DARKTRACE

■ Report

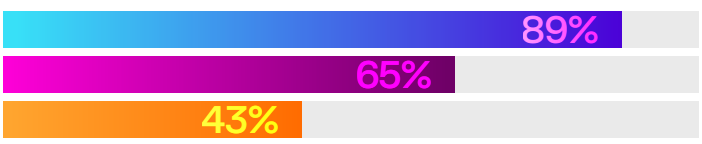
Organizations Require a New Approach to Handle Investigation and Response in the Cloud

Incident response today is too time consuming and manual, leaving organizations vulnerable to damage due to their inability to efficiently investigate and respond to identified threats.

The incident response challenge is further complicated as enterprises rapidly deploy cloud and container-based technologies and embrace a multi-cloud strategy. Organizations have come to realize a new approach is required to handle investigation and response, especially amidst the growing number and scope of incident reporting mandates across the globe and to navigate the intricacies of cloud and container-based environments. To assess the state of the incident response landscape, we worked with an external provider to conduct a survey in 2024.

Delays in investigation result in damage

When it comes to incident response, time is of the essence. Yet today, using traditional approaches, investigations are far too complex, time consuming, and reliant on expert talent. This has resulted in a gap between event detection and investigation and response. Consequently, nearly 90% of surveyed organizations have suffered some level of damage before they were able to investigate and contain incidents in the cloud. Further, nearly half of that damage was reported as significant. This underscores the urgent need for more streamlined and efficient incident response strategies specifically for cloud environments.



89% of organizations suffer damage before containing and investigating incidents

65% of organizations spend approximately 3-5 days longer when investigating something in the cloud vs on prem

43% of organizations have experienced significant damage from a cloud incident alert that didn't get investigated

Top factors contributing to investigation delays

One of the primary contributing factors to investigation delays was reported as a lack of visibility and control over cloud environments. Digging deeper, the lack of visibility and control was fueled by the need to leverage multiple tools and platforms for cloud-based investigations, especially in scenarios where resources are deployed across multiple cloud service provider platforms. Furthermore, a lack of cloud-specific knowledge also contributed to this, as traditional incident response approaches when applied to the cloud require a deep level of cloud expertise. Unfortunately, hiring top security talent is already extremely challenging, but finding security experts with in-depth knowledge of cloud infrastructure is an even more daunting task.

Other operational challenges when responding to cloud-based threats:

82% **of organizations** use multiple platforms and/or tools to perform forensics investigations in the cloudcloud-based threats

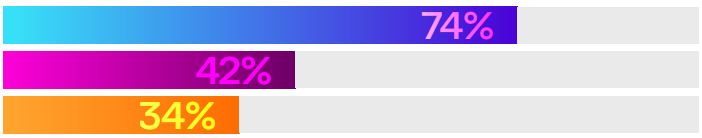
36% **of surveyed organizations** report lack of visibility and control over cloud environments was the biggest challenge faced when it comes to timely investigation and response to cloud-based threats

Biggest compliance challenges

Security teams are facing escalating pressure due to the increasing scope and number of regulatory reporting requirements worldwide, as non-compliance can result in substantial fines and significant damage to a company's reputation and revenue.

The lack of visibility into data was reported by respondents as the number one challenge when it comes to an organization's ability to meet regulatory demands. While over 70% of cybersecurity leaders say data privacy regulations complicate incident response, just over one third of respondents reported actually being fined for failing to meet regulatory requirements.

As more organizations adopt modern strategies for incident response, especially for cloud-based environments, and regulators increase their focus on cloud security, it will be interesting to see how these numbers change in the future.



74% of organizations say data privacy regulations complicate incident response

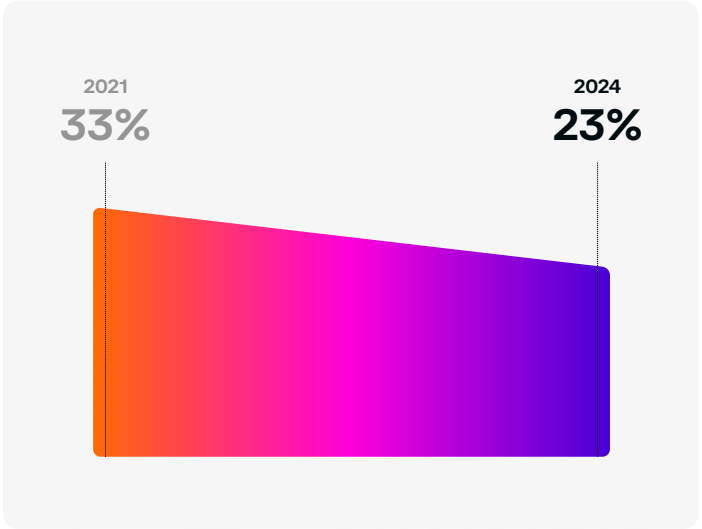
42% of organizations report that the main compliance challenge beyond cloud adoption is the lack of visibility into data

34% of companies have been fined for not meeting regulatory requirements

Organizations are enhancing their cloud investigation capabilities

While businesses have rapidly migrated to the cloud, threat actors have developed specific tools and techniques to exploit cloud environments. With an uptick in cloud-based threats, it has become clear that organizations require new techniques to better secure against evolving threats. Based on a similar survey conducted in 2021, the amount of cloud alerts that went uninvestigated has decreased, indicating that organizations have slightly improved their ability to perform investigations in cloud-based environments.

Organizations report that 23% of cloud alerts are never investigated, compared to over 33% in 2021, indicating that organizations have slightly improved their ability to handle investigations in the cloud



Organizations have budgeted for cloud forensics

The visibility challenges associated with investigation and response in the cloud has organizations increasingly turning to forensics tools. To this end, a majority of organizations (83%) have allocated budget for cloud forensics specifically.

Further, 77% of organizations noted that they expect this overall budget to increase in 2024. This investment emphasizes the growing importance of forensics capabilities in managing cloud security.

83% **of organizations** have a budget for cloud forensics

77% **expect annual overall budget** for cloud forensics and incident response IT security budget to increase in 2024

Future strategies for cloud investigation and response

Organizations are exploring various strategies to perform investigation and response in cloud environments. Naturally, security teams have attempted to leverage existing tools, such as Security Orchestration, Automation, and Response (SOAR) platforms to address these challenges. However, findings indicate that incident response automation is twice as effective as SOAR for cloud investigations. While prioritizing the implementation of automation to enhance an organization's ability to address cloud threats is crucial, this automation must be specifically customized for incident response, rather than applying general automation solutions. Additionally, the vast majority of organizations (95%) believe that AI will play a major role in cloud incident response in the near future.

2X Automation is 2X more effective than SOAR for cloud threat investigations

95% believe AI will play a major role in cloud incident response in the next two years

How Darktrace can help

Darktrace delivers a proactive approach to cyber resilience in a single cybersecurity platform, including cloud coverage.

/ CLOUD

Darktrace / CLOUD is a real time Cloud Detection and Response (CDR) solution built with advanced AI to make cloud security accessible to all security teams and SOCs. By using multiple machine learning techniques, Darktrace brings unprecedented visibility, threat detection, investigation, and incident response to hybrid and multi-cloud environments.

Darktrace's cloud offerings have been bolstered with the acquisition of Cado Security Ltd., which enables security teams to gain immediate access to forensic-level data in multi-cloud, container, serverless, SaaS, and on-premises environments.

Read solution brief ↗

Request demo ↗

Research methodology

This survey was conducted in 2024 by Cado Security in collaboration with TrendCandy and surveyed 300 security decision makers working in organizations based in the United States and United Kingdom.

To qualify for this survey, potential respondents had to be manager level and above, working within either information security or cybersecurity, and involved in cloud security.

Further, surveyed organizations had to use public clouds (e.g. AWS, Azure, GCP) for their business operations.

"With Darktrace / CLOUD, we have **clear reporting, documentation and audit-ready traceability** – exactly what's needed to meet European regulatory standards and the European Banking Authority guidelines."

■ **Risk and Compliance Leader**
Financial Technology Company

■ **About Darktrace**

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com