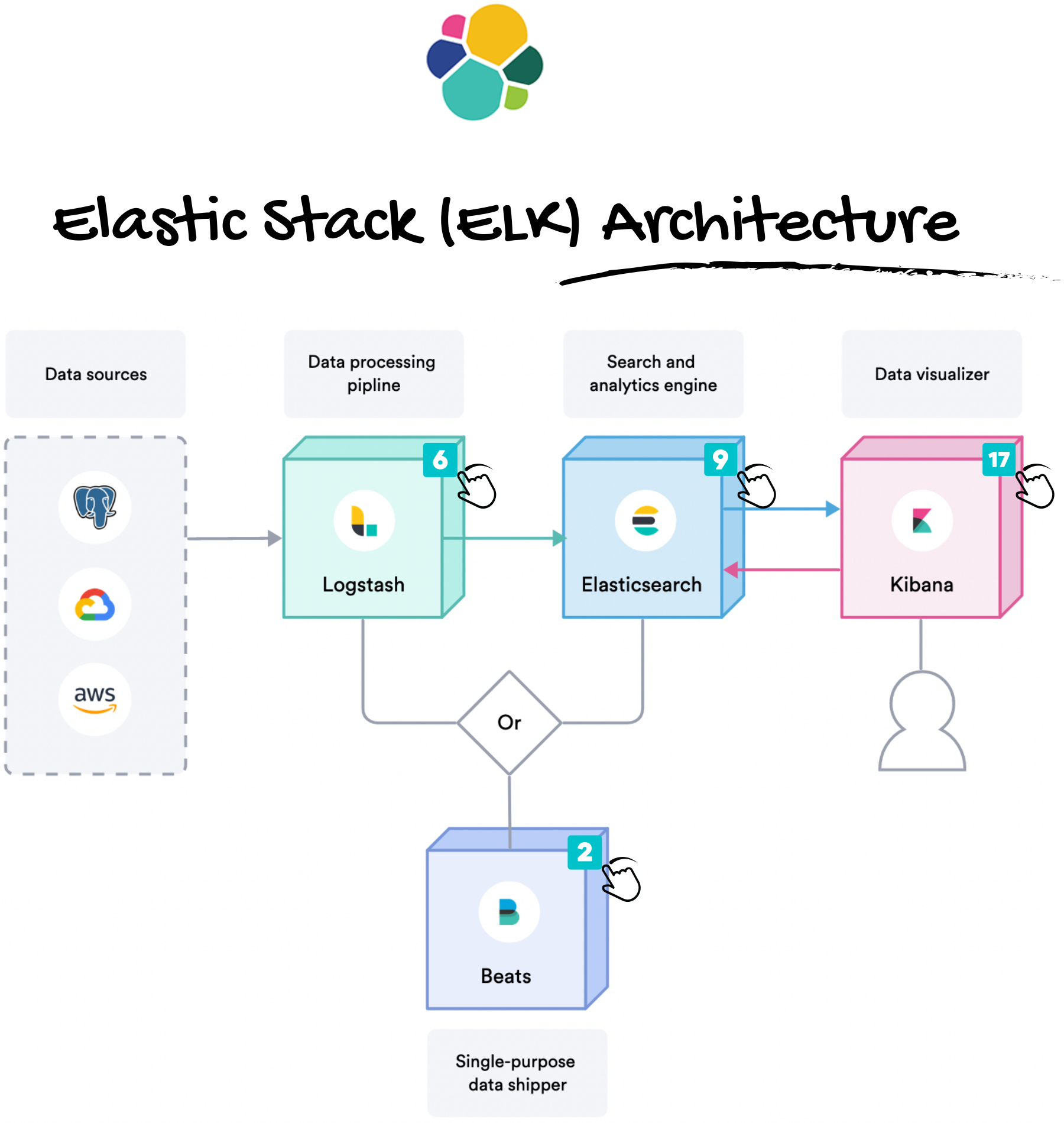
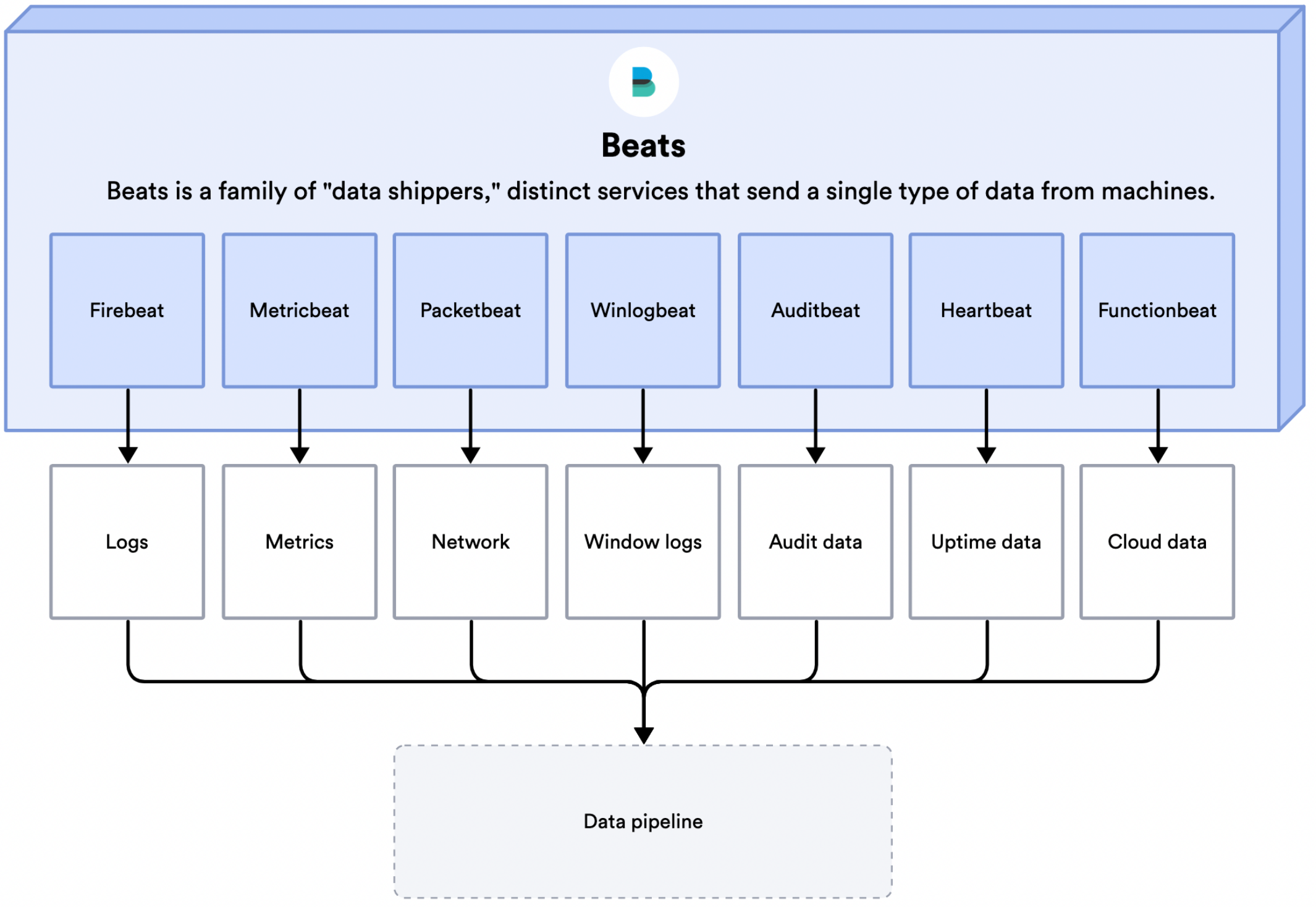
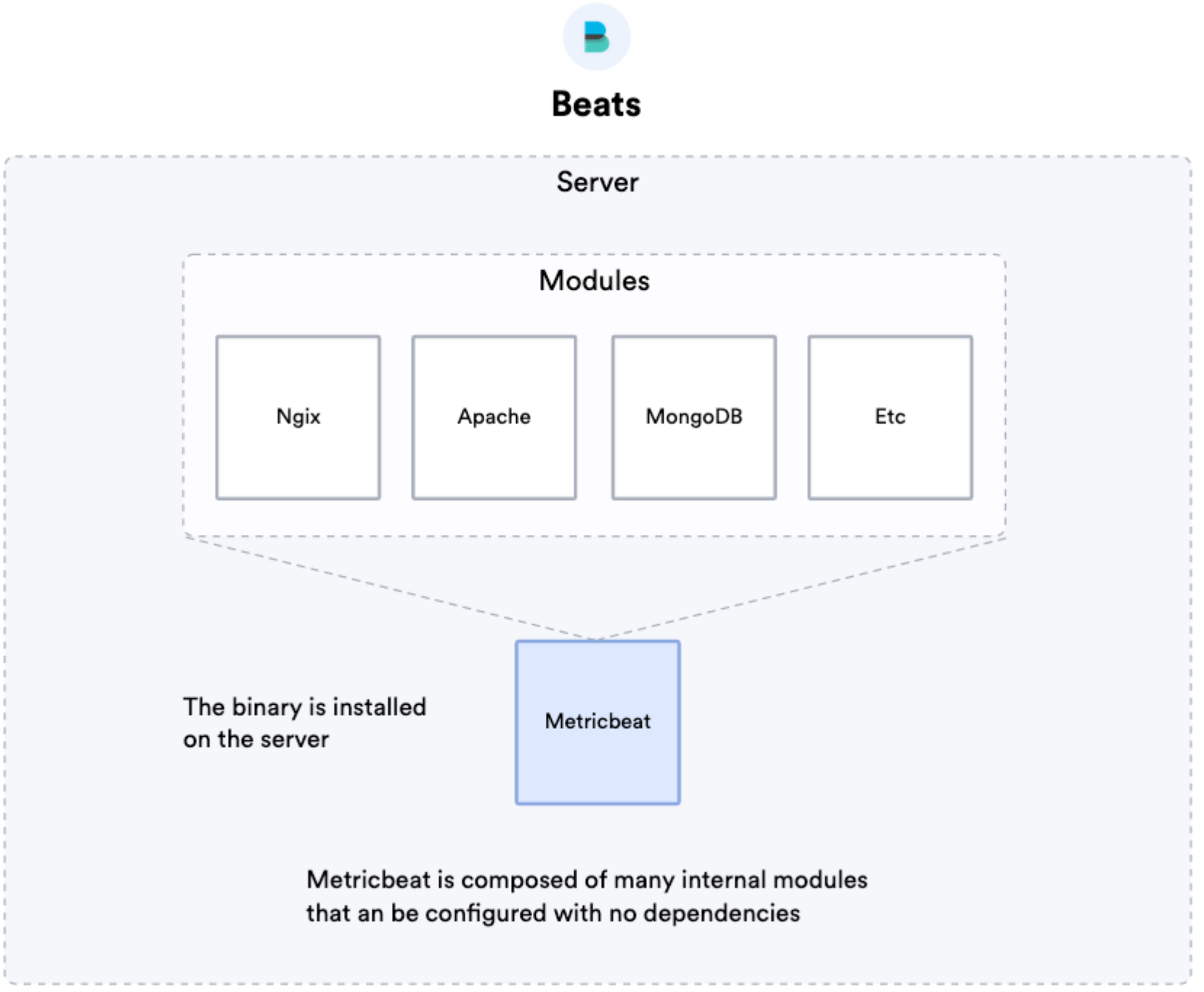
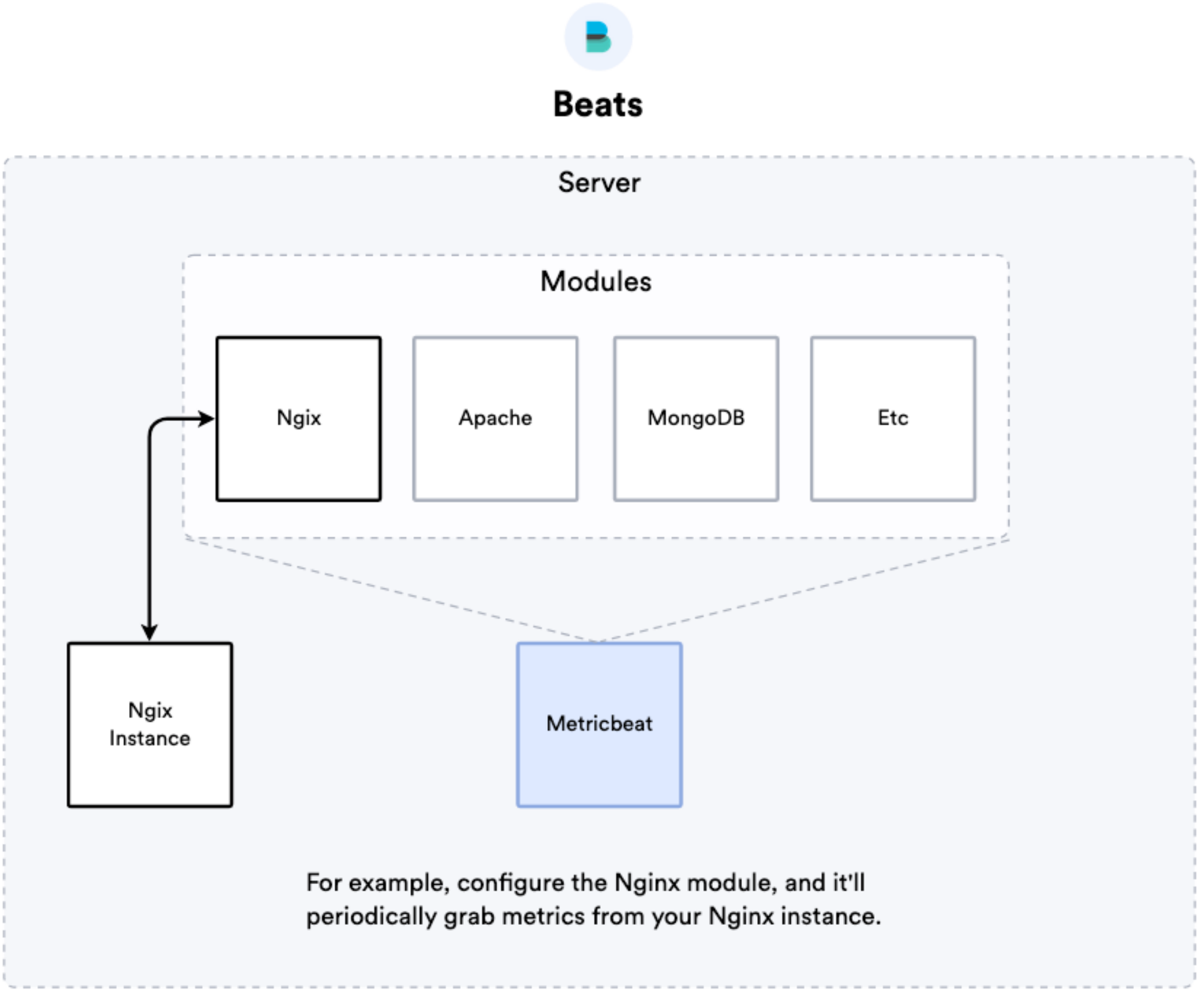
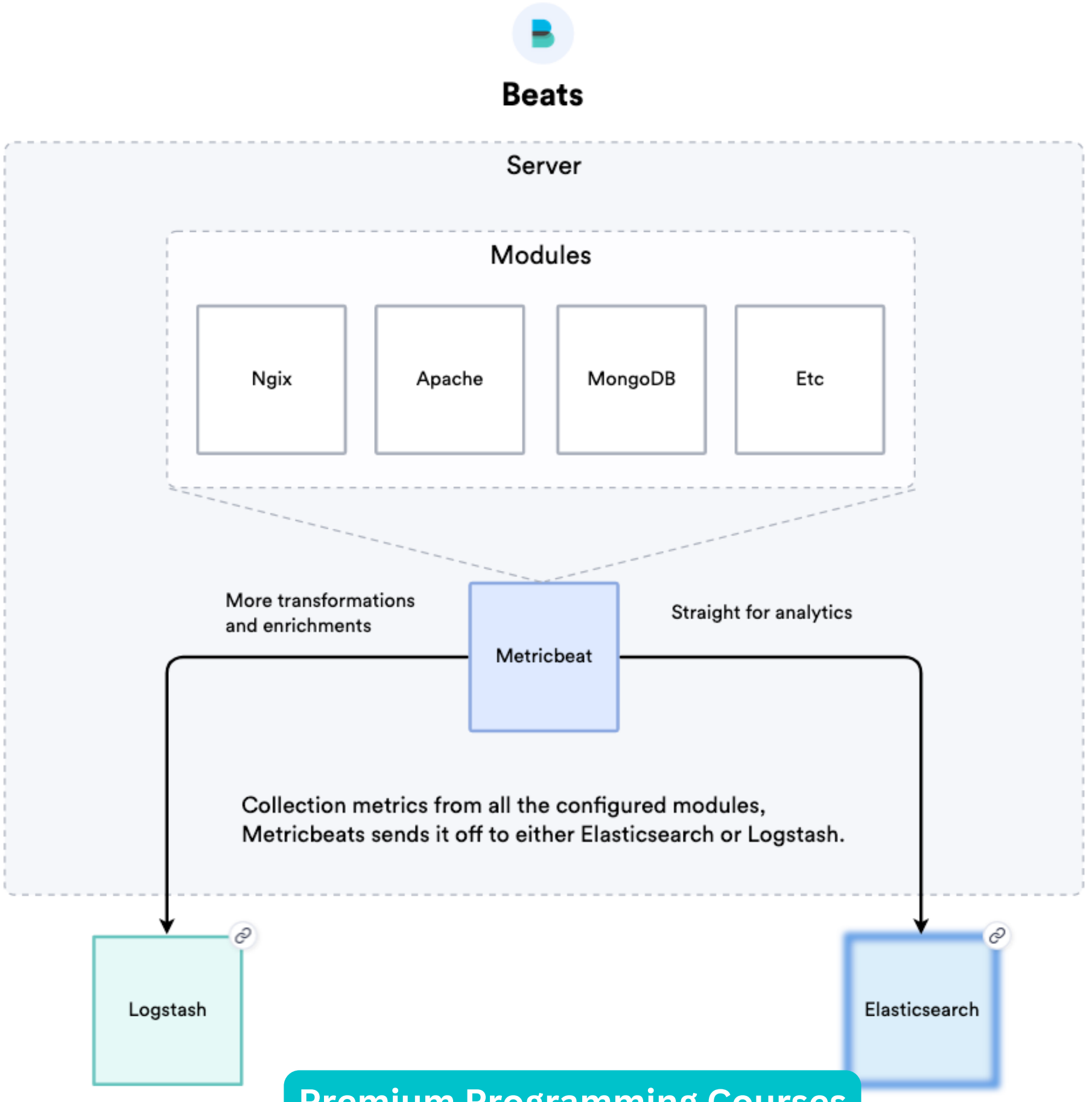


What are Beats?

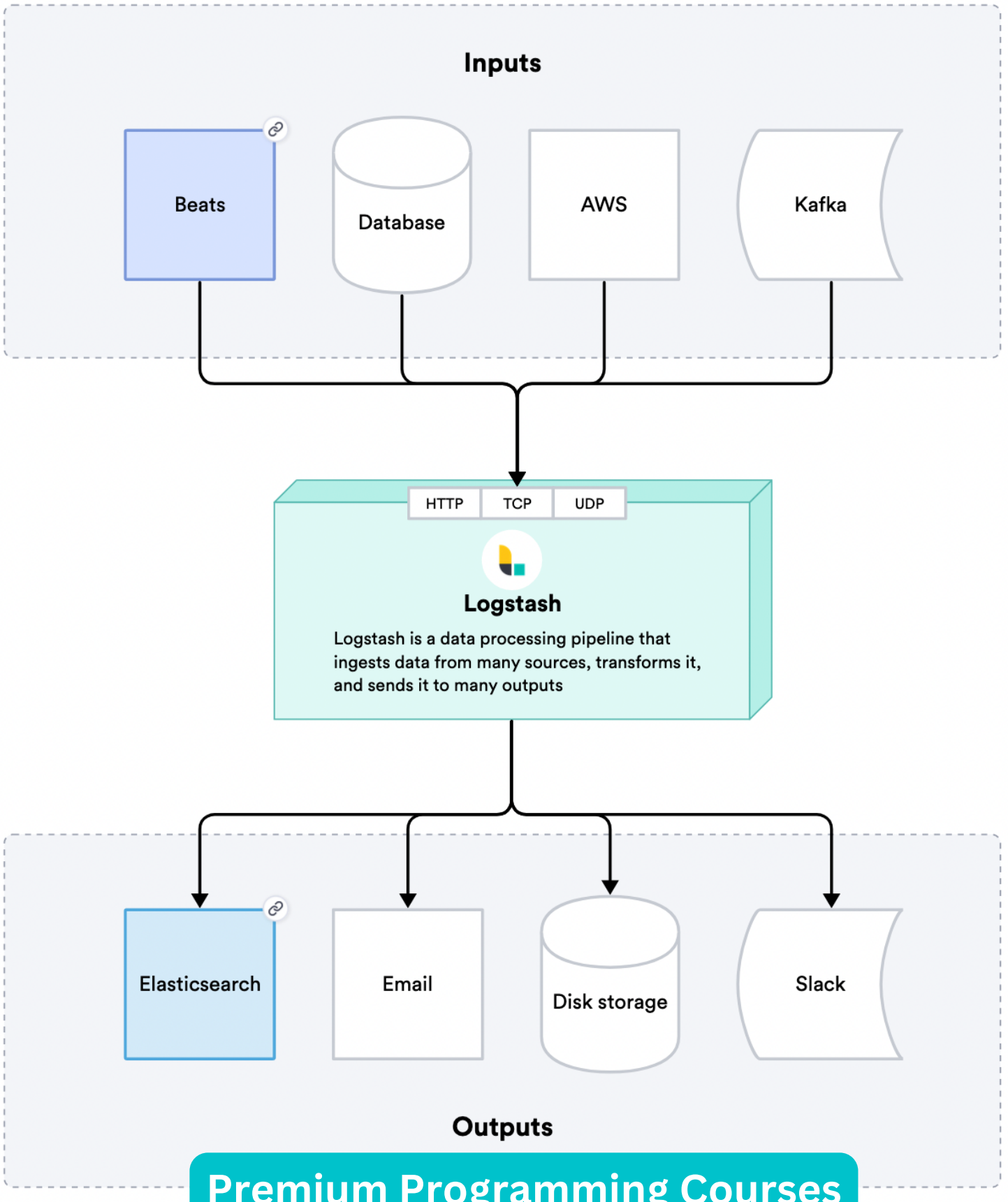


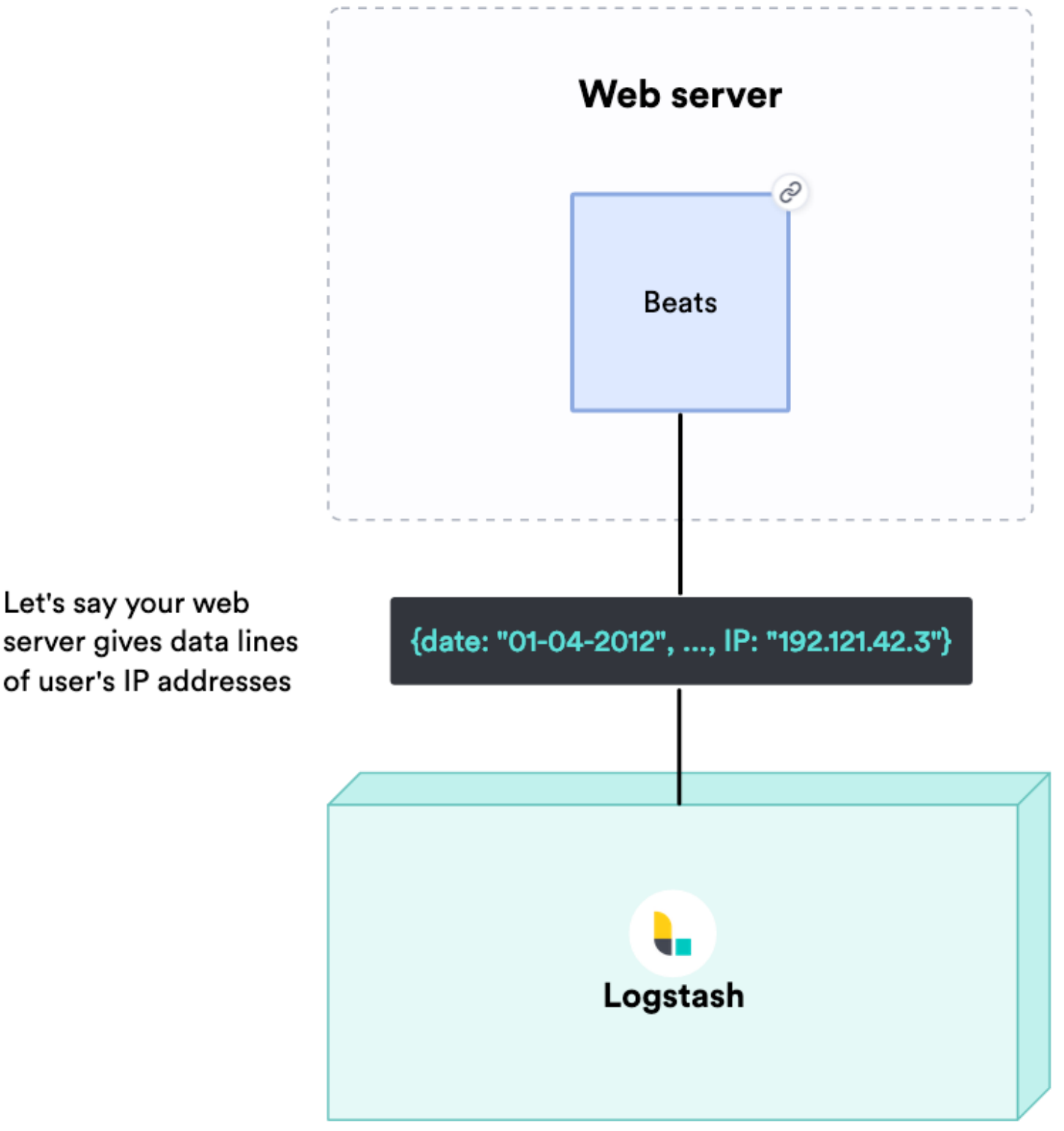






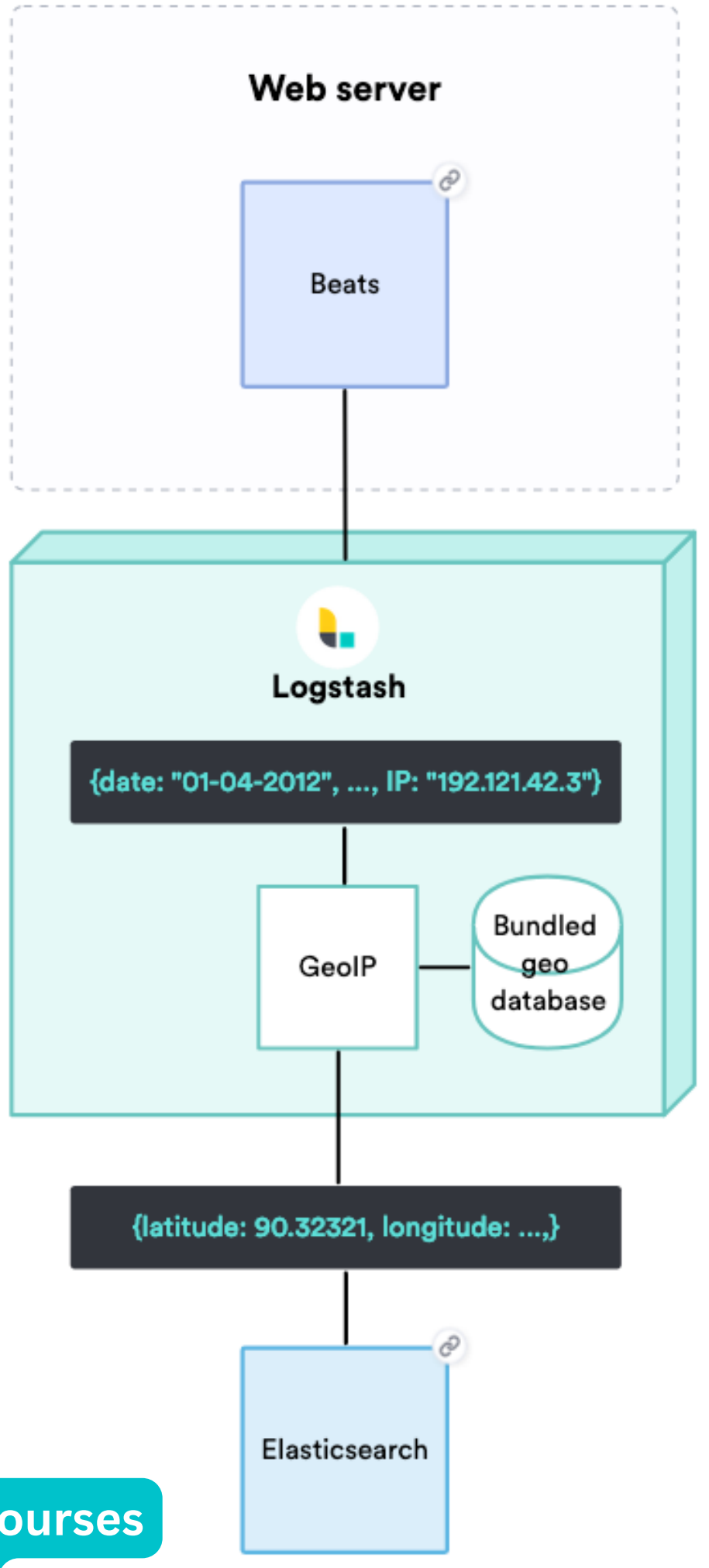
What's Logstash?

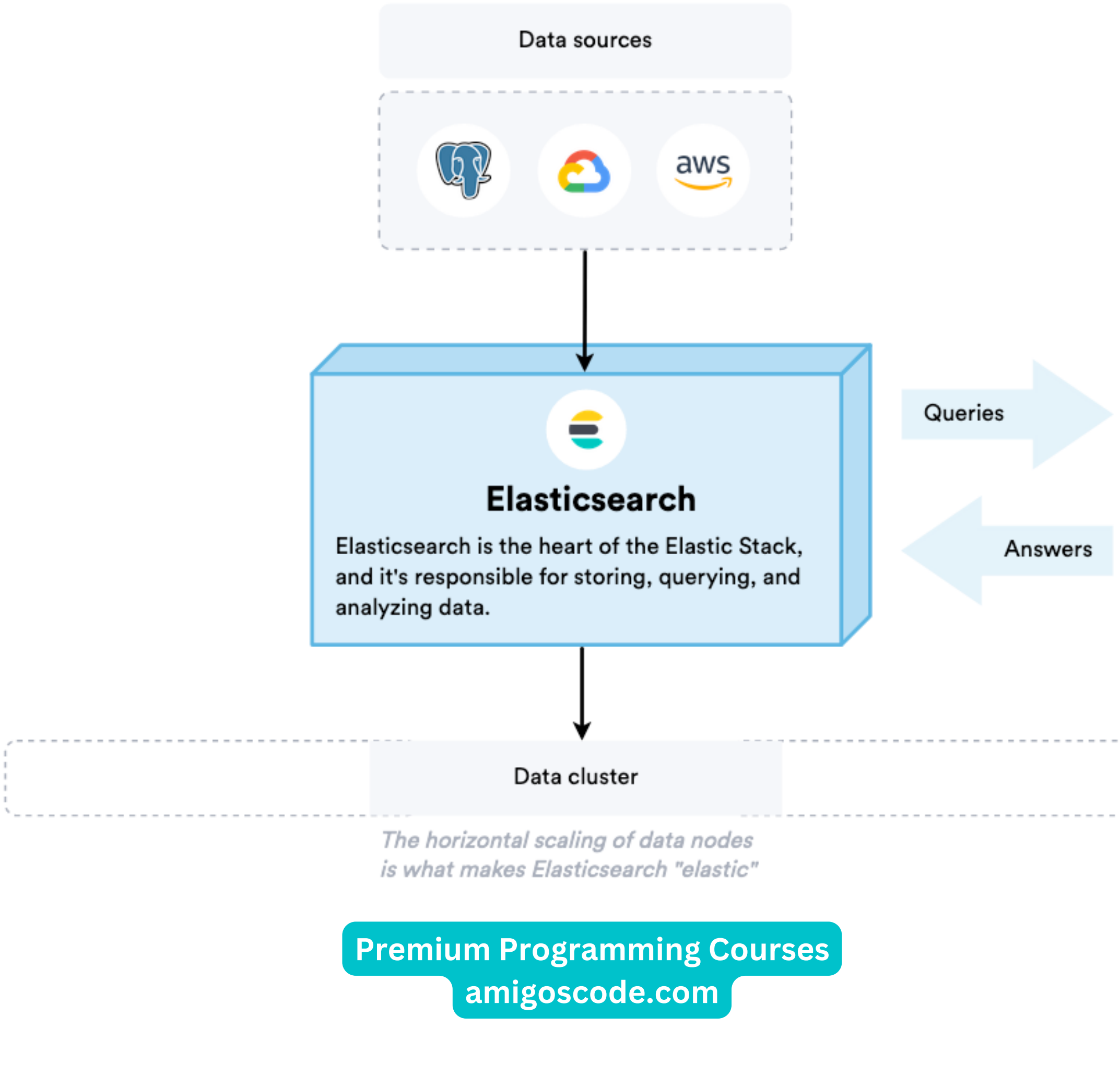




Let's say your web server gives data lines of user's IP addresses

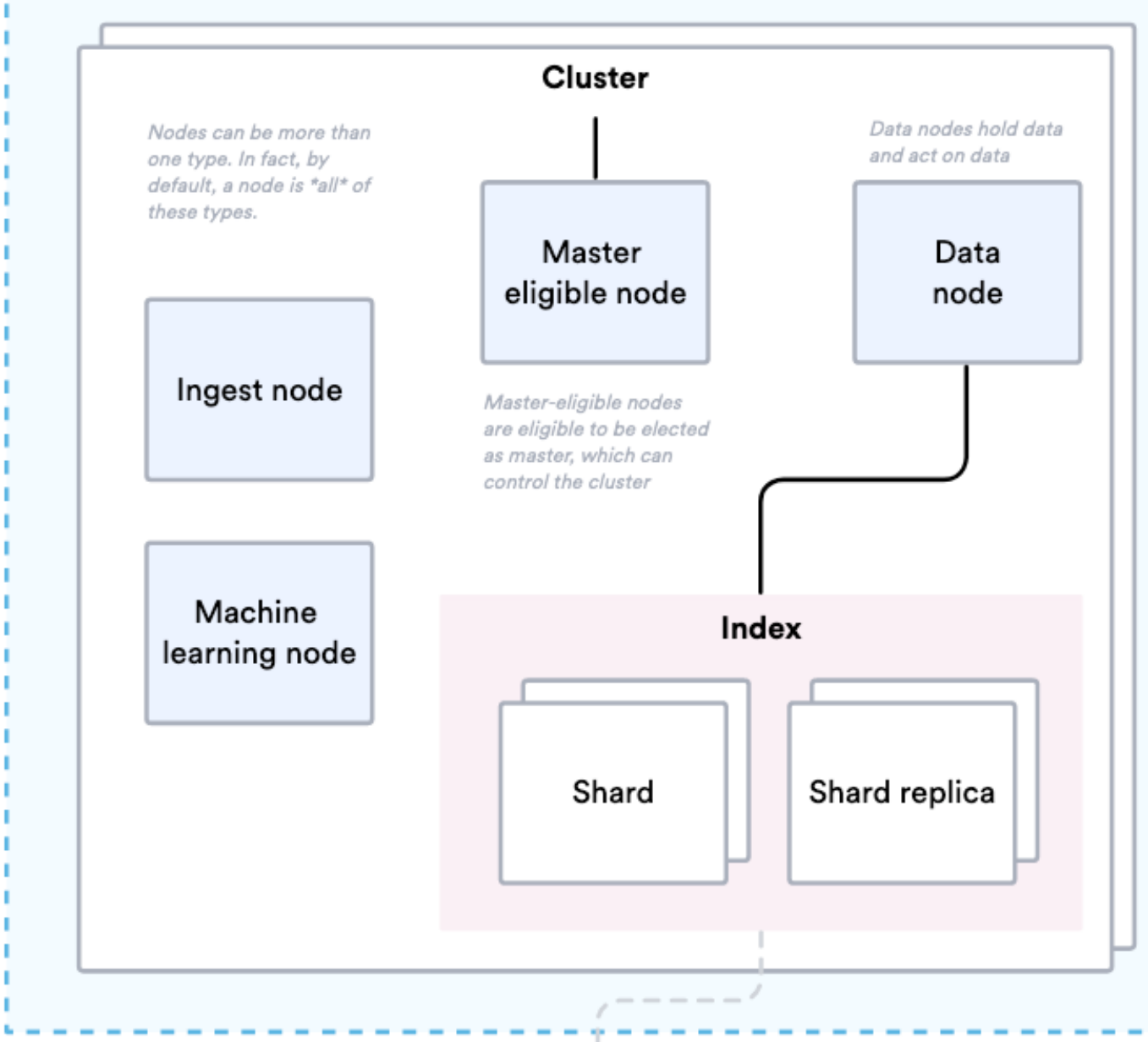
GeoIP is one of many filter plugins that help transform data in a specialized way. GeoIP takes an IP address and looks up a lat, long pair.



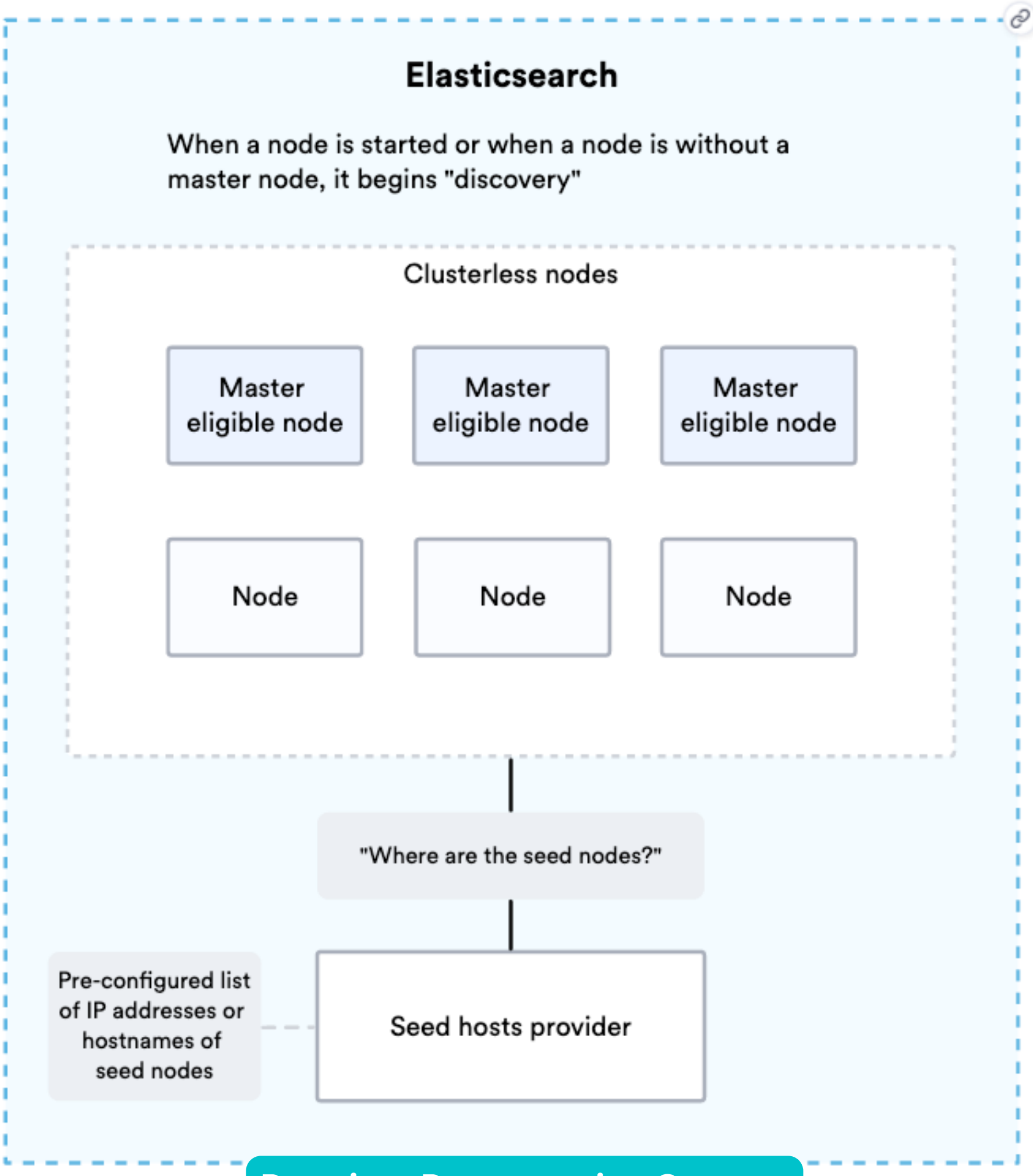


Elasticsearch

Elasticsearch is composed of many clusters (groups) of nodes, where a node is an instance of Elasticsearch

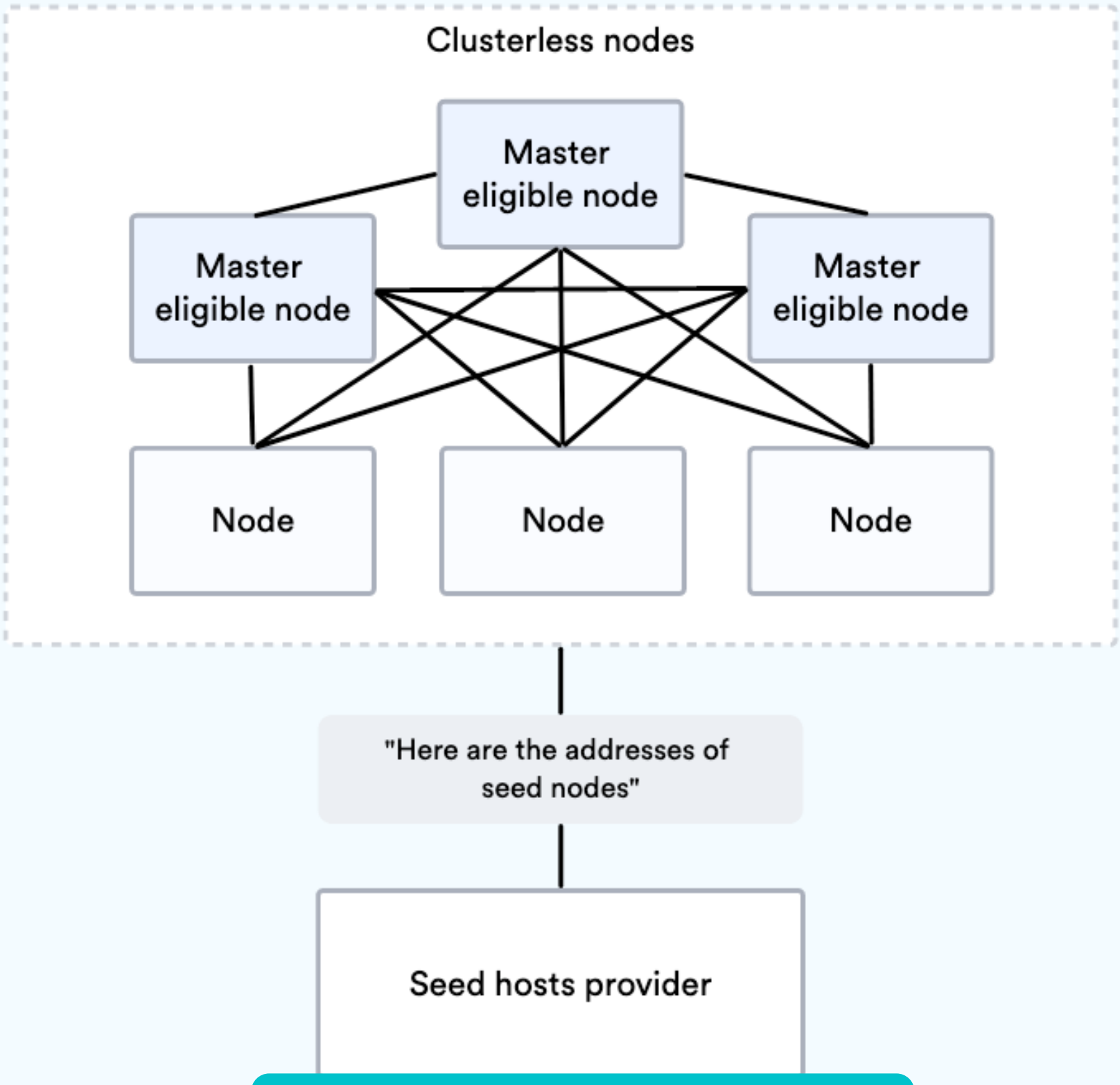


A Shard is the basic scaling unit for Elasticsearch. An Elasticsearch Shard is an instance of Apache Lucene.



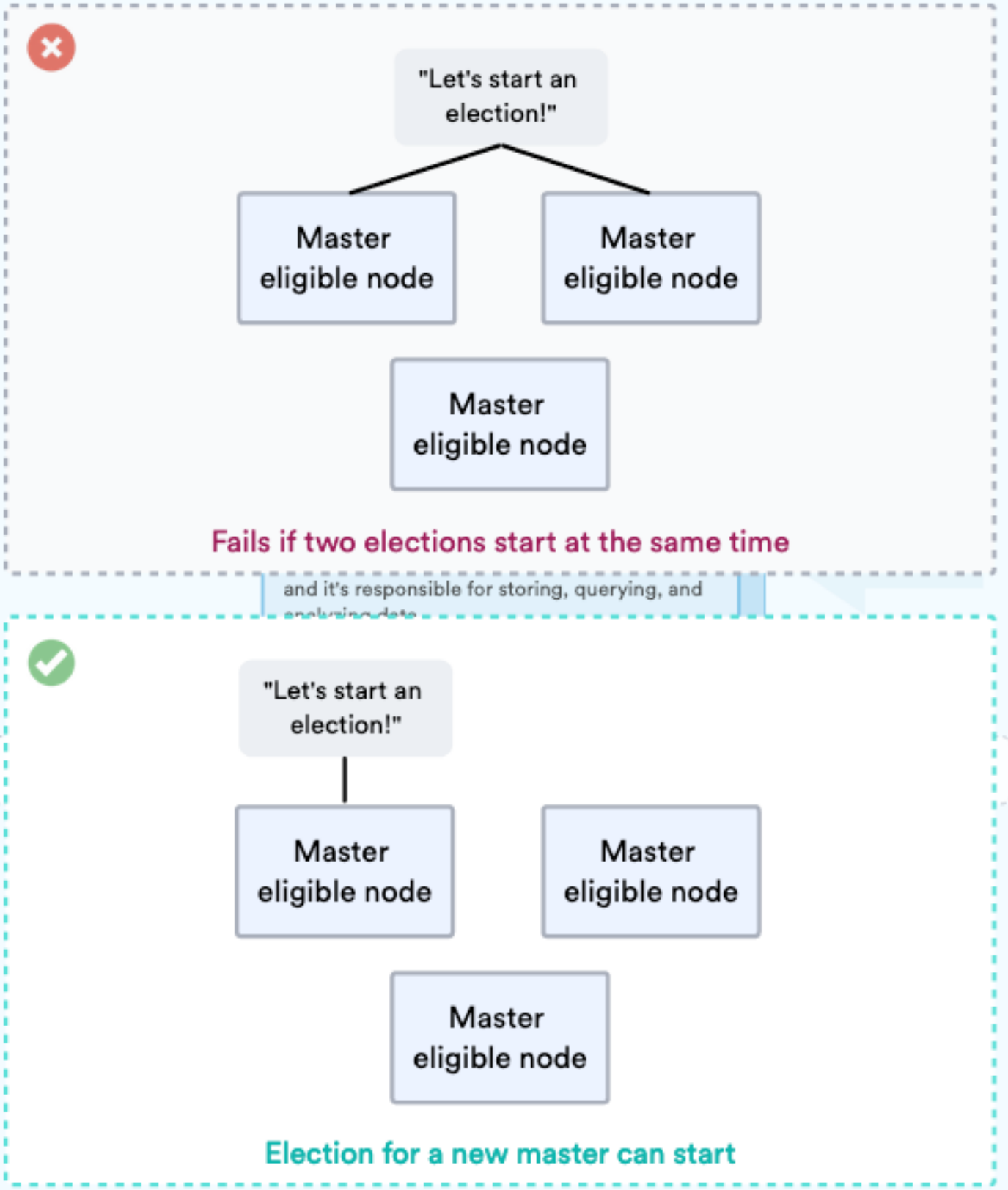
Elasticsearch

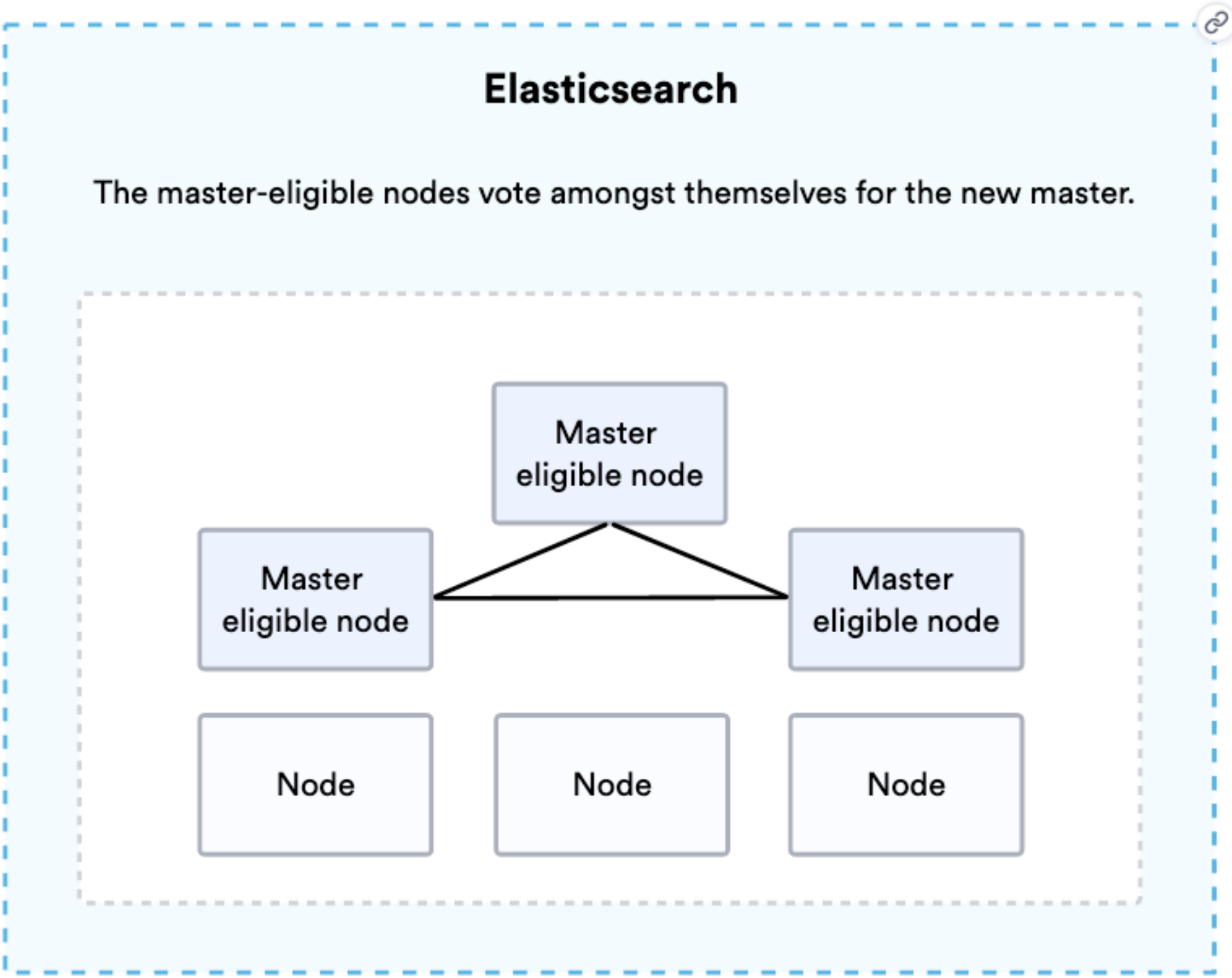
Every node connects to every seed node, and bidirectionally share other nodes that they know. After a few iterations, every node knows the existence of every other node and which ones are master-eligible



Elasticsearch

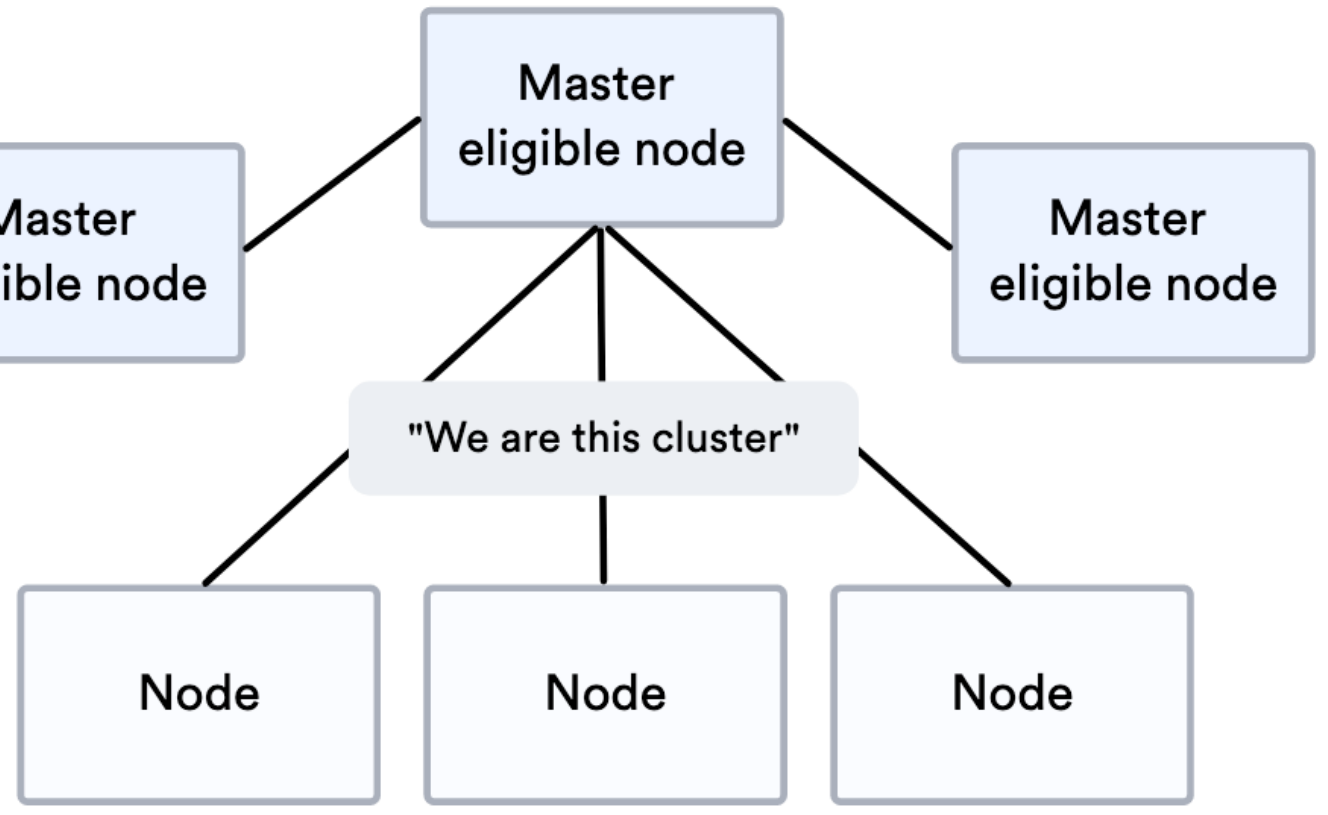
Any master-eligible node can start an election for the new master, and each one does so with some randomness so the two elections don't happen at once.





Elasticsearch

The master node is the only node that can make updates to the cluster state. It tells every other node how to behave and what their cluster is.



The settings for the cluster, like name, come from initial configurations of the nodes.

Elastic shard

A Lucerne index is made of multiple Lucerne segments. It's actually an inverted index, which maps terms to documents containing the terms. when a search is performed, every shard is queried, and the Lucerne index in turn queries all its segments