graylog

How a U.S. Telecom Provider Uses Graylog Cloud to Correlate API Activity and Spot Threats Faster

OVERVIEW

For this U.S.-based telecom company, APIs drive everything from customer self-service platforms to backend automation. But while API adoption was accelerating, visibility into that activity wasn't keeping up. The team wanted a way to ingest API logs, correlate them with other system activity, and proactively monitor for abuse without deploying additional infrastructure or committing to heavyweight tooling. Their answer: Graylog Cloud, hosted on AWS, configured to ingest API call data directly into the platform for flexible, real-time monitoring.

COMPANY SNAPSHOT

Industry: Telecommunications

Headquarters: United States

Company Size: $50M–$250M

Focus Areas:API Monitoring, Compliance, Business Agility, Risk Management

Products Used: Graylog Cloud (AWS)

> **"Using Graylog for API protection and security event logging has been effective. It gives us a centralized, searchable view of all API traffic—helping engineering and security teams detect anomalies and respond faster."**
>
> **— Product Support Lead, U.S. Telecom Provider**

THE CHALLENGE: Incomplete Visibility, Manual Correlation

The company's security and engineering teams needed better visibility into API usage patterns, especially as their attack surface expanded. However, legacy logging tools lacked centralized access, and the process of connecting API logs to broader infrastructure events was fragmented. **Key goals included:**

- Centralizing logs from APIs and infrastructure in one platform
- Building custom dashboards to track usage, anomalies, and edge cases
- Flagging suspicious behavior across correlated data sources
- Improving compliance and reducing response times

While exploring options like Equixly and Operant, the team ultimately chose Graylog for its balance of flexibility, scalability, and cost-efficiency.

WHY THEY CHOSE GRAYLOG

With Graylog Cloud, the team could set up tailored log ingestion pipelines for their API data, ingesting only what mattered and correlating it alongside existing logs from infrastructure, user activity, and third-party tools.

Highlights:

API Log Ingestion at Scale: By configuring inputs specifically for API call data, the team built selective pipelines that captured the most relevant events for analysis.

Flexible Correlation Across Sources: Graylog's stream and alerting engine allowed engineers to connect API activity with related logs, like authentication events, error rates, or abnormal traffic patterns.

Cloud-Native Scalability on AWS: With AWS as the backbone, Graylog Cloud provided an elastic, managed environment ideal for a lean IT team focused on insights, not maintenance.

Custom Dashboards for the Real World: While no prebuilt views existed for API traffic, Graylog's dashboard tools enabled the team to create purpose-built visualizations for internal stakeholders, giving each team the needed insights.

Real-World Results

CENTRALIZED API VISIBILITY

- API logs are no longer siloed; teams can search, alert, and report from one place.
- Security and engineering teams collaborate from a shared, real-time view.

FASTER INCIDENT TRIAGE

- Correlation across data streams helps quickly identify root causes of performance or security issues.
- Real-time search and alerts cut down investigation time dramatically.

CUSTOM INSIGHTS, BUILT TO FIT

- Although the platform didn't come with prebuilt dashboards for API monitoring, Graylog's flexible UI made building the right views for their environment easy.

LIGHTWEIGHT, CLOUD-FIRST DEPLOYMENT

- No infrastructure overhead. Graylog Cloud delivers high availability and performance with minimal IT burden.

A PLATFORM THAT GROWS WITH YOU

This telecom provider didn't need a turnkey API monitoring product, they needed a flexible platform they could shape to fit their needs. With Graylog Cloud, they ingest the data that matters, correlate it meaningfully, and turn insights into action.

READY TO BUILD YOUR OWN API MONITORING STRATEGY?

Graylog Cloud provides the performance, flexibility, and scale needed to make sense of API traffic on your terms. With customizable log ingestion, powerful correlation, and a fully managed AWS architecture, it's the smarter way to stay ahead of threats without overcomplicating your stack.

[Explore Graylog Cloud >]

"Graylog gives us the building blocks we need. It's not a rigid box—it's a platform we can shape around our environment to protect what matters."