



FORRESTER®

WAVE
LEADER 2023

Data Security Platforms

Automated Data Security Platform

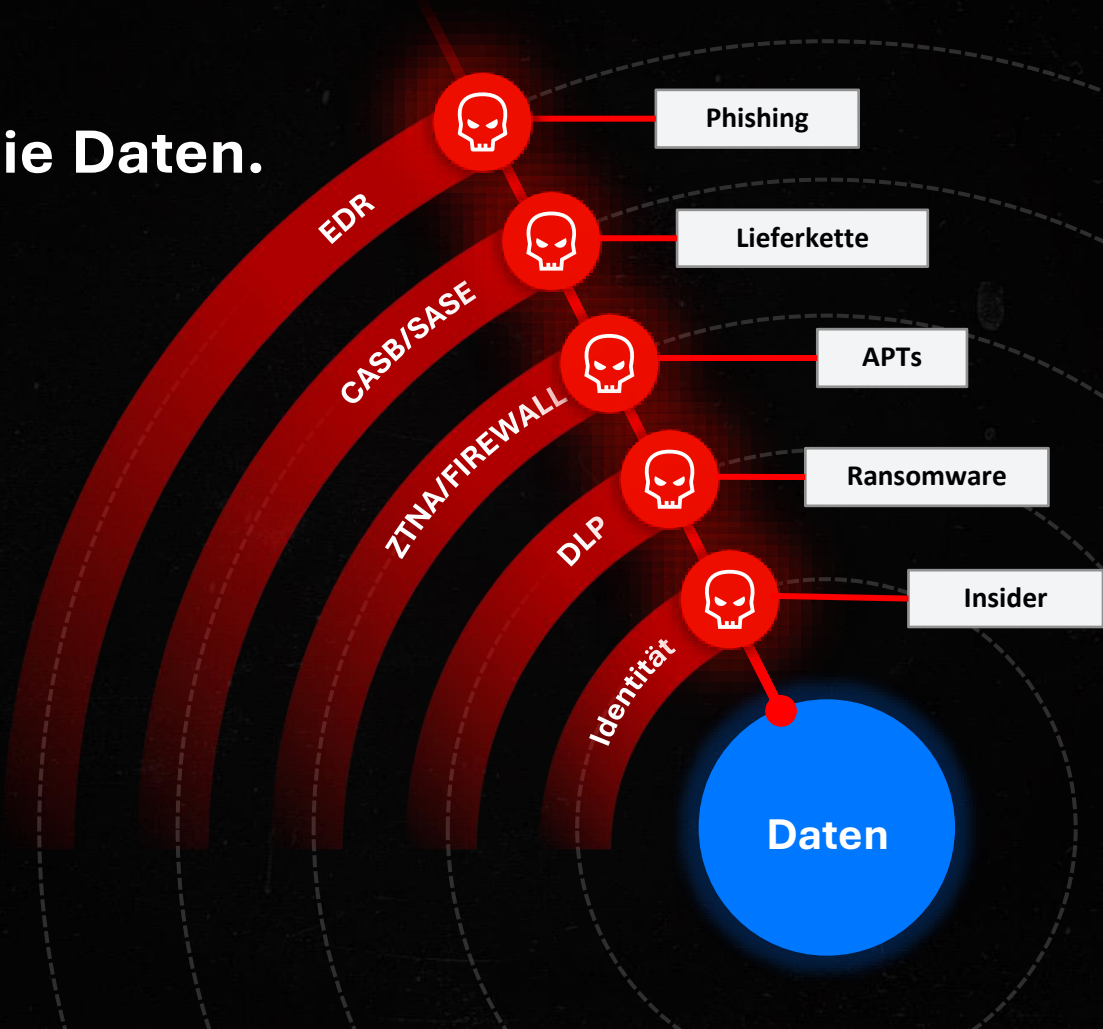
Continuously discover critical data, eliminate exposure, and stop threats without manual effort.

03.09.2024

Alles dreht sich um die Daten.

Für die meisten Unternehmen sind Daten ihr **wertvollstes** und **anfälligstes** Gut.

Daten sind **immer** das Ziel.



Der Blast Radius wächst unaufhaltsam.

Jährliches Datenwachstum **23 %** Microsoft 365 Copilot

Individuelle Berechtigungen zur Verwaltung **40 Mio.** ChatGPT

Für jeden Mitarbeiter zugängliche Dateien **17 Mio.** Einstein

Übliche Ansätze, Daten zu sichern



Native Kontrollen

Microsoft Purview
Integrierte Prüfung
Integrierte Zugriffskontrolle



Punktuelle Lösungen

Klassifizierungs-Tools
Datenschutz-Tools
Auditing-Tools



Legacy-DLP

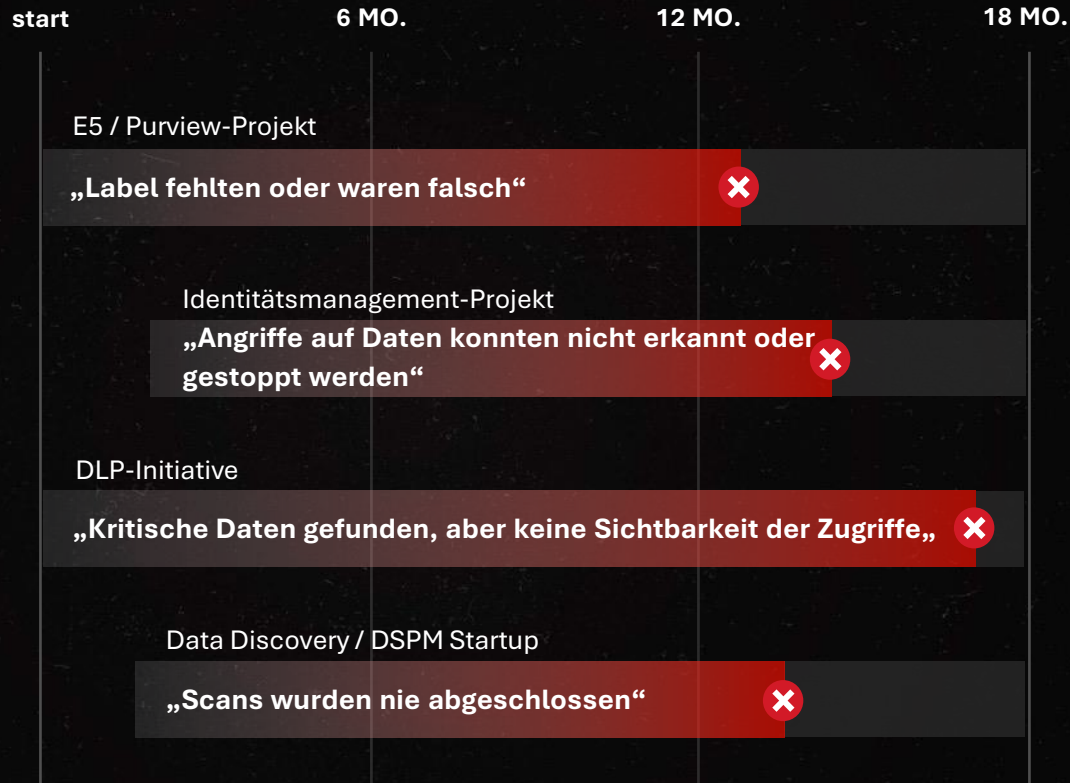
manuelles labeling
Inline blocking
Datei-für-Datei Remedierung

Wieso diese Projekte scheitern?

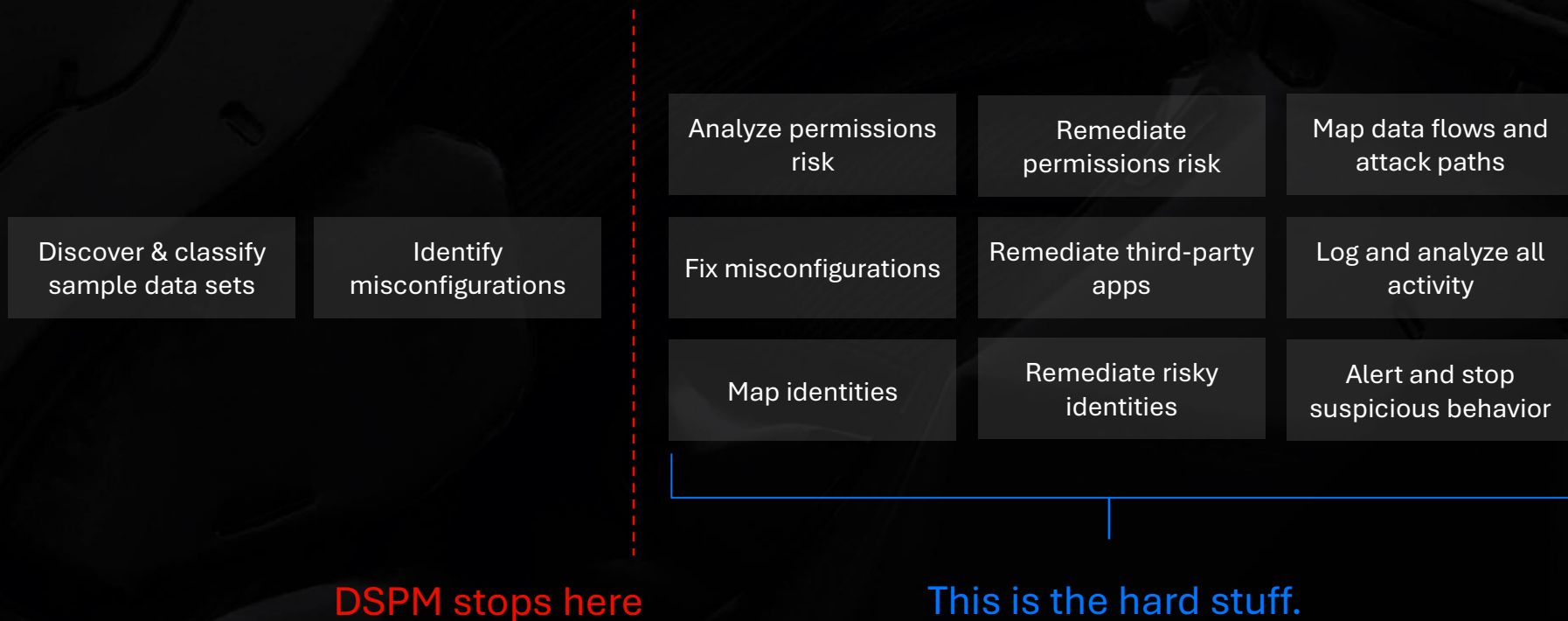
“

Wir haben 18 Monate damit verbracht, Daten ohne ein **messbares Ergebnis zu klassifizieren.**“

CISO, globales Finanzunternehmen



DSPM is the **easiest** part of the data security challenge.





“Varonis ist die **erste Wahl** für Unternehmen, die Wert auf umfassende Datentransparenz, Klassifizierungsfunktionen und automatisierte Behebung risikobehafteter Datenzugriffe legen.”

Forrester Wave™: Data Security Platforms, Q1 2023

Vollständig automatisierte Datensicherheit



Sichtbarkeit in Echtzeit

Verschaffen Sie sich in Echtzeit einen Überblick über Ihre Datensicherheit.



Automatisierte Prävention

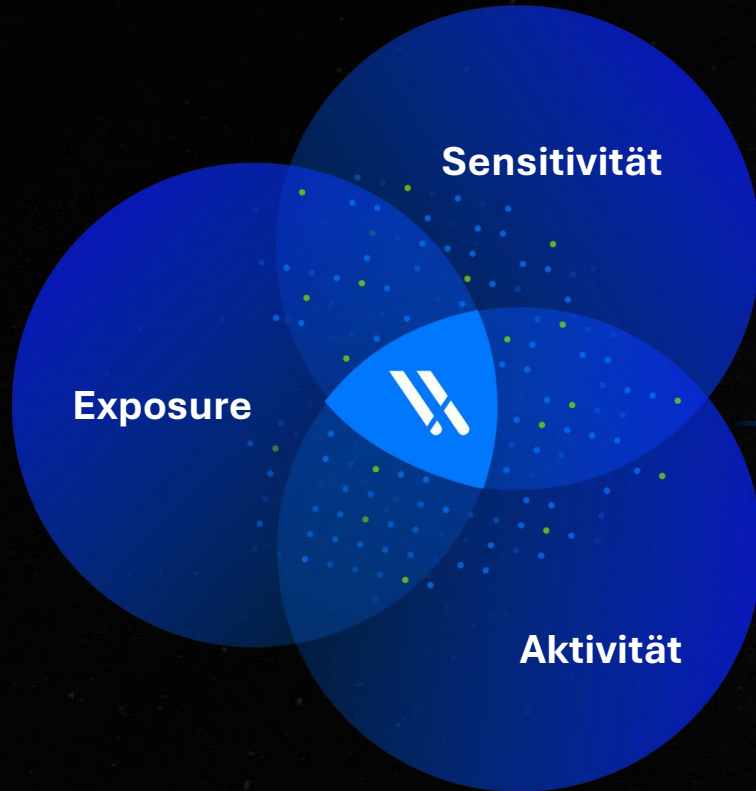
Verringern Sie kontinuierlich Ihren Blast Radius.



Proaktive Erkennung

Permanente, datenzentrierte UEBA + das Varonis IR-Team mit **24x7x365** Überwachung.

Sichtbarkeit in Echtzeit



Vollständig

Wir scannen *all* Ihre Daten, um Ihnen ein genaues Bild des Risikos zu geben.



Kontextuell

Wir wissen, wo sensible Daten offengelegt, mit Label versehen, veraltet oder angegriffen werden und beheben Risiken automatisiert.



Aktuell

Wir protokollieren alle Aktivitäten, um Bedrohungen zu erkennen und zu stoppen

Automatisierte Prävention

The screenshot displays the Varonis security console interface. At the top, there is a dropdown menu for 'Resource' set to 'prod1.sharepoint.com' and a 'Preview results' button. Below this are several filter sections:

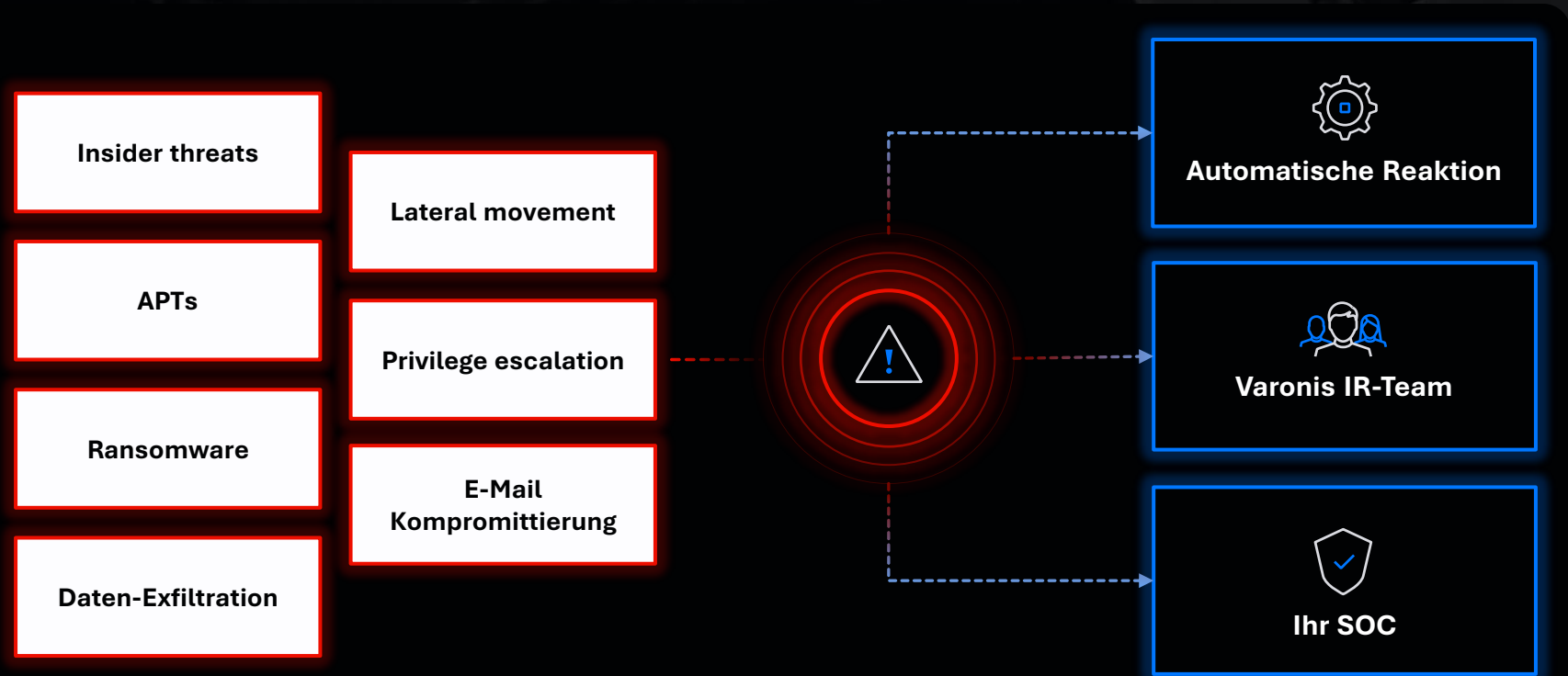
- Permission: dropdown menu
- Removal link: dropdown menu
- Yes: dropdown menu
- Permission: dropdown menu
- Link type: dropdown menu with options 'anyone on the internet' and 'org-wide'
- Resource: dropdown menu
- Sensitive (incl. subfolders): dropdown menu with options 'OneDrive' and 'SharePoint Online'

There is an '+ Add filter' button below the filters. Under the 'Actions' section, there is a blue bar with a 'Remove permission' button. Below that, there is an 'Execute actions' dropdown menu set to 'Continuously'. To the right, there is a line graph titled 'Org-wide sharing links' showing a sharp increase in activity starting in June, peaking in July, and then dropping to zero in August.

Richtlinien zur automatischen Verringerung der Risiken:

- ✓ Übermäßigen Zugriff widerrufen
- ✓ Fehlkonfigurationen finden
- ✓ Labels korrigieren
- ✓ Apps von Drittanbietern deaktivieren
- ✓ Deaktivierung von inaktiven Benutzern

Proaktive Erkennung



Eine Plattform für Multi-Cloud, SaaS & On-Premise

Dateispeicher



Windows



Azure Blob



NetApp



Nasuni



Nutanix



Unix/Linux

SaaS & E-Mail



Salesforce



Google Drive



Box



Microsoft 365



Teams



GitHub

IaaS & -Datenbanken



AWS



Azure



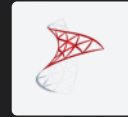
Snowflake



Databricks



MySQL



MS SQL

Identität

Endgerät

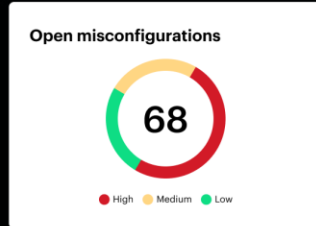
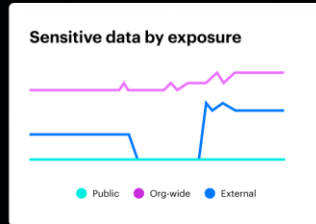
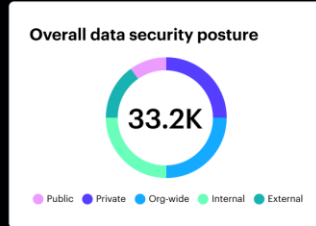
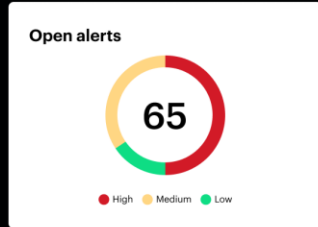
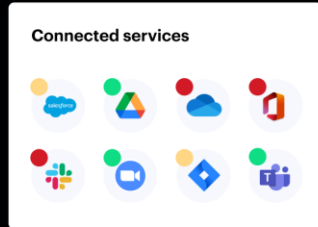
Netzwerk

Apps von
Drittanbietern

APIs

Gesamte Abdeckung
anzeigen

Wie wir beginnen: Kostenfreie Risikobewertung



Zuordnung der wichtigsten Datenspeicher

- Ermöglichen Sie den vollständigen Zugriff auf die Plattform
- Analysieren von Berechtigungen, Identitäten und Konfigurationen
- Daten entdecken und klassifizieren

Datennutzung überwachen

- Aktion aktivieren
- Aussagekräftige, realitätsnahe Warnungen aktivieren
- Untersuchungen beschleunigen

Risiken priorisieren

Gefährdete sensitive Daten, gemeinsame Links, böswillige Administratoren

Risiken bei der Konfiguration von Active Directory und SaaS

Lücken bei der Einhaltung von Vorschriften

IR-Team einsetzen

- Einführung eines dedizierten IR-Analysten
- Optimieren Sie Warnungen nach Bedarf
- Sie über jede verdächtige Aktivität benachrichtigen



Name & Contact details