FICHE PRODUIT

UBIKA WAAP GATEWAY BUSINESS EDITION

Cette solution combine des fonctions de sécurité essentielles dans un ensemble simple et rentable. Elle inclut des services de sécurité tels que le pare-feu applicatif Web pour un nombre illimité d'applications (c'est-à-dire que les clients ne sont pas limités sur le nombre d'applications en dehors de la limite matérielle), l'IP Reputation, le Web Access Manager (y compris le Web SSO) pour renforcer votre protection.

Vous disposez également de modules optionnels appelés Extended API Security pour renforcer la protection de l'intégrité de votre API et Management Console pour surveiller vos applications en temps réel.

Avantages clés

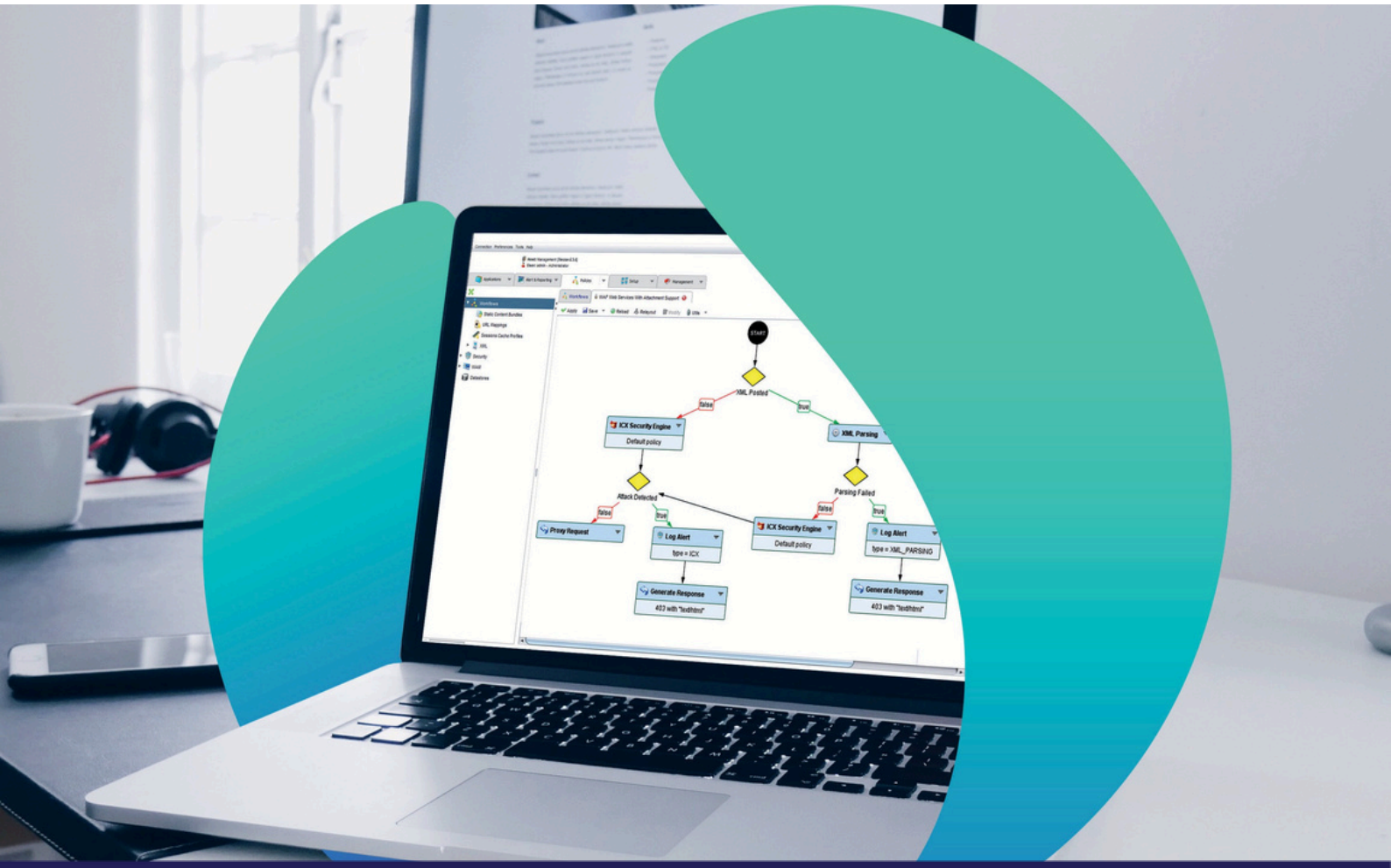
- Reconnue dans le Gartner Peer Insights 2022 «Strong Performer » for Web Application and API Protection solutions, c'est une solution sur site d'entrée de gamme avec un déploiement et une gestion facile et un TCO réduit.
- Protège activement les applications et services web en filtrant et surveillant le trafic entrant et en bloquant les attaques.
- Capable de répondre aux exigences de conformité et d'audit les plus strictes : PCI DSS, PSD2, directive NIS, RGPD, OZG.

UBIKA WAAP GATEWAY – BUSINESS EDITION est limité à une cible spécifique de clients avec des accords particuliers :

- France : Comptes publics de la santé sociale et collectivités territoriales
- Allemagne : collectivités territoriales, Stadtwerke, éducation, Hôpitaux
- Afrique & Moyen-Orient

Déploiement

- Modèles d'appliances physiques et virtuelles pour les besoins limités en bande passante (jusqu'à 21 000 transactions par seconde).
- Modèles de politique préconfigurés (sécurité, accélération, authentification) pour les applications standards.
- Déploiements actifs-passifs pour une haute disponibilité
- Prend en charge les architectures distribuées : plusieurs DMZ pour les déploiements avancés.
- Déploiement rapide et automatisation avec Terraform /Ansible.
- Possibilité de scénariser des automatisations complètes en utilisant l'API du produit.



Caractéristiques du produit

- Protection proactive contre les menaces pouvant entraîner la perte, le sabotage de données ou le déni de service (DoS).
- Efficacité prouvée contre le Top 10 des attaques de l'OWASP.
- Capacité à vérifier la signature et à chiffrer ou modifier toute ou une partie des requêtes.
- Moteur de normalisation pour interpréter toute requête HTTP et contrer les diverses techniques d'encodage.
- Moteur de liste blanche basé sur des signatures génériques pour une protection maximale contre les attaques connues.
- Des moteurs de scoring capables d'identifier en temps réel les attaques et de prévenir les exploitations de type « zero day».
- Ignorer les requêtes des robots indésirables.
- Répétition des logs pour le test des politiques et l'analyse numérique.
- Intégration facile avec des scanners de fichiers tiers.
- (ICAP).
- Géolocalisation des IP.

MODULES EN OPTION

Extended API Security

- Sécurité des API d'applications personnalisées et des communications de machine à machine
- Chiffrement et signature XML / JSON
- Analyse et génération de Tokens Web JSON

Console de Management

- Plateforme dédiée pour la configuration et la gestion centralisée de toutes les instances et applications
- Surveillance des applications web en temps réel
- Accès basé sur les rôles pour les tâches de gestion distribué

Configuration graphique du workflow

- Interface de gestion accessible et intuitive
- En un clic, possibilité de passer d'un mode bloquant à un mode journalisation sur toutes ou certaines parties de la politique de sécurité
- Visualisation du traitement du trafic et des flux d'inspection
- Configuration de la réponse d'attaque selon le contexte
- Détection et réduction de faux positifs

Web Access Manager

- Simplification de l'authentification des utilisateurs via le web SSO
- Authentification adaptée au contexte utilisateur
- Intégration avec LDAP, AD, Radius

IP Reputation

- Mise à jour de renseignements sur les menaces dans la politique de sécurité
- Filtrage des requêtes venant d'adresses IP malveillantes
- Réduction du risque de faux positifs en ajustant la politique en fonction de l'origine de la requête

Sécurité des API

- Extension de sécurité aux attaques ciblant les API
- Capacité d'analyser et de valider des schémas, de manipuler des données JSON / XML
- Capacité à détecter les attaques spécifiques aux API, notamment les entités externes XML (XXE)

Services et Support

- Equipe support technique experte basée en Europe
- Portail pour la gestion des tickets de support pour tout type d'incidents
- Assistance téléphonique 24/7 disponible en option
- Formation à la certification des produits pour les partenaires et administrateurs

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