Unit 42
AI Security Assessment

Unlock AI Potential with Expert Security Insights and Guidance

AI Adoption Challenges

AI is evolving at a rapid pace, and many organizations struggle to build a comprehensive understanding of its unique risks and governance strategies. Without a solid grasp of best practices for securing AI environments, you must rely on employees to make the right decisions in a continuously changing landscape.

The intense pressure to innovate quickly further complicates this reactive approach, often leading to a higher prioritization of speed over security. Critical steps to protect sensitive data, secure AI development processes, and address potential vulnerabilities are easy to overlook. Without a strategic framework in place, organizations risk exposing themselves to avoidable threats in their AI initiatives, including:

Shadow AI Use

Employees are increasingly using AI tools to do their work, often without proper approvals or security controls. Recent research indicates that 50% of employees are using unauthorized AI tools and 46% of these users indicate they would continue using these tools even if explicitly banned by their organizations,[1] exposing organizations to malware, data leakage, and compliance risks.

Rapid AI Transformation

A recent study found that 78% of organizations reported using AI in 2024, up from 55% the year before.[2] As organizations move quickly to keep pace with this transformation, AI solutions are being developed without proper security controls and considerations.

AI Attack Surface

Attackers are increasingly targeting vulnerable AI integrations and injecting malicious prompts into AI-generated content. This growing wave of attacks on AI applications, models, and data increases the risk of malicious inputs, compromised large language models (LLMs), model-generated threats, and accidental data exposure.

Unit 42 AI Security Assessment Benefits

Reduce AI adoption risk

Gain insights into employee AI interactions to identify and control AI applications in use and implement controls to manage risks effectively.

Secure AI innovation

Safeguard your AI initiatives with tailored and threat-informed strategies for your data, models, and applications.

Strengthen AI governance

Receive a forward-looking AI strategy and guardrails to establish a robust AI security framework aligned with your business priorities.

A Better Approach: Unit 42 AI Security Assessment

Securing AI requires structure and clarity. As your organization rapidly embraces AI, there's an opportunity to align security efforts in a way that supports innovation.

The Unit 42 AI Security Assessment provides visibility and security best practices to support responsible AI use and development within your organization. The service leverages the power of the Palo Alto Networks security platform to deliver unmatched speed and scale to identify and mitigate AI-related risks across your enterprise. We build on this technology with our industry-leading threat intelligence and AI expertise to deliver tailored best practices specific to your AI footprint, empowering your organization to adopt and innovate confidently with AI.

Build a Strong Foundation for Secure AI Adoption

Safeguard Employee AI Usage

Identify and control the AI applications and services that employees are using. Understanding how employees are using AI tools is a strong starting point. While everyday network traffic is typically well understood, AI usage requires a deeper look.

Protect AI Development and Supply Chain

As you build your own AI applications, a secure development process and architecture become essential. AI systems often operate like black boxes, making it important to trace the usage and lineage of data and models for greater transparency and accountability.

Secure AI Runtime

AI application runtime protection requires monitoring to detect threats like LLM prompt injections and adversarial inputs. Regular testing—through both automated tools and human-led threat modeling or red teaming—helps uncover vulnerabilities and strengthen defenses.

AI-Driven Security Operations

By transforming your SOC with AI, you can unify data sources for real-time insights, automate repetitive tasks, and accelerate incident response. Attackers also use AI, but to accelerate their attacks and make them more effective, so defenders must keep up.

About Unit 42

Palo Alto Networks Unit 42® brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. Our consultants serve as your trusted advisors to assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time. For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com.

1. The Shadow AI Surge: Study Finds 50% of Workers Use Unapproved AI Tools, Apri 18, 2025.
2. Artificial Intelligence Index Report 2025: Stanford University Human-Centered Artificial Intelligence, April 7, 2025.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.