Agentic AI security with Cisco AI Defense and AppOmni AgentGuard

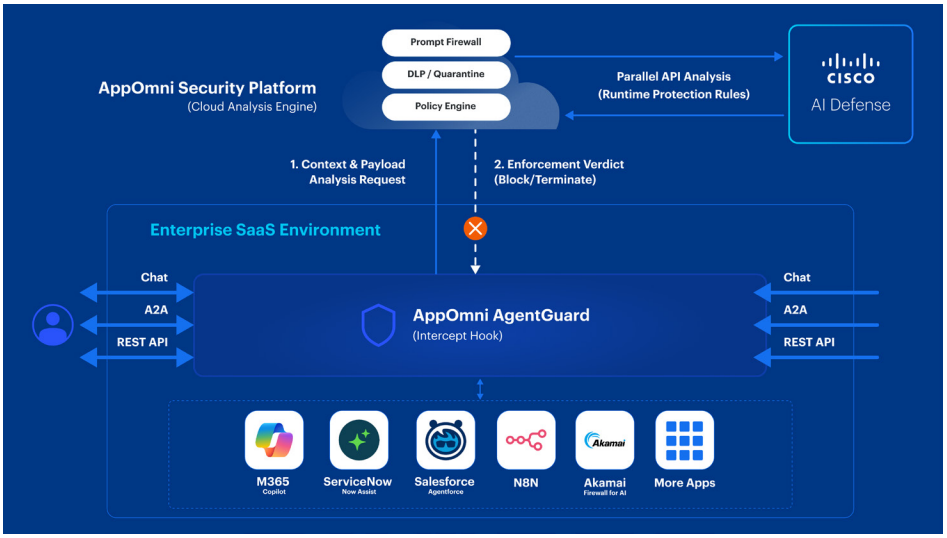
The Challenge

AI agents are proliferating across enterprise SaaS environments, operating with broad permissions and little oversight. Traditional zero trust network access (ZTNA) and SaaS security posture management (SSPM) controls were not designed to monitor agentic behavior, leaving organizations exposed to prompt injection attacks, potential data leakage, silent data exfiltration, and overprivileged non-human identities. Security teams have no native visibility into what AI agents access, modify, or share, and no audit trail to support compliance or incident response.

The Solution

AppOmni AgentGuard extends Cisco AI Defense into the SaaS layer, applying zero trust principles to every agentic workflow. Together, they deliver real-time monitoring of AI agent activity, detection and prevention of prompt injection attacks, policy-based controls on data movement, and continuous least-privilege enforcement across connected SaaS applications.

Cisco AI Defense policies propagate directly into AppOmni's platform controls, creating a single source of truth for agentic AI security posture.



THE BENEFITS

- **Complete agentic visibility.** Real-time, auditable view of every action AI agents take across connected SaaS apps.
- **Proactive threat prevention.** Prompt injection attacks and unauthorized data movement are detected and blocked before they cause harm.
- **Unified policy governance.** Consistent security posture from AI model to SaaS application, with no policy gaps.

KEY USE CASES

- **Real-time agent monitoring** Full visibility into what AI agents access, modify, and share across connected SaaS apps in real-time.
- **Prompt injection detection and preventative action** Identifies adversarial payloads embedded in SaaS content before they can hijack agent behavior or exfiltrate data and stops it.
- **Unified policy governance** Cisco AI Defense policies propagate into AppOmni's SaaS controls. One source of truth for agentic security posture.

How AppOmni AgentGuard can help

AgentGuard integrates natively with Cisco AI Defense, combining Cisco's AI threat intelligence and policy engine with AppOmni's deep SaaS access graph. AgentGuard operates where risk actually materializes: inside the SaaS applications where AI agents read, write, access, and move business-critical data. Here is how the integration works:

- **Connect.** AgentGuard passes agent interaction data to Cisco AI Defense for inspection, including identity, session context, and full conversation history.
- **Set enforcement rules.** Define how AgentGuard responds when Cisco AI Defense flags a violation. Configure a violation threshold and customize what users see when they are locked out.
- **Apply policy.** Security, privacy, and safety guardrails are configured in Cisco AI Defense. AppOmni passes the data. Cisco applies the rules.
- **Block violations.** When Cisco AI Defense flags a data loss prevention (DLP) or prompt firewall violation, AgentGuard enforces the decision instantly, quarantining users who breach the threshold stopping the agent before any data is exposed or further action is taken
- **Review and audit.** Every flagged event is logged in Cisco Cloud Control with source, violation type, severity, and the enriched context passed from AgentGuard.

Cisco AI Defense and AppOmni AgentGuard is everything your security team needs to investigate, audit, or escalate AI security threats.

See AppOmni in Action

Discover how AppOmni secures your SaaS environment with continuous monitoring, policy enforcement, and deep visibility. Learn more about our partnership or request a demo.