FICHE PRODUIT AKAMAI

App & API Protector

Dans le monde connecté d'aujourd'hui, la protection des applications Web et des API contre la diversité de menaces qui émergent et évoluent est essentielle à la réussite de l'entreprise. Cependant, avec les migrations dans le cloud, les pratiques DevOps actuelles ainsi que les applications en constante évolution, la sécurisation des interactions digitales s'accompagne de nouvelles complexités et de nouveaux défis.

Le déploiement d'une solution globale de protection des applications Web et des API (WAAP) renforce votre sécurité en mettant à jour les protections de façon adaptée, et en fournissant de manière proactive des informations sur les vulnérabilités ciblées.

App & API Protector d'Akamai est une solution unique qui réunit de nombreuses technologies de sécurité, notamment un pare-feu d'application Web (WAF), le filtrage des bots, la protection des API et la protection contre les attaques par déni de service distribué (DDoS). App & API Protector est reconnue comme la principale solution WAAP, capable d'identifier et d'atténuer rapidement les menaces au-delà du WAF traditionnel, afin de protéger des domaines digitaux entiers contre les attaques multidimensionnelles. La plateforme est facile à mettre en place et à utiliser, offre une visibilité globale et met automatiquement en œuvre des protections à jour personnalisées via la technologie Adaptive Security Engine d'Akamai.

La puissance de la sécurité adaptative

App & API Protector va au-delà des ensembles de règles grâce à Adaptive Security Engine. Grâce à cette technologie innovante, les protections de sécurité sont constamment mises à jour de manière automatique, et les recommandations de règles personnalisées peuvent être mises en œuvre d'un simple clic. Adaptive Security Engine fournit une protection nouvelle génération qui combine l'apprentissage automatique, des informations sur la sécurité en temps réel, l'automatisation avancée et l'expertise de plus de 400 professionnels de la sécurité et chercheurs spécialisés dans les menaces. Adaptive Security Engine est unique car :

- elle analyse les caractéristiques de chaque demande en temps réel et en bordure de l'Internet pour une détection plus rapide ;
- elle apprend les schémas d'attaque en utilisant des données locales et mondiales pour effectuer des ajustements de protection spécifiques au client ; et
- elle s'adaptera aux menaces futures, ce qui garantit des protections actualisées même lorsque les attaques évoluent.

Adaptive Security Engine allège le fardeau des réglages manuels fastidieux grâce à des mises à jour sans intervention, pour une expérience presque sans intervention. Lors de son lancement, il a été prouvé que cette technologie permettait de multiplier par 2 le nombre de détections et de réduire par 5 le nombre de faux positifs. Les récentes mises à jour de nos algorithmes basés sur l'apprentissage automatique réduisent désormais les faux positifs de 4 fois supplémentaires. Les professionnels de la sécurité peuvent à nouveau être des héros et disposer de plus de temps pour se concentrer sur la sécurisation et la convivialité des opérations digitales de l'entreprise.

Avantages pour votre entreprise

Une détection fiable des attaques
Adaptez-vous à l'écosystème des menaces et protégez-vous contre les menaces existantes et émergentes, telles que les attaques DDoS, les botnets, les injections, les attaques des applications et des API et bien plus encore

Des protections étendues en un seul produit
Optimisez vos investissements en matière de sécurité avec une solution qui inclut un service WAAP, la visibilité et l'atténuation des bots, une protection contre les attaques DDoS, des connecteurs SIEM, une optimisation Web, le Cloud Computing, l'accélération API et plus encore

Une sécurité sans intervention
Réduisez les tâches de maintenance manuelles fastidieuses grâce à des mises à jour automatiques et des recommandations de réglage automatique proactives, une solution optimisée par Adaptive Security Engine d'Akamai

Simplicité d'utilisation
Profitez de la conception améliorée de l'interface utilisateur pour simplifier l'intégration et les opérations de sécurité complètes, lesquelles sont accompagnées de guides de configuration et de dépannage

Une visibilité unifiée
Analysez l'ensemble de vos indicateurs de sécurité dans un seul et même tableau de bord ou rapport de découverte proactif via la fonction de télémétrie partagée des solutions de sécurité d'Akamai

Nouveau : moteur de protection contre les attaques DDoS par analyse comportementale

Le nouveau moteur de protection contre les attaques DDoS par analyse comportementale renforce et simplifie la défense contre les attaques DDoS au niveau de la couche applicative et est alimenté par l'apprentissage automatique. Les algorithmes de détection comportementale et basée sur les anomalies du moteur de protection contre les attaques DDoS examinent diverses dimensions du trafic, telles que la source du pays, l'empreinte du réseau et d'autres attributs des requêtes HTTPS, afin de créer des protections sur mesure et de fournir une approche non interventionniste contre les attaques DDoS au niveau de l'application.

L'utilisation de l'apprentissage automatique du moteur de protection contre les attaques DDoS par analyse comportementale améliore l'efficacité et la prise de décision sur les

Au-delà des ensembles de règles, App & API Protector d'Akamai est optimisé par Adaptive Security Engine.

Détection de pointe des attaques : vos protections en tant que client Akamai s'étendent au rythme du développement de votre environnement digital. En plus des mises à jour automatiques et du réglage automatique adaptatif qu'offre Adaptive Security Engine, App & API Protector réalise des détections de pointe reconnues par les analystes : détections d'attaques DDoS, de bots, de logiciels malveillants ou autres vecteurs d'attaque. Confirmez vos protections Akamai contre les CVE émergentes et en évolution grâce à notre outil de recherche sur les menaces.

Sécurité des applications : App & API Protector propose une suite complète de défenses et de personnalisations permettant d'adapter la sécurité aux besoins de votre organisation. Des fonctionnalités efficaces telles que Client Reputation, les listes de réseaux, la détection des nouvelles attaques et bien d'autres encore vous donnent l'avantage sur les adversaires tout en simplifiant les opérations de sécurité. Les défenses avancées de la couche applicative de la solution WAAP d'Akamai permettent de lutter contre les attaques DDoS, les injections SQL, le cross-site scripting, l'inclusion de fichiers locaux, la falsification de requêtes côté serveur et d'autres vecteurs d'attaque.

Protection contre les attaques DDoS et contrôle granulaire des débits : reconnue comme une solution DDoS leader sur le marché, App & API Protector offre une protection contre les attaques DDoS sur plusieurs fronts. Il commence par abandonner instantanément les attaques DDoS de la couche réseau en bordure de l'Internet afin de réduire les risques et d'économiser les ressources. Ensuite, il détecte et atténue automatiquement les attaques DDoS sophistiquées de la couche 7 en bordure de l'Internet pour une protection en temps réel et autonome contre l'évolution des menaces DDoS. Les contrôles granulaires des débits personnalisent votre défense DDoS spécifiquement pour vos profils de trafic et d'attaque.

Visibilité et atténuation des bots : bénéficiez d'une visibilité en temps réel de votre trafic de bots avec l'accès au répertoire d'Akamai, qui recense plus de 1 750 bots connus. Étudiez les analyses de sites Web faussées, empêchez la surcharge d'origine et créez vos propres définitions de bot pour permettre l'accès aux bots tiers et partenaires sans obstruction. Des contrôles étendus des bots, y compris la détection de l'usurpation d'identité du navigateur, les actions conditionnelles et les défis cryptographiques, sont désormais inclus dans App & API Protector.

10 principaux risques selon l'OWASP

Akamai atténue les 10 principaux risques de l'OWASP ainsi que les 10 principaux risques pour la sécurité des API de l'OWASP. Découvrez comment App & API Protector et Akamai Security protègent vos clients des menaces importantes, courantes ou émergentes.

Pour en savoir plus sur les protections d'Akamai contre les 10 principaux risques de l'OWASP, téléchargez le livre blanc.

Protection des API : la solution de pointe d'Akamai pour la sécurisation des API renforce votre protection et vous offre une visibilité du trafic sur l'ensemble de vos domaines digitaux, en révélant de manière proactive les vulnérabilités, en identifiant les changements d'environnement et en vous protégeant contre les attaques masquées. Grâce aux capacités API d'App & API Protector, vous pouvez :

- détecter automatiquement une gamme complète d'API connues, inconnues et changeantes sur l'ensemble de votre trafic Web, y compris leurs points de terminaison, définitions et profils de trafic ;
- enregistrer les API récemment découvertes en quelques clics ;
- assurer la protection des API contre les attaques DDoS, les injections malveillantes, les attaques par vol d'identifiants et les violations des spécifications API ; et
- contrôler le traitement des données sensibles avec la fonction de génération de rapports sur les informations personnelles identifiables d'App & API Protector pour garantir votre conformité permanente.

Performances et plus encore grâce au plus grand réseau mondial : la présence de la plateforme Akamai offre aux clients un avantage concurrentiel grâce à son envergure mondiale inégalée, offrant une visibilité en temps réel d'une part importante du trafic Internet mondial. Ces données volumineuses permettent à Akamai de fournir des informations exploitables sur les menaces afin d'aider les entreprises à garder une longueur d'avance sur les menaces de sécurité en constante évolution et de permettre une détection et une atténuation plus rapides des attaques dans divers environnements. La plateforme offre également une augmentation des performances éprouvée et une disponibilité de 100 % garantie par un accord de niveau de service (SLA).

Protection contre les logiciels malveillants : ce module complémentaire peut analyser les fichiers en amont, avant qu'ils ne soient téléchargés, afin de détecter les logiciels malveillants et de les bloquer avant qu'ils ne soient importés dans les systèmes de votre entreprise. Grâce à l'absence de configuration d'application ou d'API supplémentaire, vous ne perdez plus de temps à configurer la protection dans chaque système individuellement.

Outil Simple Start Onboarding : de bons outils de sécurité ne fonctionnent que si vous les utilisez. Akamai s'est donné pour mission de créer une plateforme facile à utiliser qui permet de rester productif tout en bénéficiant de protections solides. Vous pouvez assurer une intégration rapide grâce à notre fonction de démarrage simplifié ou appliquer des protections à de nouvelles applications en quelques clics seulement.

Tableaux de bord, alertes et outils de création de rapports : Web Security Analytics est le tableau de bord de télémétrie détailles des attaques d'Akamai. Vous pouvez y analyser les événements de sécurité, créer des alertes par e-mail en temps réel à l'aide de filtres statiques et de seuils, et utiliser les outils de création de rapports personnalisables pour surveiller et évaluer en permanence l'efficacité de vos protections sur l'ensemble de la plateforme Akamai.

Intégrations DevOps : intégrez de manière fluide la sécurité dans les flux de travail DevOps avec GitOps, en veillant à ce que la sécurité s'aligne sur un développement rapide. Les API d'Akamai, disponibles via CLI ou Terraform, permettent une gestion complète d'App & API Protector via le code et correspondent à toutes les actions disponibles dans l'interface utilisateur.

Intégrations SIEM : des API SIEM sont également disponibles, et des connecteurs pré-intégrés pour Splunk, QRadar, ArcSight et plus encore sont automatiquement inclus avec App & API Protector.

Fonctionnalités incluses : pour améliorer la visibilité et les performances, App & API Protector intègre désormais de nombreux produits parmi les plus appréciés des clients Akamai, notamment :

- Site Shield : empêchez les pirates de contourner les protections basées sur le cloud et de cibler votre infrastructure d'origine
- mPulse Lite : bénéficiez d'une visibilité approfondie sur le comportement des utilisateurs, traitez les problèmes de performances en temps réel et mesurez l'impact des changements digitaux sur les revenus
- EdgeWorkers : découvrez les avantages de l'informatique sans serveur, notamment en termes de délai de mise sur le marché et d'exécution logique au plus près des utilisateurs finaux
- Image & Video Manager : optimisez intelligemment les images et les vidéos en combinant qualité, format et taille
- Accélération des API : améliorez les performances de vos API grâce à une gestion aisée de l'accès, à une adaptation aux pics de demande et une amélioration de la sécurité des API

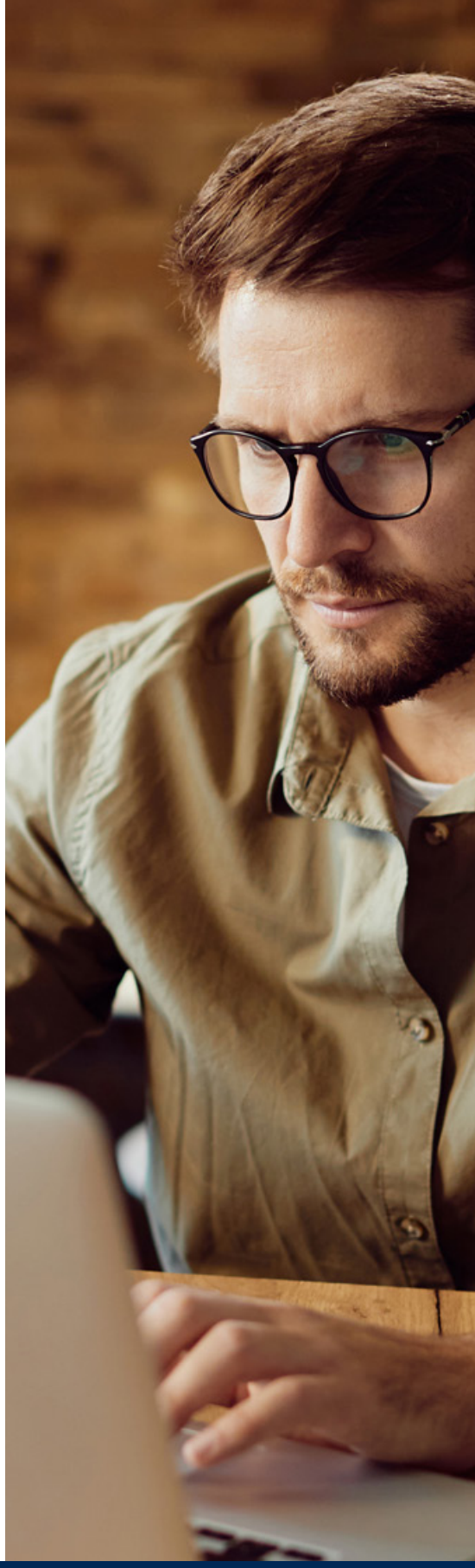
Les offres de niveau gratuit peuvent être soumises à des restrictions d'utilisation. Contactez Akamai pour plus d'informations.

Advanced Security Management

Le module optionnel Advanced Security Management offre une flexibilité d'automatisation et de configuration aux clients ayant des environnements applicatifs plus complexes et des besoins de sécurité avancés. L'option Advanced Security Management inclut des configurations de sécurité supplémentaires, des stratégies de taux, des stratégies de sécurité, des contrôles des attaques DDoS au niveau de la couche applicative, des règles WAF personnalisées, une sécurité des API positive, ainsi que l'accès aux informations sur les menaces relatives à la réputation des adresses IP (réputation du client) prêtes à l'emploi.

Managed Security Service

Un service d'assistance est proposé 24 h/24, 7 j/7 et 365 j/an à tous les clients d'Akamai. En plus des services professionnels à la demande pour le conseil ou le travail sur un seul projet, Akamai propose des niveaux de services gérés : service WAAP entièrement géré, assistance gérée en cas d'attaque et assistance spécialisée du centre d'opérations de sécurité.



Découvrez App & API Protector et inscrivez-vous pour un essai gratuit sur akamai.com/aap