graylog ENTERPRISE

Centralized Log Management
FOR LEAN TEAMS

IT and DevOps teams need complete visibility across every environment without the tuning overhead, unpredictable pricing, or infrastructure complexity that slows resolution. Graylog Enterprise delivers centralized log management that scales with your organization and stays within your budget.

What Sets Graylog Enterprise Apart

Fast Time to Value
Guided setup and rapid content activation. No expert tuning required.

Unified Insights
Parse, enrich, search, and analyze logs across your entire environment in real time.

Predictable Pricing
A built-in data lake keeps standby data off your license. Preview and retrieve only what you need.

Deploy Anywhere
Cloud, on-prem, or hybrid. Same intuitive experience, capabilities, and API-first design.

Built-in AI Assistance
AI-powered dashboard summaries and investigation analysis, with free MCP server access for every tier.

Built for IT, DevOps, and Compliance Leaders

IT Operations Teams
- Troubleshoot faster with full access to live and historical logs
- Detect and resolve issues before they impact performance
- Preview and retrieve only relevant data from standby storage
- Maintain predictable budgets through analysis-based pricing

DevOps and Site Reliability Engineering
- Monitor production environments with complete transparency
- Leverage prebuilt parsing and enrichment packs for faster insights
- Correlate across live and archived data with minimal setup
- Investigate incidents without complex restores or manual intervention

IT Leadership and Compliance
- Gain unified visibility across systems, users, and environments
- Simplify compliance with prebuilt content and selective log retrieval
- Maintain control over AI with MCP guardrails and bring-your-own-model support
- Scale role-based access across departments, regions, and teams

Feature Highlights

graylog ENTERPRISE

Detect Real Threats

- Native Impossible Travel and Log Volume detectors surface behavioral threats that rule-based detection misses
- Tunable anomaly detection with debug output showing exactly why each detector fired, no OpenSearch dependency
- Sigma rule import from private GitHub, GitLab, and Bitbucket repositories with full version control
- CrowdStrike vulnerability scan results imported directly into the Asset system for risk-aware triage

Respond with Ease

- Risk score threshold breach automatically creates an Investigation with related events and logs pre-loaded
- Consolidated remediation steps from every alert surfaced in one procedure list, no SOAR required
- Event status syncs across all attached evidence when Investigation status changes
- Full-page Investigation view with sortable, filterable event and log tables

Reduce Infrastructure Overhead

- Parallel archive restore jobs run simultaneously, cutting recovery from weeks to hours
- Shared sizes calculated automatically from each node's available OS memory, removing manual tuning
- Azure Blob Storage fully supported for archives, warm tier, and Data Lake
- Dynamic shard count for restored archive index sets prevents over-allocation during forensic restores

Improve Analyst Efficiency

- Entity table Slice-By filters alerts and events by type, priority, owner, status, and risk score in one click
- Bulk add multiple log messages to an Investigation in a single action from any log view
- Save and restore column configurations in entity tables across sessions
- Keyboard shortcut navigation to any page, stream, or saved search in large deployments

See Graylog Enterprise in Action

Schedule a demo today to see how Graylog Enterprise helps you manage logs smarter, troubleshoot faster, and maintain full control of your data without compromise.

graylog.com /see-demo

ABOUT GRAYLOG

Graylog is the AI-powered SIEM and centralized log management platform trusted by 60,000+ organizations worldwide. By combining scalable log management, real-time correlation, and explainable AI, Graylog turns overwhelming data into clear insight and confident action. **Learn more at graylog.com** or connect with us on Bluesky and LinkedIn.

www.graylog.org | info@graylog.com
1301 Fannin Street, Suite 2000, Houston, TX 77002 | ©2026 Graylog, Inc. All rights reserved.

graylog