The Cado Platform for Federal Organizations

CADO

Table of Contents

1. Introduction

Federal agencies are constantly facing rapidly evolving threats. As they migrate operations to the cloud, the need for robust, cloud-native forensic and incident response tools has become increasingly critical. Traditional on-premise solutions struggle to address the unique challenges posed by the dynamic, scalable, and often ephemeral nature of cloud ecosystems. In this context, the Cado Platform emerges as a cutting-edge solution, specifically designed to meet the demands of Digital Forensics and Incident Response (DFIR) in cloud-native environments.

The Cado platform, with its automation capabilities and integration with multiple cloud platforms and other cyber-security tools, offers federal agencies an unparalleled ability to quickly and efficiently respond to security incidents. Built from the ground up to leverage the scale and speed of the cloud, Cado Security enables security teams to capture, process, and analyze forensic data across a wide range of environments, including virtual machines, containers, and serverless infrastructures. This capability is crucial for maintaining the security and integrity of federal information systems, which often handle sensitive and mission-critical data.

In addition by automating many of the labor-intensive aspects of forensic data collection and analysis, the Cado Platform not only accelerates incident response times but also reduces the burden on overextended security teams, allowing them to focus on higher-level analysis and decision-making.

This white paper explores how the Cado Platform can be effectively utilized by federal agencies to enhance their security posture, ensure compliance with federal security mandates, and provide a rapid, scalable response to security incidents in cloud environments.

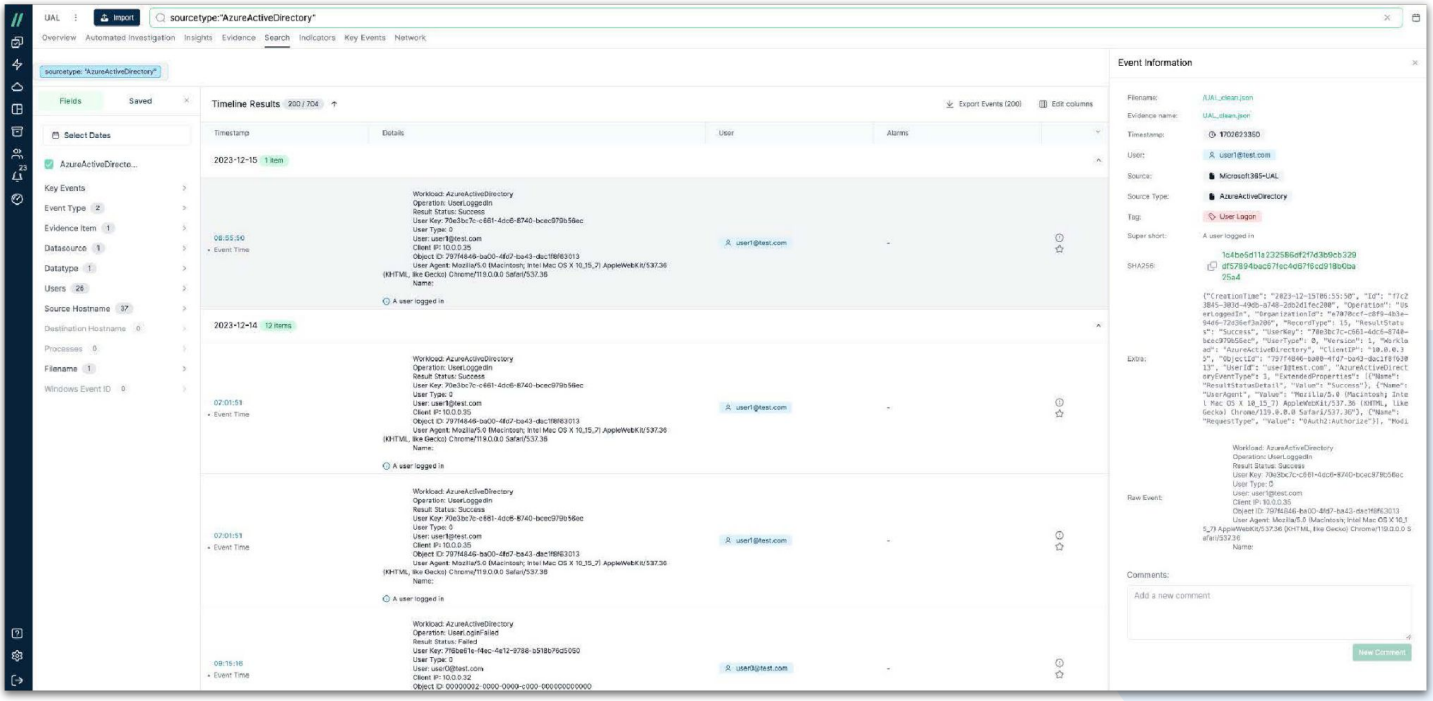
2. Defend The Nation's Most Critical Assets

Investigation and Response Automation

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.

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.



Automated Multi-Cloud Forensics and Response

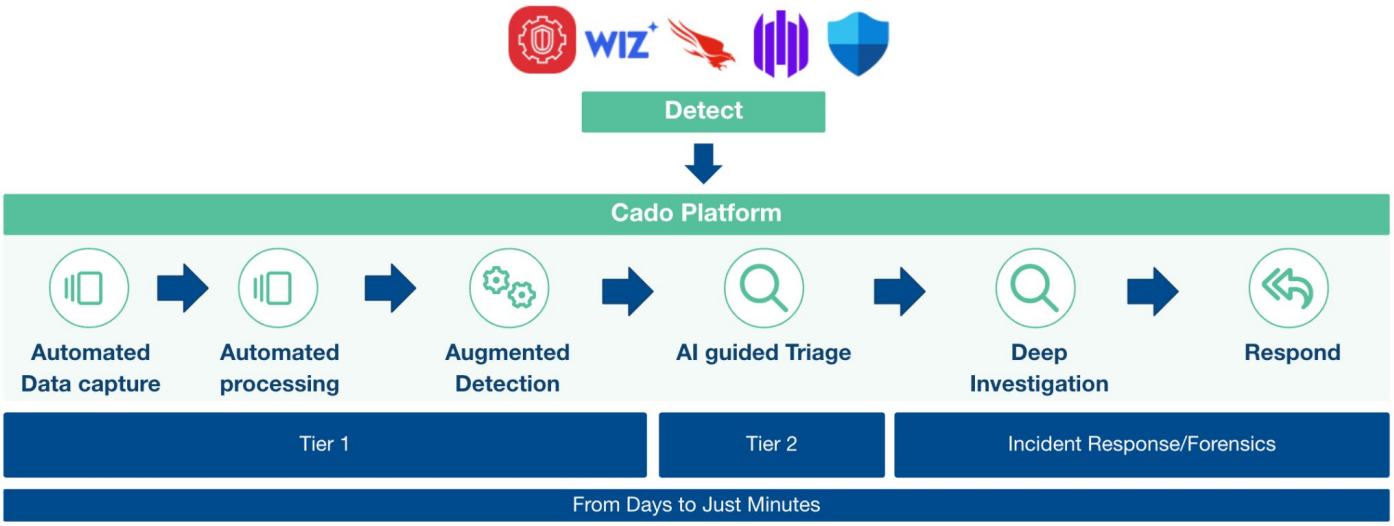
The Cado Platform excels by addressing the key challenges of investigating and responding to threats across multi-cloud and hybrid environments. Its unique ability to automate forensic data capture and analysis ensures critical evidence is preserved, even for ephemeral resources such as containers and serverless environments, which are notoriously difficult to monitor with traditional tools. With built-in cross-cloud support, Cado provides a unified view across AWS, Azure, and Google Cloud, allowing security teams to respond to incidents faster and more effectively. This platform also integrates seamlessly into existing cloud infrastructures, reducing the manual effort required for deployment and maintenance, while enabling organizations to maintain full control of their data within their own cloud environments.

3. Augment Federal SOC

Cado Security revolutionizes how SOC teams approach incident response. The Cado Platform supercharges your SOC by reducing the workload during key parts of the investigation workflow, from data capture to root cause analysis. Leveraging AI-powered forensics and actionable insights, Cado Security elevates your SOC's ability to triage incidents and respond with clarity.

Cado Security ensures that analysts of every level can efficiently handle complex incidents.

Perform seamless handoff between SOC tier 1, SOC tier 2 and Incident Response teams.



Cross Cloud Investigations

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

Cloud Detection & Response

Marry threat detection with automated forensic collection and investigation to expedite response to cloud threats.

Endpoint Triage

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

SaaS Investigations

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

Container & K8s investigations

Perform container investigations in environments including EKS, AKS, GKE, and Kubernetes.

Preserve Ephemeral Data

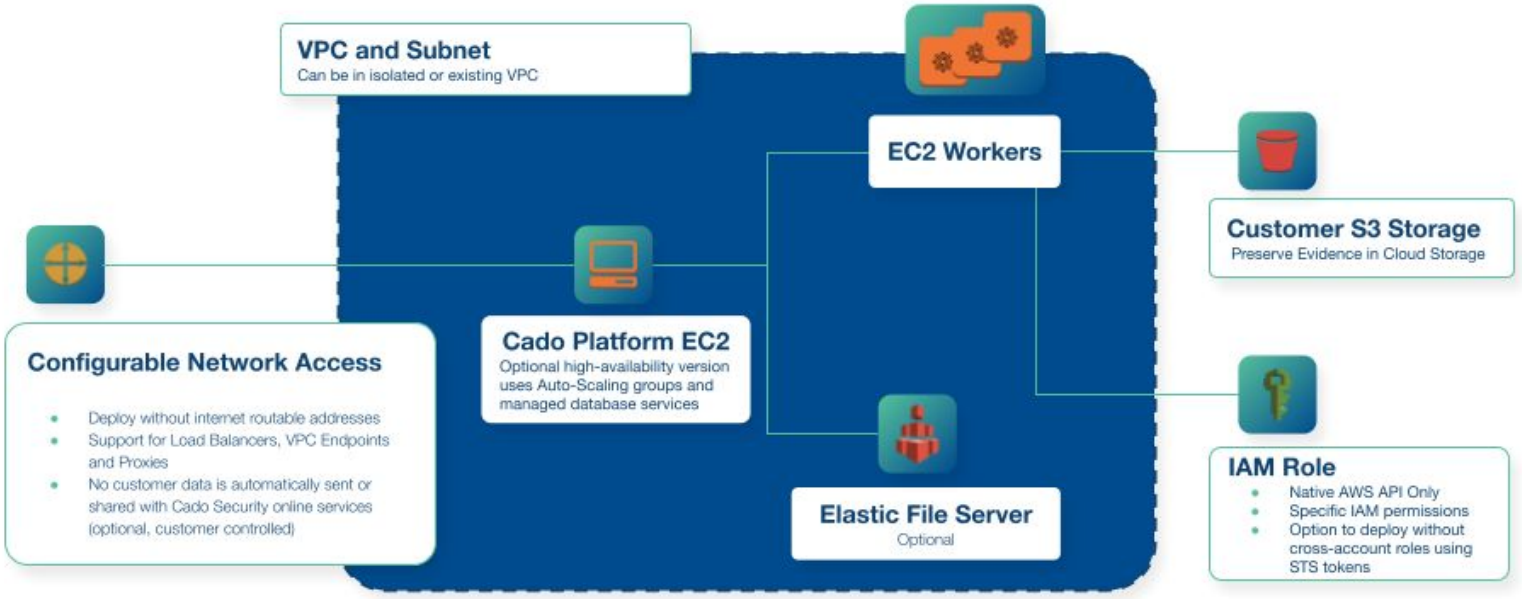
Meet regulatory requirements to capture critical data required to investigate incidents no matter where they happen.

4. Your Data In Your Cloud

With the Cado Platform, all data is stored, processed and analyzed within your cloud estate on your virtual machines. It is never sent to Cado or third party servers. Keeping your data secure.

Using the Cado Platform means that your data remains fully under your control. All data collected during incident investigations is stored, processed, and analyzed within your own cloud infrastructure. Whether in AWS, Azure, or Google Cloud, the platform integrates directly into your existing environment, ensuring compliance with cloud data governance standards and eliminating the need to rely on third-party servers or external storage. This level of security ensures full visibility into your cloud estate while maintaining complete ownership over sensitive information.

Cado – Example Architecture in AWS



5. Deploying in AWS GovCloud

Cado Security supports native deployment in AWS GovCloud (US). AWS GovCloud (US) is the set of Amazon's Regions designed to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements. This means that Cado customers can now perform investigations on workloads running in GovCloud in the same way as they would be able to for workloads in AWS Standard Regions.

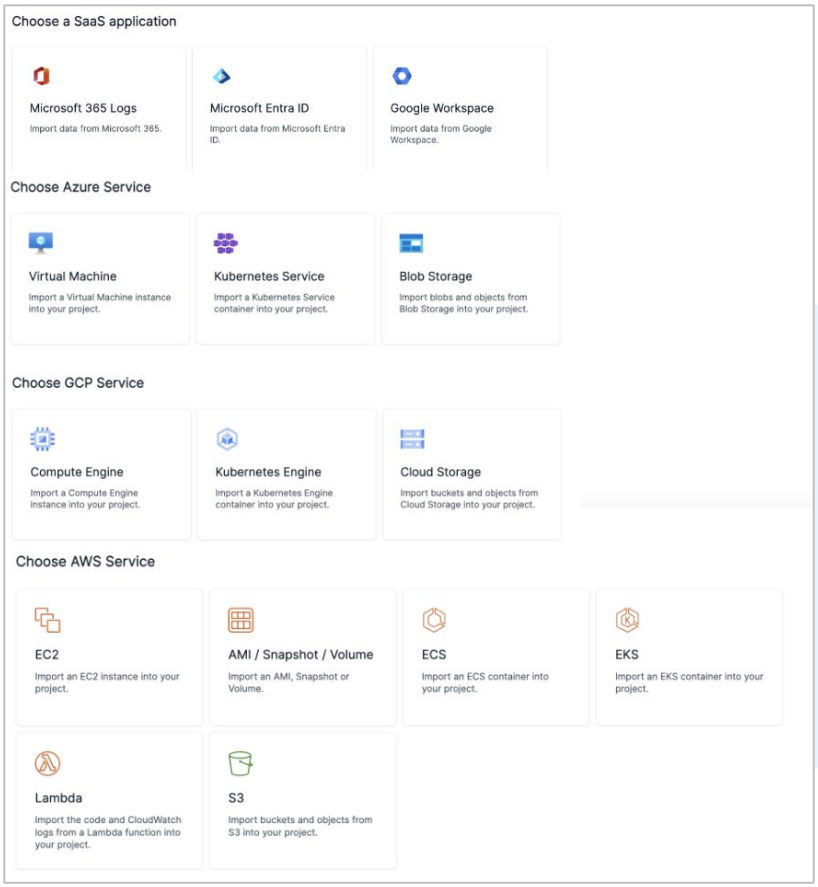
With Cado's GovCloud support, customers now have the ability to perform investigations on workloads running in GovCloud in the same way as they would be able to for workloads in AWS Standard Regions.

Securely collect data from anywhere.

Automated data capture:

- ✓ Cloud
- ✓ Containers
- ✓ Serverless
- ✓ On Premise
- ✓ SaaS

No agents required means **zero impact to production systems**



6. Meet Regulatory Requirements

Cado Security enables organizations to align with requirements such as NIST-CSF and NIST SP 800-171 through several key features that streamline cloud forensics and incident response. Here's how:

Automated Incident Response and Forensics:

Cado's platform automates the entire investigation process, from data collection to analysis and response, across multi-cloud, container, and on-premises environments. This supports NIST-CSF's Respond and Recover functions by allowing organizations to automate response workflows, reducing mean time to respond (MTTR) and enhancing recovery.

By integrating with detection systems such as GuardDuty, EDR/XDR platforms, and SIEMs, Cado can automatically trigger data collection and investigations when threats are detected, supporting the detection of "Anomalies and Events" and "Security Continuous Monitoring." These integrations also help monitor and identify unauthorized system use, aligning with NIST SP 800-171 requirements (3.14.06). Additionally, Cado supports organizations in assessing their readiness for cloud investigations, fulfilling response planning and testing requirements for both NIST-CSF and NIST SP 800-171.

By automatically preserving forensic evidence within the customer's cloud, Cado ensures compliance with chain of custody requirements, aligning with incident handling guidelines.

Comprehensive Data Collection:

Cado supports forensic-level data collection across AWS, Azure, GCP, SaaS, and on-premises environments, capturing full disk images, memory, logs, and more. This capability is vital for complying with NIST SP 800-171, which mandates secure handling of controlled unclassified information (CUI).

By using cloud-native APIs, Cado collects forensic evidence without the need for permanent agents, helping customers meet data security and privacy standards. Cado's automation of forensic data collection and processing across various environments supports "Response Planning" and "Analysis," enabling rapid investigation. This preserved forensic evidence supports post-incident analysis and continuous improvements, aligning with NIST-CSF's "Improvements" category.

Cado's ability to investigate across multiple clouds (AWS, Azure, GCP) ensures comprehensive visibility, fulfilling detection and response requirements.

6. Meet Regulatory Requirements (continued)

Data Privacy and Control:

Cado's architecture ensures all collected data remains within the customer's environment (AWS, Azure, GCP), adhering to data residency requirements outlined in NIST SP 800-171. This allows organizations to maintain control over sensitive data, ensuring it is not shared outside their cloud environment.

Repeatable and Scalable Processes:

By automating incident response and integrating with SIEMs and XDR solutions, Cado enables organizations to build repeatable, scalable processes. This aligns with the Identify and Protect functions of NIST-CSF by supporting continuous monitoring, detection, and protection against cyber threats.

Cado's automation streamlines investigation processes, enabling faster incident response and supporting both frameworks' goals of minimizing impact and improving resilience. The platform's automated reporting capabilities assist with documenting incidents and responses, crucial for compliance.

Cado also provides automated timeline analysis and AI-powered investigation tools, supporting the "Analysis" category, while its attack containment features enable quick response actions, aligning with the "Mitigation" category.

Moreover, Cado's automation and AI analysis empower less experienced analysts to perform advanced tasks, helping organizations meet skilled personnel requirements.

By leveraging Cado Security's platform, organizations can significantly enhance their ability to detect, respond to, and recover from security incidents in hybrid and multi-cloud environments. This helps them align with NIST-CSF and NIST SP 800-171 requirements, especially regarding the rapid response expectations outlined in these frameworks.

For more information:

If you'd like to learn more about what Cado Security is doing to help advance investigations and incident response, request a demo today.

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 Security enables security teams to effectively investigate and respond to cyber incidents at cloud speed. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security is based in London. For more information, please visit www.cadosecurity.com or follow us on X @cadosecurity.

See a Demo

CADO