ZSCALER AI RED TEAMING

AI Asset Discovery & Management

AT-A-GLANCE

Automatically discover and secure every AI asset—LLMs, workflows, MCP servers, and guardrails for full posture visibility.

Why AI Asset Management?

As enterprises accelerate the adoption of AI technology, LLMs, workflows, and more AI systems (like MCP servers and AI guardrails) are being built and deployed across departments at an unprecedented pace. This brings a critical challenge to security leaders: most organizations do not know how many AI components are in use, where they are deployed, or whether they are even safe to use and what their inherent security risks are.

For large enterprises, the scale is staggering — hundreds or even thousands of AI models may be used across different business units, often outside security's line of sight. Without a centralized inventory, CISOs and their teams lack the visibility needed to evaluate risks, enforce compliance, or prevent unsafe AI components from reaching production.

Zscaler AI Red Teaming's AI Asset Management solves this critical transparency and visibility gap. By unifying discovery of every LLM, workflow, MCP server, and guardrail into a single AI-BOM, Zscaler AI Red Teaming gives security executives the clarity to see exactly what's in use, analyze vulnerabilities, and decide what is fit for deployment — while meeting growing AI policy requirements for AI to be transparent and explainable. This unified view is the foundation for securing AI at enterprise scale.

UNIFIED AI INVENTORY

One single source of truth for every LLM, workflow, MCP server, and guardrail used in organizations.

STREAMLINED AI-SPM

Combine AI discovery, security testing, runtime protection, and compliance mapping in one tool.

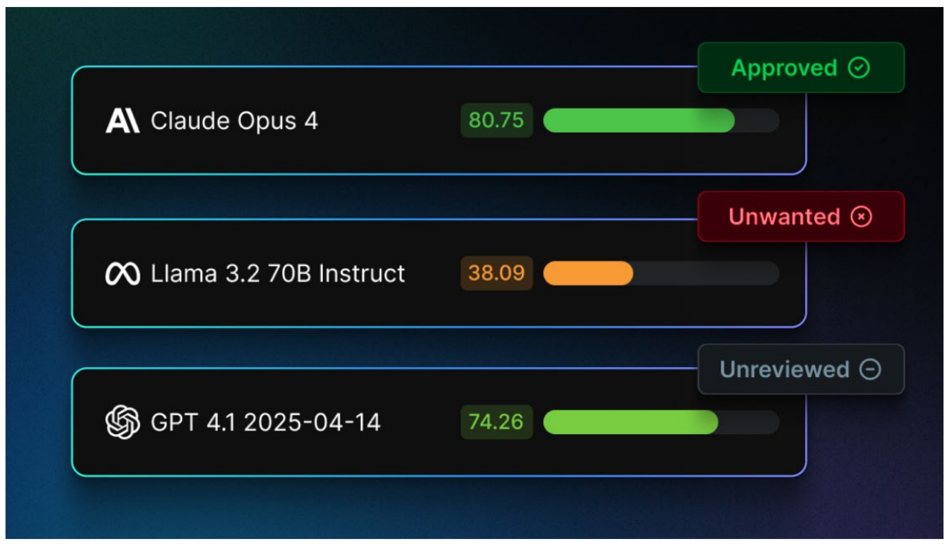
ENTERPRISE-SCALE VISIBILITY

Gain clarity across thousands of models and workflows and know what is safe for deployment.

Full Visibility into Your AI Stack with a Unified AI-BOM

DISCOVER & APPROVE EVERY AI MODEL

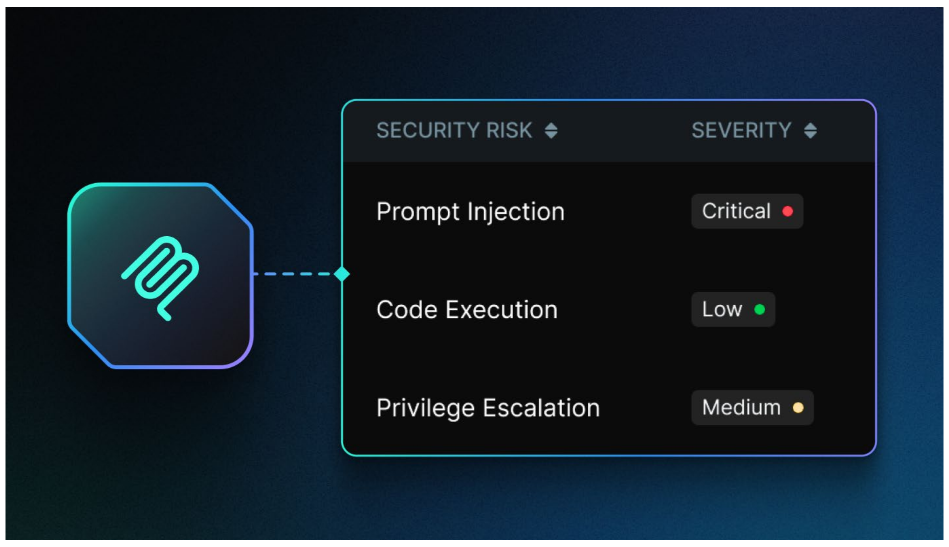
Every LLM used or deployed across your organization is automatically detected and mapped to Zscaler AI Red Teaming's trusted benchmarks. Security teams can assess risks, compare safety scores, and quickly identify unsafe models. Each model can be approved or blocked, giving CISOs full control over enterprise usage and deployment.



Claude Opus 4	80.75	Approved
Llama 3.2 70B Instruct	38.09	Unwanted
GPT 4.1 2025-04-14	74.26	Unreviewed

SCAN MCP SERVERS & FIND WEAKNESSES

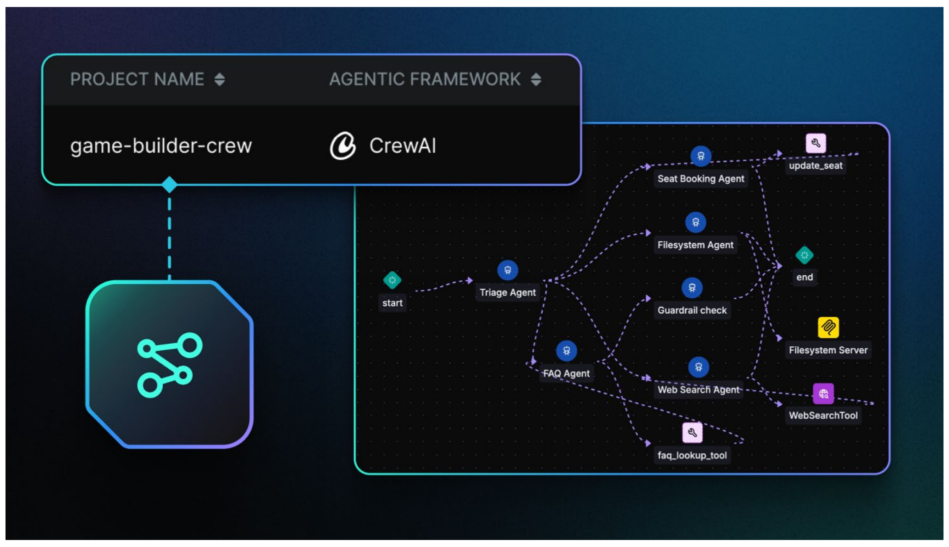
MCP servers act as critical orchestration layers in AI stacks, yet often remain unmonitored. Zscaler AI Red Teaming automatically discovers and scans them for vulnerabilities and misconfigurations that attackers could exploit. By integrating MCP visibility into a unified AI-BOM, security teams can remediate weak points and remain secure.



SECURITY RISK	SEVERITY
Prompt Injection	Critical
Code Execution	Low
Privilege Escalation	Medium

VISUALIZE AI WORKFLOWS & RUN SECURITY TESTS

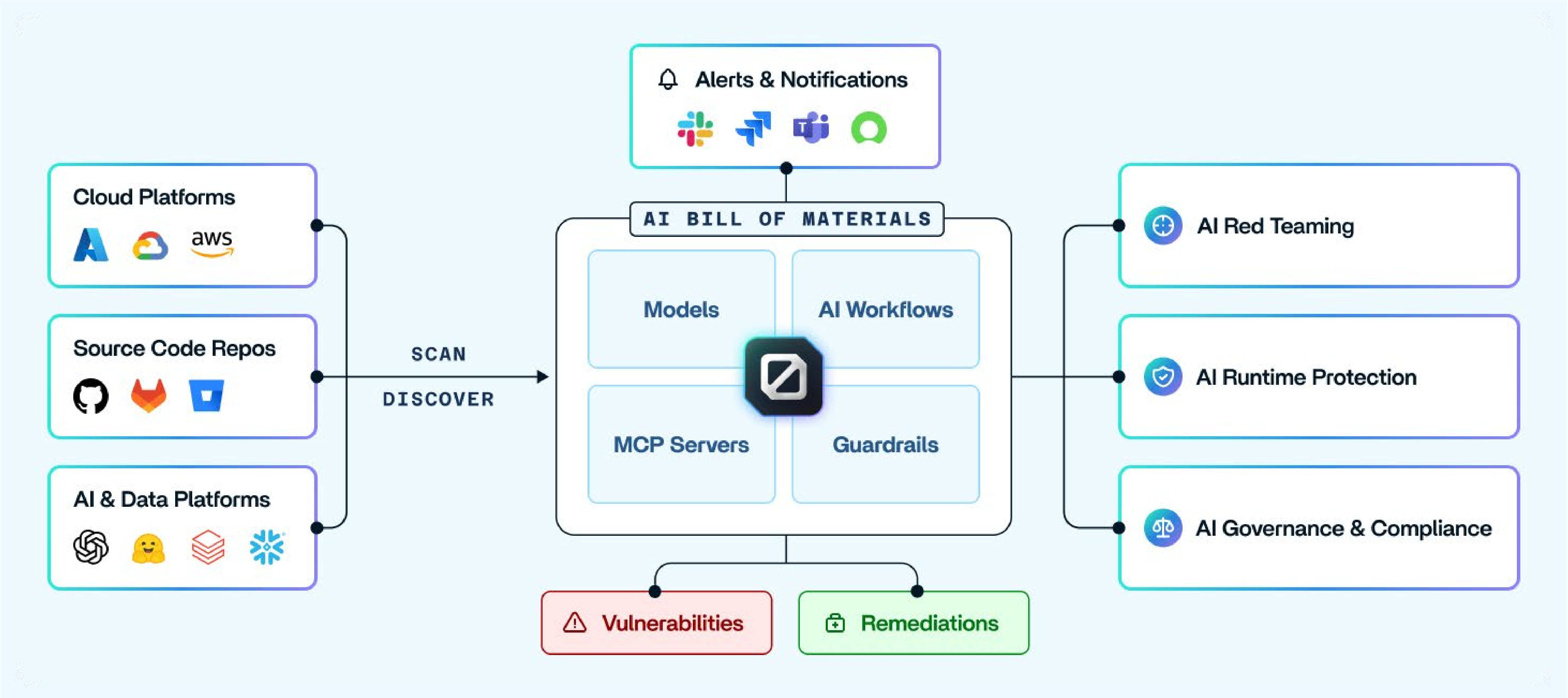
Source code repositories are continuously scanned to detect and map out AI workflows, revealing every agent, tool, and MCP server inside. Automated risk assessments point out misconfigurations and potential vulnerabilities, helping AI security teams secure workflows and reduce risk exposure before they can be exploited.



PROJECT NAME	AGENTIC FRAMEWORK
game-builder-crew	CrewAI

INTEGRATE YOUR STACK FOR COMPLETE AI VISIBILITY

Zscaler AI Red Teaming connects with major cloud providers, source code repositories, AI/ML platforms, and data systems to deliver full AI asset discovery across the enterprise. Thousands of environments are unified into a single AI-BOM, eliminating blind spots and giving security leaders the visibility and compliance readiness required at enterprise scale.

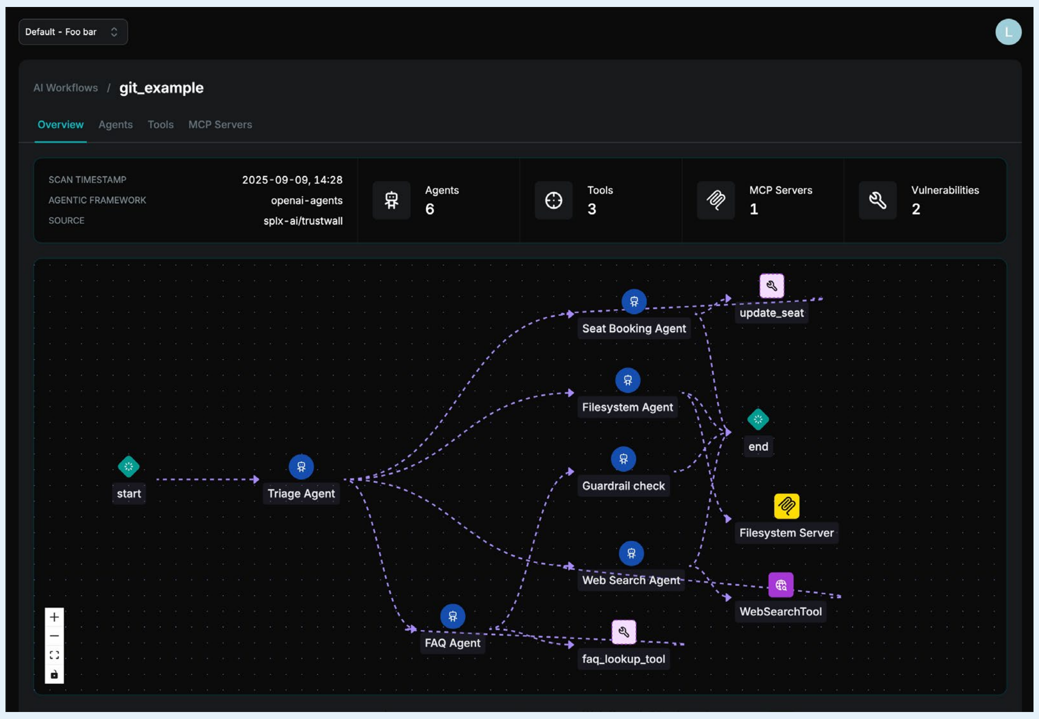


AI Security Posture Management (AI-SPM)

Gain full visibility & control of your AI security posture

Bring every AI component into a single inventory and secure your organization's AI systems at scale.

BOOK A DEMO



SCAN TIMESTAMP 2025-09-09, 14:28
AGENTIC FRAMEWORK openai-agents
SOURCE splx-ai/trustwall

Agents 6
Tools 3
MCP Servers 1
Vulnerabilities 2

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