sumo logic

Transforming DevSecOps visibility, time and efficiency in fintech

Results at a glance

- → Gained flexible platform that's easily extensible to plug in new tools
- → Streamlined onboarding reduced the time it takes to get crucial security insights by 95%
- → Enabled scalable data analysis that ingests 686GB per day
- → Reduced time to gather reports for compliance audits by 80%
- → Gained visibility to monitor and troubleshoot application performance
- → Saved >1,000 hours per year in troubleshooting platform issues

TRUELAYER

SUMO LOGIC SOLUTIONS

Cloud SIEM

Application Performance Monitoring (APM)

Audit and Compliance

Logs for Troubleshooting and Monitoring

USE CASES

Threat detection, investigation and response (TDIR)

Threat hunting

Regulatory compliance and audit readiness

Logs for incident response

Engineering efficiency with AI

Challenge

TrueLayer needed a more scalable and efficient SIEM solution for managing their security operations.

To manage security operations (SecOps) across both cloud and on-premises infrastructure, TrueLayer initially adopted a mix of open-source solutions. The tool sets were initially helpful in centralizing logs for querying, alerting, and automating response actions; however, despite diligent efforts, the approach led to a constant firefighting mode.

As Bruno Braga, SecOps Lead and Engineer at TrueLayer observed, “We quickly assessed that our open source approach just did not scale. The problem was that we built a security pipeline, but we were spending most of the time engineering solutions to issues with the technology rather than resolving alerts.”

Solution

In their pursuit of a robust cloud-native solution, TrueLayer evaluated both Splunk and Sumo Logic. Their objective was to find a SIEM solution that would seamlessly integrate with their AWS and Kubernetes environments while offering flexibility to support their custom playbooks.

After a thorough hands-on trial, Sumo Logic emerged as the preferred choice for the following reasons:

Usability and simplicity

Sumo Logic’s intuitive user interface and ease of navigation proved a perfect fit to facilitate the team’s smooth adoption and operation of the platform.

TRUELAYER

INDUSTRY

Finance

ABOUT

With its headquarters in the U.K., TrueLayer is Europe’s leading open banking payment network. The company’s platform powers smarter, safer, and faster online payments by combining real-time bank payments with financial and identity data. Businesses big and small use TrueLayer to onboard new users, accept money, and make payouts in seconds and at scale.

WEBSITE

truelayer.com

Extensibility with APIs

Given TrueLayer's use of automation, Sumo Logic's extensive support for APIs provided the desired flexibility the SecOps team needed to integrate with existing tools and workflows.

Cost-effectiveness

Sumo Logic's pricing structure offered a significant advantage over Splunk, aligning with TrueLayer's budgetary considerations without compromising on functionality or performance.

Results

Delivering granular security insights with power and ease

TrueLayer seamlessly integrated the Sumo Logic platform into their environment, encompassing in-house tooling, threat intelligence feeds, the company's core fintech system, and various external resources. This integration has empowered TrueLayer with advanced security analytics capabilities, efficiently collecting data from log files and event streams. Sumo Logic's scalability easily supports TrueLayer's data volumes with the platform adeptly ingesting and analyzing almost 700 GBs of data daily.

Sumo Logic's streamlined onboarding was a critical step for the team to obtain security alerts and conduct threat hunting activities. Getting crucial security insights went from 40 hours to two hours, a 95% improvement. Reflecting on the transition, Braga remarked, "With Sumo Logic, our security team gained visibility within hours or minutes, compared to the previous process that took several weeks to make log sources usable with our existing stack."

BY THE NUMBERS

700GB
of data ingested and analyzed daily

95%
improvement in getting crucial security insights

CUSTOMER EXPERIENCE

With Sumo Logic, our security team gained visibility within hours or minutes, compared to the previous process that took several weeks to make log sources usable with our existing stack.

Bruno Braga
SecOps Lead and Engineer
TrueLayer

Sumo Logic's SIEM functionality further bolsters TrueLayer's security efforts by providing a comprehensive view of normal and abnormal activities specific to the company. For instance, TrueLayer depends on Sumo Logic to normalize user behavior and automatically search for high-risk activity.

"We rely on Sumo Logic's scheduled searches to actively monitor for IOCs during incidents. This lets us focus on addressing ongoing incidents while staying on top of any emerging threats. With Sumo Logic, we can effectively manage incidents and be vigilant for potential additional threats," explained Braga.

Many organizations assess the "build vs buy" approach. By shifting from their custom-built open source solution over to Sumo Logic, the TrueLayer team saved approximately 1,040 hours annually spent on troubleshooting issues with their platform.

BY THE NUMBERS

~1,040 hrs

saved annually on troubleshooting issues

Streamlining compliance audits with turnkey reports

As a leading open banking payment platform, TrueLayer must adhere to a myriad of compliance requirements inherent to the financial services industry. Sumo Logic plays an integral role in helping TrueLayer meet the necessary regulatory standards and pass their annual compliance audits.

According to Braga, "We rely on Sumo Logic to generate reports and dashboards tailored for regulators as a routine aspect of our audit processes. The out-of-the-box reports, coupled with its intuitive customization features, enable us to swiftly and efficiently demonstrate our high security standards to auditors."

Using Sumo Logic's automation capabilities, TrueLayer could take that a step further. The team developed detailed, automated reports to help identify compliance gaps ensuring they are able to maintain consistent compliance standards and reduce risk to the business.

Additionally, Sumo Logic's centralized log analysis serves a broader range of company operations beyond compliance checks.

With Sumo Logic providing us with a single source of truth for our data, other stakeholders in the company rely on the solution's reporting of organization-wide metrics to glean valuable business insights and inform decision-making.

Bruno Braga
SecOps Lead and Engineer
TrueLayer

Elevating customer experience through application observability

With the security team's triumph in leveraging Sumo Logic's SIEM capabilities, TrueLayer's DevOps team has eagerly embraced the platform to enhance observability insights into the company's software solution. Now equipped with Sumo Logic, the development team can promptly pinpoint which service is impacted when deviations from expected performance occur.

Braga shared, "Using Sumo Logic, our development team can swiftly analyze what's happening when something isn't working as expected within the TrueLayer platform. Sumo Logic helps the team explore the issue and go from troubleshooting to fixing—fast."

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