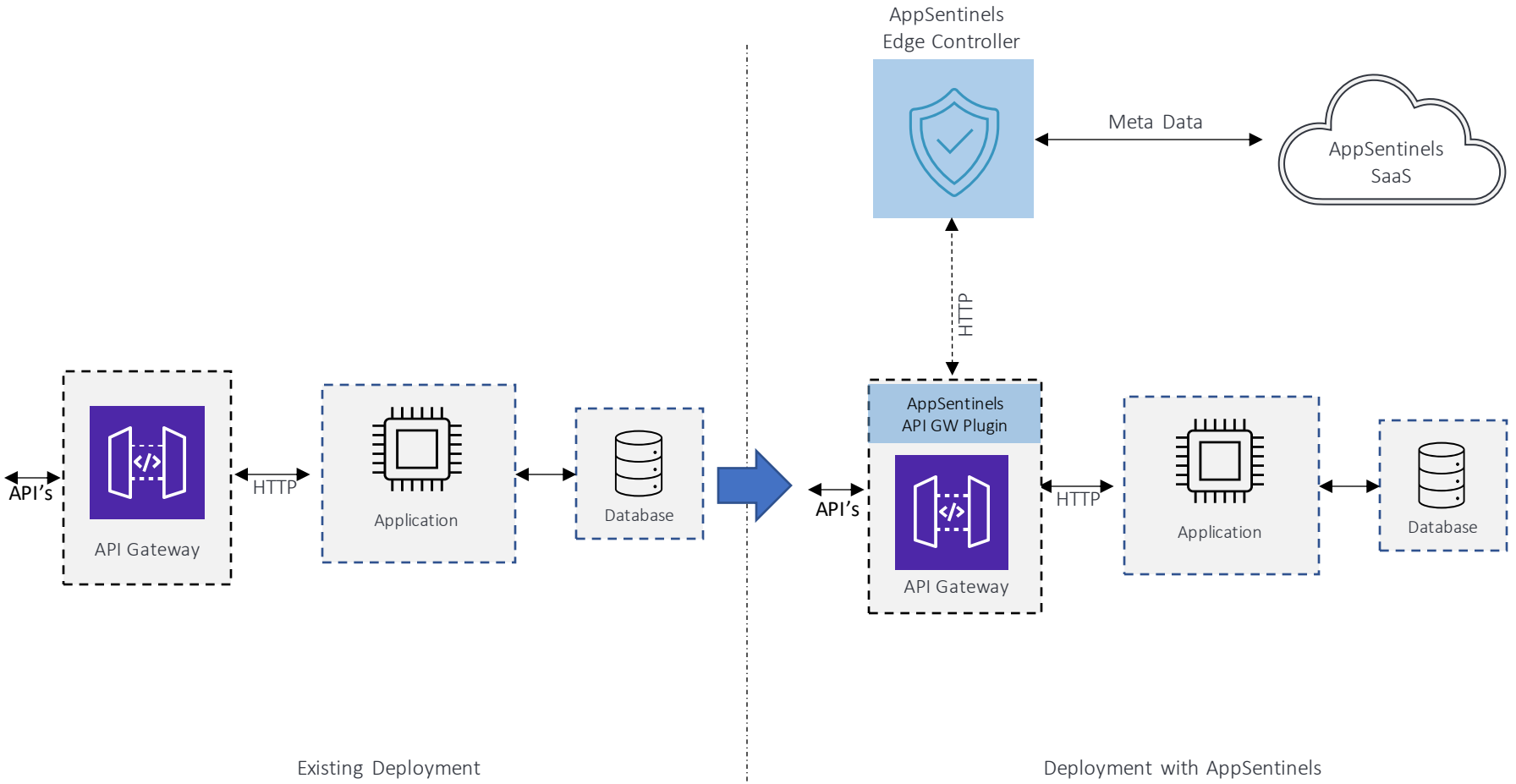
AppSentinels.ai
Application Security Re-invented

AppSentinels.ai

Application Security. Reinvented.

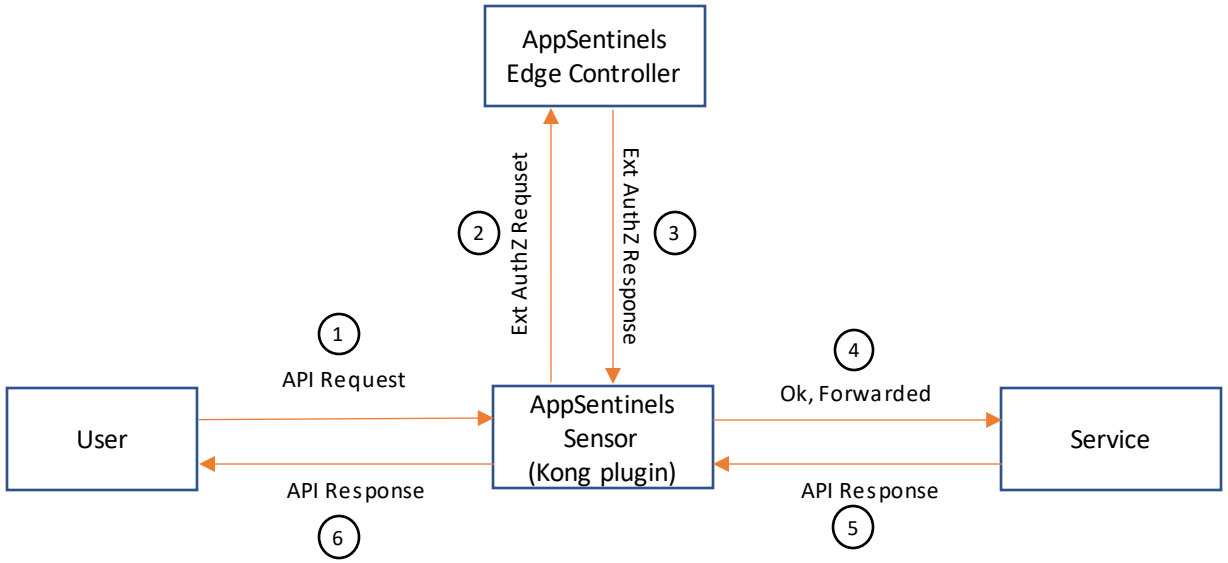
Kong support

Deployment: API Gateway (Kong)



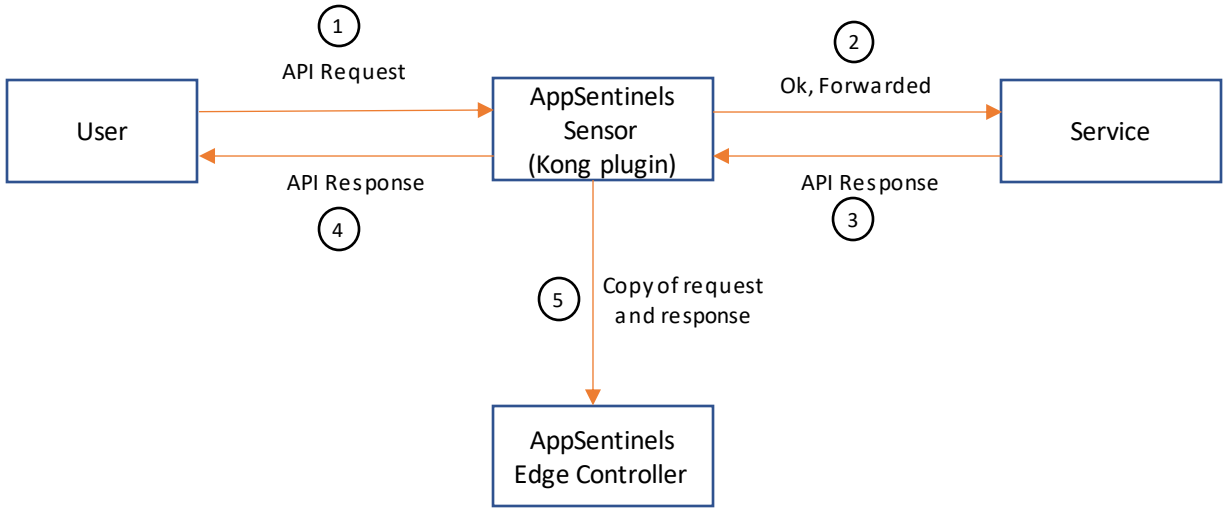
1. AppSentinels comes with Kong API GW plugin that is deployed on the Kong server.
2. Additionally AppSentinels Edge Controller is deployed in the environment and should be reachable from the Kong server.
3. AppSentinels Kong plugin gets HTTP traffic from Kong API GW and forwards logs to AppSentinels Edge Controller.
4. AppSentinels is in OOB mode (i.e, processing copy of a packet), thereby avoiding any impact to Applications in case of an outage.
5. AppSentinels has optional max latency configuration. In case latency crosses certain threshold, AppSentinels automatically gets into fail-open mode thereby ensuring latency for application traffic is maintained.
6. AppSentinels can block bad IP's or Users.

Day in the life of API Request – Service Chaining



1. In this mode, AppSentinels sensor will function by holding the packet till the security inspection is complete.
2. AppSentinels sidecars have optional max latency configuration. In case latency crosses threshold, AppSentinels sensor gets into fail-open mode thereby ensuring latency for application traffic is maintained.
3. AppSentinels can take session based actions like blocking a malicious request. The packet is forwarded to Server only after getting clean ExtAuthZ response from the Edge Controller. Otherwise, the packet will be dropped and 401 response is sent by the AppSentinels sensor.
4. The sensor can also take action against bad IP's or Users.
5. Behaviour to wait vs no-wait for Security evaluation is controlled by a knob
6. Fail-open or Fail-close behaviour is controlled by a knob

Day in the life of API Request – Out of Band (OOB)

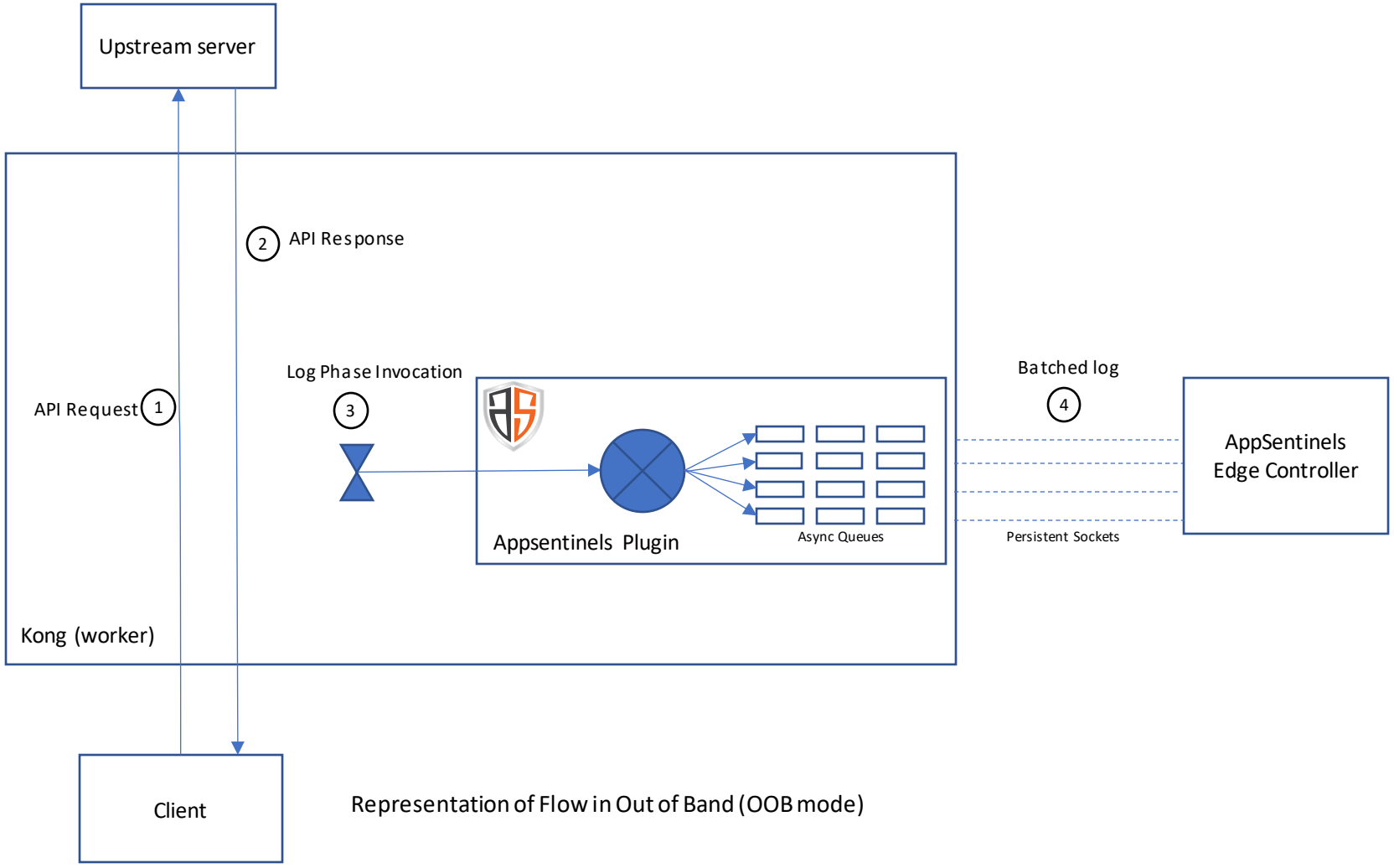


1. In this mode, AppSentinels sensor functions in OOB mode (working on copy of the packet). No impact to the application scale, response time or latency.
2. Session based actions like blocking a malicious request is not supported in this mode. Sensor can take action against bad IP's or Users.
3. Behaviour to wait vs no-wait for Security evaluation is controlled by a knob
4. Fail-open or Fail-close behaviour is controlled by a knob

Plugin Design

- Kong support is realized through plugin
- Single plugin supports both Out of Band and Service chaining mode
- Plugin supports multiple queues to asynchronously share logs with edge controller
- Optimizations like compression and batching of logs to reduce latencies and network I/O
- Cap on maximum size of payload that will be logged
- Dynamic shaper allows for upstream traffic priority over logging

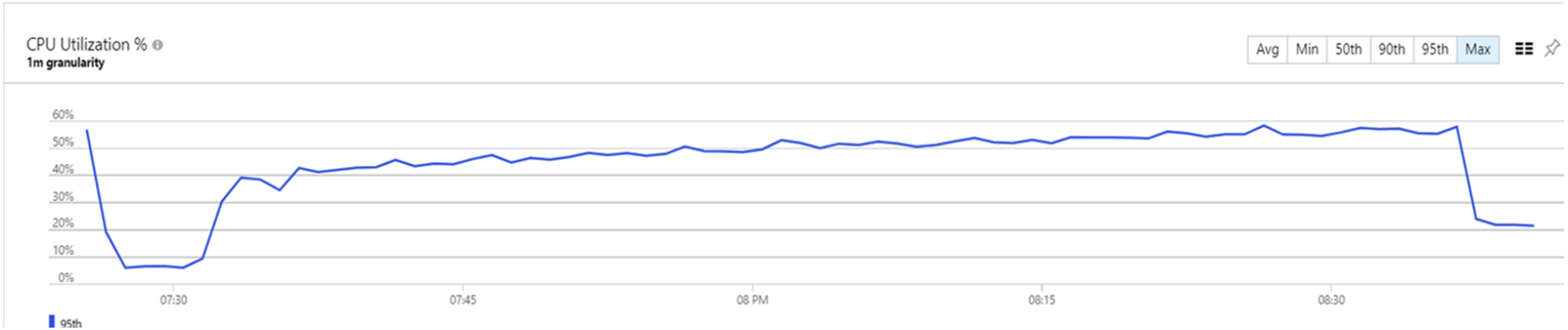
Plugin Design



Representation of Flow in Out of Band (OOB mode)

Business continuity with shaper

- Prioritizes upstream traffic over logging
- Dynamic shaper performs ramping up of logging rate
- Detects CPU limits (dynamically) and falls back on logging rate, leaving latencies unaffected
- Shaper ramp up rates are configurable along with fallback rates and error detection thresholds
- Idle fallback to ensure no surge in CPU when traffic resumes after a long time
- Representative image of slow and controller increase CPU utilization with shaper



Failure cases

- Edge Controller Disconnection
  - Services in edge controller dockers are self recovering within 10 seconds
  - Communication failure with edge controller causes fallback in logging rate in the plugin
- Traffic Burstiness
  - Shaper will increase logging only at defined rates irrespective of incoming. CPU utilization due to logging is always capped
  - Any logging failures due to eventual increase in logging rate (due to resource constraints) causes fallback to lower rate

AppSentinels.ai
Application Security Re-invented

Discover More About Your API's and Protect your API Breach

Contact:
www.appsentinels.ai
contact@appsentinels.ai