sumo logic

# Fintech compliance made fast and secure

## Results at a glance

- → Reduced time-to-detect and time-to-respond by 80%
- → Saved analysts two hours per security investigation
- → Reduced time to gather compliance audit logs from one month to one day
- → Helped enable financial audit and PCI DSS certification process
- → Gained unified platform for business-wide data analytics use cases


**SUMO LOGIC SOLUTION**

Cloud SIEM

**USE CASE**

Threat detection and investigation

Audit and compliance

## Challenge

When adopting a SIEM solution, OpenPayd needed a robust platform that would eliminate pivots across tools, streamline investigations, and support compliance requirements.

As a regulated entity embarking on its security journey, OpenPayd needed a centralized log management solution that would collectively monitor the company's growing data volumes across a sprawl of individual tools. "Managing multiple platforms and reviewing numerous dashboards became increasingly complex for our security team. From a security standpoint, we needed centralized collection and analysis that would make it easier and more efficient to keep track of everything in one place," explained Jordan Andonov, Security Engineer at OpenPayd.

In addition to the security and compliance requirements, OpenPayd wanted the solution to provide application monitoring for the company's Banking-as-a-Service (BaaS) platform. The security engineers are an independent team from the platform engineers, so OpenPayd's ideal solution needed to allow the company to apply the separation of duties principle to its fullest extent. This was important for monitoring privileged access across the environment.

## Solution

OpenPayd adopted Sumo Logic because of its comprehensive security information and event management (SIEM) and log analytics capabilities that provided a unified approach for the company's security and application monitoring use cases. Sumo Logic stood out in the vendor evaluation with its ability to simplify workflows, enhance threat visibility, and streamline security operations for the small security team.

OpenPayd

**INDUSTRY**

Finance

**ABOUT**

OpenPayd, a leading embedded finance and Banking-as-a-Service (BaaS) provider, delivers a suite of banking and payments infrastructure services for digital businesses across the UK, Europe and North America — all via an API-integrated platform.

OpenPayd's top reasons for choosing Sumo Logic included:

- **Streamlined APIs** that minimized the time and effort to integrate with the company's various cloud-based log data sources.
- **Cloud-native solution** that provided scalability and flexibility.
- **User-friendly interface** that made it easy to navigate and utilize its features without extensive training or support.
- **Customer support** with access to responsive and knowledgeable staff.
- **Pricing** that offered a cost-effective solution and delivered the necessary value and features

## Results

### Efficient data collection to meet compliance requirements

OpenPayd rapidly unlocked the power of Sumo Logic's log monitoring with out-of-the-box integrations that made it a breeze to ingest 10GB of data per day from the company's Microsoft Azure environment and other applications. "Leveraging an efficient data ingest volume, Sumo Logic helps us fully meet our regulatory requirements and maintain comprehensive monitoring of our infrastructure and environment. It showcases our effective data utilization strategies, leveraging insights from every piece of information we collect," shared Andonov.

**BY THE NUMBERS**

**10GB**
**of data monitored per day**

**CUSTOMER EXPERIENCE**

**Leveraging an efficient data ingest volume, Sumo Logic helps us fully meet our regulatory requirements and maintain comprehensive monitoring of our infrastructure and environment.**

**Jordan Andonov**
Security Engineer
OpenPayd

Sumo Logic played a crucial role in helping OpenPayd meet the necessary regulatory standards and pass its annual compliance audit. Additionally, Sumo Logic significantly reduced the time and effort required for OpenPayd's auditing processes. What used to take two people two weeks to gather audit logs, Sumo Logic makes possible in a single day.

**"Sumo Logic made a notable contribution during our financial audit and PCI DSS certification process. During the onsite audit, we showcased our Sumo Logic setup to the auditors, demonstrating how we use the platform. The auditors were impressed with what they saw, and we successfully fulfilled all the logging and privileged access monitoring requirements for a level two managed service provider," Andonov shared.**

**BY THE NUMBERS**

**1 month of audit process work**

↓

**1 day**

—

**2 hours saved**

**per threat investigation**

## Empowering the SOC team's security insights and investigations

Sumo Logic accelerates alert triage and investigations, saving the security team two hours per investigation. Once the aggregated risk analysis from the company's various data sources, such as GitLab, Azure, and their EDR solution, surpasses a threshold, Sumo Logic automatically generates an insight, enabling the team to focus on the threats that matter most.

On a typical day, the security team receives ten insight alerts that are routed directly to a high-priority Slack channel. The real-time notifications enable the team to quickly assess the threat and, if necessary, investigate further using Sumo Logic dashboards.

As Marin Mitrev, Security Engineer at OpenPayd, explains, “We used to have 30 tabs open just to do a single investigation. Sumo Logic lets us eliminate those tool pivots and gives us a good overview of our security in one place.” Highlighting a success story, Mitrev adds that “our security team has a single view into login attempts across our applications and infrastructure, so we can rapidly identify suspicious activity like a brute-force attack.”

Sumo Logic’s broad security visibility and fast investigation workflows helped OpenPayd advance its security posture and mature its security operations. As a result, the security team decreased the company’s MTTR and MTTD by 80%.

On a personal level, Andonov adds that “Sumo Logic has made my life much easier. It saves me a significant amount of time and allows our team to streamline daily tasks. This gives us the opportunity to focus on new integrations and enhance our overall security posture. As a security engineer, it’s important to constantly improve and work on new things, and Sumo Logic has been a game changer in that regard.”

**CUSTOMER EXPERIENCE**

**We used to have 30 tabs open just to do a single investigation. Sumo Logic lets us eliminate those tool pivots and gives us a good overview of our security in one place.**

**Jordan Andonov**
Security Engineer
OpenPayd

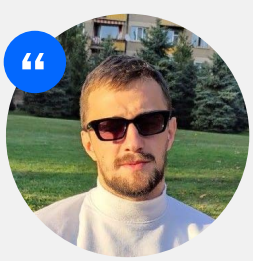
**BY THE NUMBERS**

**80%**
**decrease in MTTR and MTTD**

## Looking ahead: adding more users and use cases

Choosing Sumo Logic has been a success for OpenPayd's security team. With Sumo Logic ingesting logs from across the business infrastructure, OpenPayd gained a unified platform that allows it to support data analysis needs for other user groups beyond security. Next up, the DevOps team will start using Sumo Logic to monitor OpenPayd's product platform.

"Sumo Logic provides extensive value across our business because we can use the data analysis and dashboards to visualize everything we want across our operational processes. Beyond meeting our current security and compliance needs, we can easily spin up new users like our development and technical support teams. Sumo Logic comes in handy to do all of that," said Mitrev.



**I would recommend Sumo Logic to everyone. It's easy to use. It's fast. It's reliable. And it's perfect.**

**Jordan Andonov | Security Engineer | OpenPayd**

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