

**WIZ** Google Cloud

**3 steps to secure  
everything you  
build and run on  
Google Cloud**

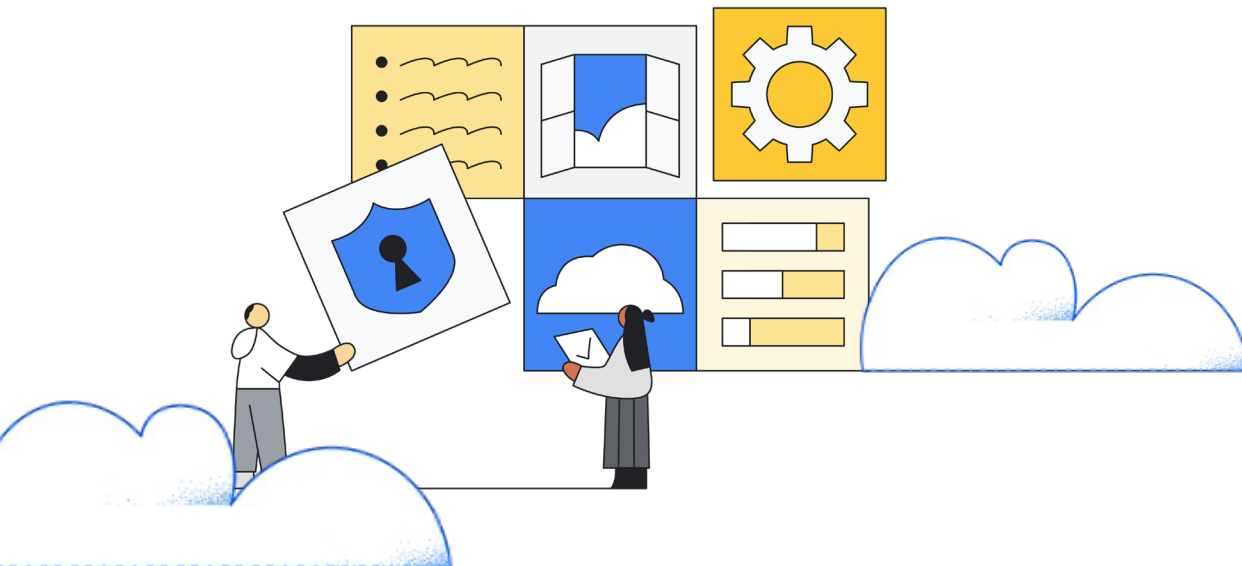


## Get the right context to prioritize risks

Google Cloud drives cost efficiency, increases productivity, and creates accelerated opportunities for innovation. However, as more companies modernize their applications and services using cloud technologies, they outpace the ability to fully secure their cloud environment. According to [IBM's 2023 Cost of a Data Breach report](#), over 80% of data breaches involved data stored in the cloud. Every day, security and operations teams receive an average of [4,484 alerts and spend nearly three hours](#) manually triaging those alerts.

## More cloud = more complexity + risk

Keeping track of assets on-premises, in Google Cloud, and in other public and private clouds is no small challenge. Most security and operations teams struggle to visualize and understand the relationships among overlapping layers of configurations, networks, and identities. This makes it hard to develop effective access or permissions: in other words, it's difficult to know what's exposed where, to whom, and why it matters.



# 80%

The number of data breaches involving data stored in the cloud

# 4,484

The number of daily alerts SOC teams manage

# 3

The number of hours SOC teams manually triage alerts daily

Enterprises adopt dozens of security tools and stitch outcomes together to gain control in an endless and often exasperating effort to close visibility gaps. As a result, a unified, coherent view becomes increasingly elusive, resulting in several challenges, including:





**A lack of visibility** across the complete multicloud environment makes it hard to know what a company has and where. This is especially true for security teams with little control or insight into developers' ongoing cloud activities compared to on-premises environments. Developers can procure and deploy cloud storage and services without oversight from the security team. They can also iterate quickly, which means a constant stream of software updates to monitor for vulnerabilities.


**An overly complex suite of cloud security tools** gives a fragmented and noisy view of security across multiple cloud environments.

**Lengthy risk resolution times** are due to a lack of perceived urgency and ownership spread across many teams.

**Alert fatigue** makes it too easy for security teams to overlook a threat buried in a sea of alerts.



It's time to cut through the noise, focus on what's important, and keep everything the organization builds and runs in the cloud secure. To identify critical risks, companies need the ability to scan their full-stack proactively. This means scanning every virtual machine (VM), container, serverless function, workload, and cloud configuration without disrupting business operations.



**Here are three critical steps companies can take to secure their cloud environment.**



## Identify critical risks

When an organization's cloud environment is breached, it rarely results from an isolated issue. Cyberattackers prey on seemingly insignificant and unrelated issues hidden in obscure corners of a company's infrastructure. These issues may seem harmless in isolation, but they can create a toxic combination that makes a full attack path possible.

To keep cyberattackers out, companies must think like the attackers. Cybersecurity teams must continuously monitor workloads for vulnerabilities and scan for misconfigurations, complex chains of exposures, lateral movement, malware, and more across the entire architecture. An agentless security solution can seamlessly scan the whole cloud environment to provide complete visibility across containers, Kubernetes, serverless environments, and data stores. This way, the company will get full coverage in minutes without disrupting business operations or requiring ongoing maintenance. An agentless solution also scales as needed without impacting resource or workload performance.

*Cyberattackers prey on the seemingly insignificant and unrelated issues hidden in obscure corners of a company's infrastructure.*

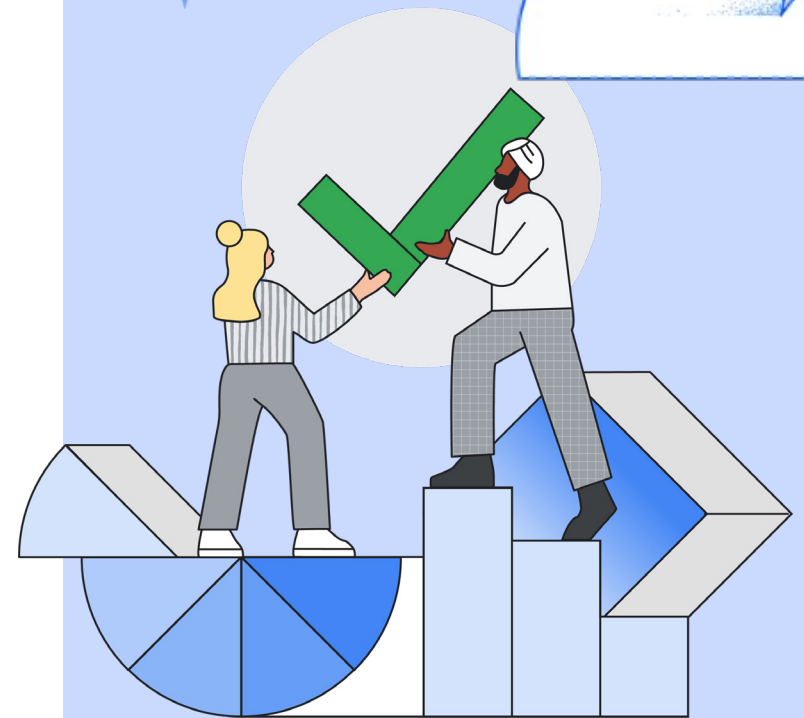


## ✦ Prioritize risk and attack paths to critical assets

To prioritize threats and remediate them before they become opportunities for cyberattackers, SOC teams need both breadth and depth of visibility to contextualize risks. This requires a comprehensive view of the tech stack. It should drill down to each workload on the network, what it's connected to, and what data it can access. SOC teams also need to know how those connections have changed over time.

When organizations can visualize interconnected risks and see the pathways to a breach, they can prioritize misconfigurations using operational, business, cloud, and data contexts. Look for tools with deep analysis capabilities to help identify toxic combinations and visualize the full attack path to critical assets. To cut through the noise and narrow focus on critical issues, insist on solutions that provide a single, prioritized view of risks.

*To cut through the noise and narrow focus on critical issues, insist on solutions that provide a single, prioritized view of risks.*



## Strengthen the cloud—proactively

With visibility and security across any cloud architecture, plus a prioritized list of actual risks in a company's cloud environment, organizations can begin to bring developers and DevOps teams into the risk remediation process with a single source of truth. This enables a partnership between developers and security to shift left and resolve issues across the application lifecycle. Developers are empowered to fix the problems before they reach production. Security teams can then act as enablers rather than blockers, confident in their ability to identify risks across fast-evolving environments.

As a result, the organization can ship applications faster by eliminating operational silos and empowering cross-functional teams to fix and proactively prevent issues across the development lifecycle.

Does this sound daunting? What if companies could begin to continuously scan their entire environment – on-premises, on Google Cloud, and elsewhere? What if they could identify and prioritize critical risks and proactively strengthen their cloud with a single solution? What if that solution could scale to any cloud environment in minutes with zero disruption to workload performance? If it sounds too good to be true—it isn't.

With Wiz and Google Cloud, organizations can.

“A lot of security teams get very good at securing the things they know about. So, the real risk lies in the things they don't know about, or the technology they didn't know was deployed. We needed a solution that could focus on our cloud security gaps, the outlier risks, and the unknowns.”

Mark Stanislav, VP of Security Engineering, Governance, Risk and Compliance, FullStory



# Secure Google Cloud and entire multicloud environments with Wiz

No matter where an organization is on its Google Cloud journey, Wiz can help rapidly improve its security posture, consolidate security tools, eliminate agent overhead, expedite detection and response, optimize security processes, and reduce noise. This results in up to 4-5x improved cloud visibility and coverage and a 10x improvement in time and effort spent to find and remediate issues.

Wiz integrates with Google Cloud's native security capabilities to help organizations:



**See everything** with a full-stack cloud inventory to identify every asset across multiple clouds and architectures.



**Detect threats** with Google Cloud Security Command Center. Ingest data and add context to cloud events to provide a single, prioritized view of issues in a unique, easy-to-use Wiz Security Graph user experience.



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

Powered by Google Cloud, Wiz uses agentless scanners on every layer of multicloud environments to provide complete visibility into every technology and securely advance the organization's cloud journey.

[Learn more about Wiz on Google Cloud.](#)

## The results

4-5x

Improved cloud visibility and coverage

10x

Time and effort improvements to find and remediate issues