

AppSentinels API Security Platform

Selection of Sensor

Revision	Date Modified	Author	Comments
1.0	19-April-26	Sagar	Initial spec for Sensor Selection

Contents

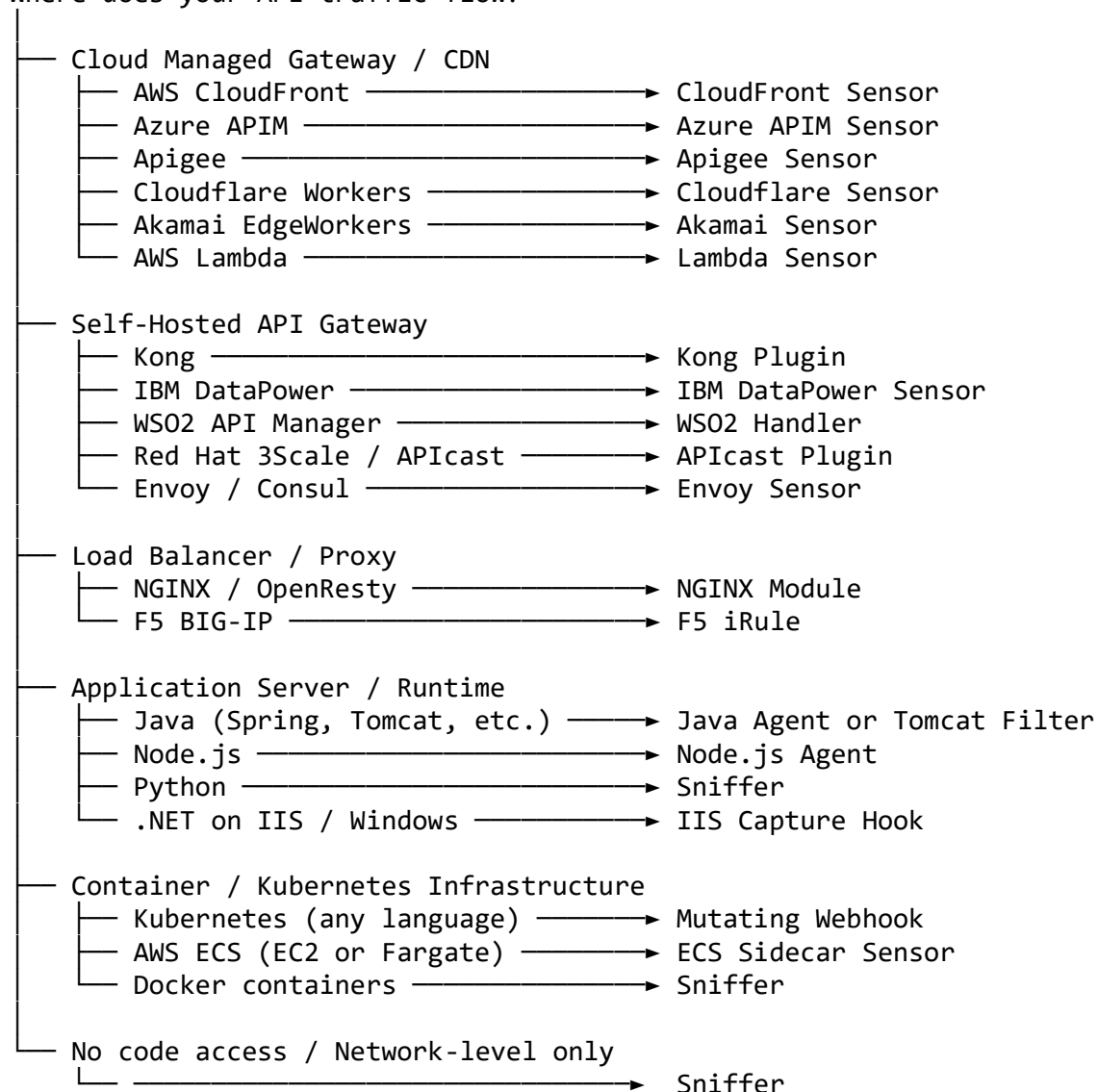
Introduction:.....	3
Type of Sensor depends on the infrastructure:.....	4
Choosing the Right Sensor:.....	5
Minimum Information Needed Per Sensor:	5
NGINX.....	6
IIS / .NET.....	6
Java Agent.....	6
Node.js Agent.....	6
AWS Lambda.....	6
AWS CloudFront.....	6
AWS ECS.....	6
Azure APIM.....	6
Apigee.....	7
Kong.....	7
IBM DataPower.....	7
WSO2.....	7
F5 BIG-IP.....	7
Cloudflare.....	7
Akamai.....	7
Kubernetes (Mutating Webhook).....	7
ECS Sidecar.....	7
SSL Sniffer.....	7
Envoy.....	7

Introduction:

A sensor is a component that is deployed on the infrastructure to capture API traffic and send it to the controller. Now the integration of sensors depends on the type of infrastructure. AppSentinels Platform requires unencrypted traffic for API Discovery; hence, the sensor/plugin integration should be implemented at the point where application traffic is decrypted

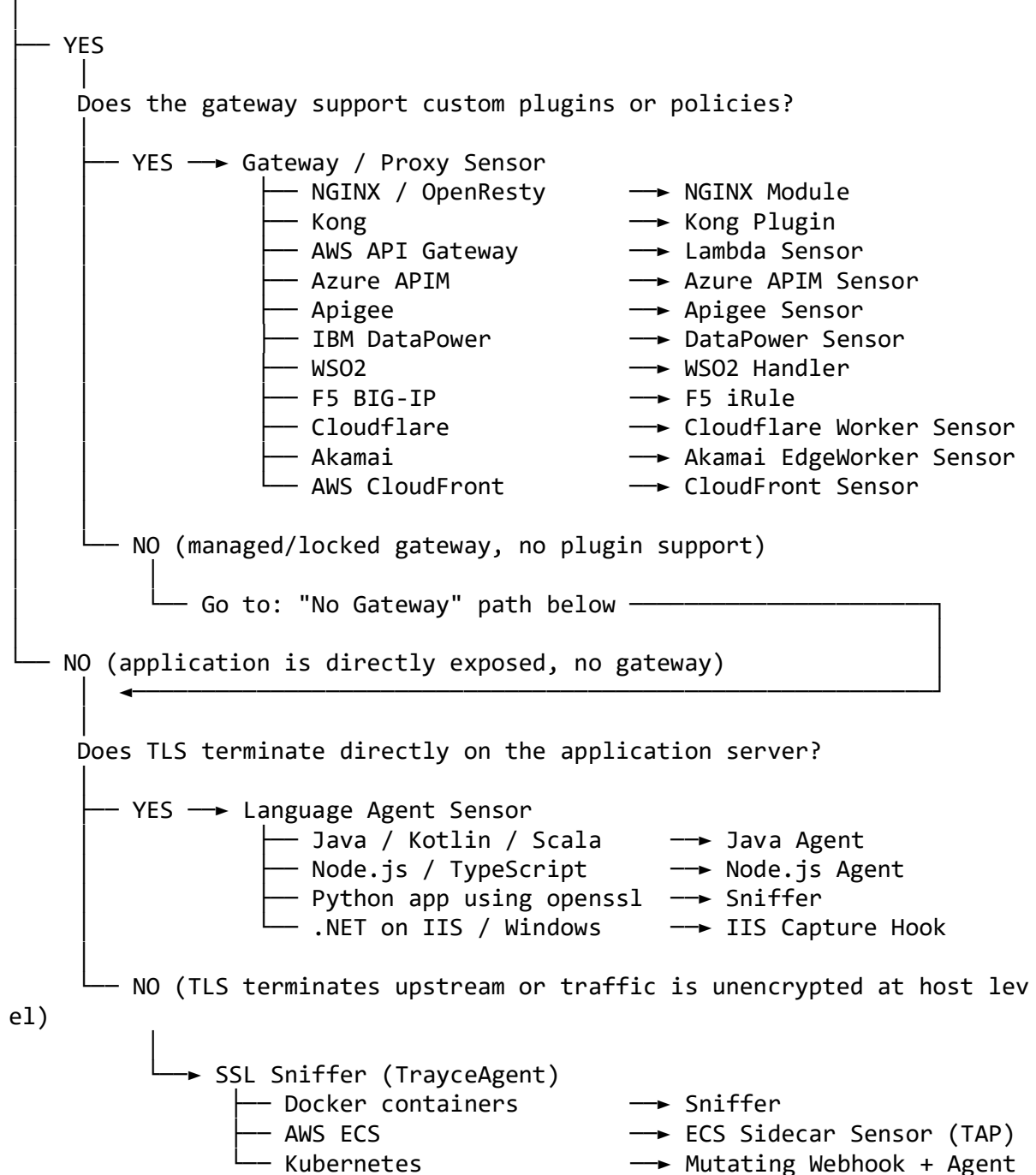
Type of Sensor depends on the infrastructure:

Where does your API traffic flow?



Choosing the Right Sensor:

Is there an API Gateway or Reverse Proxy in front of your services?



Minimum Information Needed Per Sensor:

NGINX

- OS and distribution (e.g., Ubuntu 22.04, Alpine, RHEL 8) (`cat /etc/os-release`)
- NGINX version (`nginx -V`)
- Flavor: standard NGINX or OpenResty
- Is TLS terminated at NGINX or upstream?
- Deployment method (systemd, Docker, Kubernetes Ingress Controller)

IIS / .NET

- Windows Server version (e.g., 2019, 2022)
- IIS version
- .NET version (`dotnet --version`)

Java Agent

- JVM version and vendor (e.g., OpenJDK 17, Amazon Corretto 11, Azul Zulu 21)
- Application framework (e.g., Spring Boot, Micronaut, Vert.x)
- Any existing APM agents attached? (Datadog, New Relic, Dynatrace)
- Deployment method (systemd, Docker, Kubernetes)

Node.js Agent

- Node.js version (`node --version`)
- Application framework (e.g., Express, Fastify, NestJS)
- Deployment method (bare-metal, Docker, AWS Lambda Layer)

AWS Lambda

- Lambda runtime (e.g., Node.js 20, Python 3.11, Java 17)
- Invocation model: synchronous or asynchronous
- Number of existing Lambda Layers attached

AWS CloudFront

- CloudFront Distribution ID
- Is request/response body forwarding enabled to Lambda@Edge?

AWS ECS

- Launch type: EC2 or Fargate
- Task network mode (bridge, awsvpc, or host)

Azure APIM

- Any existing policies deployed on the target APIs?

Apigee

- Apigee edition (X, hybrid, or legacy Edge)
- Java version in the Apigee environment (8, 11, or 21)
- Any existing shared flow bundles deployed on the proxies?

Kong

- Kong version and edition (OSS or Enterprise)
- Deployment method (Docker, Kubernetes/Helm, bare-metal)

IBM DataPower

- DataPower firmware version (e.g., 10.5.x)
- Standalone DataPower or IBM API Connect (managed)?
- DataPower domain where APIs are published
- Api Version V5 or V10

WSO2

- WSO2 API Manager version (e.g., 4.2.0)
- Typical request/response payload size

F5 BIG-IP

- BIG-IP version (e.g., 16.1, 17.1)

Cloudflare

- None

Akamai

- None

Kubernetes (Mutating Webhook)

- Kubernetes distribution (EKS, GKE, AKS, OpenShift, Rancher)
- Languages/runtimes used by the pods (Java, Node.js, etc.)
- Is a private container registry in use?

ECS Sidecar

- Launch type: EC2 or Fargate
- Task network mode (bridge, awsvpc, or host)

SSL Sniffer

- Linux kernel version on the Docker host (`uname -r`) — must be ≥ 4.14
- Can privileged containers run on this host?
- Container runtime in use (Docker, containerd, CRI-O)

Envoy

- Envoy version (e.g., 1.27.x)
 - Deployment: standalone proxy or service mesh (Istio, Consul Connect)?
-