# See and secure your Google Cloud environment with Wiz

## Leverage a full-stack cloud inventory to identify assets, detect and prioritize threats, and automate response

While the cloud is a non-negotiable requirement for modern organizations, the ability of security teams to secure all cloud resources is often outpaced by the speed of business.

To protect their organization, security teams need the ability to identify and understand their complete cloud environment, including the relationships between the compute layer, the architecture, applications, and exposure to the outside world. The right tool allows organizations to rapidly improve their security posture by providing complete cloud visibility so they can detect threats faster and automate remediation.

### Wiz for Google Cloud enables contextual cloud security

The partnership between Wiz and Google Cloud enhances Google Cloud's highly performant global infrastructure and native security tools and technologies with Wiz's contextual view. This exposes the real risk that cybersecurity threats pose to your business. It also helps you understand how you should prioritize your remediation effort across your Google Cloud and multi-cloud deployments.

Wiz works with Google Cloud to help you answer the most complex questions about your cloud security, compliance and risk via a unique agentless solution that's easy to deploy and maintain, and doesn't interfere with performance. By jointly leveraging Wiz and Google Cloud, customers can rapidly improve their security posture, consolidate security tools, eliminate agent overhead, expedite detection and response, optimize security processes, and reduce noise.
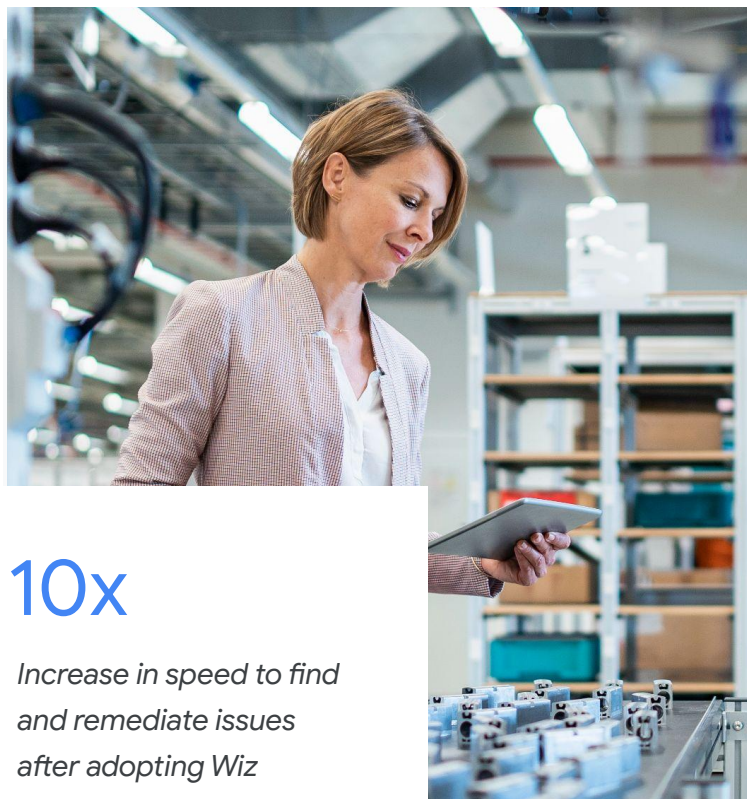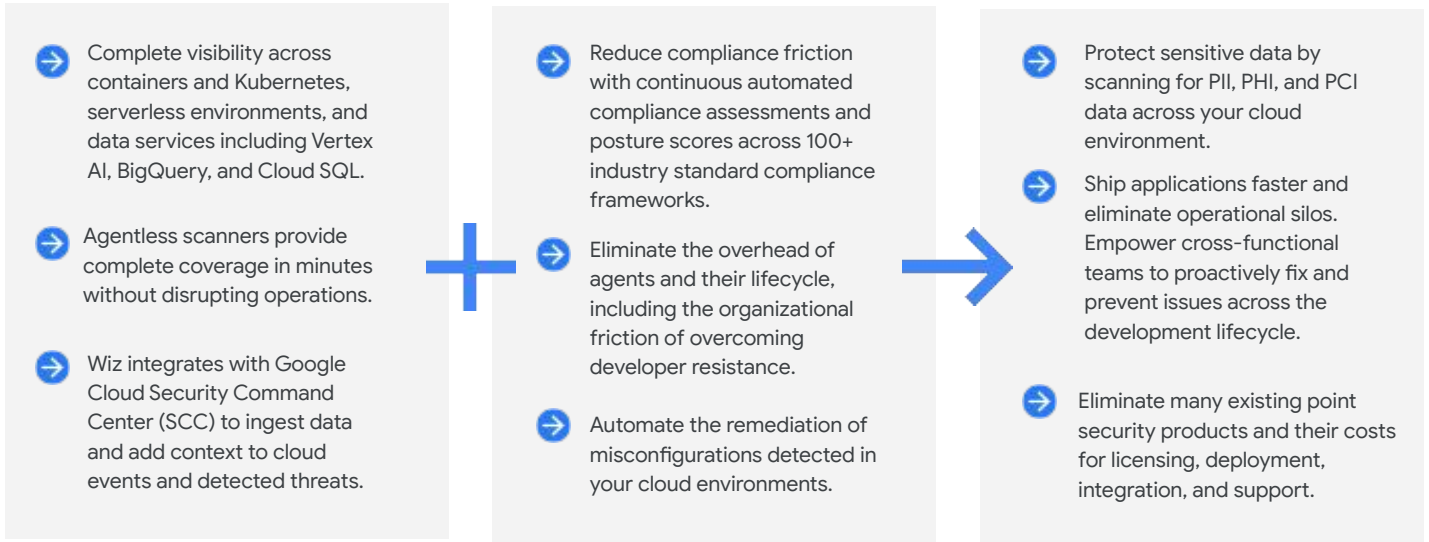


## 10x

*Increase in speed to find and remediate issues after adopting Wiz*

The deep integration of Wiz's Cloud-Native Application Protection Platform (CNAPP) with Google Cloud helps customers improve security and accelerate cloud adoption, while staying in control of their environment.

Provided with actionable insight and context, security teams can see what's most important to fix first. They can also scale security across the CI/CD pipeline by enabling developers to proactively detect, fix, and prevent issues across the development lifecycle while still focusing on innovation and business agility.

→ Complete visibility across containers and Kubernetes, serverless environments, and data services including Vertex AI, BigQuery, and Cloud SQL.

→ Agentless scanners provide complete coverage in minutes without disrupting operations.

→ Wiz integrates with Google Cloud Security Command Center (SCC) to ingest data and add context to cloud events and detected threats.

→ Reduce compliance friction with continuous automated compliance assessments and posture scores across 100+ industry standard compliance frameworks.

→ Eliminate the overhead of agents and their lifecycle, including the organizational friction of overcoming developer resistance.

→ Automate the remediation of misconfigurations detected in your cloud environments.

→ Protect sensitive data by scanning for PII, PHI, and PCI data across your cloud environment.

→ Ship applications faster and eliminate operational silos. Empower cross-functional teams to proactively fix and prevent issues across the development lifecycle.

→ Eliminate many existing point security products and their costs for licensing, deployment, integration, and support.

## Accelerate your cloud journey

Wiz for Google Cloud gives you everything you need to modernize your organization. The cloud-agnostic Cloud Native Application Protection Platform (CNAPP) facilitates large migration efforts while helping you consolidate your various cloud security solutions, including vulnerability management, cloud security posture management (CSPM) and cloud workload protection platform (CWPP).

Automated attack path analysis helps you remediate toxic combinations that can come up when you shift workloads between environments.

Leverage the visibility and automation required to enforce custom policies and frameworks across your cloud environments and IaC code.

## Gain visibility across containers and Kubernetes

As an agentless CNAPP, Wiz assesses and correlates container security risk across container images, identities, the Kubernetes network, and the cloud environment while ensuring compliance.

The Wiz Sensor provides real time detection of malicious behavior in Kubernetes clusters for rapid response.

Discover and scan all of your containers, hosts, and clusters across cloud-managed and self-managed Kubernetes, serverless containers, and standalone containers running on virtual machines.

This enables a productive partnership between developers and security to shift left and resolve issues across the containerized application lifecycle.

## Enhance your posture management

Use Wiz to protect data within the Google Cloud environment with fully-integrated data security posture management (DSPM) for your data. Discover your sensitive data with rapid, agentless visibility into critical data in your buckets, data and OS volumes, and managed and hosted databases.

Automatically correlate your sensitive data with the underlying cloud context, including public exposure, identities and entitlements, and vulnerabilities. Understand who can access what data, how data assets are configured and used, and how data moves within your environments.

Wiz automatically triggers alerts and remediation workflows to the relevant teams when policies are violated, ensuring security keeps pace with the business.

---

Wiz and Google Cloud help you see and secure your cloud with actionable context so your teams can proactively identify, prioritize, remediate, and prevent risks to your business. Scan every layer of your multicloud environments for complete visibility into every technology across virtual machines, containers, serverless functions, and Data Cloud stores.

**Learn more**