VARONIS

Varonis for Amazon Web Services

Protect AWS identity management (IAM), storage (S3), and compute (EC2) solutions from threats.

aws partner network

Challenge

Amazon Web Services (AWS) is one of the world's most comprehensive and broadly adopted cloud platforms. However, the multitude of options for identity management, permission levels, and access controls, makes AWS resources extremely difficult to secure at scale. Native AWS security tools don't provide an easy way to enforce least privilege, uncover sensitive data exposure, and detect abnormal behavior.

Solution

Varonis offers a comprehensive solution to protect AWS identity (IAM), storage (S3), and compute (EC2) services from insider threats and cyberattacks. We identify where sensitive data lives within AWS, monitor for suspicious activity, detect and alert on public exposure, and spot misconfigurations. By integrating permissions, activity, and data sensitivity information, you can identify and address exposures, provide detections for internal and external threats, and accelerate cross-cloud investigations.

Cloud resources monitoring report

Service	Name	Type	Tags
aws	Vtest2 AWS	Account	content may be public
aws	acme-customers	Bucket	public
aws	acme-test-mc	Bucket	public

Key Benefits

- Discover and classify sensitive data stored in S3 buckets
- Prevent data exposure in AWS
- Detect and investigate threats in AWS and across the cloud ecosystem
- Find and automatically fix critical misconfigurations

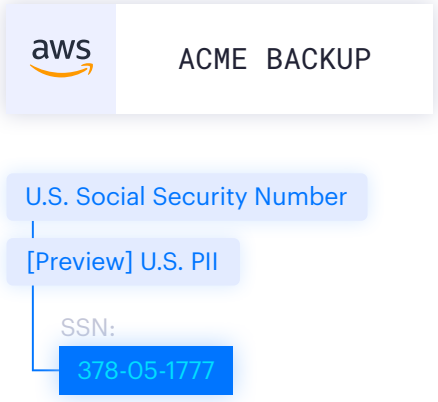
"Varonis' ability to provide cloud detection and response alerts on access abuse and misuse, insider threats, data leakage, and account takeovers across mission-critical cloud services was everything we asked for."

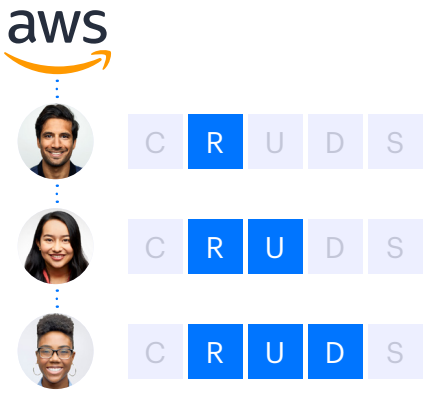
Ian Amit
Cimpress CSO

Read the case study →

Auto-classify sensitive AWS data.

Varonis scans every file stored in your AWS S3 buckets, flags the sensitive data within, and shows you exactly where it lives with an easy-to-read file tree. Easily customize your classification scope to optimize speed and processing power.





Limit exposure in AWS.

With several roles and permissions sets, AWS configurations are incredibly complex, making it difficult to spot and fix data exposure. Varonis maps, normalizes, and simplifies AWS permissions providing a real-time view of effective permissions and surfaces critical misconfigurations enabling you to quickly spot all the ways your data is exposed to risk. Discover and fix misconfigured, publicly exposed AWS buckets or EC2 instances, uncover privileged inline policies, and monitor identities to reduce your exposure and secure your sensitive assets.

Detect and investigate suspicious user activity.

Protect your critical data from malicious actors with notifications on abnormal activity, unauthorized access and risky misconfigurations. We connect identities across cloud platforms to provide a holistic view into a user's activity across the cloud ecosystem.

Try Varonis for AWS 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