FICHE PRODUIT

UBIKA WAAP GATEWAY
Advanced Package

Une solution sur mesure conçue pour répondre à vos besoins de sécurité les plus élevés.

Nos modules de sécurité de l'Advanced Package fournissent un niveau de protection supérieur pour votre entreprise, assurant la tranquillité d'esprit et la confiance dans vos opérations. Choisissez la solution UBIKA WAAP Gateway boostée avec l'Advanced Package pour une protection complète de vos applications.

Advanced API Security

Validation de schéma JSON, XML ou OpenAPI3

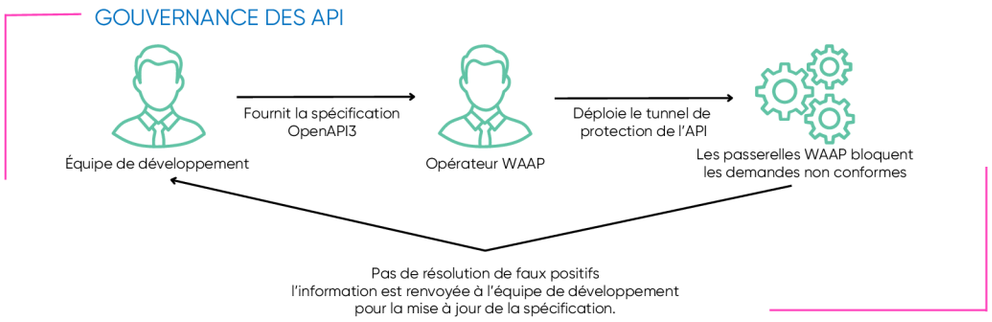
La prolifération des API en a fait une cible privilégiée des cyberattaques. Assurer la protection de cette nouvelle surface d'attaque est devenu un challenge important pour les entreprises. OpenAPI3 est la dernière version de la spécification OpenAPI, la norme industrielle pour décrire les points de terminaison, les paramètres et les réponses de vos API dans un format lisible.

Êtes-vous préoccupé par la sécurité de vos API ?

Grâce au module Adv. API Security, boostez la sécurité de vos API en liste blanche avec la validation de schéma : JSON, XML, Swagger2, OpenAPI3 ou même en mode apprentissage, sans avoir le schéma.

Bénéfices

- Renforcer la sécurité de vos API.
- Sécurité en liste blanche : seules les requêtes respectant le schéma fourni pourront atteindre vos API. Pas de gestion de faux positifs.
- Favoriser la collaboration avec vos équipes de développement.



Chiffrement et Authentification

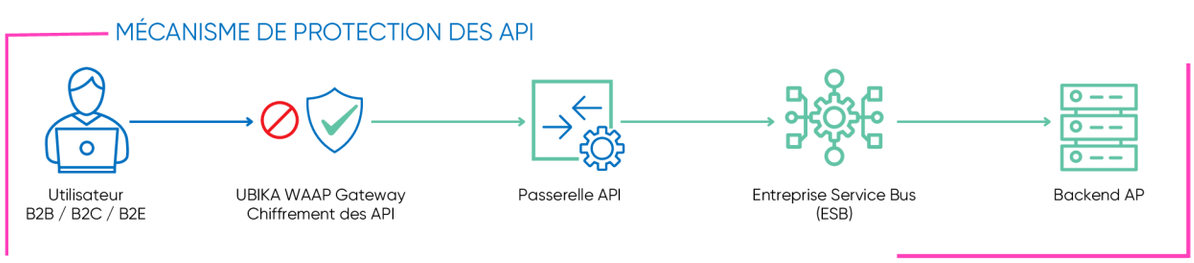
L'authentification, qui consiste à valider l'identité des utilisateurs, constitue une autre problématique majeure lorsqu'on fait appel aux API. Tous les utilisateurs ne doivent pas pouvoir accéder aux informations requérant un haut niveau de privilège.

Le module API Encryption renforce la protection des API en assurant l'intégrité des données et des identités. Cette fonctionnalité est accessible directement depuis le worfklow du WAAP Gateway UBIKA.

API Encryption permet d'effectuer la prise en charge de l'authentification SAML avec le module optionnel correspondant. Il ajoute de la sécurité aux API en utilisant le cryptage et la signature.

Bénéfices

- Filtrage avancé des API XML et JSON
- Jeton Web JSON pour intégrer les normes industrielles d'authentification des API (OAuth, OpenID Connect)
- Validation des schémas JSON / XML (vérification de la conformité du contenu
- Obfuscation, filtrage et manipulation des données JSON / XML
- Chiffrement et signature XML, transformation de données XSLT



Advanced Web Application Security

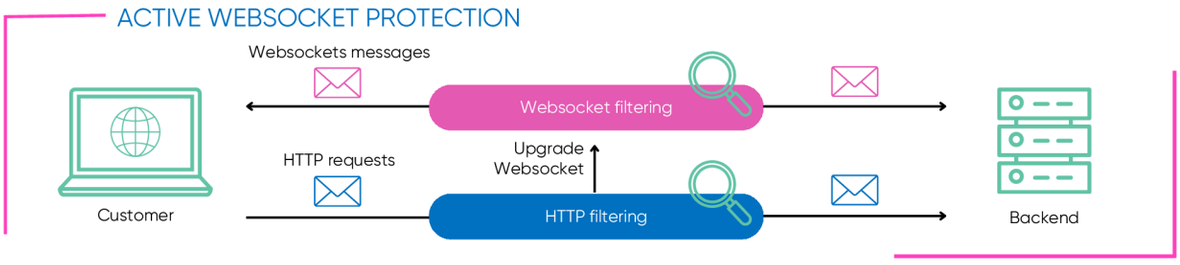
Sécurité des flux WebSockets

Les WebSockets sont un protocole puissant qui permet une communication bidirectionnelle en temps réel entre un client et un serveur. Contrairement aux requêtes HTTP traditionnelles, les WebSockets permettent un transfert de données instantané, ce qui les rend idéales pour les applications qui nécessitent des mises à jour en direct ou des temps de réponse rapides. En utilisant les WebSockets, les développeurs peuvent créer des applications web dynamiques et interactives qui offrent une expérience utilisateur transparente.

Il est essentiel de sécuriser le contenu des échanges WebSockets pour se protéger contre les menaces de sécurité telles que les scripts intersites (XSS), les attaques par injection et les violations de données.

Bénéfices

- Le contenu des messages WebSocket est analysé par le moteur de sécurité principal du WAAP
- Flexibilité du worflow avec possibilité de bloquer le message malveillant ou stopper la session complète



Log des requêtes exceptées

Avec les moteurs fonctionnant en sécurité négative, la gestion des faux positifs est un point crucial pour les entreprises. Des exceptions sont ajoutées à la politique de sécurité. Lorsque ces exceptions sont trop larges ou obsolètes, elles peuvent être la source de failles dans la sécurité des applications.

La fonctionnalité de log des requêtes exceptées vous permettra d'identifier les exceptions de sécurité qui matchent le plus. Ceci indique les exceptions les plus ouvertes car elles laissent passer beaucoup de trafic. La génération de logs sur les exceptions permet de gagner en lisibilité et vous pourrez vous assurer que cette règle en question ne soit pas trop large.

Bénéfices

- Durcir la sécurité en identifiant les exceptions trop larges.
- Fournir toutes les informations nécessaires aux équipes de développement pour qu'ils puissent corriger le trafic légitime afin qu'il ne soit plus détecté comme une menace.
- Nettoyer la liste des exceptions en supprimant celles qui ne sont plus utiles. Améliorer la lisibilité des exceptions

Avantages

Cyber-résillience / Atténuation des risques
Réduction des coûts
Satisfaction des clients
Agilité / DevSecOps
Innovation

Version 01.00 | juin 2022
Données sous réserve de modification
Image : Adobe Stock

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