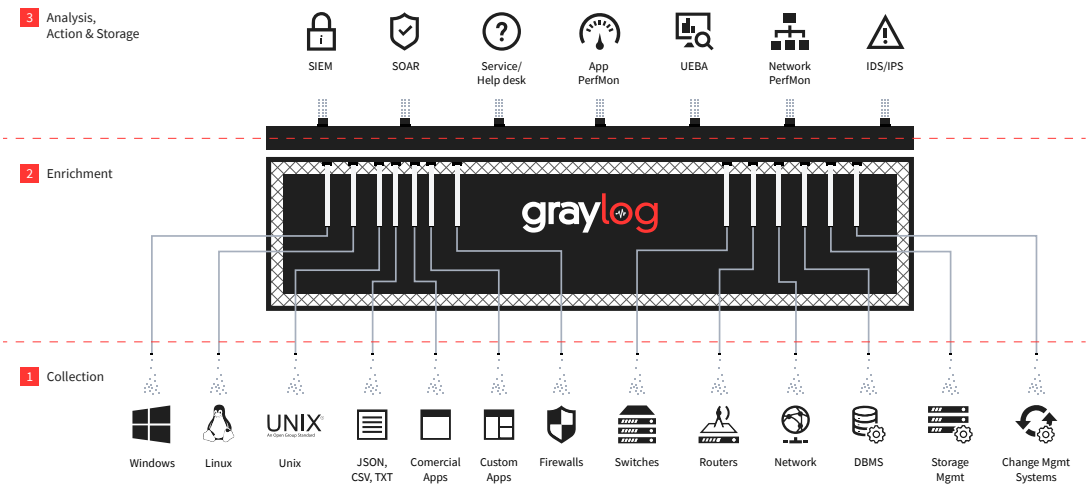
GRAYLOG ENTERPRISE EDITION

OVERVIEW

Graylog is a centralized log management (CLM) platform that seamlessly collects, enhances, stores, and analyzes log data. Logs are fundamental to any IT operations or security program, and placing them all in a single location greatly simplifies their use.

ARCHITECTURE

Graylog is composed of three components: Graylog, MongoDB, and Elasticsearch. All components can be installed on one server for evaluation or POC deployments. For production installations, we recommend that you separate the Elasticsearch component onto a separate server.



WHAT MAKES GRAYLOG UNIQUE

COMPREHENSIVE

Horizontally scale to meet any size workload from a gigabyte to petabytes per day. Built in fault tolerance enables distributed and load-balanced operations to prevent data loss. Our comprehensive procession algorithm to parse logs and search through virtually unlimited data.

TREMENDOUS VALUE

There are many facets to price—licensing, processing, storage, and system maintenance—and Graylog is more cost-effective than others across all of them. Graylog Enterprise is free up to 5 GB/day, and beyond that ingest rate, typically ⅓ to ½ the price of major competitors. And that lower price includes collection of all data across your environment. Throw in our top-notch customer experience from initial conversations to purchase to ongoing technical support and product enhancements, and your value skyrockets.

EASY EXPLORATION

Graylog lets you analyze data without having to know exactly what you are looking for before querying. Graylog expands and reveals more information as you go, delving deeper into the search results to explore further to find the right answers.

INCREDIBLE FLEXIBILITY

Graylog is built to open standards for connectivity and interoperability for seamless collection, transfer, storage, and analysis of log data. We now centrally manage any machine data collector—ours, custom, or 3rd party vendor—from the admin console, including stopping or starting any whitelisted system processes. Not only that, we can collect other structured data as well, such as DNS lookups from the wire.

RIDICULOUS SPEED

When working with enterprise-scale data, every second—or millisecond—matters. The longer it takes to analyze data coming in, the longer it takes to find and resolve issues. Graylog lets you search and investigate multiple issues at once with multi-threaded data retrieval, saving considerable time and delivering results much faster.

VALUE FOR EVERYONE

Make repetitive tasks and routine investigations efficient, ensure consistency, and empower less technical members of the team through dashboards and saved searches.

FEATURES

ARCHIVING

Store older data on slow storage and easily re-import it into Graylog when you need it.

CONTENT PACKS

Share configurations of extractors, inputs, pipelines, dashboards and more. Move easily from Test to Production.

CORRELATED ALERTS

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

DYNAMIC LOOKUP TABLES

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

FORWARDER

Easily send data to Graylog Cloud or to an on-premise Graylog Server installation.

ILLUMINATE

Start fast with prebuilt content — search templates, dashboards, correlated alerts, dynamic look-up tables, and more.

INTEGRATIONS

Easily share data with other business-critical systems for full transparency and collaboration.

INTERACTIVE DASHBOARDS

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

LOG VIEW

View data in real-time, ensure continued availability, streamline investigations.

PARAMETERIZATION

Enter one or more criteria for a more comprehensive search. Easily save and share as templates.

PIPELINES

Set rules for data processing to ensure the right parser, data enrichment and lookup table(s) are applied.

REST API

Easily integrate your data into 3rd party systems to automate reporting, workflow and research.

SCALABLE SEARCH

Build complex queries in minutes with Graylog's web console—no proprietary query language needed.

SCHEDULE REPORTS

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

SEARCH WORKFLOW

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

STREAMS

Categorize log messages in real-time to easily target queries, reports and dashboards for faster results.

TEAMS MANAGEMENT

Control entity access and capabilities. Includes LDAP/Active Directory integration.

USER AUDIT LOGS

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

ABOUT GRAYLOG

Log management done right. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning centralized log management solution built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog enables hundreds of thousands of users to explore their data every day to solve security, compliance, operational, and application development issues.

SYSTEM REQUIREMENTS

For a typical installation up to a 5 GB daily ingest volume, we recommend starting with the following requirements:

- 4 CPU cores
- 8 GB RAM
- SSD hard disk space with high IOPS for Elasticsearch Log Storage