Agentic AI Security for ServiceNow

Visibility, control, and protection for Now Assist AI agents operating within ServiceNow

The Challenge

AI is transforming how organizations use ServiceNow to automate workflows and improve productivity. As AI agents handle more operational and decision-making tasks, they introduce new security and compliance risks.

Limited visibility, misconfigurations, and unsafe prompts can expose sensitive data or disrupt workflows. Securing agentic AI requires real-time control and protection.

The Solution

AppOmni agentic AI security for ServiceNow extends our market-leading SaaS Security Posture Management (SSPM) platform with foundational AI Security Posture Management (AISPM) capabilities that deliver near real-time visibility, control, and protection for AI agents in ServiceNow.

The evolution of SaaS security must include AISPM, AI Threat Detection & Response (AITDR), and AI Prompt Security to keep pace with the speed and autonomy of agentic AI.

AppOmni AgentGuard, a real-time defense engine for ServiceNow Now Assist AI agents, blocks prompt-injection attempts, identifies and contains DLP violations, and suspends repeat offenders before additional damage occurs.

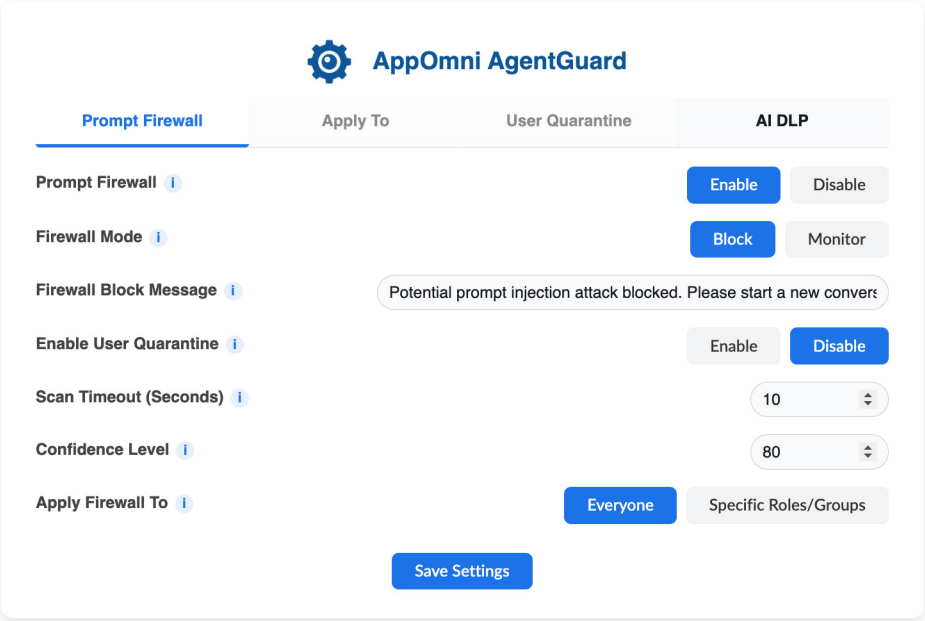
AppOmni AgentGuard ensures ServiceNow Now Assist AI agents operate securely, consistently, and comply with enterprise policies. AppOmni combines continuous posture checks, AI agent inventory, and behavior analysis to safeguard data, minimize risk, and promote safe AI use across ServiceNow environments.

THE BENEFITS

- **Prevent AI-driven breaches** by blocking unsafe prompts.
- **Stop sensitive data exposure** to LLMs using AI-DLP.
- **Gain visibility** into all AI agents and activities.
- **Enforce secure configurations** to reduce compliance risk.
- **Detect malicious prompts** before data exposure occurs.
- **Extend SaaS security controls** to AI agents.

KEY FEATURES

- AppOmni AgentGuard
- AI Agent Inventory
- AI Agent Posture Policy
- Action Analysis
- AI-centric AppOmni Insights



> "Adopting AI without first sorting your SaaS security means you're layering two complex security challenges, which will only exacerbate existing issues."
>
> **Oli Newbury, Former Global Financial Services CISO**

What Powers AI Agent Security

AppOmni AgentGuard works with agent inventory, continuous posture checks, and behavior analysis to deliver complete visibility and real-time defense for Now Assist AI agents in ServiceNow. These capabilities form the foundation of agentic AI security for ServiceNow.

The table below outlines each feature and its security impact.

Feature	How It Works	Security Impact
AppOmni AgentGuard	Reviews and optionally blocks malicious or unsafe prompts before execution.	Prevents data exfiltration and unauthorized AI actions in real time via prompt injection.
AI Agent Inventory	Maps all AI agents, their access, and activity across SaaS apps.	Eliminates visibility issues and highlights over-permissioned or risky agents.
AI Agent Posture Policy	Continuously checks and enforces secure AI agent configurations.	Reduces misconfigurations and ensures compliance with security standards.
AI Agent Action Analysis	Analyzes agent actions after execution.	Detects abnormal or unsafe activity to speed investigation and response.
AI-centric AppOmni Insights	Context-aware scans analyze AI/LLM deployments to uncover hidden risks and misconfigurations.	Detects unseen vulnerabilities and AI-specific risks missed by traditional SaaS scans.

Why AppOmni

- Proven leader in SaaS and AI security
- Deep, native expertise securing complex ServiceNow environments
- Unified platform delivering continuous visibility, control, and protection