

UBIKA Smart Protection

PROTECTION PRÉDICTIVE EN TEMPS RÉEL AUGMENTÉE PAR IA

Des nouvelles menaces indétectables

Les solutions WAAP traditionnelles peinent à détecter les menaces modernes, de plus en plus sophistiquées et furtives. Les attaques de type APT (Advanced Persistent Threat) combinent reconnaissance préalable, tests de résistance et ajustements dynamiques pour contourner les défenses classiques. Ces attaques adaptatives évoluent en temps réel, exploitant les failles comportementales et les angles morts des systèmes.

Retrouvez la sérénité

Smart Protection est notre nouvel outil propriétaire d'analyse comportementale augmentée par IA, nativement intégré dans **UBIKA Cloud Protector** et prochainement dans **UBIKA WAAP Gateway**. Smart Protection de UBIKA bloque de manière proactive les attaques sophistiquées que les WAAP classique ne parviennent pas à bloquer. Les politiques de sécurité applicative s'ajustent automatiquement en temps réel, tout en éliminant les faux positifs.



FONCTIONNEMENT

1

Phase de reconnaissance

L'attaquant sonde le système pour recueillir des informations et teste la vulnérabilité. Il génère ainsi des traces dans les requêtes et les réponses.

2

Analyse comportementale

Smart Protection détecte en amont et en temps réel les tentatives d'exploitation en corrélant les signaux comportementaux, même les plus faibles.

3

Alertes et blocages

Smart Protection alerte en temps réel sur les comportements suspects et peut bloquer automatiquement les requêtes à haut risques.

4

Ajustements automatisés

Grâce à l'analyse comportementale, Smart Protection ajuste automatiquement le niveau de sécurité des fonctionnalités (liste de contrôle d'accès, le limiteur de taux, etc.).

BÉNÉFICES



Ajustement automatisé de la protection



Blocage proactif des menaces



Élimination des faux positifs



Simplicité d'administration

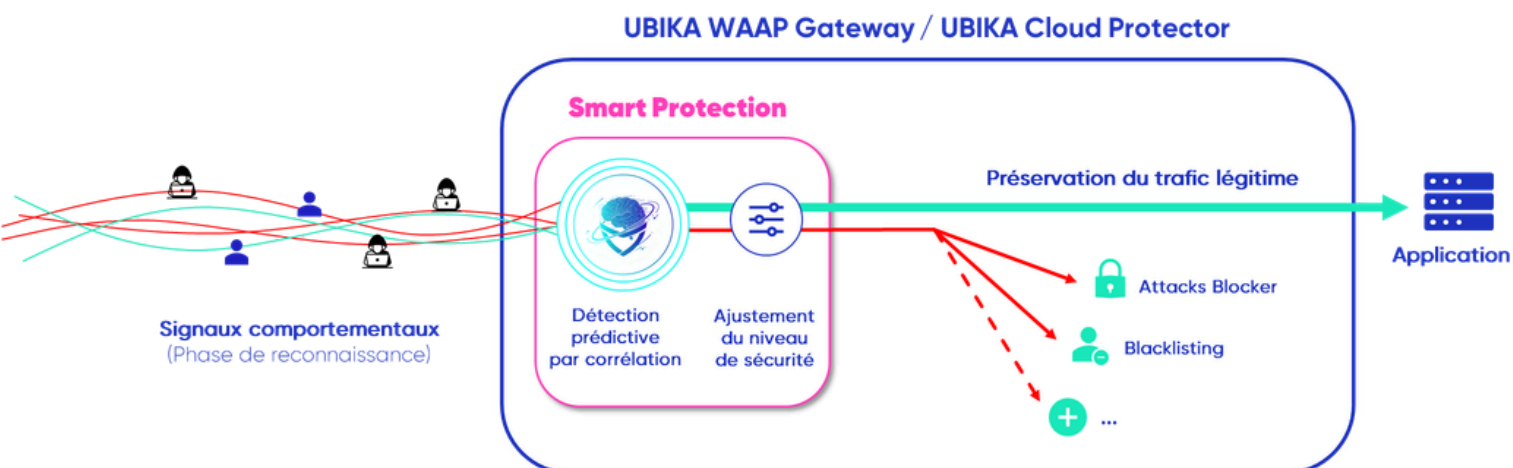


Disponibilité des serveurs préservée



Gain de temps et de tranquillité

UNE PROTECTION PRÉVENTIVE ET ADAPTATIVE



SIGNAUX FAIBLES REPÉRÉS CÔTÉ **REQUÊTES**

Ce qu'analyse Smart Protection pour chaque demande entrante.



SIGNAUX FAIBLES REPÉRÉS CÔTÉ **RÉPONSES**

Les états de réponse HTTP qui sont des indicateurs comportementaux analysés par Smart Protection

