FICHE PRODUIT

# UBIKA
# WAAP CONTAINER

## Une cloud workload protection platform (CWPP) accompagnant votre « shifting left », dédiée aux applications cloud natives, leurs micro services et APIs.

Avec l'utilisation des microservices, le trafic est-ouest augmente considérablement. Sécuriser ces flux latéraux est essentiel pour minimiser la surface d'attaque. En outre, les attaques du Top 10 de l'OWASP sont plus que jamais pertinentes pour les applications et APIs Cloud native et DevOps ; tout en intégrant certaines attaques sous-estimées, comme le « credential stuffing ». Plusieurs organisations s'appuient sur des outils tels que du SAST, DAST ou SCA qui ne couvrent que partiellement le Top 10 de l'OWASP et ne récupèrent pas des informations précises des développeurs pour décrire facilement leur application. De plus, du SAST génère de nombreux faux positifs et ne détecte pas l'exploitation de nouvelles vulnérabilités dans une phase de RUN. Quant aux DAST et SCA, ils peuvent identifier de nombreuses vulnérabilités mais les résoudre peut devenir un véritable cauchemar pour les équipes DevOps. Ces outils ne sont donc pas suffisants pour garantir la sécurité de vos applications, notamment contre les attaques zero-day.

- Misez sur une technologie conteneurisée, associant sécurité avancée et cycles de déploiements agiles, au cœur du développement.

## Aperçu de la solution

UBIKA WAAP Container supporte l'automatisation complète de votre écosystème DevOps – du développement à la production en passant par la validation du code et les tests de sécurité – et améliore vos délais de déploiement. La possibilité d'intégrer la configuration de la sécurité au plus près de l'application permet aux équipes DevOps d'aborder les problèmes complexes de sécurité dès la phase de BUILD, en complément des outils SAST / DAST. Elle crée une valeur ajoutée dès la phase de CI en testant l'application dans un environnement de préproduction afin de la protéger en phase d'exécution. Vous pouvez hiérarchiser, suivre et accélérer le temps nécessaire à la correction des nouvelles vulnérabilités en créant des règles virtuelles personnalisées. Les développeurs disposent ainsi de plus de temps et de sérénité pour effectuer une correction tout en respectant leur planning.

## Simplification avec un fichier de configuration standard

Cette solution conteneurisée est intégrée dans le pipeline CI / CD avec les outils déjà existants comme Gitlab, Jenkins, etc. pour simplifier la collaboration. L'interopérabilité est assurée avec l'utilisation de mêmes formats (YAML, GO...), facteurs de forme (images Docker), langages, concepts... Cela facilite la gestion et réduit le coût total de possession évitant ainsi la multiplication des compétences.

## Moteurs proactifs associés à approche positive

La solution intégre des moteurs de sécurité reposant sur 20 ans d'expertise, du rate limiting et des capacités de mitigation des robots pour répondre au TOP 10 de l'OWASP, aux attaques « zero-day », DoS et autres menaces telles que le « credential stuffing » qui n'exploitent pas les CVE. Conçue dans une approche API, elle gère l'import d'Open-API, sécurisant ainsi la circulation nord-sud et est-ouest.

## Augmente le ROI en s'adaptant au trafic

La solution est déployée au plus proche de l'application, permettant d'augmenter ou diminuer ses capacités parallèlement à l'utilisation de l'application en utilisant l'orchestrateur, dans des clusters Kubernetes, OpenShift ou Docker. Ainsi, elle peut s'adapter automatiquement au trafic. Cela diminue ainsi les coûts et améliore le retour sur investissement.

## Améliore la sécurité grâce à une description du contexte

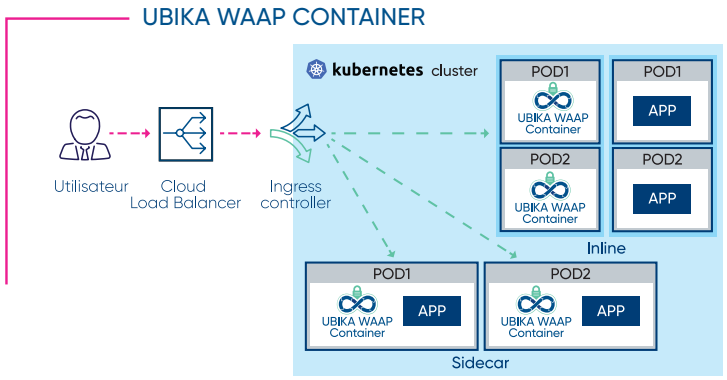
La solution ainsi que la description du contexte (comme le type de persistance utilisé, le langage de programmation, le système d'exploitation du serveur, le format des données) sont intégrées dans un fichier de configuration proche du code de l'application. La sécurité reste ainsi à jour et alignée sur la version de l'application. Les politiques de sécurité peuvent donc être adaptées automatiquement en invoquant les moteurs de sécurité associés les plus pertinents.

## Optimise les coûts : évite faux positifs et pertes de données

UBIKA WAAP Container crée des exceptions en détectant de manière automatique les faux positifs dans une préproduction et limite leur survenue en production. Elle peut détecter les données sensibles avec des capacités de filtrage sortant agissant sur la réponse du backend afin de prévenir la perte de données et assurer votre conformité.

## Assure l'agnosticité via un déploiement rapide et flexible

La solution peut être rapidement déployée à la fois sur site et sur le cloud (privé et public) avec un minimum d'effort. Les moteurs de sécurité sont déployés en local et les autres fonctionnalités dans un environnement SaaS. Le form factor garantit la haute disponibilité et la performance des applications pour les utilisateurs.




| ENVIRONNEMENTS SUPPORTÉS | | |
|---|---|---|
| Cloud | | |
| AWSG | CP | Microsoft® Azure |
| Conteneurs | | |
| Docker | Kubernetes | OpenShift |
| Service Mesh | | |
| IstioA | Ambassador | Consul |
| Insights | | |
| Syslog | Logstash | Fluentd |
| Outils CI / CD | | |
| Gitlab | Jenkins | CircleCI |


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*