

Cado Response

Most data is moving to the cloud. Cyber attackers are moving to the cloud. Yet digital forensics has not made this critical leap yet. As a result, when security teams need to investigate a threat in a modern environment, it's incredibly complex and time consuming.

The Cloud is Cloudy

Despite the benefits the cloud can offer, there is still a realistic fear that security incidents in cloud environments can be a financial, legal, and technical minefield. When a cyber incident occurs in the cloud today, security analysts face a lose-lose decision:

- Close an incident without digging deeper than the surface level that's presented in a detection platform
- Rely on a combination of outdated tools, open-source platforms, and spreadsheets to stitch together an investigation

Either way, hackers are slipping through the net.

It's Time to Uncomplicate the Cloud

Digital forensics in the cloud is finally here.

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing across cloud and container environments, Cado Response enables security teams to investigate and respond to cyber incidents at cloud speed.

How it Works



Collect

Capture data in a single click



Process

Process massive amounts of data in minutes



Analyze

Enrich data with machine learning and threat intelligence

"With Cado we've seen a **significant increase** in the number of cases our analysts are able to take on at one time"

—CTO, A Global Incident Response Services Firm

Key Benefits



Save Time

Drastically reduce the time and effort required to analyze a security incident by automating data capture and processing across cloud and container environments.



Reduce Risk

Minimize the impact of compromises and empower fully-informed decision making by identifying the root cause of incidents 5x faster.



Meet Legal & Regulatory Compliance

Meet compliance requirements for digital forensic investigations by capturing every bit and byte of information surrounding a security breach.

Cado Response Use Cases

Cloud Forensics

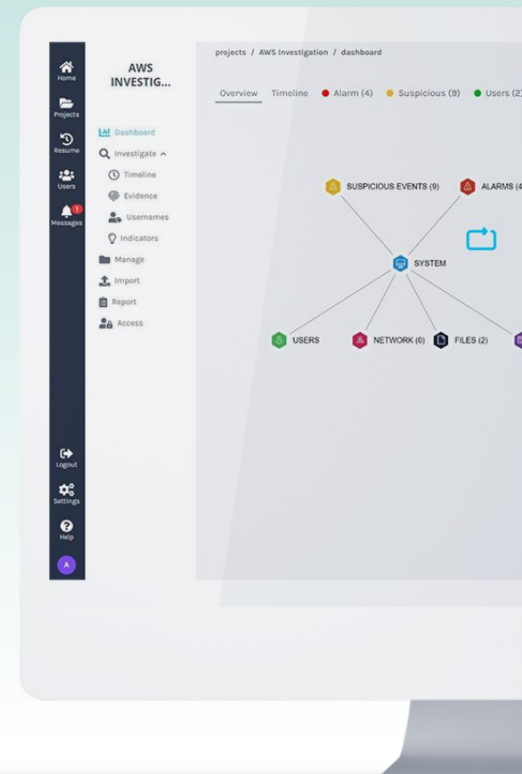
Cado Response makes it easy to conduct forensic investigations across complex and expansive cloud environments. Whether you have a single or multi-cloud approach, or your investigation spans countless regions, systems and accounts, Cado Response delivers a centralized view of the data so you can immediately visualize incident timeline and scope.

Container Forensics

Cado Response is the only solution that enables forensic capture, processing, and investigation of container environments and autoscaling groups. These resources grow, shrink, and recycle data in a way that makes it almost impossible to investigate a potential breach. With Cado Response, you can capture incident data before it's gone.

Cloud Threat Hunting

The Cado response platform ensures organizations are protected even where an agent-based detection solution can't be deployed. For example, organizations often have zero visibility across high-availability production systems because deploying a collection agent can risk downtime. But because Cado Response is completely agentless, you can hunt across top cloud assets with zero impact.



“Cado is the only solution I know that supports Kubernetes and cloud. They're changing the way we do forensics.”

**—DFIR Director at
A Top Global Consulting Firm**

Key Features

- Automate data capture across cloud and container environments
- Process massive amounts of data acquired across countless assets simultaneously
- Analyze multiple data sources in a single pane of glass including cloud provider logs, disk information memory, and more
- Enhance incident investigations using machine learning, threat intelligence, and built-in YARA rules
- Make the Cado Response platform your own with user-customizable rulesets and reporting
- Upload on-prem forensic data and take advantage of Cado's scalable architecture and parallel processing
- Collaborate on a single, or multiple investigations at once, from anywhere

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing across cloud and container environments, Cado Response enables security teams to efficiently investigate and respond to cyber incidents at cloud speed. Backed by 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](https://twitter.com/cadosecurity).

