From Budget Constraints to Cloud Scale

How Kennedy Krieger Institute Strengthened Security with Graylog Cloud

COMPANY SNAPSHOT

Industry: Healthcare

Headquarters: Baltimore, Maryland

Company Size: 2500+ employees

Core Mission:

Neurology, rehabilitative care, developmental services, education, and research

Solutions Used:

AWS, Graylog Cloud Onboarding Services

Primary Stakeholders:

Director of Cybersecurity, Network Security Engineer, Cybersecurity Analyst

Partner: GuidePoint Security

OVERVIEW

Kennedy Krieger Institute (KKI) supports tens of thousands of patients every year across inpatient programs, outpatient clinics, home and community services, and research initiatives. With a lean IT and Security team safeguarding sensitive clinical and operational data, KKI needed a logging and SIEM platform that was powerful, cloud ready, and simple to operate.

The team had a strict budget ceiling, an evolving hybrid environment, and a mandate to retain logging data long enough to meet compliance expectations without drowning the small SOC in maintenance work.

After evaluating multiple competitors, including Splunk, Sentinel, QRadar, CrowdStrike SIEM, and Devo, the Institute selected Graylog Cloud for its predictable cost model, faster onboarding, analyst friendly workflows, and ability to support a stronger security posture without extra headcount.

GuidePoint Security worked alongside KKI and Graylog to validate scale, build confidence, and ensure smooth adoption.

THE CHALLENGE

KKI faced several pressure points at once:

Long term logging retention without runaway cost

The team needed to maintain security logs for audit and compliance needs while keeping total cost of ownership predictable.

A lean IT and Security team

With limited staff, the solution had to be easy to deploy, easy to manage, and easy for analysts of all skill levels to use daily.

Desire to move SIEM operations into the cloud

KKI wanted a cloud forward platform that lowered infrastructure overhead and could scale without complexity.

Faster and more confident investigations

Analysts needed the ability to identify, prioritize, and respond to real incidents with less noise and fewer manual steps.

Strict purchasing constraints

Any solution had to fit within the Institute's budget cap without sacrificing visibility or response capability.

THE SOLUTION

Graylog Cloud on AWS for Scalable Logging and Stronger Analyst Experience

KKI deployed Graylog Cloud hosted on AWS at 200GB per day with Security Cloud Onboarding Services, giving the team instant access to a modern SIEM experience without maintaining infrastructure or building custom pipelines.

Intelligent Data Control

Aligned with Graylog's No Compromise Data Retention value hook, KKI can retain the logs they need while keeping cost predictable and usage right sized. Hot data stays fast for investigations while bulk archives shift to lower cost storage as needed.

Intuitive Analyst Experience

Built in shortcuts, guided searches, right click actions, and clean normalized data keep analysts in a single screen. This reduces clicks, cuts triage time, and minimizes fatigue for a small SOC that cannot afford inefficient workflows.

Context Aware Incident Response

KKI analysts now have fused alerts, context, and guided response steps in one place, enabling quicker decisions and more confident actions, even during higher volume days.

Rapid Value Delivery

With onboarding support and prebuilt content, KKI reached useful visibility fast. No complex tuning, no multi month rollout, and no hidden setup tasks. New cloud sources and services can be added without creating new work for the already busy team.

Cloud Forward Deployment

Running in AWS gives KKI a scalable, low maintenance footprint that removes infrastructure overhead and ensures resilience for future expansion.

WHY THEY CHOSE GRAYLOG

KKI selected Graylog Cloud because it delivered on four priorities that mattered most:

1. Ease of use for a small team
Graylog demonstrated simple deployment, intuitive operations, and no steep training curve. Analysts could get value immediately instead of wrestling with misaligned dashboards or complicated pipelines.

2. Better pricing with no surprise costs
KKI compared multiple vendors and found Graylog offered stronger value with clearer control of licensing and storage usage. Predictability mattered more than anything.

3. Stronger technology fit for healthcare SOC workflows
Graylog's detection content, context driven views, and faster triage workflow aligned well with the Institute's needs and resource constraints.

4. Confirmed scale and performance through third party validation
External testing exceeded KKI's requirements, giving leadership confidence that Graylog could handle growth and future cloud expansion.

Partner Value

GuidePoint Security played a key role in the success of the project:

ACCESS AND ALIGNMENT ACROSS KKI TEAMS

GuidePoint's longstanding relationships helped connect cybersecurity, infrastructure, and compliance stakeholders early in the buying and validation cycle.

DEEP UNDERSTANDING OF KKI'S ENVIRONMENT

The partner guided critical conversations between Graylog and KKI, helping each side understand internal processes, expectations, and constraints.

COLLABORATIVE SUPPORT MODEL

GuidePoint, Graylog sales, and Graylog technical teams worked as a unified front to build trust and move quickly.

Special recognition goes to Julia Riemer and Matt Casey (GuidePoint) and John O'Connor and Joel Duffield (Graylog) for enabling a smooth evaluation and deployment path.

RESULTS

KKI now benefits from:

- **Predictable and scalable cloud based SIEM operations**
  No more infrastructure overhead or fear of escalating storage costs.
- **Faster investigations with less analyst fatigue**
  Context rich workflows let analysts spot and act on real threats quickly.
- **Simple onboarding of new log sources**
  No more time consuming mini projects to add critical cloud or network logs.
- **A platform that fits under budget without reducing visibility**
  KKI gains stronger threat detection and retention flexibility while staying within financial constraints.
- **A solution built for healthcare grade security expectations**
  Audit readiness, long term log access, and efficient workflows support both clinical and operational requirements.

ABOUT GRAYLOG

Graylog is the AI powered SIEM and centralized log management platform that helps security and IT teams detect threats faster, investigate smarter, and control data costs without compromise. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.