StackRox

Looker

Case Study

Looker is a unified data platform supporting multi- and hybrid-cloud environments to deliver actionable business insights to employees at the point of decision. Looker's founders recognized that companies were accumulating enormous amounts of data but unable to get real-time insights.

Looker began by linking to data warehouses without requiring data to be dumped into Looker's datastore and eliminated the need to learn complex SQL statements. Looker was able to tell customers: we'll make it so that anyone in your organization can be empowered to make data-driven decisions. And it worked – for its customers, Looker provides a single source of truth for data, regardless of origin.

A Relentless Focus on Security

Looker uses a cloud-native architecture that allows them to be agile and resilient and is built for scale and portability. The company initially ran its data platform in Amazon Web Services (AWS) and has broadened to work across Google Cloud Platform (GCP) as well. Other cloud environments will be supported in the future. To provide additional scaling and failover capabilities, Looker made a strategic decision to use Kubernetes to manage containerized workloads and services for customers who select that environment.

"Looker's data platform sits on top of existing databases, so while we do not store any data, we have a relentless focus on securing the data visible on our platform," says Richard Reinders, Looker's manager for security operations. "The more customers can trust us, the more private data they can work with, and the more insights we can then provide. It provides value to us and them."

looker

Looker is a unified data platform that allows every user to easily explore, analyze and share real-time business analytics.

Headquarters:
Santa Cruz, CA

Founded: 2012

Environment:
AWS, GCP, Azure, Docker, Kubernetes

www.looker.com

> “We want to leverage what already exists rather than complicating things by adding more components. The Kubernetes-native architecture of StackRox enables us to do that.”
>
> – Richard Reinders, manager, security operations

Adopting Kubernetes to manage Looker’s container-based platform both provides new security capabilities and increases the attack surface. “Network visibility and vulnerability management are key components to ensuring that we can continue to build and retain trust with our customers,” states Reinders. “Plus Kubernetes itself represents a new layer that has to be secure as well.”

The Value of Kubernetes-native Security

Looker chose the StackRox Kubernetes Security Platform because of its broad set of security capabilities and its Kubernetes-native architecture. StackRox provides visibility into Looker’s cloud-native infrastructure, including images, containers, pods, namespaces, deployments, and clusters.

“It’s imperative for us to know where our vulnerable images are in our infrastructure and to know when Kubernetes is exposing something to the outside world,” says Reinders. “StackRox is giving us that visibility and vulnerability management. And StackRox serves up actionable security insights, so we maintain compliance with our commitments.”

Where the company’s infrastructure is at risk due to new developments is another critical element for Looker. Reinders points out, “With StackRox, we are notified right away where we can take action.”

He goes on to explain that Looker’s philosophy is to use the services embedded in the infrastructure, either in the software Looker runs or the cloud services they use, regardless of the cloud vendor. “We don’t want more variables,” he asserts. “We want to leverage what already exists rather than complicating things by adding more components. The Kubernetes-native architecture of StackRox enables us to do that.”

Leveraging StackRox Capabilities

- Visibility and Control – StackRox finds and secures all running containers, so Looker can track its deployments and protect its data platform.
- Vulnerability Management – StackRox identifies vulnerabilities in Looker’s images and running deployments.
- Compliance – Looker taps StackRox to immediately identify those rare instances that fail to meet Looker’s internal policies or industry standards.
- Network Segmentation – StackRox recommends network policies that reduce the attack surface and generates updated YAML files for Kubernetes to apply.

StackRox

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native start- ups Global 2000 enterprises, and government agencies.

LET’S GET STARTED

Request a demo today!
info@stackrox.com
+1 (650) 489-6769
www.stackrox.com