Solution Brief

MANDIANT
NOW PART OF Google Cloud
/ CADO//

# Revolutionizing Cloud Incident Response

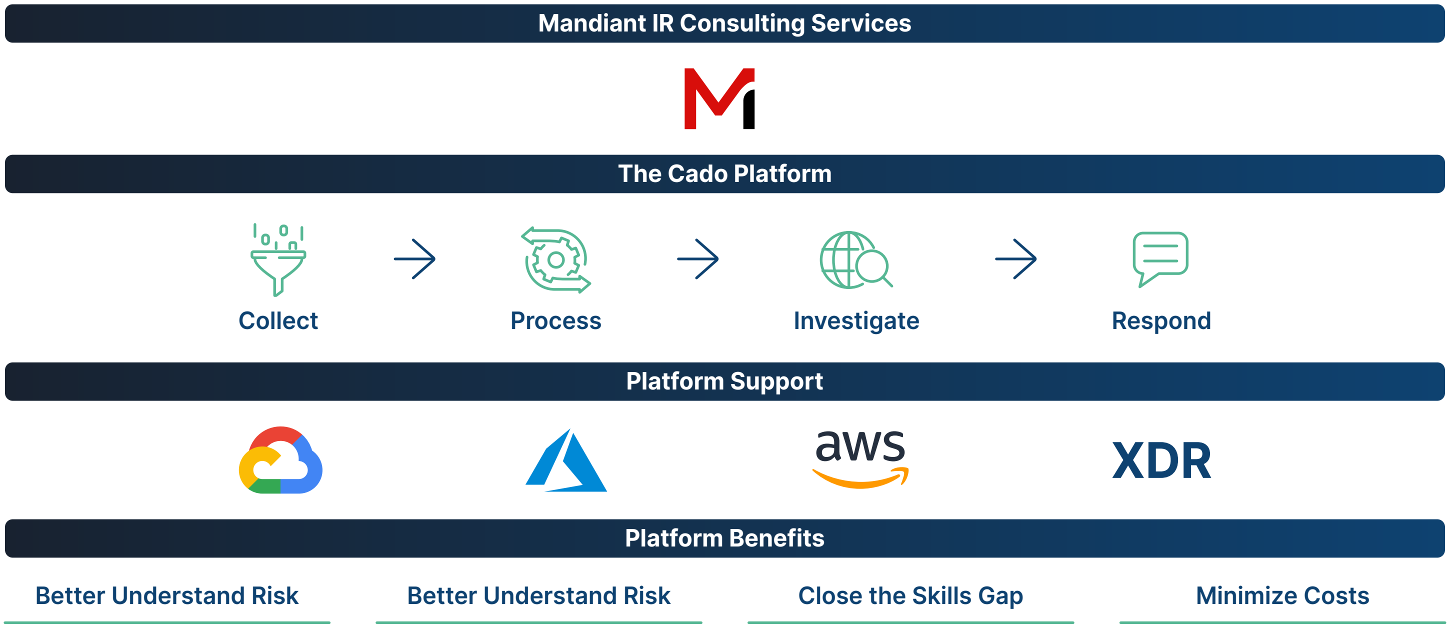
## Mandiant IR Consulting  Powered by the Cado Security Platform

Enterprises are rapidly deploying cloud and container-based applications which are increasingly targeted by threat actors. Being impacted by an incident is a 'when', not 'if' situation, and Mandiant customers need quick and accurate answers. This is especially important in context of the growing number and scope of incident reporting requirements across the world. In order to navigate the evolving threat landscape and intricate dynamics of cloud environments, service providers require modern technologies specifically designed for cloud-based scenarios.

## Joint Solution

Mandiant and Cado have partnered to deliver cutting-edge cloud incident response services to global enterprises. The Cado Security platform is rapidly deployed in the customer's environment to expedite forensic data collection and analysis. Cado delivers essential context and depth Mandiant incident responders can use to identify the root cause of incidents and craft an effective response plan. Together, Cado and Mandiant can deliver prompt and effective incident investigation and response.

*Mandiant IR Consulting Powered by the Cado Security Platform*



Mandiant IR Consulting Services

The Cado Platform

Collect → Process → Investigate → Respond

Platform Support

XDR

Platform Benefits

Better Understand Risk

Better Understand Risk

Close the Skills Gap

Minimize Costs

## Benefits

### Rapid Deployment

Deployment via a cloudformation template or terraform script happens in minutes. All collected data resides in the customer’s cloud environment to ensure unique data privacy requirements are met.

### Better Understand Cloud Risk

Cloud challenges demand cloud solutions. Cado offers the speed, adaptability, and depth required to truly understand cloud risk. Cado delivers visibility even in the most complex ephemeral environments.

### Reduce MTTR

Automation is applied to the end-to-end incident response process – from data capture to analysis. With Cado, Mandiant incident responders can determine the root cause and scope faster, reducing response times.

## How it Works

Cado Security’s cloud forensics and incident response platform empowers Mandiant incident responders to efficiently manage risk identified in cloud, container, and serverless environments.

### Collect 01

- Automated forensic data capture, no agents required
- Multi-cloud, container, serverless support

### Process 02

- Patented cloud-native architecture
- Rapid, parallel data processing to normalize hundreds of data formats

### Analyze 03

- Data enriched by third-party and proprietary intelligence
- Single pane of glass for collaborative investigations

*“We are thrilled to embark on this strategic partnership with Mandiant. At Cado, our commitment to innovation in cloud forensics and incident response aligns with Mandiant's dedication to excellence. Together, we aim to elevate cloud incident response, providing organizations with top-notch services for their evolving security needs.”*

— James Campbell, CEO & Co-Founder of Cado Security

## Platform Highlights

### API-Based Visibility

Cloud-native by nature, APIs are leveraged for visibility without the need for a permanent agent. No additional friction or fuss.

### Hosted by You

Deploy natively within your cloud environment to ensure your unique privacy requirements are met. You choose: Deploy in GCP, AWS, GovCloud, or Azure.

### Cross Cloud Support

Multi-cloud is the new norm. Cado supports the collection and analysis of data captured across multiple Cloud Service Providers (CSPs).

### Historical Context

Historical evidence is often key in identifying the root cause and scope of an incident. Cado collects data since the time the system was spun up.

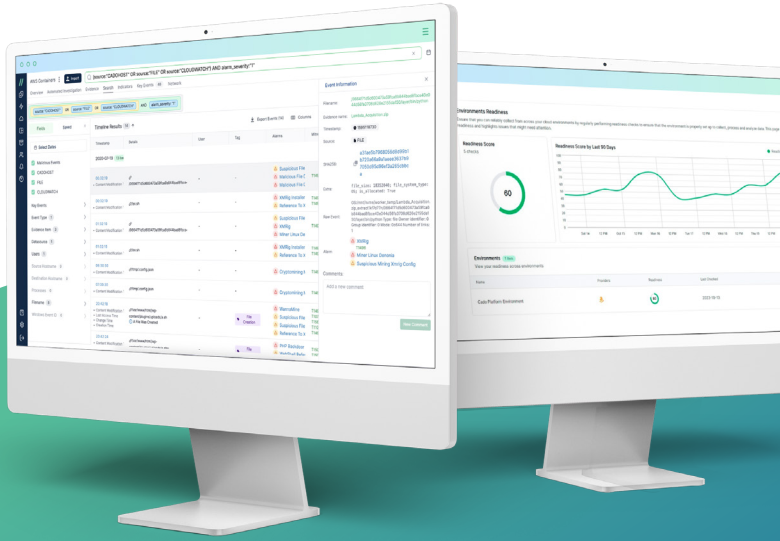
### Ephemeral IR

In container-based and serverless environments, evidence can disappear in the blink of an eye. Cado preserves forensic data, making forensics possible in ephemeral environments.

### Solution Agnostic

Rapid response requires tools that work together. The Cado platform seamlessly integrates with popular detection tools to process alerts coming from XDR, EDR, and CNAPP solutions.

MANDIANT®
NOW PART OF Google Cloud



## Conclusion

By prioritizing speed, adaptability, and depth, the partnership between Mandiant and Cado Security addresses the challenges posed by dynamic cloud environments. Together, Mandiant and Cado Security empower enterprises to navigate the complexities of cloud security and reduce the time it takes to mitigate risks identified in cloud environments.

CADO//