paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Secure AI by Design

Proving That AI Adoption and AI Security Are Complementary

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 being outpaced by business or geopolitical competitors who do. But rapid AI adoption has exposed the AI ecosystem— the AI models, agents, data, infrastructure, and beyond—to unique threats that traditional cybersecurity solutions were not explicitly designed to address.

2024 Federal AI Use Case Inventory

41 government agencies reported a total of 2,133 AI use cases, up from just 710 in 2023.*

* "2024 Federal AI Use Case Inventory," US Chief Informations Officers Council, December 16, 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 adoption, but how governments define "AI security" remains poorly articulated. The unique attributes of the AI era demand an evolved approach to security.

Secure AI by Design: A Policy Roadmap for Securing our AI Future

Elements	Examples
AI Ecosystem WHAT WE NEED TO SECURE	AI applications, AI agents, AI models, AI data, AI infrastructure, and user interaction with AI tools.
AI Threats 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. For example, these risks include prompt injection, data and model poisoning, and excessive agency.
Secure AI by Design Framework HOW TO DEFINE A COMPREHENSIVE AI SECURITY APPROACH	Organizations need to prioritize the following four critical security imperatives in the AI era: • Securing use of external AI tools. • Monitoring and controlling AI agents. • Securing underlying AI infrastructure and data. • Safely building and deploying AI apps.
AI Security Technologies HOW TO SECURE AGAINST THREATS TO THE AI ECOSYSTEM	A unified approach that protects every layer of the AI stack—combining AI model security, AI posture management, AI red teaming, AI runtime protection, AI agent security, AI access security, and secure browser controls.