DATA SHEET

Advanced AI Guardrail Services

Plan, Design and Implement
AI Governance Strategy with Confidence

4.9/5
Avg. CSAT Score
Zscaler deployment of customer security strategy.

Clear outcomes, tailored to your engagement

Zscaler's professional services consultants and project managers accelerate Zero Trust transformation for AI by applying deep expertise and cutting-edge Zscaler leading practices. This strategic engagement connects customers with highly experienced AI strategists who align your executive stakeholders, security team and Zero Trust technologies to translate your business priorities into customized configurations. Designated Remote Resources focus on your most critical use cases within the allotted hours and days. The exact scope flexes with your use case complexity and the level of participation from your internal teams, ensuring you get maximum value from every stage of the engagement.

Advanced AI Guardrails and Governance Services

2 Designated Remote Resources:
1 Professional Services Consultant &
1 Implementation Engineer

Common scope of engagement:

- *Extended strategic business discovery and technical planning of Zero Trust transformation for AI, with verifiable outcomes and time-bound milestones*
- *Comprehensive AI security design*
- *End-to-end hands-on and advisory implementation within all entitled AI products*
- Unified AI governance strategy articulation
- Configuration of custom guardrail logic to met use cases
- End User, App, Probe and/or Asset security fine tuning
- Clear and actionable change management documentation
- Translation of governance into bottom-line impact for AI security investments

114 Credits | 86 hrs in 60 days

Key Deliverables

Strategic Project Planning – presentation of a prescriptive planning deck outlining methodology, milestones and leading practices.

Prerequisite Checklist – a simple, specific outline of everything your team needs to provide for a successful Zscaler engagement.

Comprehensive Design Document, including specifications for:

- **AI Security Strategy translation into AI product configuration** – within entitled products: AI Assets, AI Users, Read teaming and/or AI Posture Management.
- **Advanced Traffic Steering** – technical configuration specifications for proxy chains, API Integrations and explicit proxy configurations, optimizing tradeoffs.
- **Signal to action mapping for ongoing optimization** – documents how risk factors and mitigating controls are managed to protect against AI Security threats.

Guardrail Testing – to validate performance, with programmatic quality control protocols.

Production Rollout – with seamless transition from guardrail visibility to guardrail enforcement for all configured governance strategies.

Knowledge Transfer – continuous up-leveling of AI Security service owner expertise, for autonomous troubleshooting and resilience.

Post Engagement Transition – with live hand-off to Technical Success Manager (where applicable) and documented Support plan.

+1 408.533.0288 Zscaler, Inc. (HQ) | 120 Holger Way, San Jose, CA 95135 Terms and Conditions Zscaler.com