WIZ + aws

AWS Security Incident Response

JOINT SOLUTION BRIEF

Executive summary

Wiz Defend and AWS Security Incident Response together empower SecOps teams to detect, investigate, and respond to cloud threats with precision and speed. By combining Wiz's deep cloud context with AWS's automated response framework, teams gain a unified view of cloud activity and a streamlined incident response workflow.

Wiz Defend delivers high-fidelity alerts built for cloud scale, helping teams cut through noise and focus on what matters most. AWS Security Incident Response (SIR) enhances that power with automation, communication, and direct access to the AWS Customer Incident Response Team (CIRT). Together, they enable faster, more confident decisions that reduce risk and operational overhead across the cloud environment.

Market challenge

In modern cloud environments, incident response remains fragmented and slow. Security teams often rely on disconnected tools that generate too many alerts and too little context, making it difficult to identify which threats matter most. Manual processes for escalating incidents to response teams add delays and increase risk exposure. Legacy solutions lack the automation and cloud context needed to connect detection with response, leaving organizations struggling to meet the speed and scale of today's cloud attacks.

Benefits of the integration

- **Contextualized Alerts for Actionable Insights:** Deliver clear, detailed context from Wiz Defend to the AWS SIR teams enabling faster, more informed remediation and response decisions.
- **Unified Visibility & Prioritized Response:** Utilize Wiz's complete visibility across cloud environments and runtime monitoring to detect and prioritize emerging cloud threats, ensuring the most critical issues are surfaced to share with AWS SIR.
- **Reduced MTTR and Improved Efficiencies:** Create an AWS SIR case directly in Wiz Defend, sharing real-time threat details from Wiz with AWS to accelerate incident resolution.

The better together story

Wiz and AWS Security Incident Response work seamlessly to accelerate detection, investigation, and recovery. Wiz brings deep cloud context through the Wiz Security Graph and AI-driven threat storylines that guide teams through what happened and its impact, helping identify and prioritize high-fidelity threats. AWS Security Incident Response provides hands-on expertise through the AWS Customer Incident Response Team (CIRT), helping investigate and contain threats quickly.

Together, Wiz and AWS enable faster Mean Time to Respond (MTTR) and more effective incident response. Security teams gain real-time collaboration between both platforms and experts, ensuring they can move as fast as the threats they face.

Challenge and Solution Overview

Challenge: Limited Visibility and Fragmented Response

The complexity of modern, distributed cloud stacks makes it hard to maintain a clear, organization-wide view of security posture. Traditional tools lack the context to map activity to the MITRE ATT&CK framework, slowing detection and response. Without a single source of truth, teams struggle to prioritize critical threats and coordinate an effective response.

Solution: Unified Cloud Detection and Response with Wiz Defend and AWS SIR

Wiz Defend and AWS Security Incident Response empower security teams with centralized visibility and seamless incident handling across multi-cloud environments. When Wiz identifies a high-fidelity threat, the integration uses the AWS Security Incident Response (SIR) API to automatically open a case with AWS. This eliminates manual handoffs and immediately engages the AWS Incident Response team to investigate and contain the incident. Wiz Defend provides detailed threat intelligence and context, while AWS Security Incident Response accelerates remediation and ensures alignment with governance standards.

Together, Wiz and AWS SIR deliver a scalable, automated approach to detect, prioritize, and respond to threats faster, strengthening organizational resilience in the cloud.