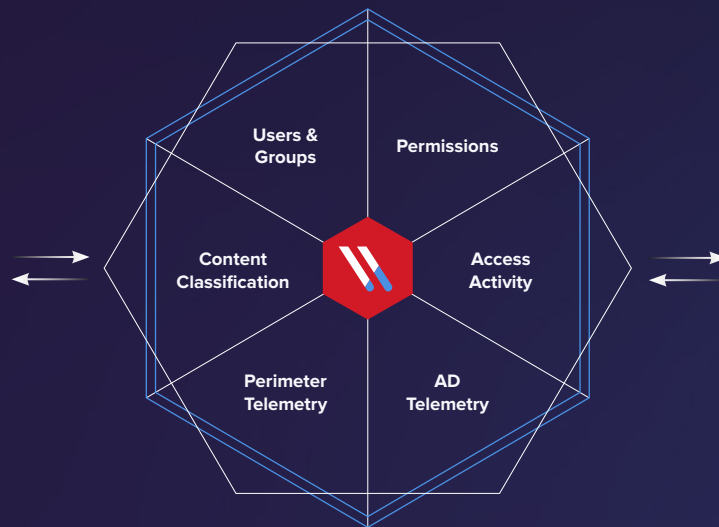# Data Security Platform

The most powerful way to find, monitor, and protect sensitive data on premises and in the cloud

Gain visibility into your critical data and infrastructure

Combine multiple data streams to discover security risks

Solve board-level data security problems at scale with automation

Users & Groups

Permissions

Content Classification

Access Activity

Perimeter Telemetry

AD Telemetry

Data Protection

Privacy & Compliance

Threat Detection & Response

"When you have to meet compliance regulations, gain visibility into your network, or protect your file shares, Active Directory, and Office 365 from potential threats, **Varonis is the all-in-one Swiss Army Knife you need.**"

IT Security Administrator, U.S. Federal Credit Union

READ THE CASE STUDY ›

The all-in-one Data Security Platform that won't slow you down

DatAdvantage
Data Audit & Protection

DatAdvantage maps who can (and who does) access data across file and email systems, shows where users have too much access, and safely automates changes to access control lists and groups.

Automation Engine
Automated Remediation

The Automation Engine safely removes open access at scale, dramatically reducing the attack surface in days, not years.

DatAlert
Security Analytics

DatAlert uses behavioral analytics to quickly detect and contain threats that other security solutions miss.

Edge
Perimeter Telemetry

Varonis Edge analyzes VPN, DNS, and web activity in context with data, email, and Active Directory behavior to detect threats such as brute force attacks, DNS cache poisoning, and data exfiltration.

DataPrivilege
Data Access Governance

DataPrivilege gives business users the power to review and manage permissions, groups, and access certification, while automatically enforcing business rules.

Data Classification Engine
Sensitive Data Discovery

The Data Classification Engine identifies sensitive and regulated data with built-in patterns, predefined categories, customizable regexes, and dictionaries.

Policy Pack
GDPR & CCPA Compliance

Policy Pack automatically identifies and classifies data that falls under the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Data Classification Labels
Policy Enforcement

Data Classification Labels automatically applies sensitivity labels in order to encrypt, obfuscate, or lock down your most important files.

DatAnswers
DSAR Compliance

DatAnswers enables rapid response to data subject access requests (DSARs) by surfacing personal information across cloud and on-prem files with fast and powerful search.

Data Transport Engine
Data Retention and Migration

Data Transport Engine automatically finds, moves, archives, quarantines, or deletes data based on content type, age, access activity, and more.

Try Varonis for free

All Varonis products are free to try and come with an engineer-led risk assessment.
The easiest way to get started is with a short 1:1 demo and discovery conversation.

CONTACT US

VARONIS

VARONIS

DatAdvantage Cloud

Say hello to the new standard in cloud security

Challenge

As companies boost their reliance on cloud services, securing sensitive data against cyberattacks and accidental overexposure becomes exponentially more complex. Each siloed cloud service has its own data types, permissions models, and activity log formats. The lack of unified visibility and control over data within SaaS and IaaS services leaves companies vulnerable to devastating breaches.

Solution

DatAdvantage Cloud correlates cross-cloud identities with privileges and activities across AWS, Google Drive, Box, Salesforce, Zoom, Okta, GitHub, Slack, and Jira. As a result, organizations can finally see and **prioritize their biggest cloud risks,** proactively **reduce their blast radius,** and conduct **faster cross-cloud investigations.**

Customer Success

"Being able to right size access and detect misuse in the **same platform** makes the security process easy to manage and provides protection when incidents occur."

CISO & DPO
Apps Flyer

READ THE CASE STUDY ›

Get deep SaaS & IaaS coverage
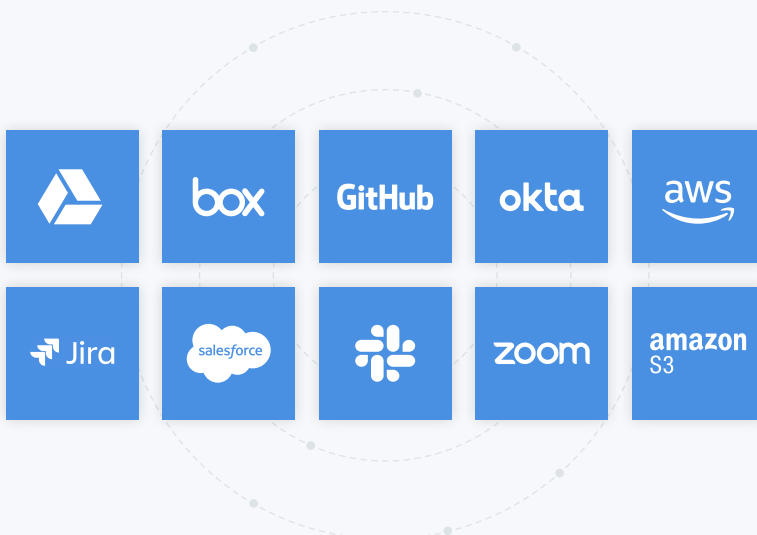
Cloud Risk Insights

43% of cloud users
are abandoned, sitting ducks for attackers

20% of cloud users
can access sensitive corporate data

15% of employees
move business data to personal cloud accounts

VARONIS

Reduce your blast radius

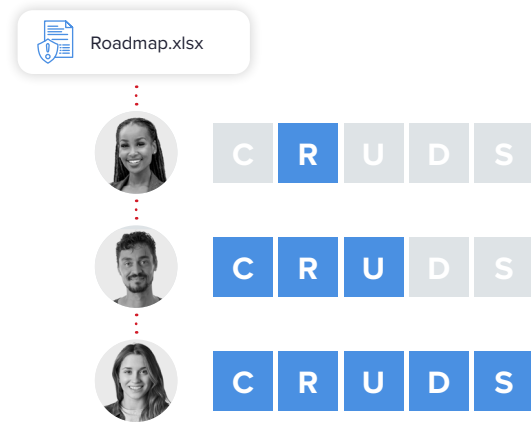DatAdvantage Cloud maps and normalizes permissions into to a simple create, read, update, delete, and share model (CRUDS) so you can proactively reduce your blast radius. Answer critical questions in a heartbeat:

- Who has access to our sensitive product roadmap?
- How are they getting access?
- What are they doing with it?

Roadmap.xlsx

	C	R	U	D	S

Conduct fast cross-cloud investigations

We standardize and enrich cloud events from all your cloud services, giving you simple answers to complex questions:

- Which external users have granted permissions in any SaaS app?
- Are any admins logging in without MFA?
- What config changes have watchlist users made across all our apps?

Actor	Service	Type
	Jira	Authentication
	aws	Access
	okta	User Management

Alert on suspicious activity and policy violations

Prevent cloud account takeovers, insider threats, and inadvertent policy violations with cross-cloud auditing and alerting. Use out-of-the-box alerts or create your own.

Insider Threat Indication
Anomalous Number of Account Records Accessed
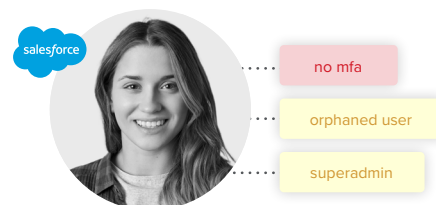
salesforce

no mfa
orphaned user
superadmin

Try Varonis for free

All Varonis products are free to try and come with an engineer-led risk assessment
The easiest way to get started is with a short 1:1 demo and discovery conversation.

CONTACT US

VARONIS

DATA RISK ASSESSMENT

Want to know where your biggest data security threats are?

Schedule a personalized
Data Risk Assessment

Our assessments are 100% obligation-free and non-intrusive.

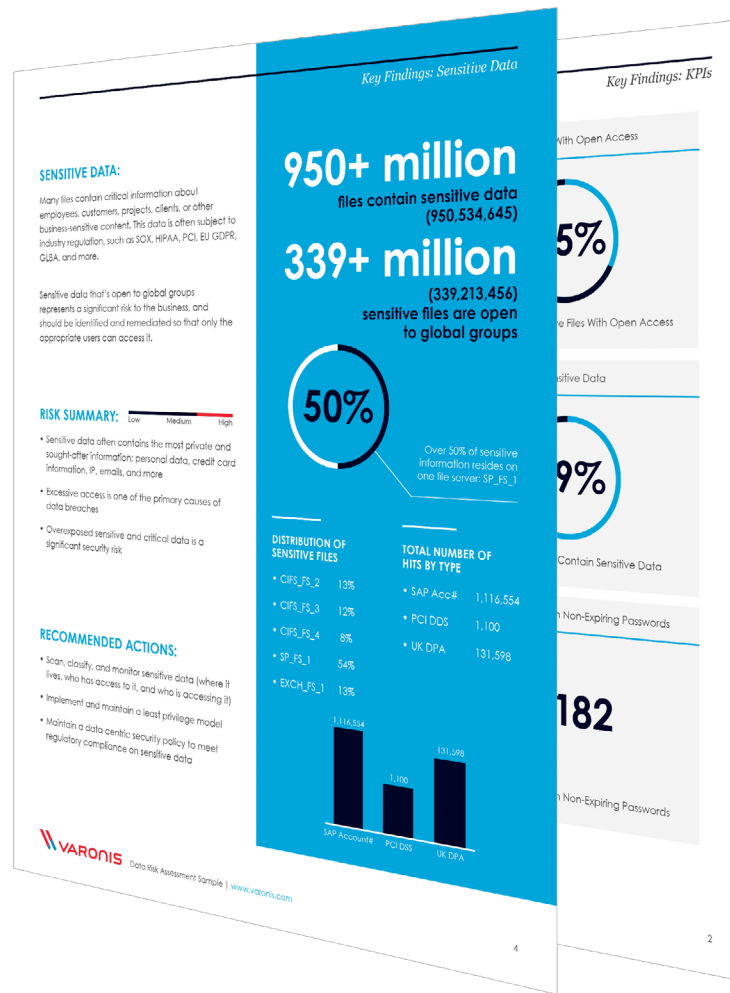A dedicated engineer will do all the heavy-lifting and you'll get a comprehensive report that highlights at-risk sensitive data, flags access control issues, and quantifies risk - so that when you're asked what you're doing to prevent becoming the next cybersecurity headline, you're already ahead of the game.

SCHEDULE NOW

SENSITIVE DATA:

Many files contain critical information about employees, customers, projects, clients, or other business-sensitive content. This data is often subject to industry regulation, such as SOX, HIPAA, PCI, EU GDPR, GLBA, and more.

Sensitive data that's open to global groups represents a significant risk to the business, and should be identified and remediated so that only the appropriate users can access it.

RISK SUMMARY: Low   Medium   High

• Sensitive data often contains the most private and sought-after information: personal data, credit card information, IP, emails, and more

• Excessive access is one of the primary causes of data breaches

• Overexposed sensitive and critical data is a significant security risk

RECOMMENDED ACTIONS:

• Scan, classify, and monitor sensitive data (where it lives, who has access to it, and who is accessing it)

• Implement and maintain a least privilege model

• Maintain a data-centric security policy to meet regulatory compliance on sensitive data

Key Findings: Sensitive Data

950+ million
files contain sensitive data
(950,534,645)

339+ million
(339,213,456)
sensitive files are open to global groups

50%

Over 50% of sensitive information resides on one file server: SP_FS_1

DISTRIBUTION OF SENSITIVE FILES

• CIFS_FS_2   13%
• CIFS_FS_3   12%
• CIFS_FS_4   8%
• SP_FS_1   54%
• EXCH_FS_1   13%

TOTAL NUMBER OF HITS BY TYPE

• SAP Acc#   1,116,554
• PCI DDS   1,100
• UK DPA   131,598

1,116,554

131,598

1,100

SAP Account#   PCI DDS   UK DPA

Key Findings: KPIs

VARONIS Data Risk Assessment Sample | www.varonis.com

4

2

Join thousands of enterprises
that **trust Varonis.**

WHAT WE DO

Our engineers will collect and analyze the metadata from your email, file systems, and directory services (AD, LDAP, NIS), discover and isolate in-scope infrastructure, and perform capabilities and environmental assessments. We'll build out a custom security assessment designed specifically for you: based on company needs, regulations, and configurations.

WHAT YOU GET

A detailed report based on your company data, analyzing risk, identifying strengths and weaknesses — and we'll help you fix real production security issu es while we're at it.

The data risk assessment will summarize key findings, expose data vulnerabilities, provide a detailed explanation of each finding, and include prioritized remediation recommendations.

HOW IT WORKS

We outline your problem areas — wondering about global access? Exposed sensitive data? Stale data? We got this. We'll prioritize risk, and give you concrete steps to take to improve your data security.

NON-INTRUSIVE

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

FAST AND HASSLE FREE

Our dedicated engineers will do all the heavy-lifting for you: setup, configuration, and analysis — with concrete steps to improve your data security.