API Security Audit

A partnership between 42Crunch and WSO2

28th May 2020

8.30 P.M (IST), 8.00 A.M (PST), 11.00 A.M (EST), 4.00 P.M (BST), 3:00 P.M (UTC)

WSO2 API Manager

WSO2 API Manager 3.1.0 - Introduction

Problem

An increase in the number of consumers makes managing services/microservices hard such as security, access control etc.

Solution

WSO2 API Manager

100% Open Source

Full API Lifecycle Management

Policy Enforcement

Monetization

What is the WSO2 API Manager?

Design

API Publisher

Design & Publish API

API Developer Portal

Consume APIs

API discovery, read API docs, quick try out etc.

Runtime

Gateway/Microgateway

Intercepts all requests applies policies, mediates messages & feeds data to analytics engine

Key Manager

Issues/validates secure tokens for consuming devices/applications

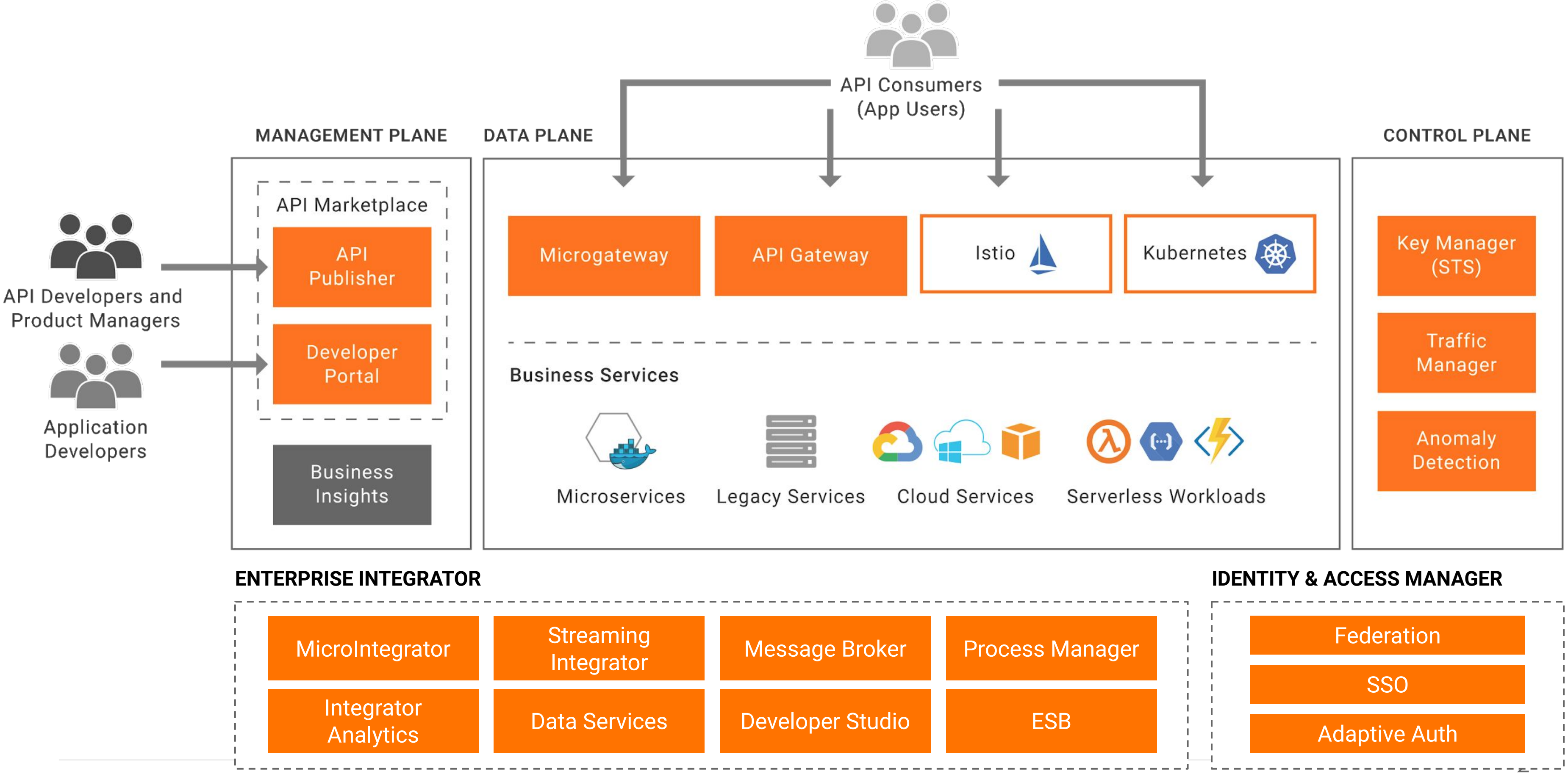
Traffic Manager

Applies rate limiting policies on the gateway

Analytics

Collects & processes data to give insights on the business

WSO2 API Management Overview



API Consumers (App Users)

API Developers and Product Managers

Application Developers

MANAGEMENT PLANE

API Marketplace

API Publisher

Developer Portal

Business Insights

DATA PLANE

Microgateway

API Gateway

Istio

Kubernetes

Business Services

Microservices

Legacy Services

Cloud Services

Serverless Workloads

CONTROL PLANE

Key Manager (STS)

Traffic Manager

Anomaly Detection

ENTERPRISE INTEGRATOR

MicroIntegrator

Streaming Integrator

Message Broker

Process Manager

Integrator Analytics

Data Services

Developer Studio

ESB

IDENTITY & ACCESS MANAGER

Federation

SSO

Adaptive Auth

API Security

The State Of API Security

- **83%** of all web traffic is now API traffic *(Akamai, 2019)*
- **363** different APIs are being managed by organizations on average, with **69%** of them making those APIs public *(Survey: APIs a Growing Cybersecurity Risk | Imperva, 2018)*
- APIs will be the most frequently attacked vector for enterprise web application data breaches by **2022** *(How to Build an Effective API Security Strategy, 2017)*

Why API Security Must Not Be An Afterthought

Not taking API Security seriously can have devastating consequences on organizations:

- Operation disruptions
- Negative publicity
- Legal problems
- Repeat attacks
- Suppliers can be compromised

Facebook Data Breach - 2019*

- Security expert Bob Diachenko discovered database containing sensitive information of more than **267 million** Facebook users were left exposed.
- Exposed data included *Facebook ID*, *phone number*, *email address* and *other profile details*.
- It is highly suspected that the data was stolen from Facebook's Developer API, which allowed third-party developers access to phone numbers until 2018.
- Could have been prevented if vulnerabilities in the Developer API are identified and fixed pro-actively.

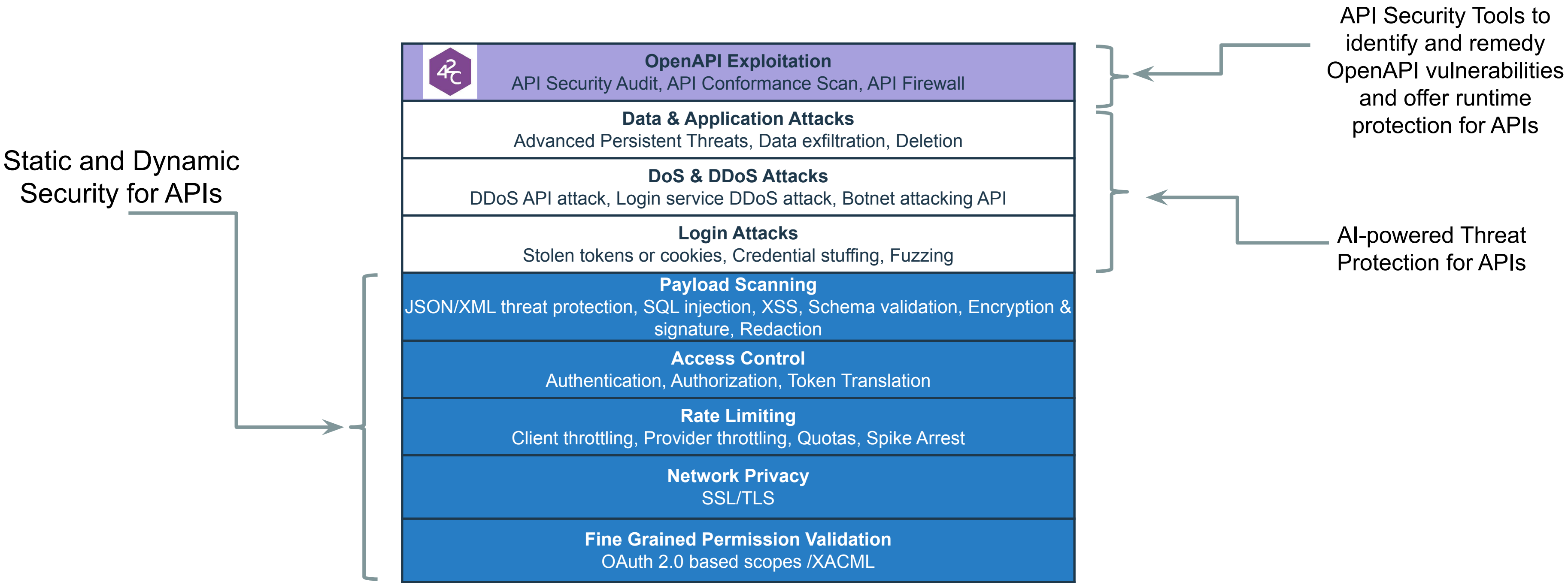
*(267M Facebook Users' Phone Numbers Exposed Online, 2019)

API Security in WSO2 API Gateway

- Static Checks
  - SQL injection
  - Parsing attacks(XML/JSON)
  - Payload attacks*
  - **OpenAPI Security Violations/Vulnerabilities**
  - Schema violations*
  - SSL/TLS
  - **API Implementation and API Contract mismatches**

- Dynamic Checks
  - Rate limiting for API calls.
  - Throttle API calls.
  - Authentication/Authorization.
  - Anomaly detection.
  - AI based threat detection.
  - **Real-time protection for APIs via API Firewall**

Combined Security Features



API Security Tools to identify and remedy OpenAPI vulnerabilities and offer runtime protection for APIs

AI-powered Threat Protection for APIs

Static and Dynamic Security for APIs

OpenAPI Exploitation
API Security Audit, API Conformance Scan, API Firewall

Data & Application Attacks
Advanced Persistent Threats, Data exfiltration, Deletion

DoS & DDoS Attacks
DDoS API attack, Login service DDoS attack, Botnet attacking API

Login Attacks
Stolen tokens or cookies, Credential stuffing, Fuzzing

Payload Scanning
JSON/XML threat protection, SQL injection, XSS, Schema validation, Encryption & signature, Redaction

Access Control
Authentication, Authorization, Token Translation

Rate Limiting
Client throttling, Provider throttling, Quotas, Spike Arrest

Network Privacy
SSL/TLS

Fine Grained Permission Validation
OAuth 2.0 based scopes /XACML

42crunch

Platform Overview

Design

Developer initiates security work at design time.

Best practices and recommendations are documented.

APIsecurity.io

Develop

Developer documents the API contract with OpenAPI/Swagger.

API Contract security is evaluated from VSCode using 42Crunch plugin.

Integrate & Test

API Contract quality is enforced via CI/CD pipeline. Builds are blocked when minimal security requirements defined by security teams are not met.

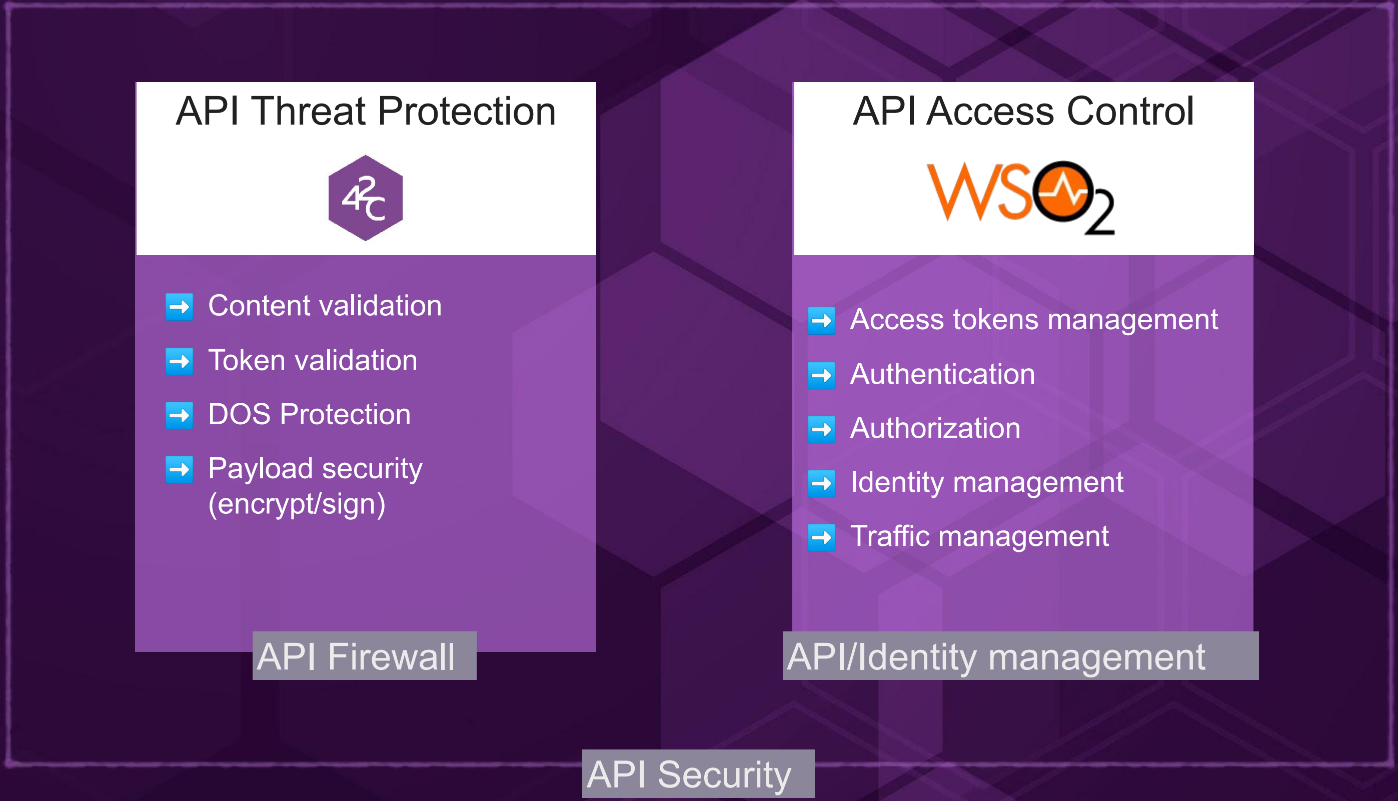
API implementation is tested via Conformance Scan

Deploy & Protect

API Firewall is automatically configured from OAS file and deployed in line of traffic.

The firewall can be deployed as sidecar in Kubernetes or reverse proxy in front of API Management solutions.

42CRUNCH AND API MANAGEMENT ARE COMPLEMENTARY



API Threat Protection

- Content validation
- Token validation
- DOS Protection
- Payload security (encrypt/sign)

API Firewall

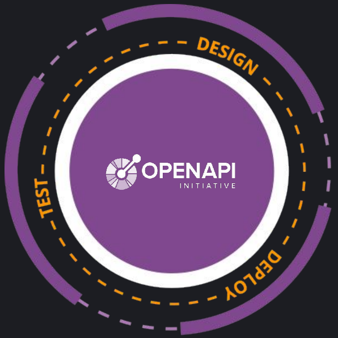
API Access Control

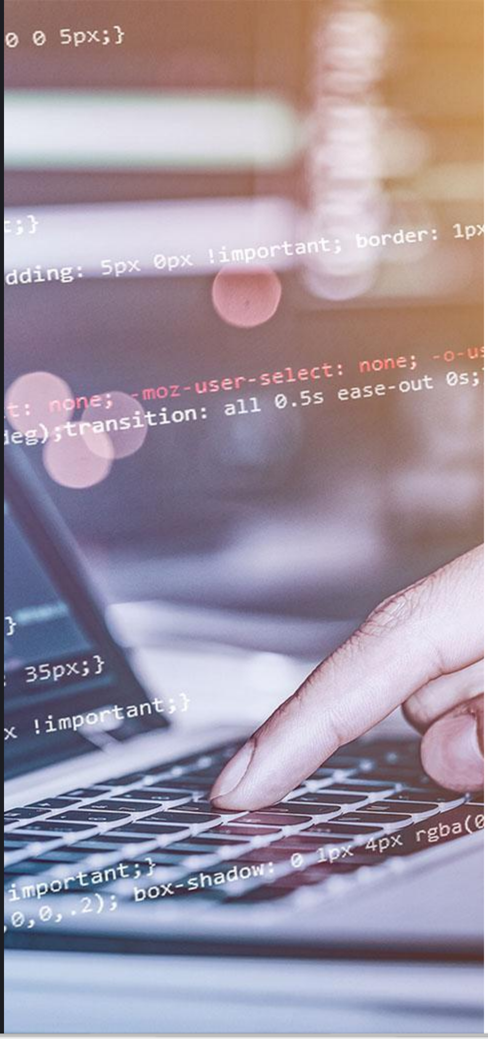
- Access tokens management
- Authentication
- Authorization
- Identity management
- Traffic management

API/Identity management

API Security

DEVELOPERS INITIATE SECURITY AT DESIGN TIME





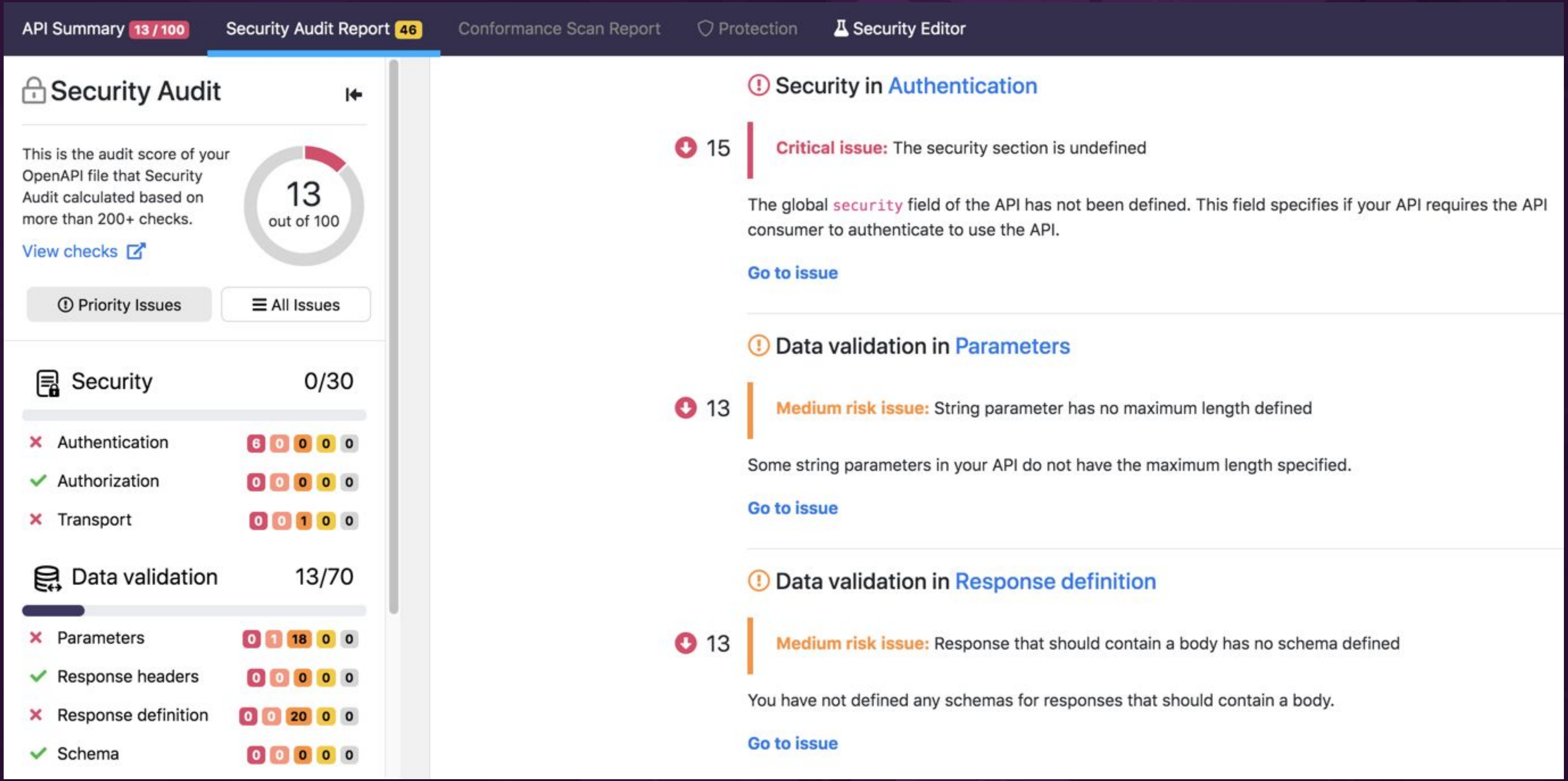
The **42C Audit service** performs 200+ security checks

- Developers describe the API contract in a language they know
- Audit is available from IDEs and CI/CD plugins
- Actionable report with **zero false positives**

Key Benefits

- Instant visibility into API security status
- Governance of corporate security standards
- Required security is declared instead of developed/maintained manually across multiple tools/environments

SAMPLE REPORT



Security Audit

This is the audit score of your OpenAPI file that Security Audit calculated based on more than 200+ checks.

View checks

13 out of 100

Security 0/30

✗	Authentication	6	0	0	0	0
✓	Authorization	0	0	0	0	0
✗	Transport	0	0	1	0	0

Data validation 13/70

✗	Parameters	0	1	18	0	0
✓	Response headers	0	0	0	0	0
✗	Response definition	0	0	20	0	0
✓	Schema	0	0	0	0	0

Security in Authentication

15 **Critical issue:** The security section is undefined

The global `security` field of the API has not been defined. This field specifies if your API requires the API consumer to authenticate to use the API.

Go to issue

Data validation in Parameters

13 **Medium risk issue:** String parameter has no maximum length defined

Some string parameters in your API do not have the maximum length specified.

Go to issue

Data validation in Response definition

13 **Medium risk issue:** Response that should contain a body has no schema defined

You have not defined any schemas for responses that should contain a body.

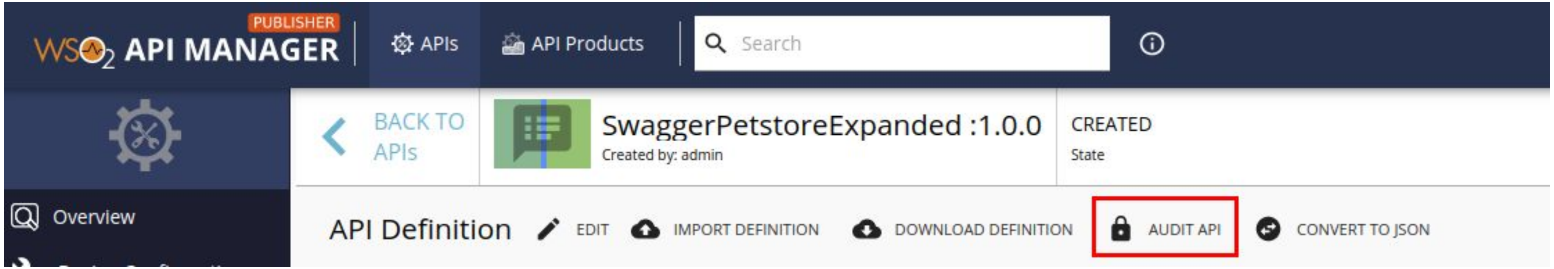
Go to issue

How To Secure APIs Proactively?

- Step 1 - Make sure API Definitions conform to OAS.
- Step 2 - Perform comprehensive security audits on API Definitions

Integration Implementation

- The API Security Audit functionality is built-in to WSO2 API Manager
- Once it is enabled, an Audit API button will be shown in the API Definition tab in API Publisher
- Clicking on the Audit API button will send the API Definition to 42Crunch to be audited
- The result from the audit will be shown as a report in API Publisher



Demo

bit.ly/security-audit-doc

Q&A

THANK YOU

wso2.com