PRODUCT SHEET

UBIKA WAAP GATEWAY
Advanced Package

A tailor-made solution designed to meet your highest security needs

Our Advanced Package security modules provide a higher level of protection for your business, ensuring peace of mind and confidence in your operations. Choose the UBIKA WAAP Gateway solution boosted with the Advanced Package for complete protection of your applications.

Advanced API Security

JSON, XML or Open API3 schema validation

The proliferation of APIs has made them a prime target for cyberattacks. Ensuring the protection of this new attack surface has become a significant challenge for companies. OpenAPI3 is the latest version of the OpenAPI specification, the industry standard for describing your API endpoints, parameters, and responses in a readable format.

Are you concerned about the security of your APIs?

Thanks to the Adv module. API Security, boost the security of your whitelisted APIs with schema validation: JSON, XML, Swagger2, OpenAPI3 or even in learning mode, without having the schema.

Goals

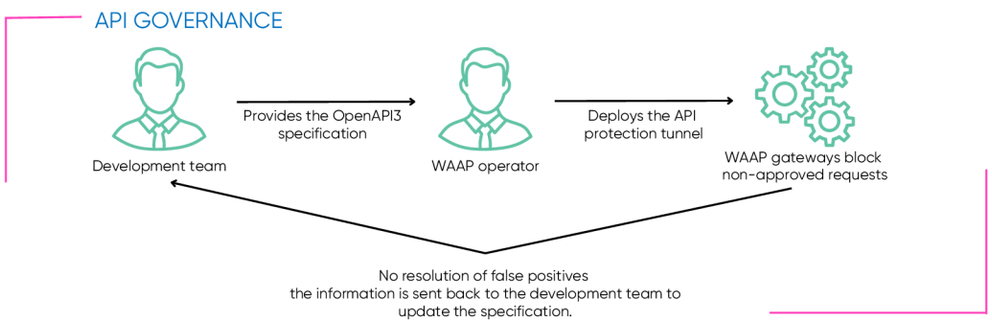
- Strengthen the security of your APIs.
- Whitelist security: only requests respecting the provided schema will be able to reach your APIs.
- No management of false positives.
- Promote collaboration between your development teams.
- Strengthen the security of your APIs.

How to proceed ?

1. Load the OpenAPI3 file into the WAAP Gateway UBIKA.
2. Add an "OpenAPI3 Validation" type node in your workflow.
3. Requests not respecting the descriptor will be automatically detected.
4. Thanks to the flexibility of the workflow you will be able to block these requests and adapt the response to your uses

Benefits

- Cyber Resilience / Risk Mitigation
- Cost reduction
- Customer satisfaction
- Agility / DevSecOps
- Innovation



Encryption and Authentication

Authentication, which consists of validating the identity of users, constitutes another major problem when using APIs. Not all users should be able to access information requiring a high level of privilege.

The API Encryption module strengthens API protection by ensuring data and identity integrity. This functionality is accessible directly from the WAAP Gateway UBIKA workflow.

API Encryption allows strong authentication with optional Web Access Manager (WAM) modules. It adds security to APIs using encryption and signing or modern authentication protocols.

How ?

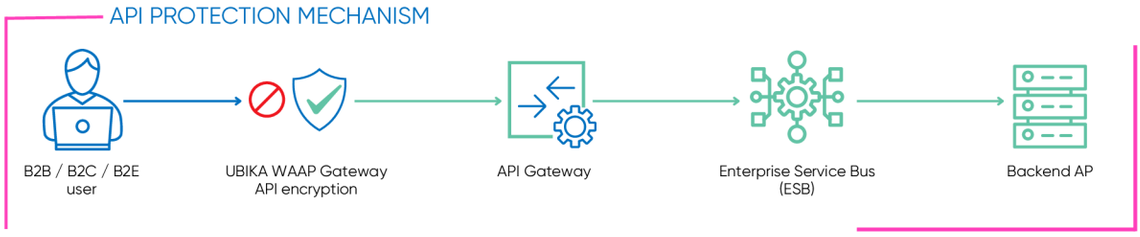
By using the bricks from the "API Security" category in your workflow: XML Decrypt, XML Encrypt, XML Signature Verify, XML Sign, XML Schema Validation, JSON Schema Validation, JWT Generate, JWT Parsing.

Goals

- Advanced filtering of XML and JSON APIs.
- JSON web token to integrate industry standards for API authentication (OAuth, OpenID Connect).
- Validation of JSON / XML schemas (checking the conformity of the data content).
- Obfuscation, filtering and manipulation of JSON/XML data.
- XML encryption, signing and XSLT.

Benefits

- Cyber Resilience / Risk Mitigation
- Customer satisfaction
- Innovation



Advanced Web Application Security

WebSockets flow security

WebSockets are a powerful technology that enables real-time, two-way communication between a client and a server. Unlike traditional HTTP requests, WebSockets enable instantaneous data transfer, making them ideal for applications that require over-the-air updates or fast response times. Using WebSockets, developers can create dynamic, interactive web applications that provide a seamless user experience. UBIKA is the unique WAAP provider securing Websocket flow.

Securing the content of WebSockets exchanges is essential to protect against security threats such as cross-site scripting (XSS), injection attacks, and data breaches.

Goals

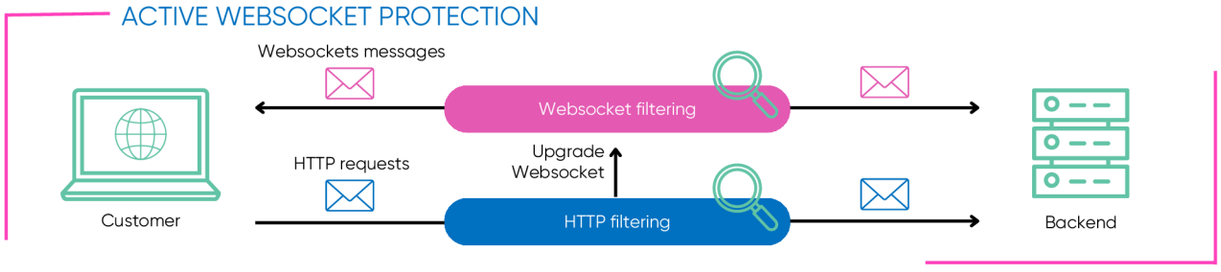
- Secure WebSocket traffic.
- Block malicious WebSockets messages.

How to proceed ?

1. Activate the authorization to switch to WebSocket in the tunnel (disabled by default).
2. WebSocket messages automatically pass through the workflow.
3. Configure the ICX security policy so that the engine works on Websockets.
4. The ICX security engine analyzes the content of WebSocket messages.
5. Add a traffic type decision node and bricks to transmit or block a WebSocket message based on the result of the ICX analysis.

Benefits

- Cyber Resilience / Risk Mitigation
- Customer satisfaction
- Innovation



Log of excepted requests

With Blacklist security engines, managing false positives is a crucial point for businesses. Exceptions are added to the security policy, creating vulnerabilities in application security.

The excepted query log feature will allow you to identify the security exceptions that match the most. This indicates the most dangerous exceptions because they let a lot of traffic through. By having the list of excepted requests for a given security rule, you can ensure that this rule is not too broad.

Goals ?

Provide all necessary information to development teams so that they can remediate legitimate traffic so that it is no longer detected as a threat. Clean up the list of exceptions by removing those that are no longer useful. Harden security by identifying exceptions that are too broad.

How to proceed ?

1. Enable the “Log Excepted Requests” option in the exception profile to analyze.
2. Wait for a time interval representative of the traffic,
3. Use WAFAPI endpoints to retrieve, for a given profile, security exceptions and the number of times they matched between two given dates.
4. Identify the rules that match too much and retrieve the logs of excepted requests via WAFAPI for each of these rules in order to check whether this traffic was legitimate or not.

Benefits

- Cyber Resilience / Risk Mitigation
- Customer satisfaction
- Increases readability of exceptions
- Agility / DevSecOps
- Innovation

Services & support

- Expert technical support team based in Europe.
- 24/7 portal to log support tickets for all types of incidents.
- 24/7 telephone support available as an option.
- Product certification training for partners and administrators.

UBIKA
9-11 rue Jeanne Braconnier - 92366 Meudon | France
Tel +33 (0)1 46 20 96 00 | www.ubikasec.com