Barracuda WAF-as-a-Service

Protégez toutes vos applications Web, où qu'elles soient hébergées, en quelques minutes.

Déployer et configurer un pare-feu d'applications Web traditionnel (WAF) peut s'avérer extrêmement complexe et long. En conséquence, il n'est pas rare de voir des sites se contenter d'installer un WAF en mode par défaut à des fins de conformité mais ne jamais prendre la peine de le configurer correctement, le laissant ainsi totalement vulnérable aux menaces basées sur les applications.

La solution Barracuda WAF-as-a-Service peut quant à elle être déployée, configurée et mise en service en quelques minutes seulement. Les modèles pré-intégrés offrent une protection immédiate et l'interface intuitive permet de mettre en place des politiques personnalisées en toute simplicité. Une protection complète contre les attaques de type DDoS garantit en outre une disponibilité continue des applications. Et le service Barracuda intégré de correction des vulnérabilités analyse automatiquement les applications afin de remédier à toute faille.

Simplicité et flexibilité

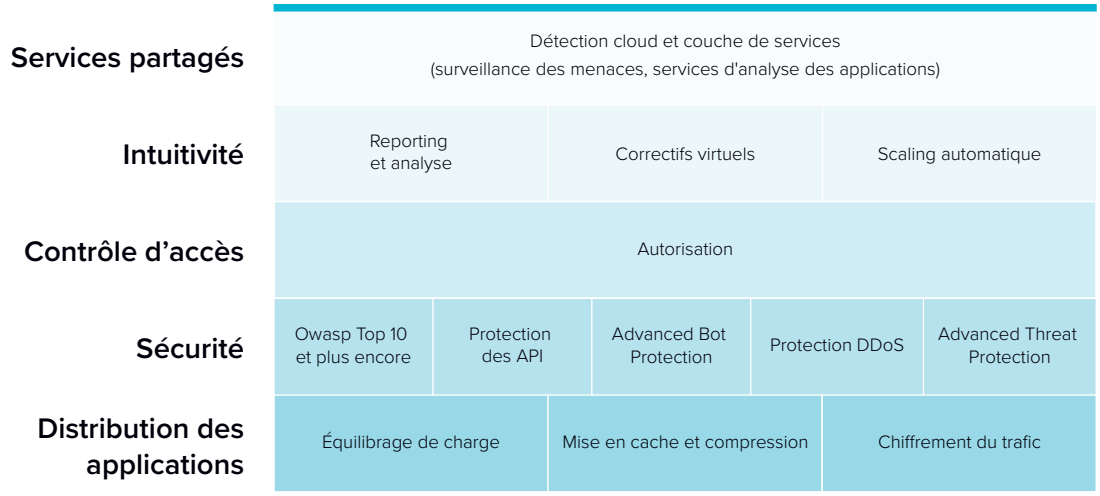
Barracuda WAF-as-a-Service inclut un assistant d'installation convivial en 5 étapes, afin de vous permettre de protéger vos applications en quelques minutes seulement. Les modèles pré-intégrés offrent ainsi une protection complète pour une grande majorité des applications les plus répandues. Les utilisateurs avancés apprécieront en outre de bénéficier d'un contrôle granulaire permettant de définir des politiques personnalisées. Il suffit d'ajouter les éléments à paramétrer à la liste des composants de configuration et de les personnaliser afin de répondre à des besoins spécifiques.

Protection contre les attaques de nouvelle génération

Le service s'appuie sur une technologie éprouvée qui permet de contrer les 10 principales failles de sécurité identifiées par l'OWASP, les menaces automatisées visant les applications Web, les menaces « Zero Day » et bien plus encore. La défense avancée contre les bots bloque ainsi les attaques automatisées comme le Web scraping, le scalping, le carding, le spam par bot, ainsi que le credential stuffing et le piratage de comptes. La protection anti-DDoS illimitée empêche par ailleurs les attaques DDoS volumétriques et applicatives. Enfin, des rapports d'analyse détaillés permettent de documenter le respect des exigences de conformité.

Protection pour les applications de nouvelle génération

Que vos applications soient hébergées sur site, dans le cloud, dans un conteneur ou encore dans un environnement sans serveur, vous bénéficiez d'une API REST ainsi que de Barracuda Vulnerability Remediation Service, qui analyse les applications et remédie aux vulnérabilités en un seul clic. Cela permet une sécurité optimale en continu, même lors des mises à jour et du déploiement de nouvelles applications en réponse à l'évolution de vos besoins, le tout sans surcharge administrative.



Basé sur API et prêt pour le DevSecOps

Protection contre un large éventail de menaces

- Top 10 des failles de sécurité applicatives identifiées par l'OWASP
  - Y compris les SQL injections, XSS, CSRF, XXE, etc.
- Advanced bots
  - Menaces automatisées visant les applications Web identifiées par l'OWASP
- Credential stuffing et piratage de comptes
- Attaques ciblant les API XML et JSON
- Attaques DDoS applicatives et volumétriques
- Attaques de type « Zero Day »
  - Puissant modèle de sécurité positive associé à une technologie de signature intelligente pour la sécurité négative

Protocoles pris en charge

- HTTP/S/0.9/1.0/1.1/2.0
- WebSocket
- IPv4

Autres fonctionnalités de sécurité avancées

- Protection de réputation d'IP
  - Géolocalisation IP et flux de réputation basés sur des capteurs de terrain et d'autres données
- Protection des téléchargements de fichiers
  - Intégration avec Barracuda Advanced Threat Protection incluse
- Altération des paramètres
- Manipulation des cookies et formulaires
- Navigation forcée
- Altération des applications
- Validation des métadonnées de champs de formulaires
- Masquage de site Web
- Contrôle de réponse
- Politiques précises pour les éléments HTML
- Vérifications des limites de protocole
- Base de données de réputation d'IP Barracuda
- Fingerprinting heuristique
- Tests CAPTCHA
- Protection contre les attaques de type Slow Client
- Nœuds de sortie ToR
- Liste de blocage Barracuda
- Protection illimitée contre les attaques DDoS L3 à L7

Barracuda®
Your journey, secured.