Datasheet

Wiz Defend

Detection and response re-imagined for the cloud

Wiz Defend enables SecOps teams to overcome the challenges of detection and response in the cloud. As cloud environments become increasingly complex, traditional security tools fall short. These tools lack critical cloud context, provide inadequate detection coverage, generate excessive noise, and do not facilitate rapid containment, leaving organizations unnecessarily susceptible to breaches and business disruptions.

Wiz Defend addresses these challenges and more with a unified platform powered by Wiz Cloud Threat Intelligence and the Wiz Security Graph. Threat intelligence is key to Defend's thousands of pre-built detection rules, which are based on a recommended set of telemetry sources, that ensure teams are prepared to respond to incidents as they occur. The Security Graph provides complete code-to-cloud context, improving the prioritization of detections by correlating broader security risks and giving SOC analysts the information needed to understand and rapidly investigate incidents.

During an incident, time is a critical factor in reducing overall business impact. Defend promotes collaboration between SecOps, CloudSec, and developers, and enables Incident Responders to issue actions from the platform to contain a threat.

Incident Readiness

The SOC needs to know if they are prepared for a threat and have the necessary telemetry for root cause analysis. Defend Incident Readiness continuously closes visibility gaps, automatically surfacing where telemetry is missing and providing actionable recommendations to improve visibility tied to the MITRE ATT&CK framework.

High-fidelity detections

The SOC needs to reduce noise and gain confidence that each detection accurate and actionable. Defend delivers high-fidelity cloud-native detections, combining unique cloud threat intelligence from the Wiz Research team with behavioral analanalytics and the deep context of the Wiz Security Graph.

Accelerated Investigation & Response

The SOC needs to reduce the time and manual effort required to investigate cloud detections. Defend delivers by grouping individual detections into an attack story and visualizing it on the Wiz Investigation Graph. For deeper analysis the threat is shown on a timeline with the detection events and surrounding resource activity.

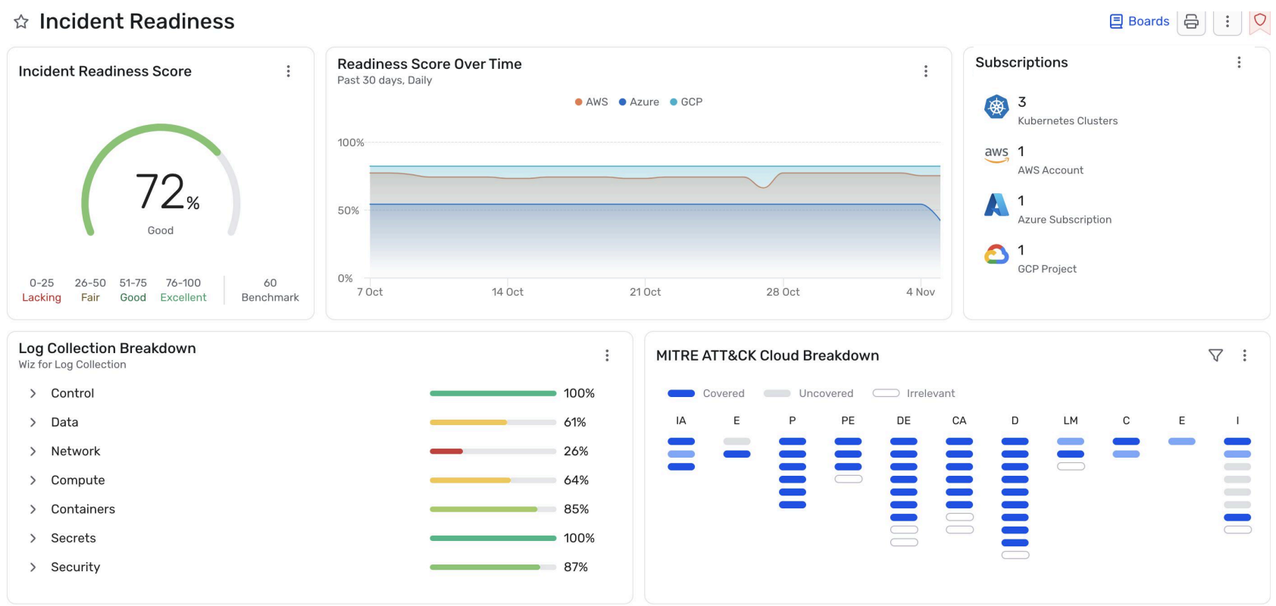
Trusted by the world's best brands

Wiz provides coverage for

A unified cloud security platform to enable SecOps teams to stop cloud incidents before they become breaches

Empower SecOps to perform at cloud speed

- **Cloud threat intelligence:** With data from the largest cloud environments in the world, the Wiz Research team is uniquely positioned to stay ahead of evolving threat tactics, techniques, and procedures seen in the wild. These research findings are developed into detection rules so customers always have coverage for the latest attack trends.
- **Telemetry collection:** Defend's Incident Readiness maps cloud telemetry to the MITRE ATT&CK cloud matrix, enabling teams to prioritize telemetry collection most relevant to their threat model and facilitate conversations between infrastructure, SecOps, and security architecture teams.
- **Runtime blocking:** The Wiz sensor blocks known and unknown cloud threats, including malware, cryptominers, reverse shell, suspicious IOCs, and more. By automating these responses, the SOC can focus on more critical tasks.
- **Advanced detections:** The Defend detection engine combines specialized detection rules with behavioral analytics and context from the Wiz Security graph to generate high-fidelity alerts across runtime, control plane, identity, data, network, version control systems, and more - expanding detection coverage while reducing noise
- **Reduce mean time to respond:** Graph context provides analysts with actionable detections. Defend also automates the collection of resource activity surrounding a detection and identifies the blast radius of an attack, eliminating time-consuming, manual investigation steps. The Wiz SecOps AI Agent accelerates this even further by automatically investigating and delivering trusted verdicts on every single threat
- **Seamless containment:** Stop threats before business impact is achieved with automated recommendations for immediate containment, both at the workload level with process-level blocking and at the cloud level through the CSP native control plane. Run containment actions manually with one click or construct automated playbooks, integrated with existing SOAR solutions.
- **Cloud forensics and threat hunting:** Copy volumes to forensic accounts, download forensic packages, retain execution data, and access process tree information to preserve the chain of custody, enable root cause analysis, and support threat hunting. For VMs with Sensor, auto collect and analyze forensics packages based on TDR triggers.
- **Complimentary workflow:** With hundreds of pre-built integrations with SIEM, SOAR, and other SecOps tools, Wiz Defend enables teams to maintain their existing operational workflows for threat response.
- **Wiz Incident Response:** Even the most prepared teams feel the pressure when faced with a true-positive incident. Wiz Incident Response helps you investigate and contain threats with deep visibility into your cloud environment. By combining expert guidance with Wiz's technology, we give your team the clarity to act quickly and confidently.



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

> The MITRE ATT&CK framework is like my Bible. Wiz Defend gives me a clear way to understand what we're missing, so we can focus our time on specific logs, and I can be confident that if there's a problem, we'll catch it
>
> Suzanne Senoff
> CISO, PROS

> A few months ago, we had an incident related to cryptominers in one of our sandboxes. I had to do all of the investigation manually to understand the situation. The next time we had a similar incident, we had Wiz Forensics, and we were able to send a snapshot to a new account in minutes."
>
> Steve Litras,
> Senior Director of IT & Security, Cribl

> The products today aren't designed to help drive incident response in the cloud. [CDR] is a fresh perspective to me that I think is critical for the industry and really solves a problem that I think most CISOs have today.
>
> Nicole Ford
> CISO, Rockwell Automation