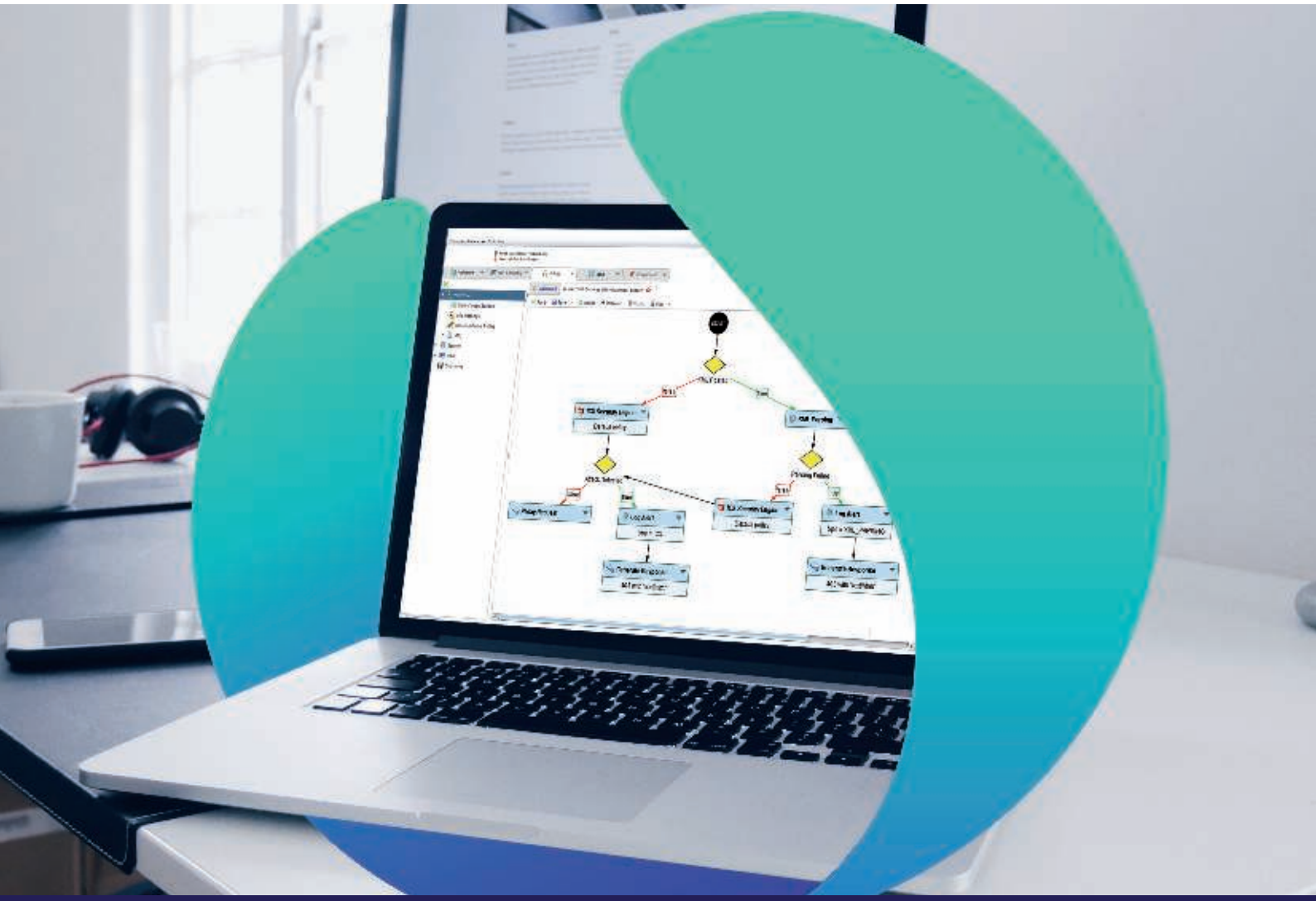
FICHE PRODUIT

UBIKA
WAAP GATEWAY

UBIKA WAAP GATEWAY offre une large gamme de fonctionnalités pour gérer la sécurité des applications de l'entreprise. Conçue pour protéger les applications métier les plus critiques, y compris les applications existantes et les API personnalisées, contre les attaques complexes, elle respecte les exigences en matière de confidentialité des données. Elle s'adapte à tout type d'environnements clients et supporte les applications web à haute performance ainsi que le développement continu de nouveaux logiciels.

Avantages clés

- Reconnue dans le Gartner Peer Insights 2022 «Strong performer» for Web Application and API protection solution, c'est une solution puissante conçue pour les entreprises afin de répondre à leurs besoins spécifiques.
- Aide les organisations à adopter un mode de fonctionnement DevOps en réduisant les risques de sécurité et le coût total de possession tout en améliorant les performances des applications.
- Entièrement évolutive et agnostique, elle permet de gérer les applications déployées dans des environnements multi-clouds ou de clouds hybrides, en évitant l'adhérence au fournisseur ou les hausses de coûts.
- Capable de répondre aux exigences de conformité et d'audit les plus strictes : PCI DSS, PSD2, directive NIS, RGPD, OZG.



Déploiement

- Large gamme d'appliances physiques et virtuelles sélectionnées et testées pour des performances maximales (de 21 000 à 100 000 transactions par seconde)
- Disponible sur les places de marché AWS (Amazon Web Services), Microsoft® Azure et GCP (Google Cloud Platform)
- Modèles de sécurité préconfigurés pour les applications standard telles que Microsoft® SharePoint, OWA365, Exchange, SAP®, WordPress, Drupal
- Déploiements actif-passif et actif-actif pour une haute disponibilité
- Supporte les architectures distribuées : DMZ multiples et «Pooling Mode» pour les déploiements avancés
- Déploiement rapide et automatisation à l'aide de Terraform / Ansible

MODULES EN OPTION

Extented 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

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

- Ajout de renseignements sur les menaces à jour à la politique de sécurité
- Garantie l'optimisation des performances en filtrant les requêtes provenant de sources IP malveillantes
- Réduction du risque de faux positifs en ajustant la politique en fonction de l'origine de la requête
- Ignore les requêtes de robots indésirables

Console de Management

- Plate-forme dédiée pour la configuration et la gestion centralisée de toutes les instances et applications
- Déploiement automatisé de la politique de sécurité des applications sur toutes les instances, y compris celles dans le cloud
- Surveillance des applications web en temps réel
- Accès basé sur les rôles pour les tâches de gestion distribuée

Principales fonctionnalités du produit

- Protection proactive contre les menaces connues et inconnues pouvant entraîner la perte ou le sabotage de données, le déni de service (DoS)
- Efficacité prouvée contre le Top 10 des attaques de l'OWASP
- Capacité à signer, vérifier la signature, chiffrer, déchiffrer, modifier toute ou partie de la demande ou de la réponse
- Sécurité standard basée sur des patterns génériques et un mécanisme de scoring combiné avec des moteurs de sécurité avancés pour une détection plus granulaire et plus précise
- Rejeu des logs pour tester les politiques et mener une analyse forensic
- Scoring de réputation des utilisateurs pour prévenir la fraude et le vol en bloquant les utilisateurs illégitimes
- Détection et mitigation proactives des robots
- Pare-feu JSON et parsing et validation XML
- Intégration facile avec des scanners de fichiers tiers (ICAP)
- Mode apprentissage des applications pour une protection renforcée et de meilleures performances pendant le cycle de développement logiciels
- Import / Export d'OpenAPI pour la sécurité des API et le DevOps
- Géolocalisation des IP
- Analyse puissante des logs permettant de descendre jusqu'à un problème de sécurité spécifique
- Le datastore Redis crée des mécanismes de sécurité en temps réel

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 en fonction du contexte
- Capacité à 'enchaîner' plusieurs moteurs de sécurité via le workflow pour une détection précise et pour réduire les faux positifs

Services et Support

- Equipe support technique experte basée en Europe
- Portail 24/7 pour la gestion des tickets de support pour tous types 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