graylog

Redefining SIEM: Affordable, Effective Security for AWS Workloads

The Hidden Costs of Legacy SIEM

Security teams working in AWS environments often encounter unnecessary complexity and cost when relying on traditional SIEM platforms. These legacy tools typically require dedicated infrastructure teams, long deployment cycles, complex tuning, and rigid licensing models tied to unpredictable data volumes. The result is a slower path to operational value and reduced agility for fast-moving cloud security teams.

Graylog Security, an AWS Global Startup Program participant, offers a streamlined, cloud-aware SIEM platform designed to reduce complexity and cost. Built with an understanding of AWS-native services, Graylog delivers the essential capabilities security teams rely on without requiring extensive manual setup or expensive license commitments. From fast onboarding to operational efficiency and flexible deployment, Graylog is helping modern security teams secure AWS workloads without compromise.

AWS-Specific Capabilities and Integrations

Graylog is designed for operating within and securing AWS workloads. It offers out-of-the-box integration with a broad range of AWS-native services, including:

Security and Identity Services:

- AWS CloudTrail
- Amazon GuardDuty
- IAM Identity Center
- AWS Inspector
- AWS Macie
- AWS Security Hub
- AWS Security Lake
- AWS WAF and Shield
- AWS Firewall Manager

Compute and Container Services:

- EC2 (via optional agent for OS and application logs)
- AWS Fargate
- AWS Lambda
- AWS Lightsail
- Amazon EKS

Networking and Storage:

- Amazon VPC
- Route 53
- Amazon S3
- S3 Glacier

Management and Monitoring:

- AWS Config
- AWS Health

This direct integration enables automated event collection, data enrichment, and security analytics tailored for cloud workloads. With version 7.0, Graylog supports selective data ingestion from AWS Security Data Lake. This helps customers reduce data duplication, manage transfer costs, and streamline investigations.

The platform ensures only actively used data is applied to a customer's Graylog instance through filtered inputs, data preview, and selective retrieval. The result is a cost-efficient and scalable detection and response process purpose-built for AWS environments.

Graylog is available through the AWS Marketplace for streamlined deployment.

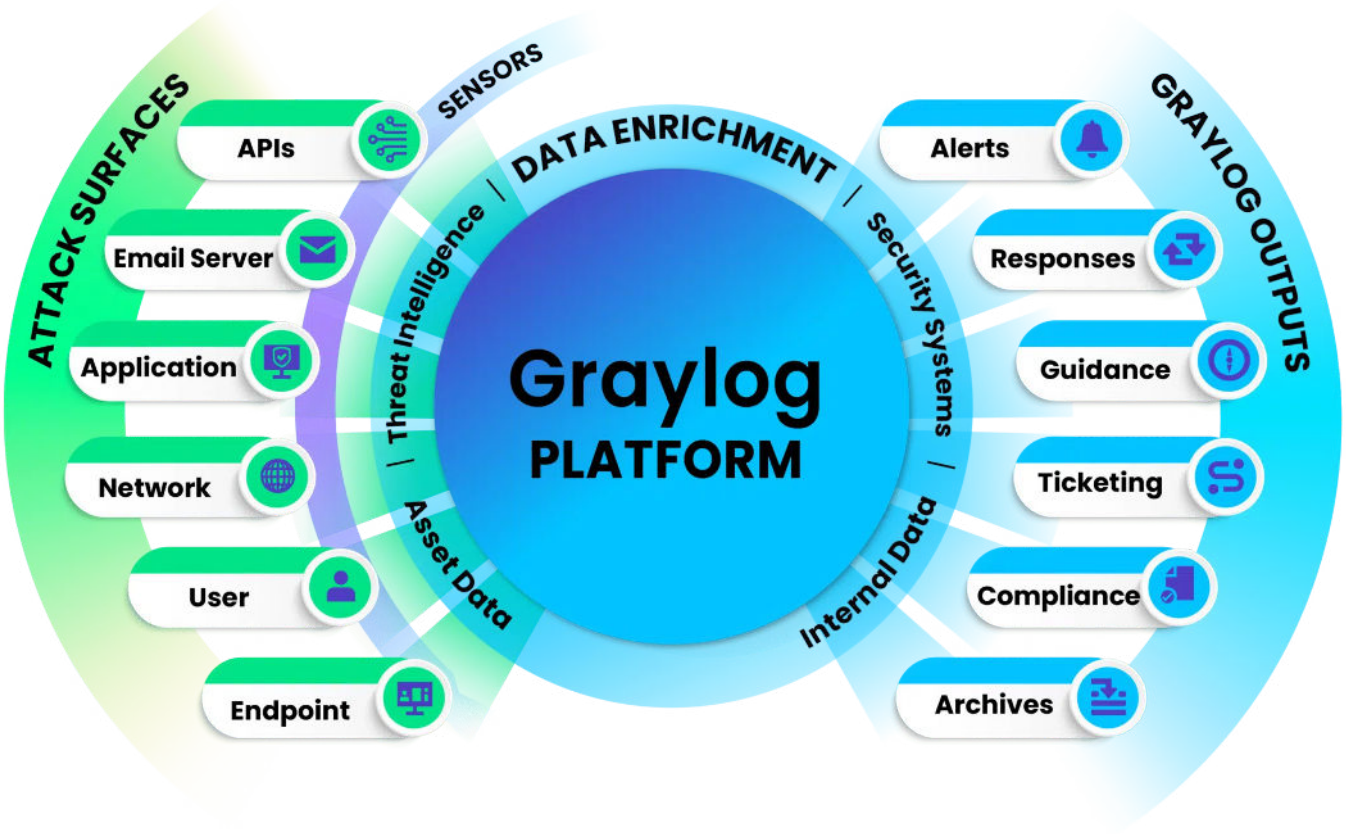
Graylog was built to enhance the experience of security analysts and SOC managers by removing operational bottlenecks. It surfaces relevant signals without overwhelming analysts with noise, allowing them to investigate and respond more quickly.

Value for Security Analysts and SOC Teams

The platform offers recommended threat detection content and built-in response workflows that reduce administrative overhead and support faster decision-making. When something unusual happens, such as a change to an IAM role or an unexpected network activity, Graylog delivers enriched alerts with full log trails, correlated data, and guidance for next steps, including dynamic recommendations from AI analysis.

According to internal subject matter experts, customers may choose to dedicate team members specifically to operating the platform for activities such as threat analysis and identifying areas of weak security posture.

At the same time, the solution is not dependent on a large infrastructure team to deploy or maintain. This enables security teams to operate more effectively in hybrid environments, especially for mid-enterprise organizations balancing on-premise and cloud workloads.



Transparent Pricing and Deployment Flexibility

Graylog's pricing model is designed to provide clarity, flexibility, and alignment with the value delivered. Traditional ingest-based licensing models require organizations to commit to their highest expected data usage, which can lead to overpaying for infrequent usage spikes.

Graylog takes a different approach by basing its pricing on **Active Data in the indexing tier**. This consumption-based model ensures organizations only pay for data that provides value. Native pipeline management further optimizes log processing, aligning cost with outcome.

Customers can deploy Graylog in a variety of environments:

- Self-managed on-premises installations
- AWS Marketplace deployments
- Graylog Cloud (managed deployment hosted on AWS)

Feature parity exists across these deployment models. Customers with hybrid infrastructures can also forward select data to centralized regions without sacrificing capability or requiring major trade-offs.

graylog

Conclusion

Graylog Security offers an efficient, accessible alternative to legacy SIEM platforms. Its cloud-aware architecture, support for AWS-native services, and thoughtful data management practices help organizations secure AWS workloads while maintaining budget and operational flexibility.

Designed for AWS environments, Graylog reduces administrative effort and enables faster threat detection and response. With streamlined deployment, intuitive workflows, and transparent pricing, it provides everything security teams need to modernize cloud operations without the traditional trade-offs.

aws PARTNER