Elastic Cloud managed service features

Elastic Cloud gives you the flexibility to run where you want. Deploy our managed service on Google Cloud, Microsoft Azure, or Amazon Web Services, and we'll handle the maintenance and upkeep for you.

Managed Elasticsearch and Kibana	✓	✓	✓	✓
Deployment autoscaling	✓	✓	✓	✓
Same day version availability	✓	✓	✓	✓
Instant access to security patches	✓	✓	✓	✓
Single-click deployment upgrades	✓	✓	✓	✓
In-place configuration change	✓	✓	✓	✓
Deployment templates	✓	✓	✓	✓
Hot-warm-cold architecture, with automated index curation	✓	✓	✓	✓
Hot-warm-cold architecture, with automated index curation and searchable snapshots	—	—	—	✓
Frozen data tier with automated index curation and searchable snapshots	—	—	—	✓
Automated snapshots (configurable, default every 30 minutes)	✓	✓	✓	✓
REST API for deployment management	✓	✓	✓	✓
REST API support in ecctl CLI, Golang SDK, and generated SDKs	✓	✓	✓	✓
Providers: AWS, Azure, Google Cloud	✓	✓	✓	✓
FedRAMP authorized at Moderate Impact level on AWS GovCloud (US)[2]	✓	✓	✓	✓
High availability across zones	✓	✓	✓	✓
Console signup with Google Account	✓	✓	✓	✓
Console signup with Microsoft Account	✓	✓	✓	✓
Multi-factor authentication	✓	✓	✓	✓
Multi-user management	✓	✓	✓	✓
Role-based access control	✓	✓	✓	✓
Elastic Cloud SAML single sign-on (SSO)	—	—	—	✓
AWS Marketplace billing integration	✓	✓	✓	✓
Microsoft Azure Marketplace billing integration	✓	✓	✓	✓
Google Cloud Marketplace billing integration	✓	✓	✓	✓
AWS PrivateLink integration	✓	✓	✓	✓
Azure Private Link integration	✓	✓	✓	✓
Google Cloud Private Service Connect integration	✓	✓	✓	✓
Encryption at rest with AWS KMS keys	—	—	—	✓
Encryption at rest with Azure Key Vault keys	—	—	—	✓
Encryption at rest with GCP KMS keys	—	—	—	✓
IP filtering	✓	✓	✓	✓
SOC 2 and CSA Star 2 compliance	✓	✓	✓	✓
HIPAA BAA ready	✓	✓	✓	✓
ISO 27001/27017/27018	✓	✓	✓	✓

AutoOps

Real-time root cause analysis and resolution steps	✓	✓	✓	✓
Insights on how to improve performance and stability	✓	✓	✓	✓

Resource utilization visibility	✓	✓	✓	✓
Default data retention	✓	✓	✓	✓
Notifications to alerting and messaging frameworks (Slack, MS teams, PD, custom webhooks, and more)	✓	✓	✓	✓
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	✓	✓	✓	✓

Storage types

Inverted index (for search)	✓	✓	✓	✓
Evaluating calculated fields at index time	✓	✓	✓	✓
Runtime fields	✓	✓	✓	✓
Lookup runtime fields	✓	✓	✓	✓
Document store (for unstructured)	✓	✓	✓	✓
Columnar store (for analytics)	✓	✓	✓	✓
Doc-values only fields	✓	✓	✓	✓
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	—[13]	—[13]	—[13]	✓

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	✓	✓	✓	✓

Stack management

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

Scalability & resiliency

Clustering and high availability	✓	✓	✓	✓
Cluster rebalancing	✓	✓	✓	✓
Advanced cluster rebalancing[11]	✓	✓	✓	✓
Cross-region cross-cluster replication	—	—	—	✓
Same-region cross-cluster replication	—	—	✓	✓
Cross-environment cross-cluster replication	—	—	—	✓
Cross-region cross-cluster search	—	—	—	✓
Same-region cross-cluster search	✓	✓	✓	✓
Cross-environment cross-cluster search	—	—	—	✓

Dedicated master nodes	✓	✓	✓	✓
Dedicated coordinating nodes	✓	✓	✓	✓

Elastic Stack security

Secure settings	✓	✓	✓	✓
Data encryption at rest	✓	✓	✓	✓
Encrypted node-to-node communications	✓	✓	✓	✓
Role-based access control	✓	✓	✓	✓
Anonymous access control (public sharing)	✓	✓	✓	✓
Native authentication	✓	✓	✓	✓
Kibana Spaces	✓	✓	✓	✓
Kibana feature controls	✓	✓	✓	✓
Kibana subfeature privileges[8]	—	—	✓	✓
Prelogin access agreement	—	—	✓	✓
API Keys management	✓	✓	✓	✓
Elasticsearch Token Service	✓	✓	✓	✓
Single sign-on (SAML, OpenID Connect, Kerberos, JWT)	—	—	✓	✓
Attribute-based access control	—	—	✓	✓
Field- and document-level security	—	—	✓	✓
Advanced security for remote clusters	—	—	—	✓
Custom authentication and authorization realms	—	—	✓	✓

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	✓	✓	✓	✓
Search threshold rule types for Discover	✓	✓	✓	✓
Case Management	✓	✓	✓	✓
Case user assignment	—	—	✓	✓
Elastic Connectors (e.g., Server Log and Index)	✓	✓	✓	✓
Connectors (Actions) (e.g., email, webhook, Jira, MS Teams, OpsGenie, PagerDuty, Slack, IBM Resilient, ServiceNow®, Tines, Torq)	—	✓	✓	✓
Watcher	✓	✓	✓	✓

Clients

REST APIs	✓	✓	✓	✓
Language clients	✓	✓	✓	✓
Query DSL	✓	✓	✓	✓
Console	✓	✓	✓	✓
JDBC client	—	—	✓	✓
ODBC client	—	—	✓	✓
Tableau Connector	—	—	✓	✓

Localized UI

English	✓	✓	✓	✓
Chinese (Simplified)	✓	✓	✓	✓
French	✓	✓	✓	✓
Japanese	✓	✓	✓	✓

Custom plugins

Custom plugins	—	✓	✓	✓

Full-text search

Relevance scoring	✓	✓	✓	✓
Highlighting	✓	✓	✓	✓
Type ahead	✓	✓	✓	✓
Corrections	✓	✓	✓	✓
Suggestions	✓	✓	✓	✓

Percolations	✓	✓	✓	✓
Async search	✓	✓	✓	✓
Results pinning	✓	✓	✓	✓
Query profiler	✓	✓	✓	✓
Dynamically updateable synonyms	✓	✓	✓	✓
Similarity functions for vector fields	✓	✓	✓	✓
Vector search	✓	✓	✓	✓
Semantic search	—	—	✓	✓
Reciprocal Rank Fusion (RRF)	—	—	—	✓
Synonym management	✓	✓	✓	✓
Query Rules	—	—	—	✓
Learning to Rank	—	—	—	✓
Retrievers	✓	✓	✓	✓

Analytics

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	✓	✓	✓	✓
Top metrics aggregation	✓	✓	✓	✓
T-test aggregation	✓	✓	✓	✓
Graph exploration	—	—	✓	✓
Vector tiles API	✓	✓	✓	✓

Query languages

Elasticsearch SQL APIs	✓	✓	✓	✓
Event Query Language (EQL)	✓	✓	✓	✓
ES|QL (Elasticsearch Query Language)	✓	✓	✓	✓
Cross-cluster ES|QL - Tech Preview	—	—	—	✓

Data exploration for machine learning

Data Visualizer	✓	✓	✓	✓
File upload wizard	✓	✓	✓	✓
Data drift	—	—	✓	✓
Dashboard embeddables	—	✓	✓	—

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	—	—	✓	✓

Inference and model management

Language identification	✓	✓	✓	✓
Third party model management	—	—	✓	✓
Kibana space model separation	—	—	✓	✓
Elastic Learned Sparse Encoder (ELSER) for AI Search	—	—	✓	✓
Elastic Reranker model for AI search	—	—	—	✓
Inference API - Elastic managed (ELSER, e5, Elastic Rerank)	—	—	—	✓
Inference API - completion integrations: Amazon Bedrock, Azure AI Studio, Azure OpenAI, Cohere, Google AI Studio, OpenAI	—	—	—	✓
Inference API - embedding integrations: Amazon Bedrock, Azure AI Studio, Azure OpenAI, Cohere, Google AI Studio, Google Vertex AI, Hugging Face, Mistral, OpenAI	—	—	—	✓
Inference API - rerank integrations: Cohere, Google Vertex AI	—	—	—	✓
Playground (tech preview)	—	—	—	✓
Inference API - streaming support	—	—	—	✓

AIOps

Explain log rate spikes	—	—	✓	✓
Log Pattern Analysis	—	—	✓	✓
Change Point Detection	—	—	✓	✓

Search server	✓	✓	✓	✓
Search management UI	✓	✓	✓	✓
Search stack monitoring	✓	✓	✓	✓
Dashboards for web and search analytics	✓	✓	✓	✓
Embedded Dev Console	✓	✓	✓	✓
AI Assistant for Search	—	—	—	✓

Content Management

Content management UI	✓	✓	✓	✓
Ingestion pipeline management	✓	✓	✓	✓
Inference processor management	—	—	✓	✓
Extraction Service (Beta)	—	—	✓	✓

Machine Learning / AI

Third party model management	—	—	✓	✓
Inference API - Elastic managed (ELSER, e5 and Elastic Rerank)	—	—	—	✓
Inference API - completion integrations: Amazon Bedrock, Azure AI Studio, Azure OpenAI, Cohere, Google AI Studio, OpenAI	—	—	—	✓
Inference API - embedding integrations: Amazon Bedrock, Azure AI Studio, Azure OpenAI, Cohere, Google AI Studio, Google Vertex AI, Hugging Face, Mistral, OpenAI, Watson.x AI, Alibaba	—	—	—	✓
Inference API - rerank integrations: Cohere, Google Vertex AI	—	—	—	✓
Playground (tech preview)	—	—	—	✓

Query and relevance

Search Applications	—	—	✓	✓
Elasticsearch query DSL	✓	✓	✓	✓
ES|QL (Elasticsearch Query Language)	✓	✓	✓	✓
Language-specific relevance	✓	✓	✓	✓
Vector search	✓	✓	✓	✓
Semantic search	—	—	✓	✓
Similarity functions for vector fields	✓	✓	✓	✓
Reciprocal Rank Fusion (RRF)	—	—	—	✓
Synonym management	✓	✓	✓	✓
Query Rules	—	—	—	✓
Behavioral analytics	—	—	✓	✓
Learning to Rank	—	—	—	✓
Retrievers	✓	✓	✓	✓

Native Integrations

Web crawler for Elasticsearch	✓	✓	✓	✓
Azure Blob Storage connector	✓	✓	✓	✓
Box connector	✓	✓	✓	✓

Box connector	✓	✓	✓	✓
Confluence Cloud & Server connector	✓	✓	✓	✓
Confluence Data Center connector	✓	✓	✓	✓
Dropbox connector	✓	✓	✓	✓
GitHub & GitHub Enterprise Server connector	✓	✓	✓	✓
Gmail connector	✓	✓	✓	✓
Google Cloud Storage connector	✓	✓	✓	✓
Google Drive connector	✓	✓	✓	✓
Jira Cloud & Server connector	✓	✓	✓	✓
Jira Data Center connector	✓	✓	✓	✓
MongoDB connector	✓	✓	✓	✓
Microsoft SQL connector	✓	✓	✓	✓
MySQL connector	✓	✓	✓	✓
Network Drive connector	✓	✓	✓	✓
Notion connector	✓	✓	✓	✓
OneDrive connector	✓	✓	✓	✓
Oracle connector	✓	✓	✓	✓
Outlook connector	✓	✓	✓	✓
PostgreSQL connector	✓	✓	✓	✓
S3 connector	✓	✓	✓	✓
Salesforce connector	✓	✓	✓	✓
ServiceNow connector	✓	✓	✓	✓
Sharepoint Online connector	✓	✓	✓	✓
Slack connector	✓	✓	✓	✓
Teams connector	✓	✓	✓	✓
Zoom connector	✓	✓	✓	✓

Client Integrations

Elastic open web crawler	✓	✓	✓	✓
Connector Framework	✓	✓	✓	✓
Connector API	✓	✓	✓	✓
Azure Blob Storage connector client	✓	✓	✓	✓
Box connector client	✓	✓	✓	✓
Confluence Cloud & Server connector client	✓	✓	✓	✓
Confluence Data Center connector client	✓	✓	✓	✓
Dropbox connector client	✓	✓	✓	✓
GitHub & GitHub Enterprise Server connector client	✓	✓	✓	✓
Gmail connector client	✓	✓	✓	✓
Google Cloud Storage connector client	✓	✓	✓	✓
Google Drive connector client	✓	✓	✓	✓
GraphQL connector client	✓	✓	✓	✓
Jira Cloud & Server connector client	✓	✓	✓	✓
Jira Data Center connector client	✓	✓	✓	✓
MongoDB connector client	✓	✓	✓	✓
Microsoft SQL connector client	✓	✓	✓	✓
MySQL connector client	✓	✓	✓	✓
Network Drive connector client	✓	✓	✓	✓
Notion connector client	✓	✓	✓	✓
OneDrive connector client	✓	✓	✓	✓
OpenText Documentum connector client	✓	✓	✓	✓
Oracle connector client	✓	✓	✓	✓
Outlook connector client	✓	✓	✓	✓
PostgreSQL connector client	✓	✓	✓	✓
Redis connector client	✓	✓	✓	✓
S3 connector client	✓	✓	✓	✓
Salesforce connector client	✓	✓	✓	✓
ServiceNow connector client	✓	✓	✓	✓
SharePoint Online connector client	✓	✓	✓	✓
Sharepoint Server connector client	✓	✓	✓	✓
Slack connector client	✓	✓	✓	✓

Teams connector client	✓	✓	✓	✓
Zoom connector client	✓	✓	✓	✓
Clients				
Language clients	✓	✓	✓	✓
Search UI (open source)	✓	✓	✓	✓
Web and search analytics client (Beta)	✓	✓	✓	✓
Security				
Encrypted communications	✓	✓	✓	✓
Role-based access control	✓	✓	✓	✓
Single sign-on (SAML, OpenID Connect, Kerberos, JWT)	—	—	✓	✓
Encryption at rest support	✓	✓	✓	✓

Ingest products & features				
Filebeat, Metricbeat, Winlogbeat, Packetbeat[10], Heartbeat, Auditbeat, real browser-based synthetic monitoring agent (Beta)	✓	✓	✓	✓
Functionbeat	✓	✓	✓	✓
Logstash	✓	✓	✓	✓
ES-Hadoop	✓	✓	✓	✓
File import wizard	✓	✓	✓	✓
Auto Import (Tech Preview)	—	—	—	✓
Fleet				
Fleet Server	✓	✓	✓	✓
Fleet app	✓	✓	✓	✓
Fleet integrations	✓	✓	✓	✓
Elastic Agent	✓	✓	✓	✓
Selective agent binary updates	✓	✓	✓	✓
Scheduled agent binary upgrades	—	✓	✓	✓
Selective agent policy reassignment	✓	✓	✓	✓
Selective agent unenrollment	✓	✓	✓	✓
Per Policy output assignment	—	✓	✓	✓
Per Integration output assignment	—	—	—	✓
Reusable Integration policies	—	—	—	✓
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	✓	✓	✓	✓
File Integrity Monitoring	✓	✓	✓	✓
Google Workspace	✓	✓	✓	✓
Microsoft 365 Defender & Defender for Endpoint	✓	✓	✓	✓
Microsoft (Office) 365	✓	✓	✓	✓
Network Packet Capture	✓	✓	✓	✓
NetFlow and IPFIX	✓	✓	✓	✓
Okta	✓	✓	✓	✓
Palo Alto Networks Cortex XDR	✓	✓	✓	✓
Palo Alto Networks Firewalls	✓	✓	✓	✓
SentinelOne	✓	✓	✓	✓
Tenable	✓	✓	✓	✓
Zscaler	✓	✓	✓	✓
Data transformation				
Index time enrichment	✓	✓	✓	✓
Processors	✓	✓	✓	✓
Analyzers	✓	✓	✓	✓
Tokenizers	✓	✓	✓	✓
Filters	✓	✓	✓	✓

Filter on ANN - vector Search	✓	✓	✓	✓
Grok	✓	✓	✓	✓
Field transformation	✓	✓	✓	✓
External lookup enrichment	✓	✓	✓	✓
Circle ingest processor	✓	✓	✓	✓
Match and geo-match enrich processor[9]	✓	✓	✓	✓
Support for MaxMind commercial databases	—	—	—	✓
Support for IPinfo commercial databases	—	—	—	✓
Redact ingest processor	—	—	✓	✓

Elastic Common Schema

Elastic Common Schema	✓	✓	✓	✓

Visualizations

Time series	✓	✓	✓	✓
Geo	✓	✓	✓	✓
Metrics	✓	✓	✓	✓
Tables	✓	✓	✓	✓
Tag cloud	✓	✓	✓	✓
Custom (Vega)	✓	✓	✓	✓
Lens	✓	✓	✓	✓

Data exploration

ES|QL (Elasticsearch Query Language)	✓	✓	✓	✓
Dashboards	✓	✓	✓	✓
Drilldown between dashboards	✓	✓	✓	✓
Drilldown to URL	—	✓	✓	✓
Discover	✓	✓	✓	✓
Field statistics (Beta)	✓	✓	✓	✓
Console	✓	✓	✓	✓
Kibana query autocomplete	✓	✓	✓	✓
Kibana runtime fields editor	✓	✓	✓	✓
Run search sessions in background	✓	✓	✓	✓
Graph analytics	—	—	✓	✓
Data views	✓	✓	✓	✓

Canvas

Canvas	✓	✓	✓	✓
Canvas shareables	✓	✓	✓	✓

Share & collaborate

Embeddable dashboards	✓	✓	✓	✓
Anonymous access control (public sharing)	✓	✓	✓	✓
CSV exports	✓	✓	✓	✓
PDF and PNG reports	—	✓	✓	✓
Saved queries	✓	✓	✓	✓

Content management

Kibana Spaces	✓	✓	✓	✓
Custom banners	—	✓	✓	✓
Object export UI & APIs	✓	✓	✓	✓
Tags	✓	✓	✓	✓
Navigational search	✓	✓	✓	✓

Observability overview	✓	✓	✓	✓
User Experience overview	✓	✓	✓	✓
Curated ad hoc data exploration	✓	✓	✓	✓
Service Level Objectives (SLOs)	—	—	✓	✓
Kibana alerting and actions[4]	✓	✓	✓	✓
Universal Profiling	✓	✓	✓	✓
Elastic AI Assistant	—	—	—	✓

Elastic APM

APM server	✓	✓	✓	✓
Jaeger intake	✓	✓	✓	✓
OpenTelemetry intake for traces and metrics[6]	✓	✓	✓	✓
APM app	✓	✓	✓	✓
Distributed tracing	✓	✓	✓	✓
Service maps	—	—	✓	✓
Correlations	—	—	✓	✓
Synthetic _source for APM indices	—[13]	—[13]	—[13]	✓

APM language support

Java	✓	✓	✓	✓
.NET	✓	✓	✓	✓
Go	✓	✓	✓	✓
Ruby	✓	✓	✓	✓
RUM (JavaScript)	✓	✓	✓	✓
PHP	✓	✓	✓	✓
Python	✓	✓	✓	✓
Node	✓	✓	✓	✓

Stack integrations

Elastic Logs and Metrics	✓	✓	✓	✓
Kibana alerting and actions[4]	✓	✓	✓	✓
Machine learning	—	—	✓	✓
Synthetic _source for Profiling indices	—[13]	—[13]	—[13]	✓

Log shipper (Filebeat)	✓	✓	✓	✓
Dashboards for common data sources	✓	✓	✓	✓
Logs app	✓	✓	✓	✓
Logsdb indices for logs	✓	✓	✓	✓
Synthetic _source for logsdb indices	—[13]	—[13]	—[13]	✓

Integrations

Elastic Uptime and APM	✓	✓	✓	✓
Kibana alerting and actions[4]	✓	✓	✓	✓
Log categorization	—	—	✓	✓
Machine learning	—	—	✓	✓

Metric shipper (Metricbeat)	✓	✓	✓	✓
Dashboards for common data sources	✓	✓	✓	✓
Metrics app	✓	✓	✓	✓
Time series indices for metrics (TSDS)	✓	✓	✓	✓
Synthetic _source for time series indices	—[13]	—[13]	—[13]	✓
Downsampling	✓	✓	✓	✓

Integrations

Elastic Logs, APM, Synthetic Monitoring Private Locations	✓	✓	✓	✓
Kibana alerting and actions[4]	✓	✓	✓	✓
Machine learning	—	—	✓	✓

Synthetic Monitoring UI	✓	✓	✓	✓
Project Monitors	✓	✓	✓	✓
Managed Test Execution Service[12]	✓	✓	✓	✓
Private Testing Locations	✓	✓	✓	✓
Point and Click Script Recorder	✓	✓	✓	✓

Elastic Common Schema	✓	✓	✓	✓
Extended detection & response (XDR)	✓	✓	✓	✓
Security information and event management (SIEM)	✓	✓	✓	✓

Host security analysis	✓	✓	✓	✓
Network security analysis	✓	✓	✓	✓
User security analysis	✓	✓	✓	✓
Timeline event explorer	✓	✓	✓	✓
Case management	✓	✓	✓	✓
Detection engine (e.g., correlation, indicator match, threshold)	✓	✓	✓	✓
Prebuilt detection rules	✓	✓	✓	✓
Detection alerts suppression	—	—	✓	✓
Detection alert external actions	—	✓	✓	✓
Machine learning anomaly detection	—	—	✓	✓
Prebuilt anomaly detection jobs	—	—	✓	✓
Malware prevention	✓	✓	✓	✓
Admin-defined endpoint blocklist	✓	✓	✓	✓
Ransomware prevention	—	—	✓	✓
Malicious behavior protection	—	—	✓	✓
Memory threat protection	—	—	✓	✓
Self-healing	—	—	✓	✓
Host Isolation	—	—	✓	✓
Interactive response console	—	—	—	✓
Tamper Protection	—	✓	✓	✓
Elastic AI Assistant	—	—	—	✓
Threat intelligence management	—	—	—	✓
Threat Intelligence Platform (TIP)	—	—	—	✓
Customizable on-endpoint protection notifications	—	—	✓	✓
Cloud and Kubernetes Security Posture Management (K/CSPM)	✓	✓	✓	✓
Workload session auditing	—	—	—	✓

Integrations

Elastic Agent	✓	✓	✓	✓
Elastic APM	✓	✓	✓	✓
IPinfo Commercial Database	—	—	✓	—
Elastic Maps	✓	✓	✓	✓
Osquery Manager	✓	✓	✓	✓
Network Packet Capture[10]	✓	✓	✓	✓
Threat intelligence feeds and platforms	✓	✓	✓	✓
Machine learning	—	—	✓	✓
Kibana Alerts and Actions[4]	✓	✓	✓	✓
Atlassian Jira	—	✓	✓	✓
Swimlane SOAR	—	✓	✓	✓
IBM Resilient	—	—	✓	✓
ServiceNow ITOM, ITSM, SecOps	—	—	✓	✓
Generative AI Connector for Open AI, Azure Open AI, AWS Bedrock, Google Vertex AI	—	—	—	✓

Elastic Maps Service[5]

Base layer maps	✓	✓	✓	✓

Maps app

Shapefile and GeoJSON upload	✓	✓	✓	✓
Multiple layers	✓	✓	✓	✓
Native vector tile support	✓	✓	✓	✓
Layer-based filtering	✓	✓	✓	✓
Client-side styling	✓	✓	✓	✓
Individual points and shapes	✓	✓	✓	✓
Tracking alerts	—	✓	✓	✓
Containment alerts	—	✓	✓	✓
Embed maps in dashboard	✓	✓	✓	✓
Embed maps in Canvas	✓	✓	✓	✓
Geo-threshold alerts	—	✓	✓	✓
Display up to 24 zoom levels	✓	✓	✓	✓

Custom raster and vector tile service support	✓	✓	✓	✓
Kibana Alerts: tracking containment (geofencing)	—	✓	✓	✓

Elastic App Search

Index once, sort all you want	✓	✓	✓	✓
Customizable relevance model	✓	✓	✓	✓
Language-specific relevance	✓	✓	✓	✓
Synonym management	✓	✓	✓	✓
Analytics API	✓	✓	✓	✓
Clickthrough API	✓	✓	✓	✓
Adaptive Relevance: Curations (Beta)	—	—	✓	✓
Precision tuning (Beta)	✓	✓	✓	✓
Web crawler	✓	✓	✓	✓
Web crawler HTTP proxy authentication	—	✓	✓	✓
Web crawler HTTP authentication	—	✓	✓	✓
Web crawler PDF Extraction	—	✓	✓	✓
Index lifecycle management	✓	✓	✓	✓
Passthrough Elasticsearch queries	✓	✓	✓	✓
Elasticsearch-based App Search engines	✓	✓	✓	✓

Operations

One-click monitoring	✓	✓	✓	✓

Analytics

Searches	✓	✓	✓	✓
Clicks	✓	✓	✓	✓
Insights	✓	✓	✓	✓

Clients

Python	✓	✓	✓	✓
Ruby	✓	✓	✓	✓

Security & collaboration

Multi-user collaboration	✓	✓	✓	✓
Signed search keys	✓	✓	✓	✓
Engine scoping	—	—	✓	✓
Role-based access control	—	—	✓	✓
Engine-scoped API keys	—	—	✓	✓
Single sign-on (SAML, OpenID Connect, Kerberos, JWT)	—	—	✓	✓
Meta engines	✓	✓	✓	✓
Audit logging	—	✓	✓	✓

Unified organizational search experience

Workplace Search server	✓	✓	✓	✓
Unified search interface	✓	✓	✓	✓
Out-of-the-box search applications	✓	✓	✓	✓
Customizable look and feel	✓	✓	✓	✓
Natural language query filtering	✓	✓	✓	✓
Search history	✓	✓	✓	✓
Typo-tolerant relevance model	✓	✓	✓	✓
Synonym management	✓	✓	✓	✓
Customizable filtering and faceting	✓	✓	✓	✓
Content source prioritization	✓	✓	✓	✓
Search analytics	✓	✓	✓	✓
Search API	—	—	✓	✓

Operations

One-click full stack monitoring	✓	✓	✓	✓

Clients

Python	✓	✓	✓	✓
Ruby	✓	✓	✓	✓

Content sources

First-party cloud source synchronization	✓	✓	✓	✓
First-party on-premises source synchronization	✓	✓	✓	✓
Global sync scheduling configuration	✓	✓	✓	✓
Source-level scheduling configuration	—	—	✓	✓
Custom source support via API and connector packages	✓	✓	✓	✓
Custom source support via API	✓	✓	✓	✓
Full-text content indexing for files, documents, and records	✓	✓	✓	✓
Document-level permission support	—	—	✓	✓
Object synchronization selection	✓	✓	✓	✓
Path-based content synchronization	✓	✓	✓	✓
File extension-based content synchronization	✓	✓	✓	✓
Private sources	—	—	✓	✓
Content source indexing rules and scheduling	—	✓	✓	✓

User management & security

Organizational groups	✓	✓	✓	✓
Single sign-on (SAML, OpenID Connect, Kerberos, JWT)	—	—	✓	✓
Role-based access control	—	—	✓	✓
Encrypted communications	—	—	✓	✓
Encryption at rest support	✓	✓	✓	✓
Audit logging	—	✓	✓	✓

Support level	Limited	Base	Enhanced	Premium
Support coverage	—	Business hours	24/7/365	24/7/365
Target initial response time	—	Urgent: 4 business hours High: 1 business day Normal: 2 business days	Urgent: 1 hour High: 4 hours Normal: 1 business day	Urgent: 30 minutes High: 4 hours Normal: 1 business day
Unlimited # of incidents	—	✓	✓	✓
Support contacts[7]	2	6	8	8
Ticket-based support	✓	✓	✓	✓
SLA-based support	—	✓	✓	✓

[2] *Elastic Cloud subscriptions on AWS GovCloud (US) are only available annually at this time (not monthly).*

[3] *Elastic APM is not supported on Elastic Cloud Standard when purchased through the AWS Marketplace.*

[4] *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.*

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

[6] *There are two options for OpenTelemetry intake: native support of the OpenTelemetry protocol directly into APM Server (experimental), and the Elastic exporter on the OpenTelemetry collector, which is the recommended approach. If you choose the latter, note that Elastic Cloud does not host the Elastic exporter on the OpenTelemetry collector exporter, refer to **documentation** to set one up adjacent to your applications.*

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

[10] *Re-distributing the Windows release of Packetbeat and the Network Packet Capture agent integration for Windows hosts requires an additional license to npcap, a Windows packet sniffing library, that may be obtained from nmap.org.*

[11] *Advanced cluster rebalancing is based on observed data stream write loads described in cluster-level shard allocation.*

[12] *Access to the synthetic monitoring managed testing infrastructure is limited to Elastic Cloud users only or users consuming Elastic Cloud through a CSP marketplace. Test runs executed on the managed testing infrastructure incur an additional cost.*

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

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.

elastic
The Search AI Company

FOLLOW US

ABOUT US
About Elastic
Leadership
DE&I
Blog
Newsroom

JOIN US
Careers
Career portal
How we hire

PARTNERS
Find a partner
Partner login
Request access
Become a partner

TRUST & SECURITY
Trust center
EthicsPoint portal
ECCN report
Ethics email

INVESTOR RELATIONS
Investor resources
Governance
Financials
Stock

EXCELLENCE AWARDS
Previous winners
ElasticON Tour
Become a sponsor
All events