

Which Graylog Edition Is Right For You?

Feature Comparison List by Product



Graylog Open

Collect, store, search, and analyze log data at your own pace. Start free, scale when you're ready.



Graylog Enterprise

Centralized log management without compromise — faster insights, lower costs, and full visibility across your environment.



Graylog Security

The SIEM that ends tradeoffs — complete visibility, faster threat detection, and predictable costs.

Operational Efficiency & Productivity

Graylog brings every data source into one place, with native input listeners for standard protocols and prebuilt integrations for leading SaaS, cloud, and security platforms, and centralized log collector management that simplifies deployment at scale.

Feature	Open	Enterprise	Security
Embedded MCP Server for Natural Language Tools	✓	✓	✓
REST API	✓	✓	✓
Log Collector Management	✓	✓	✓
Customized Data Normalization & Enrichment	✓	✓	✓
Input Listeners: Syslog, CEF, GELF, BEATS, HTTP JSON, AWS Kinesis, IPFIX, Netflow, Plain Text	✓	✓	✓
SaaS/API Integrations: IPassword Events, AWS S3, AWS Security Lake, Azure Event Hubs, Bitdefender Gravity Zone, CrowdStrike, External Data Lake Filtered Input, F5 BIG-IP, GCP, Google Workspace, MS Defender for Endpoint, MS Graph, Mimecast V2, Office 365, Okta, Salesforce, Sophos Central, Symantec EDR/SES Events	—	✓	✓

Search

Graylog's search helps analysts find what matters fast, with type-ahead query assistance, reusable filters, and parameterized searches that turn common investigations into repeatable, one-click workflows. Results come alive through visualizations, aggregations, and any search can be saved, shared with teammates, or pinned to a dashboard so insights never have to be rebuilt from scratch.

Feature	Open	Enterprise	Security
Custom Visualizations, Aggregations, Favorites Fields on Search Results	✓	✓	✓
Save Searches to Dashboards	✓	✓	✓
Type-ahead query assistance	✓	✓	✓
Save & Share Search Queries	✓	✓	✓
Search Filters	—	✓	✓
Saved Parameterized Searches	—	✓	✓

Dashboards & Reports

Turn data into clear, shareable dashboards that summarize what's happening and let you act on it right away. Scheduled reports keep leadership, auditors, and security teams informed without the manual effort.

Feature	Open	Enterprise	Security
Save & Share Dashboards	✓	✓	✓
Charts with support for Markdown text	✓	✓	✓
Visualization Threshold Annotations	✓	✓	✓
Take Action from Dashboard Charts	Limited	✓	✓
AI Summarization of Dashboards	—	✓	✓
Right-click Graylog + Custom Saved Searches	—	✓	✓
Scheduled Email Reports	—	✓	✓
Saved Parameterized Dashboards	—	✓	✓
Custom Compliance & Management Reports	—	✓	✓
Dashboards and Reports by Attack Surface	—	—	✓

Events & Alerts

Define the events that matter to your environment and connect the dots across activity to surface real threats, not noise. Alerts reach your team through the tools they already use and can trigger automated responses the moment something happens.

Feature	Open	Enterprise	Security
Custom Event Creation	Limited	✓	✓
Alert Notification Delivery Integrations: (Email, Pager Duty, MS Teams, Slack, HTTP)	Limited	✓	✓
Automated Script Triggers	—	✓	✓
Correlation Engine	—	✓	✓

Graylog Illuminate Content & 3rd Party Data Enrichment

Graylog Illuminate delivers ready-made content, from parsing and dashboards to detections, guided responses, and compliance reports, so you get value from your data from day one. Built-in enrichment adds user, device, location, and threat context automatically, giving every event the meaning it needs for faster decisions.

Feature	Open	Enterprise	Security
Geolocation (Additional subscription required)	✓	✓	✓
Data Enrichment Connectors	Limited	✓	✓
Lookup Tables	Limited	✓	✓
Illuminate Content Hub	Limited	✓	✓
Input Wizard	Limited	✓	✓
Graylog provided data normalization, enrichment, and dashboards	Limited	✓	✓
Graylog provided reports, detections, and saved searches	—	✓	✓
Graylog provided threat detections, guided responses, and compliance reports	—	—	✓
Automatic User and Device Context	—	—	✓

Verascend™ Incident System

Alert fatigue drains lean teams before a real threat ever surfaces. Verascend turns risk-scored alerts into verified incidents through algorithms, event consolidation, and agentic workflows, tuning rules and automating evidence gathering so analysts investigate instead of filtering.

Feature	Open	Enterprise	Security
Import Sigma Rules	—	—	✓
MITRE ATT&CK Framework Alignment	—	—	✓
Event Procedures With Guided Remediation	—	—	✓
Third Party SOAR and Ticketing Integration	—	—	✓
detection chain dynamic risk scoring	—	—	✓
Threat Intel Lookups and Watchlists	—	—	✓
AI Investigation Report Summarization Generation	—	—	✓
Embedded AI Agentic Framework with Asset Triage and Alert Fatigue Agents	—	—	✓
User Activity, Suspicious Data Movement, File and System Integrity, Network and Perimeter Threats	—	—	✓
Evidence Collection	—	—	✓
Investigation Timeline Visualization and Analytics	—	—	✓
Impossible Travel Detection & Log Volume Detectors	—	—	✓
Events and Alerts Risk Scoring	—	—	✓
Composite Risk Scoring for Users and Systems	—	—	✓
Threat Coverage Analyzer and Visualization	—	—	✓
System Vulnerability Risk Amplifier	—	—	✓
Variance-Based Risk Amplifier	—	—	✓
Threat Intelligence Detection Chain Risk Amplifier	—	—	✓

Intelligent Data Management and Scalability

Scale confidently with a node-based architecture, built-in health monitoring, and flexible forwarding that grows with your environment. Smart routing, data tiering, and data lake storage keep costs under control while ensuring the data you need is always within reach.

Feature	Open	Enterprise	Security
Node Based Architecture	✓	✓	✓
Embedded Management for OpenSearch	✓	✓	✓
Graylog System Health Panel	—	✓	✓
Content Pack Import/Export for sharing rules and configurations across Graylog environments	✓	✓	✓
Cluster Metrics for Graylog Node, Graylog Data Node and MongoDB	—	✓	✓
Enterprise Forwarder	—	✓	✓
Cluster to Cluster Forwarder	—	✓	✓
Data Pipeline Management and Routing	—	✓	✓
Data Tiering: Hot, Warm and Archive	—	✓	✓
Internal Data Lake: AWS, GCS, Azure, SysEleven, and OVH and File System	—	✓	✓
Data Lake Preview and Selective Retrieval	—	✓	✓
Filtered AWS Security Lake Input (3rd-party data lake)	—	✓	✓

System Security & Compliance

Control exactly who can see and do what, with role-based access, data separation, and seamless integration with your existing identity systems. Built-in user audit logs provide a clear record of activity to support security reviews and compliance requirements.

Feature	Open	Enterprise	Security
Role-based Feature Access Control with AD, LDAP, or Native	✓	✓	✓
Logical Data Separation & Permissions	✓	✓	✓
AD/LDAP Group Sync	—	✓	✓
Single Sign-On	—	✓	✓
Graylog User Audit Logs	—	✓	✓
Content & Data Sharing Management	—	✓	✓

Customer Support & Services

Get up to speed quickly with comprehensive documentation, on-demand and instructor-led training through Graylog Academy, and an active user community. For deeper partnership, accelerator programs and dedicated Technical Account Managers help your team get the most from Graylog at every stage.

Feature	Open	Enterprise	Security
Documentation	✓	✓	✓
Graylog Academy On-Demand	✓	✓	✓
Graylog Community	✓	✓	✓
Graylog Academy Instructor-Led	—	✓	✓
Graylog Accelerator	—	✓	✓
Technical Account Manager (add on)	—	Optional	Optional