AppSentinels API Security Platform Deployment

Contents

Revision	Date Modified	Author	Comments
1.0	01-Aug-24	Elango	Initial spec
1.1	05-Aug-24	Elango	Minor comments addressed

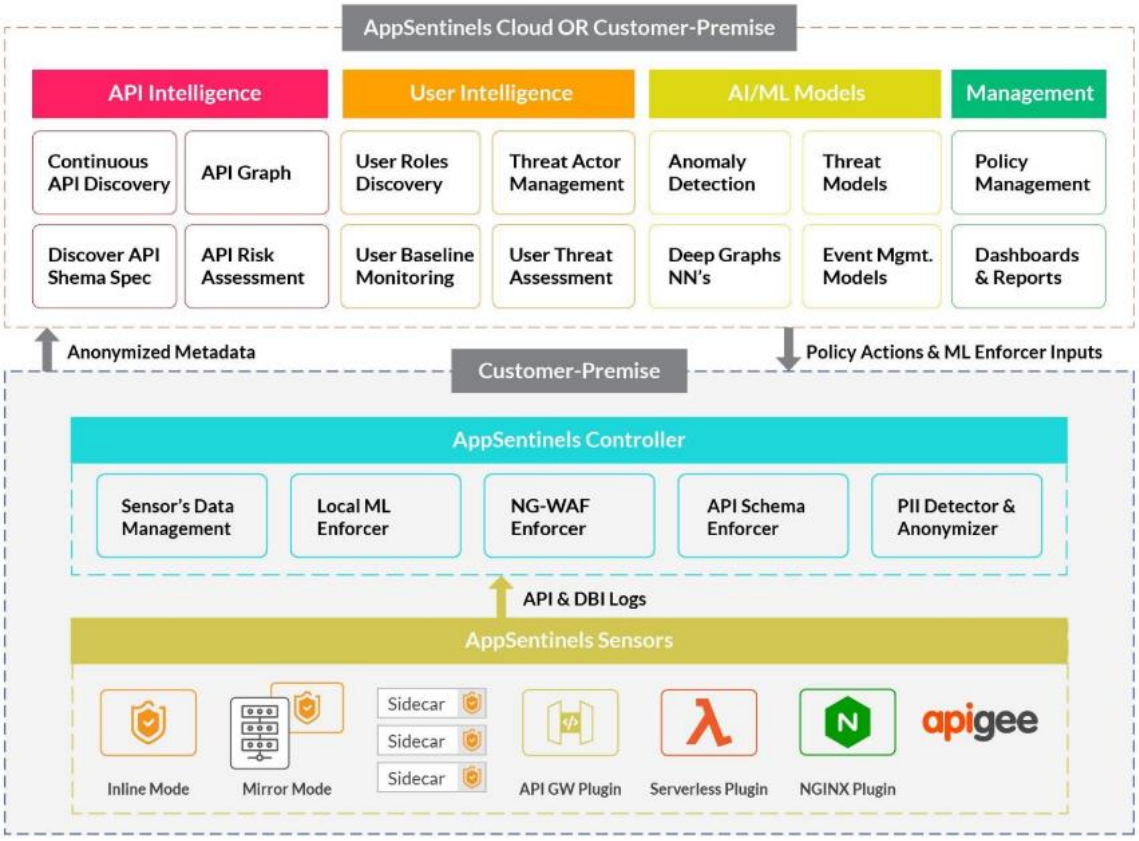
On-Prem Installation Pre-Requisites

The AppSentinels API Security Platform is a SaaS-delivered application security solution designed for high availability, low latency, and ultra-high scalability.

The platform is built on a three-tier architecture with the AppSentinels Sensor, AppSentinels Edge Controller, and API Security Platform as its components. It has an add-on component for Dynamic Application Security Testing (DAST).

For highly regulated industries AppSentinels also offers a complete on-premises instance where all advanced AI/ML models are hosted internally, ensuring no data leaves the organization's boundary.

The following diagram illustrates this architecture in detail.



The following are the requirements for a complete on-premises deployment:

Operating System and Hardware Requirements

- Operating System: Ubuntu 20.04 (preferred) or REDHAT 8.6
- CPU: 16 cores x86_64
- RAM: 64G of RAM.
- Storage:
    - 100 GB free disk space in /var partition
    - 250GB to 1TB disk for data and logs, depending on the volume of traffic

Packages Required

- docker version 23.0 or higher
- docker-compose version 1.28.6 or higher

Network Connectivity Requirements

- TCP Port 443 should be opened to allow access to the AppSentinels Platform UI Console
- The TCP port range 9002-9007 should be opened for the AppSentinels Sniffer Sensor/Plugin to send traffic logs to the AppSentinels Controller. The specific port used will depend on the integration between the Sensor/Plugin and the AppSentinels Controller. – This is applicable only if AppSentinels Controller deployed on the same server.
- Access to *.docker.io to download the Docker images. If *.docker.io can't be allowed, access has to be provided to the following domains
    - docker.io
    - auth.docker.io
    - registry-1.docker.io
    - production.cloudflare.docker.com
- Access to fs.appsentinels.ai to download the installation package.
- Signed SSL certificate for communication between AppSentinels Controller & AppSentinels Server (optional)."

Proxy Configuration

If proxy installed on the system,

- Proxy should be disabled or excluded for the local host, hostname and host IP communications.
- Proxy should be disabled for Docker environment

DAST Requirements

- Network connectivity to application under test from AppSentinels Platform server
- Two test users with credentials for API security testing of authenticated APIs

AppSentinels API Security Platform Installation

Information Required:

OSENV="RHEL" or "UBUNTU" *# Operation System*

HOSTNAME="CONFIGURE.appsentinels.ai" *#Host name of the Server*

IPADDRESS="1.2.3.4" *# IP Address of the server*

ADMIN_USER="admin@appsentinels.ai" *# Org admin user for AppSentinels Platform*

ORG_ID="demo" *# Organization Name*

ORG_NAME="Demo" *# Application Name*

RELEASE_VERSION="24.07.R2-latest" *# AppSentinels Platform Version*

BASE_DIR="/appsentinels" *# AppSentinels Platform Install and data directory*

Pre-Installation Checks

- Proxy Configuration check
- docker & docker-compose installed on the machine
- Signed or Self-signed certificates are copied to INSTALL_DIR/certs
- BASE_DIR (/appsentinels) is created and has 777 permission
- Host name should be DNS reachable, if not update the /etc/hosts file
- TCP Port 443 is open and accessible from outside

Install Procedure

*** Please contact AppSentinels Support team (support@appsentinels.ai) for installation package**

Follow the readme in the installation for installing AppSentinels API Security Platform

- Copy the installation package
- Copy the microservice images (~15 GB) if access to docker hub is not allowed
- Load the docker images
- Install the AppSentinels Platform (login & logout after installation)
- Configure the Platform requirements
- Create organization for application to monitor
- Login to AppSentinels Platform and upload the license file for dashboard access

