CADO

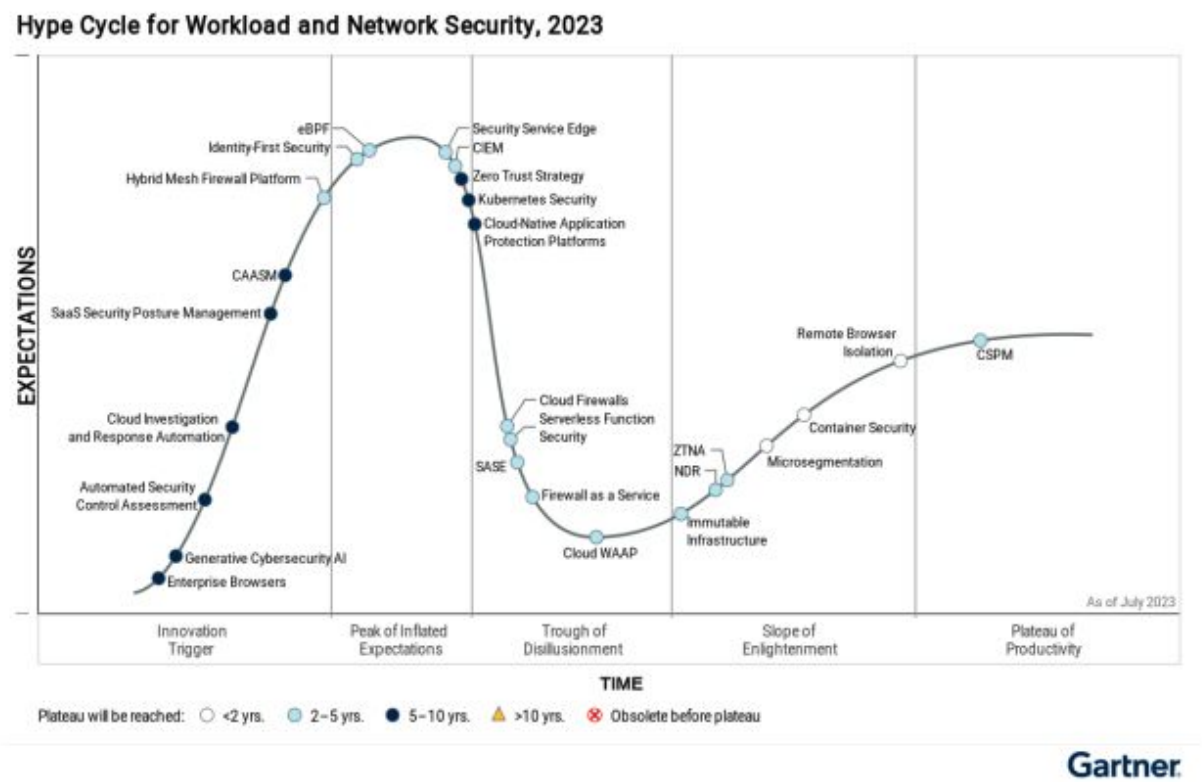
White Paper

Five Reasons Why You Need

Cloud Investigation & Response Automation

What is **Cloud Investigation and Response Automation?**

Cloud Investigation and Response Automation (CIRA) is an emerging category within cloud security. CIRA technologies enable security teams to automate the collection and analysis of forensic data in cloud environments to expedite response. The category was first coined by Gartner® in 2023 and was included in the latest **Hype Cycle for Workload and Network Security**.



The rapidly evolving attack methods observed in cloud environments coupled with the growing number and scope of regulatory requirements has increased urgency among organizations to adopt a modern approach to cloud incident response. CIRA technologies deliver key capabilities to enable organizations to thoroughly understand and mitigate cloud risks.

Core capabilities of CIRA technologies include:

- ➔ Forensic data collection and analysis across multi-cloud environments
- ➔ Ability to preserve evidence acquired across dynamic and ephemeral resources such as containers
- ➔ Seamless investigation of various data sources acquired from both cloud resources and logs
- ➔ Automated remediation actions to enable rapid response

With more than 60% of corporate data currently stored in the cloud, cloud computing has influenced a true renaissance in how we manage and deliver applications and services. The appeal of migrating to the cloud is clear – greater speed, agility, flexibility, cost savings, and more.

Digital transformation also poses new security challenges – especially when it comes to forensics and incident response. The cloud is complex. Cloud VMs, containers and functions can be extremely difficult to access, or worse, disappear in the blink of an eye. In this modern cyber world – where new blind spots provide attackers with a greater window of opportunity – it is essential that security teams have the proper visibility to investigate and respond to potential compromises.

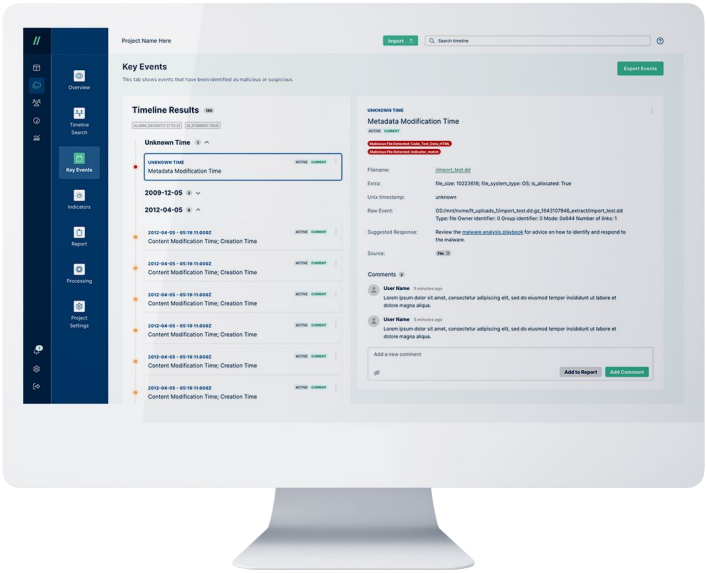
This white paper covers five reasons why you need Cloud Investigation and Response Automation (CIRA) to ensure your organization is equipped to efficiently understand and respond to cloud threats.

REASON #1

Developers are There, Attackers are There, You Need to be There too!

A match made in heaven, cloud computing and DevOps provide the scalability, accessibility, and automation required to implement new software at cloud-speed. Prototypes can be developed in just weeks, versus months or years. Sounds like a dream, right? It would be – if cyber security had kept pace with the speed of innovation.

Much of the security team's effort to date has been focused on securing feedback loops early in the DevOps and software development life cycle, meaning many organizations have adopted cloud protection and detection technology such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP). However, when it comes to investigation and response, there is a huge gap. Once something bad is identified, organizations often don't have the ability to understand the true scope and root cause of the incident.



Today, when a cyber incident occurs, security teams often have little choice but to resort to a "lift and shift" approach, leaning on their existing on-premise investigation and detection tools for cloud visibility. However, these tools weren't designed for dynamic cloud environments encompassing virtual machines, containers and serverless resources. This means security teams often respond to an incident without understanding its full scope and they leave elements behind that attackers can leverage. For example, recent research shows **80% of Ransomware victims** that pay out are attacked again. This is happening because security teams aren't conducting a proper and thorough investigation to completely remove an attacker's access.

To adequately manage risk in today's cloud-first world, security teams require deep visibility across the next generation of technology. This is where Cloud Investigation and Response Automation (CIRA) comes in. While getting forensic data in the cloud may seem like a daunting task, cloud providers now make a range of automation options available, and it is these automation techniques that make it possible for security teams to effortlessly dive deep. With visibility beyond what a detection platform can provide, security teams are able to make more informed response decisions – and therefore, better manage risk across modern environments.

REASON #2

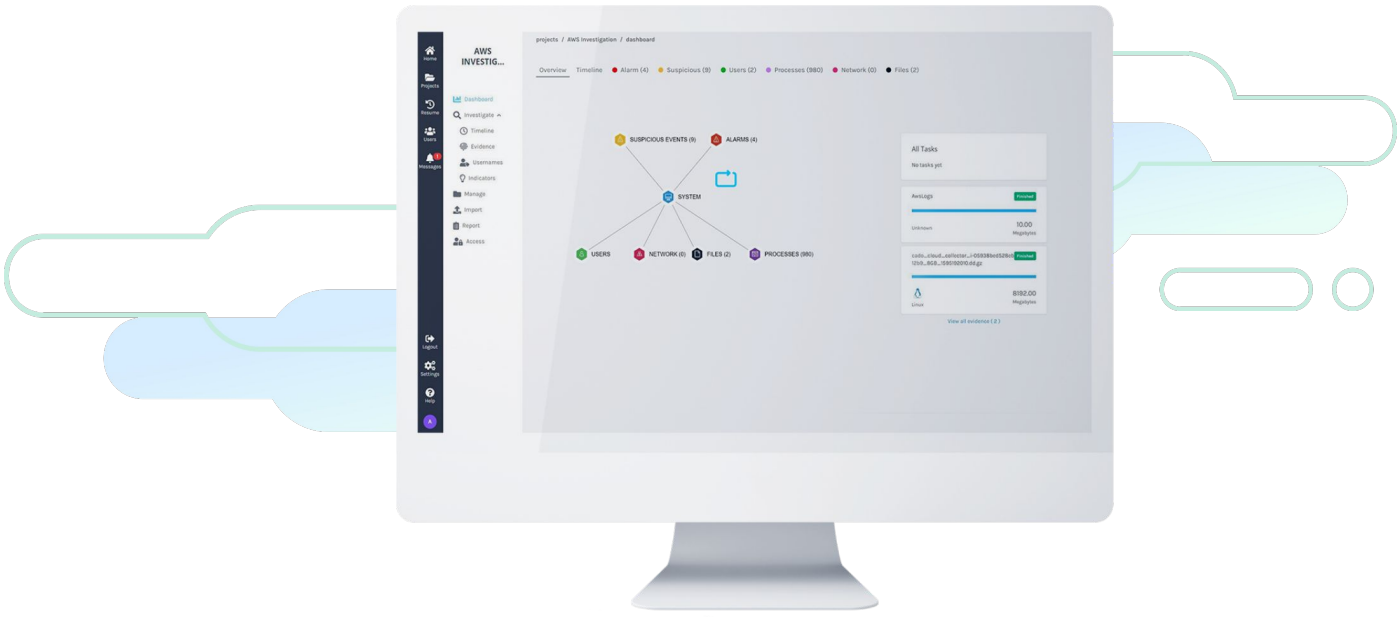
Cloud Experts are Hard to Find

The cybersecurity skills gap is a well known problem. According to the 2022 (ISC)2 Cybersecurity Workforce Study, there is a global shortage of 3.4 million cybersecurity workers. And with the rapid transition to cloud, organizations are now tasked with hiring security talent with deep cloud knowledge, on top of everything else. It's often just not possible for security teams to perform forensics and incident response in the cloud with the knowledge, tools and resources they have.

For example, even before an analyst can start their investigation, they need to be able to determine the types of cloud data sources that will be of most value - and in today's evolving cloud landscape, this is no easy task. For example, there are over 200 products and services in AWS, each with different security best practices and data sources. Once security teams have identified the types of data sources they wish to analyze, gaining access is another obstacle. The cloud APIs are much better than their on-premises equivalents, but leveraging them still requires an in-depth understanding of each cloud providers' capabilities and the skillset to write the scripts to call the APIs.

Done right, though, the advantages are innumerable - you can automate elements of the process from end to end - from acquisition, processing and analysis, to taking response actions.

While it's important to have a basic understanding of the different data sources available in the cloud (e.g. core logging platforms such as AWS CloudWatch, Azure Monitor Logs, GCP Logs, Kubernetes Logs, etc.), it's unreasonable to expect any one individual to have all the cloud expertise to perform incident response investigations in the cloud. Using traditional incident response approaches, analyzing all of these different data sources can feel close to impossible, but with Cloud Investigation and Response Automation (CIRA), analysts of all levels can perform forensics investigations in the cloud. Cloud Investigation and Response Automation solutions unify hundreds of data sources across cloud-provider logs, disk, memory and more in a single pane of glass. Further, this modern approach means security teams can leverage the cloud in a way that enables them to collect, process and store critical incident evidence in a secure, flexible and efficient way, while also allowing for easy collaboration.



REASON #3

Risk Escalates at Cloud Speed

Cloud, containers and serverless architecture have completely changed the way we build business applications, and it has also fundamentally changed the way attacks and adversaries operate. Attackers are evolving quickly – consistently developing new tools, tactics and techniques to compromise the next generation of technology.

For example, **the first publicly-known case of malware** specifically designed to execute in an AWS Lambda environment was discovered fairly recently. Although the first sample discovered was fairly innocuous in that it only runs crypto-mining software, it demonstrates how attackers are using advanced cloud-specific knowledge to exploit complex cloud infrastructure, and is indicative of potential future, more nefarious attacks.

```
2022/04/01 11:37:21 expected AWS Lambda environment variables
[_LAMBDA_SERVER_PORT AWS_LAMBDA_RUNTIME_API] are not defined
```

Lambda-specific log statement from Denonia

But while attackers are moving at cloud speed, organizations are struggling to keep pace. According to research released by **ESG in November 2021**, 89% of organizations have experienced a negative outcome in the time between detection and investigation of a cloud security incident. The primary reason, according to respondents, is that it takes too much time to collect and process the data required to perform forensics investigations (approximately 3.1 days on average). What's worse, because of this, over one-third of cloud security alerts are never investigated, according to ESG.

To keep pace with the adversary, security teams require the ability to perform incident investigations quickly and deeply. Thorough incident response requires security teams to retrace an attacker's every move in order to close any existing gaps that could leave the organization vulnerable to future compromise. Moreover, they need to do this quickly, before ephemeral workloads get spun down, destroying clues attackers might leave behind. Cloud Investigation and Response Automation solutions address this challenge by enabling security teams to leverage cloud speed and automation to eliminate the window between detection and investigation and response.

REASON #4

Multi-Cloud is On the Rise

Today, most organizations leverage more than one cloud provider. According to Gartner's 2020 Cloud End-User Buying Behavior Survey, 76% of respondents have adopted multi-cloud infrastructure – whether it be to maintain SLAs and protect against outage, capitalize on regional coverage, manage costs, or to simply maximize functionality. Even the United States Financial Industry Regulatory (FINRA) has stated that broker-dealers should be able to switch cloud providers when needed and "consider the risks associated with vendor lock-in", including "an exit strategy to mitigate against an unfavorable lock-in scenario." Similarly, the European Banking Authority warns against risk management associated with one provider, urging its members to take "concentration risk" into account by avoiding a "dominant service provider that is not easily substitutable."

While security teams already struggle to get the data they need to perform incident response in the cloud, the rise of multi-cloud makes this task even more challenging for a few major reasons:

- **Data silos -** Each cloud provider has their own terminology, security tools, monitoring logs, and APIs, making it difficult to know which data sources are most valuable to capture, how to capture them, and moreover, how to efficiently investigate all of these different sources from multiple cloud platforms and environments.

- **Skill & knowledge gaps -** As previously mentioned, it's already painfully difficult to hire cyber security professionals with deep cloud knowledge, but finding security talent that has the skill set to work in multiple clouds can feel close to impossible.

As a result, when an incident occurs in the cloud today, security and incident response professionals face a lose-lose decision – do they close an incident without understanding the full scope and impact or spend days to weeks stitching together an investigation which may not yield the desired results? With so many companies adopting a multi-cloud strategy, security teams need solutions that provide cross-cloud, a key point raised in the 2023 Gartner® Hype Cycle on Workload and Network Security. Cloud Investigation and Response Automation is key to removing the complexities associated with performing forensics and incident response across multi-cloud environments. By completely automating data capture and processing, Cloud Investigation and Response Automation solutions enable security teams to seamlessly dive into incident data — regardless of where it resides.

REASON #5

Ephemeral Means Data Disappears in the Blink of an Eye

One of the biggest challenges security teams face is securing ephemeral environments consisting of cloud, container-based and serverless resources. These resources spin up and down continuously, making it almost impossible for security experts to investigate an incident and understand which assets and data have been compromised. If malicious activity occurs between the time one of these resources is spun up and down, that data is lost forever. Attackers are taking advantage of this because it helps them cover their tracks.

When investigating an environment that utilizes containers or other ephemeral resources, data collection needs to happen immediately following detection so that valuable evidence isn't destroyed. This can only be achieved through automation. Additionally, because many organizations have thousands of containers, it's also critical that automation is applied to expedite data processing and enrichment as well.

Cloud Investigation and Response Automation (CIRA) solutions make incident response in ephemeral environments possible by delivering the following capabilities:

- **Automated Data Capture:** Automation ensures critical evidence is captured and preserved for investigation immediately following incident detection. This means security teams preserve critical evidence and reduce time to incident containment and resolution.

- **Container Asset Discovery:** Since containers operate as virtualized environments within a shared host kernel OS, it's often challenging to keep track of asset workloads running across all containerized machines in a scaled environment. An agentless discovery process that can efficiently discover and track container assets enforces appropriate security protocols across all container apps.

- **Ability to Quickly Isolate:** In the event a resource is compromised, it's critical that security teams have the ability to quickly isolate it in order to stop the active attack and prevent further spread and damage. In some cases, isolation can be a good first step to take following initial detection. This allows security analysts to perform a more thorough investigation in the background and ensure proper remediation and containment steps are taken after you have a better understanding of the true scope and impact of the incident.

Conclusion

Security teams shouldn't have to be cloud experts to secure their environment. Analysts shouldn't have to work across multiple cloud teams, jump through hopes to gain access to a potentially compromised system, or require deep knowledge across all major cloud providers. Applying modern security techniques and technology empowers security teams to automate where possible and drastically reduce the complexity and time required to perform forensics and incident response in the cloud.

For a cloud-specific cybersecurity strategy, security teams need solutions that are built for the cloud. Cloud Investigation and Response Automation (CIRA) enables security teams to streamline data capture, processing and analysis so they can easily understand risk across the most complex cloud environments.

At Cado, we believe that the cloud makes security easier, not harder. Cloud Investigation and Response Automation allows security teams to augment the end-to-end incident response process by leveraging cloud speed and automation. By ruthlessly automating where we can, common investigative techniques can be replicated – from capturing the right data to identifying incident root cause, scope and impact.

This automation frees up valuable focus time so that security teams can prioritize the most important incidents and drastically reduce overall Mean Time To Respond (MTTR).

How Cado Delivers CIRA

The Cado Platform was specifically designed to empower organizations to effectively manage the unique challenges of cloud environments in the context of incident response. Cado delivers CIRA by leveraging the scale and speed of the cloud to automate as much of the incident response workflow as possible – from data capture and processing to analysis and attack containment. The platform enables security teams to gain immediate access to forensic-level data in multi-cloud, container, and serverless environments. Evidence items extracted from cloud-provider logs, disk, memory and more, are processed in parallel to drastically reduce time to investigation. 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 organisations can quickly contain active attacks.

With Cado's CIRA capabilities security teams can:

- **Automate the end-to-end incident investigation and response process:** from processing the alert, to collecting and preserving the evidence, analyzing the data, containing the threat and limiting its impact.

- **Prepare comprehensively for an incident:** setting up accesses, automation rules, and integrations with third party systems (such as incident management platforms, XDR, SOAR, CNAPP, and SIEM) to make sure you have a robust, comprehensive and defensible process and architecture.

- **Test your preparedness and understand your risk posture:** know where your gaps are and where you need to invest to reduce your exposure.