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 detection and incident response (TDIR), threat intelligence, incident investigation, and anomaly detection capabilities 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.

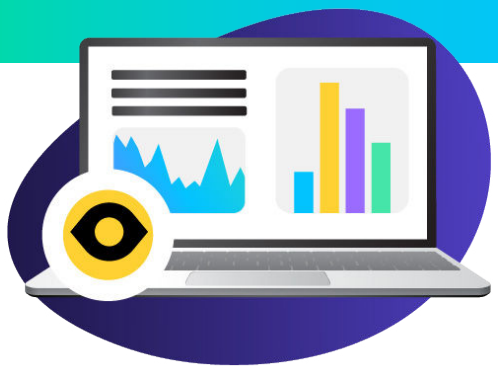
Graylog Security at a Glance

Security-Focused UI

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

Graylog Security Benefits

- Scour volumes of data in seconds with lightning-fast search capabilities
- Easily track assets and quickly identify where a problem or log is coming from
- Focus security efforts on what matters by filtering out alert noise
- Increase productivity with automation you can trust for repetitive and security-intensive tasks
- Leverage an anomaly detection ML engine that continuously learns your security behaviors over time



Risk-Based Scoring

Focus on the "right now" risk with automated risk-based scoring. Graylog Security assigns a risk score to individual 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.

Dedicated Workspace for Incident Investigations

Easily manage incident investigations from start to finish in Graylog Security with an all-in-one workspace to collect and organize datasets, reports, evidence, and other context while investigating a potential incident or issue, collaborate across teams throughout the entire investigation process, and quickly identify trends by using data saved from prior investigations.

Quickly Find Misbehaving Assets

Graylog Security's Asset module allows you to track different types of assets across the environment and enrich log messages with their information. Information about your assets can be easily added through the Graylog UI or synced through LDAP or AD.

Curated Threat Coverage

Graylog Security helps you detect threats across your environment by leveraging advanced cyber techniques like anomaly detection, Sigma Rules, threat intelligence, and the MITRE ATT&CK® framework.

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.

ASSET ENRICHMENT
Gain insight across your environment with the ability to track different assets and enrich log messages with additional information.

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

CORRELATION AND ALERTING
Receive alerts via email, text, Slack, and more. Update alert criteria based on a dynamic list in a lookup table.

DATA NORMALIZATION AND ENRICHMENT
Perform faster research by adding WHOIS, IP Geolocation, threat intelligence, or other structured data.

GRAYLOG USER LOGS
Track who accessed what log data and what actions they took against it to ensure compliance and security.

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.

SEARCH QUERY BUILDER
Build and combine multiple searches for any type of analysis into one action and export results to a dashboard.

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 INTELLIGENCE FEEDS
Add context to event log data with your existing threat intelligence feeds and pinpoint potential security issues.

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 is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

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

graylog