Zscaler AI Security at a Glance

AT-A-GLANCE

AI Security Benefits

DISCOVER AI ASSETS & RISK
Discover and map your entire AI ecosystem—from shadow AI and risky apps to AI models and pipelines, and more.

FIND AI VULNERABILITIES
Red Team Test AI systems for vulnerabilities and risks with continuous and automatic testing.

SECURE AI ACCESS
Leverage inline AI guardrails to Enforce real-time protections across threats, data loss and safe usage.

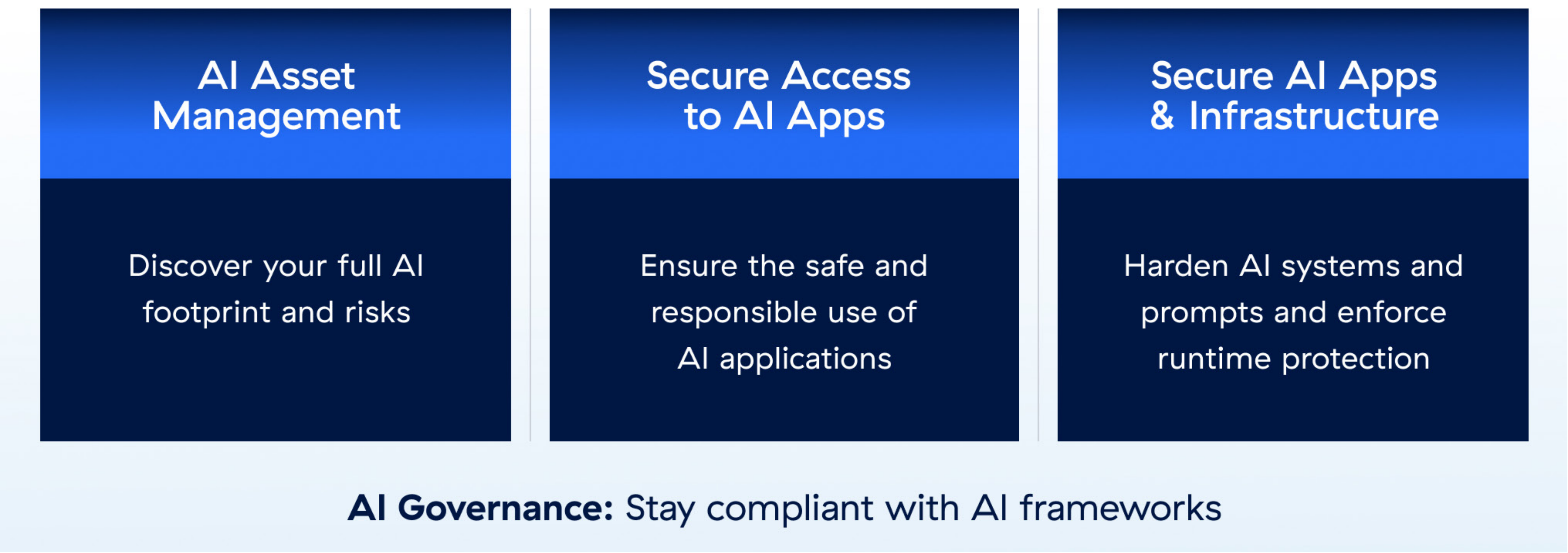
GOVERN AI COMPLIANCE
Govern your AI footprint and deployments using AI frameworks to maintain risk compliance

End-to-End AI Security with Zscaler

Zscaler delivers AI-driven solutions designed to help businesses embrace the transformative power of AI while managing associated risks.

With capabilities that span from identifying risky AI usage to ensuring secure development and protecting sensitive builds through advanced inline defenses.

Zscaler redefines what it means to secure AI innovation. Unlock AI's potential confidently and drive fearless progress with Zscaler.



AI Asset Management

Discover your full AI footprint and risks

Secure Access to AI Apps

Ensure the safe and responsible use of AI applications

Secure AI Apps & Infrastructure

Harden AI systems and prompts and enforce runtime protection

AI Governance: Stay compliant with AI frameworks

Why Zscaler for AI Security

FULL AI LIFECYCLE
AI Security from discovery through deployment

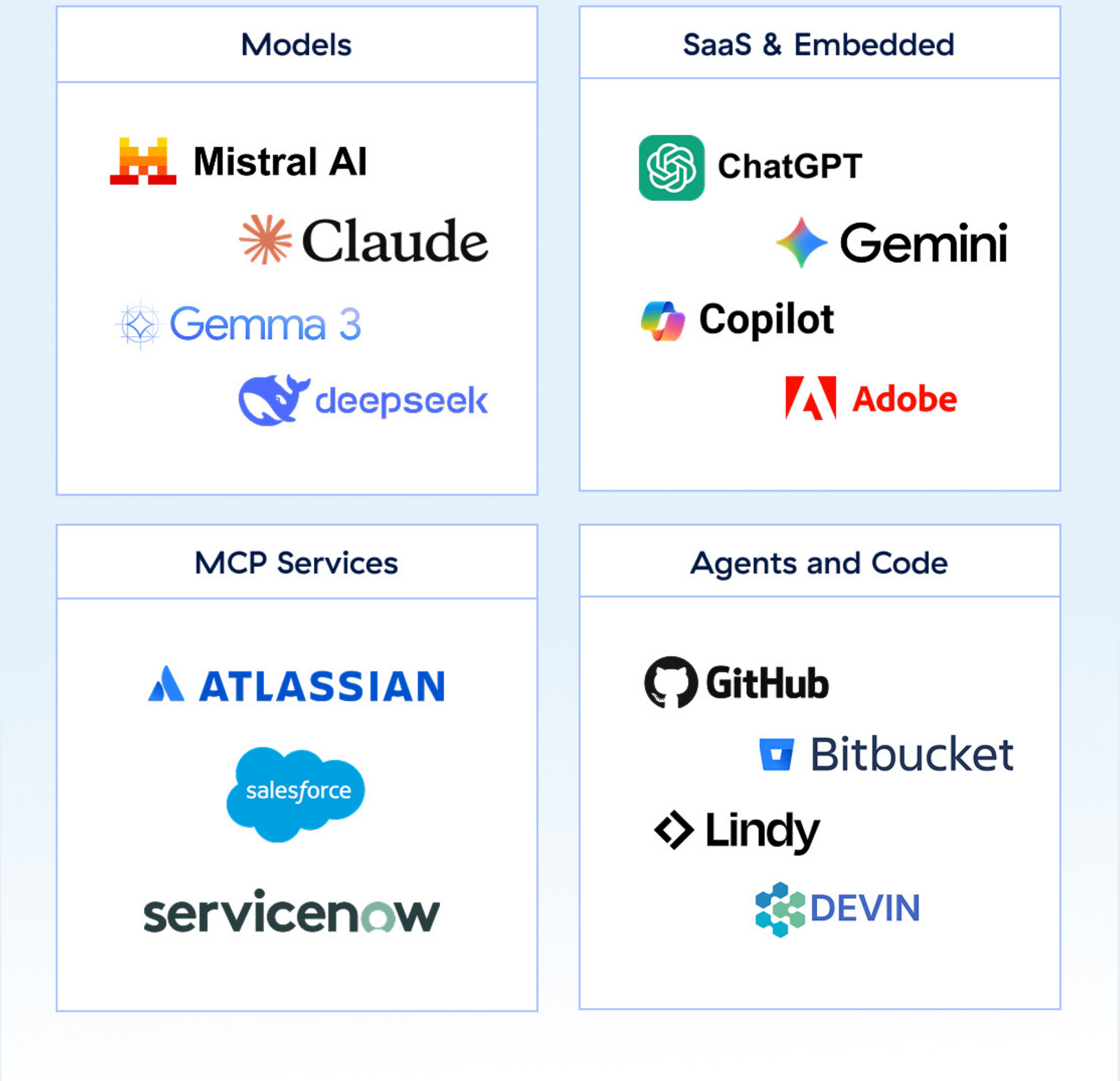
UNIFIED PLATFORM
Proven platform integrates AI Security with Zero Trust

PROVEN PARTNER
Expertise in customer success and transformation

Asset Discovery with AI SPM

Discovering your AI footprint is challenging in today's fast-paced AI environment. Without clear visibility into Shadow AI, models, services, MCP servers, and pipelines, organizations struggle to detect and respond to risks effectively.

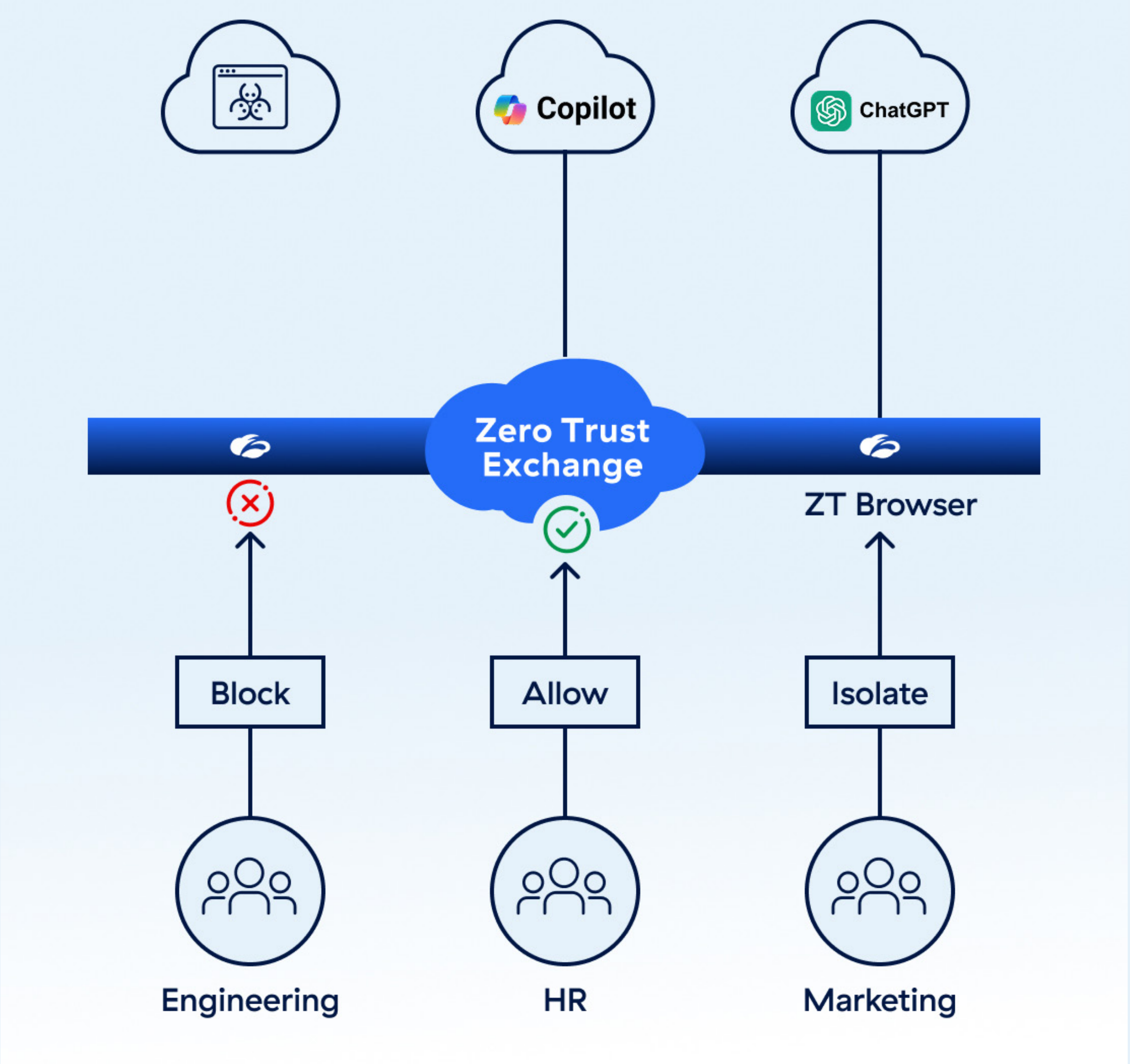
With Zscaler AI SPM, organizations gain comprehensive visibility into their AI ecosystems. It provides insight into your footprint across Gen AI apps, LLMs, models, MCP servers, and pipelines, helping you identify risky exposures and vulnerabilities that could compromise your data and business.



AI Access Security

Controlling access and ensuring security for GenAI SaaS applications is increasingly challenging. With Shadow AI spreading unchecked and the growing risks of data loss or non-compliant usage, organizations need effective solutions to address these threats.

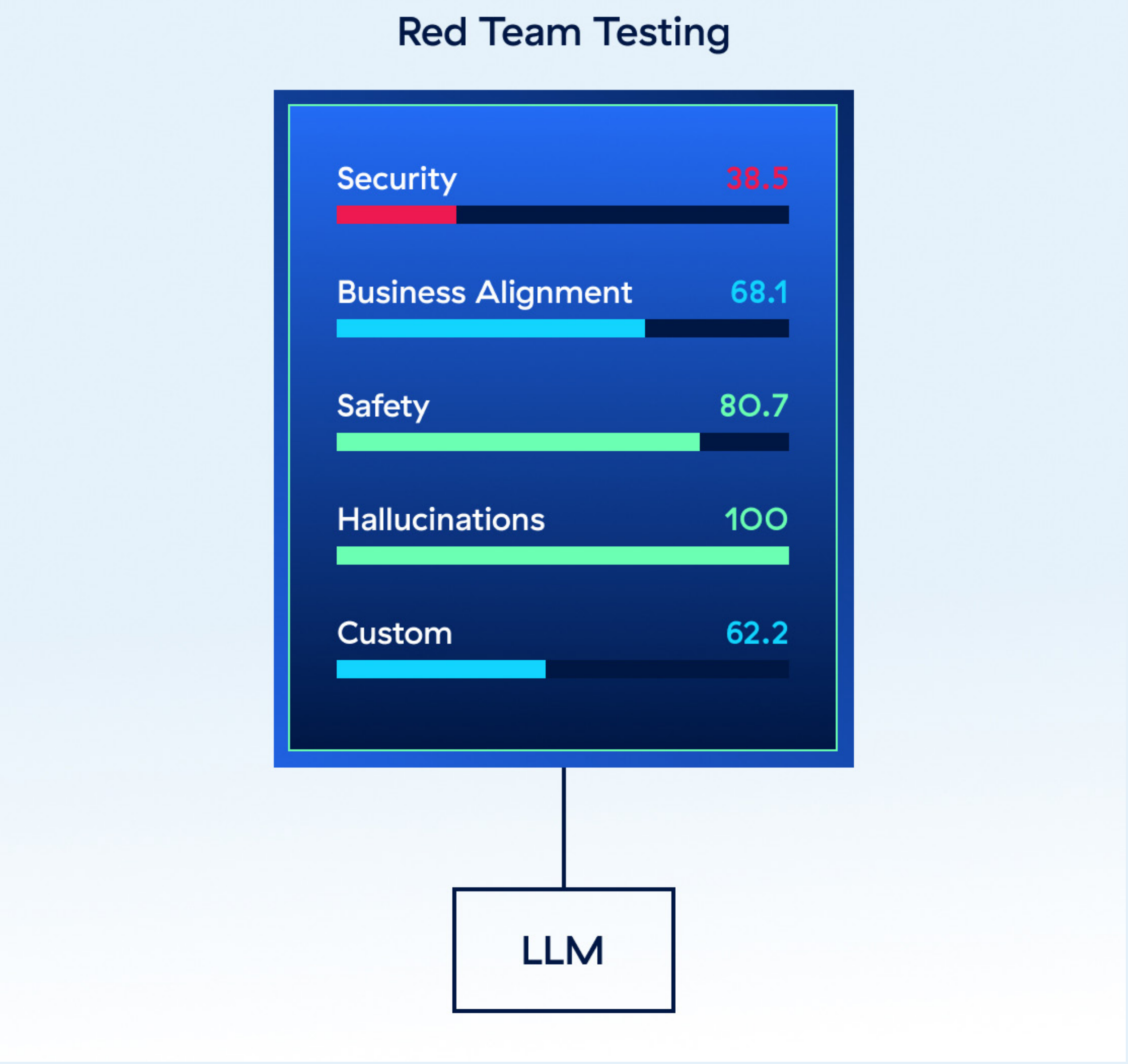
With Zscaler's AI Access Security, you can enforce the safe, compliant, and responsible use of AI applications. Apply granular access controls to govern which users or apps can interact with AI tools. Leverage DLP protection or isolation to prevent data loss through prompts, and enforce content moderation to ensure compliance with corporate acceptable use policies.



Testing with Automated Red Teaming

Testing AI systems for vulnerabilities is often a complex and time-intensive process. For organizations without dedicated Red Team resources, it can feel nearly impossible to conduct thorough evaluations.

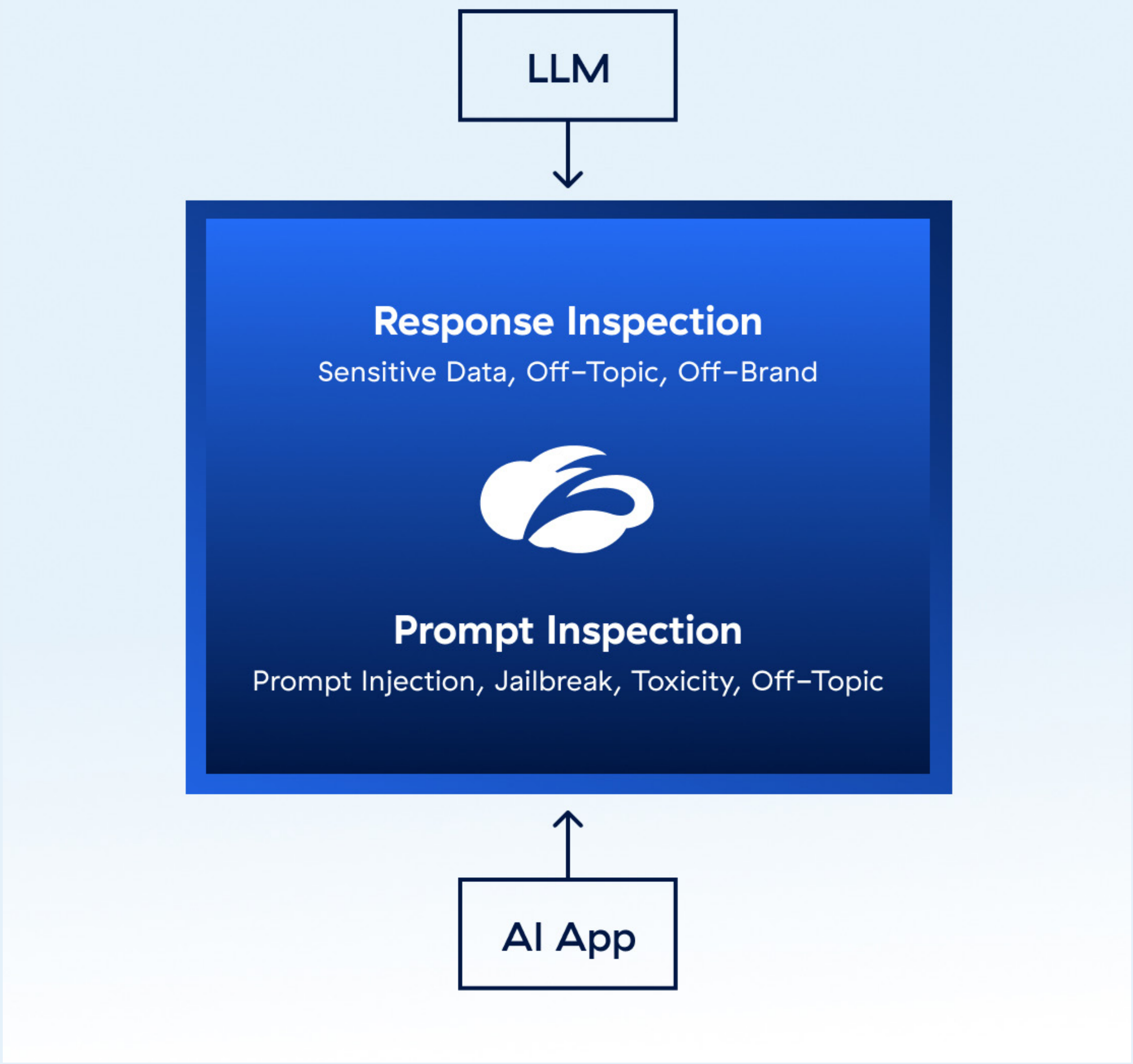
Zscaler's Automatic and Continuous Red Teaming addresses these challenges with an innovative, automated red teaming engine. With over 25 predefined probes and support for fully custom probes and dataset uploads, SPLX enables organizations to tailor testing scenarios to their specific domains, regulatory environments, and use cases.



Inline Protection with AI Guard

LLMs have quickly become a dangerous new vector for threats and data loss. Without high-performance inline inspection of these connections, organizations are vulnerable to data exposure, compromised AI systems, and malicious threats.

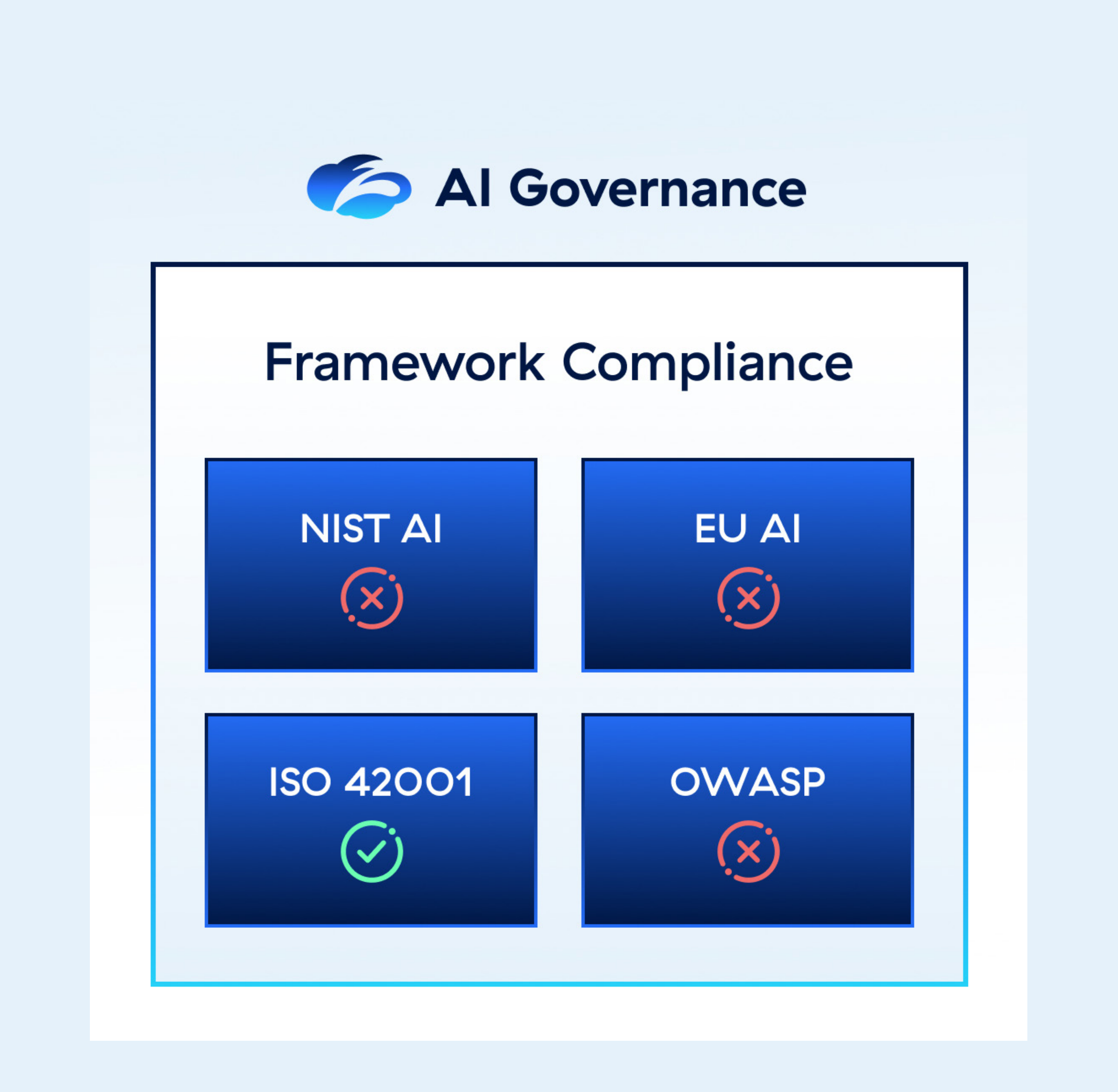
With Zscaler AI Guard, organizations can deliver high-performance inline inspection of AI prompts and interactions. Detect risky threats like prompt injections and jailbreaking, prevent sensitive data loss, and moderate content to enforce safe usage and acceptable use policies. Built on the expertise of a trusted leader in inline inspection, Zscaler ensures robust protection for your critical AI traffic.


LLM
Response Inspection
Sensitive Data, Off-Topic, Off-Brand
Prompt Inspection
Prompt Injection, Jailbreak, Toxicity, Off-Topic
AI App

AI Governance with AI SPM

Ensuring compliance and governance for AI systems is becoming increasingly complex as organizations adopt AI at scale. Without proper oversight of policy adherence and AI frameworks, businesses risk exposure to legal, financial, and reputational harm.

With Zscaler's approach to AI Governance, you can automate compliance monitoring and streamline reporting processes. Continuously monitor AI systems for alignment with internal policies and regulatory standards, while providing the necessary evidence to support audits and meet requirements. Ensure AI usage complies with governance frameworks, helping your organization mitigate risks and maintain operational integrity.



AI Governance

Framework Compliance

NIST AI ✗

EU AI ✗

ISO 42001 ✓

OWASP ✗

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere