Graylog Security

Empowering Your Cybersecurity with Advanced SIEM Technology

graylog SECURITY

Delivered to you in a self-managed or SaaS experience, Graylog Security is a scalable cybersecurity solution that combines Security Information and Event Management (SIEM), threat intelligence, anomaly detection capabilities, and efficient data management to help your security professionals simplify identifying, researching, and responding to cyber threats.

SIEM Done Right

Resource-constrained organizations need affordable and proactive threat detection, incident analysis, and response, and compliance reporting to strengthen their security posture. Built on the Graylog platform, Graylog Security combines enterprise log management, threat detection, suggested remediation steps, and reporting that's easy to deploy, manage, and use. We've designed our security platform to provide the functionality you need without the complexity and cost of traditional SIEM solutions.

Graylog Security at a Glance

Security-Focused Workflows

Watch your productivity and efficiency increase with Graylog Security's unique security-focused workflows, tailored for analysts to quickly access investigations, alerts, and reporting capabilities.

Graylog Security Benefits

- Immediately see which assets (machines/users) pose the most risk when prioritizing TDIR work
- Streamline licensing for lower-value log data while it is being stored for future incident investigations
- Get contextual insight for Incident Response reports that help inform key stakeholders
- Quickly understand the temporal relationships of specific events within an incident investigation
- Visually understand your current threat coverage and quickly address any gaps

Risk-Based Scoring

Focus on the "right now" risk with automated risk-based scoring. Graylog Security assigns a risk score to alerts so analysts can prioritize security incidents easily.

Lightning-Fast Search for Forensic Analysis and Troubleshooting

Every second counts when trying to keep your environment secure and safe from cyber threats. Graylog Security is designed to parse terabytes of data in seconds, allowing you to find important log data in real time. Quickly access previous query history from an easy, drop-down menu.

Anomaly Detection That Makes Sense

Stay ahead by keeping bad actors out. Graylog Security anomaly detection capabilities are designed with a powerful Machine Learning (ML) anomaly detection engine that can automatically understand your environment and alert you on what's not normal behavior for your users and entities (UEBA).

Identify Priority Security Events in a Sea of Alerts

Cutting through the noise to get to the data you need quickly doesn't have to be difficult. The Graylog Security alert engine makes it easy to filter out the noise so you can focus on the security events that really matter, reducing alert fatigue and maximizing productivity.

Actionable Data vs Standby Data with Graylog - No Cribl Needed for Lower TCO

Graylog's Data Routing capability allows you to easily filter lower-value log data to a less expensive Data Warehouse (standby data) before it is processed by Graylog, allowing the selective restoration of your standby data into actionable data for future investigations.

Visually Follow the Investigation Breadcrumbs

Graylog Security provides an overview of an investigation in a compact and easy to customize widget that provides analysts with a dynamic, real-time visualization of the investigation's progress for a comprehensive timeline view of a security investigation from inception to resolution.

Understand Your Threat Coverage

Graylog Security provides real-time insight into the state of your threat coverage in relation to the tactics and techniques outlined in the MITRE ATT&CK Matrix at a glance. See which Sigma Rules are currently enabled in your environment, and strengthen your security posture by enabling additional rules to extend your threat coverage based on Graylog's recommendations.

How Well Are You Mitigating Risk?

Understand your cyber resilience with Graylog Security by measuring critical security KPIs that represent how effectively you mitigate risk so you know where to focus improvement initiatives.

Reduce TCO While Strengthening Your Security

Graylog Security's cloud-native capabilities, intuitive UI, and out-of-the-box content means you can start getting valuable data from your logs quicker when compared to legacy SIEMs. Lower your labor costs with features designed to significantly reduce alert fatigue, get answers fast, and empower your security professionals. Leverage a "warm" tier where data can be placed, enabling less expensive remote or on-prem storage options while providing the same lightning-fast and robust search experience.

POWERFUL, LIGHTNING-FAST FEATURES

ANOMALY DETECTION / UEBA
Capabilities that quickly learn "normal" behavior and automatically identify deviations for users and entities at scale, with continuous fine-tuning and improvement over time.

COMPLIANCE REPORTING
Leverage Graylog's dashboard functionality to easily build and configure scheduled reports.

DATA ROUTING
Filter lower-value data to a Data Warehouse before it is processed for selective restoration at a later time.

INVESTIGATION SUMMARY REPORT
GenAI is leveraged to summarize evidence pieces to provide contextual insight for IR Reports that help inform key stakeholders.

INCIDENT INVESTIGATION
All-in-one workspace to collect and organize datasets, reports, evidence, and other context while investigating a potential incident.

PREBUILT DASHBOARDS, ALERTS
Start fast with prebuilt content for security use cases — search templates, dashboards, correlated alerts, dynamic look-up tables, and more.

RISK-BASED SCORING
Focus your work around events and issues specific to assets (users/machines) that present the highest risk.

SECURITY ANALYTICS DASHBOARDS
Combine widgets to build customized data displays and automate the delivery of reports to your inbox.

S.O.A.R. INTEGRATIONS
Easily share data with other business-critical systems for full transparency and collaboration.

THREAT COVERAGE WIDGET
Visualize the threat coverage enabled and mapped to the MITRE ATT&CK Framework tactics.

TIMELINE INVESTIGATION WIDGET
An easy-to-understand, time-based visualization of an investigation.

VULNERABILITY SCAN INGEST
Nessus and MS Defender scans are ingested to help calculate higher-fidelity risk scores.

graylog SECURITY

Ask Our Experts and See Graylog Security in Action

Seeing is definitely believing. At Graylog, we want you to get all your questions answered before you buy. We offer scheduled product demos that demonstrate product functionality and allow time for Q&A. Schedule your Graylog Security demo today and see our powerful cybersecurity platform in action.

Graylog Security allows you to gain insight into event correlations across tens of thousands of network components for identified threats or suspicious activity.

ABOUT GRAYLOG

Graylog empowers security teams with cutting-edge, scalable solutions that make threat detection, investigation, and response (TDIR) faster, smarter, and more efficient—keeping organizations ahead of ever-evolving cyber threats. Graylog's machine learning algorithms enhance anomaly detection, while AI-assisted investigation reports and remediation instructions enable security teams to respond to incidents with speed and precision. Scalable and cost-effective, Graylog's solutions are trusted by large enterprises and smaller teams alike, enabling efficient log management and streamlined security workflows. With open-source roots and over 50,000 installations globally, Graylog's product suite—Graylog Enterprise, Graylog Security, Graylog API Security, and Graylog Open—ensures that security teams can focus on what truly matters: protecting their systems. Learn more at graylog.com or connect with us on X (Twitter) and LinkedIn.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog