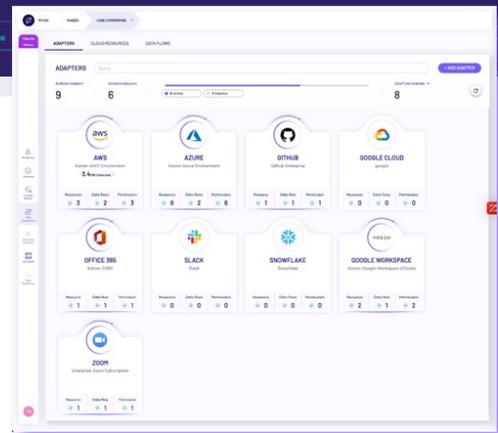


Mitiga IR² Cloud Readiness

Mitiga’s Cloud Incident Readiness and Response (IR²) solution enables organizations to prepare for and recover from breaches faster than any other approach. Mitiga IR² seamlessly integrates with cloud service provider (CSP) and software as a service (SaaS) environments, delivering proactive forensic data collection using an agentless architecture that eases cloud deployment, scalability, and performance.

With our **IR² Cloud Readiness and Resilience packages**, Mitiga has further enhanced cloud IR options for today’s global organizations by including onboarding activities that help our customers get ahead of breaches before the next occurrence and quickly return to business-as-usual operations.



Cloud Readiness Service Definition

For many organizations, there are challenges related to cybersecurity and cloud operations expertise, as well as effective log collection and storage. Our **Cloud Readiness** package delivers value today by enhancing your in-house IT team’s preparedness before breaches occur.

IR ² Cloud Readiness Platform and Services	Definition
<p>Access to IR² Platform</p>	<p>As part of IR² Platform Access and formalized customer introduction activities, Mitiga Squad subject matter experts (SMEs) conduct an onboarding Kickoff Meeting with key customer stakeholders. The Kickoff Meeting focuses on IR² platform onboarding activities and provides a formal customer introduction to their Mitiga Squad. Mitiga Squad SMEs coordinate customer communications capabilities for 24/7/365 availability via Call Center, Slack, and 1Password.</p> <p>Mitiga SMEs coordinate IR² platform access for up to five customer contacts. The IR² platform:</p> <ul style="list-style-type: none"> • Enables scalable, rapid cloud IR response • Increases situational awareness • Delivers Cloud Log ingestion, Incident Documentation/Timelining, and Incident Dashboard features

IR ² Cloud Readiness Platform and Services	Definition
Forensic Data Acquisition	<p>The Mitiga Squad identifies required CSP/SaaS logs, then collects them continuously thereafter.</p> <p>As part of Forensic Data Acquisition, Mitiga identifies which vendor-specific logs should be collected, with flexibility to assist monitoring for the newest threats.</p> <p>Logs are securely stored for up to 1,000 days for our CSP/SaaS connectors in Mitiga's Data Lake.</p> <p>Aggregated for use in the Mitiga Cloud Attack Scenario Library (CASL), Mitiga's Forensics as Code technology queries this data to proactively hunt for and investigate potential breaches in the customer environment.</p>
Forensic Data Readiness	<p>The Data Readiness Assessment provides review of forensic data and configuration, ensuring settings meet industry standards for cloud investigations.</p> <p>Mitiga SMEs review the customer's forensic data, checking for completeness and availability, including:</p> <ul style="list-style-type: none"> • Cloud and SaaS forensics data • Security configurations • Event data
Threat Hunting	<p>When a new malicious pattern is detected at another client or a relevant, industry-wide breach has occurred, Mitiga will proactively hunt for similar patterns in the customer environment.</p> <p>The Mitiga CASL and Forensics as Code automate detections and hunting filters to accelerate investigations.</p>

Mitiga's technology and services optimize readiness for cloud and hybrid incidents and accelerate both response and recovery times when incidents occur. Importantly, Mitiga's resilience prioritization also enhances rapid return to business-as-usual organizational operations.

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

