WIZ Google Cloud

Secure every workload — including AI — with Wiz and Google Cloud

While the cloud is a non-negotiable requirement for modern organizations, the speed of business often outpaces the ability of security teams to protect all cloud resources. This disconnect can make it difficult to know precisely what data is where.

In addition, AI's dramatic surge has created new security and visibility challenges to manage. These challenges include unique threats specific to generative AI beyond the infrastructure scope of traditional security solutions. Generative AI workloads and workflows create opportunities for data corruption or exposure — both intentional and accidental.

Wiz and Google Cloud support safe, secure cloud and AI innovation

Powered by Google Kubernetes Engine (GKE), Wiz works with Google Cloud to help organizations answer the most complex questions related to cloud security, compliance, and risk.

Receive answers via an agentless solution that's easy to deploy and maintain and doesn't interfere with performance. The deep integration of Wiz's Cloud-Native Application Protection Platform (CNAPP) with Google Cloud helps customers improve security, accelerate cloud and AI adoption, and maintain control over their environment.

As a result, customers reduce time to value by allowing teams to innovate quickly and safely. Whether developing and deploying modern, container-based applications or deploying large language models (LLMs) trained on proprietary data, Wiz and Google Cloud help organizations do so securely.

Google Cloud customers can rely on Wiz to protect the entire AI lifecycle, from model building and training to deployment and use. AI workloads get the same security controls as traditional workloads at the platform and application levels. These controls span clouds, development platforms, storage, and virtual machines (VMs). Easily reveal misconfigurations, external exposure, sensitive data, and identity risks.

Wiz and Google Cloud understand why visibility and control over AI workloads are required for secure innovation. This is why Wiz and Google Cloud are founding members of the Coalition for Secure AI (CoSAI). CoSAI is a collaboration between major tech companies to develop comprehensive security measures, standards, and best practices for working with AI systems.

10x

Increase in speed to find and remediate issues after adopting Wiz

See everything

Wiz brings exceptional visibility to the Google Data Cloud and the AI Cloud. It performs a full-stack cloud inventory identifying every asset across clouds and architectures.

Wiz's agentless scanning maps all components in cloud environments and AI services. The solution scans and correlates exposed secrets, keys, and certificates in cloud environments, workloads, and technologies. Wiz scans the Google Data Cloud – including Vertex AI and Cloud SQL – as well as GKE and Cloud Run serverless workloads.

Wiz helps customers get complete visibility along the AI pipeline. It is easy to reveal attack paths that externally expose AI models and to protect against data leakage and poisoning.

Detect threats

Wiz ingests Event Threat Detection findings from Security Command Center to detect threats and add correlation and context to security events.

It correlates this information against all other cloud risk factors. Get a single, prioritized view of issues — including those related to generative AI workflows — in a user-friendly graphical interface.

Protect cloud workloads in real time with Runtime Sensor for native detection and response capabilities. Accelerate investigation and response to limit a threat's blast radius and harden the environment. Reduce mean time to response (MTTR), the likelihood of a breach, and its potential cost.

Automate responses

Wiz detects misconfigurations and enables customers to automate and integrate remediation workflows using Google Cloud services, such as Cloud Pub/Sub, Cloud Function Playbook, or Google SecOps.

Accelerate problem resolution using automated least-privilege actions. Alert teams to detected issues via Google Chat integration. Prevent data leakage during AI-powered chat sessions by filtering and monitoring HTTP traffic between applications and the internet.

Prevent unauthorized access to sensitive data. Google Sensitive Data Protection scans all data during training and production to remove personally identifiable information from results. Fix misconfigurations with a single click and optional auto-remediation.

WIZ

- Complete visibility across containerized, serverless environments, and data services such as Vertex AI, BigQuery, and Cloud SQL
- Agentless scanners provide complete coverage in minutes without disrupting operations
- Protect data used to train and fine-tune models and for generative AI capabilities, such as retrieval augmented generation

\+ Google Cloud

- Reduce compliance friction with continuous automated compliance assessments and posture scores across 100+ industry standard compliance frameworks
- Eliminate agent overhead and their lifecycle, including the organizational friction of overcoming developer resistance
- Automate the remediation of misconfigurations detected in cloud environments

=

- Protect sensitive data by scanning for it in models and across cloud environments
- Ship applications faster, eliminate operational silos, and empower cross-functional teams to proactively fix and prevent issues across the development lifecycle
- Defend the infrastructure and platforms underpinning AI applications to enable compliance and control

Wiz and Google Cloud help organizations see and secure every workload — including AI. Receive actionable context to proactively identify, prioritize, remediate, and prevent risks to the business. Get complete visibility into every technology across LLMs, AI, chatbots, VMs, containers, serverless functions, and Data Cloud stores.

See everything now