Double down on actionable context to improve your cloud security

Wiz and Amazon Security Lake help you bolster protection through cloud security data sharing

Security and data teams spend a lot of time wrangling data and piecing together information from disparate security solutions to make sense of the alerts they receive. For organizations using multiple Amazon Web Services (AWS) accounts, staying on top of continuous logs from their cloud environments and managing access and permission levels to maintain security is challenging.

Benefits of the integration

Consolidate security logs, run investigations, and analyze security metrics—all within a centralized data lake

Since Wiz integrates with Amazon Security Lake, you can bring together risks identified by Wiz as well as security events and log data—from both AWS and third-party services—into a single customer owned data lake. Amazon Security Lake supports the Open Cybersecurity Scheme Framework (OSCF), eliminating the extract, transform, and load (ETL) process and making it easier to surface the right data. Integrate Wiz as an Amazon Security Lake custom source to include security issues detected by Wiz as part of your security alerts, providing a comprehensive view of your security state in AWS.

Centralized data for full visibility

Amazon Security Lake centralizes security data from cloud and on-premises sources, making it easier to aggregate, manage, and derive value from log and event data. This enables greater visibility for security teams across organizations. With Amazon Security Lake, logs, such as flow logs from Amazon Virtual Private Clouds (VPCs), are automatically brought in from every AWS account into a customer owned data lake.

Common format for easier queries and sharing

The OCSF standard is designed to enable an extensible and normalized exchange of security data. Through a common format, information from various tools is aligned and can be easily queried or shared. For instance, security teams can quickly investigate incidents by reviewing logs from distributed services and infrastructure in the same format, then send it out to other team members through JIRA or Slack.

Alerts with the right context

Each security alert is enriched with detailed insights, such as the affected resources, associated misconfigurations, and relevant compliance frameworks. This additional context empowers your security teams to understand the full scope and impact of each alert, enabling more effective and targeted remediation actions.

Better Together

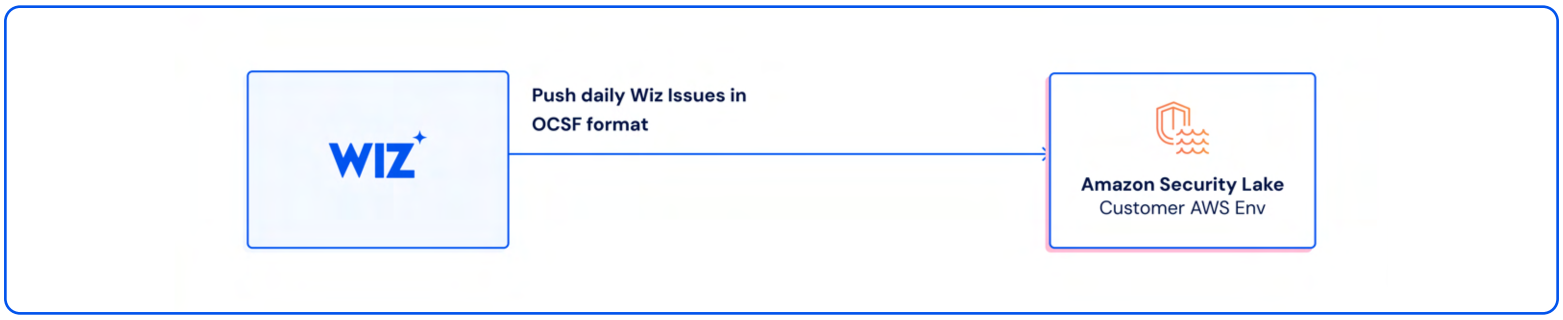
Wiz is focused on delivering the business and security context your team needs to proactively identify, prioritize, remediate, and prevent risks. Integrating with Amazon Security Lake allows Wiz to deliver a full picture of what's happening, helping you contextualize information and correlate it against additional data sources.

Use Case

See the full picture for better cloud security

The integration between Wiz and Amazon Security Lake has been designed with both security analysts and application developers in mind.

With a single data lake that uses a standard framework, teams can eliminate compatibility issues and easily leverage analysis from Wiz—including toxic combinations, lateral movement paths, and risk prioritization.



About Wiz

Wiz has fundamentally reimagined cloud security and enables cloud builders and defenders to know what needs their attention. Wiz provides organizations with instant visibility across their cloud environments without deploying agents and continuously analyzes security data across multiple risk factors—configurations, vulnerabilities, networks, identities and access, and secrets—across accounts, users, and workloads to discover the toxic combinations of risk that create attack paths into cloud environments. The correlated risk data provided by Wiz is powerful for security investigations and gathering security analytics.

For more information visit: https://wiz.io

Get started today

Sign up for a demo to learn more or check out the Wiz listing in AWS Marketplace to get started.

Get a Demo