mitiga

Mitiga Solution Brief

Stop Active SaaS Attacks In Their Tracks

One unified, agentless platform delivers Agentic Runtime Security across SaaS, cloud, and AI.

Modern attackers don't break in. They log in through stolen identities and abused OAuth grants, trusted integrations, APIs, and embedded AI workflows. While SaaS security posture management (SSPM) helps identify exposure, enterprises need a real-time safety net and compensating control for when posture gaps cannot be closed quickly. That means runtime visibility, investigation-grade context, and response that can detect misuse, reconstruct what happened, and contain the attack before impact.

Visibility gaps

SOC teams struggle to achieve a panoramic view across their SaaS apps and identities. The result is missed detections, fragmented context, and slower response.

Manual triage

Stitching together attack paths from disconnected data sources consumes valuable time and delays critical response. Modern SaaS attacks do not wait for manual analysis.

SaaS sprawl

Hundreds of apps, integrations, OAuth connections, APIs, and service accounts expand the attack surface faster than siloed tools and teams can keep up.

Identity chaos

By abusing stolen credentials, tokens, and over-permissioned human and non-human identities, attackers gain access that looks legitimate and often goes undetected.

Embedded AI risk

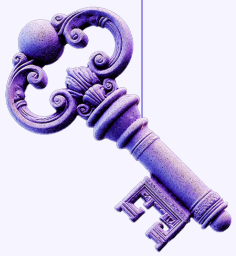
SaaS now includes copilots, AI agents, and API-driven automation —extending the runtime attack surface from human users to AI-connected workflows and autonomous agents.

AI-enabled attacks

Threat actors are weaponizing AI to accelerate phishing, reconnaissance, credential abuse, and cloud-speed attacks. Human-only response models will not keep pace.

“Thank God we had Salesforce logs in Mitiga to stop the Salesloft attack! We need to have as much coverage by Mitiga as possible.”

SecOps Leader, Major Publishing Firm



Attackers will get in. It's never been easier. What matters is whether the attack causes impact.

Preemptive, real-time detection and response across SaaS, cloud, AI, and identity.

Mitiga gives cloud-first enterprises a critical safety net across today's expanding SaaS and AI attack surface. Built for the reality that attacks are inevitable, Mitiga's AI-native cloud detection and response platform (CDR) delivers Zero-Impact Breach Prevention by turning fragmented runtime signals into high-fidelity incidents, clear attack timelines, and guided or autonomous containment.

Mitiga AI-native CDR: Agentic runtime SaaS defense

How do you stop an attacker with stolen credentials before they turn access into impact?

Mitiga detects, investigates, and contains active SaaS attacks in real time—including identity compromise, OAuth abuse, connected-app misuse, and malicious API activity across business-critical applications such as Salesforce, Workday, Microsoft 365, GitHub, Google Workspace, Jira, Confluence, ServiceNow, and more.

Runtime security now extends to embedded AI within your SaaS

SaaS security no longer stops at human users and includes:

- Embedded AI copilots
- Autonomous AI agents
- API-driven workflows
- Non-human identities operating against sensitive business data

Mitiga treats AI-connected SaaS activity as part of the same runtime defense fabric as SaaS, cloud, and identity.

mitiga

Stop SaaS attacks now.

Learn how Mitiga helps cloud-first security teams prepare for incidents, investigate faster, and respond before business impact.

www.mitiga.io/demo

Mitiga solves 4 key SaaS risks

01 Inability to detect and stop active SaaS threats

Mitiga continuously analyzes SaaS activity for compromised tokens, suspicious connected-app use, anomalous API access, identity misuse, and data exfiltration patterns – before they become headlines.

02 Manual SOC processes that slow down response

Mitiga automatically correlates SaaS, cloud, identity, and AI threat signals into a single attack timeline. What normally takes days of console pivoting and log stitching is compressed into one coherent incident view.

03 Accepted risk from posture gaps the business cannot close quickly

When a posture gap stays open for months or years, the organization needs a compensating control. Mitiga watches the open window in real time, detects exploitation, reconstructs what happened, and stops impact before it spreads.

04 New runtime exposure from embedded AI and SaaS automation

Modern SaaS applications now include embedded AI, copilots, and agents. Mitiga extends runtime security to these AI-connected SaaS workflows, service identities, and trust relationships.