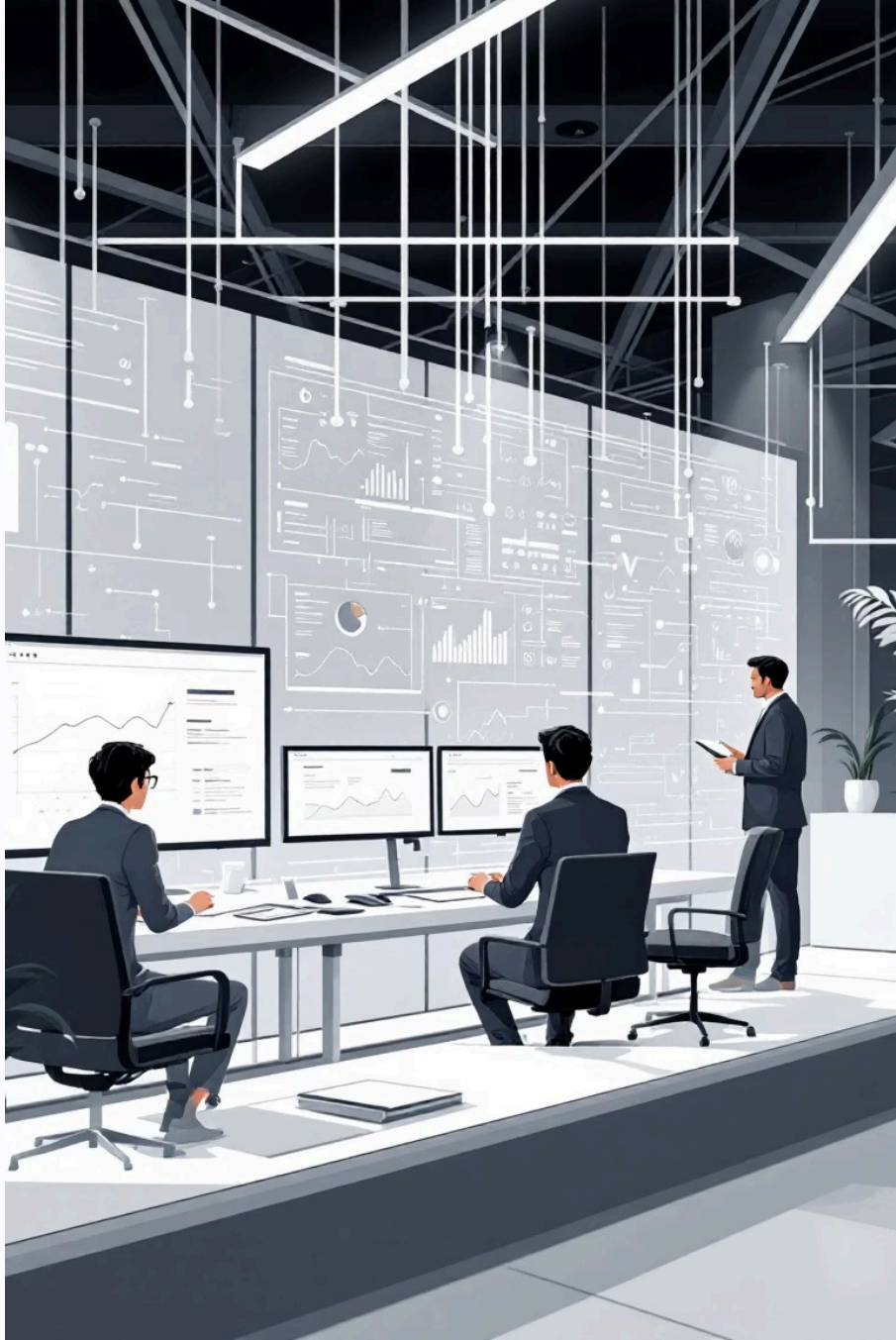
Elasticsearch Usecases

Harnessing the power of real-time data for search, analytics, and operational insights across diverse applications and industries.



Log and Event Data Analytics

Ingest, parse, and index logs from various systems to enable real-time searching, filtering, and troubleshooting. Popular for centralized logging platforms that support DevOps and incident response.

Real-time Log Aggregation

From multiple sources, consolidating all your critical data in one place.

Advanced Parsing & Indexing

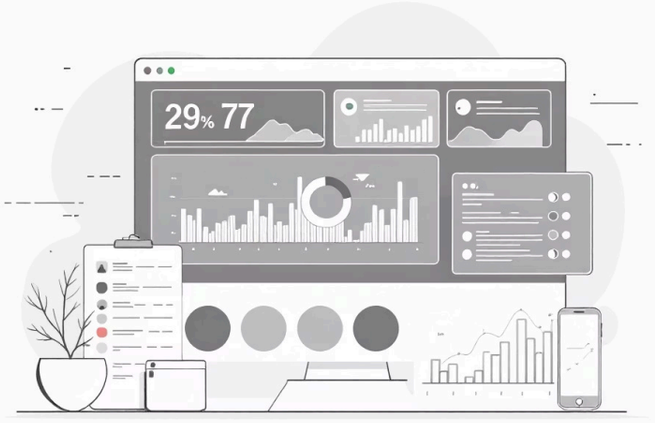
Structured indexing for efficient data retrieval and analysis.

Fast Full-Text Search

Across massive datasets, enabling quick identification of issues.

Monitoring & Alerting Integration

Seamlessly connect with existing systems for proactive incident response.



Full-Text Search Excellence

Full-text search enables rapid and efficient searching through large volumes of unstructured or semi-structured text data, providing users with the ability to quickly find relevant information by matching keywords and phrases within documents. Unlike traditional database queries, it processes natural language, delivering highly accurate and contextually relevant results.

High Performance

Enable fast and flexible search in applications with complex text queries, relevance scoring, and ranking capabilities.

Advanced Features

Supports fuzzy matching, Boolean operators, phrase searches, and proximity queries with millisecond response times.

Scalable Architecture

Distributed search across clusters handling billions of documents with consistent performance.

Key Usecases

E-commerce Product Search

Enabling customers to quickly find desired products within extensive catalogs using keywords, categories, and filters.

Document Management Systems

Allowing employees to efficiently search for specific reports, articles, or internal documents within vast corporate archives.

News & Media Platforms

Providing readers with instant access to relevant articles, news updates, or multimedia content based on topics or keywords.

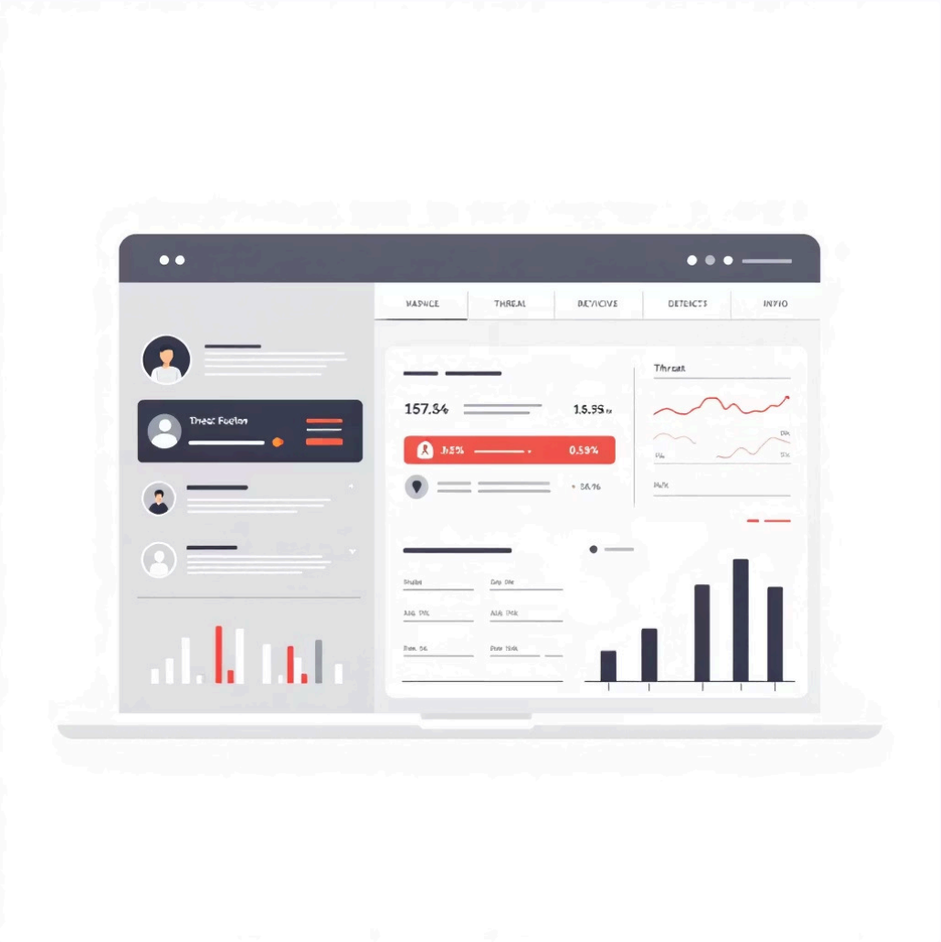
Customer Support Knowledge Bases

Helping support agents and users quickly retrieve solutions, FAQs, and answers to common queries.

Security & Business Intelligence

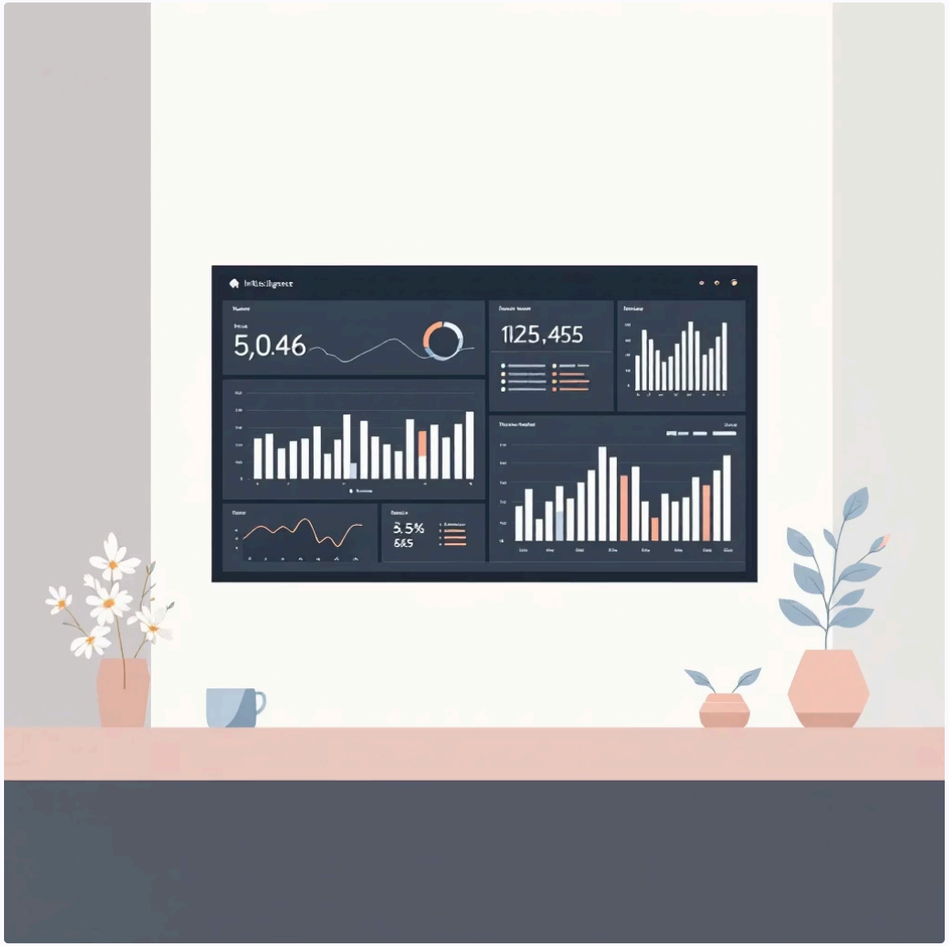
Security Analytics

Correlate and analyze security event logs for anomaly detection, threat hunting, and compliance reporting. Integrate with SIEM systems to enable real-time alerting and comprehensive security dashboards.



Business Intelligence

Visualize aggregated data using Kibana or Grafana for monitoring KPIs, operational metrics, and customer insights. Supports drill-downs, filtering, and interactive analysis enabling data-driven decision making.



Application Performance Monitoring

Application Performance Monitoring (APM) is a critical practice for tracking, monitoring, and managing the performance and availability of software applications. It provides comprehensive insights into how applications are performing, enabling organizations to ensure optimal user experience and maintain system health.

Trace Collection

Capture application calls, latency, errors, and transaction details using Elastic APM agents across distributed systems.

Performance Analysis

Analyze bottlenecks, error rates, and response times with detailed service maps and dependency tracking.

Operational Insights

Enable developers and operators to monitor system health and optimize performance efficiently.

Key Use Cases for APM

Web Application Performance

Monitor the responsiveness and availability of web applications to ensure fast load times and a seamless user experience.

Microservices & Distributed Systems

Gain end-to-end visibility across complex microservices architectures, tracking transactions and identifying inter-service dependencies.

Database Performance Tuning

Identify slow database queries and optimize performance to reduce latency and improve overall application efficiency.

Proactive Issue Resolution

Detect and alert on anomalies before they impact users, allowing teams to address problems proactively and minimize downtime.

Telecom Use Cases

Elasticsearch's powerful capabilities make it an indispensable tool across various critical functions within the telecommunications industry, enhancing efficiency, ensuring reliability, and driving business insights.

Network Performance Monitoring (NPM)

- Collects logs, SNMP traps, and telemetry from routers, switches, firewalls, and cell towers.
- Detects latency, packet loss, and congestion in near real-time.
- Uses Kibana dashboards for visualizing KPIs like jitter, throughput, and bandwidth utilization.

Example: Monitoring 5G network nodes to ensure SLA compliance.

Call Detail Record (CDR) Analysis

- CDRs are high-volume structured logs generated for every call/SMS/session.
- Perform search and analytics on call duration, drops, and network usage patterns.
- Supports fraud detection, revenue assurance, and customer experience analysis.

Example: Spotting international call fraud by detecting unusual call patterns.

Subscriber Behavior Analytics

- Subscriber logs and data usage reveal behavior patterns across services.
- Analyze session frequency, data volume, and app usage trends.
- Supports churn prediction, personalized offers, and service enhancements.

Example: Flagging at-risk high-data users for targeted retention campaigns.

Fraud Detection & Security Analytics

- Ingests real-time data from OSS/BSS, firewalls, and IDS/IPS.
- Detects anomalies like SIM card cloning, unusual roaming usage, and DDoS attacks.
- Elastic Security (SIEM) can be used to automate detection rules.

Example: Identifying sudden spikes in SMS traffic from a single subscriber for potential spam or fraud.

Customer Experience Management (CEM)

- Combines network KPIs, app logs, and customer support data.
- Helps identify causes of poor Quality of Experience (QoE).
- Can link network events with subscriber complaints in real-time.

Example: Detecting when 4G customers in a specific region face repeated call drops to trigger investigation.

IoT & 5G Data Analytics

- Telecoms manage millions of IoT device connections.
- Elasticsearch helps monitor IoT device connectivity and detect unusual patterns.
- Enables predictive maintenance for connected devices.

Example: A utility company's smart meters sending irregular data bursts detected via anomaly detection.

Log & Event Management (OSS/BSS Operations)

- Telecom systems like OSS and BSS generate massive logs.
- Elastic Stack provides centralized logging and root cause analysis.
- Facilitates faster troubleshooting by avoiding manual log searches.

Example: Tracing failed prepaid recharges across billing, CRM, and gateway logs.

Regulatory Compliance & Audit

- Telecoms must retain certain logs for compliance (e.g., GDPR, FCC).
- Elasticsearch allows efficient storage and search of regulatory logs.
- Ensures secure access controls for authorized users.

Example: Retaining and searching subscriber usage logs for legal audits.

Thank you!