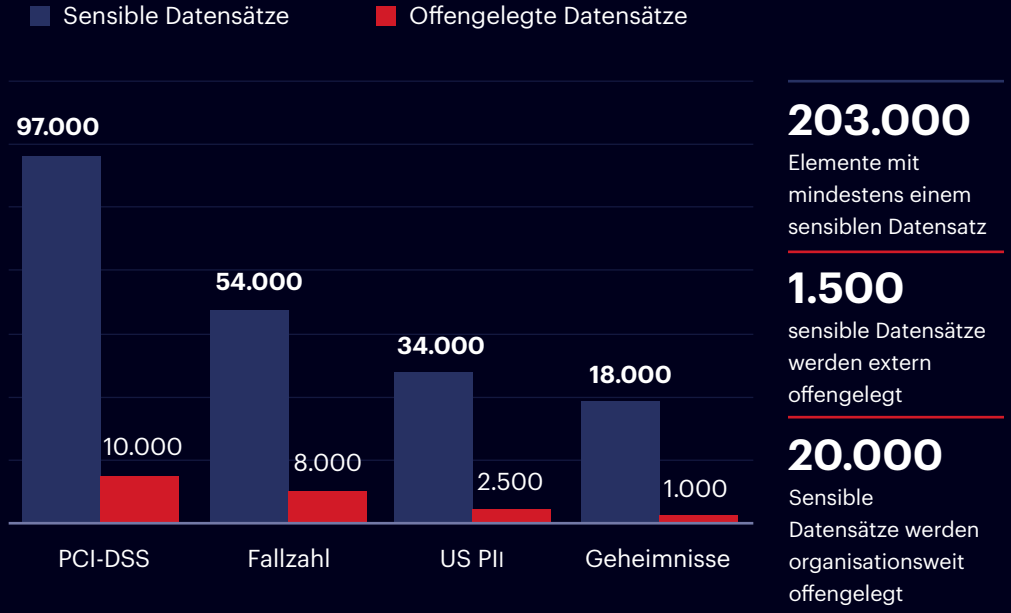


Umfang der Bewertung

Umgebungen	• Produktion • Sandbox	• Dev
Daten	• 234.240 Datensätze • 8.241 Dokumente • 520 Felder • 9.214 sensible Ressourcen	• 203 externe/öffentliche freigegebene Datensätze • 22 überwachte Apps von Drittanbietern
Identitäten	• 2.012 interne Benutzer • 425 externe Benutzer • 124 Auftragnehmer	• 212 Gastbenutzer • 55 Super-Admins
Berechtigungen	• 89 Profile • 52 privilegierte Profile • 22 Community-Profile • 3 Gastprofile	• 55 Berechtigungssätze • 27 Berechtigungssatz-gruppen • 33 Rollen
Top 3 externe Domains	Gmail.com	Hotmail.com Proton Mail Protonmail.com

SALESFORCE DATEN-EXPOSURE

Welche Art von Daten befinden sich in Salesforce und welche Exposure haben sie?



203.000
Elemente mit mindestens einem sensiblen Datensatz

1.500
sensible Datensätze werden extern offengelegt

20.000
Sensible Datensätze werden organisationsweit offengelegt

Datenexfiltrationsrisiko von Umbrella Corp

Es gibt eine Handvoll unten beschriebener Berechtigungen, die als äußerst privilegiert gelten sollten. Wenn sie zu vielen Benutzern gewährt werden, können diese Rechte ein erhebliches Risiko für Daten-Exposure und Exfiltration darstellen.

235 Berechtigungen mit aktiviertem Exportbericht

Exportbericht ermöglicht es Benutzern, Daten direkt aus Salesforce zu exportieren. Falls erforderlich, sollte er auf Berechtigungssätze angewendet werden.

124 Berechtigungen mit aktivierter Option „Alle Daten anzeigen“ oder „Alle Daten ändern“.

Benutzer mit dieser Berechtigung können alle Daten innerhalb der Organisation anzeigen und ändern.

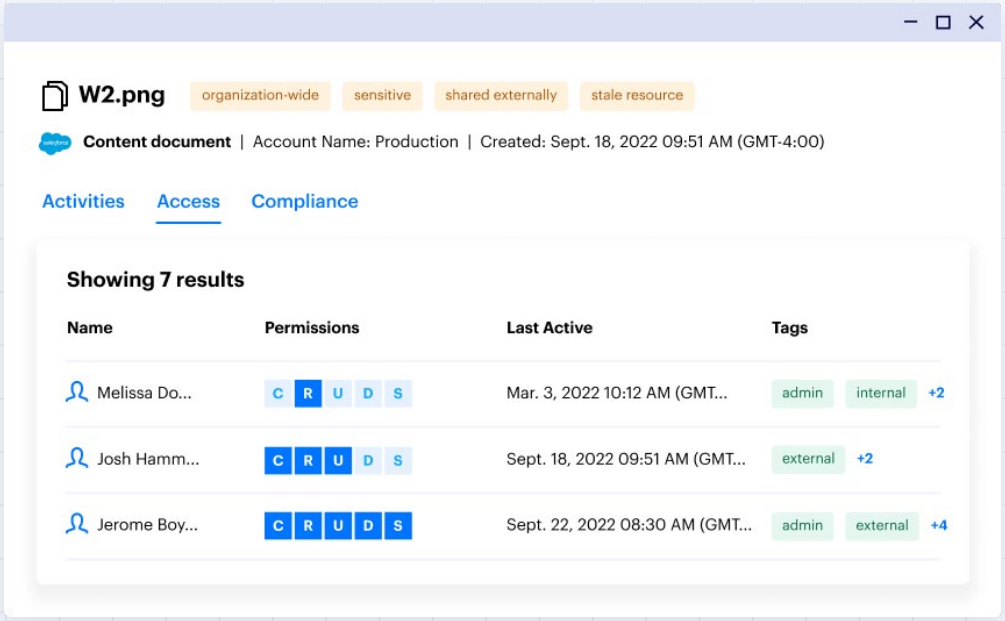
52 Berechtigungen mit aktivierter API

Ermöglicht Benutzern die Kommunikation mit allen Salesforce-APIs, das Exfiltrieren von Daten oder das Ausführen anderer Aktionen.

Varonis bietet Umbrella Corp einen Echtzeit-Überblick über kritische Berechtigungen und die Möglichkeit, die Zugriffsrechte schnell anzupassen und die geringsten Berechtigungen durchzusetzen. Wir empfehlen außerdem, Varonis-Alerts einzurichten, die ausgelöst werden, wenn sich diese privilegierten Berechtigungen ändern.

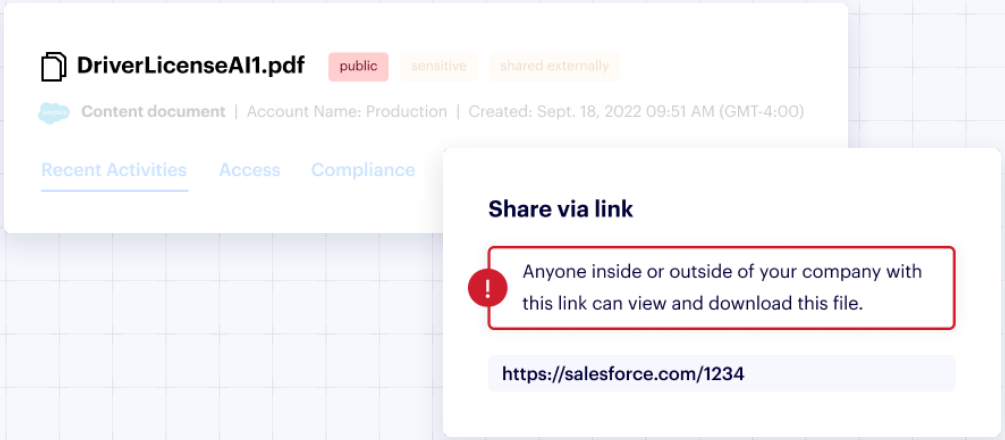
SENSIBLE DATEN WERDEN EXTERN GETEILT

Die Salesforce-Instanzen von Umbrella Corp ermöglichen Gastbenutzerzugriff. Es gibt auch mehrere Benutzerkonten, die als Servicekonten für Drittanbieter-Apps fungieren. Varonis hat mehr als 1.500 vertrauliche Datensätze erkannt, die extern offengelegt werden, wie z. B. den folgenden W2-Dateianhang.



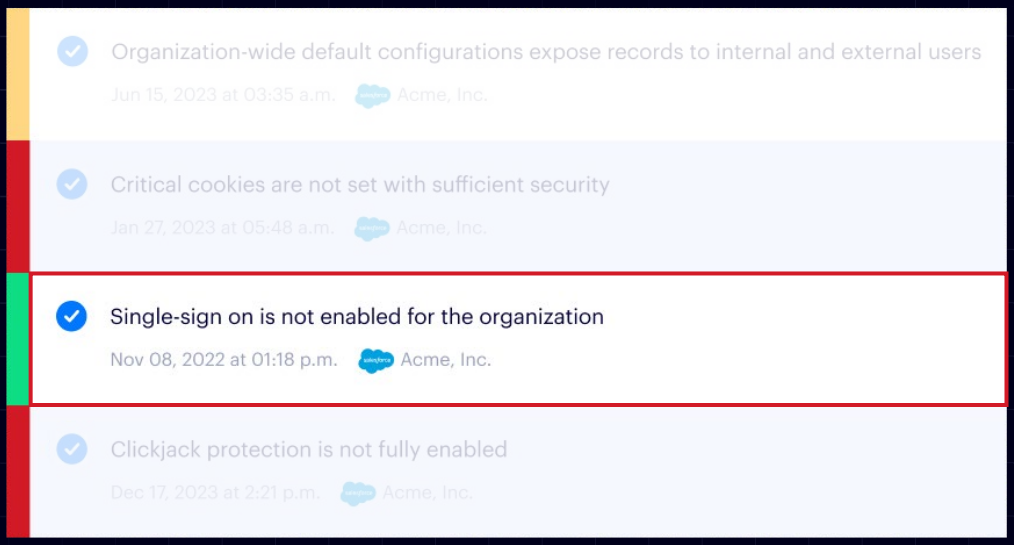
Benutzer außerhalb des Unternehmens können in Ihrer Salesforce-Instanz auf PCI- und PII-Daten zugreifen, diese aktualisieren oder löschen.

Zusätzlich zur Offenlegung von Daten für Gastbenutzer, Auftragnehmer und andere authentifizierte Dritte wurden bei unserer Prüfung auch Daten aufgedeckt, die über öffentliche Links ins Internet gelangen.



FEHLKONFIGURATIONEN VON SALESFORCE

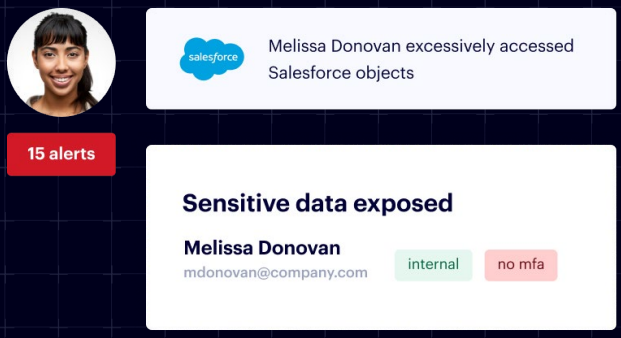
Varonis hat vier Fehlkonfigurationen oder unsichere organisationsweite Standardeinstellungen erkannt und behoben, die einen Angriffspfad darstellen könnten.



Gekündigte Auftragnehmer griffen auf das Sandbox-Konto zu, obwohl die Bereitstellung von Okta-Konten aufgehoben worden war.

Salesforce-Alarme

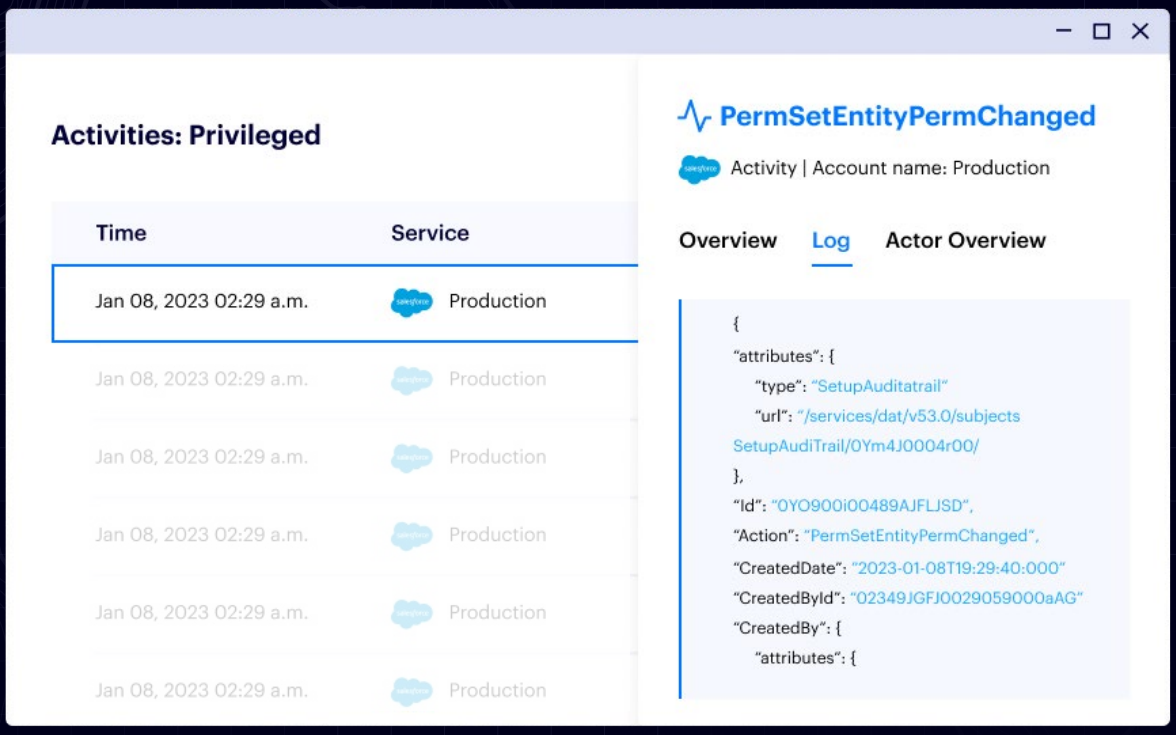
15 Alerts wurden von Varonis IR ausgelöst und behoben, darunter ein Fall, in dem die interne Melissa Donovan auf eine abnormale Anzahl von Datensätzen im Vergleich zu ihrem Ausgangsverhalten zugegriffen hat. Unsere Untersuchung zeigte, dass Melissa eine Browser-Erweiterung installiert hat, die schnell auf Salesforce-Datensatz-URLs zugreift.



Melissa Donovan ist von ihrer normalen Tätigkeit abgewichen – sie hat auf Aufzeichnungen zugegriffen, die sie normalerweise nicht nutzt.

Überwachen von Administratoränderungen

Josh Hammond hat außerhalb der Änderung mehrere administrative Änderungen der Produkten außerhalb des Fensters zur Änderungskontrolle vorgenommen. Nachfolgend finden Sie das detaillierte Änderungsprotokoll.

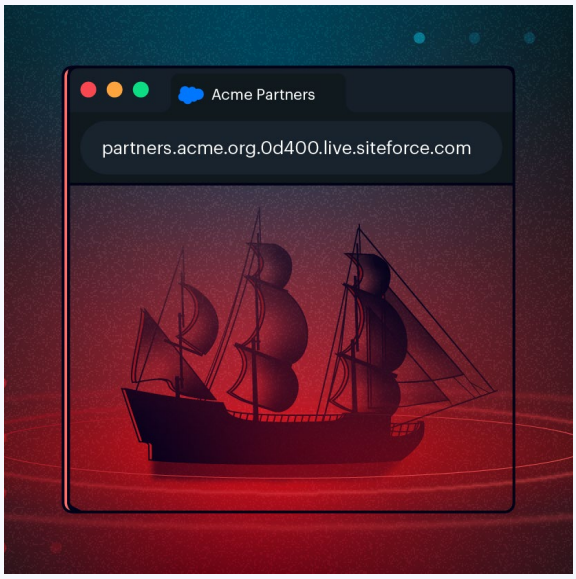


VARONIS
THREAT LABS

SALESFORCE-FORSCHUNG

Unser Team sucht nach Sicherheitslücken und schädlichen Konfigurationen in Salesforce und deckt sie auf.

Ghost Sites: Datendiebstahl aus deaktivierten Vertriebs-Communitys



Einstein's Wormhole: Erfassen von Outlook- und Google-Kalendern über den Gastbenutzer-Bug in Salesforce

Über Varonis Threat Labs

Unser Team aus Sicherheitsforschern und Datenwissenschaftlern gehört zu den besten Cyber-Security-Experten der Welt. Mit jahrzehntelanger Erfahrung in den Bereichen Militär, Nachrichtendienste und Unternehmen sucht das Team von Varonis Threat Labs proaktiv nach Schwachstellen in den von unseren Kunden genutzten Anwendungen, um Lücken zu finden und zu schließen, bevor Angreifer sie finden. All diese Erkenntnisse werden auf unsere Plattform programmiert, damit Sie Cyberangriffen immer einen Schritt voraus sind.

Informieren Sie sich über die neuesten Forschungsergebnisse: **www.varonis.com/blog/tag/threat-research**

VERRINGERN SIE IHR RISIKO, OHNE NEUE RISIKEN EINZUGEHEN.

Die Einrichtung unserer kostenlosen Risikobewertung dauert nur wenige Minuten und bietet sofortigen Mehrwert. In weniger als 24 Stunden haben Sie einen klaren, risikobasierten Überblick über die wichtigsten Daten und einen klaren Weg zur automatischen Sanierung.

Voller Zugriff auf die Varonis SaaS-Plattform

Erhalten Sie für die Dauer Ihrer Bewertung vollen Zugriff auf unsere Datensicherheitsplattform und erhalten Sie umsetzbare Erkenntnisse für Ihre wichtigsten Daten.

Engagierter IR-Analyst

Mit der Varonis SaaS Data Security Platform verbunden zu sein bedeutet, dass unsere Experten Ihre Alerts im Auge haben und wir Sie anrufen, wenn wir etwas Alarmierendes sehen.

Bericht über die wichtigsten Ergebnisse

Eine detaillierte Zusammenfassung Ihrer Datensicherheitsrisiken und eine Präsentation für Führungskräfte, um die Ergebnisse und Empfehlungen zu überprüfen. Dieser Bericht gehört Ihnen, auch wenn Sie kein Kunde werden.

Erhalten Sie eine kostenlose Risikobewertung

Tausende von Kunden vertrauen uns

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

VON FORRESTER ALS FÜHREND EINGESTUFT

Varonis wurde zum führenden Anbieter von Datensicherheitsplattformen ernannt.

„Varonis ist die erste Wahl für Unternehmen, die Wert auf umfassende Datentransparenz, Klassifizierungsfunktionen und automatisierte Behebung für den Datenzugriff legen."

Forrester Wave™: Data Security Platforms, Q1 2023

VON FORRESTER ALS FÜHREND EINGESTUFT

0 10 20 30 FÜR 40 50 60 70

VARONIS