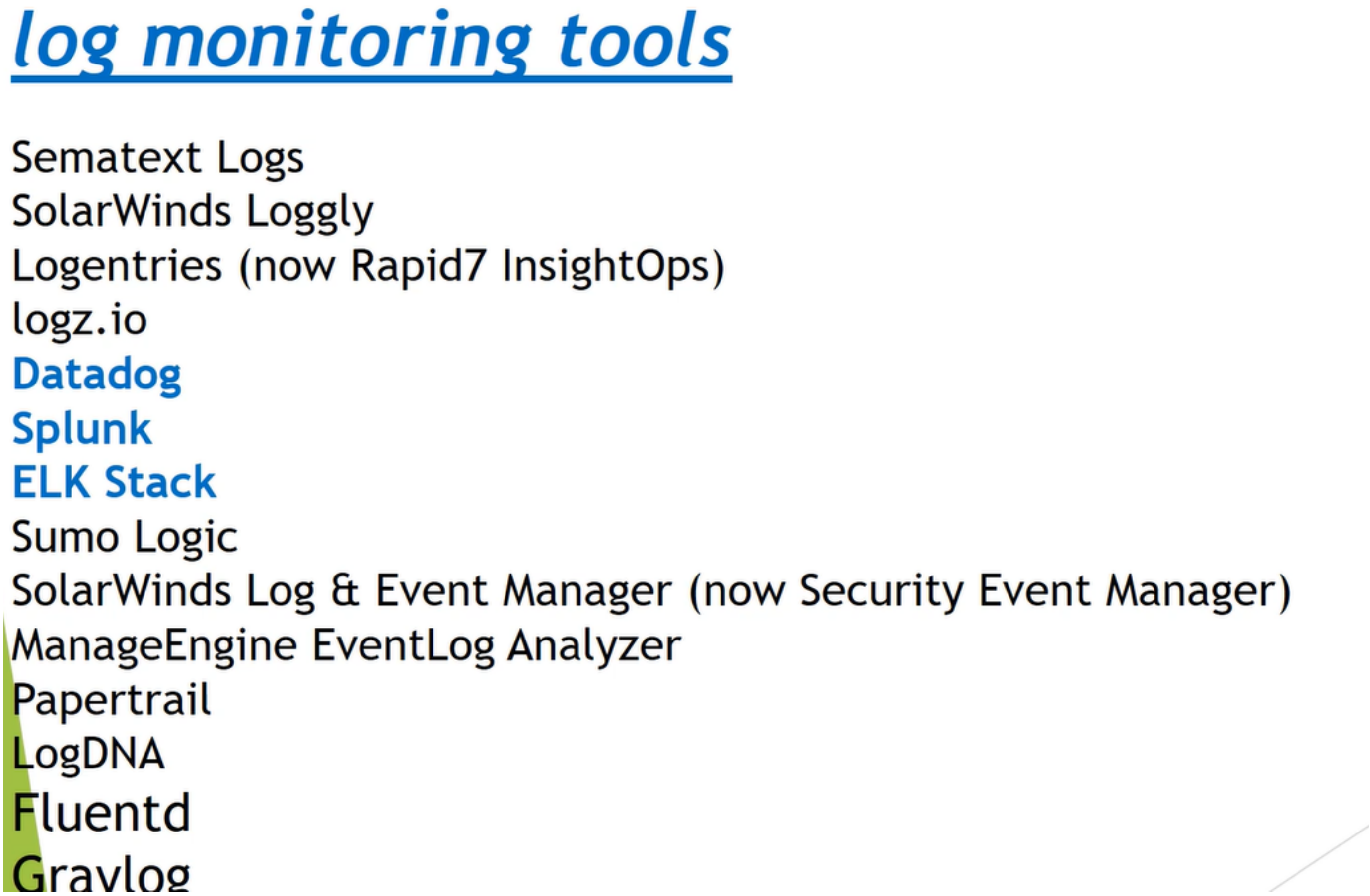
1. ELK Overview



log monitoring tools

Sematext Logs
SolarWinds Loggly
Logentries (now Rapid7 InsightOps)
logz.io
Datadog
Splunk
ELK Stack
Sumo Logic
SolarWinds Log & Event Manager (now Security Event Manager)
ManageEngine EventLog Analyzer
Papertrail
LogDNA
Fluentd
Graylog

What is ELK stacks/ ELK data pipeline

Elastic Search - It stores the log data in the form of index.

Logstash - It is used to parse the log data and transform data before sending it to elastic search. it can also be used as data shipper. It sends the parsed data in the form of JSON to ES.

Kibana - it reads data from ES and visualizes it. We can create graphs ,charts etc. also write the ES queries.

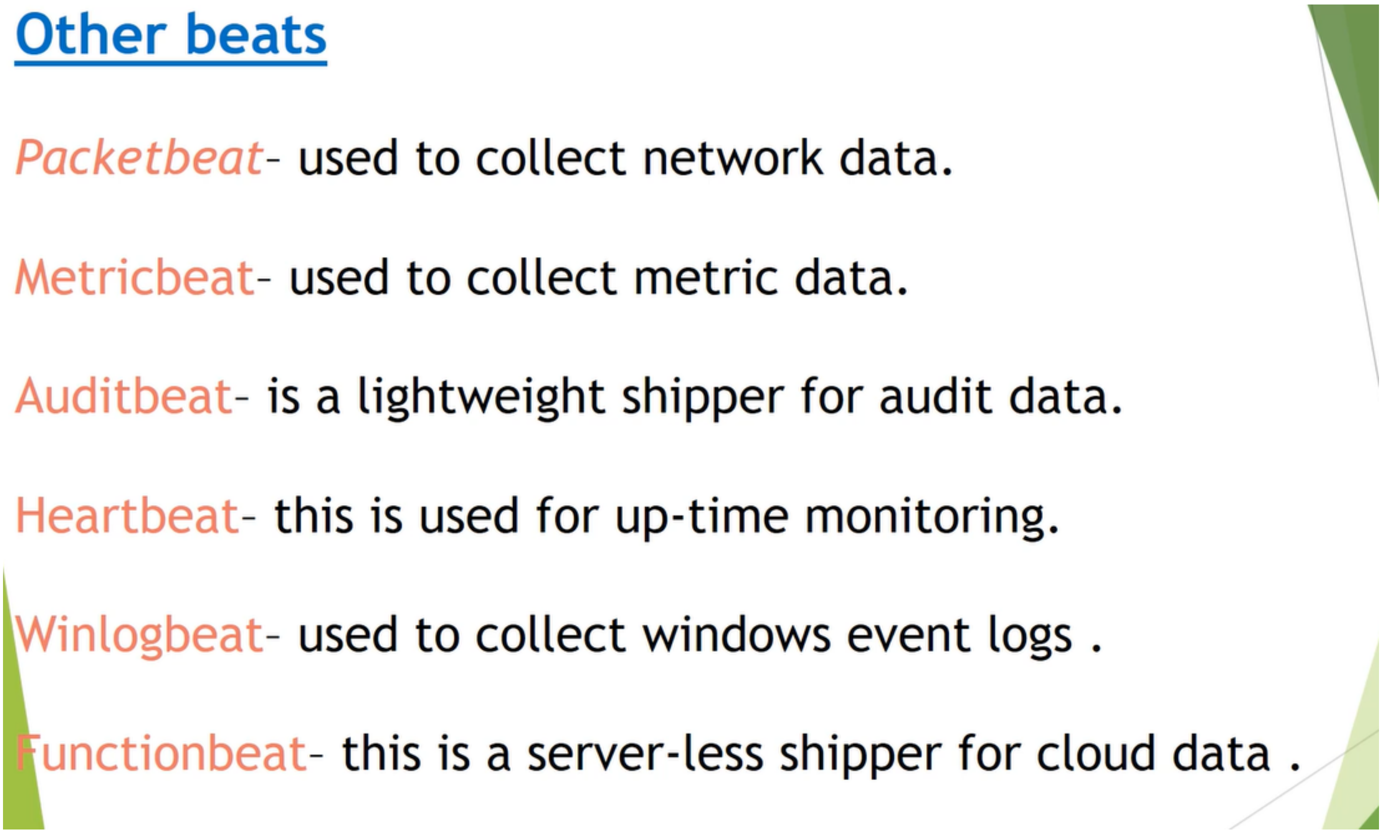
To create application related to server log monitoring, infrastructure monitoring

File Beat - Lightweight data shippers which sends the log data from file source (log file) to next ELK element like logstash/ES

For monitoring. It is recommended not mandatory to create ELK pipeline with file beat.

File Beat vs Logstash

If logstash can be used in the same server where log file is present then it is fine to use logstash as data collector. But when reading log files from remote server it is good to use file beat since it is quite lightweight.



Other beats

Packetbeat- used to collect network data.

Metricbeat- used to collect metric data.

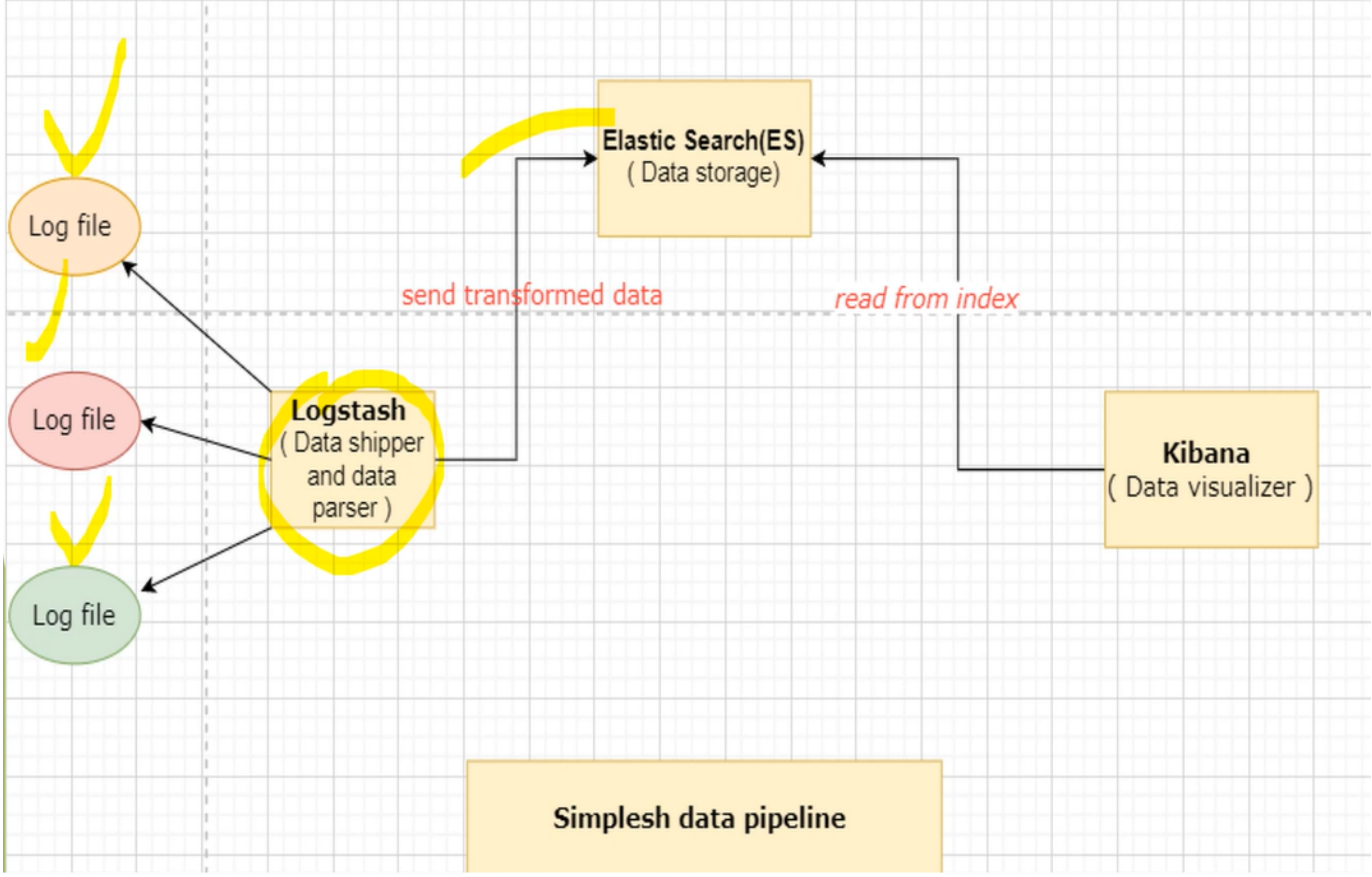
Auditbeat- is a lightweight shipper for audit data.

Heartbeat- this is used for up-time monitoring.

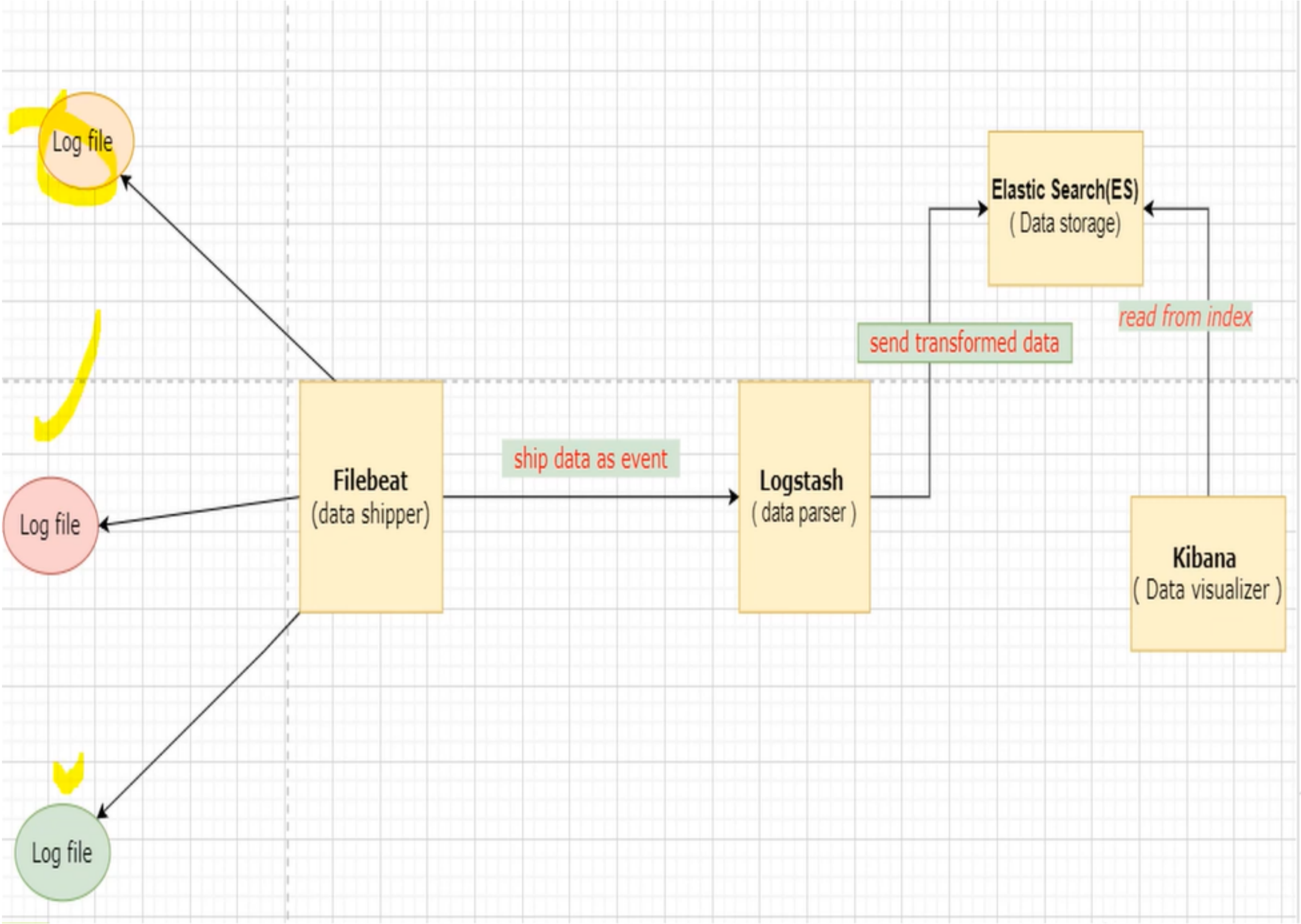
Winlogbeat- used to collect windows event logs .

Functionbeat- this is a server-less shipper for cloud data .

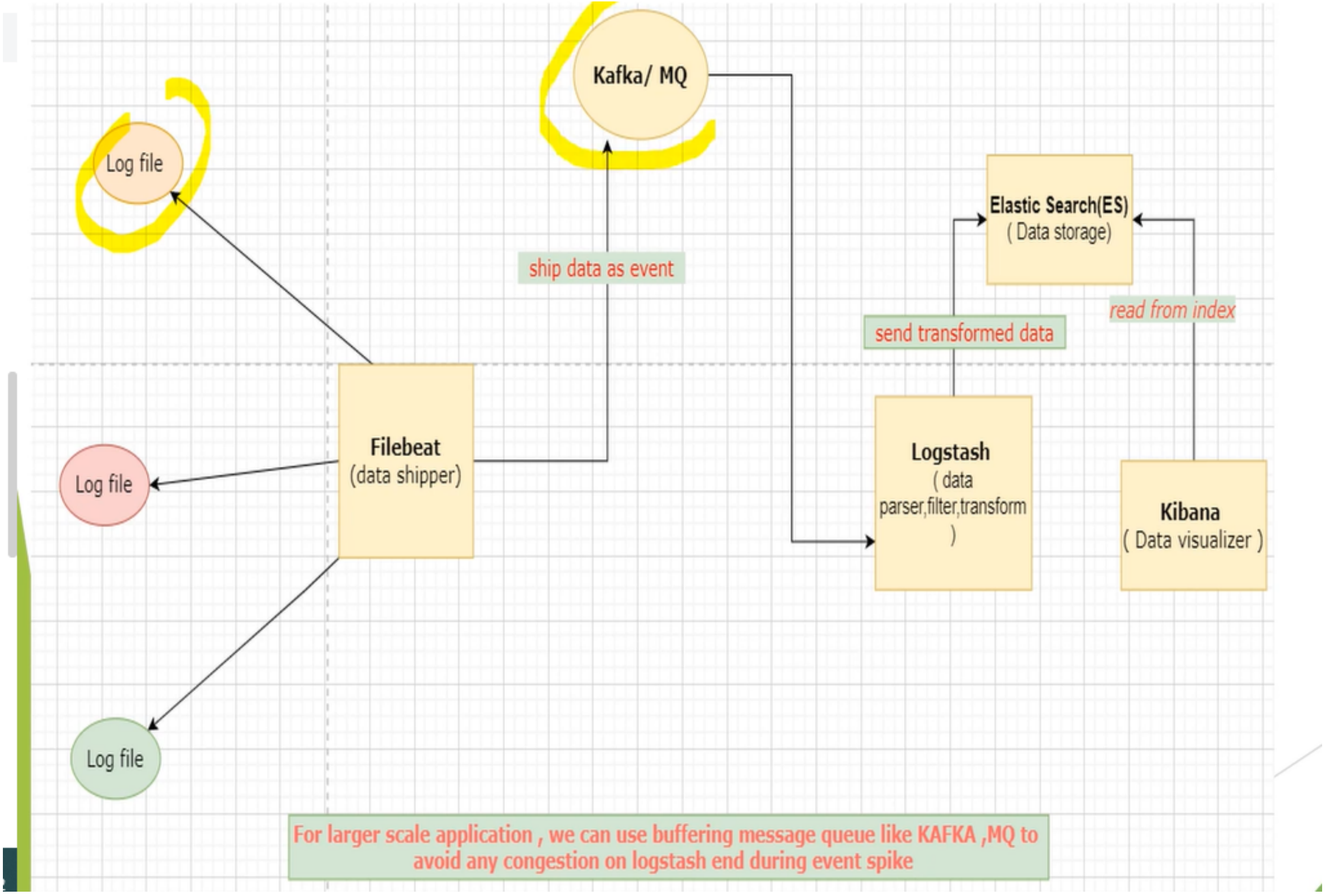
The architecture style:



Another architecture style



Another with file beat and kafka



For larger scale application , we can use buffering message queue like KAFKA ,MQ to avoid any congestion on logstash end during event spike