The Cado Platform

Investigate Any System. Anywhere. Anytime.

Investigations are Hard

Current investigation processes are too manual, too slow, and too reliant on specialized expertise. Further, the rapid adoption of cloud, container, and serverless technologies has made investigations that much more complex. **Old school, legacy technology doesn't cut it.** Stop wasting cycles on tedious, manual investigations. **Doing nothing isn't an option.** Stop closing incidents without the full picture. **The skills gap is real.** Over-reliance on highly-skilled talent results in zero repeatability. **It's time we evolve.**

Investigation and Response Automation is Here.

Cado Security is revolutionizing investigation and response for the hybrid world.

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 to reduce potential impact and damage of threats and preparedness use cases to enable organizations to continuously optimize their incident response program.

> ""After testing out the product, the decision to purchase was a no brainer. Cado makes things simple."
>
> **— Director, Incident Response, Large Video Gaming Company**

Meet the Cado Platform
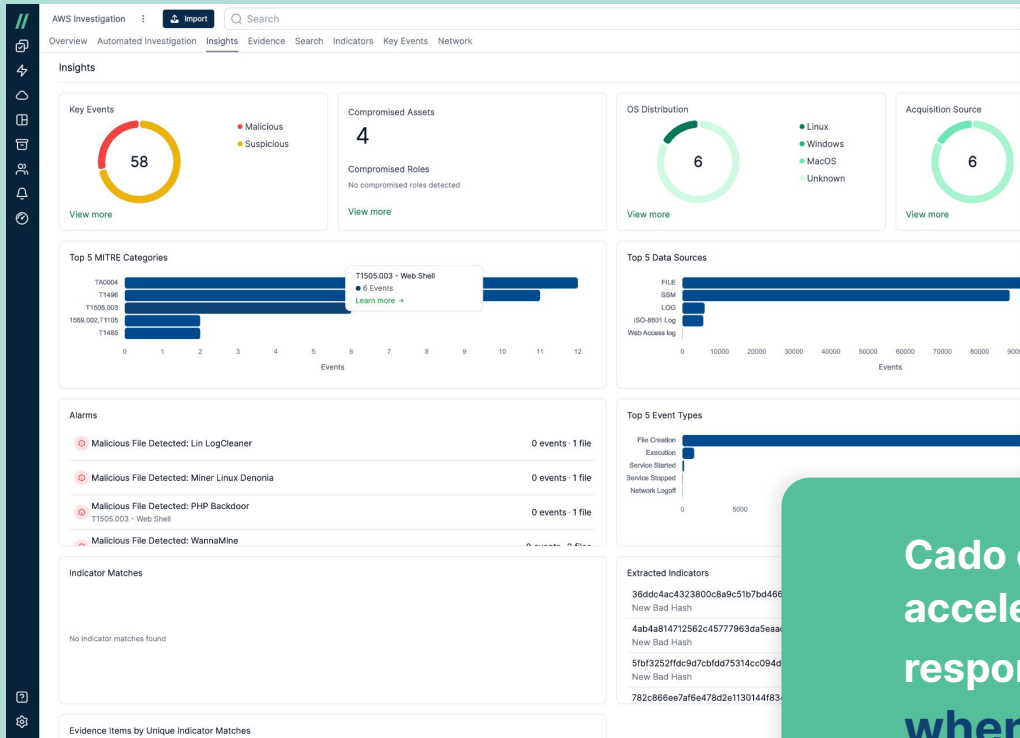
Collect From Anywhere

Automate forensic data capture across multi-cloud, container, serverless, SaaS, and on-premises environments. No permanent agents required.

Cloud Native

All collected data remains in your cloud environment to ensure your privacy requirements are met. You choose: Deploy in AWS, GovCloud, Azure, or GCP in minutes.

AI-Powered Forensics

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

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

Cado Platform Use Cases

Cross Cloud Investigations
Investigate incidents identified in AWS, Microsoft Azure, and GCP in a single solution.

Container & K8s Investigations
Perform container investigations in environments including EKS, AKS, GKE, and Kubernetes.

Endpoint Triage
Automate triage acquisition of endpoint resources to gain immediate event insights and facilitate quick escalation.

BEC Investigations
Analyze critical SaaS logs to investigate Microsoft 365 compromises, such as Business Email Compromise (BEC).

Attack Containment
Perform response actions including stopping, containing, and isolating systems to prevent damage and spread.

Incident Response Preparedness
Assess your readiness to investigate and respond to threats, and establish a repeatable IR process.

CADO//