

Security teams need full detection and response capability without the complexity, cost, or tuning overhead that makes enterprise SIEM impractical. Graylog Security delivers the coverage, automation, and analyst experience that lean teams require to stay ahead of real threats.

What Sets Graylog Security Apart



The Verascend™ Incident System

Graylog's agentic triage layer turns millions of log lines into a ranked queue of verified incidents. Noise stays buried. The High-Risk Asset Triage Agent builds the case; the Alert Fatigue Agent tunes detection to your environment. Every case opens with its evidence already attached and closes with an AI-generated summary and remediation plan.



Fast Time to Value

Most SIEMs ship generic rules. Security Core ships mapped to the threats mid-market teams actually face: phishing, ransomware, credential misuse. Detection starts day one. No custom rules required.



Deploy Anywhere, Full Data Sovereignty

Graylog deploys the same way everywhere, whether data stays in the EU, APAC, or anywhere else. Any S3-compatible store works, OVHcloud and Secunet SysEleven included. MCP access is standard.



Bring Your Own AI Stack

Graylog's MCP server lets any AI agent or LLM query logs, alerts, and investigations directly. Ask a custom agent to pull open cases, or trigger an investigation straight from Slack.



Predictable Retention Costs

A built-in data lake stores years of logs outside your active license. Preview and retrieve only what an investigation requires, with full stream-level size visibility.

Built for Analysts, Trusted by Security Leaders

Security Analysts	SIEM Architects/Admins	CISOs
- High-fidelity detections surface only the alerts that require attention - Open an investigation and find every related event already pre-loaded, plus an AI agent's risk assessment - Move from alert to action faster with consolidated remediation procedures - Share AI-written case summaries without leaving the platform	- Go live with coverage across 7 attack surfaces for coverage of top 10 threats on day one - Onboard new data sources with schema-aware parsing and minimal rework, now including a native collector for system log collection. - Route data by policy and cost to eliminate over-ingestion - Eliminate manual tuning with dynamic shard sizing and parallel restore jobs, plus a GUI-managed warm tier repositories page	- Surface the risks that matter most without wading through noise - Control licensing and storage costs with no surprise invoices - Reclaim analyst shift time lost to manual triage and case assembly, now automated by an AI agent for asset risk triage - Audit-ready incident reports generated automatically at case closure

Threat Detection & Prioritization



- 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
- Entity-based risk scoring with configurable thresholds by asset group, including separate scoring for privileged accounts
- Sigma rule import from private GitHub, GitLab, and Bitbucket repositories with full version control, now edited as a unified Graylog Event Definition

Faster Investigation & Response



- Risk score threshold breach automatically creates an investigation with related events and logs pre-loaded, now triaged by an AI agent
- Consolidated remediation steps from every alert surfaced in one procedure list, no SOAR required
- AI-written incident reports generated at case closure, including timelines, evidence lists, and audit-ready documentation
- Event status syncs across all attached evidence when Investigation status changes, with dedicated alert page views for assets and investigations

Cost-Efficient Log Management



- Built-in data lake stores standby logs outside the active license with data preview and selective retrieval included
- Parallel archive restore jobs run simultaneously, cutting recovery from weeks to hours
- Azure Blob Storage fully supported for archives, warm tier, and data lake
- Transparent, analysis-based pricing with no per-GB ingest fees

Security Coverage & Compliance



- 68 prebuilt alerts, 42 reports, and 7 dashboards covering the top 10 security threats ship ready at deployment
- Entity table slice-by filters alerts and events by type, priority, owner, status, and risk score, and MITRE ATT&CK technique, in one click
- Bulk add multiple log messages to an Investigation in a single action from any log view
- MCP server access included at no extra cost across all tiers, with bring-your-own-LLM support and centralized agent administration

See Graylog Security in Action

Schedule a live demo today to see how you can cut costs, speed investigations, and strengthen detection strategy — **without compromise.**



graylog.com/see-demo

ABOUT GRAYLOG



Graylog delivers a centralized log management platform designed around how IT and DevOps teams actually work: full visibility, AI-driven insights, and faster troubleshooting without unpredictable costs. Trusted by more than 60,000 organizations worldwide, Graylog helps teams move from raw data to actionable insight with less effort. Automate routine tasks. Focus on real performance issues. Keep costs predictable. Learn more at graylog.com