

Modern Platforms

Cisco AI Defense

THE CHALLENGE

Organizations are rapidly adopting AI models, applications, agents, and MCP-enabled workflows, but many lack visibility into AI assets, Shadow AI usage, and AI supply chain dependencies. This increases exposure to security, governance, and compliance risks while making it difficult to securely scale AI initiatives.

THE SOLUTION

Presidio's Cisco AI Defense is a structured professional services engagement designed to help organizations establish visibility into their AI environment, assess AI-specific security risks, deploy runtime protections, and build a roadmap for secure AI adoption. The engagement includes AI asset discovery, AI model and application validation, runtime protection configuration, AI supply chain risk management capabilities, executive reporting, and a prioritized roadmap for the next 90-days.

THE APPROACH

Presidio leverages Cisco AI Defense to discover AI assets, validate AI applications through algorithmic red teaming, and implement runtime protections for models, agents, and workflows. The engagement combines visibility, validation, protection, and governance capabilities across the AI lifecycle.

KEY BENEFITS

- ◆ Establish visibility into AI assets, models, agents, MCP servers, and Shadow AI activity.
- ◆ Identify AI security risks through algorithmic red teaming and validation testing.

- ◆ Implement runtime guardrails to protect AI applications, agent workflows, and model interactions.
- ◆ Improve AI governance through AI BOM generation, MCP discovery, and supply chain risk management capabilities.
- ◆ Deliver executive-ready findings and a prioritized roadmap for expanding AI security capabilities.

WHY PRESIDIO

Clients choose Presidio to lead their modern platform and hybrid cloud journey because we put their business requirements first. We go deep in each major vendor's technology – 80+ products across 20+ vendors – but we're not tied to any one vendor. Our full services lifecycle, led by data center architects, engineers and managing consultants with more than eight years with Presidio on average, can handle strategy PLUS execution PLUS ongoing management of your modern platform.

DISCOVER. DETECT. PROTECT.

Built on Cisco AI Defense, Presidio helps organizations discover AI applications and Shadow AI activity, validate models and applications through advanced testing, and protect AI interactions using runtime guardrails and enforcement controls. The engagement provides visibility into AI risk, governance of AI assets, and a prioritized roadmap for secure AI adoption.

Schedule your Cisco AI Defense Quick Start Assessment.

Contact Presidio today:
www.presidio.com/contact-us