Data Sheet

Expedite Incident Response in the Cloud

With over 60% of corporate data now stored in the cloud[1], organizations are facing increased risk of cloud-based cyber attacks and breaches. While there has been significant advancement in cloud prevention and detection technologies, when it comes to investigation and response, there is still a major gap.

Cloud Breaches are Hard

When an incident occurs in the cloud today, security teams face a number of obstacles that lead to significant delays in response. Access to the data required for an investigation is often managed by another team and can take days to manually acquire. Worse, evidence may reside in ephemeral resources, such as containers, and disappear in the blink of an eye. Further, the increase in multi-cloud adoption only exacerbates these challenges.

As a result, security teams face a lose-lose decision:

- Close an incident without digging deep enough, leaving significant risk on the table
- Rely on a combination of outdated and open source tools to stitch together an investigation, a tedious and manual endeavor

Incident Response at Cloud Speed

The Cado Platform leverages the scale and speed of the cloud to automate as much of the incident response workflow as possible – from data capture and processing to root cause analysis and attack containment. The platform was built to empower security analysts of all levels by automatically highlighting the most important events related to an incident including its root cause, scope and impact. Cado also supports remediation actions so that organizations can quickly contain active threats.

[1]Statistia: Share of Corporate Data Stored in the Cloud in Organizations 2015-2022

> "The fact that we no longer have to manually request access to a potentially compromised system via our cloud team is a game changer."
>
> **—Incident Response Lead at #1 Cloud Computing-Based Data Warehousing Company**

How it Works

Collect From Anywhere

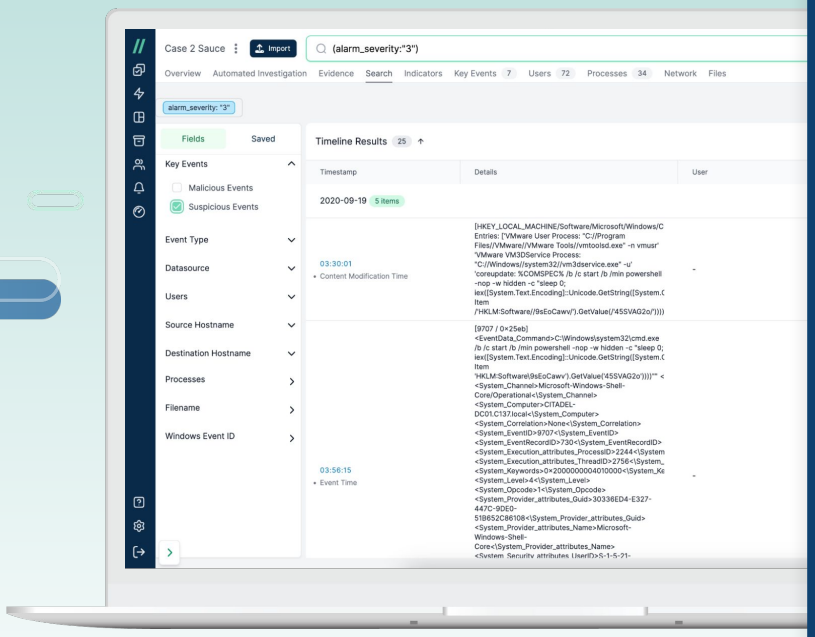
Automate forensic data capture across multi-cloud, container and serverless environments.

Take Advantage of Cloud Speed

Parallel data processing means security teams can normalize hundreds of data sources in minutes, not days.

Automate Investigations

Speed up investigations and reduce MTTR with key incident details at your fingertips including root cause, scope, and a complete timeline of events.



Cado Use Cases

Cross Cloud Investigations

> Respond to incidents identified in AWS, Azure, and GCP in a single pane of glass.

Container Investigations

> Investigate container environments including EKS, AKS, and Kubernetes.

Triage & Full Disk Acquisition

> Automate triage and full volume captures across cloud resources for immediate investigation.

Evidence Preservation

> Ensure evidence residing in ephemeral environments is immediately captured and preserved before it disappears.

Incident Containment

> Perform remediation actions including stopping, containing or isolating cloud instances to prevent damage and spread.

Incident Response Preparedness

> Assess your level of preparedness to properly identify, preserve & analyze incident evidence.

Key Benefits

Better Understand Risk

With visibility beyond what a traditional detection solution provides, security teams can better understand and manage cloud risk.

Reduce MTTR

Cloud-native means security teams can apply cloud speed to the end-to-end IR process, drastically reducing time to response.

Close the Skills Gap

By ruthlessly automating where we can, security analysts of all levels can perform forensics and incident response in the cloud (especially in multi-cloud environments).

Minimize Costs

Empower your organization to bring cloud incident response capabilities in house and reduce reliance on external service providers to lower costs associated with cloud investigations.

Cado customers have accelerated investigation and response by at least 6X when compared to traditional tools.

Cado Security is the provider of the first cloud forensics and incident response platform. By leveraging the scale and speed of the cloud, the Cado platform automates forensic-level data capture and processing across cloud, container, and serverless environments. Only Cado empowers security teams to respond at cloud speed. Backed by Eurazeo, Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit **www.cadosecurity.com** or follow us on Twitter **@cadosecurity**.

CADO//