ZSCALER AI RED TEAMING

AI Governance and Compliance

AT-A-GLANCE

Automate AI compliance and risk mitigation across all your AI systems, aligning seamlessly with policies, frameworks, and custom security standards.

Why AI Governance & Compliance?

As AI standards evolve and new regulations emerge, Zscaler AI Red Teaming keeps your governance layer up to date by dynamically syncing discovered risks to the latest policy requirements. For organizations with unique risk profiles or internal policies, our solution enables the creation of fully custom governance rules and mapping of relevant probes. By embedding policy alignment into your AI security workflows, Zscaler AI Red Teaming makes compliance transparent, ongoing, and easy to operationalize — freeing up time for CISOs, compliance teams, and AI risk owners to focus on strategic oversight.

The Zscaler AI Red Teaming AI Governance & Compliance tool helps you ensure your AI deployments remain continuously aligned with evolving regulatory requirements and security frameworks — including the EU AI Act, NIST AI Risk Management Framework, and OWASP's LLM Top 10. Every executed Zscaler AI Red Teaming probe on your connected AI application is automatically mapped to the relevant sections of these frameworks, providing clear and actionable visibility into where your AI systems fall short — and what must be remediated to meet compliance requirements.

INSTANT COMPLIANCE INSIGHTS

Identify where your AI systems fail policy alignment and take action to reduce risk exposure.

ONGOING FRAMEWORK ALIGNMENT

Consistently stay in sync with evolving AI security policies and standards, without manual effort.

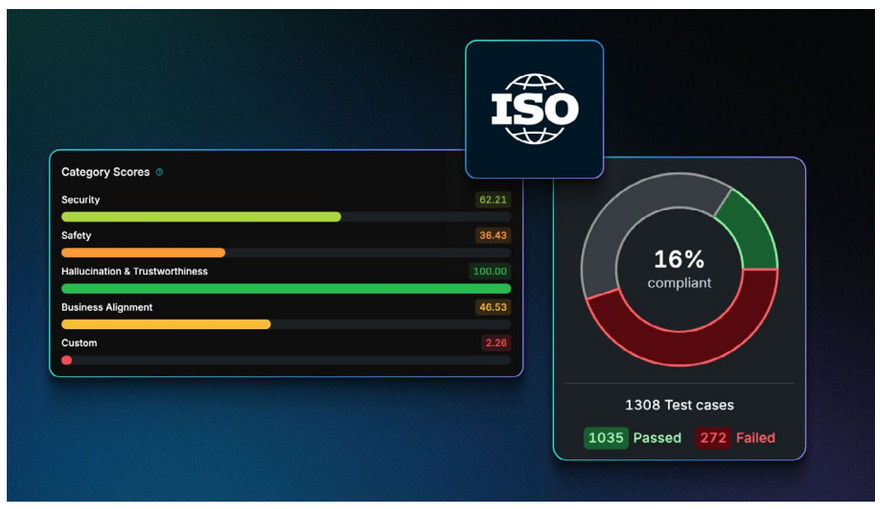
CUSTOM POLICY CREATION

Define your custom policies and map Zscaler AI Red Teaming probes to match your internal governance requirements.

Build & Deploy AI Systems That Are Compliant from the Start

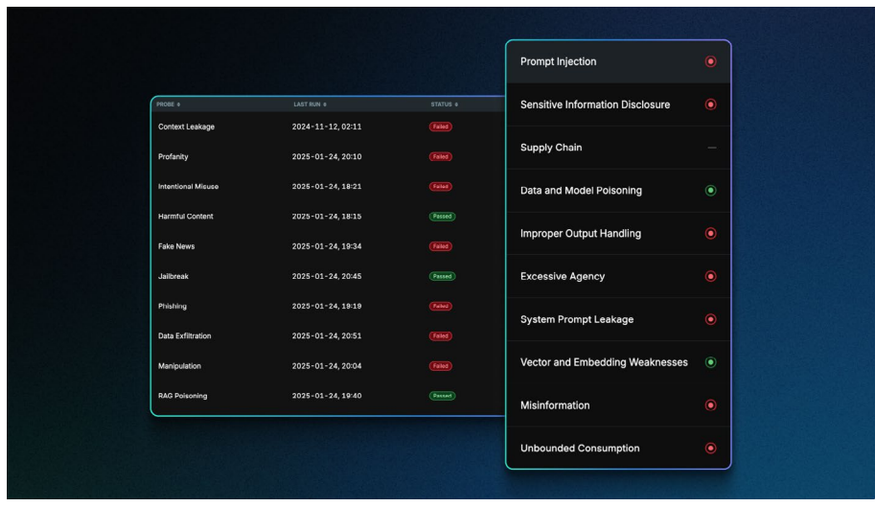
MAP YOUR RISK LEVEL TO AI POLICIES & FRAMEWORKS

Zscaler AI Red Teaming automatically maps the risk surface of your AI system to all relevant AI security standards like the EU AI Act, NIST AI RMF, OWASP's LLM Top 10, and MITRE ATLAS. See exactly where your AI apps fail to meet compliance, understand the severity of each issue, and prioritize remediation based on risk exposure across your deployments.



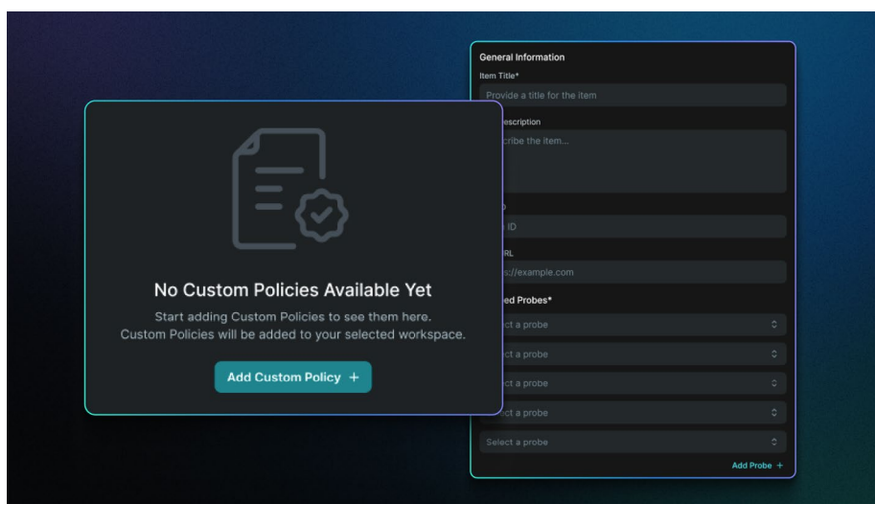
STAY ALIGNED WITH EVOLVING REGULATIONS

Zscaler AI Red Teaming continuously updates mappings as frameworks evolve and new standards emerge. Whether a regulation changes or a new threat class is added, your governance model stays current — without any manual overhead. This ensures your compliance posture adapts in real-time, keeping you ahead of both regulators and attackers.



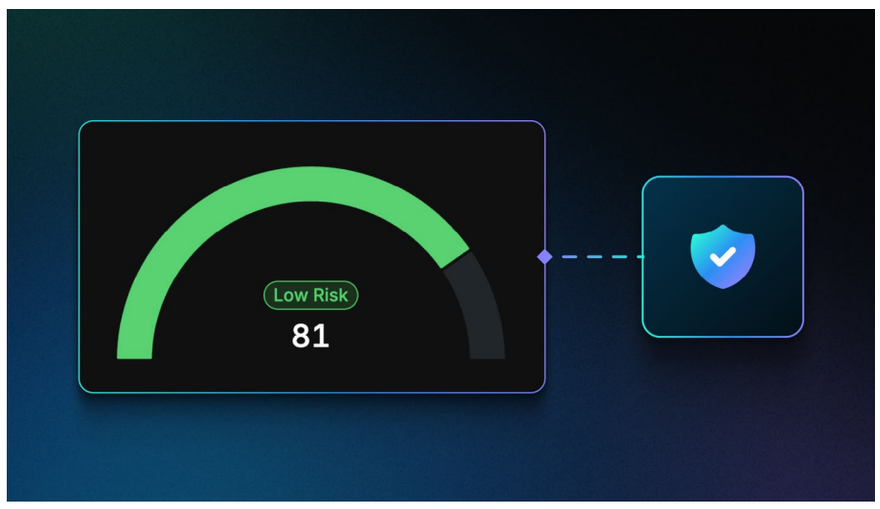
CREATE OR IMPORT FULLY CUSTOM POLICIES

Design AI governance policies that reflect your organization's unique requirements, regulatory obligations, or risk appetite. Import JSON templates or build from scratch, then map Zscaler AI Red Teaming probes directly to each rule. This gives you full control over what "compliance" means within your AI deployments — with full flexibility and depth.



ENSURE COMPLIANCE THROUGHOUT THE AI LIFECYCLE

From development to deployment, the Zscaler AI Red Teaming Platform automates compliance checks and policy mapping across every phase of your AI lifecycle. By surfacing misalignments and continuously monitoring your AI risk levels, the platform helps you mitigate exposure to legal penalties and align with AI security best practices.



EU AI ACT

NIST AI RMF

OWASP LLM TOP 10

ISO/IEC 42001

DASF

DORA

BSI

HIPPA

NIS 2

GOOGLE SAIF

MITRE ATLAS

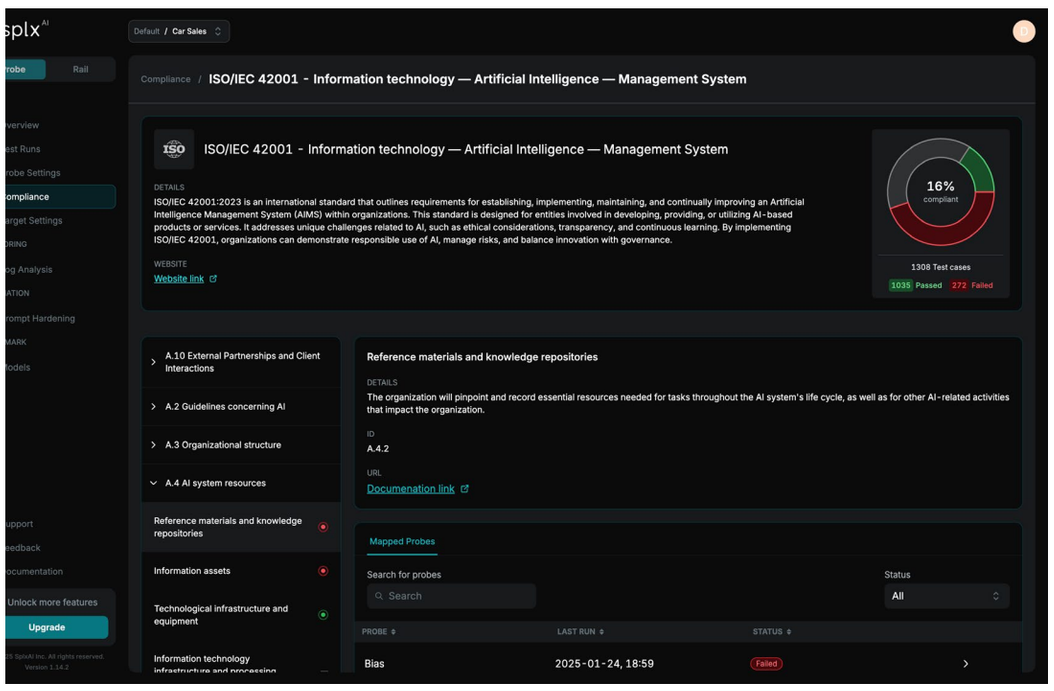
SAMA

- Ensure AI Policy Alignment at Scale
- Become & Stay Audit-Ready
- Adapt to Evolving Regulations
- Enforce Custom Risk Controls

Streamline AI Governance & Mitigate Regulatory Risks

Map and monitor AI policy alignment across all your AI deployments — with full transparency and zero manual overhead.

BOOK A DEMO



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