Akamai

LIVRE BLANC

Simplifiez la sécurité de vos applications Web

Les attaques applicatives Web

Les nouvelles applications Web sont devenues complexes, en particulier avec l'adoption croissante d'architectures basées sur les microservices. La forte dépendance vis-à-vis des API pour pratiquement toutes les interactions en ligne contribue à cette complexité et entraîne de potentiels nouveaux points d'entrée pour les pirates informatiques. Les failles de sécurité Web connues, quant à elles, sont toujours présentes et sont réintroduites dans les applications par chaque nouvelle génération de codeurs. Les hackers d'aujourd'hui ont évolué en conséquence, utilisant des bots, des DDoS-for-hire et des attaques multivecteurs pour cibler des applications Web, des API et même des failles côté client.

Les attaques opportunistes, cependant, restent les attaques Web les plus courantes : elles ne sont pas spécifiquement configurées pour cibler votre organisation, mais le feront dès qu'elles détecteront une faille. Les analyseurs de vulnérabilités utilisent des bots automatisés pour parcourir les sites Web au hasard, en recherchant constamment des milliers de failles. Dès lors qu'une faille est détectée, les hackers peuvent faire en sorte qu'une base de données révèle ses secrets, charger des fichiers malveillants sur un serveur Web ou s'acharner sur un site en le submergeant de trafic.

Quel sont les risques associés aux attaques Web ?

Les organisations ayant une faible tolérance au risque nécessitent d'excellents résultats en matière de sécurité pour établir une chaîne de confiance, tant en interne (entre les systèmes, la chaîne d'approvisionnement, les opérations, etc.) qu'en externe (avec les partenaires, les clients, les organismes de réglementation, etc.). Il est particulièrement important de sécuriser les API, qu'il s'agisse de simples flux internes entre les parties d'une application microservice ou d'importantes transactions interentreprises, car elles servent de ciment numérique reliant divers systèmes et écosystèmes de partenaires et permettant des expériences digitales et omnicanal pour les clients.

Malheureusement, les cybercriminels disposent d'un arsenal presque illimité de méthodes d'attaque Web conçues pour causer un maximum de dégâts. Un piratage réussi qui entraîne l'exfiltration de données sensibles, ou une attaque DDoS qui rend vos sites indisponibles, peut briser cette confiance et causer des dommages importants tels que la perte de la fidélité des clients, des pénalités réglementaires, des poursuites judiciaires et une réputation de marque amoindrie.

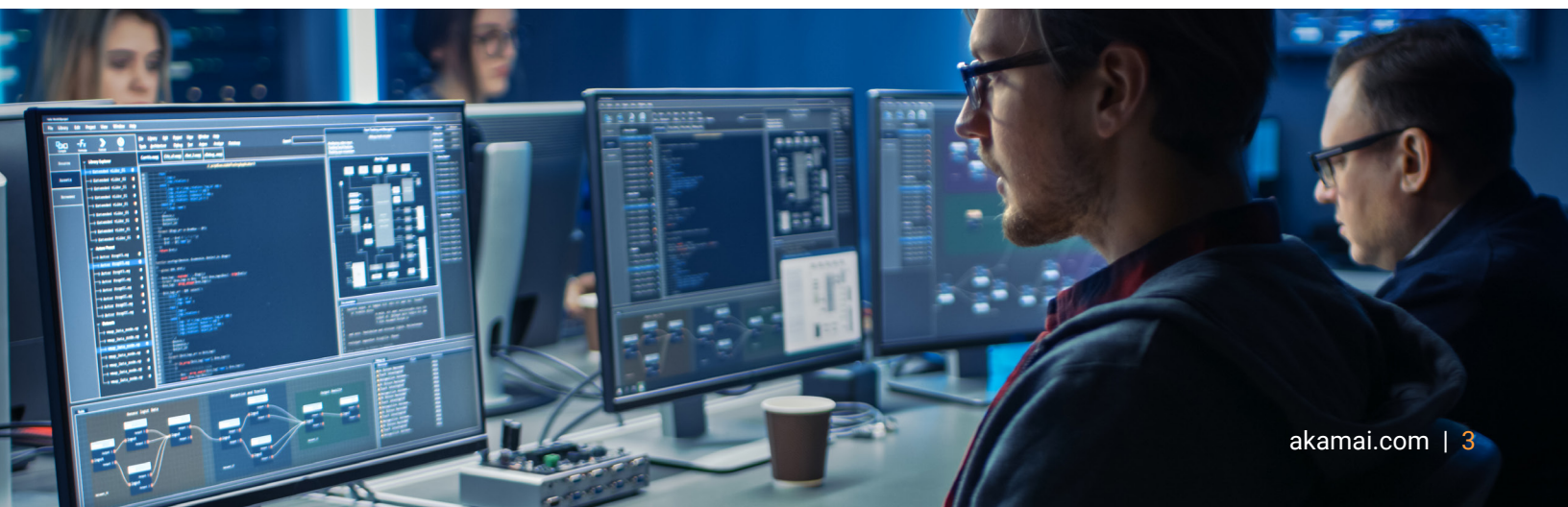
Défis liés à la sécurité des applications Web

Les solutions de protection des API et des applications Web (WAAP) basées dans le cloud sont conçues pour atténuer de nombreuses formes d'attaques d'applications Web, DDoS et API. Toutefois, l'un des principaux défis liés aux pare-feu est que les équipes AppSec doivent constamment analyser et ajuster les règles au fur et à mesure que les applications changent, que les menaces évoluent et que les mises à jour deviennent disponibles. La dotation en personnel de de la sécurité expérimenté reste un défi, les personnes qualifiées changeant souvent de poste tous les deux ans. Il s'agit souvent d'un processus manuel qui prend du temps, qui nécessite des opérateurs qualifiés et qui n'est pas évolutif pour la plupart des organisations en raison de la rotation des effectifs, des cycles de formation et des architectures d'intégration technologique spécialisées.

Les stratégies de sécurité obsolètes peuvent devenir source de frustration, car la fatigue liée aux alertes diminue considérablement la capacité à différencier avec précision les faux positifs des attaques réelles. Les équipes de sécurité qui ne sont pas en mesure de préciser efficacement les règles peuvent également retirer leurs protections et accepter sciemment une posture de risque accrue par crainte d'avoir un impact sur les utilisateurs légitimes et de perturber les activités.

Pourquoi Akamai WAAP ?

Akamai App & API Protector est une solution WAAP basée dans le cloud, offrant visibilité sur les bots et atténuation de ces derniers, et conçue pour vous aider à protéger vos applications et vos API à l'échelle contre de très nombreuses menaces au niveau du réseau et des couches applicatives, avec moins d'efforts et à moindres frais. L'assistant d'intégration en libre-service d'Akamai réduit le besoin de connaissances préalables, en fournissant des conseils et des informations pour sécuriser rapidement et facilement vos ressources. Notre processus de configuration automatisé analysera les déclencheurs de sécurité et apprendra le comportement des applications pour auto-ajuster les protections, ce qui conduira à plus d'économies de ressources. App & API Protector supprime de nombreux problèmes de pare-feu actuels provoquant des frictions au sein de l'organisation et représentant un poids pour les opérations et un obstacle au déploiement.



Les protections automatisées, qui peuvent être entièrement gérées par Akamai, sont appliquées sur la plateforme la plus distribuée au monde, ce qui vous permet d'adopter une approche autonome de la sécurité des applications et des protections des API. La protection automatique contre les attaques Web telles que l'injection SQL, le cross-site scripting (XSS) et l'inclusion de fichiers locaux offre une couverture étendue, sans besoin de maintenance permanente. Et en appliquant l'apprentissage automatique et l'heuristique, nous parvenons à améliorer l'identification des modèles de faux positifs dans votre trafic, règle par règle (et non en effectuant une vérification générique à l'échelle du réseau), pour des résultats plus pertinents et exploitables.

Validez votre position de sécurité avec notre outil de recherche CVE, qui fournit des informations détaillées par CVE, y compris les niveaux de menace et des informations sur les protections actuelles d'Akamai, pour vous aider à orienter vos stratégies de sécurité et de développement internes. De plus, améliorez l'alignement en interne et accélérez les délais de mise sur le marché grâce aux intégrations SecDevOps prédéfinies d'Akamai, notamment le code Akamai, les API, l'interface de ligne de commande, Terraform et les intégrations.

Placer la barre haut avec les protections adaptatives

Comment la solution App & API Protector offre-t-elle à la fois simplicité et précision ? Tout d'abord, le moteur de sécurité adaptatif d'Akamai, technologie de base dans App & API Protector, est unique, car il apprend les modèles de trafic et d'attaque propres à chaque client, analyse les caractéristiques de chaque demande en temps réel et utilise ces connaissances pour intercepter les menaces futures et s'y adapter. Cette technologie facilite les opérations de sécurité en prenant en compte tous les points de données anormaux ou suspects et en attribuant un score de menace à chaque requête. Plus le score de menace est élevé, plus les protections sont agressives et, en modifiant les protections de manière dynamique pour qu'elles correspondent au niveau de menace détectée, nous pouvons identifier les attaques les plus discrètes, tout en maintenant le taux de faux positifs extrêmement bas.

Les attaques d'applications impliquent généralement une certaine stratégie de reconnaissance, mais alors que les pirates cherchent des failles, Akamai établit des preuves de leurs techniques et tactiques. Cela permet non seulement de procéder à une identification rapide, mais aussi de laisser une empreinte historique de votre trafic spécifique, au cas où les attaquants reviendraient. Plus un hacker tente d'attaques, plus vos protections sont renforcées.

Akamai a une visibilité sur :

Plus de 780 millions
d'alertes quotidiennes d'attaques d'applications Web

Plus de 26 milliards
de requêtes de bots

Plus de 932 To
de données quotidiennes analysées

Informations collaboratives sur les menaces

Un grand nombre des sites Web les plus attaqués sur Internet sont des clients d'Akamai, notamment 9 des 10 plus grandes entreprises de commerce de détail, les 10 plus grandes banques, 9 des 10 plus grandes entreprises de santé, les 6 branches de l'armée américaine, et bien d'autres encore. Nous avons une visibilité sur plus de 780 millions d'attaques quotidiennes d'applications Web et plus de 26 millions de requêtes de bots. Des centaines de data scientists et de spécialistes des menaces, experts dans leur domaine, interrogent quotidiennement plus de 932 To de nouvelles données sur les menaces. Ce niveau de visibilité mondiale, associé à l'apprentissage automatique avancé, à l'intelligence artificielle et à l'analyse humaine, nous permet de bloquer de manière proactive et prédictive les attaques courantes et hautement sophistiquées.

Akamai lutte contre les attaques d'applications depuis plus d'une décennie. Nous protégeons nos clients et garantissons la disponibilité de leurs infrastructures en faisant face à certaines des attaques les plus redoutables. Nous continuons d'étudier et de signaler les menaces émergentes. À mesure que les attaques continuent d'évoluer et de s'étendre et qu'elles deviennent plus sophistiquées, nous continuons d'innover et d'adapter nos solutions pour garder une longueur d'avance sur les hackers. Et étant donné que App & API Protector est basée sur l'Intelligent Edge Platform d'Akamai, elle est équipée de fonctionnalités de performance préintégrées conçues pour offrir des performances optimales à vos sites Web, applications et API.

Passez en revue vos besoins en matière de protection d'applications Web et d'API, et découvrez les avantages d'Akamai App & API Protector en utilisant cette version d'essai gratuite.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer le Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 06/24.