La liste de contrôle ultime pour l'évaluation des WAF

Un outil pour trouver la solution adaptée à vos besoins en matière de sécurité des applications et des API

Trouvez plus facilement le fournisseur de pare-feu d'application Web (WAF, Web Application Firewall) ou de protection des applications Web et des API (WAAP) qu'il vous faut. Utilisez cette liste de contrôle complète pour évaluer les fournisseurs de WAF et de WAAP, de façon à trouver la solution qui répond à vos besoins en matière de sécurité, de performances, de finances et d'opérations.

Fonctions de sécurité

Sécurité des applications

- Assurez **la couverture des 10 principales vulnérabilités selon l'OWASP**, telles que les attaques par injection SQL, par XSS, par LFI et par SSRF. Vérifiez si la protection peut être personnalisée et déployée automatiquement.
- Évaluez si votre solution contrôle de manière proactive le trafic des **adresses IP ayant une mauvaise réputation** et vous avertit si une **exception précédente est utilisée de manière abusive**.
- Évaluez la **flexibilité des listes blanches et noires** : pouvez-vous corréler des attributs tels que les empreintes IP, Geo, ASN et TLS pour créer des stratégies efficaces ?

Protection contre les attaques DDoS

- Vérifiez que le fournisseur offre une **protection DDoS multicouche** pour les applications et les API, y compris l'infrastructure DNS, les couches 3/4 et la couche 7.
- Confirmez que la solution offre une **détection comportementale des attaques DDoS** pour la sécurité des applications.
- Déterminez la granularité des contrôles de **limitation de débit**. Ces configurations sont-elles automatiques ou manuelles ? Ces mesures peuvent-elles protéger contre les attaques volumétriques et les attaques Slow POST ?
- Passez en revue les fonctionnalités qui **réduisent la charge** pendant les attaques DDoS et améliorent les performances.
- Déterminez les **coûts supplémentaires potentiels** liés à l'augmentation du trafic pendant les événements DDoS.
- Assurez-vous que **la protection contre les attaques DDoS sur la couche 7 est automatisée** pour faire gagner du temps à votre équipe et exploiter son expertise à meilleur escient. Les **protections s'adaptent-elles** à votre profil de trafic ou à votre tolérance au risque spécifique ?

Protection contre les vulnérabilités Zero Day

- Vérifiez que le WAF dispose de **protections existantes pour les CVE connues** et qu'il peut s'adapter rapidement pour se défendre contre les nouvelles attaques Zero Day. Étudiez l'**historique de la solution en matière de défense Zero Day** et ses temps de réponse.
- Déterminez si vous disposez de **protections contre des CVE spécifiques** en tant que client.

Protection des API

- Assurez-vous que la solution **protège les points de terminaison des API** contre les attaques par injection, les attaques DoS et les violations des spécifications.
- Vérifiez la fonction de **découverte des API** : peut-elle détecter automatiquement les API nouvelles et modifiées ? Dans quelle mesure pouvez-vous facilement leur appliquer une protection ?
- Confirmez les capacités de **détection des informations à caractère personnel et d'alertes** pour protéger les données sensibles et empêcher les violations de données.

Protection contre les bots

- Vérifiez si le WAF **détecte et atténue les menaces automatisées** à l'aide d'un répertoire de bots et de définitions. La solution dispose-t-elle d'un répertoire de bots étendu ? À quelle fréquence est-il mis à jour avec des bots nouveaux et modifiés ?
- Identifiez les **définitions de bots** dont dispose l'outil. Pouvez-vous **créer vos propres** définitions de bots ?
- Vérifiez si la solution inclut un **CAPTCHA ou un mécanisme de vérification humaine** sans impact sur l'expérience utilisateur. Le CAPTCHA ou le mécanisme de vérification exige-t-il que vos utilisateurs finaux interagissent avec lui avant de poursuivre ?

Informations sur les menaces et automatisation

Informations sur les menaces

- Assurez-vous que le fournisseur utilise les **données internes** pour les renseignements sur les menaces, en évitant les retards et les risques de falsification de données.
- Vérifiez la taille de **l'équipe de recherche des menaces du fournisseur** et du réseau mondial d'experts en sécurité qui surveillent les risques émergents.
- Évaluez **le volume et la pertinence des données** traitées par la base de données de renseignements. Inclut-elle des données provenant de secteurs similaires au vôtre ou d'organisations fréquemment ciblées par les cyberattaques ?

Automatisation

- Vérifiez si le WAF s'appuie sur **une technologie d'ensemble de règles obsolète**. Utilise-t-il des technologies récentes et avancées, telles que des mises à jour automatisées via une heuristique avancée et l'apprentissage automatique ?
- Assurez-vous que les ensembles de règles sont automatiquement mis à jour pour **éliminer toute intervention manuelle**. Les mises à jour automatiques sont-elles appliquées au niveau mondial ? Quelles sont vos options pour supprimer une mise à jour précédemment appliquée ou **la tester sur le trafic en temps réel** ?
- Déterminez si la solution personnalise les protections en fonction de votre environnement sans intervention. La solution **ajuste-t-elle** automatiquement les stratégies de sécurité en continu selon le profil de trafic en temps réel de votre entreprise ?
- Évaluez la façon dont la solution contrôle les **faux positifs**. Comment trouve-t-elle un équilibre entre la réduction des faux positifs et la réduction des **perturbations du trafic valide** ?

Visibilité et création de rapports

Visibilité granulaire

- Assurez-vous que le WAF offre **une visibilité détaillée sur les menaces** et les performances, grâce à des tableaux de bord et à des rapports personnalisables qui couvrent les environnements multisolutions.
- Lorsqu'elles utilisent un WAF, les équipes de sécurité passent la plupart de leur temps dans la console de données. Examinez les **options de personnalisation**, les fonctionnalités d'analyse proactive et **la granularité des rapports** dont vous bénéficierez.
- Évaluez la capacité de la solution à **surveiller efficacement le trafic des API** et des applications, à détecter les abus et à fournir des informations détaillées sur la prolifération des API.

Alertes en temps réel et analyse proactive

- Vérifiez si la solution dispose de fonctionnalités **d'alerte en temps quasi réel** qui avertissent votre équipe des menaces critiques. Les alertes doivent être personnalisables en fonction de critères spécifiques, tels que la gravité, la source ou le type d'attaque, pour une meilleure compréhension et une réponse rapide.
- Vérifiez si la solution fournit des **informations préanalysées** sur l'endroit, le moment et la manière dont les attaques se produisent, afin de réduire la charge de travail de votre équipe de sécurité. La solution doit également **recommander les étapes suivantes** pour améliorer votre position en matière de sécurité.

Plateforme et architecture

Portée mondiale

- Vérifiez si le WAF fournit un accès à un réseau mondial en bordure de l'Internet ou à des services de réseau de diffusion de contenu (CDN) pour des performances et une sécurité accrues. Confirmez la **disponibilité de la solution au niveau mondial** pour assurer la couverture de vos sites principaux et de ceux de vos clients.

Prise en charge cloud et hybride

- Vérifiez que la solution est **indépendante du cloud** et capable de prendre en charge vos environnements multicloud, hybrides et sur site. Si la solution repose sur un réseau de diffusion de contenu (CDN), assurez-vous qu'elle peut étendre la protection au-delà de la bordure de l'Internet.

Résilience et basculement

- Évaluez la **résilience de la solution** : le service informatique peut-il basculer automatiquement pour maintenir la protection en cas de panne ou d'interruption ?
- Passez en revue les **interruptions de service et les réponses récentes** du fournisseur.
- Déterminez si les **contrats de niveau de service** (SLA) répondent aux besoins de votre entreprise.

Assistance et services gérés

Assistance et accès aux services inclus

- Déterminez **les niveaux d'assistance inclus** et disponibles moyennant un coût supplémentaire avec la solution WAF.
- Vérifiez si **une réponse aux incidents 24 h/24, 7 j/7** est disponible et si vous aurez un accès direct au centre d'opérations de sécurité (SOC) pendant les attaques.
- Assurez-vous que le fournisseur propose des **services de sécurité entièrement gérés** pour combler les lacunes potentielles dans vos ressources internes, y compris l'expertise en matière de gestion des attaques, de configuration ou de rotation du personnel.

Intégration et compatibilité DevSecOps

API, CLI et automatisation de l'infrastructure

- Vérifiez l'intégration **des API, de l'interface de ligne de commande (CLI) et de Terraform** pour automatiser et intégrer la sécurité dans vos processus de développement. La prise en charge de GitOps et d'autres modèles d'infrastructures en tant que code est cruciale pour assurer la sécurité de façon cohérente dans tous les environnements.

Intégration SIEM

- Assurez-vous que le WAF **s'intègre sans accroc aux outils SIEM** tels que Splunk ou QRadar pour une surveillance, une réponse aux incidents et des rapports améliorés.

Résultats commerciaux et efficacité

Évolutivité et performances

- Vérifiez la capacité de la solution à **évoluer par elle-même** pour gérer de grands volumes de trafic sans dégrader les performances. À quel moment la solution introduit-elle une latence ou devient-elle vulnérable en cas de forte charge ?
- Assurez-vous qu'un accord de niveau de service (SLA) garantit une **disponibilité totale** et déterminez si la solution peut également accroître les performances, telles que la mise en cache et l'accélération du trafic, afin d'améliorer vos applications.

Gestion unifiée

- Vérifiez si le fournisseur propose une interface unique pour **gérer les stratégies de sécurité dans tous les environnements** (cloud, sur site et hybride). Assurez-vous que la solution peut être intégrée à votre pile actuelle et offre une expérience fluide aux équipes de sécurité et de développement.

Rentabilité

- Évaluez la capacité de la solution à **unifier les WAF, la prévention des attaques DDoS, la gestion des bots et la protection des API** sous un seul fournisseur, réduisant ainsi la complexité et les coûts de gestion. Examinez l'équilibre entre l'efficacité de la sécurité et le coût opérationnel pour déterminer la valeur globale.

Confiance et fiabilité des fournisseurs

Historique du service et de la stabilité

- Passez en revue **l'historique des interruptions et des perturbations de service du fournisseur** au cours des 5 dernières années.
- Vérifiez la **stabilité financière** de l'entreprise. Génère-t-elle des bénéfices ? Depuis combien de temps est-elle active ? Quels sont la taille et le type des clients auxquels elle fournit ses services ?

Réputation et avis

- Recherchez des avis vérifiés et des témoignages clients pour vérifier si des entreprises similaires dans votre secteur **font confiance au fournisseur**. Les cas d'utilisation des clients actuels correspondent-ils à vos besoins ?
- Vérifiez si le fournisseur est **reconnu par des analystes du secteur** comme Gartner et Forrester pour ses solutions de protection des applications et des API.
- Après avoir discuté avec le fournisseur, demandez-vous si vous **pouvez avoir confiance** en sa réactivité et en ses services d'assistance en cas de problème une fois que deviendrez client. Demandez-lui qui prendra en charge votre compte après l'intégration initiale.