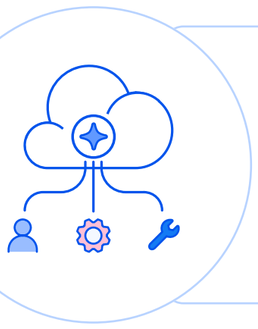
Solution Brief

Wiz Defend: Solution Brief

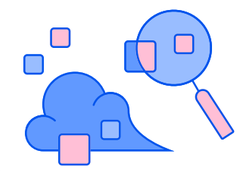
Wiz Defend enables the Security Operations team to detect and respond to cloud threats in real time, leveraging the power of the Wiz Security Graph to correlate signals across the cloud environment – ranging from runtime signals from our lightweight sensor, to cloud-native telemetry, to identity providers, version control systems, and more – and drive down mean time to respond.

Key Capabilities



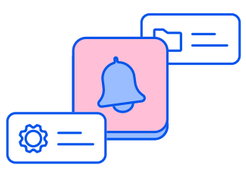
PREPARE

Automatically map your visibility – over both runtime and control plane – and ensure you're ready to respond to an incident.



INVESTIGATE

Automated threat timelines, blast radius graphs, and more. Hunt for threats and surface cloud context to get to the bottom of alerts faster.



DETECT

High fidelity cross-layer threat detection across runtime, data, identity, and network.

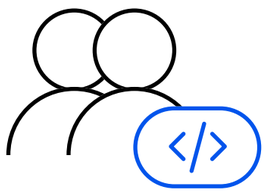
RESPOND

Cloud-native containment, workload level process termination, forensics, and more: stop threats and remediate root causes.

The Last Line of Defense in the Wiz Cloud Security Platform

Wiz Code
Secure Cloud Development

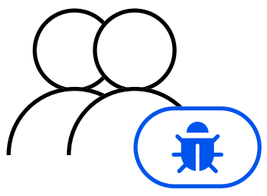
Secure every stage of your SDLC to gain visibility & prevent risks in code, pipeline, registries and images



Dev

Wiz Cloud
Manage Security Posture

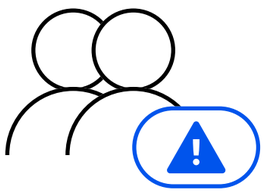
Agentless visibility & risk prioritization that proactively reduces the attack surface



Cloud Security

Wiz Defend
Respond to Cloud Threats

Analyze cloud events and lightweight eBPF-based sensor telemetry to protect against real-time threats



SOC

Get a demo →

Solution Brief

Cloud Incident Response Readiness

Collect What Matters Most to Prepare for the Worst

The Challenge

For security operations and incident response teams, the cloud generates huge amounts of real-time telemetry – but **ingesting and writing detection rules is extremely challenging** with traditional SOC tools. **Logging configurations drift**, leaving organizations with blind spots, and it's difficult to know **what telemetry is most important to detect and respond to cloud threats.**

During an Incident, We Ask...

- **Where are the logs?**
- Do we **store what we need?**
- Do I have **runtime visibility where I need it?**
- How do I know **who did what?**

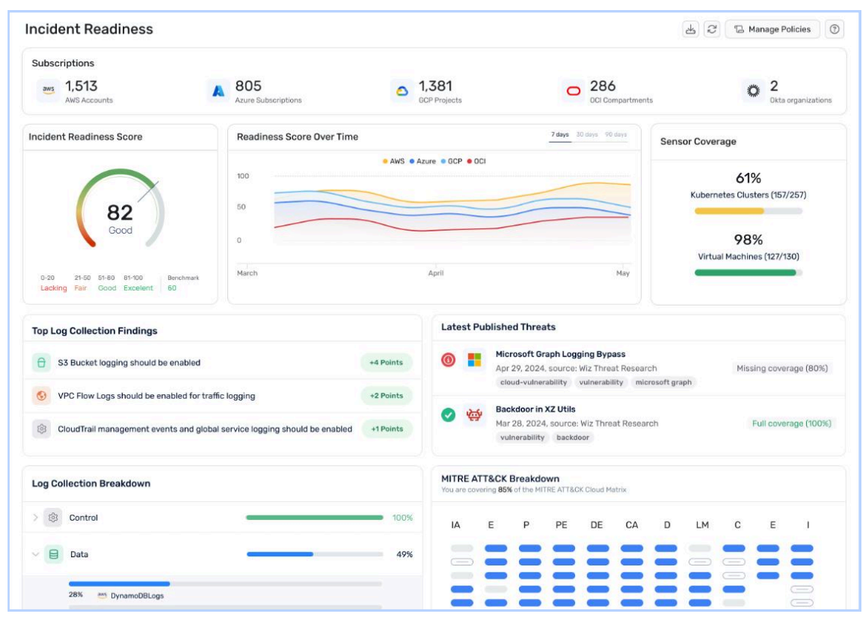
Before an Incident, the Reality Is...

- Logs are **too expensive**
- Telemetry configurations constantly **drift from policy**
- Teams struggle to understand **which telemetry is critical**

The Wiz Defend Solution

Ensure you're collecting the logs you need: **eliminate blind spots** with a **real-time asset inventory and telemetry gap analysis**, with coverage **benchmarked against the MITRE ATT&CK** matrix to optimize your collection for your **specific threat model**

- Wiz Defend provides **actionable recommendations for improving real-time visibility**, prioritized by security impact
- The platform provides automated code snippets and remediation options, enabling **security and infrastructure teams to work together more effectively**
- Wiz Defend continuously monitors for logging drifts, enabling organizations to **continuously close visibility gaps**



Get a demo →

Solution Brief

Multi-Cloud Threat Detection

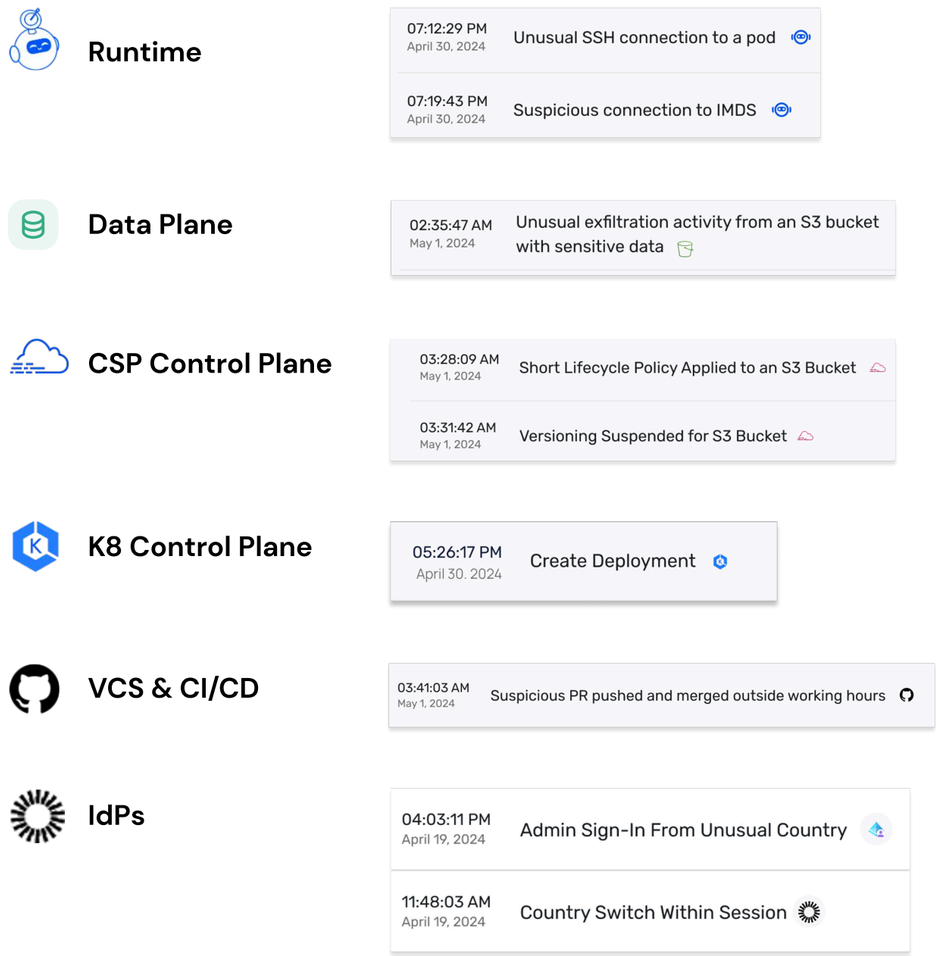
Eliminate Cloud Detection Engineering

The Challenge

- Cloud detection engineering is far too manual - organizations spend **years building custom rules, only to end up with partial coverage**
- Cloud detection knowledge and **talent remains incredibly difficult to find**
- **Existing SecOps tools, like SIEM, aren't built for the cloud environment**, and don't support the cloud-specific behavioral analysis required to detect cloud threats
- Multi-cloud environments drive unparalleled complexity, and organizations **struggle to maintain detection parity across CSPs**

The Wiz Defend Solution

- Save time and effort developing and maintaining custom rules, with **thousands of cloud-native detection rules curated by the Wiz Threat Research team**
- **Reduce noise** with our innovative blend of detection logic combined with cloud-specific behavioral analytics, all **normalized by the Wiz Security Graph**, for high-fidelity alerts
- Integrate data from all the tools in your environment, like ticketing systems, identity providers, and more to bring **context and explainability to alerts**



Get a demo →

Solution Brief

Investigation & Threat Hunting

Get Context You Need to Respond Faster

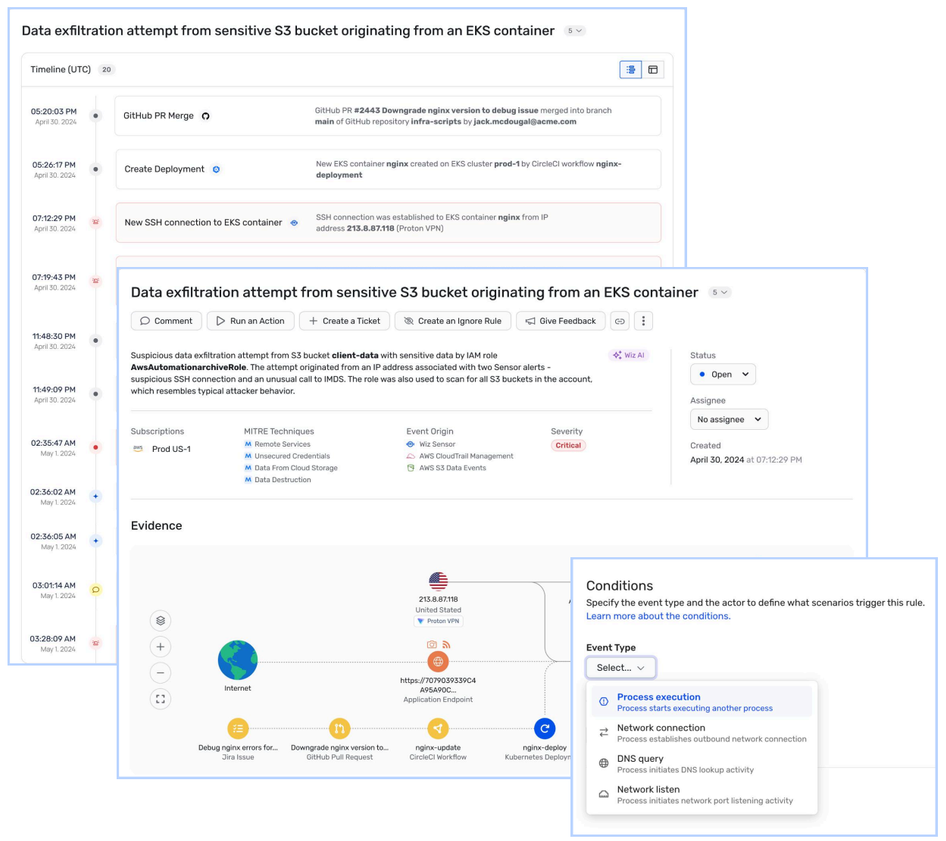
The Challenge

- The complexity of the cloud environment makes it **next to impossible to get a real-time view of an attack in progress**
- Security teams **struggle to gather enough context** to triage quickly and effectively and **correlate data across runtime, identity, data, and control planes**
- **Acquiring and analyzing forensic data requires specialized knowledge** and deep understanding of CSP APIs

The Wiz Defend Solution

Get the context you need to resolve alerts faster. Wiz Defend **eliminates manual cloud data correlation and endless SIEM querying**, enabling operations teams to quickly and easily answer key questions in an alert investigation.

- Automatically correlate thousands of cloud events from disparate sources including audit logs, service level logs, and numerous others to **condense data into a single attack timeline**
- Get the full view across your cloud runtime, control plane, identity providers, ticketing systems, and more to immediately piece together a **full picture of a threat**
- Conduct **host-level threat hunting and forensics** with Wiz's lightweight, **eBPF-based runtime sensor**



Get a demo →

Solution Brief

Multi-Cloud Threat Detection

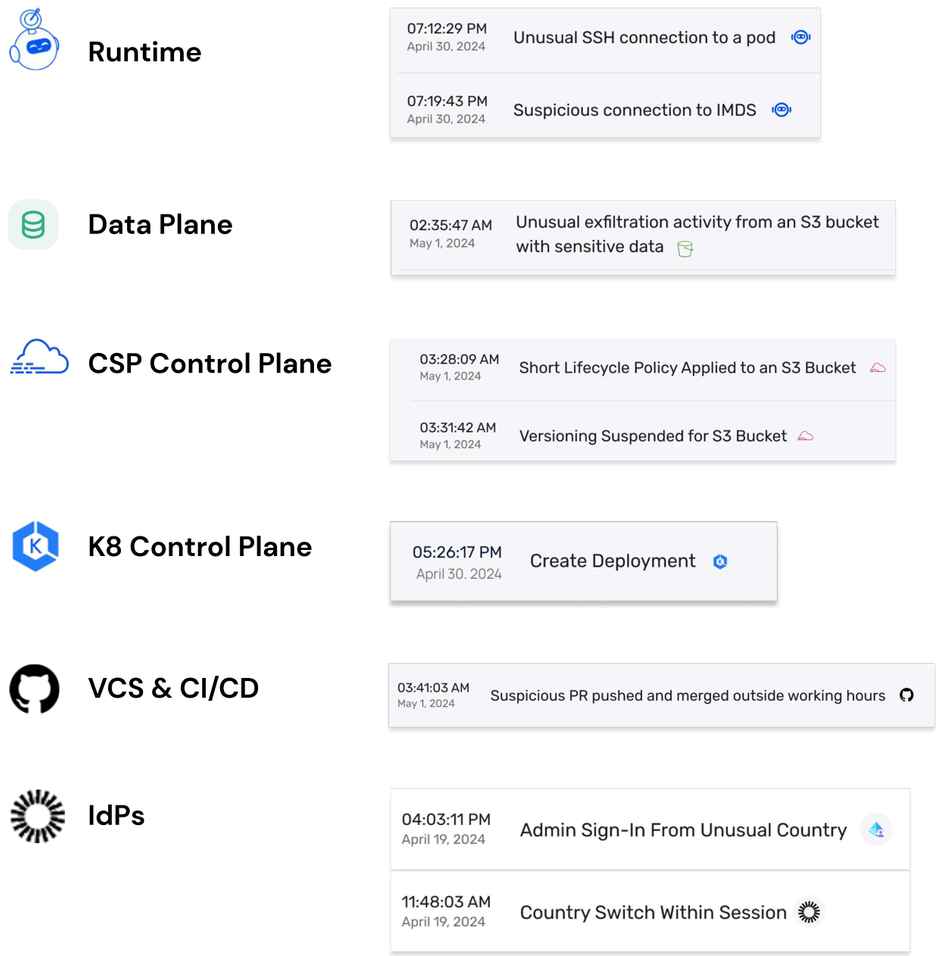
Eliminate Cloud Detection Engineering

The Challenge

- Cloud detection engineering is far too manual - organizations spend **years building custom rules, only to end up with partial coverage**
- Cloud detection knowledge and **talent remains incredibly difficult to find**
- **Existing SecOps tools, like SIEM, aren't built for the cloud environment**, and don't support the cloud-specific behavioral analysis required to detect cloud threats
- Multi-cloud environments drive unparalleled complexity, and organizations **struggle to maintain detection parity across CSPs**

The Wiz Defend Solution

- Save time and effort developing and maintaining custom rules, with **thousands of cloud-native detection rules curated by the Wiz Threat Research team**
- **Reduce noise** with our innovative blend of detection logic combined with cloud-specific behavioral analytics, all **normalized by the Wiz Security Graph**, for high-fidelity alerts
- Integrate data from all the tools in your environment, like ticketing systems, identity providers, and more to bring **context and explainability to alerts**



Get a demo →

Solution Brief

Cloud-Native Containment & Response

Stop Attacks and Uncover the Root Cause of the Incident

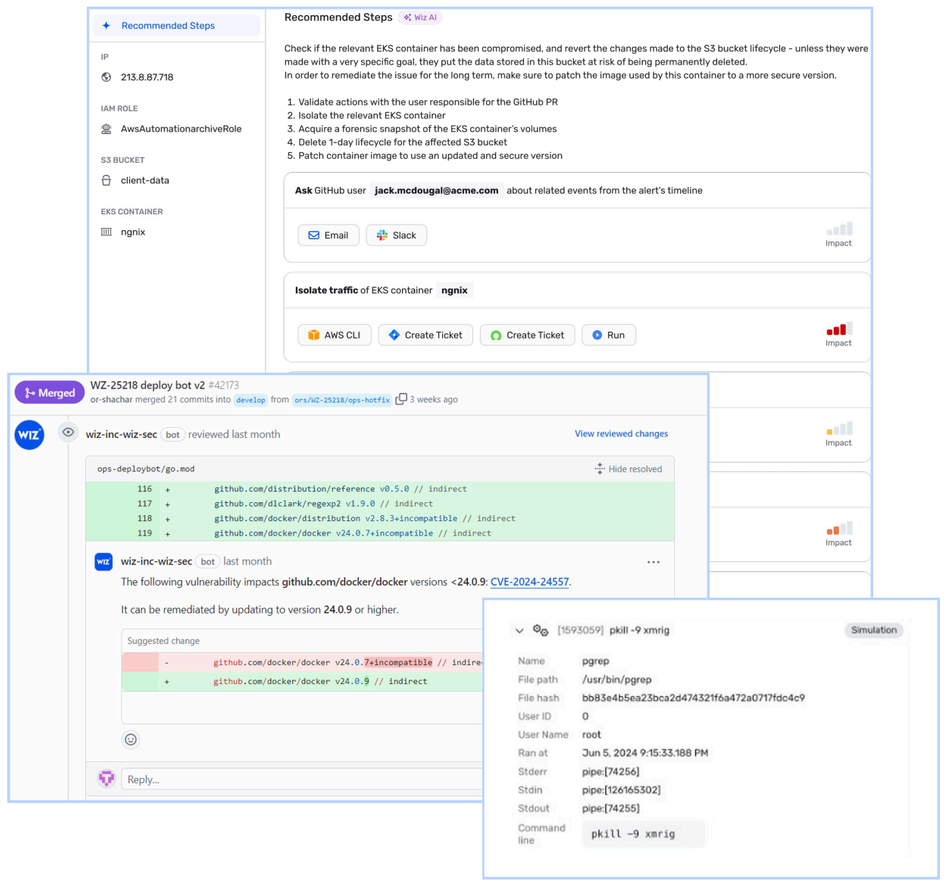
The Challenge

- **Cloud attacks are automated and efficient**, and teams need to contain an emerging threat in minutes to prevent business impact
- Forensic evidence often resides in **ephemeral resources**, and without advance preparation, **necessary data for root cause analysis can be unrecoverable**
- Remediation often requires **tracing activity back to vulnerabilities in code, and working with development teams** to implement fixes

The Wiz Defend Solution

Wiz Defend's threat response functionality provides automated next steps to contain every threat. Apply autogenerated IaC snippets, block processes with the Wiz Sensor, and collaborate with development teams to apply root cause fixes in code.

- Get **immediate next steps to stop every threat** – from reaching out to users, to isolating resources through the control plane, to terminating running processes
- Automate **acquisition of disk images, memory snapshots, forensic logs, and more**, while preserving chain of custody
- Integrate with version control systems and developer workflows to **identify and remediate issues at the code level**



Get a demo →