Datasheet

Cloud native container security for cloud native applications

Cross-cloud contextualized container & Kubernetes security

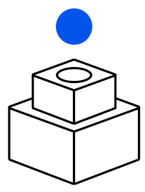
Get complete visibility across containers, Kubernetes, cloud environments, and architectures in minutes without agents. Leverage the power of the Wiz Security Graph to analyze and prioritize risk with complete context. Use a single security platform to partner with developers to shift left and resolve issues across the lifecycle of the containerized application.

The cloud has enabled every organization to innovate faster and with more agility. As environments grow more complex (new workloads, architectures, roles, users, etc.), answering questions like “what databases are exposed to the internet” is painfully difficult. Maintaining a strong security posture and ensuring that security can scale with developers and DevOps is hampered by fragmented tooling and limited context.

The Wiz security stack includes a full-fledged container security solution for containerized workloads. Unlike traditional solutions that rely on agents, Wiz delivers complete agentless visibility into your containers and Kubernetes clusters across clouds and architectures. The graph-based approach spans the full risk landscape of your environments to bring together context across risk factors and perform deep risk assessment, so security teams can understand and prioritize risks in their containerized environments.

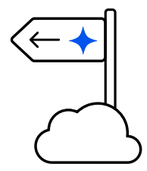
Complete visibility

Discover and scan all your containers, hosts, and clusters across cloud-managed and self-managed Kubernetes, serverless containers, and standalone containers running on virtual machines to build a complete understanding of your containerized environments without blind spots.



In-depth risk assessment

Correlate and prioritize container risks using the power of the Security Graph by combining data from containers, hosts, cloud providers, and Kubernetes APIs to identify vulnerabilities and misconfigurations, internet-facing containers, excessive permissions, and exposed secrets to proactively remove container risk and stop attack paths into your environments.



Shift left

Partner with your development team to identify and prevent container security issues across the SDLC. Secure container images from the developer’s sandbox into run-time. Scan the infrastructure, including Kubernetes YAML files, Docker files, Terraform and ensure security compliance while deploying.

Trusted by the world’s best brands

Wiz provides coverage for

A unified cloud security platform providing a simple way to assess threats in context and rapidly respond to minimize impact

Secure container images across the lifecycle

Scan container images in the CI/CD pipeline to detect vulnerabilities and exposed secrets before pushing images to the registry.

Scan IaC (DockerFile, Kubernetes YAMLs, Helm) with Wiz Guardrails

Scan container images with Wiz Guardrails and registry scanning

Block security riskswith Wiz AdmissionController

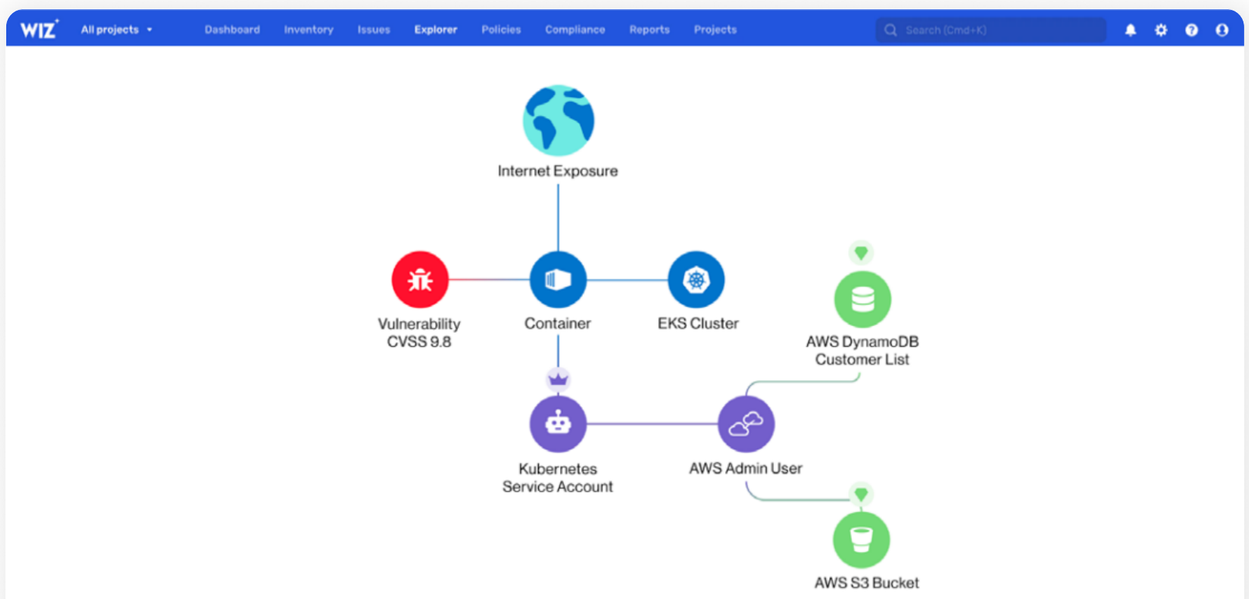
Agentless scanning of running containers

Graph-based risk correlation and prioritization

- **Leverage the power of context:** Correlate multiple risk factors across containers, hosts, Kubernetes clusters, and the cloud environment to identify the most critical risks and prioritize remediation.
- **Unified security policies:** Scan Infrastructure-as-code (IaC) files across Dockerfiles, Kubernetes YAML manifests, and Helm charts for misconfigurations and security risks. Automatically assess one security policy across your cloud and Kubernetes development lifecycle and decide whether to block builds that violate it. Validate compliance with security policy before container images are deployed in the cluster.

Automatic Kubernetes Security Posture Management (KSPM)

- **Continuous monitoring:** Continuously assess Kubernetes clusters to identify misconfigurations and suggest remediation steps to mitigate threats and harden your clusters.
- **Compliance assessment:** Get reports mapped to the CIS Foundation Benchmarks for Kubernetes, EKS, AKS, and GKE to assess the security of your Kubernetes environments and ensure compliance.
- **Built-in & custom rules:** Leverage built-in rules and create custom rules using OPA's Rego querying language.



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 35 percent of the Fortune 100, 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, Lightspeed and Aglaé. Visit https://www.wiz.io/ for more information.

WIZ

"We needed a non-intrusive solution for our containerized production environment that didn't require agents, wasn't too noisy, and didn't require real-time scanning. Choosing Wiz was a no-brainer — no other tool comes even close."

Adam Schoeman
Interim CISO, Copper

copper

"We use most major cloud providers and saw immediate value as we deployed Wiz. We found misconfigurations and other issues, and Wiz gave us visibility into the overall security posture in our cloud that we couldn't easily stitch together with other solutions."

Jeremy Smith,
VP Infrastructure Security Officer, Avery Dennison

AVERY DENNISON

"Pairing engineers who understand the risks with the tools to remediate them is incredibly powerful. There are 10X as many environment owners, developers, and engineers using Wiz than there are security team members at FOX. This helps us to ensure that the products shipped across over 1,000 technologists across the company have security baked in, which is beyond the impact that a small and mighty cybersecurity team can have alone."

Melody Hildebrant,
CISO, Fox

FOX

"If you're deployed in the cloud, right now, and you need to close down your issues, go talk to Wiz."

Igor Tsyganskiy
CTO, Bridgewater Associates

BRIDGEWATER