

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
OPERATIONAL EFFICIENCY & PRODUCTIVITY			
Support for Syslog, CEF, GELF, BEATS, HTTP-JSON, IPFIX, Netflow, Plain Text	✓	✓	✓
Log Collection	✓	✓	✓
Sidcar Central Log Collector Management	✓	✓	✓
Index Field Type Profiles	✓	✓	✓
Pipelines and Streams	✓	✓	✓
Data Normalization	✓	✓	✓
Collections	X	✓	✓
Asset History	X	X	✓
Asset Event Definition	X	X	✓
Distinguish Illuminate vs. User-Created Entities	✓	✓	✓

SEARCH			
Visualization Widgets	✓	✓	✓
Save To Dashboard	✓	✓	✓
Guided Search	✓	✓	✓
Save & Share	✓	✓	✓
Filters	X	✓	✓
Parameters	X	✓	✓

DASHBOARDS & REPORTS			
AI Dashboard Summarization	X	✓	✓
Drill Down from Aggregation Widgets	✓	✓	✓
Widget Thresholds and Labels	✓	✓	✓
Text Widgets with Markdown	✓	✓	✓
Revert Changes When Canceling Widget Edit	✓	✓	✓
Data Table Row Numbers	✓	✓	✓
Right-click Graylog + Custom Saved Searches	X	✓	✓
Scheduled Email Reports	X	✓	✓
Dashboard Drill Down	X	✓	✓
Custom Reports	X	✓	✓
Customizable Visualization Widgets	✓	✓	✓
Save and Share	✓	✓	✓

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
GRAYLOG CONTENT & ILLUMINATE			
Input Wizard	Partial	✓	✓
Illuminate Content Hub	Limited with free Illuminate content	✓	✓
Illuminate Content	Parsers (free packs) only available for certain Open-source tools	Ops Content	All Content
Sharing Searches for Illuminate + Content Packs	X	✓	✓
Graylog Schema	Manual	Illuminate	Illuminate
REST API	✓	✓	✓
Content Pack Import/Export	✓	✓	✓
Distinguish Illuminate vs. User-Created Entities	✓	✓	✓
TCP Raw & TCP Syslog Outputs	✓	✓	✓
Security Detection content (e.g. Sigma Rules)	X	X	✓

DATA ENRICHMENT AND AI			
Data Enrichment Connectors	✓	✓	✓
IPInfo + MaxMind GeoIP (vendor subscription required)	X	✓	✓
Lookup Tables	Static	Dynamic	Dynamic
Asset Data	X	X	✓
Vulnerability Scan Support (Qualys, Tenable Cloud, Nessus, Microsoft Defender)	X	X	✓
MCP Server Integration for Natural Language Tools	✓	✓	✓
AI Dashboard Summarization	X	✓	✓
UEBA + Anomaly Detection (ML)	X	X	✓
AI Investigation Report Generation	X	X	✓

	Graylog Open <i>(Self Managed)</i>	Graylog Enterprise <i>(Self-Managed, Hybrid, Cloud)</i>	Graylog Security <i>(Self-Managed, Hybrid, Cloud)</i>
THREAT DETECTION, INVESTIGATION, AND RESPONSE			
Basic Triggers and Aggregations	X	✓	✓
Alerting	X	✓	✓
Notifications	Basic	Advanced	Advanced
Automated Script Triggers	X	✓	✓
Correlation Engine	X	✓	✓
Sigma Rules	X	X	✓
MITRE ATT&CK Framework Alignment	X	X	✓
UEBA and Case Management			
User activity + suspicious movement + integrity + network/perimeter threats	X	X	✓
Custom Detectors	X	X	✓
Evidence Collection	X	X	✓
AI Investigation Report Generation	X	X	✓
Investigation Timeline Visualization and Analytics	X	X	✓
SOAR and Guided Response			
Event Procedures (guided steps)	X	X	✓
Automation	X	X	✓
Guided Response and Workflow	X	X	✓
Third-Party SOAR + Ticketing Integration (add-on)	X	X	✓

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
COMPLIANCE & RISK MANAGEMENT			
Risk Management			
Compliance Reports	X	✓	✓
Asset-based Risk Scoring	X	X	✓
Events and Alerts Risk Scoring	X	X	✓
Adversary Campaign Intelligence	X	X	✓
Field Actions with Threat Intel Lookups + Watchlists	X	X	✓
Threat Coverage Analyzer + Visualization	X	X	✓
Vulnerability Scan Ingest (Qualys, Tenable Cloud, Nessus, Microsoft Defender)	X	X	✓
Access Control			
Teams Management	X	✓	✓
OIDC, OKTA, Auth0, AzureAD, Google, Keycloak, Pingidentity, OneLogin Support	X	✓	✓
Graylog User Audit Logs	X	✓	✓
Role-based	Internal	AD/LDAP	AD/LDAP

COST OPTIMIZATION & SCALABILITY			
Scalable Architecture			
Multi-Node Clusters	✓	✓	✓
Enterprise Forwarder	X	✓	✓
Cluster-to-Cluster Forwarder	X	✓	✓
Cloud Forwarder	✓	✓	✓
Data Node (OpenSearch 2.19)	✓	✓	✓
Data Management			
Data Pipeline Management + Routing	✓	✓	✓
Data Lake	X	✓	✓
Data Lake Preview + Selective Retrieval	X	✓	✓
Amazon Data Lake Preview + Retrieval	X	✓	✓
Filtered AWS Security Lake Input (3rd-party data lake)	X	✓	✓
Lake Retrievals Page	X	✓	✓
Data Tiering (Hot/Warm/Archive)	X	✓	✓
HDFS Warm Tier Support	X	✓	✓

CUSTOMER SUPPORT & SERVICES			
Documentation	✓	✓	✓
Graylog Academy	✓	✓	✓
Graylog Community	✓	✓	✓
Onboarding + Architecture Review Services	X	✓	✓
Technical Account Manager (add-on)	X	Optional	Optional