FICHE PRODUIT

UBIKA WAAP GATEWAY

Une solution complète conçue pour répondre à vos besoins de sécurité

Le WAAP Gateway UBIKA offre une large gamme de fonctionnalités pour gérer la sécurité des applications de l'entreprise. Conçu pour protéger les applications métier les plus critiques, y compris les API personnalisées, contre les attaques complexes, tout en répondant aux exigences de confidentialité des données. Il convient à tout type d'environnement client et prend en charge les applications Web mondiales à haute performance ainsi que le développement continu de nouveaux logiciels.

Avantages clés

- Reconnu comme « Strong Performer » par Gartner Peer Insight en 2022 pour les WAAP - solutions de protection des applications Web et des API - le WAAP UBIKA fournit une solution puissante tout-en-un conçue pour les entreprises des secteurs public et privé qui apprécient l'innovation et la flexibilité pour répondre à leurs besoins spécifiques.
- Version software 6.11 certifiée CSPN premier niveau par l'ANSSI.
- Aide les organisations en mode DevOps en réduisant les risques de sécurité et le coût total de possession tout en améliorant les performances des applications.
- Entièrement évolutif et indépendant des technologies, il permet de gérer de manière cohérente les applications déployées dans des environnements multi-cloud ou cloud hybride, en évitant l'adhérence au fournisseur et la hausse des coûts. Compatible avec les Cloud Providers Google, AWS, Microsoft, ainsi que les cloud souverains OVHcloud et Outscale.
- Flexibilité et puissance du workflow graphique pour la création des politiques de sécurité au plus près de vos besoins.
- Capable de répondre aux exigences les plus strictes en matière de conformité et d'audit : PCI DSS, PSD2, directive NIS2, DORA, RGPD.

Fonctionnalités principales

- Protection proactive contre les menaces connues et inconnues 0-day pouvant entrainer des pertes / vols de données, sabotage, déni de service applicatif (DoS en couche L7).
- Efficacité prouvée contre les attaques du Top 10 de l'OWASP.
- Gestion du chiffrement et de la signature, modification de tout ou partie de la requête et de la réponse.
- Cœur de la sécurité basé sur une combinaison de plusieurs moteurs pour une sécurité plus poussée dont un moteur de patterns génériques détectant les attaques dans le contenu des requêtes et un moteur de scoring.
- Détection des attaques même dans les contenus encodés.
- Possibilité de rejouer les requêtes pour tester les politiques et mener une analyse forensique.
- Détection et mitigation proactive des robots.
- Manipulation de contenu JSON et 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 logiciel.
- Géolocalisation des IP.
- Analyse puissante des logs permettant de descendre jusqu'à un problème de sécurité spécifique.
- Le datastore Redis permet une interaction entre différents éléments pour créer des mécanismes de sécurité.

Configuration graphique du workflow

- Editeur de workflow graphique accessible et intuitif.
- En un clic, possibilité de passer d'un mode bloquant à un mode d'observation sur tout ou partie de la politique de sécurité.
- Visualisation du traitement du trafic et des flux d'inspection.
- Personnalisation de la page de réponse en fonction du contexte de l'attaque.
- Capacité à combiner plusieurs moteurs de sécurité via l'éditeur de workflow pour une détection plus précise.

Services & Support

- Equipe de support technique experte, en français ou anglais, basée en France.
- 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.

Déploiement

- Large gamme d'appliances physiques et virtuelles sélectionnées et testées pour des performances maximales (de 21 000 à 100 000 transactions par seconde).
- Compatible multi cloud provider :
  - Disponible sur les marketplaces AWS (Amazon Web Services), Microsoft Azure, GCP (Google Cloud Platform) et Outscale.
  - Image cloud générique compatible cloud privés et cloud souverains : OVHcloud, Outscale et Cloud Temple.
- Déploiements actif-passif pour une haute disponibilité.
- Supporte les architectures distribuées : DMZ multiples pour les déploiements de haute sécurité.
- Déploiement rapide et automatisation par API, grâce à Ansible et Terraform.

Modules optionnels

Advanced Package

Adv. API Security

Renforcement de la sécurité des API pour les applications propriétaires basées sur les API et les communications machine à machine.

- Chiffrement et signature XML
- Analyse et génération de Tokens Web JSON
- Validation de schéma JSON, XML, OpenAPI3 pour une sécurité renforcée en liste blanche - sans gestion de faux positifs.

Adv. Web Security

- Protection du contenu des messages WebSocket
- Amélioration et facilitation de la gestion des faux positifs avec le log des requêtes exceptées permettant de détecter les exceptions de sécurité pouvant exposer les applications.

Authentication Package

- Web Access Manager
- Simplification de l'authentification des utilisateurs via le web Single Sign On (SSO)
- Authentification adaptée au contexte utilisateur
- Intégration avec LDAP, AD, Radius
- Packages pour l'authentification SAML et OAuth.

IP Reputation

- Renforcement de la sécurité avec l'ajout de la réputation de l'IP provenant de source usant de Threat Intelligence.
- Optimisation des performances en filtrant les requêtes provenant d'IP sources malveillantes.
- Flexibilité du niveau de sécurité demandé.

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