Déconstruction des 5 mythes sur les pare-feux d'applications Web

Les entreprises qui réalisent des activités stratégiques en ligne doivent utiliser le WAF (pare-feu d'applications Web) comme première ligne de défense pour tenir à l'écart le trafic malveillant, tout en permettant au trafic légitime de passer à travers le pare-feu. La technologie WAF étant disponible depuis de nombreuses années, sa définition d'origine est beaucoup trop simpliste pour refléter ses utilisations actuelles, qui ont bien évolué. Cette dichotomie explique pourquoi un certain nombre de mythes et perceptions désuètes restent tenaces chez de nombreux dirigeants et professionnels de la sécurité.

Ces mythes risquent d'amener les entreprises à sous-estimer et à sous-exploiter la puissance du WAF qui fait probablement déjà partie de leur pile, ouvrant la porte aux attaques et augmentant les risques opérationnels. Le besoin de la technologie WAF de pouvoir s'appuyer sur une sécurité digitale totale continue de croître. Pour améliorer les stratégies de sécurité et tirer parti des dernières technologies de protection WAF, nous devons commencer par nous attaquer aux mythes les plus courants.

Nous avons observé 9,93 milliards d'attaques d'applications Web au troisième trimestre 2023

Les attaques quotidiennes au cours du troisième trimestre 2023 ont culminé à environ 327 millions

Source : Recherches sur les menaces d'Akamai

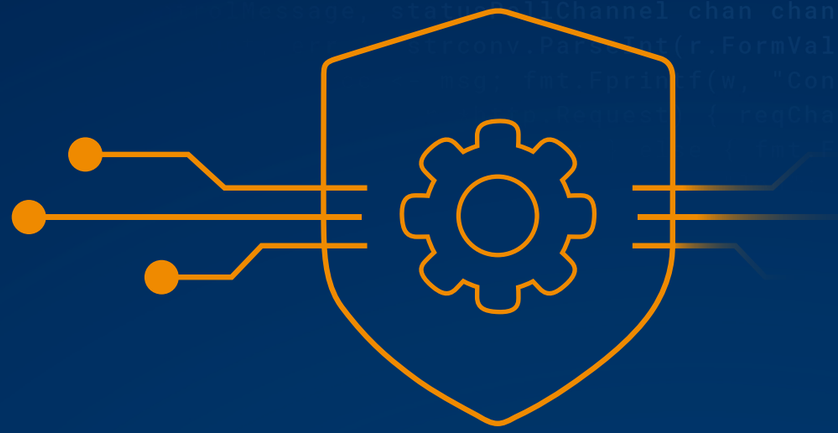
Mythe 1

Les WAF nécessitent des mises à jour manuelles constantes pour rester efficaces

S'il est vrai que les dernières mises à jour fournissent les dernières protections, il existe plusieurs idées reçues à ce sujet qui demandent à être clarifiées. À l'heure actuelle, de nombreuses entreprises ne disposent pas de l'expertise en matière de sécurité ou des ressources nécessaires pour mettre à jour et ajuster en permanence les règles WAF. L'impact des mises à jour automatisées et adaptatives sur les entreprises va bien au-delà du gain de temps et de la facilité d'utilisation : c'est aussi une question de réduction des risques. En examinant les entreprises ayant opté pour les mises à jour manuelles, nous avons constaté que plus de 77 % d'entre elles étaient en retard de cinq versions ou plus en matière de mise à jour des ensembles de règles. Akamai diffuse automatiquement et continuellement des mises à jour WAF, ce qui permet à votre entreprise de gagner du temps, d'économiser des ressources et de réduire les risques inutiles.

Mythe 2

Les WAF sont de simples gardiens du trafic



Là où un WAF hérité s'interposait entre les utilisateurs et les applications Web pour inspecter le trafic HTTP par rapport à une liste définie de règles, la solution d'Akamai a apporté des innovations rapides et marquées, fournissant davantage de fonctionnalités et de protections, notamment l'atténuation contre les attaques DDoS, la sécurité des API, la réduction des bots, la détection des logiciels malveillants, l'identification des données sensibles et l'accélération des performances. Et, avec la nouvelle version d'App & API Protector, votre solution de sécurité WAF est désormais associée à encore plus de technologies appréciées des clients, notamment Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager, API Acceleration et plus encore. L'exécution par Akamai d'une solution WAF est une technologie multifonction qui offre aux professionnels de la sécurité une visibilité et des contrôles complets sur les protections de sécurité de l'ensemble du domaine.

Mythe 3

Les WAF contribuent à la fatigue liée aux alertes des défenseurs

Demandez à n'importe quel défenseur de première ligne, il vous dira à quel point les équipes de sécurité sont saturées par le volume impressionnant d'alertes et de déclencheurs sur lesquels elles doivent enquêter, en particulier ceux qui sont générés par les défenses WAF. C'est la raison pour laquelle Akamai a développé Adaptive Security Engine, la technologie au cœur de sa solution WAF. Grâce à Adaptive Security Engine, votre entreprise bénéficie d'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 chercheurs Akamai spécialisés dans les menaces.

Conçue pour protéger des domaines entiers d'applications Web et d'API, la technologie Adaptive Security Engine est unique, car elle apprend les modèles de trafic et d'attaque spécifiques 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. En s'appuyant sur Adaptive Security Engine, les défenseurs peuvent dire adieu à la lassitude liée aux alertes, tout en économisant un temps précieux et en réduisant le niveau d'effort nécessaire pour protéger les applications et les API.

Il a été démontré que les recommandations de réglage d'Adaptive Security Engine divisaient le nombre de faux positifs par

5

Mythe 4

Plus de règles WAF personnalisables signifie plus de sécurité

Plus de règles, c'est souvent plus de configuration, plus de tests et plus d'analyses. L'augmentation du nombre de règles ne se traduit pas toujours par une amélioration de la sécurité, mais on peut en dire autant de la diminution du nombre de règles. Si vous êtes un professionnel de la sécurité convaincu qu'on peut faire plus avec plus, soyez tranquille. Notre solution WAF comprend un nombre illimité de règles personnalisées, et nous fournissons des mises à jour proactives et adaptatives quel que soit le nombre de règles dont vous disposez. Grâce aux mises à jour et à l'auto-réglage automatiques, votre équipe peut vérifier efficacement la configuration WAF sur l'ensemble de vos domaines digitaux. Vous souhaitez ajouter une nouvelle règle ? Le mode d'évaluation vous permet d'évaluer l'impact des nouvelles règles et des règles modifiées sur le trafic réel, en affichant les effets en temps réel dans les tableaux de bord du portail client. Ce type de test en mode fantôme garantit que votre nouvelle règle offre exactement la protection prévue lors du déploiement.

Mythe 5

Les WAF ne font qu'entraver l'activité des développeurs

Aujourd'hui, les développeurs génèrent de la valeur qui est reconnue par les clients. Si la sécurité complique les choses, l'innovation ralentit, les cycles de lancement sont retardés et le délai de rentabilisation augmente. Mais les versions non testées peuvent aussi avoir des effets dévastateurs sur la sécurité et provoquer l'arrêt des activités de l'entreprise. Chez Akamai, nous défendons la cause des professionnels de la sécurité et des développeurs. Nous sommes convaincus que les défenses WAF, celles qui protègent entre autres les applications et les API, permettent d'établir une culture DevSecOps qui favorise la rapidité, l'agilité et la collaboration. C'est pourquoi toutes nos fonctionnalités WAF peuvent être gérées via une API AppSec ouverte ou un outil Terraform qui permet à votre équipe d'automatiser l'intégration des applications et des API, ainsi que la gestion des configurations de sécurité. Et si vous avez besoin d'un coup de pouce, vous pouvez compter sur TechDocs d'Akamai, qui fournit des fonctionnalités dernier cri, interactives et intuitives spécialement conçues pour les développeurs.

Comment Akamai peut vous aider

Confrontés à des surfaces d'attaque en expansion rapide et à des menaces en constante évolution, auxquelles il faut ajouter des pirates extrêmement motivés, les défenseurs ont besoin d'une visibilité qui va au-delà des protections WAF traditionnelles. App & API Protector d'Akamai est une solution unique qui réunit de nombreuses technologies de sécurité, notamment un pare-feu d'applications Web, le filtrage des bots, la sécurité des API et la protection contre les attaques DDoS. Avec App & API Protector, 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, la technologie au cœur d'App & API Protector, offre une protection nouvelle génération qui combine l'apprentissage automatique, les informations sur la sécurité en temps réel, l'automatisation avancée et l'expertise de plus de 400 chercheurs spécialisés dans les menaces.

Testez une version gratuite ou découvrez comment Akamai protège vos ressources en ligne les plus stratégiques afin de réduire les risques (et les frictions opérationnelles) pour votre entreprise.