# Wiz makes generative AI secure from the start

Accelerate your adoption of AWS AI services with a unified security platform

## AI security starts with visibility

Artificial intelligence (AI) has introduced an era of unparalleled innovation, empowering organizations across industries to efficiently build cutting-edge applications. Employees are increasingly adopting tools—especially those leveraging generative AI—that streamline work and provide AI-powered assistance. But a lack of visibility into these tools can broaden your attack area, proliferate shadow AI, and make protecting your cloud environment a challenge.

Without knowing how or what AI tools your teams are using, it's difficult to ensure a comprehensive view of your AI pipeline and protect against misconfigurations and vulnerabilities. Ingraining security into AI development goes hand-in-hand with safely accelerating its adoption in your cloud environment.

### What is shadow AI?

Shadow AI is the unauthorized use or implementation of AI that is not controlled by, or visible to, an organization's IT department. According to Wiz research, 70% of organizations are now using managed AI services. But are employees following security best practices?

## Remove barriers, not guardrails

Wiz is one of the first Cloud Native Application Protection Platforms (CNAPPs) to provide AI Security Posture Management (AI-SPM) capabilities. Deeply integrated into Amazon Web Services (AWS), Wiz now gives your teams an extensive view of AI security within your cloud environment. With this fuller context, organizations can remove the barriers to safe AI adoption while protecting against AI-related risks.

### Gain full-stack visibility into your AI pipeline

Detect AI services in your environment without agents. Use Wiz's AI bill of management (AI-BOM) to uncover shadow AI through comprehensive visibility into every AI technology in your environment.

### Detect AI misconfigurations

Enforce secure configuration baselines for your AI services with built-in rules to detect AI services that are misconfigured.

### Remove AI attack paths

Proactively remove attack paths to your AI models and protect your sensitive training data from being compromised.

## Accelerate AI innovation on AWS

### Build securely with Amazon Bedrock

By extending Wiz's AI-SPM to Amazon Bedrock, AWS customers can bring their generative AI applications to production even faster. See pipelines and misconfigurations from a graph-based visualizer and prioritize risks with the help of a holistic AWS viewpoint.

### Empower your practitioners on Amazon SageMaker

Push AI models to production more quickly and safely using Wiz's comprehensive visibility into Amazon SageMaker workflows. Wiz also scans and minimizes risks so that data scientists, engineers, and other machine learning practitioners can focus on creating AI-powered innovation.

## Wiz and AWS work better together

As an AWS Security Competency Partner and 2023 AWS Marketplace Partner of the Year, Wiz is committed to effectively reducing risk for AWS customers by seamlessly integrating into AWS services. The AWS Partner Network (APN) designation recognizes Wiz's deep technical expertise and success with AWS. It's part of the reason why 600+ AWS customers and 40% of Fortune 100 companies use Wiz to enhance their security postures.

Together, Wiz and AWS deliver a robust security framework that aligns with architectural best practices from AWS, ensuring your organization can accelerate AI adoption within a secure cloud environment.

# Set your AI adoption up for success with Wiz and AWS

Wiz integrates with 50+ AWS services to speed AI innovation in the cloud without compromising your protection.

Infuse your AWS environment with a secure dose of AI.
**Request a Security Health Check with AWS and Wiz experts ›**