MITIGA

Datasheet

Mitiga IR² Forensic Data Acquisition Brings Readiness to Cloud-based Incident Response

Mitiga's proactive Forensic Data Acquisition approach enhances the peacetime value provided to enterprises by our Incident Readiness and Response (IR²) solution, using an approach like no other. By collecting forensic logs from dozens of Cloud and SaaS providers as part of initial onboarding, Mitiga shifts crucial Forensic Data Acquisition to complete before the breach occurs — all at zero-cost to IR² customers.

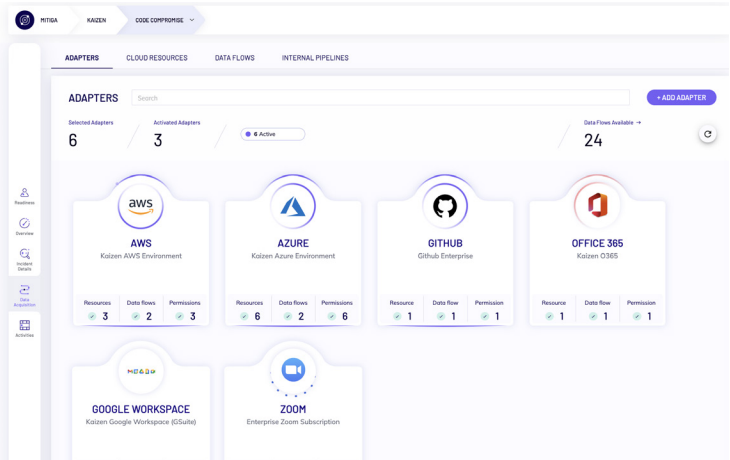
Advanced forensic collection escalates rapid Cloud IR

Detecting a network penetration is frequently a slow process — attackers are typically not identified until months after they have gained access. Part of the difficulty relates to crucial cloud service provider (CSP) and SaaS log data that is not gathered systematically, nor stored for a duration necessary to build an accurate forensic baseline.

Our Forensic Data Acquisition approach automates this process, enabling Mitiga IR² Squad responders to team with customers and quickly focus on unusual activity, rather than racing against the clock ineffectively, retrieving and processing the limited forensic data available.

Forensic Data Acquistion Value

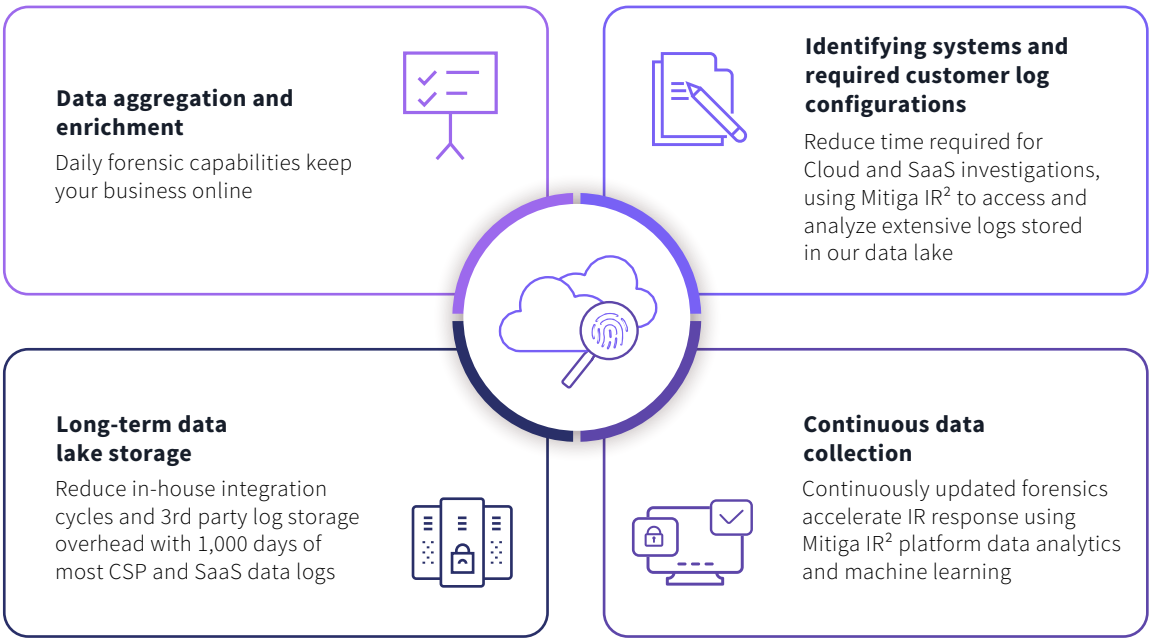
- Enhanced IR Preparedness and Cyber Resilience
- Reduced business downtime, with fast, efficient Cloud and SaaS IR
- Lower integration and data storage overhead
- Advanced IR, with Mitiga Attack Library fine-tuning detections



We collect CSP and SaaS logs during customer onboarding and store them in our tamper-proof data lake in a matter of hours.

IR² Forensic Data Acquisition at work

Proactive IR² Forensic Data Acquisition captures, stores, and processes comprehensive CSP and SaaS forensic logs using these processes.



Mitiga IR² Forensic Data Acquisition collects, transforms, and stores critical forensic data from dozens of CSP and SaaS providers, leveraging our unique Forensics as Code technology to query this data. In enhancing Incident Readiness, Forensics as Code checks collected forensic data and proactively hunts for and investigates potential breaches. When a breach occurs, Forensics as Code automates investigation workflows.

Mitiga's technology and services provide continuous, proactive breach investigation, lower the impact of cyber breaches, and optimize readiness for critical cloud and hybrid incidents. This readiness-first approach accelerates response and recovery time, increasing resilience when incidents occur. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for critical cloud incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** + 972-3-978-6654 | **SG** +65-3138-3094

MITIGA aws partner network