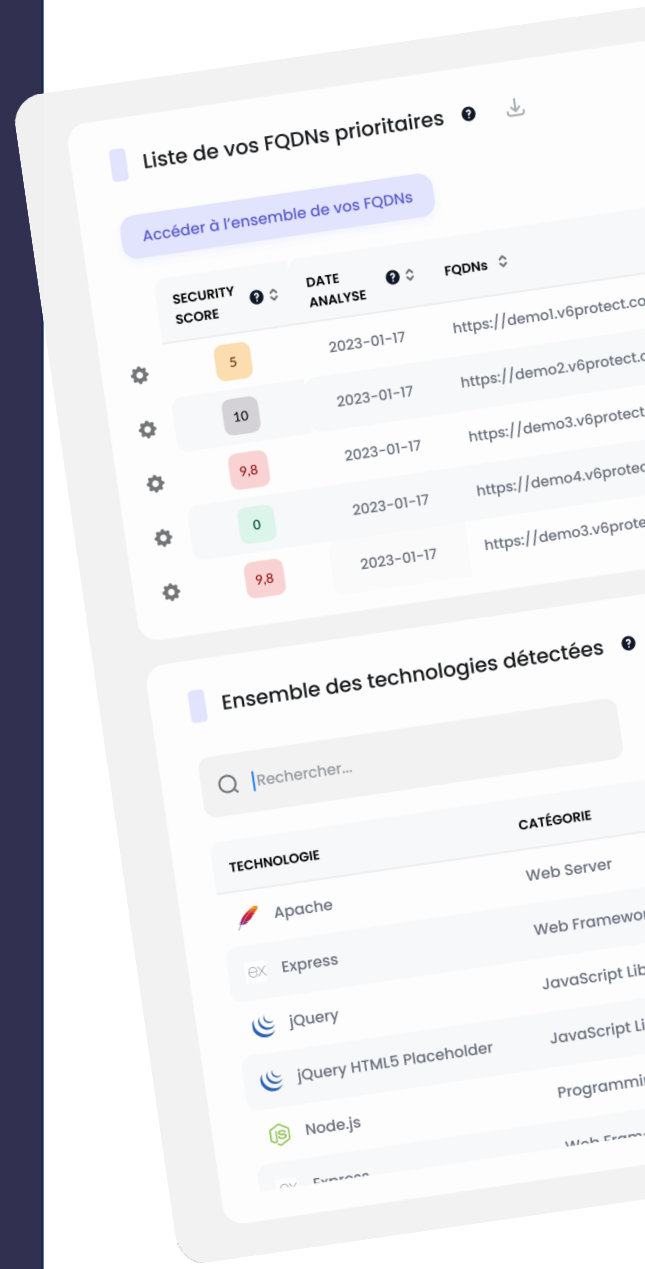
v6Protect

Sécurité des applications web

Supervision des vulnérabilités

Firewall Applicatif Nouvelle Génération



v6Protect

Éditeur français

Depuis 2019

Entreprise indépendante

Support en France

Solution SaaS

Hébergement en France

Haute disponibilité

Chiffrement des données

Référencement

Orange Cyberdefense

C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière

resah

adista

UGAP

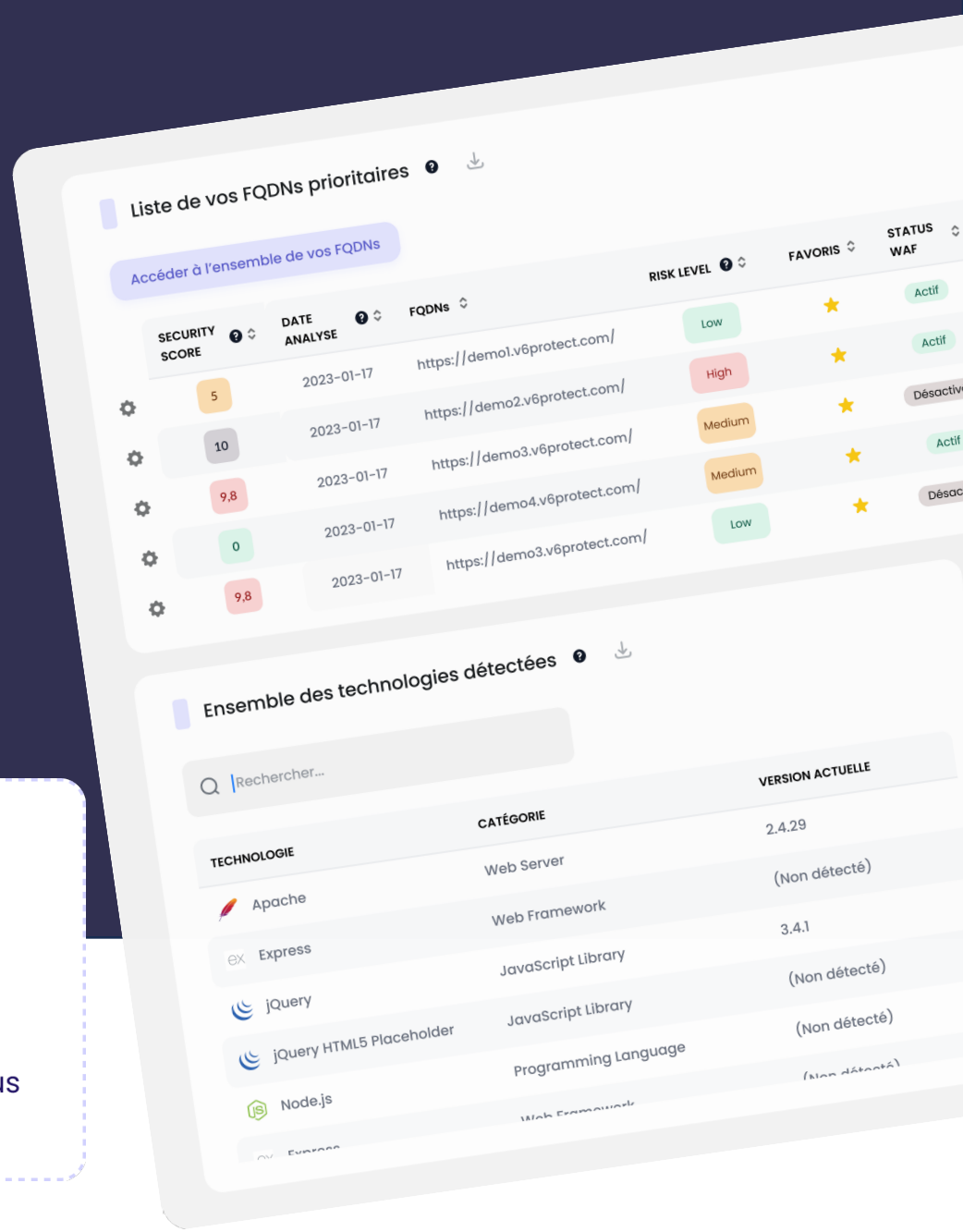
CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE Nouvelle-Aquitaine

ACN Alliance pour la confiance numérique

FRANCE CYBER SECURITY

FRANCE RELANCE

Plateforme unifiée de sécurité offensive et défensive



Supervision des vulnérabilités

Identifiez, supervisez et corrigez vos vulnérabilités en quelques minutes

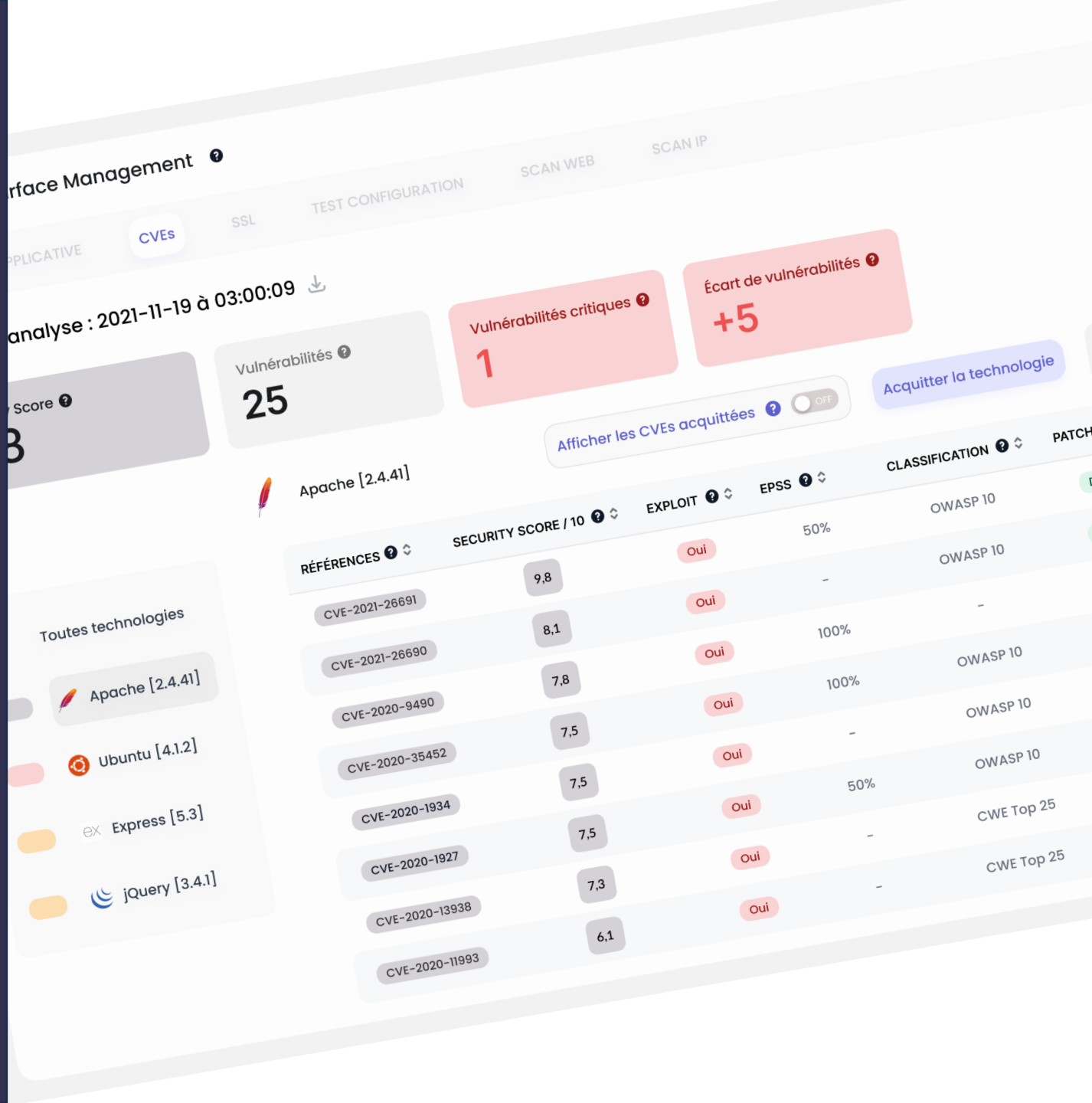
Firewall Applicatif nouvelle génération

Protégez-vous des attaques web les plus sophistiquées grâce à l'IA

Supervision des vulnérabilités

Automatisez simplement la gestion de vos vulnérabilités

- Surveillance continue des vulnérabilités
- Priorisation des risques
- Aide à la remédiation



Gestion de la surface d'attaque externe

Vue unifiée de votre exposition

- Cartographie de la surface applicative
- Identification des CVEs / CWEs
- Test TLS/ SSL
- Scan de ports
- Scan de la configuration web
- Scan dynamique intrusif

Synthèse fonctionnelle

Cartographie de la surface applicative

- Inventaire passif des composants applicatifs
- Gestion des technologies et suivi des évolutions

Scan Ports

- Scan Top **5000** des ports (Protocol TCP)
- Identification des ports ouverts / fermés

Identification des CVEs / CWEs

- Identification des menaces (CVEs / CWEs)
- Vérification de la présence d'Exploit
- Priorisation des risques (CVSS Score, EPSS, CISA KEV)
- Présentation des faiblesses (MITRE ATT&ACK, WASC)
- Management et acquittement des risques
- Proposition de correctifs par OS

Scan de la configuration web

- Tests de configuration (17 points de contrôle)
- Security Header, Robot.txt, Security.txt, Cookies, ...

Test TLS/ SSL

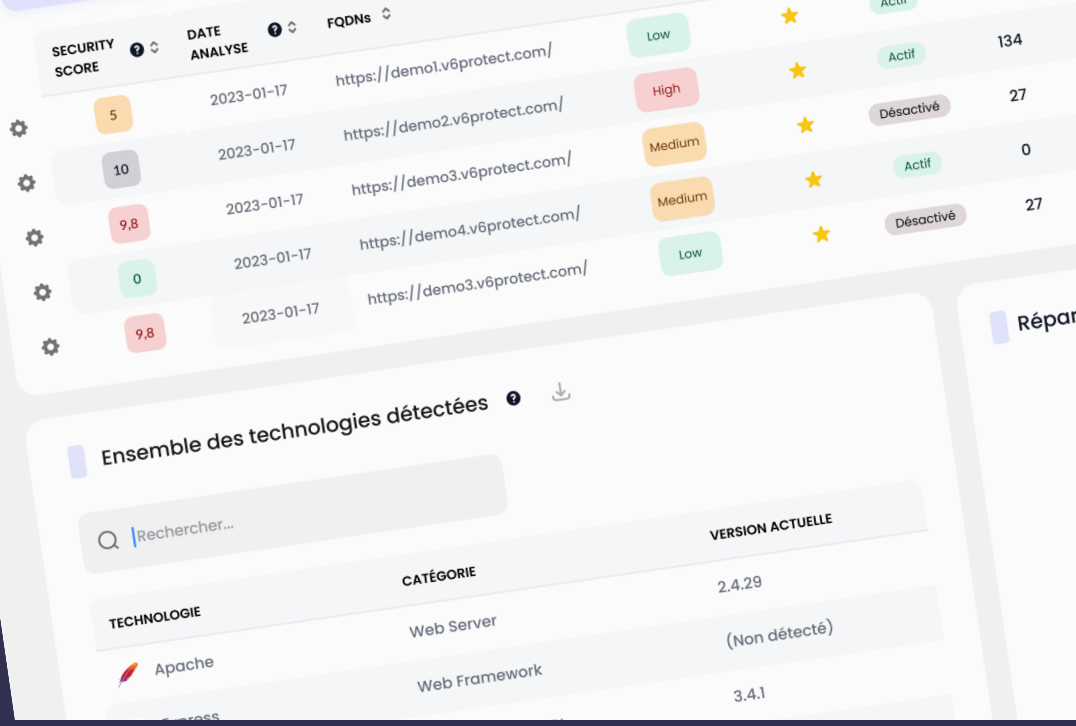
- Analyse de l'ensemble de la chaîne SSL
- Contrôle de CVEs (LOGJAM, LUCK13, BREACH, ...)

Scan dynamique intrusif

- Tests intrusifs (60 points) dont l'OWASP Top 10, Injection, Broken Authentifcation, Cross-Site Scripting, XXE, CSRF, Security Misconfiguration, Insufficient, ...
- Remote Code Execution Log4j
- Recommandation et bonnes pratiques

Pilotage continu de la sécurité applicative

Tel que le préconise Gartner, Web App Vulnerability offre un pilotage continu de la sécurité des applications.



1. Audit automatisé

- Cartographie de l'exposition externe
- Priorisation des risques

2. Correction des failles

- Correctifs et recommandations
- Amélioration continue

3. Suivi dans le temps

- Alertes 24/7 et rapports synthétiques
- Suivi du plan d'action

4. Vision d'ensemble

- Indicateurs clés, tableaux de bord
- Pilotage

Cas d’usage au quotidien

Maintien en Condition de Sécurité

- File conducteur entre deux tests d'intrusion
- Homologation d'un service numérique
- Audit automatisé & test des faiblesses
- Gestion des mises à jour des composants applicatifs
- Suivi de la mise en conformité technique et légale
- Pilotage des équipes techniques et des partenaires

Les +

- Multi-indicateurs : CVSS • EPSS • KEV
- Alertes 24/7 • Surveillance continue
- Prise en main immédiate

Firewall Applicatif avec IA

Protégez-vous grâce à l'analyse comportementale

- Protection web automatisée
- Adaptation aux évolutions
- Optimisation du trafic

Protection des applications web et APIs par l'IA

- Protection préventive en temps réel — Protection active
- Protection anti-DDoS — Protection active
- Analyse contextuelle (IA/ML) — Suspicieux
- Prévention des bots malveillants — Bloquées

Synthèse fonctionnelle

Protection active

Protection préventive en temps réel

- Détection des signatures d'attaques (OWASP)
- Protection contre les malwares/ ransomwares, vol de données, brute force, manipulation des cookies, injection, Cross-Site Scripting, ...)
- Prévention des intrusions (IPS)
- Sécurisation des fichiers
- Protection contre les attaques DDoS couches 3, 4 et 7
- Fourniture d'un certificat SSL Let's Encrypt

Bloquées

Prévention des bots

- Blocage : trafic des bots malveillants
- Blocage : scraping, credential stuffing, création de compte automatisée, craquage de jetons

Suspicieux

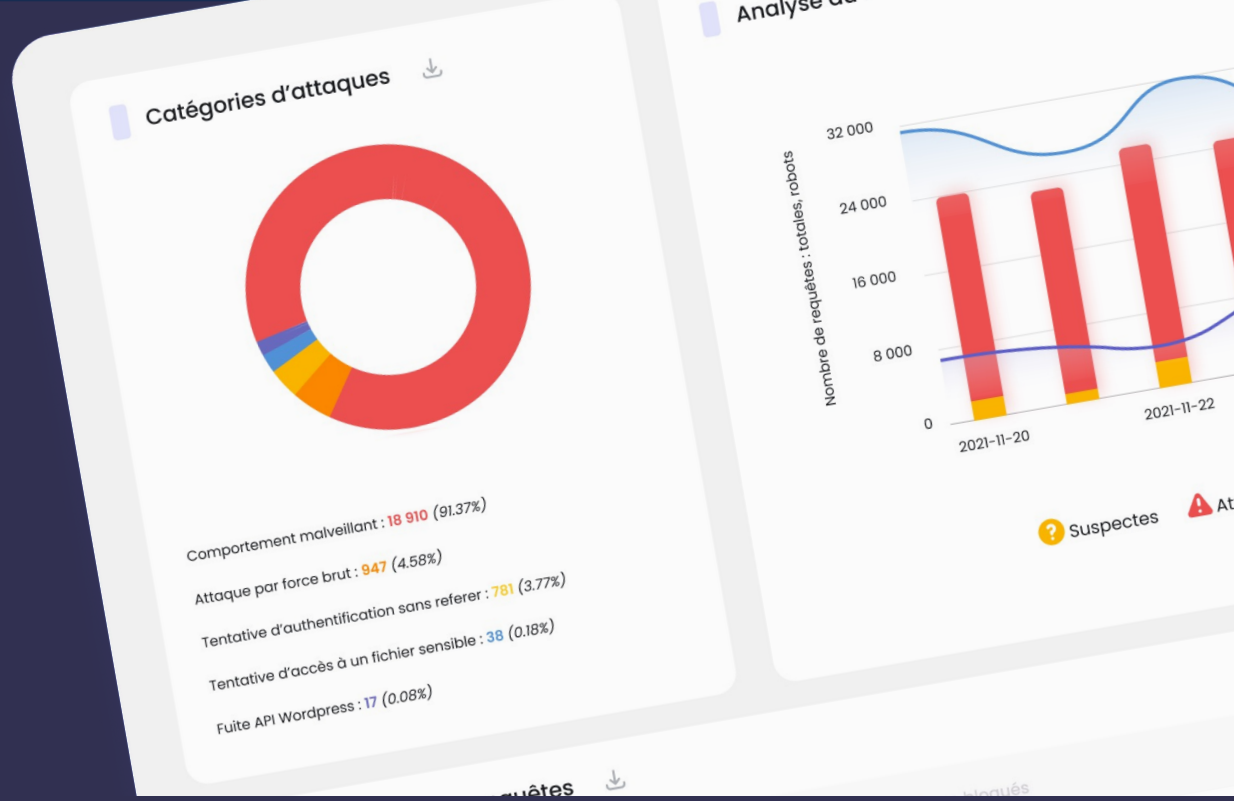
Analyse contextuelle

- Définition d'un comportement « modèle » :
  - Nombre/ récurrence des hits,
  - Vitesse du crawl,
  - Fréquence/ poids des requêtes,
  - Réputation et fiabilité,
  - Historique,
  - IP géolocalisation,
  - Activité biométrique.

- Détection des comportements suspects
- Géoblocage des IPs
- Blocage des menaces « non connues » Zero-Day
- Apprentissage automatique contextuel
- Réduction des faux positifs

Prévenir des attaques web sophistiquées

WAAP automatisé qui exploite l'analyse contextuelle pour fournir une prévention précise des menaces web



1. Déploiement simplifié

- Redirection des DNS
- DevOps friendly by design

2. Protection précise

- Protection préventive
- Analyse contextuelle

3. Efficacité maximale

- Apprentissage continu
- Réduction des faux-positifs

Cas d'usage au quotidien

Protection des applications web et APIs

- Protection automatisée des applications web et des APIs
- Protection des données sensibles
- Simplification et gain de temps des opérations de sécurité
- Amélioration des performances et de la disponibilité
- Filtrage du trafic et analyse des évènements de sécurité
- Amélioration du développement de l'application

Les +

- Intégration rapide
- Protection immédiate
- Mise à jour automatique des règles
- Aucune administration

v6Protect

Distributeur exclusif Océan Indien, Afrique & Caraïbes :

Hodi
www.hodi.host
hello@hodi.host
+262 262 800 750

Plus d'informations sur www.v6protect.fr