

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
OPERATIONAL EFFICIENCY & PRODUCTIVITY			
Operational Efficiency & Productivity			
Log Collection & Fleet Management	✓	✓	✓
Support for Syslog, CEF, GELF, BEATS, HTTP-JSON, IPFIX, Netflow, Plain Text	✓	✓	✓
Sidecar Centralized Configuration Management	✓	✓	✓
Index Field Type Profiles	✓	✓	✓
Pipelines & Streams	✓	✓	✓
Data Normalization	✓	✓	✓
Collections		✓	✓
Asset History			✓
Asset Event Definition			✓
Search			
Filters		✓	✓
Parameters		✓	✓
Visualization Widgets	✓	✓	✓
Save To Dashboard	✓	✓	✓
Guided Search	✓	✓	✓
Save & Share	✓	✓	✓
Favorite Fields	✓	✓	✓
Dashboards & Reports			
Security Core Reports			✓
AI Dashboard Summarization		✓	✓
Right-click Graylog & Custom Saved Searches		✓	✓
Scheduled E-mail Reports		✓	✓
Dashboard Drill Down	✓	✓	✓
Dashboard Widget Thresholds	✓	✓	✓
Dashboard Table Row Numbers	✓	✓	✓
New Widget Placement & Revert Edits	✓	✓	✓
Custom Reports	✓	✓	✓
Customizable Data Visualization Widgets	✓	✓	✓
Save & 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		✓	✓
Direct Ingest	Basic	Advanced	Advanced
Direct Output	GELF Output STDOUT	GELF, STDOUT-Enterprise, Google Cloud Big Query	GELF, STDOUT-Enterprise, Google Cloud Big Query
Graylog Schema	Manual	Illuminate	Illuminate
Illuminate Content	Basic Parsers	Ops Content	All Content
REST API	✓	✓	✓
Content Pack Import/Export	✓	✓	✓
Distinguish Illuminate vs. User-Created Entities	✓	✓	✓
TCP Raw & TCP Syslog Outputs		✓	✓
Support for IPinfo, MaxMind GeoIP Integration	✓	✓	✓
Alerting	✓	✓	✓
Notifications	Basic	Advanced	Advanced
Distinguish Illuminate vs. User-Created Entities	✓	✓	✓
Data Enrichment			
Asset Data			✓
IPinfo GeoIP Data		Cloud	Cloud
Filtered AWS Security Data Lake Input		✓	✓
Preview/Retrieval for AWS Security Data Lake		✓	✓
Data Lake Retrievals Page		✓	✓
Lookup Tables	Static	Dynamic	Dynamic
Data Enrichment Connectors	✓	✓	✓
Support for IPinfo, MaxMind GeoIP Integration	✓	✓	✓
Vulnerability Scan Support (Qualys & Tenable Cloud, CrowdStrike)			✓
AI & Machine Learning			
MCP Server Integration	✓	✓	✓
AI Dashboard Summarization		✓	✓
UEBA and Anomaly Detection (ML)			✓
AI Investigation Report Generation			✓

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
THREAT / PERFORMANCE DETECTION, INVESTIGATION, & RESPONSE			
Events & Alerts			
Sigma Rules			✓
MITRE ATT&CK Framework			✓
Automated Script Triggers		✓	✓
Correlation Engine		✓	✓
AI Dashboard Summarization	✓	✓	✓
Dashboard Drill Down	✓	✓	✓
Dashboard Widget Thresholds	✓	✓	✓
Dashboard Table Row Numbers	✓	✓	✓
New Widget Placement & Revert Edits	✓	✓	✓
Basic Triggers & Aggregations	✓	✓	✓
Alerting	✓	✓	✓
Notifications	Basic	Advanced	Advanced
Distinguish Illuminate vs. User-Created Entities	✓	✓	✓
UEBA Anomaly Detection			
Evidence Collection			✓
AI Investigation Report Generation			✓
Investigation Timeline Visualization			✓
Investigations Analytics			✓
SOAR			
Automation			✓
Guided Response			✓
Workflow			✓
3rd Party SOAR, Ticketing Integration (custom add-on)			✓
COMPLIANCE & RISK MANAGEMENT			
Risk Management			
Asset-based Risk Scoring			✓
Events & Alerts Risk Scoring			✓
Adversary Campaign Intelligence			✓
Field Action Menus with Threat Intel Lookups and Watchlists			✓
Threat Coverage Analyzer			✓
Threat Coverage Visualization			✓
Vulnerability Scan Ingest			✓
Compliance Reports		✓	✓
Vulnerability Scan Support (Qualys & Tenable Cloud)			✓

	Graylog Open (Self Managed)	Graylog Enterprise (Self-Managed, Hybrid, Cloud)	Graylog Security (Self-Managed, Hybrid, Cloud)
Access Control			
Teams Management		✓	✓
OIDC, OKTA, Auth0, AzureAD, Google, Keycloak, Pingidentity, OneLogin Support		✓	✓
Graylog User Audit Logs		✓	✓
Role-based	Internal	AD/LDAP	AD/LDAP

COST OPTIMIZATION & SCALABILITY (INTELLIGENT DATA MANAGEMENT)			
Scalable Architecture			
Cluster Metrics for Graylog Node, Graylog Data Node and MongoDB	✓	✓	✓
Enterprise Forwarder		✓	✓
Cluster-to-Cluster Forwarder		✓	✓
Cloud Forwarder		✓	✓
Multi-Cluster	✓	✓	✓
Data Node	✓	✓	✓
Data Management			
Data Pipeline Management / Data Routing		✓	✓
Data Lake - S3, GCS and Azure Blob		✓	✓
Data Lake Preview		✓	✓
Selective Retrieval		✓	✓
Data Tiering - Hot, Warm, Archive		✓	✓
Searchable Snapshots		✓	✓
3rd Party SOAR, Ticketing Integration (custom add-on)			✓
Filtered AWS Security Data Lake Input		✓	✓
Preview/Retrieval for AWS Security Data Lake		✓	✓
Data Lake Retrievals Page		✓	✓
Collections		✓	✓
Asset History			✓
Asset Event Definition			✓

CUSTOMER SUPPORT			
Onboarding & Architecture Review Services		✓	✓
TAM Services (optional add-on)		✓	✓
Access To Professional Services (SOW required)		✓	✓
24x5 Global Technical Support		✓	✓
Documentation	✓	✓	✓
Graylog Academy	✓	✓	✓
Graylog Community	✓	✓	✓