

# Graylog Cloud Security SIEM 安全平台 1GB/day 升級包

· Graylog Cloud Security SIEM安全平台 1GB/day 升級包

購買此升級包需先購買【Graylog Cloud Security SIEM安全平台 10GB/day 一年授權版本】

Graylog Cloud Security SIEM安全平台 1GB/day 升級包提供彈性的每日日誌流量擴充，可以以1GB為單位，擴充單位所需的日誌流量。

· Graylog Security是一款完整的SIEM安全平台解決方案，專門提供單位對IT環境中安全與風險的可見性。具備以下主要功能和規格：

1. SIEM功能：提供全面的安全信息和事件管理 ( SIEM ) 功能，包括威脅檢測、事件響應、威脅情報和異常檢測，幫助安全專業人員簡化識別、研究和應對網路威脅的過程。

2.集中日誌數據：能夠從各種設備、應用程序和系統中收集並集中日誌數據，進行分析與管理。

3. 快速搜索和過濾：具備快速搜索能力，能在數秒內掃描大量數據，並通過標記來進行過濾和識別問題。

通過Graylog，單位可以有效地收集、規範和分析日誌數據，快速檢測和解決安全和性能問題，降低停機時間並簡化管理。

# GRAYLOG CLOUD FACT SHEET



## GRAYLOG CLOUD ISN'T A PRODUCT...IT'S AN EXPERIENCE

Our cloud-native solutions offer a powerful, flexible, and seamless experience without the added burden of infrastructure or operational costs. We are committed to keeping our secure, high availability cloud environment up to date with the latest product features so you can continue to use event log data to gain insight into the overall health of your IT infrastructure, systems, and applications, performance bottlenecks, unusual or suspicious activity, and potential cyber threats across your entire environment.

## ACTIVE SOC 2 TYPE 2 FOR YOU

We understand that data security is one of your top priorities when considering cloud solutions. That's why we sought out and earned SOC 2 Type 2 certification to test and verify the design and upkeep of our security controls, and ensure that when we transmit, store, maintain, process, and dispose of your data, it is kept confidential at all times.

## SLAS AND SUPPORT THAT GO ABOVE AND BEYOND

Enjoy the peace of mind that comes with the Graylog Cloud SLA. Our terms are stated clearly, like our commitment to 99.9% service uptime and 24/7 operational support, Graylog Cloud is designed to meet and exceed your workload requirements, establish clear and measurable guidelines, and adapt to your organization's evolving needs.

## EVENT LOG STORAGE

A Graylog Cloud instance can provide centralized live storage of event log data for up to 90 days, aligning with PCI DSS log retention requirements. Once your event logs are centralized and stored, Graylog Operations and Graylog Security can automatically aggregate your log data, quickly correlate disparate pieces of information to piece together potential performance issues or cyber threats and provide you with actionable insight you can use to resolve errors faster.

## EVENT LOG ARCHIVAL

The 1-year log archival capabilities of Graylog Cloud can help provide a glimpse into the state of your environment over a set period of time. Graylog Operations and Graylog Security can leverage archived log data to identify performance trends, audit security events, and pinpoint periods of high demand so you can make informed decisions.

## REALIZE VALUE QUICKLY

Graylog Cloud capabilities allow you to focus your investment on day-to-day analysis activities, and not physical infrastructure. We'll get you up and running in a few days so you can access and analyze your log data from anywhere at any time. From there, Graylog Cloud makes it easy to scale up or down to meet the needs of your business.

# Graylog Security

Empowering Your Cybersecurity with Advanced SIEM Technology



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.

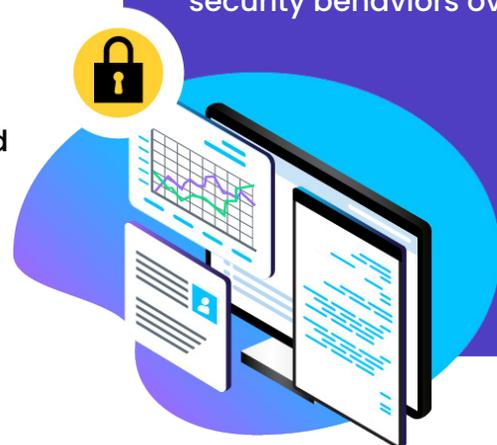
## Graylog Security at a Glance

### 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.



## 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](http://www.graylog.org)

[info@graylog.com](mailto:info@graylog.com) | 1301 Fannin Street, Suite 2000, Houston, TX 77002

©2024 Graylog, Inc. All rights reserved.

