sumo logic

Monitor and secure 10,000 clouds

Results at a glance

- → Efficient, scalable security monitoring for 10,000 clouds and growing
- → Gained broad security visibility across three cloud environments
- → Accelerated security investigations with automated workflows
- → Optimized incident response decision-making using custom dashboards
- → Improved team productivity and focus

HashiCorp

SUMO LOGIC PRODUCTS

Infrastructure Monitoring

Logs for Security

Cloud SIEM

USE CASE

Security Operations

Multi-cloud Monitoring

s u
mo

Challenge

Collectively supporting cloud infrastructure for tens of thousands of customers and HashiCorp itself generates massive volumes of various events.

Sifting through this telemetry to conduct a single security investigation and search on a series of related events was a time-consuming process for the security team, plagued with excruciatingly slow search results.

"Our sheer mass of data made everything slow. From collecting all the events we needed to gaining context around alerts and seeing what was going on, we couldn't investigate in real time to understand if something was relevant or find things that are critically important," said Ryan Breed, Senior Security Engineer at HashiCorp, noting that "running a large search took so long that it would break an analyst's concentration and slow down the investigation process."

Solution

HashiCorp, known for its innovation that never sleeps, requires security that can keep up. For that, they selected Sumo Logic.

Unlocking security visibility for HashiCorp required real-time monitoring across the company's complex operating environment, which spans three infrastructure-as-a-service (IaaS) cloud environments and API integrations with each cloud vendor's full suite of products.

As a cloud-native solution, Sumo Logic provides Hashicorp with centralized and scalable Cloud Security Analytics and security information and event management (Cloud SIEM) across the company's and its customers' multi-cloud environments.

HashiCorp

INDUSTRY

Cloud computing infrastructure services

ABOUT

HashiCorp's suite of multi-cloud infrastructure automation products underpin the most important applications for the largest enterprises in the world, supporting thousands of customers. They have open source and commercial offerings for HashiCorp Terraform, Vault, Consul, Nomad, and also maintain open source projects for HashiCorp Vagrant, Packer, Boundary, and Waypoint. Their open source products are downloaded by IT practitioners more than 100 million times a year.

"Sumo Logic helps us scale our security visibility and keep pace with the business as we launch new products, add customers and adopt new tools. As we grow, the marginal cost of adding visibility and enhancing what we have is minimal, which allows us to accommodate some pretty fundamental changes and scale the business much more quickly."

HashiCorp

Ryan Breed
Senior Security Engineer

Results

Low latency, insight-driven security investigations — in real time

After deploying Sumo Logic Cloud SIEM to integrate and ingest telemetry from all aspects of the company's infrastructure, HashiCorp experienced the first game changer for managing security investigations: the ability to do low-latency search.

Sumo Logic's cloud scale empowers HashiCorp security experts to search and conduct investigations in real time. In addition, Cloud SIEM streamlined workflows enabled the security operations center (SOC) team to implement a system where alerts automatically initiate searches.

"Sumo Logic proactively helps us understand an alert, whether it's important or not and, in some cases, automatically disposes of the alert," said Breed, adding that "having a low latency search system with Sumo Logic makes that kind of real-time workflow automation possible."

Applies Alerting and Detection Strategy (ADS) to optimize security investigations

Cloud SIEM parses, maps and creates normalized records upon ingestion from HashiCorp's structured and unstructured data and then automatically triages alerts to provide the security experts with actionable insights. To further optimize Cloud SIEM's performance in distilling down tens of thousands of daily alerts, the SOC team applies Palantir's ADS framework.

The framework helps the security team develop theories and think deeply about how best to leverage Cloud SIEM during investigations. For example, the team has mapped out threat-hunting searches to uncover traces a threat actor might leave on the infrastructure and workflows to support the next steps the analyst should take if they find one of those traces.

"Leveraging ADS lets us really focus on the performance side of using Cloud SIEM. Having an idea of what we're looking for before we go looking helps us optimize things like field extractions and making the most common search patterns return very quickly. This helps the analyst stay in the zone when an investigation has multiple layers of abstraction and Cloud SIEM has made all of that supporting information available up front," said Breed.

Reduced time-to-decision with interactive dashboards

Sumo Logic's security analytics and dashboards provide the security team with single-pane-of-glass visibility across HashiCorp's extensive cloud environments. The SOC has also implemented a range of custom dashboards to advance the team's playbooks and processes for conducting daily investigations.

When an analyst is investigating suspicious login activity, for example, they can fill in important parameters into the dashboard, such as the user ID and a time range, which then returns an interactive heads-up display where the analyst can 'click' to drill further into specific data.

"Interactive dashboards give us the context and color that help our security analysts minimize the time-to-decision. They can plug in the parameters and get the information very quickly, so they don't have to stop whatever they're doing to reach a decision and take action," said Breed.

Learn more

Monitoring 10,000 clouds with HashiCorp

WATCH THE FULL SESSION

305 Main Street, Redwood City, CA 94603

Learn More

Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700

sumologic.com