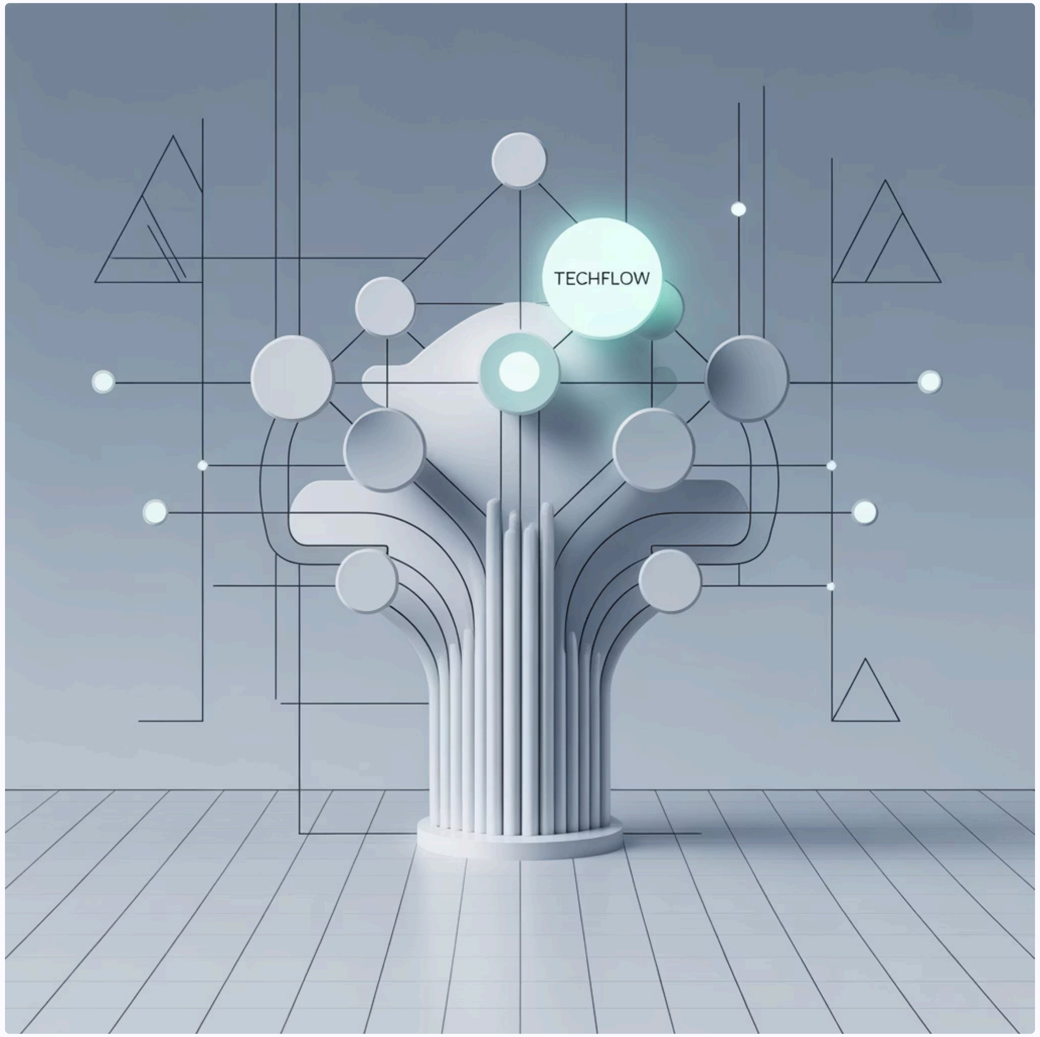
The Elastic Stack

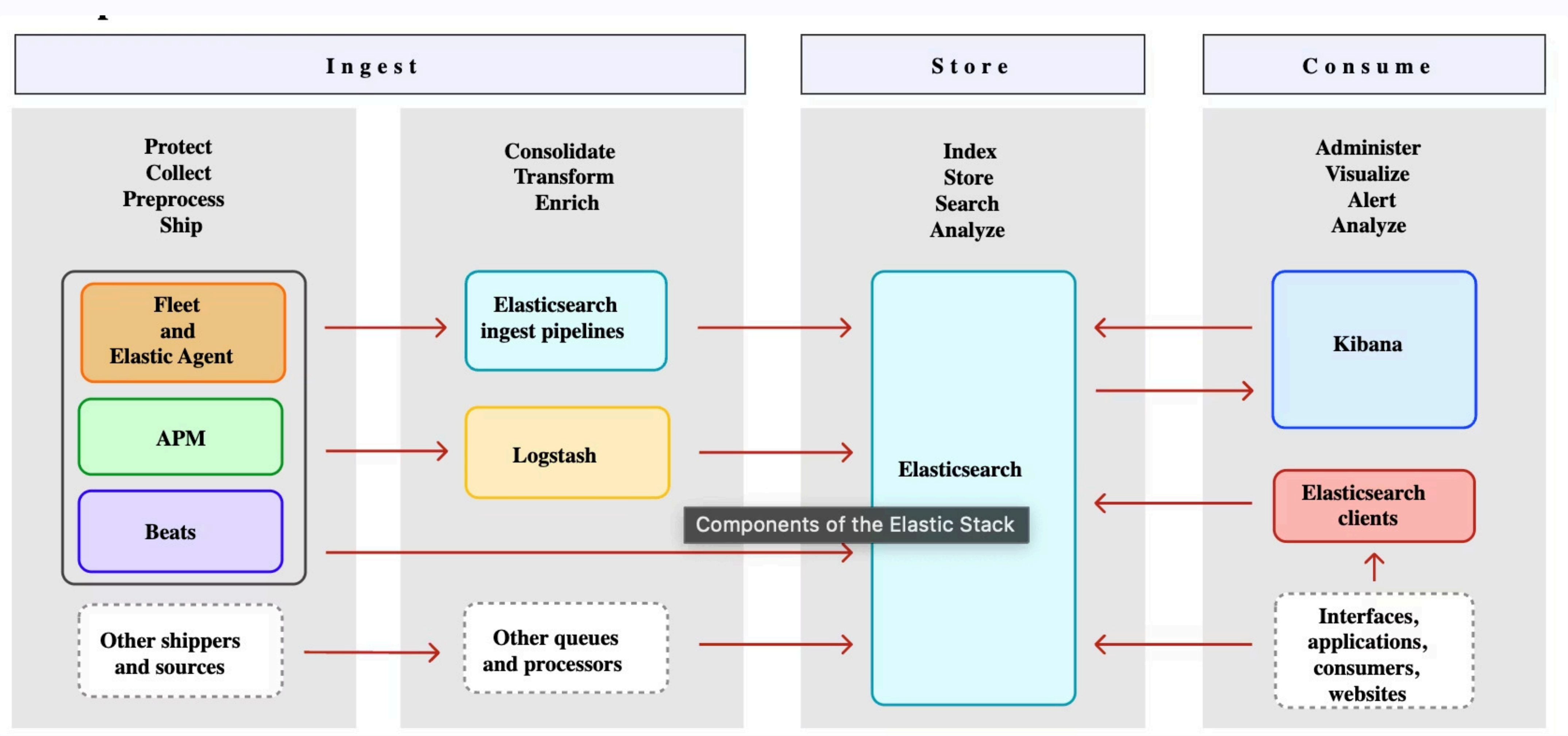
A comprehensive overview of the fast, scalable components that enable secure data ingestion, storage, search, analysis, and visualization from any source in any format.

What is the Elastic Stack?

- The Elastic Stack is a powerful collection of synchronized components designed to work seamlessly together.
- It transforms raw data from any source into actionable insights through search, analysis, and visualization capabilities.
- All products are synchronized for simplified installation and upgrades.
- It offers flexible deployment options from on-premise hardware to cloud-managed services.



Components of Elastic Stack



Components of the Elastic Stack

Core Stack Components

Ingest

Collect and ship data with Elastic Agent, Beats, and Logstash

Store

Distributed search and analytics with Elasticsearch

Consume

Visualize and analyze with Kibana and client libraries

Data Ingest Solutions

Multiple components work together to collect, transform, and forward your data efficiently:

Fleet & Elastic Agent

Unified monitoring for logs, metrics, and security with centralized management through Fleet.

APM

Real-time application performance monitoring with detailed insights into response times and database queries.

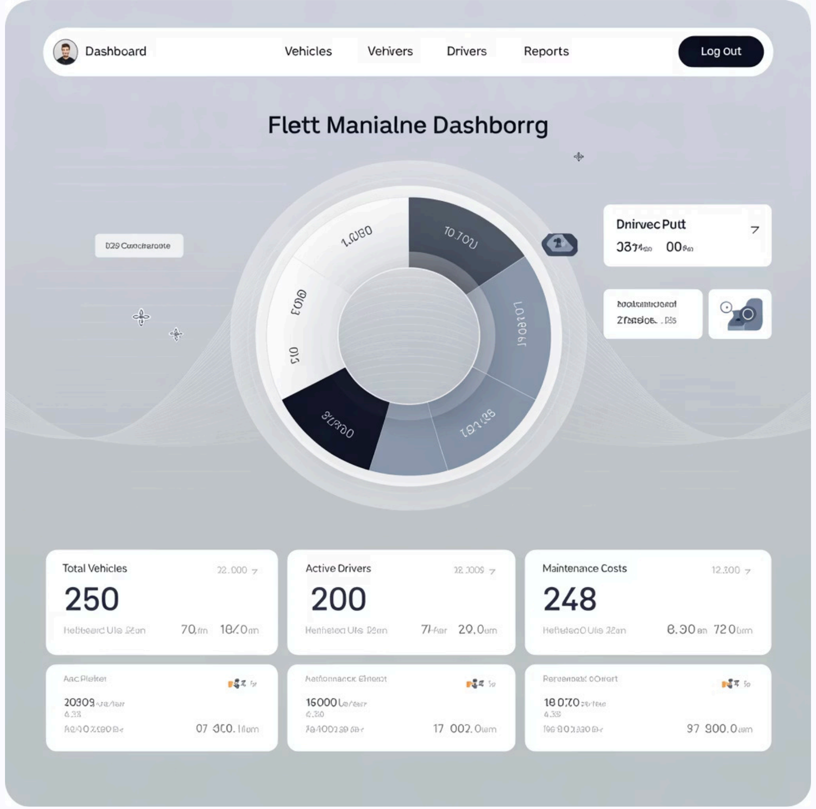
Beats

Lightweight data shippers for logs, metrics, network traffic, and system data collection.

Fleet and Elastic Agent

Unified Data Collection

- Elastic Agent provides a single, streamlined approach to add monitoring for logs, metrics, security threats, and remote services.
- Each agent operates under one policy where you can easily add integrations.
- Fleet enables centralized management of all Elastic Agents, monitoring their status, managing policies, and handling upgrades seamlessly.



Data Processing Options

Elasticsearch Ingest Pipelines

Transform data with sequential processors before indexing into Elasticsearch.

Logstash

Real-time data collection engine that unifies disparate sources with extensive plugin support.

Choose ingest pipelines for simple transformations or Logstash for complex data processing workflows with multiple sources and destinations.

Elasticsearch

The distributed search and analytics engine at the heart of the Elastic Stack

Near real-time search and analytics

Handles structured, unstructured, numerical, and geospatial data with lightning-fast searches

REST API access

Store, retrieve, search, and analyze data through comprehensive REST endpoints

Data Consumption & Visualization

Kibana

The primary interface for querying and visualizing Elasticsearch data. Kibana serves as the central hub for Search, Observability, and Security solutions.

Elasticsearch Clients

Direct programmatic access through official and community clients for Java, Python, Ruby, Go, and other popular languages.

Deployment Flexibility

On-Premise

Deploy on your own hardware for maximum control and customization

Self-Managed Cloud

Leverage cloud infrastructure while maintaining operational control

Elastic Cloud

Fully managed service with automatic updates and scaling

Choose the deployment option that best fits your organization's requirements, security policies, and operational capabilities.