Accelerate Secure AI Adoption with Zscaler AI Security Posture Management

AT-A-GLANCE

Challenges in Securing AI Resources and Data

IDC predicts global spending on AI applications, infrastructure, and services will reach US$632 billion by 2028, at a 29% CAGR. This surge will constitute 40% of public cloud spending within three years. Organizations increasingly deploy generative AI models on public clouds (like AWS, Azure and Google cloud), leveraging scalability, specialized infrastructure (GPUs, TPUs), and platforms like Amazon Bedrock, Azure AI Foundry, and Google Vertex AI. However, as AI adoption grows, so does its appeal to cybercriminals. Threat actors exploit misconfigured AI infrastructure to manipulate models or steal sensitive data. Organizations must proactively secure AI systems to mitigate both emerging and existing risks.

AI models often work with highly sensitive data, placing the responsibility for their security squarely on organizations. Similar to a cloud service providers (CSPs) shared responsibility model, organizations must secure the AI resources and data utilized for training and inference.

The OWASP Top 10 for LLM Applications highlights critical risks organizations need to address to protect AI assets in the cloud:

- **Data poisoning:** Manipulation or fine-tuning of training data to introduce vulnerabilities, backdoors, or biases, undermining model integrity and security.

- **Prompt injection:** Malicious injection of prompts designed to extract sensitive information.

- **Supply chain exploits:** Compromise of training data, ML models, and deployment platforms, causing biased results, security breaches, or total system failures.

- **Data exposure:** Data leaks due to excessive permissions and inadequate access governance frameworks.

- **Model abuse:** Over-autonomous AI functionality can lead to unintended security risks. Prevent this by limiting permissions and closely managing user authorizations.

- **Model theft:** Unauthorized access to large language models (LLMs), resulting in financial loss, reputational damage, and exposure of proprietary or sensitive data.

Zscaler AI Security Posture Management (AI-SPM)

Zscaler AI-SPM protects against AI-specific risks, including data exposure, misuse, and model governance, with a focus on securing generative AI (GenAI) workloads in the public cloud. As a part of the Zscaler AI Data Protection platform and integrated with our existing data security posture management (DSPM) solution, AI-SPM provides end-to-end visibility into AI models , sensitive inference data, model deployments, and risk correlation. By monitoring model configuration, data flows, and system interactions, it identifies security and compliance risks traditional tools often miss.

How Your Organization Can Leverage AI-SPM

Zscaler AI-SPM brings a sophisticated yet simple approach to AI risk management. AI leaders and security teams get unified visibility of AI services, risk analysis, and prioritized correlated risk remediation to eliminate potential AI risks as well as foster a culture of collaboration without compromising enterprise compliance. As AI continues to evolve, Zscaler ensures your organization remains innovative and secure.

Zscaler AI-SPM can help you:

- **Achieve uniform security oversight across environments to protect enterprise-wide AI deployments.**
- **Detect unauthorized AI initiatives and prevent data leaks or compliance violations from unsanctioned deployments.**
- **Monitor every phase of the AI life cycle, from data ingestion to deployment, ensuring no blind spots in AI operations.**
- **Proactively identify and mitigate AI-specific risks like data misuse, model vulnerabilities, and adversarial attacks.**
- **Simplify adherence to global regulations (e.g., GDPR, CCPA) by auditing and enforcing AI governance and role-based access controls.**

Features and Benefits

COMPREHENSIVE AI MODEL DISCOVERY

Managing the growing number of AI models—whether managed, semi-managed, or unmanaged—can be challenging. Zscaler AI-SPM simplifies oversight with robust visibility into AI deployments, enabling you to:

- **Control model sprawl:** Maintain an inventory of AI models, open source models, and models deployed in virtual machines, eliminating shadow AI.
- **Prevent unauthorized use:** Track and control model usage to identify and block unsanctioned or inappropriate applications with full visibility into your organization's AI footprint. Get full visibility into who can access AI resources and their permissions.
- **Strengthen governance:** Get real-time alerts for new model deployments, ensuring all necessary controls are implemented.

SENSITIVE DATA PROTECTION

AI models are trained on vast data sets that may include sensitive or regulated information, such as personally identifiable information (PII) or trade secrets. These AI models are vulnerable to inadvertent leaks or adversarial attacks. Zscaler AI-SPM monitors and protects sensitive data usage by AI model, helping you to:

- **Discover and classify training data:** Leverage auto data discovery and AI-powered classification to help build precise training data sets and prevent oversharing.
- **Secure AI training data:** Identify and prevent data poisoning by ensuring models are not trained or fine-tuned with sensitive data before deployment.

- **Monitor RAG and inference data flows:** Gain visibility into data sets and data flows used for retrieval, and understand their impact on data access.
- **Analyze model interactions:** Review prompt and output logs to detect model misuse and mitigate potential data exposure risks.
- **AI attack path visualization:** Map and eliminate connections between vulnerabilities, misconfigurations, and permissions to uncover hidden attack paths and more effectively reduce risks.

RISK ASSESSMENT

It's critical to ensure proper configuration, manage vulnerabilities on AI workloads, and govern access to AI resources. Misconfigurations and weak access controls in AI data pipelines, training environments, and deployment infrastructure can pose significant security and compliance risks. Zscaler AI-SPM provides comprehensive risk assessment, scanning, and actionable insights to strengthen your AI security posture so you can:

- **Identify risk:** Assess end-to-end AI deployments to uncover vulnerabilities across applications, data, and pipelines, leveraging built-in rules and contextual insights from Zscaler DSPM.
- **Prioritize risks:** Get a prioritized queue of AI security issues in an intuitive dashboard, helping your teams focus on the most critical ones.
- **Strengthen model access governance:** Visualize access mapping for deployed AI models, including associated resources such as compute, data, and applications.
- **Optimize permissions:** Identify and correct overpermissioned access. Ensure internal AI deployments, including RAG, don't cause data oversharing and prevent unauthorized access to sensitive information.
- **Reduce risk:** Map knowledge of AI applications, for RAG and fine-tuning architectures, to control sensitive data exposure and ensure compliance with current and upcoming regulations.
- **Prevent threat exposure:** Deep-scan AI models for vulnerabilities across the OWASP Top 10 for LLMs. Get remediation recommendations to help quickly address identified security issues.
- **Govern AI usage:** Evaluate AI systems against operational, regulatory, and reputational risks.

Zscaler AI Security Posture Management accelerates AI adoption by providing continuous visibility and proactive risk mitigation across your AI models, training data, and AI services. With comprehensive security measures, your organization can confidently scale AI initiatives while protecting sensitive data and staying compliant.

To learn more about Zscaler AI-SPM, schedule a demo with our experts.

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