paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

# Secure AI by Design

## Where AI Adoption Meets Security

## Undeniable Reality: Rapidly Accelerating AI Usage

Governments and businesses are embracing AI for unprecedented efficiency and competitive advantages. The choice has become clear: Integrate AI into your operations or risk having business or geopolitical competitors outpace you. But, rapid AI adoption has exposed organizations' AI infrastructure—the AI models, agents, data, and beyond—to unique threats that traditional cybersecurity solutions weren't explicitly designed to address.

**2025 Federal AI Use Case Inventory**

41 government agencies reported a total of 3,611 AI use cases, up 70% from 2024.

## Our Mandate: Ensure AI Is Secure

The only viable path forward is to fully embrace AI, while ensuring that unacceptable security risks do not compromise the pursuit of innovation. Through numerous policies, governments are now increasingly recognizing AI security as a fundamental prerequisite to AI deployment, but how governments define AI security remains poorly articulated. The unique attributes of the AI era demand an evolved approach to security.

## Framework to Secure Our AI-Powered Future

| Elements | Examples |
|---|---|
| **AI Ecosystem**<br>WHAT WE NEED TO SECURE | AI applications, AI agents, AI models, AI data, AI infrastructure, and user interaction with AI systems. |
| **AI Threats**<br>WHAT WE NEED TO SECURE AGAINST | Security and safety risks unique to the development, deployment, and use of AI applications and systems, including techniques described in common frameworks such as MITRE ATLAS® and the OWASP Top 10 for LLMs. |
| **AI Standards and Guidelines**<br>HOW WE DEFINE COMPREHENSIVE AI SECURITY | Emerging standards and guidelines on AI security such as NIST CSF "AI Cyber Profile," NIST "SP 800-53 Control Overlays for Securing AI Systems," and CISA joint Five Eyes AI security guidance series, as well as *Careful adoption of agentic AI services*, ETSI EN 304 223 on Securing Artificial Intelligence, and CSA Singapore *Guidelines and Companion Guide on Securing AI Systems*.<br>**Common pillars:** Discover, Assess, and Protect. |
| **AI Security Capabilities and Technologies**<br>HOW TO SECURE AGAINST THREATS TO THE AI ECOSYSTEM | AI artifact scanning, AI posture management, AI red teaming, AI runtime security, AI identity security, agent security gateway, endpoint agent gateway, and AI access security. |