WIZ | Google Cloud

Accelerate your cloud journey in a secure way with Wiz and GCP

Google Cloud Platform and Wiz CNAPP are better together, giving customers of all sizes unmatched contextual visibility across their cloud organization with the ability to prioritize risk mitigation.

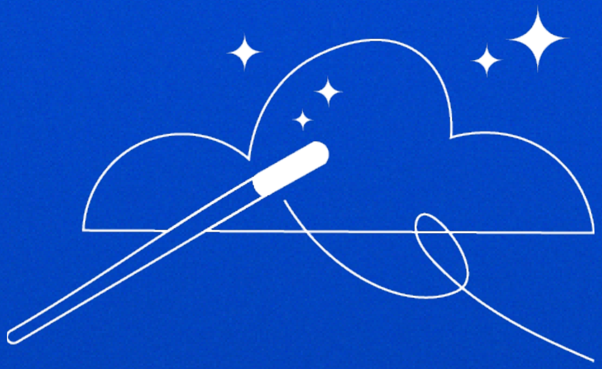


Table of Contents:

As more organizations start modernizing their applications and services using cloud technologies to drive digital transformation, they typically find security and dealing with compliance while limiting risk extremely challenging.

It's a challenging task to keep track of assets in cloud related to risks: security and operations teams often struggle to visualize and understand the relationships between the compute, the architecture, its exposure to the outside world and the technologies associated with the application that is composed of all those items.

It becomes even more challenging as overlapping layers of configurations, networks, and identities make it hard to get a firm grasp of effective access or effective permissions—in other words, what's exposed where, to whom, and why they should care. In the effort to gain control, they adopt myriad security tools stitching outcomes together in an endless effort to stay in control of those things that matter the most while still leaving visibility gaps. A unified, coherent view based on a unique data model becomes more and more elusive.

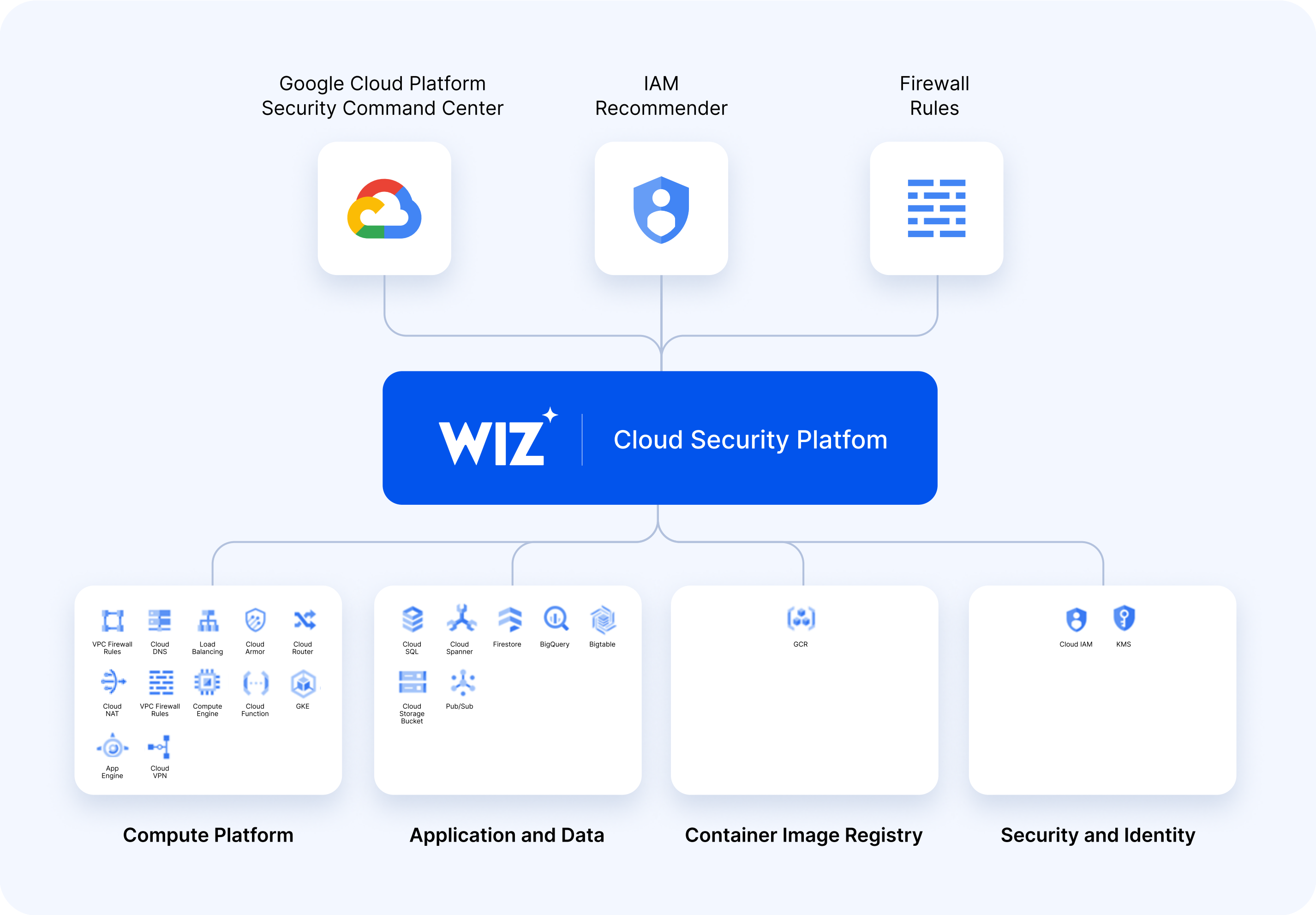
Cloud adoption is a non-negotiable requirement for modern organizations to keep that competitive advantage by building a new channel for their products and services, it can't come at the expense of risk management. Before you can move forward with your cloud strategy, you must be able to ensure the security of your evolving Infrastructure, its entitlements and platform technologies that represent what you build and like to run in the cloud.

Google Cloud Platform provides valuable cloud native security capabilities for Google Cloud Platform customers with tools such as Security Command Center (SCC), IAM Recommender, and Chronicle.

If you deal with multi-cloud providers and environments, the security stack google offers with these solutions will give you a part of the answers you need to deal with related to questions around cross-cloud risk, compliance and security.

For real risk mitigation, you need a way to fully understand its relation to the workload, cloud, and business context. The full contextual view will expose the real risk they pose to your business helping you to understand where you should prioritize and begin with your remediation effort across your multi-cloud and GCP cloud organization.

Wiz works together with Google to help you to answer the hardest questions related to cloud security, compliance, and risk and we do this in a unique agentless and frictionless way. By integrating our Cloud-Native Application Protection Platform with GCP we give our joint customers the ability to improve security and accelerate cloud adoption while staying in control, while accelerating the journey to the cloud, increasing cloud workloads usage, more securely, giving customers of all sizes a fast time-to-value, unlocking the full potential of their multi-cloud strategy.



Solving the challenges of cloud and multi-cloud security

Cloud environments are a highly appealing target for hackers. Beyond their highly distributed and connected nature, their complexity makes it especially difficult for organizations to locate and address critical risks to their resources. There are often multiple platforms in use—GCP, AWS, Azure, Kubernetes, and more—as well as diverse architectures such as virtual machines (VMs), containers, serverless computing, and Platform as a Service (PaaS). Within this sprawling environment, developers might be running thousands of different services, applications, and libraries, with more technologies added every day.

There are also dozens of ways of adding or implementing these assets and technologies, where individual resources might become exposed to the internet! Before you know it a threat actor might find countless ways to move laterally through your cloud organization to ultimately gain internal access to your crown jewels. Adding a layer of complex identities for different human roles and machine functions will add another dimension to the already breathtaking 3D puzzle of security, compliance and risk.

Preventing breaches and impacts across this diverse and dynamic environment poses a major challenge and falling short can have devastating consequences for the business. That's especially true when the multi-dimensional complexity of configurations, networks, and identities results in what Wiz calls toxic combinations, which are sets of risks that, when they occur together, create a perfect storm and opportunity for attackers and threat actors. In fact, we found that 90 percent of all cloud breaches are the result of these toxic combinations.

In order to secure their multi-cloud environment, security and operations teams must gain a full understanding of the risks they face: the who, what, where, and how of security in with a full contextual view across all assets involved. The Wiz approach to security begins with providing clear answers to these questions across all three levels of the cloud environment: configuration, network, and identity. How are individual systems and resources configured, or misconfigured? How are they connected to each other, to the internet, and into the corporate network? Who has access to what? Which permissions are involved to gain that access? Wiz gives you also view of how a threat actor or threat could enter the environment, how it would be able to travel, what it could reach, and what kind of impact it could have?

By providing a single place to discover, understand, and prioritize risk, Wiz helps security and operations teams overcome key struggles in the effort to operationalize security:

- **A lack of visibility** across the complete cloud environment makes it hard to know exactly what you have, where—especially for security teams with no control and little insight into ongoing cloud deployment. Wiz provides complete information across configurations, networks, and identities for a full understanding of the risks present in the multi-cloud environment.
- **An overly complex suite of cloud security tools**—five or so in the typical organization—gives only a fragmented view of security. With Wiz, teams gain comprehensive visibility through a single screen.
- **The reliance of most of these tools on agents** slows deployment in the face of developer resistance, resulting in gaps and blind spots. As an agentless solution, Wiz scans every layer of the environment without compromising resources.
- When risks are found, they take a long time to resolve due to a **lack of perceived urgency** and ownership **spread across many different teams**. By providing a clear sense of the dangers posed by vulnerabilities and misconfigurations, with tools to help remediate them, Wiz makes insight actionable.

Wiz and Google's native security capabilities: Better together to give you a full contextual view

Google's native security tools are a tremendous resource for GCP customers. For example, Security Command Center (SCC), a security and risk management platform for Google Cloud resources, provides centralized visibility and control, threat detection and remediation, and actionable recommendations to fix security misconfigurations and compliance violations.

Wiz complements the information captured and services provided by Google Security Tools with comprehensive contextual views to help organizations act more effectively without introducing additional complexity to reduce risk, and gain insight into compliance, security posture, and protection status. It all starts by ingesting, enriching, and complementing SCC data: the Wiz solution adds vital context enabling customers to fully understand the significance of runtime telemetry information such as events, threat detection, container threat detection, and anomalous behavior. This in turn helps organizations work more effectively with other Google services such as IAM Recommender, firewall rules, compute vulnerabilities, and access controls, to flag critical risks such as excessive permissions which contributes to identifying real exploitable toxic combinations. The Goal? limit noise and give you prioritized risk with actionable insights enabling everyone involved in the security and risk pipeline to act with the right context and recommended remediation steps.

For security and operations teams, the most important question is how they should prioritize the risks present in the cloud environment. Which goes first and why. Which issue creates the greatest impact on the business and the risk of the service? To answer these questions, we at Wiz take a four-step approach.

01.

Scan everything

Wiz scans the entire cloud stack in read-only mode, including all VMs, containers, serverless apps, data repositories, and PaaS services. This includes all the traditional checks found in cloud security posture management (CPSM) solutions, vulnerability scanners, and malware tools.

02.

Compile data

The Wiz cloud risk engine compiles multiple layers of configuration, network and identity data to surface effective external exposure, unintentionally excessive permissions, exposed secrets, and lateral movement paths.

03.

Plot a 3D risk graph

Wiz then maps your entire cloud architecture and components across infrastructure, workloads, and Kubernetes on a single 3D graph database. By visualizing your entire multi-cloud infrastructure, you can see effective network exposure from both inside-out and outside-in to understand the paths hackers can take to your assets, and the connection of each asset to the internet.

04.

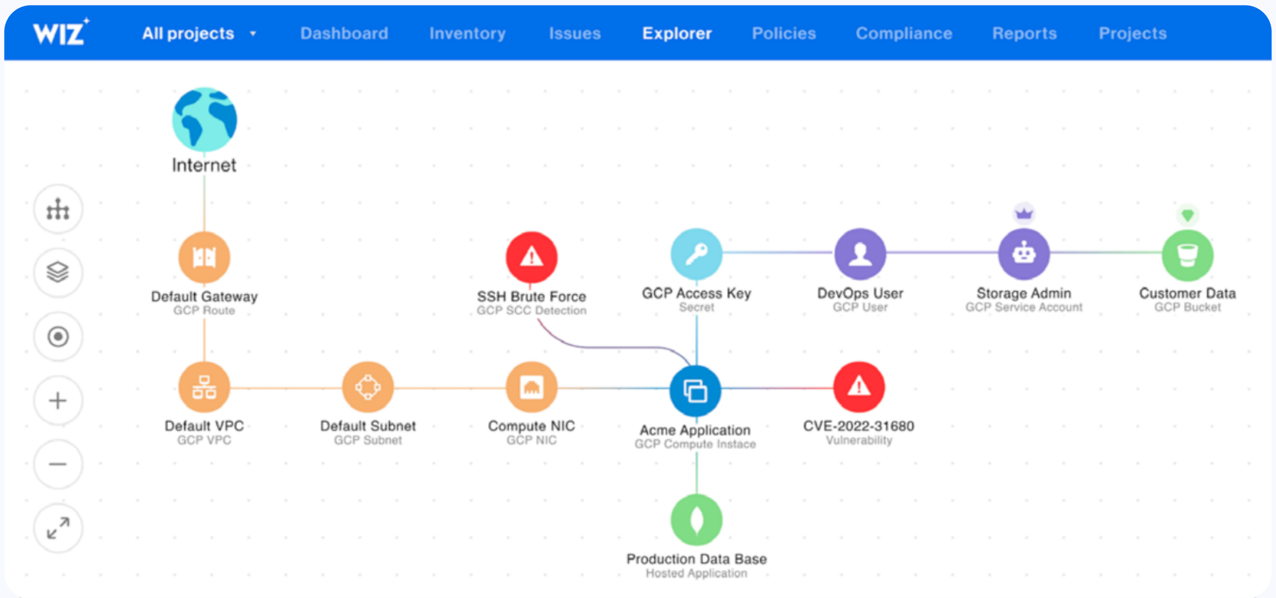
Identify toxic combinations

By layering the risk factors identified in Step 2 onto the risk graph from Step 3, Wiz makes it easy to see toxic combinations that make your cloud susceptible to a breach—the actual attack vectors available to hackers.

In this way, security teams can focus on identifying critical risks such as:

- Critical/high vulnerability issues such as a known exploit found on a publicly exposed VM instance with high permissions
- IAM users with high permissions and excessive access
- Publicly exposed containers with effective admin Kubernetes privileges
- Publicly exposed VM instances with cleartext cloud keys allowin cross-account access
- Publicly exposed KMS encryption keys
- And many more

Provided with actionable insight and context, security teams can see what's most important to fix first, and push this information out to developers with both a full understanding of its urgency, and clear steps to remediate the vulnerability before it's too late. As wiz integrates with many tools these personas in the risk and security pipeline can be informed by sending these notifications and recommendations with the associated context to the tools they already use and love: Examples are Jira, ServiceNow, Splunk and slack, and many more.



Wiz Security Graph visualization of an exposed Google Cloud Compute Instance with a critical vulnerability and a lateral movement finding on which Google Cloud's Security Command Center has also detected potentially suspicious events.

How Wiz complements the GCP ecosystem

As a cloud-agnostic solution, Wiz enables a standardized approach to vulnerability management and risk prioritization across GCP, AWS, and Azure clouds as well as Kubernetes. Within the GCP ecosystem, Wiz integrates with Google's native security capabilities to help organizations:

- **Enhance cloud inventory and asset management –** Wiz performs a full-stack cloud inventory to identify every asset across clouds and architectures. Going even further, the solution also scans, and correlates exposed secrets, cloud keys, and certificates in cloud environments, workloads, and technologies.
- **Identify high-risk lateral movement –** As a full-fledged Cloud Infrastructure Entitlement Management (CIEM) tool, Wiz complements GCP IAM Recommender and provides additional context to show possible lateral movement from a VM or container to a GCP Role with high permissions and excessive access.

- **Automate remediation –** Wiz allows you to automate the remediation of misconfigurations detected in your cloud environments. To do so, we rely on a least-privileges approach and use GCP Cloud Services such as Cloud Pub/Sub and Cloud Functions deployed in the enterprise organization. Automated actions speed up problem resolution while alerting teams about detected issues via integration with google chat.

- **Automate remediation** – Wiz allows you to automate the remediation of misconfigurations detected in your cloud environments. To do so, we rely on a least-privileges approach and use GCP Cloud Services such as Cloud Pub/Sub and Cloud Functions deployed in the enterprise organization. Automated actions speed up problem resolution while alerting teams about detected issues via integration with google chat.

What Wiz delivers for GCP customers

As organizations face urgent cloud security and compliance needs, Wiz delivers key benefits with rapid return on investment and a low total cost of ownership.

- **Risk mitigation –** Organizations can eliminate blind spots in their multicloud environments to identify and prioritize vulnerabilities wherever they exist. By working quickly to remediate the most critical risks, you can protect your business's most important assets more effectively. The context captured by Wiz also speeds threat detection and response to minimize the impact of any incidents that do occur.

- **Data Cloud Security** - Wiz helps protect data within the Google Cloud environment with fully integrated data security posture management (DSPM) for your data as well as support for Google Cloud Vertex AI. With Wiz for DSPM, you can easily discover sensitive data in your buckets, data and OS volumes, and managed and hosted databases. Wiz can also protect ML models in Vertex AI against data leakage and data poisoning to innovate faster and more securely in Google Cloud.

- **Operational efficiency –** With security resources and talent stretched thin, Wiz helps teams get more done, more easily. Agentless scanning eliminates the overhead of agents and their lifecycle including the organizational friction of overcoming developer resistance. With less alert noise and manual effort, skilled personnel can focus more effectively on core security priorities. Automated governance helps maintain security standards without diverting team focus. Enriched tickets and automated workflows speed remediation.

- **Cost reduction** – With a single solution to scan their entire cloud environment, detect and analyze risks, and manage cloud entitlements and configurations, organizations can eliminate many of their existing point security products and their costs for licensing, deployment, integration, and support.

- **Business acceleration** – Developers can focus on building services and driving integration without getting bogged down in security. They don't need to do regression or impact testing as the Wiz Cloud-Native Protection Platform is agentless; Wiz can be integrated pre-deployment and scan container images, VM images, and Infrastructure as Code (IaC) to prevent issues in production. With full confidence in their ability to identify risks across fast-evolving environments, security teams can act as enablers rather than blockers.

Accelerating GCP and multi-cloud adoption by simplifying security management

By migrating to GCP and integrating into WIZ, organizations gain access to the most innovative tools and services on the cloud market, allowing their business to move faster, be more agile, and beat the competition in a secure way. Wiz helps you to support your cloud journey so that you can move confidently by taking an entirely new approach to cloud security. Instead of working through piecemeal point solutions and patchwork visibility, security teams can seamlessly scan the entire cloud environment with a single tool. Instead of being overwhelmed by high volumes of noise with low-value signals resulting in a flood of undifferentiated alerts, they can now quickly identify and address the real risks associated with the combined workload, cloud, and business context.

Wiz CNAPP helps organizations to simplify security, compliance, and risk management across their entire cloud organization relentless of cloud solution provider, technology, infrastructure, or architecture. The solution provides full feature parity and standardized security controls across GCP, AWS, Azure, and every flavor of Kubernetes to eliminate vendor lock-in, inconsistencies, and duplicative effort. With a single graph database across clouds, workloads, and Kubernetes, security and operations teams gain the truly holistic visibility they've needed to deal with the most challenging questions.

On an organizational level, Wiz helps to solve some of people and dynamic process problems in addition to technology problems. By bringing Developers and DevOps teams together into the risk remediation process, empowered with the context they need to understand its urgency as well as actionable steps for a fast response, Wiz contributes to a culture of security in everything employees do.

Conclusion

Wiz gives you full visibility across your cloud organization helping you to unlock the transformative value of the cloud in a secure and compliant way, providing organizations of all sizes an effective way to manage the challenge cloud could bring related to security, risk and compliance. Wiz leverages a strong partnership with Google and deep expertise in GCP technologies, security tools, and processes to help our customers solve the security challenges posed by their multi-cloud strategy. As the first cloud security platform to integrate with Google Cloud Security Command Center (SCC), Wiz extends and complements Google's native security capabilities for a faster, simpler, and more effective approach to threat prevention, detection, and response in Google Cloud workloads. Listed on Google Cloud Marketplace, the Wiz Cloud Infrastructure Security Platform makes it possible for companies to find and fix risks that matter most to their business before they fall victim to a threat, or threat actor so they can move forward in their cloud journey to unleash the full potential of value of cloud with confidence.

To learn more about how you can enhance your security posture and accelerate your cloud adoption, contact Wiz to see a demo of the integration in action.

About Wiz

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 30 percent of the Fortune 500, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks and Aglaé. Visit https://www.wiz.io/ for more information.