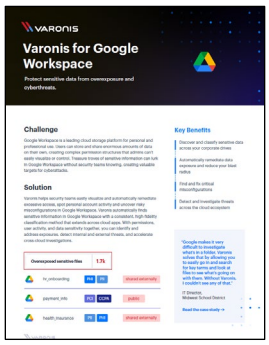


Varonis For Google Workspace

Thank you for downloading this Varonis Datasheet.

To learn how to take the next step toward acquiring Varonis solutions, please check out the following resources and information:

For additional resources:
carah.io/VaronisResources

For upcoming events:
carah.io/VaronisEvents

For additional Varonis solutions:
carah.io/VaronisSolutions

For additional cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Varonis@carahsoft.com
877-468-7962

To purchase, check out the contract vehicles available for procurement:
carah.io/VaronisContracts

Varonis for Google Workspace

Protect sensitive data from overexposure and cyberthreats.

Challenge

Google Workspace is a leading cloud storage platform for personal and professional use. Users can store and share enormous amounts of data on their own, creating complex permission structures that admins can't easily visualize or control. Treasure troves of sensitive information can lurk in Google Workspace without security teams knowing, creating valuable targets for cyberattacks.

Solution

Varonis helps security teams easily visualize and automatically remediate excessive access, spot personal account activity and uncover risky misconfigurations in Google Workspace. Varonis automatically finds sensitive information in Google Workspace with a consistent, high-fidelity classification method that extends across cloud apps. With permissions, user activity, and data sensitivity together, you can identify and address exposures, detect internal and external threats, and accelerate cross-cloud investigations.

Overexposed sensitive files	1.7k

hr_onboarding	PHI	PII	shared externally
payment_info	PCI	CCPA	public
health_insurance	PII	PHI	shared externally

Key Benefits

- Discover and classify sensitive data across your corporate drives
- Automatically remediate data exposure and reduce your blast radius
- Find and fix critical misconfigurations
- Detect and investigate threats across the cloud ecosystem

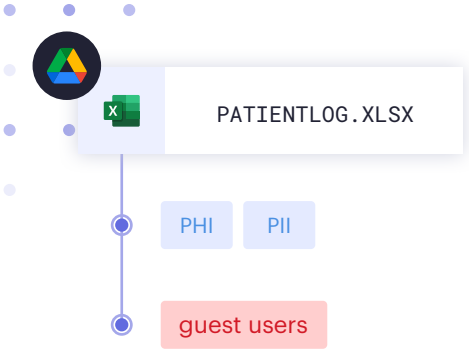
"Google makes it very difficult to investigate what's in a folder. Varonis solves that by allowing you to easily go in and search for key terms and look at files to see what's going on with them. Without Varonis, I couldn't see any of that."

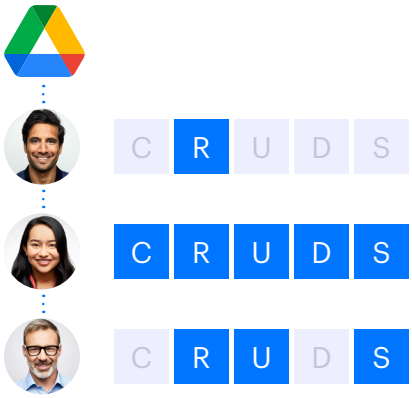
IT Director,
Midwest School District

Read the case study →

Discover and protect sensitive data in Google Workspace.

Varonis automatically discovers and classifies sensitive data in Google Workspace with pinpoint accuracy so you can find and fix your biggest data risks. See where sensitive data is open to too many people, monitor usage, and make smart decisions about how to quickly and safely reduce your risk.



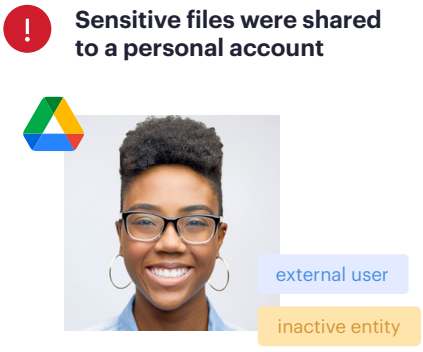


Proactively reduce sensitive data exposure.

Simplify Google Workspace's complex permissions and external sharing to prevent unauthorized access to sensitive data and permissions creep. Get a real-time, interactive view of effective data access, roles, and permissions. Quickly identify overexposed sensitive data and employ Varonis' least privilege automation capabilities to automatically and continuously remediate excessive permissions and reduce your blast radius.

Alert on suspicious user activity.

Protect your critical data from malicious actors with real-time alerts on suspicious login activity and abnormal data access in Google Workspace. Varonis monitors activity—file sharing, logins, permissions, and configuration changes—and correlates a user's Google Workspace activity to other SaaS apps, giving you a unified forensic audit trail.



Try Varonis for Google Workspace 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