sumo logic

Faster incident detection and response with Cloud SIEM

Results at a glance

- → 22% faster threat detection and response with a modern SIEM solution
- → 30% increase in proactive issue identification and resolution
- → Improved support and engineering team efficiency with playbooks and custom rules for automated alert triage
- → Increased operational efficiencies with resource management insights

SINGLETRACK

PRODUCTS

Cloud SIEM

Sumo Logic Platform

USE CASES

DevSecOps

Threat Detection Investigation and Response

SINGLETRACK

Challenge

Singletrack needed to replace its homegrown security and log management solutions

At the time of its founding, Singletrack had to custom-build its cloud-native security monitoring solution using Papertrail on top of AWS and Salesforce technology stacks. Visibility across apps and systems was limited, and workflows required navigating through multiple screens.

As Singletrack grew its business, adding dedicated support and engineering teams, their homegrown security solution became increasingly difficult to manage. Every time they wanted to improve their solution, it would be a project to determine how to refactor or rebuild it. For new employees, it wasn't always clear how to address incoming alerts and log messages. Singletrack needed a modern security information event management (SIEM) solution that could scale.

Singletrack's Co-founder and CTO Paul Dyson explains "Techie people like me prefer competent products more than just something that demos well. I'm good at spotting the difference between something that looks great in a demo but can be difficult to use vs truly comprehensive technology."

Solution

Singletrack evaluated eight different platforms, including Splunk and Sumo Logic, in their search for a comprehensive out-of-the-box SIEM solution.

INDUSTRY

Financial Services

ABOUT

Founded in 2009, Singletrack delivers mission critical client engagement tools & analytics for Capital Markets firms.

The company's mission critical platform enables Investment Banks and Independent Research Providers to enhance client relationships, distribute research and analysis, deliver corporate access services and manage deals in ways that grow revenue and reduce costs.

WEBSITE

www.singletrack.com

> We evaluated Splunk, but it looked like we'd have to do as much work doing the integration and setting Splunk up as we had done building our own solution.

Paul Dyson
CTO and co-founder
Singletrack

After an evaluation process that included receiving a one-on-one product demo, Singletrack found Sumo Logic to be the right fit for the following reasons:

Usability and simplicity

Sumo Logic centralizes logs, events, metrics, and traces for a unified view of Singletrack's apps and systems. Its streamlined user interface makes it easy to onboard new employees and quickly learn how to use the platform.

Extensibility with integrations

Enabling other teams such as Support and CS to pro-actively identify and address issues before they impact the business of our clients.

Actionable insights

Sumo Logic's Cloud SIEM allows Singletrack to add context to security alerts with integrated threat intelligence, including details of a log record that triggered a signal.

Flexible pricing

Price is always a consideration and Singletrack needed a solution that would not only replace the homegrown solution, but also work within the team budgets and allow for flexibility as the company grows.

"It's been a while since I last worked with a technology company and thought, 'Wow, these guys really know what they're doing,' and Sumo Logic is very, very easy to work with."

Onboarding with Sumo Logic was steady and uncomplicated for Dyson and his team. He explains, "We were very busy with maintaining day-to-day operations, so it took us three months end-to-end, but frankly, we could have done it in one month."

Results

Faster incident investigation and response

Dyson oversees a 30 to 40-person team comprised of software engineers, customer support, and SecOps—building and maintaining the cloud-based product, managing all the customer environments and integration points, and handling customer requests for help. This variety of roles and responsibilities shares a common commitment to security, anchored by the team's focus on cloud-native SIEM.

Singletrack uses Sumo Logic's Cloud SIEM solution as the cornerstone of its SecOps, with a centralized view of its apps and systems that powers a monthly security review process. Covering everything from role-based access controls and resource allocations to SecOps policy reviews, Dyson says, "It's a good focal point for assessing how things are looking in general, which wasn't possible with our homegrown solution."

With Cloud SIEM, Singletrack can run automated playbooks and predefined remediation actions to respond to a given event or incident type, choosing from the 900+ out-of-the-box integrations and playbooks — or write their own. Dyson shares, "We love the playbook stuff because it removes the risk around, 'does the person who sees the alert really understand what's going on?'"

CUSTOMER EXPERIENCE

We love the playbook stuff because it removes the risk around whether the person who sees the alert really understands what's going on.

Paul Dyson
CTO and co-founder
Singletrack

Easy access to structured and unstructured data

As a log analytics solution, Sumo Logic brings Singletrack another added advantage: Log mapping and normalization. Log messages from different sources use various names to identify users, applications, devices, and so on. The normalization process allows Singletrack to apply the same Cloud SIEM rule to all records, regardless of the message source.

Dyson explains, "You can do a much more structured query and text search, which is immensely helpful in getting to what you need quicker, especially since I can just send a URL via Slack to the engineer to ask if they can have a quick look at it."

Robust log queries of all datasets, a rich operator library, and easy-to-use search templates to quickly filter real-time insights and results accelerate threat detection and troubleshooting performance issues for Singletrack.

"We've been able to improve first response times, because we're already aware there may be a problem, from 85% to 93% and improve our second response times, because we can more quickly and easily diagnose, from 68% to 83%," he says.

Faster customer support

Prior to using Sumo Logic, when customers reported an issue to Singletrack, Dyson's team would need to spin up an exploratory project to determine how to monitor and alert for it. This process, which would typically take as long as two weeks, is now "something we can do in real time," says Dyson.

This accelerated feedback loop between customers reporting an issue and the support team creating rules to detect that issue happens within the same support ticket for a more efficient process.

BY THE NUMBERS

22%
improvement in response time

2 weeks → seconds
accelerated feedback loop

Proactive application monitoring

On an annual basis, Singletrack executes 100,000 mission-critical research distributions to around 250 million paying clients, amounting to 15GB of pure application data a day. Sumo Logic's Log Analytics Platform provides a conduit to unify data from disparate apps and systems into a single source of truth.

Using the unique search query language allows for faster root cause analysis. "It's very easy to navigate from alerts through to the underlying log messages and then filter those and search them again, even as we're collecting gigabytes of logs a day," explains Dyson before adding, "And then the alerts are very well integrated into the things that actually alert our people like Slack and PagerDuty."

This enhanced application observability has seen Singletrack increase its proactive handling of issues by 30 percent.

With Sumo Logic, Singletrack is saving significant time previously spent maintaining its homegrown solution, allowing Dyson and his team to focus on value-driven work.

"I genuinely can't think of another infrastructure project I've done that was quite so straightforward as this with the results as impressive as working with Sumo Logic," says Dyson.

BY THE NUMBERS

15GB
daily application data ingest

30%↑
Proactive issue handling

CUSTOMER EXPERIENCE

I genuinely can't think of another infrastructure project I've done that was quite so straightforward as this with the results as impressive as working with Sumo Logic.

Paul Dyson
CTO and co-founder
Singletrack

Read more about other customer successes — from retail to healthcare to fintech here.

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

sumologic.com

855 Main Street, Redwood City, CA 94603