**Cloud security reimagined**

As previously discussed, the legacy approach to cloud security not only leaves organizations vulnerable to risks and bad actors, but it can also impede the speed of doing business.

Wiz addresses this challenge by creating a normalizing layer between cloud environments, allowing customers to swiftly identify and eliminate critical risks. Our cloud-native visibility solution provides a 360° view of security risks across clouds, containers, and workloads, utilizing graph-based analysis to delve deep into risks and provide actionable insights without requiring an agent.

Wiz's approach to cloud security is revolutionary and based on four key steps: (see image below)

metin, ekran görüntüsü, yazı tipi, logo içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Connect**

You don't install or deploy Wiz, you only connect it, and connecting takes only a few minutes per cloud provider. One Wiz customer got everything running in less than a week after spending 18 months trying and failing to deploy a competing product. Moreover, you only need a single connector per cloud provider to cover your entire stack: VMs, containers, serverless functions, and PaaS. Wiz offers this coverage for all major cloud providers, including Amazon Web Services,

**Analyze**

Analyzing every layer of your stack, evaluating your architecture, and calculating risk factors such as internet exposure, software and configuration vulnerabilities, effective permissions, exposed secrets, and malware

With this detailed and comprehensive understanding of your environment, Wiz is able to perform all of the checks found in traditional CSPM, patch and vulnerability assessment, network exposure, secrets scanning, and malware tools.

**Focus**

Modeling your assets and their interconnections using a node-and-edge graph makes it possible to identify the most toxic risk combinations that need to be prioritized for remediation

**Harden**

Wiz gives you a rich set of tools and information to proactively protect your environment both post- and pre- implementation:

• A wide variety of built-in integrations with ticketing, workflow, and messaging applications make it easy to route key information generated by Wiz to the teams responsible for performing remediations.

• A powerful and flexible set of tools to automate this routing and to track resolution helps you set, enforce, and follow up on your organization's policies.

•Integration with your CI/CD pipeline helps you shift left in your enforcement of security policies, preventing at-risk software or assets from even reaching production environments in the first place.

Security in the cloud can often be reactive, causing unnecessary friction and hindering business growth. Wiz offers a better approach to cloud security that enables customers to proactively identify and mitigate risks while supporting business objectives. By utilizing Wiz's unique perspective, organizations can view their cloud environment through a lens that provides clarity and actionable insights, empowering them to secure their cloud and drive business forward.