# Elastic self-managed subscriptions

The Elastic Stack — Elasticsearch, Kibana, and Integrations — powers a variety of use cases. And we have flexible plans to help you get the most out of your on-prem subscriptions.

Our resource-based pricing philosophy is simple: You only pay for the data you *use*, at any scale, for every use case.

Contact sales for more pricing information about self-managed licensing.

Contact us

| | Free and open - Basic [1, 2] | Platinum (Existing Customers Only)[18] | Enterprise | Gold (Discontinued)[9] |
|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Inverted index (for search) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Evaluating calculated fields at index time | ✓ | ✓ | ✓ | ✓ | ✓ |
| Runtime fields | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lookup runtime field | ✓ | ✓ | ✓ | ✓ | ✓ |
| Document store (for unstructured) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Columnar store (for analytics) | ✓ | ✓ | ✓ | ✓ | ✓ |
| BKD trees (for numeric, dates, & geo) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Flattened field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Histogram field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Match only text field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Shape field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vector field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Version field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Wildcard field type | ✓ | ✓ | ✓ | ✓ | ✓ |
| Synthetic _source | 15 | 15 | ✓ | 15 | |

| | | | | |
|---|---|---|---|---|
| Synthetic columnar _source (Tech Preview) | | | ✓ | |
| **Data management** | | | | |
| Searchable snapshots | | | ✓ | |
| Snapshot/restore APIs | ✓ | ✓ | ✓ | ✓ |
| Snapshot as simple archives | | | ✓ | |
| Snapshot lifecycle management | ✓ | ✓ | ✓ | ✓ |
| Snapshot-based peer recoveries | | | ✓ | |
| Data rollups | ✓ | ✓ | ✓ | ✓ |
| Data streams | ✓ | ✓ | ✓ | ✓ |
| Data tiers | ✓ | ✓ | ✓ | ✓ |
| Data transforms | ✓ | ✓ | ✓ | ✓ |
| Index lifecycle management | ✓ | ✓ | ✓ | ✓ |
| Data stream lifecycle | ✓ | ✓ | ✓ | ✓ |
| Downsampling lifecycle | ✓ | ✓ | ✓ | ✓ |
| Streams | ✓ | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Data import tutorials | ✓ | ✓ | ✓ | ✓ |
| Ingest Node Pipeline Builder UI | ✓ | ✓ | ✓ | ✓ |
| Grok Debugger | ✓ | ✓ | ✓ | ✓ |
| Upgrade Assistant | ✓ | ✓ | ✓ | ✓ |
| License management | ✓ | ✓ | ✓ | ✓ |
| Centralized Logstash pipeline management | | ✓ | ✓ | ✓ |

**Scalability & resiliency**

| | | | | |
|---|---|---|---|---|
| Clustering & high availability | ✓ | ✓ | ✓ | ✓ |
| Cluster rebalancing | ✓ | ✓ | ✓ | ✓ |
| Advanced cluster rebalancing[13] | | | ✓ | |
| Cross-cluster search (legacy certificate based security model / _search only)[19] | ✓ | ✓ | ✓ | ✓ |
| Cross-cluster search (advanced API-key based security model / including ES\|QL) | | | ✓ | |
| Cross-cluster ES\|QL | | | ✓ | |
| Cross-cluster replication[19] | | ✓ | ✓ | |

| | | | | | |
|---|---|---|---|---|---|
| Encrypted communications | ✓ | ✓ | ✓ | ✓ | ✓ |
| Role-based access control | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anonymous access control (public sharing) | ✓ | ✓ | ✓ | ✓ | ✓ |
| File and native authentication | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kibana Spaces | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kibana feature controls | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kibana sub-feature privileges[8] | | ✓ | ✓ | ✓ | ✓ |
| Prelogin access agreement | | ✓ | ✓ | ✓ | ✓ |
| API keys management | ✓ | ✓ | ✓ | ✓ | ✓ |
| Elasticsearch audit logging | | ✓ | ✓ | ✓ | ✓ |
| Kibana audit logging | | ✓ | ✓ | ✓ | ✓ |
| IP filtering | | ✓ | ✓ | ✓ | ✓ |
| LDAP, PKI[3], Active Directory authentication | | ✓ | ✓ | ✓ | ✓ |
| Elasticsearch Token Service | | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Field- and document-level security | | ✓ | ✓ | | |
| Custom authentication & authorization realms | | ✓ | ✓ | | |
| Encryption at rest support | | ✓ | ✓ | | |
| FIPS 140-3/140-2 mode | | ✓ | ✓ | | |
| Advanced security for remote clusters | | | ✓ | | |
| Elastic Cloud SAML SSO for Cloud Connected clusters | | ✓ | ✓ | | |
| **Alerting** | | | | | |
| Noise reduction capabilities (e.g: Scheduled Snooze, Muting, Deduping, etc.) | ✓ | ✓ | ✓ | ✓ | |
| Maintenance Windows | | ✓ | ✓ | | |
| Tracking containment rule type (geofencing) | | ✓ | ✓ | ✓ | |
| Anomaly detection rule types by Machine Learning | | ✓ | ✓ | | |
| Operational rule type for transforms | ✓ | ✓ | ✓ | ✓ | |

| | | | | | |
|---|---|---|---|---|---|
| Case user assignment | | ✓ | ✓ | | |
| Elastic Connectors (e.g., Server Log and Index) | ✓ | ✓ | ✓ | ✓ | |
| Connectors (Actions) (e.g., email, webhook, Jira, Jira service management, MS Teams, IBM Resilient, OpsGenie, PagerDuty, Slack, ServiceNow®, Tines, Torq, Swimlane, xMatters, D3 Security, TheHive, XSOAR) | | ✓ | ✓ | ✓ | |
| Connectors (Actions) (e.g., OpenAI, Amazon Bedrock, Google Gemini, Sentinel One, CrowdStrike, AI Connector, Microsoft Defender for Endpoint) | | | ✓ | | |
| Watcher | | ✓ | ✓ | ✓ | |
| **Clients** | | | | | |
| REST APIs | ✓ | ✓ | ✓ | ✓ | |
| Language clients | ✓ | ✓ | ✓ | ✓ | |
| Query DSL | ✓ | ✓ | ✓ | ✓ | |
| Console | ✓ | ✓ | ✓ | ✓ | |
| ES-Hadoop | ✓ | ✓ | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Tableau Connector | | ✓ | ✓ | |
| **Localized UI** | | | | |
| English | ✓ | ✓ | ✓ | ✓ |
| Chinese (Simplified) | ✓ | ✓ | ✓ | ✓ |
| French | ✓ | ✓ | ✓ | ✓ |
| Japanese | ✓ | ✓ | ✓ | ✓ |
| German | ✓ | ✓ | ✓ | ✓ |

## MONITORING & DIAGNOSTICS

| | | | | |
|---|---|---|---|---|
| **AutoOps for self-managed clusters via Cloud Connect** | | | | |
| Real-time root cause analysis and resolution steps | ✓ | ✓ | ✓ | |
| Insights on how to improve performance and stability | ✓ | ✓ | ✓ | |
| Resource utilization visibility | ✓ | ✓ | ✓ | |
| Default data retention | ✓ | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Customization of events | ✓ | ✓ | ✓ | |
| **Stack monitoring** | | | | |
| Full-stack monitoring (including Beats and Logstash) | ✓ | ✓ | ✓ | |
| Multi-stack monitoring | | ✓ | ✓ | |
| Configurable retention policy | | ✓ | ✓ | |
| Kibana alerting and actions[4] | ✓ | ✓ | ✓ | |
| Automatic stack issue alerts | ✓ | ✓ | ✓ | |

## SEARCH & ANALYSIS

| | | | | |
|---|---|---|---|---|
| **Full-text search** | | | | |
| Relevance scoring | ✓ | ✓ | ✓ | ✓ |
| Highlighting | ✓ | ✓ | ✓ | ✓ |
| Type ahead | ✓ | ✓ | ✓ | ✓ |
| Corrections | ✓ | ✓ | ✓ | ✓ |
| Suggestions | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Results pinning | ✓ | ✓ | ✓ | ✓ | |
| Dynamically updateable synonyms | ✓ | ✓ | ✓ | ✓ | |
| Query profiler | ✓ | ✓ | ✓ | ✓ | |
| Similarity functions for vector fields | ✓ | ✓ | ✓ | ✓ | |
| Vector search | ✓ | ✓ | ✓ | ✓ | |
| DiskBBQ | | | ✓ | | |
| Rank Vectors (for MaxSim) | | | ✓ | | |
| Doc-value-only fields | ✓ | ✓ | ✓ | ✓ | |
| Synonym management | ✓ | ✓ | ✓ | | |
| Retrievers: Standard, kNN, pinned, rescorer | ✓ | ✓ | ✓ | | |
| Retrievers: linear, rule, RRF, text similarity re-ranker | | | ✓ | | |
| Reciprocal Rank Fusion (RRF) for hybrid search | | | ✓ | | |
| Query Rules | | | ✓ | | |
| Learning to Rank | | | ✓ | | |

| | | | | | |
|---|---|---|---|---|---|
| Aggregations | ✓ | ✓ | ✓ | ✓ | ✓ |
| Boxplot aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cumulative cardinality aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Geoline aggregation | | ✓ | ✓ | ✓ | ✓ |
| Geoshape aggregations | | ✓ | ✓ | ✓ | ✓ |
| Geohexgrid aggregations | | ✓ | ✓ | ✓ | ✓ |
| Geogrid query | ✓ | ✓ | ✓ | ✓ | ✓ |
| Moving percentiles aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Multi terms aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Normalize aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Range aggregation over histogram fields | ✓ | ✓ | ✓ | ✓ | ✓ |
| Random sampler aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rate aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Significant terms aggregation p-value score | ✓ | ✓ | ✓ | ✓ | ✓ |
| String stats aggregation | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| T-test aggregation | ✓ | ✓ | ✓ | ✓ |
| Graph exploration | | ✓ | ✓ | |
| Vector tiles API | ✓ | ✓ | ✓ | ✓ |
| **Query languages** | | | | |
| Elasticsearch SQL APIs & CLI | ✓ | ✓ | ✓ | ✓ |
| Event Query Language (EQL) | ✓ | ✓ | ✓ | ✓ |
| ES\|QL (Elasticsearch Query Language) | ✓ | ✓ | ✓ | ✓ |
| Cross-cluster ES\|QL | | | ✓ | |

## MACHINE LEARNING

| | | | | |
|---|---|---|---|---|
| **Data exploration for machine learning** | | | | |
| Data Visualizer | ✓ | ✓ | ✓ | ✓ |
| File upload wizard | ✓ | ✓ | ✓ | ✓ |
| Data drift | | ✓ | ✓ | |
| Dashboard embeddables | | ✓ | ✓ | |
| **Agent Builder** | | | | |

| | | | | |
|---|---|---|---|---|
| Custom agent creation | | | ✓ | |
| External integration - API/MCP/A2A | | | ✓ | |
| **Anomaly detection** | | | | |
| Single metric and multi-metric | | ✓ | ✓ | |
| Population/entity analysis | | ✓ | ✓ | |
| Log message categorization | | ✓ | ✓ | |
| Rare analysis | | ✓ | ✓ | |
| Root cause indication | | ✓ | ✓ | |
| Forecasting on time series | | ✓ | ✓ | |
| DST support | | ✓ | ✓ | |
| **Data frame analysis** | | | | |
| Outlier detection | | ✓ | ✓ | |
| Regression | | ✓ | ✓ | |
| Classification | | ✓ | ✓ | |
| Feature importance | | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Third party model management, for ML nodes | | ✓ | ✓ | |
| Kibana Space access to models | | ✓ | ✓ | |
| Elastic Learned Sparse Encoder (ELSER) - packaged for ML nodes | | ✓ | ✓ | |
| e5 - packaged for ML nodes | | ✓ | ✓ | |
| Elastic Rerank | | | ✓ | |
| Elastic Inference Service[17] | | | ✓ | |
| Inference API - support for Elastic managed, third party, and self managed embeddings, reranking, and LLM providers | | | ✓ | |
| **AIOps** | | | | |
| Explain log rate spikes | | ✓ | ✓ | |
| Log Pattern Analysis | | ✓ | ✓ | |
| Change Point Detection | | ✓ | ✓ | |

ELASTICSEARCH

| | | | | | |
|---|---|---|---|---|---|
| Search stack monitoring | ✓ | ✓ | ✓ | ✓ | |
| Dashboards for web and search analytics | ✓ | ✓ | ✓ | ✓ | |
| Dev Console | ✓ | ✓ | ✓ | ✓ | |
| Elastic AI Assistant | | | ✓ | | |
| Elastic Workflows | | | ✓ | | |
| **Content Management** | | | | | |
| Content management UI | ✓ | ✓ | ✓ | ✓ | |
| Ingestion pipeline management | | ✓ | ✓ | | |
| Inference processor management | | ✓ | ✓ | | |
| Extraction Service (Beta) | | ✓ | ✓ | | |
| **Machine Learning / AI** | | | | | |
| Third party model management, for ML nodes | | ✓ | ✓ | | |
| Elastic Learned Sparse Encoder (ELSER) - packaged for ML nodes | | ✓ | ✓ | | |
| e5 - packaged for ML nodes | | ✓ | ✓ | | |

| | | | | |
|---|---|---|---|---|
| Inference API - support for Elastic managed, third party, and self managed embeddings, reranking, and LLM providers | | | ✓ | |
| Playground | | | ✓ | |
| **Query and relevance** | | | | |
| Elasticsearch query DSL | ✓ | ✓ | ✓ | ✓ |
| ES\|QL (Elasticsearch Query Language) | ✓ | ✓ | ✓ | ✓ |
| ES\|QL Lookup Joins | ✓ | ✓ | ✓ | ✓ |
| ES\|QL Subqueries in FROM | ✓ | ✓ | ✓ | ✓ |
| ES\|QL JSON Extraction | ✓ | ✓ | ✓ | ✓ |
| ES\|QL Unmapped Fields control | ✓ | ✓ | ✓ | ✓ |
| ES\|QL Data Federation (Experimental, opt-in) | | | ✓ | |
| Language-specific relevance | ✓ | ✓ | ✓ | ✓ |
| Vector search | ✓ | ✓ | ✓ | ✓ |
| Similarity functions for vector fields | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Query rules | | | ✓ | |
| Learning to Rank (LTR) | | | ✓ | |
| Search Applications (beta) | | | ✓ | |
| **Clients** | | | | |
| Language clients (open source) | ✓ | ✓ | ✓ | ✓ |
| Search UI (open source) | ✓ | ✓ | ✓ | ✓ |
| AI ecosystem client integrations (open source) | ✓ | ✓ | ✓ | ✓ |
| Web and search analytics client (Beta) | ✓ | ✓ | ✓ | ✓ |
| **Security** | | | | |
| Encrypted communications | ✓ | ✓ | ✓ | ✓ |
| Role-based access control | ✓ | ✓ | ✓ | ✓ |
| LDAP, PKI[3], Active Directory authentication | | ✓ | ✓ | ✓ |
| Single sign-on (SAML, OpenID Connect, Kerberos, JWT) | | ✓ | ✓ | |
| Encryption at rest support | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Filebeat, Metricbeat, Winlogbeat, Packetbeat[12], Heartbeat, Auditbeat | ✓ | ✓ | ✓ | ✓ |
| Functionbeat | ✓ | ✓ | ✓ | ✓ |
| Real browser-based synthetic monitoring agent | ✓ | ✓ | ✓ | ✓ |
| Logstash | ✓ | ✓ | ✓ | ✓ |
| ES-Hadoop | ✓ | ✓ | ✓ | ✓ |
| File import wizard | ✓ | ✓ | ✓ | ✓ |
| Auto Import | | | ✓ | |
| **Fleet** | | | | |
| Fleet Server | ✓ | ✓ | ✓ | ✓ |
| Fleet app | ✓ | ✓ | ✓ | ✓ |
| Fleet integrations | ✓ | ✓ | ✓ | ✓ |
| Elastic Agent | ✓ | ✓ | ✓ | ✓ |
| Selective agent binary updates | ✓ | ✓ | ✓ | ✓ |
| Scheduled agent binary upgrades | | ✓ | ✓ | |

| | | | | | |
|---|---|---|---|---|---|
| Selective agent unenrollment | ✓ | ✓ | ✓ | ✓ | |
| Per Policy output assignment | | ✓ | ✓ | | |
| Per Integration output assignment | | | ✓ | | |
| Reusable Integration policies | | | ✓ | | |
| Fleet Space Awareness | | | ✓ | | |
| Fleet Multi-Cluster support | | | ✓ | | |
| Fleet Agent Migration to another cluster | | | ✓ | | |

**Data sources - For a full list of integrations available, check out our Integrations page.**

| | | | | |
|---|---|---|---|---|
| Abuse.ch | ✓ | ✓ | ✓ | ✓ |
| Audit system data | ✓ | ✓ | ✓ | ✓ |
| Cisco Firepower | ✓ | ✓ | ✓ | ✓ |
| Check Point Firewall | ✓ | ✓ | ✓ | ✓ |
| Cloudflare | ✓ | ✓ | ✓ | ✓ |
| CrowdStrike Falcon | ✓ | ✓ | ✓ | ✓ |
| Fortinet Fortigate | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Microsoft 365 Defender & Defender for Endpoint | ✓ | ✓ | ✓ | ✓ |
| Microsoft (Office) 365 | ✓ | ✓ | ✓ | ✓ |
| Network Packet Capture | ✓ | ✓ | ✓ | ✓ |
| NetFlow & IPFIX | ✓ | ✓ | ✓ | ✓ |
| Okta | ✓ | ✓ | ✓ | ✓ |
| Palo Alto Networks Cortex XDR | ✓ | ✓ | ✓ | ✓ |
| Palo Alto Networks Firewalls | ✓ | ✓ | ✓ | ✓ |
| SentinelOne | ✓ | ✓ | ✓ | ✓ |
| Tenable | ✓ | ✓ | ✓ | ✓ |
| Zscaler | ✓ | ✓ | ✓ | ✓ |
| **Data transformation** | | | | |
| Index time enrichment | ✓ | ✓ | ✓ | ✓ |
| Processors | ✓ | ✓ | ✓ | ✓ |
| Analyzers | ✓ | ✓ | ✓ | ✓ |
| Tokenizers | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Grok | ✓ | ✓ | ✓ | ✓ | |
| Field transformation | ✓ | ✓ | ✓ | ✓ | |
| External lookup enrichment | ✓ | ✓ | ✓ | ✓ | |
| Circle ingest processor | ✓ | ✓ | ✓ | ✓ | |
| Match & Geo-match enrich processor[10] | ✓ | ✓ | ✓ | ✓ | |
| Support for MaxMind commercial databases | | | ✓ | | |
| Support for IPinfo commercial databases | | | ✓ | | |
| Redact ingest processor | | ✓ | ✓ | | |
| **Elastic Common Schema** | | | | | |
| Elastic Common Schema | ✓ | ✓ | ✓ | ✓ | |
| **Content Integrations[16]** | | | | | |
| Elastic open web crawler | | ✓ | ✓ | ✓ | |
| Connector Framework | ✓ | ✓ | ✓ | ✓ | |
| Connector API | ✓ | ✓ | ✓ | ✓ | |
| Elastic Azure Blob Storage connector | | ✓ | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Elastic Confluence Data Center connector | | ✓ | ✓ | ✓ |
| Elastic Dropbox connector | | ✓ | ✓ | ✓ |
| Elastic GitHub & GitHub Enterprise Server connector | | ✓ | ✓ | ✓ |
| Elastic Gmail connector | | ✓ | ✓ | ✓ |
| Elastic Google Cloud Storage connector | | ✓ | ✓ | ✓ |
| Elastic Google Drive connector | | ✓ | ✓ | ✓ |
| Elastic GraphQL connector | | ✓ | ✓ | ✓ |
| Elastic Jira Cloud & Server connector | | ✓ | ✓ | ✓ |
| Elastic Jira Data Center connector | | ✓ | ✓ | ✓ |
| Elastic MongoDB connector | | ✓ | ✓ | ✓ |
| Elastic Microsoft SQL connector | | ✓ | ✓ | ✓ |
| Elastic MySQL connector | | ✓ | ✓ | ✓ |
| Elastic Network Drive connector | | ✓ | ✓ | ✓ |
| Elastic Notion connector | | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Elastic Outlook connector | | ✓ | ✓ | ✓ |
| Elastic PostgreSQL connector | | ✓ | ✓ | ✓ |
| Elastic Redis connector | | ✓ | ✓ | ✓ |
| Elastic S3 connector | | ✓ | ✓ | ✓ |
| Elastic Salesforce connector | | ✓ | ✓ | ✓ |
| Elastic ServiceNow connector | | ✓ | ✓ | ✓ |
| Elastic SharePoint Online connector | | ✓ | ✓ | ✓ |
| Elastic SharePoint Server connector | | ✓ | ✓ | ✓ |
| Elastic Slack connector | | ✓ | ✓ | ✓ |
| Elastic Teams connector | | ✓ | ✓ | ✓ |
| Elastic Zoom connector | | ✓ | ✓ | ✓ |

## DATA EXPLORATION & VISUALIZATION

**Visualizations**

| | | | | |
|---|---|---|---|---|
| Time series | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Tables | ✓ | ✓ | ✓ | ✓ | |
| Tag cloud | ✓ | ✓ | ✓ | ✓ | |
| Custom (Vega) | ✓ | ✓ | ✓ | ✓ | |
| Lens | ✓ | ✓ | ✓ | ✓ | |
| **Data exploration** | | | | | |
| ES\|QL (Elasticsearch Query Language) | ✓ | ✓ | ✓ | ✓ | |
| Dashboards | ✓ | ✓ | ✓ | ✓ | |
| Drilldown between dashboards | ✓ | ✓ | ✓ | ✓ | |
| Drilldown to URL | | ✓ | ✓ | ✓ | |
| Discover | ✓ | ✓ | ✓ | ✓ | |
| Console | ✓ | ✓ | ✓ | ✓ | |
| Kibana query autocomplete | ✓ | ✓ | ✓ | ✓ | |
| Kibana runtime fields editor | ✓ | ✓ | ✓ | ✓ | |
| Run search sessions in background | ✓ | ✓ | ✓ | ✓ | |
| Graph analytics | | ✓ | ✓ | | |

| | | | | |
|---|---|---|---|---|
| Embeddable dashboards | ✓ | ✓ | ✓ | ✓ |
| Anonymous access control (public sharing) | ✓ | ✓ | ✓ | ✓ |
| CSV exports | ✓ | ✓ | ✓ | ✓ |
| PDF and PNG reports | | ✓ | ✓ | ✓ |
| Saved queries | ✓ | ✓ | ✓ | ✓ |
| **Content management** | | | | |
| Kibana Spaces | ✓ | ✓ | ✓ | ✓ |
| Custom banners | | ✓ | ✓ | ✓ |
| Custom branding | | | ✓ | |
| Object export UI & APIs | ✓ | ✓ | ✓ | ✓ |
| Tags | ✓ | ✓ | ✓ | ✓ |
| Navigational search | ✓ | ✓ | ✓ | ✓ |

## ELASTIC OBSERVABILITY

| | | | | |
|---|---|---|---|---|
| Observability overview | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Service Level Objectives (SLOs) | | | ✓ | ✓ | |
| Kibana alerting and actions[5] | | ✓ | ✓ | ✓ | ✓ |
| Elastic AI Assistant | | | | ✓ | |
| Universal Profiling | | | | ✓ | |
| LLM Observability | | ✓ | ✓ | ✓ | ✓ |
| AI-assisted pipelines and parsing with Streams | | | ✓ | ✓ | |
| Elastic Workflows | | | | ✓ | |

**ELASTIC APM**

| | | | | | |
|---|---|---|---|---|---|
| APM Server | | ✓ | ✓ | ✓ | ✓ |
| Jaeger intake | | ✓ | ✓ | ✓ | ✓ |
| OpenTelemetry intake for traces and metrics | | ✓ | ✓ | ✓ | ✓ |
| APM app | | ✓ | ✓ | ✓ | ✓ |
| Distributed tracing | | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Correlations | | ✓ | ✓ | |
| Synthetic _source for APM indices | 15 | 15 | ✓ | 15 |
| LLM tracing | ✓ | ✓ | ✓ | ✓ |
| **APM agents** | | | | |
| Java | ✓ | ✓ | ✓ | ✓ |
| .NET | ✓ | ✓ | ✓ | ✓ |
| Go | ✓ | ✓ | ✓ | ✓ |
| Ruby | ✓ | ✓ | ✓ | ✓ |
| RUM (JavaScript) | ✓ | ✓ | ✓ | ✓ |
| PHP | ✓ | ✓ | ✓ | ✓ |
| Python | ✓ | ✓ | ✓ | ✓ |
| Node | ✓ | ✓ | ✓ | ✓ |
| **Integrations** | | | | |
| Elastic Logs, Metrics | ✓ | ✓ | ✓ | ✓ |
| Kibana alerting and actions[5] | ✓ | ✓ | ✓ | ✓ |

| ELASTIC LOGS | | | | |
|---|---|---|---|---|
| Log shipper (Filebeat) | ✓ | ✓ | ✓ | ✓ |
| Dashboards for common data sources | ✓ | ✓ | ✓ | ✓ |
| Logs app | ✓ | ✓ | ✓ | ✓ |
| Logsdb indices for logs | ✓ | ✓ | ✓ | ✓ |
| Synthetic _source for logsdb indices | 15 | 15 | ✓ | 15 |
| Custom routing on sort fields for logsdb | | | ✓ | |
| Pattern-based Compression for log messages | | | ✓ | |
| Columnar indices for logs (Tech Preview) | ✓ | ✓ | ✓ | ✓ |
| Synthetic columnar _source for logs (Tech Preview) | | | ✓ | |
| **Integrations** | | | | |
| Elastic APM, Synthetic Monitoring private locations | ✓ | ✓ | ✓ | ✓ |
| Kibana alerting and actions[5] | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| **ELASTIC METRICS** | | | | |
| Metric shipper (Metricbeat) | ✓ | ✓ | ✓ | ✓ |
| Dashboards for common data sources | ✓ | ✓ | ✓ | ✓ |
| Metrics app | ✓ | ✓ | ✓ | ✓ |
| Time series indices for metrics (TSDB) | ✓ | ✓ | ✓ | ✓ |
| Synthetic _source for time series indices | 15 | 15 | ✓ | 15 |
| Downsampling | ✓ | ✓ | ✓ | ✓ |
| **Integrations** | | | | |
| Elastic Logs, APM | ✓ | ✓ | ✓ | ✓ |
| Kibana alerting and actions[5] | ✓ | ✓ | ✓ | ✓ |
| Machine learning | | ✓ | ✓ | |
| **ELASTIC SYNTHETIC MONITORING** | | | | |
| Synthetic Monitoring UI | ✓ | ✓ | ✓ | ✓ |
| Project Monitors | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Point and Click Script Recorder | ✓ | ✓ | ✓ | ✓ |
| **Integrations** | | | | |
| Elastic Logs, Metrics, APM | ✓ | ✓ | ✓ | ✓ |
| Kibana alerting and actions[5] | ✓ | ✓ | ✓ | ✓ |
| Machine learning | | ✓ | ✓ | |
| **ELASTIC SECURITY** | | | | |
| Elastic Common Schema | ✓ | ✓ | ✓ | ✓ |
| Extended detection and response (XDR) | ✓ | ✓ | ✓ | ✓ |
| Security information and event management (SIEM) | ✓ | ✓ | ✓ | ✓ |
| Host security analysis | ✓ | ✓ | ✓ | ✓ |
| Network security analysis | ✓ | ✓ | ✓ | ✓ |
| User security analysis | ✓ | ✓ | ✓ | ✓ |
| Timeline event explorer | ✓ | ✓ | ✓ | ✓ |
| Case management | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Prebuilt detection rules import/export | ✓ | ✓ | ✓ | | |
| Prebuilt detection rules customization | | | ✓ | | |
| Detection alerts suppression | | ✓ | ✓ | | |
| Analyst Insights | | ✓ | ✓ | | |
| Detection alert external actions | | ✓ | ✓ | ✓ | |
| Machine learning anomaly detection | | ✓ | ✓ | | |
| Prebuilt anomaly detection jobs | | ✓ | ✓ | | |
| Attack Discovery | | | ✓ | | |
| Malware prevention | ✓ | ✓ | ✓ | ✓ | |
| Admin-defined endpoint blocklist | ✓ | ✓ | ✓ | ✓ | |
| Ransomware prevention | | ✓ | ✓ | | |
| Malicious behavior protection | | ✓ | ✓ | | |
| Memory threat protection | | ✓ | ✓ | | |
| Self healing | | ✓ | ✓ | | |
| Host Isolation | | ✓ | ✓ | | |

| | | | | |
|---|---|---|---|---|
| Elastic AI Assistant | | | ✓ | |
| Agent Builder for Security | | | ✓ | |
| Threat intelligence management | | | ✓ | |
| Customizable on-endpoint protection notifications | | ✓ | ✓ | |
| Cloud and Kubernetes Security Posture Management (K/CSPM) | | | ✓ | |
| Workload session auditing | | | ✓ | |
| Device Control | | | ✓ | |
| Automatic Migration | | | ✓ | |
| Manual rule runs | ✓ | ✓ | ✓ | ✓ |
| Rule gaps information | ✓ | ✓ | ✓ | ✓ |
| Automatic rule gaps fill | | | ✓ | |
| Entity Store | ✓ | ✓ | ✓ | |
| Entity Analytics (Risk Score, Entity Graph, Watchlist) | | ✓ | ✓ | |
| Advanced Entity Analytics (AI Skill, Entity | | | ✓ | |

| | | | | |
|---|---|---|---|---|
| Elastic Workflows | | | ✓ | |
| **Integrations** | | | | |
| Elastic Agent | ✓ | ✓ | ✓ | ✓ |
| Elastic APM | ✓ | ✓ | ✓ | ✓ |
| IPinfo Commercial Database | | | ✓ | |
| Elastic Maps | ✓ | ✓ | ✓ | ✓ |
| Kibana Alerts and Actions[5] | ✓ | ✓ | ✓ | ✓ |
| Response actions on 3rd-party endpoint solutions | | | ✓ | |
| Osquery Manager | ✓ | ✓ | ✓ | ✓ |
| Network Packet Capture[12] | ✓ | ✓ | ✓ | ✓ |
| Threat intelligence feeds and platforms | ✓ | ✓ | ✓ | ✓ |
| Atlassian Jira | | ✓ | ✓ | ✓ |
| Swimlane SOAR | | ✓ | ✓ | ✓ |
| IBM Resilient | | ✓ | ✓ | |
| ServiceNow ITOM, ITSM, SecOps | | ✓ | ✓ | |

| | | | | |
|---|---|---|---|---|
| Machine learning | | ✓ | ✓ | |

## ELASTIC MAPS

| | | | | |
|---|---|---|---|---|
| **Elastic Maps Service**[6] | | | | |
| Base layer maps | ✓ | ✓ | ✓ | ✓ |
| Elastic Maps Server[11] | | | ✓ | |
| **Maps app** | | | | |
| Shapefile and GeoJSON upload | ✓ | ✓ | ✓ | ✓ |
| Multiple layers | ✓ | ✓ | ✓ | ✓ |
| Native vector tile support | ✓ | ✓ | ✓ | ✓ |
| Layer-based filtering | ✓ | ✓ | ✓ | ✓ |
| Client-side styling | ✓ | ✓ | ✓ | ✓ |
| Individual points and shapes | ✓ | ✓ | ✓ | ✓ |
| Geo aggregations | ✓ | ✓ | ✓ | ✓ |
| Embed Maps in dashboard | ✓ | ✓ | ✓ | ✓ |
| Tracking alerts | | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Display up to 24 zoom levels | ✓ | ✓ | ✓ | ✓ |
| Custom raster and vector tile service support | ✓ | ✓ | ✓ | ✓ |
| Kibana Alerts: tracking containment (geofencing) | | ✓ | ✓ | ✓ |

## ORCHESTRATION

**Elastic Cloud Enterprise**

| | | | | |
|---|---|---|---|---|
| Deploy anywhere: bare metal, VMs, private or public cloud | | | ✓ | |
| Centrally provision, manage, and monitor multiple clusters | | | ✓ | |
| Resource tagging, and tag-based deployment configuration | | | ✓ | |
| Online same-day version updates | | | ✓ | |
| Single-click upgrades & scaling | | | ✓ | |
| User and role management | | | ✓ | |
| Automated periodic snapshots | | | ✓ | |

| | | | | |
|---|---|---|---|---|
| Cross-cluster search and replication across ECE installations | | | ✓ | |
| Deployment autoscaling | | | ✓ | |
| Advanced security for remote clusters | | | ✓ | |
| **Elastic Cloud on Kubernetes**[4] | | | | |
| Deploy Elasticsearch, Kibana, and APM Server, Beats, Enterprise tier, and Elastic Agent on Kubernetes | ✓ | | ✓ | |
| Deploy Search and Elastic Maps Server on Kubernetes | | | ✓ | |
| Provision, manage, and monitor multiple clusters | ✓ | | ✓ | |
| Default Elastic Stack security and authentication for every deployment | ✓ | | ✓ | |
| Single command upgrades and scaling | ✓ | | ✓ | |
| Cross-cluster replication and search within or outside of a Kubernetes cluster | | | ✓ | |
| Autoscaling Elasticsearch and Machine learning nodes | | | ✓ | |

| | | | | |
|---|---|---|---|---|
| Target initial response times | | Critical: 1 hr<br>L2: 4 hrs<br>L3: 1 business day | Critical: 1 hr<br>L2: 4 hrs<br>L3: 1 business day | Critical: 4 hrs<br>L2: 1 day<br>L3: 2 days |
| Unlimited # of incidents | | ✓ | ✓ | ✓ |
| Unlimited # of projects | | | ✓ | |
| Support contacts[7] | | 8 | 8 | 6 |
| Web and phone support | | ✓ | ✓ | ✓ |
| Emergency patches | | ✓ | ✓ | |

*[1] For a more detailed discussion of our licensing options and 2021 licensing changes, please refer to the **licensing FAQ on our website**.*

*[2] Available under the Elastic License. Select features are also available under SSPL or Apache License 2.0. For questions about which features may be licensed under SSPL and Apache License 2.0, please contact **elastic_license@elastic.co**.*

*[3] Feature is currently not available in deployments on Elastic Cloud Enterprise.*

*[4] Customers whose Enterprise subscriptions use ECE/ECE Instances as the billing metric must agree to additional terms before they can access the Enterprise-level features listed in this section. Please **contact us**.*

*[5] Refer to the Alerting section (Kibana Alerts and Kibana Actions items) for further details. Alerting rules based on anomaly detection or SLOs are only available on Platinum and Enterprise tiers.*

*[6] **Elastic Maps Service - Terms of Service***

*[7] Elastic Certified Professionals can be added as additional Support contacts on paid subscriptions at no additional charge.*

*[8] Access to administering Kibana subfeature privileges start at the Gold tier and are available on a per-feature basis matching the feature's subscriptions tier.*

*[9] Gold Subscription tier is no longer available for new customers, try Elastic Cloud Gold instead. Customers with existing Gold Subscriptions will continue to be supported through the end of its current subscription term.*

*[10] **Elastic GeoIP Database Service Agreement***

*[11] Subject to Elastic Vector Tiles Data License Agreement*

*locations.*

*[15] Synthetic _source is an Enterprise feature from 8.17 onward.*

*[16] Updates provided through this subscription page exclude End-of-Life (EOL) products such as Enterprise Search or included features such as App Search, Workplace Search, Elastic web crawler or native connectors. For more details on discontinued products, please consult our **product subscription archive**.*

*[17] Additional usage charges apply.*

*[18] Platinum Subscription tier is no longer available for new customers, try Elastic Cloud Serverless or Elastic Cloud Platinum instead. Customers with existing Platinum Subscriptions can continue to expand or renew. Any future changes to the Platinum tier will be communicated to customers.*

*[19]Cross-cluster operations require the same subscription tier for all involved clusters.*

*The list above reflects the features available in the latest version of the Elastic Stack. Any features or functions of services or products referenced on this page or other pages, or in any presentations, press releases or public statements, which are not currently available or not currently available as a GA release, may not be delivered on time or at all. The development, release, and timing of any features or functionality described for our products remains at our sole discretion. Customers who purchase our products and services should make the purchase decisions based upon services and product features and functions that are currently available.*

Download PDF Version or Previous Versions Available Here
RSS

FOLLOW US

About Elastic
Leadership
Blog
Newsroom

JOIN US

Careers
Career portal
How we hire

Find a partner
Partner login
Request access
Become a partner

TRUST & SECURITY

Legal
Trust center
Privacy at Elastic
Trade Compliance
Ethics & Compliance

Investor resources
Governance
Financials
Stock

EXCELLENCE AWARDS

Previous winners
Elastic{ON} Tour
Become a sponsor
All events