

# Secure AI Enablement Platform

## Enable Enterprise AI, Safely

### THE AI SECURITY AND GOVERNANCE CHALLENGE

Organizations are rapidly adopting AI to drive innovation and productivity, but this adoption presents significant security challenges:

- **Unmanaged AI proliferation:** Most organizations use 3-5X more AI tools than they realize
- **Data leakage risks:** Employees inadvertently share sensitive information with external AI models
- **Model manipulation:** Public-facing chatbots vulnerable to prompt injection and jailbreak attacks
- **Compliance concerns:** Lack of visibility and controls to demonstrate regulatory adherence
- **Supply chain risks:** Open-source models may include backdoors or harmful code

### SECURE AI INTERACTIONS WITHOUT HINDERING INNOVATION

WitnessAI empowers enterprises to safely adopt AI with comprehensive security across all interactions—from shadow AI discovery to runtime protection—without compromising business innovation. Through network-level integration with your existing security stack, we capture all AI activity without productivity-killing agents or browsers.

### PROVEN RESULTS

- ✓ 3000+ AI APPLICATIONS DETECTED
- ✓ 99% OF MALICIOUS PROMPTS BLOCKED
- ✓ 24+ RISK DIMENSIONS ANALYZED
- ✓ 3-5X MORE SHADOW AI USAGE FOUND THAN EXPECTED

### SECURE AI ENABLEMENT PLATFORM

#### DISCOVER

Find every AI tool and conversation in your environment

- Catalog thousands of AI applications, including shadow AI
- Capture actual conversations to understand what information is being shared
- Classify interactions by intent for smarter policy enforcement

#### PROTECT

Shield models and chatbots from manipulation

- Block prompt injections and jailbreak attempts before they reach your models
- Filter harmful or off-brand responses before they reach users
- Tokenize sensitive data in real-time while maintaining usability
- Monitor organizational behavior to detect insider threats

#### CONTROL

Enforce policies based on user intent and context






- Create department and role-specific AI governance
- Generate comprehensive audit trails for compliance
- Route requests intelligently to appropriate models based on sensitivity
- Secure VIPs with high privacy mode Role Based Access Control

#### ANALYZE





Identify risks and optimize AI investments

- Detect concerning behavior patterns like potential insider threats
- Identify which teams leverage AI most effectively
- Track productivity gains and ROI from AI adoption with advanced analytics

## KEY PLATFORM CAPABILITIES




-  **Network-Level Visibility:** See all AI activity across your enterprise including thick clients like Windows 11 Copilot and Office 365 without relying on browser extensions or agents.
-  **Intelligent Policy Engine:** Apply context-aware policies based on user intentions, rather than relying solely on the tools being used. Our behavioral analysis categorizes activities to enable nuanced policies that balance security with productivity.
-  **Complete AI Attack Protection:** Protect against sophisticated attacks with best-in-class defenses against prompt injection, jailbreaking, and model manipulation.
-  **Organizational Analytics and Insights:** Deliver actionable intelligence on AI usage while detecting anomalous behavior patterns that could indicate insider threats. Our Organizational Behavior feature integrates with your SIEM and XDR solutions to help you see between the lines of AI usage.
-  **Built for Regulatory Compliance:** Secure single-tenant environment with your own key encryption. Deploy regional sandboxes with customized policies to meet compliance requirements. Our Role Based Access Control with VIP mode ensures executive communications remain private.

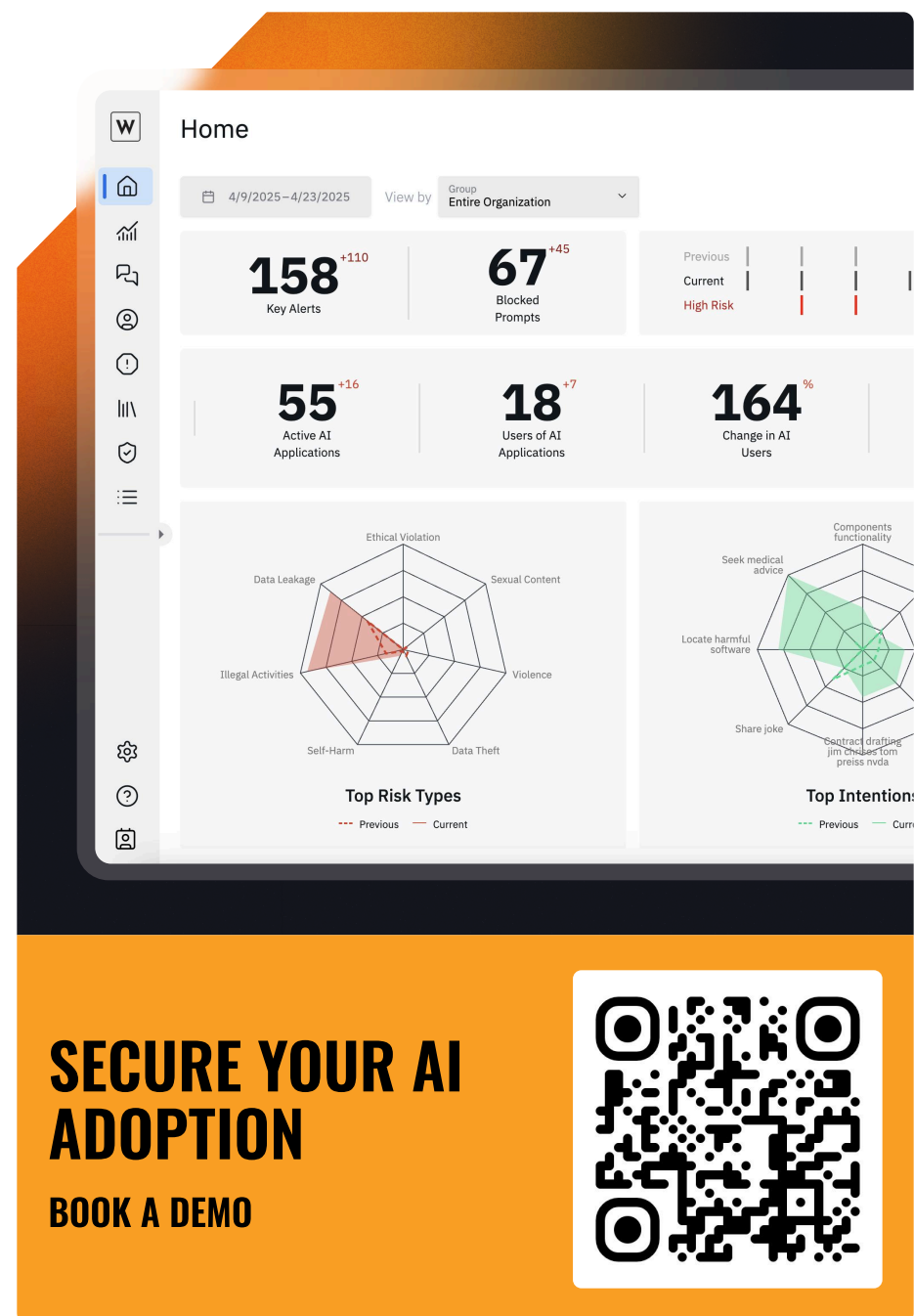
## ENTERPRISE SOLUTIONS

-  **Compliant Employee AI Use:** AI is a powerful productivity tool, but it introduces risks when employees overshare sensitive information. WitnessAI ensures that employees can leverage AI tools without exposing company data by enforcing acceptable use policies with automatic data tokenization.
-  **Protected Enterprise Models and AI Apps:** Your customer-facing chatbots represent your brand and must remain secure. WitnessAI offers superior protection against prompt injection and jailbreak attacks, ensuring your AI applications remain safe and deliver consistent, brand-aligned responses.
-  **Secure Source Code and IP:** AI coding tools supercharge developer productivity but can expose valuable intellectual property. WitnessAI intercepts developer prompts from GitHub Copilot, Cursor and other tools, enabling productivity while ensuring your IP never leaves your network.
-  **Demonstrable AI ROI:** As AI investments grow, measuring impact becomes critical. WitnessAI provides comprehensive usage analytics, highlighting productivity gains and identifying optimization opportunities across your organization.

## DEPLOYMENT OPTIONS

WitnessAI seamlessly integrates with your existing security infrastructure through:

-  **Network Connectors:** Zscaler, Palo Alto Networks, Netskope, Fortinet, F5
-  **Witness Anywhere:** Extend protection to remote workers without agents
-  **API Integration:** Connect to existing analytics and security systems



## About WitnessAI

WitnessAI enables safe and effective adoption of enterprise AI, through security and governance guardrails for public and private LLMs. The WitnessAI Secure AI Enablement Platform provides visibility of employee AI use, control of that use via AI-oriented policy, and protection of that use via data and topic security.

Learn more at [witness.ai](https://witness.ai).