DatAdvantage Cloud for Amazon Web Services

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

Challenge

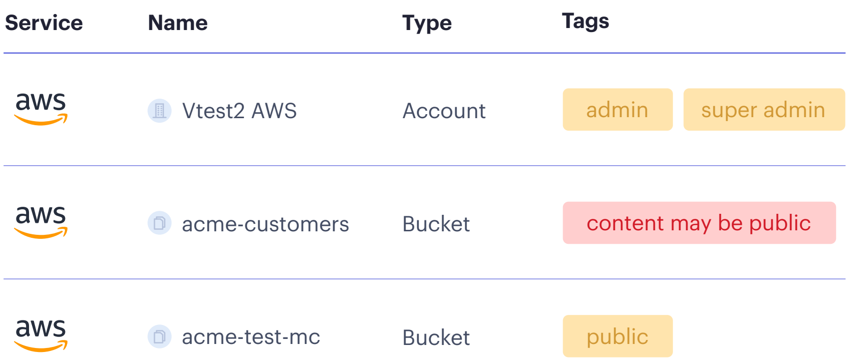
Amazon Web Services (AWS) is one of the world's most comprehensive and broadly adopted cloud platforms. However, the multitude of options for identity management, permission levels, and access controls, makes AWS resources extremely difficult to secure at scale. Native AWS security tools don't provide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

Solution

DatAdvantage Cloud offers a comprehensive solution to protect AWS identity (IAM), storage (S3), and compute (EC2) services from insider threats and cyberattacks. We monitor AWS environments for suspicious activity, alert on public exposure, and spot misconfigurations.

By integrating permissions, activity, and data sensitivity information, you can identify & 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	admin super admin
aws	acme-customers	Bucket	content may be public
aws	acme-test-mc	Bucket	public

Cloud risk insights

43%
of cloud users are abandoned, sitting ducks for attackers[1]

44%
of cloud user privileges are misconfigured[1]

3 / 4
identities of ex-contractors remain active[1]

> "DatAdvantage Cloud's 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."

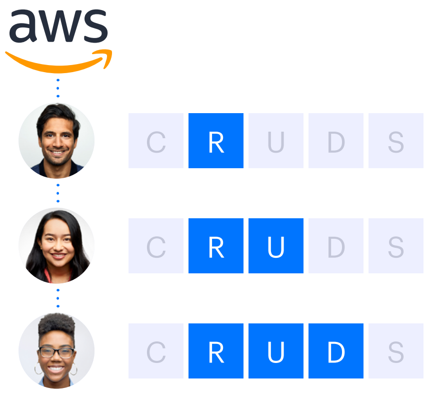
Ian Amit
Cimpress CSO

Read the case study →

[1] Varonis 2021 SaaS Data Risk Report

Limit exposure in AWS.

With several roles and permissions sets, AWS configurations are incredibly complex, making it difficult to spot and fix excessive data access. DatAdvantage Cloud maps and normalizes AWS permissions into a simple CRUDS (create, read, update, delete, and share) model, providing a real-time view into effective permissions. Discover misconfigured, publicly exposed AWS buckets or EC2 instances, uncover privileged inline policies, and monitor identities to reduce your exposure and secure your sensitive assets.



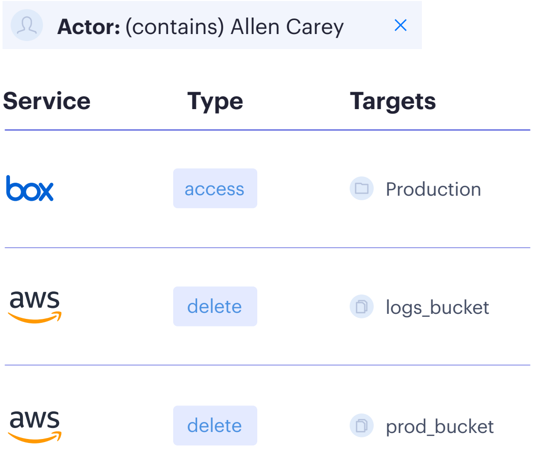
Excessive AWS S3 bucket deletion attempts
aws
privileged entity
inactive entry
no mfa

Alert on suspicious user activity.

Protect your critical data from malicious actors with notifications on abnormal activity and unauthorized access. Get alerts on risky misconfigurations, excessive bucket deletion attempts, or suspicious connection requests, and when stale admin accounts become active and begin accessing or sharing data.

Conduct fast cross-cloud investigations.

DatAdvantage Cloud makes investigations faster and more effective than with built-in AWS security capabilities alone because we enrich events and correlate identities across AWS services and cloud apps. Easily bundle cross-cloud activities to see things like all access management events or all authentication events, or sort and filter the audit trail by user or cloud service.



Actor: (contains) Allen Carey ×

Service	Type	Targets
box	access	Production
aws	delete	logs_bucket
aws	delete	prod_bucket

Try DatAdvantage Cloud 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

www.varonis.com | 1.877.292.8767

PRESIDIO® | VARONIS