

Marlin AI™ Autonomous AI-powered SaaS Security

Correlate and investigate security indicators faster — no manual analysis.

The Challenge

Security and IT teams are stretched thin. The rapid expansion of SaaS and AI applications has created an attack surface that grows faster than any team can manually monitor. The result: crushing alert volumes, chronic investigation fatigue, and security analysts spending the majority of their time correlating logs, events, and data; instead of remediating threats. Without deep SaaS context, generalized AI tools can't cut through the noise or offer relief. Critical indicators get missed, investigation timelines balloon, and organizations are left reactive in an increasingly automated threat landscape.

Less Investigating. More Resolutions with Marlin AI.

Marlin AI™ transforms how security teams operate inside SaaS, and this specialty is what sets it apart. Unlike generalized AI tools that lack deep application context, Marlin AI understands SaaS the way AppOmni does, making its correlations accurate, its investigations meaningful, and its remediation guidance actionable. It autonomously surfaces security signals, conducts in-depth investigations, and delivers prescriptive guidance grounded in AppOmni Labs' deep SaaS security expertise.

All of this happens without custom configuration, scripting, or third-party integrations. The result is a meaningful reduction in mean time to investigate (MTTI) and mean time to resolve (MTTR), freeing security teams to focus less on researching issues and more on implementing solutions.



THE BENEFITS

- **More than Gen AI.** An autonomous security engine built from an AI toolbox including machine learning and data science; not a conversational assistant, that turns data into decisions.
- **Reduced MTTI.** Automatically correlates signals that need attention to perform in-depth investigations across your entire SaaS ecosystem.
- **Reduced MTTR.** Provides guided remediation methods for security teams from investigations for actionable solutions.



KEY USE CASES

- **Overstretched security teams.** Organizations with lean security teams that cannot keep pace with the volume and complexity of SaaS security monitoring.
- **Complex, multi-application SaaS environments.** Enterprises running multiple business-critical SaaS applications where security indicators span systems and require cross-platform correlation.
- **Maturing SaaS security programs.** Teams looking to operationalize SaaS security without building deep in-house expertise or relying on manual investigation workflows.

Marlin AI™ Observations

Marlin AI is an autonomous SaaS security AI that starts investigating your connected services and provides security recommendations.

Risk: High Service Type: ServiceNow

Investigation of top 3 identities with administrative access

SaaS Security Analysis Summary

6 detection alerts, 116 occurrences, and 30 objects analyzed administrative access misconfigurations and high-risk authentication permissions and lack of essential security controls, alongside Critical administrative access misconfigurations and authentication systems, while a potential exploitation alert requires urgent investigation.

Risk: Critical Observed: 05/19/2026, 05:02 AM Service Types: ServiceNow

Investigation of AI agents in the ServiceNow monitored services

ServiceNow AI Security Posture and Threat Analysis

Review 20 posture findings and 47 threat detection alerts related to AI agents in ServiceNow Production, recommending remediation for critical misconfigurations and suspicious prompting attempts. Significant risks include unrestricted AI skill ACL modification, disabled AI search field security, and persistent user attempts to manipulate AI agents for unauthorized actions, such as updating administrator passwords, indicating potential T1648: Serverless Execution.

Risk: High Observed: 05/21/2026, 03:00 AM Service Types: ServiceNow

Investigation of AI agents in the ServiceNow monitored services

Observed by Marlin AI

Playbook Details

This playbook runs once per day and investigates observations related to AI agents in the ServiceNow monitored services. Data from threat detection alerts as well as findings are used in this investigation.

Risk: High Service Types: ServiceNow Observed: 05/21/2026, 03:00 AM

Summary

ServiceNow AI Security Posture and Threat Analysis

Review 20 posture findings and 47 threat detection alerts related to AI agents in ServiceNow Production, recommending remediation for critical misconfigurations and suspicious prompting attempts. Significant risks include unrestricted AI skill ACL modification, disabled AI search field security, and persistent user attempts to manipulate AI agents for unauthorized actions, such as updating administrator passwords, indicating potential T1648: Serverless Execution.

Analysis Remediation Supporting data

Data Analyzed: This analysis is based on **20 unique posture findings** and **47 unique threat detection alerts** related to AI agents in ServiceNow, across 3 monitored services.

Links to Data Analyzed:

- [Findings related to AI security in ServiceNow](#)
- [Alerts related to AI security in ServiceNow](#)

See Marlin AI in Action

Your SaaS environment isn't waiting for threats to be manually investigated. Neither should you. [Learn more about Marlin AI](#) or [request a demo](#).

About AppOmni

AppOmni prevents SaaS data breaches by delivering end-to-end SaaS and AI security. Our platform gives security teams unified visibility into posture, access, third-party connections, and AI-related activity — applying the same SSPM principles to AI security. With continuous monitoring, real-time threat detection, and autonomous correlation of security signals, AppOmni helps enterprises identify, respond to, and block threats across their entire SaaS environment. Request a personalized demo at appomni.com/demo or get in touch with one of our security experts at info@appomni.com.