AI Secure FAQ

1. What is AI Secure?

A: AI Secure is a comprehensive solution that ensures the safe, secure, and ethical use of AI across your organization. It provides real-time risk detection, threat prevention, and governance capabilities to protect sensitive data, maintain compliance, and promote responsible AI adoption among employees.

2. Why do organizations need AI Secure?

A: With the rapid adoption of generative AI, employees often use AI tools without visibility or controls, leading to risks such as data leakage, prompt injection, malicious responses, and policy violations. AI Secure eliminates these risks by offering full visibility, runtime protection, and governance for all AI activities.

3. How does AI Secure protect against AI-related threats?

A: AI Secure uses real-time monitoring and NLP-based detection models to identify and block:

- Prompt injection and jailbreak attempts
- Unsafe or malicious AI responses
- Data exfiltration via AI prompts
- Harmful or misleading AI-generated content

It enforces runtime guardrails to prevent unsafe interactions before damage occurs.

4. What makes AI Secure different from traditional security tools like CASB or DLP?

A: Traditional tools were not designed for AI-driven interactions or natural language–based risks. AI Secure adds a contextual understanding layer using AI-aware inspection, enabling it to:

- Understand and analyze natural language prompts
- Detect intent and semantic risk, not just keywords
- Enforce AI-specific data and compliance policies
- Govern employee AI behavior across sanctioned and unsanctioned tools

5. What are the core pillars of AI Secure?

A: AI Secure is built on three key pillars:

- Discovery & Insight – Identify all AI tools, users, and data interactions (Shadow AI visibility).
- Runtime Protection & Prevention – Detect and stop unsafe prompts, malicious responses, and sensitive data exposure in real time.
- Governance & Reporting – Maintain compliance with evolving AI regulations (EU AI Act, NIST AI RMF, ISO) and provide audit-ready reporting.

6. How does AI Secure help with compliance and governance?

A: AI Secure automatically maps AI usage to key compliance frameworks, including:

- EU AI Act
- ISO 42001 (AI Management System)
- NIST AI Risk Management Framework
- SOC 2 / GDPR alignment

It provides policy-based access control and ensures ongoing responsible AI governance.

7. Can AI Secure detect "Shadow AI" usage?

A: Yes. AI Secure's Discovery & Insight module continuously monitors AI traffic to detect unauthorized or unknown AI tools used by employees. It provides app risk scores, usage dashboards, and user-level visibility, helping security teams control unapproved AI usage.

8. How does AI Secure prevent data leaks to public AI tools like ChatGPT or Gemini?

A: When employees interact with AI platforms, AI Secure inspects prompt and response content in real time. If sensitive data (PII, source code, CC, etc.) is detected, AI Secure can:

- Block / Deny the prompt
- Coach the user with feedback
- Log the event for audit and compliance tracking

9. How is AI Secure delivered and deployed?

A: AI Secure is a cloud-delivered solution, requiring no endpoint agent or complex setup.

10. How does AI Secure integrate with existing security tools?

A: AI Secure integrates seamlessly with:

- SIEM / SOAR for incident visibility and response
- Identity providers (Okta, Azure AD) for user context

11. How is AI Secure's protection enforced in real time?

A: AI Secure sits in the AI interaction path, analyzing prompts and responses on the fly. It applies AI Guardrails using:

- NLP based context analysis
- Policy-driven action (block, coach, allow)
- Continuous learning from user and threat patterns

12. How does AI Secure promote responsible AI usage among

A: AI Secure embeds user coaching directly into the workflow, providing real-time feedback when unsafe or non-compliant prompts are detected. This helps employees learn responsible AI behavior, fostering trust, and accountability while maintaining productivity.

13. What benefits does AI Secure provide to CISOs and compliance teams?

- 360° visibility into all AI activity and risks
- Reduced data exposure from unsanctioned tools
- Continuous compliance and audit readiness
- Improved employee AI awareness
- Stronger overall AI security posture

14. What ROI can organizations expect from AI Secure?

A: Customers typically see:

- 20–30% reduction in AI-related security incidents
- 55% cost optimization with NLP model improvements
- Higher user productivity due to safe enablement of AI tools
- Faster compliance reporting through automation