Datasheet

Runtime Sensor

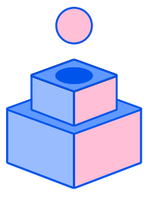
Agentless with runtime context gives the best of both worlds

Wiz started with and continues to push the boundaries of what agentless technology can do. The Wiz approach to cloud security will always be agentless first, but there are distinct use cases that can be strengthened by capturing runtime context. Attackers' actions in the cloud span numerous layers, from the infrastructure control plane to Kubernetes control planes and individual workloads. This complex architecture further complicates efforts to piece together the puzzle of cloud-native attacks, hindering the ability to detect and respond quickly.

The Wiz sensor is developed specifically for cloud environments to support ephemeral resources and reduce concerns about resource consumption that have plagued traditional agents. It is a lightweight eBPF-based agent that can be deployed on container hosts, Linux workloads, and serverless compute to provide real-time visibility and monitoring of running processes, network connections, file activity, system calls, and more to detect malicious behavior affecting the workload. When combined with the agentless, API-based visibility and cloud risk assessment of the Wiz Security Graph, organizations gain the best of both worlds.

Container security

The sensor supplements agentless container security by validating vulnerabilities in memory on container hosts, giving teams improved prioritization. Additionally, drift detection, runtime FIM and SBOM features are supported to help ensure there is no unwanted or nefarious activity on the container host.



Defense in depth

The sensor itself provides standalone runtime detection and response by supporting custom runtime threat detection rules and automated response policies. Detection matching these runtime rules can range from adding a finding to the graph to triggering a response policy. Common response policies include simulation and blocking.

Cloud detection and response

The sensor is a critical component of cloud detection and response. It captures kernel-level runtime events, sending them to the Wiz backend for use in advanced cross-layer behavioral and anomaly-based detections. The sensor also expands the possible response actions by allowing SecOps teams to respond at the process level container hosts, workloads, or serverless compute.

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

Runtime container security

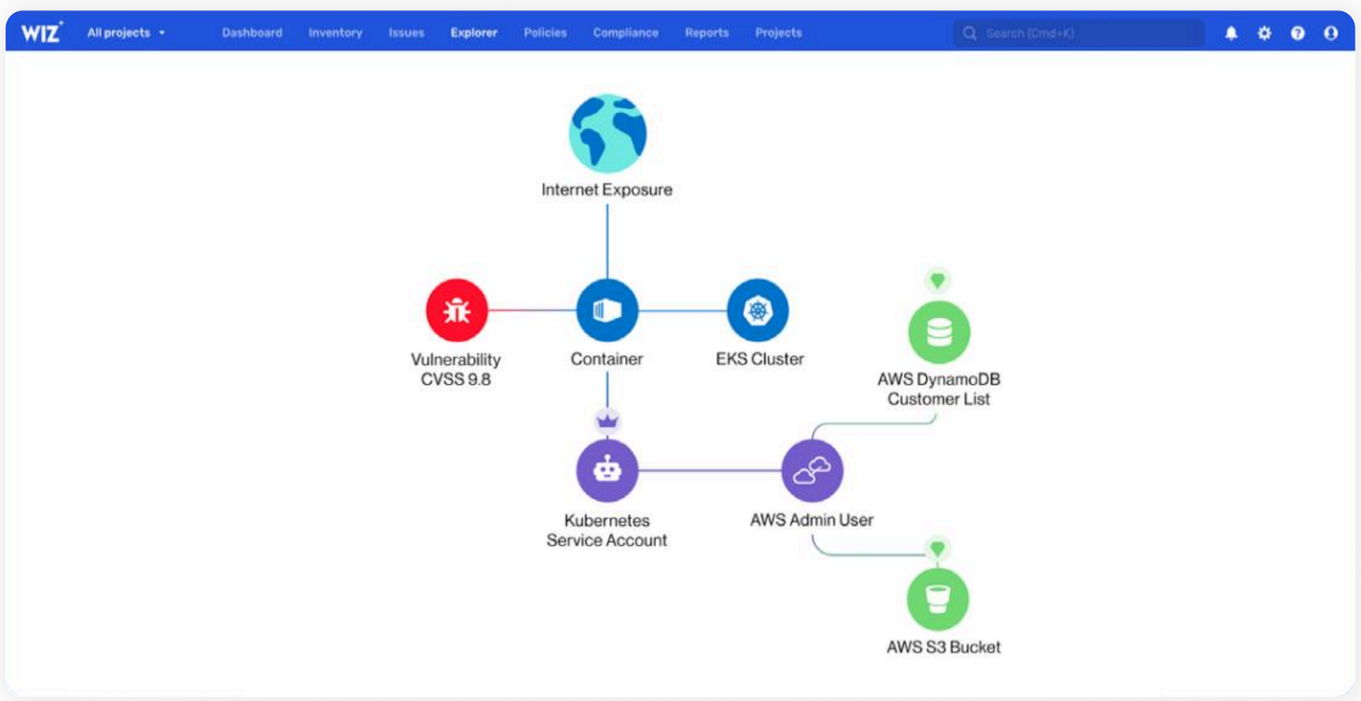
- **Improve prioritization:** Container images can be notorious for having many open source packages or other unused packages. The sensor validates vulnerabilities at runtime, further improving prioritization.
- **Container host integrity:** The sensor provides drift detection and runtime file integrity monitoring to detect and alert on changes to the container image or unauthorized changes to files matching detection rules.

Runtime monitoring and response policies

- **Custom runtime rules and response policies:** Users can create custom detection rules, evaluated in real-time on the sensor, to inform responses ranging from informational alerts to automated blocking of known malware and malicious processes.
- **Real-time monitoring and blocking:** Wiz ensures comprehensive coverage against known and emerging threats, including cryptocurrency miners, ransomware, remote shells, and various techniques employed by threat actors.

Runtime context for cloud detection and response

- **End-to-end visibility into attacks:** By correlating events across runtime signals, cloud and K8 audit logs, identity, data, and network, SecOps teams can detect threats across layers and gain a unified, contextual view of attacks.
- **Precision response.:** The sensor extends response actions to the workload, including process termination and additional runtime actions.
- **Powerful forensics:** The sensor is essential for comprehensive forensic collection. It automatically collects runtime execution data, process tree information, and raw telemetry for every resource running a sensor. This greatly improves root cause analysis for any detection.
- **Runtime hunting:** The collection of runtime execution data (RED) enables teams to proactively hunt for threats. The RED Explorer collects and retains all runtime execution data across any cloud environment.



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