Akamai

LIVRE BLANC

Du WAF au WAAP : l'approche d'Akamai pour une solution complète de sécurité des applications et des API

Table des matières

Introduction

Face à des surfaces d'attaque de plus en plus vastes et diversifiées, à des frictions et des coûts opérationnels croissants et à des menaces multidimensionnelles toujours plus évasives, les équipes de sécurité ont besoin d'une visibilité allant au-delà du Web Application Firewall (WAF) traditionnel. Plus précisément, elles ont besoin d'outils plus automatisés pour accroître leur efficacité, et de protections plus poussées dans l'écosystème des applications et des interfaces de programmation d'applications (API). La terminologie la plus récente pour ces protections est la protection des applications Web et des API (WAAP). Les organisations perspicaces qui accordent la priorité à la sécurité de leur entreprise et à la sûreté de leurs clients exigent une protection complète contre plusieurs menaces sur l'ensemble de leur patrimoine digital. En plus de protéger les applications contre les attaques connues, inconnues et de type « zero day », ces protections comprennent les éléments suivants :

- Détection adaptative des menaces
- Mises à jour automatisées des règles
- Défense robuste contre les attaques DDoS
- Identification et protection des API
- Visibilité et atténuation des bots
- Intégrations faciles pour les cycles de développement

Ce document traite de la technologie WAF traditionnelle, du passage du WAF au WAAP et de la demande continue du marché qui fait évoluer les solutions WAAP. En tant que leader établi dans le domaine de la sécurité, Akamai concentre son approche sur l'innovation dans les technologies de sécurité qui soutiennent et protègent la vie en ligne des utilisateurs finaux.

Définition traditionnelle d'un WAF

Un WAF traditionnel se situe au milieu du flux de trafic entre les utilisateurs finaux et une application Web. Le WAF inspecte le trafic HTTP chiffré ou non qui le traverse afin de détecter toute attaque définie par une liste de règles.

La plupart des WAF s'appuient sur une liste prédéfinie de règles pour identifier les requêtes HTTP malveillantes intercalées dans le trafic HTTP légitime afin de se prémunir contre des milliers de failles potentielles connues. En outre, de nouveaux vecteurs d'attaque ou des permutations supplémentaires de vecteurs existants évoluent continuellement et sont exploités par les acteurs malveillants. C'est pourquoi un WAF traditionnel doit continuellement mettre à jour ses règles et les adapter aux caractéristiques du trafic légitime, qui diffèrent selon les applications et évoluent avec le temps.

Les utilisateurs finaux ayant exigé davantage de protection et de performance, les WAF ont élargi leur champ d'action pour inclure des technologies et des services de sécurité adjacents tels que l'atténuation des attaques par déni de service distribué (DDoS), la sécurité des API et les capacités d'atténuation des bots. Cette évolution continue justifie une nouvelle définition et une nouvelle terminologie.

Les défis d'un WAF traditionnel

Les organisations dotées d'un WAF affirment souvent qu'il ne répond pas aux attentes initiales en termes d'efficacité, de facilité de gestion et d'impact sur les applications et API protégées. En raison des problèmes de performance Web qui surviennent souvent lors de l'inspection de milliards de requêtes Web et API à la recherche de code malveillant, les WAF ont souvent été une source de tension interne à l'entreprise, de dégradation des performances et d'obstruction au déploiement en raison des protocoles de sécurité.

Certains des défis de déploiement les plus importants avec les WAF traditionnels découlent des éléments suivants :

- Les détections inexactes et les faux positifs élevés créent une saturation d'alertes, et donc plus de risques
- Les WAF reposent sur une révision, un réglage et une maintenance manuels
- L'absence de contrôles granulaires conduit à des règles de refus trop strictes qui perturbent l'expérience de l'utilisateur final et les processus métier
- Des renseignements obsolètes sur les menaces augmentent les vulnérabilités
- Une baisse des performances et de la couverture en raison des restrictions et d'un manque de flexibilité
- Trop limités pour protéger l'expansion digitale

Les WAF traditionnels sont un outil de sécurité puissant. Cependant, ils peuvent souvent laisser les organisations face à des difficultés opérationnelles et des risques non atténués, qui seront abordés dans ce document.

Les organisations qui cherchent à mettre à jour leur technologie WAF avec une solution WAAP doivent s'assurer que la solution offre à la fois une valeur commerciale et des protections de sécurité robustes. La conversion du WAF au WAAP combine cette puissance de protection avec des fonctionnalités, des gains d'efficacité et une facilité d'utilisation pour répondre aux besoins des entreprises, tant pour les équipes de sécurité que pour les autres équipes.

Principes de conception : du WAF au WAAP

Comme le produit WAF traditionnel se concentre sur la création de règles par l'utilisateur final, n'importe quel fournisseur peut construire une solution WAF et la mettre sur le marché avec une relative facilité, comme le démontre la prévalence des offres commerciales construites autour du projet open source Open Worldwide Application Security Project ModSecurity Core Rule Set (OWASP CRS).

Cependant, il est difficile pour un fournisseur de concevoir une solution WAAP complète qui puisse répondre aux critères suivants :

- Être déployée en ligne pour protéger les applications et les API à mesure que de nouvelles vulnérabilités apparaissent
- Suivre le rythme des pratiques récentes de développement d'applications
- Fournir des couches tout aussi solides de défense DDoS, d'atténuation des bots, de protection des API et de protection des applications Web côté client

Alors qu'Akamai concevait notre solution WAAP, nous pensions qu'elle devait être plus que « suffisamment bonne ». App & API Protector a été créé pour répondre aux risques de sécurité tout en permettant à nos clients de se concentrer sur leurs principaux objectifs commerciaux. Dans le cadre de notre conception, nous pensions qu'une solution WAAP idéale devait fournir les avantages suivants :

Sécurité efficace
Les applications exécutent tous les aspects de l'entreprise. Les protéger contre les actes malveillants est l'objectif fondamental d'une équipe de sécurité d'entreprise. Les équipes de sécurité sont mises au défi de trouver une solution WAAP qui offre les meilleures détections de sa catégorie. L'outil de sécurité idéal donne la priorité à l'efficacité de la détection, car c'est l'aspect le plus important d'une solution WAAP, et a fait ses preuves en matière de défense contre les attaques « zero day », les vulnérabilités et failles courantes (CVE), ainsi qu'en matière de disponibilité.

Précision
Les équipes de sécurité doivent trouver le juste équilibre entre l'atténuation des risques et la rapidité d'exécution de l'entreprise. Les solutions idéales disposeront de mécanismes de réglage automatique qui contribuent à réduire les faux positifs sans compromettre l'expérience de l'utilisateur final et les processus métier.

Protections de pointe
Les organisations doivent continuellement (et souvent manuellement) mettre à jour leurs protections en fonction des règles les plus récentes afin de faire face aux nouvelles vulnérabilités au fur et à mesure qu'elles sont découvertes. Pour ce faire, elles ont besoin de deux capacités clés : l'accès aux derniers renseignements sur les vecteurs d'attaque et des ressources de sécurité qualifiées capables d'adapter la stratégie de défense pour faire face aux attaques malléables. Une solution idéale sera un leader dans la communauté du renseignement sur les menaces et fournira des capacités qui simplifient les opérations de sécurité à travers les protections du domaine.

Adaptabilité
L'écosystème des menaces évolue à un rythme rapide. Avec les attaques alimentées par l'IA qui se profilent à l'horizon, les équipes de sécurité doivent être plus efficaces que jamais dans leurs opérations de sécurité. Les solutions WAAP idéales combineront automatisation avancée, apprentissage automatique et intelligence globale approfondie pour fournir des mises à jour automatiques et des suggestions de modification de règles personnalisées mises en œuvre en un clic.

Visibilité
Les solutions WAF traditionnelles fournissent généralement un flux d'alertes sans fin et s'appuient sur les professionnels de la sécurité pour analyser attentivement chaque alerte, ce qui mobilise des ressources internes. Une solution WAAP plus efficace offre une visibilité multi-solutions et un contexte proactif autour des attaques en notifiant à une organisation quand, où et comment elles se sont produites afin d'alléger la charge des ressources.

Évolutivité
Une solution dont l'échelle est insuffisante pour gérer le trafic entrant peut facilement devenir un goulet d'étranglement qui augmente la latence du Web et risque de céder sous la charge. Une approche WAAP efficace s'adapte de manière fluide et automatique aux demandes de trafic et aux attaques qui varient au fil du temps, et offre une protection continue sans interruption ni réduction des performances.

Coopération
Une solution de sécurité efficace doit pouvoir s'intégrer à la pile actuelle, être programmable, simple à utiliser et sans friction. Une solution idéale établit un pont entre les équipes de sécurité et de développement.

Assistance
Lors d'événements de sécurité exigeants, les organisations sont souvent dépassées par les compétences et les ressources nécessaires pour fournir une résolution rapide. Une solution idéale offrira des options de services gérés réguliers, ainsi que des options de services à la demande, qui peuvent fournir une expertise et une atténuation des risques pour les scénarios courants, notamment les attaques actives, les problèmes de services, la rotation du personnel, les lacunes internes en matière de compétences, etc.

En gardant ces principes de conception à l'esprit, examinons comment Akamai aborde la construction de notre solution WAAP de pointe, App & API Protector, en commençant par la technologie de base. Notre solution combine plusieurs produits de sécurité en un seul pour relever de manière globale les défis posés par la sécurisation des applications, la défense contre les attaques DDoS volumétriques, la protection des API dans l'ensemble du domaine et le contrôle du trafic des bots.

L'approche d'Akamai en matière de WAAP

Aller au-delà des ensembles de règles

Alors que le marché passait des principes de conception traditionnels des WAF à la solution de sécurité de pointe et efficace qu'est le WAAP, la priorité restait la mise en place d'une technologie efficace de détection et d'atténuation.

Akamai a lancé son WAF en 2009, le premier WAF en bordure de l'Internet au monde. Les fournisseurs de solutions de sécurité proposaient alors des WAF reposant sur des ensembles de règles statiques comme base de détection. Akamai s'est différencié à l'époque en créant un moteur propriétaire basé sur des règles appelé Kona Rule Set, qui utilisait un petit nombre de règles flexibles (plutôt que des règles statiques) en conjonction avec un modèle de notation des anomalies pour améliorer la précision et la visibilité des attaques.

Puis, en 2017, Akamai a introduit les groupes d'attaques automatisés, qui ont éliminé le besoin pour les organisations de configurer et de mettre à jour continuellement les règles avec les protections gérées par Akamai. Les groupes d'attaques automatisés ont été une révolution, rapidement activés dans des milliers de stratégies WAF actives des clients d'Akamai pour tirer parti de cette nouvelle approche.

Akamai a continué à faire évoluer son approche de la sécurité des applications, en donnant la priorité à la protection combinée des applications et des API, y compris les capacités de défense contre les bots, avec le lancement d'App & API Protector en 2021. Cette solution WAAP visait à remplacer le WAF Kona Site Defender pour les organisations et les entreprises mondiales en pleine croissance. App & API Protector a modifié la façon dont Akamai a abordé les opérations de sécurité en modernisant la technologie Kona Rule Set dans Adaptive Security Engine.

Moderniser les défenses contre les attaques DDoS au niveau des applications au-delà de la limitation du débit

En matière de DDoS, la limitation du débit est un outil éprouvé et efficace. Cependant, l'augmentation des attaques DDoS sophistiquées de couche 7, des attaques multivectorielles et de l'exploitation des API a laissé les défenses DDoS traditionnelles en difficulté. Les défenses statiques, qui reposent sur des seuils fixes et des signatures prédéfinies, sont réactives et sujettes aux faux positifs, d'autant plus que les pirates informatiques mélangent de plus en plus le trafic malveillant avec des requêtes légitimes. C'est là qu'Akamai a changé l'approche de la défense DDoS et introduit de nouvelles innovations telles que la protection des URL et le moteur Behavioral DDoS Engine.

Le moteur Behavioral DDoS Engine est un ajout de pointe à Akamai App & API Protector, rejoignant Adaptive Security Engine comme l'une de ses technologies de base. Ensemble, ces moteurs offrent une protection sans précédent contre les menaces actuelles, faisant d'Akamai un leader des solutions WAAP. Cette approche à double moteur distingue Akamai en fournissant des mises à jour automatisées, des fonctionnalités de réglage automatique et une détection contextuelle pour une expérience sans intervention.

Une solution unique pour une protection complète

Aujourd'hui, le changement continue de redéfinir la sécurité des applications avec les pratiques de développement de pointe via l'Edge Computing sans serveur, les architectures basées sur les microservices, les applications monopages et les approches SaaS/IaaS/PaaS/FaaS qui façonnent la sécurité des applications.

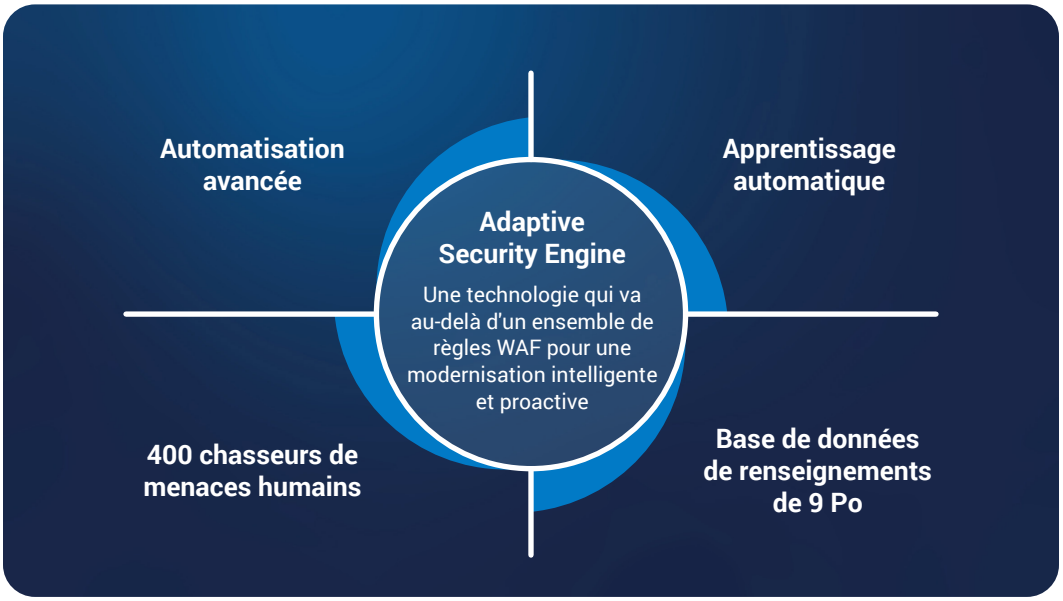
Pour protéger les applications et API d'aujourd'hui dans des environnements informatiques complexes, Akamai a repensé l'architecture de sa technologie de sécurité des applications en adoptant une approche plus adaptative, flexible et complète. Lorsque la solution WAAP d'Akamai est passée de Web Application Protector et Kona Site Defender à App & API Protector, de nouvelles fonctionnalités de sécurité et de nouveaux outils ont été intégrés.

App & API Protector offre désormais de nombreuses améliorations supplémentaires en matière de sécurité, toutes visibles et contrôlables via une interface unique. Ce que combine la solution WAAP d'Akamai :

1. Adaptive Security Engine
2. La sécurité des applications avec des contrôles granulaires
3. La défense DDoS, y compris la protection DDoS avancée de couche 7
4. La protection des API, y compris les fonctionnalités de découverte et de protection des informations personnelles identifiables
5. La visibilité des bots et les capacités d'atténuation
6. Une plateforme pour l'échelle mondiale, la veille sur les menaces et la résilience

Adaptive Security Engine

Adaptive Security Engine offre une protection de nouvelle génération à l'intersection de l'apprentissage automatique (AA), de la veille en matière de sécurité en temps réel, des experts en cybersécurité et de l'automatisation avancée. En tant que technologie de base d'Akamai pour la détection et la défense, Adaptive Security Engine permet une approche sans intervention pour protéger l'ensemble des applications Web et des API. Il s'ajoute également aux avancées d'Akamai, du WAF au WAAP, qui intègrent des solutions de sécurité corrélées, notamment un gestionnaire de bots, une protection DDoS, des intégrations DevOps, etc.



Le moteur Adaptive Security Engine 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. Il utilise les mêmes informations et renseignements sur la plateforme pour réduire les faux positifs grâce à des recommandations de réglage. Cette fonctionnalité de réglage automatique offre une facilité d'utilisation aux équipes de sécurité et de développement en fournissant des protections adaptatives contre les menaces sous forme de mises à jour proactives.

Détection adaptative des menaces

Le moteur utilise un modèle multidimensionnel de notation des menaces qui combine les informations de plateforme avec les données/métadonnées de chaque requête. Ces données sont traitées selon une logique décisionnelle afin d'identifier avec précision les véritables attaques.

La détection adaptative est particulièrement efficace pour identifier les attaques très ciblées, évasives et furtives, car les attaquants habiles investissent plus de temps et d'efforts dans leur approche. Alors que les attaquants recherchent les vulnérabilités et les erreurs de configuration, Adaptive Security Engine collecte et met en corrélation les preuves de leurs tactiques afin de rendre leurs empreintes historiques plus identifiables.

En plus de la charge utile réelle de l'attaque et de l'endroit où elle se situe dans la requête, les éléments d'attaques suivants sont évalués pour chaque client :

- Un historique de reconnaissance et/ou d'attaques (par exemple, fréquence, ampleur, gravité)
- Tout signe d'automatisation malveillante et d'outils d'attaque
- Corrélation avec les sources connues de trafic d'attaque

De plus, Adaptive Security Engine est amélioré grâce à deux technologies propriétaires : Smart Detect, qui indexe l'entrée sous forme d'empreinte digitale pour une détection très précise, et Smart Sniff, qui détecte le type de contenu approprié du corps de la requête pour empêcher la manipulation et le contournement du contenu. L'équipe de recherche sur les menaces d'Akamai exploite l'infrastructure et les systèmes étendus d'Akamai pour exécuter passivement de nouvelles détections sur tout le trafic de production, puis analyser ces résultats à l'aide de modèles d'apprentissage automatique.

Mises à jour automatiques

De nombreuses organisations ne disposent pas aujourd'hui des ressources ou de l'expertise en matière de sécurité nécessaires pour suivre en permanence l'évolution des menaces, mettre à jour les configurations et tester à nouveau leur trafic Web afin d'optimiser leurs stratégies. En guise de réponse, Akamai met continuellement à jour Adaptive Security Engine en utilisant un cadre de test automatique IA/AA pour tenir compte des menaces changeantes, tout en assurant une grande précision. Ces mises à jour ont souvent permis de se protéger contre les attaques de type « zero day » avant même qu'elles ne soient annoncées.

Cadre de test pour garantir l'exactitude

Le test d'une solution WAAP repose sur un principe simple : tester différents vecteurs d'attaque et arrêter les attaques Web. Cependant, les facteurs suivants doivent être pris en compte :

- Les environnements réels sont plus complexes que les environnements de test et conduisent souvent à des faux positifs et des faux négatifs.
- La conception d'un cadre de test axé sur la précision nécessite une vérification supplémentaire (non seulement la détection des attaques, mais aussi le fait de le faire sans déclencher par inadvertance de faux positifs ou de faux négatifs).
- Les tests nécessitent l'utilisation d'un trafic Web réel, à la fois légitime et d'un trafic d'attaque.

Les mises à jour d'Adaptive Security Engine se composent de plusieurs étapes pour garantir que le trafic légitime n'est pas affecté de manière négative :

- Toutes les détections sont testées en laboratoire à l'aide d'un trafic synthétique afin de s'assurer qu'elles détectent correctement les attaques sans introduire de faux positifs.
- Les mises à jour sont ensuite testées sur le trafic de production réel afin de s'assurer que l'échantillon est valide pour le trafic actuel de la plateforme. Ce processus implique l'exécution de la mise à jour en mode fantôme sur le trafic réel des clients. L'exécution en mode fantôme garantit l'absence d'impact sur le trafic des clients, tout en continuant à tester la précision de la détection.
- Une fois qu'une mise à jour a passé la deuxième étape, l'apprentissage automatique identifie les modèles ou les déclencheurs que l'analyse humaine aurait pu manquer, après quoi l'équipe de recherche sur les menaces examine manuellement les résultats.
- Ce n'est que lorsque ces vérifications sont passées à chaque phase qu'un changement peut passer à la phase suivante et être déployé sur un segment plus large du réseau. Après un déploiement total, les fonctionnalités de réglage automatique élimineront tout faux positif restant, propre aux modèles de trafic des clients.

Réglage automatique

Le réglage automatique allège la charge du réglage manuel, qui peut conduire à des stratégies obsolètes et à des erreurs humaines, pour une expérience quasi automatique. Adaptive Security Engine applique l'apprentissage automatique, des modèles statistiques et des méthodes heuristiques à tous les déclencheurs de chaque règle de sécurité afin de différencier avec précision les attaques réelles du trafic des utilisateurs finaux identifié à tort comme des attaques. Il ne s'agit pas d'un contrôle générique à l'échelle de la plateforme qui n'est appliqué que lors de l'intégration, mais plutôt d'un processus d'ajustement continu effectué 24 h/24, 7 j/7, 365 jours par an, sans configuration ni intervention de l'utilisateur final.

Le réglage automatique est fluide et simple. Les administrateurs de sécurité peuvent facilement examiner et accepter les recommandations en un seul clic via l'interface utilisateur, ou ils peuvent automatiser le processus en utilisant les API AppSec, l'interface de ligne de commande (CLI) ou Terraform. Pour plus de transparence, un lien préfiltré vers Web Security Analytics affiche toutes les requêtes considérées comme de faux positifs, avec une justification fournie pour chaque recommandation d'ajustement.

Flexibilité de configuration et d'automatisation

Lorsqu'un fournisseur de solutions WAAP dépasse la technologie traditionnelle des ensembles de règles, la configuration et l'automatisation deviennent plus flexibles. Adaptive Security Engine offre les possibilités suivantes :

- Disposer de différents types de mises à jour WAF (automatiques ou manuelles) pour différentes applications et leur appétence au risque associée
- Contrôler l'action par groupe d'attaque et règle contributive nécessaire à la personnalisation si le comportement de l'application/du trafic n'est pas standard
- Configurer des conditions simples et complexes pour différentes caractéristiques de demande, telles que l'adresse IP, la zone géographique, l'en-tête, la charge utile, etc.
- Atténuer de manière proactive les sources de menaces qui ont été détectées en effectuant une analyse/attaque WAF suspecte pour vos propres applications, avec une « mise sur la touche »
- Modifier l'en-tête de débogage
- Modifier la taille d'inspection de la charge utile de la requête ou les paramètres de journalisation de la charge utile de l'attaque
- Exécuter des simulations de changement dans la logique de détection pour appliquer en toute confiance ces changements en production

Vérification dans le monde réel

Le mode d'évaluation offre aux clients d'Akamai la flexibilité et la granularité nécessaires pour configurer des versions spécifiques d'Adaptive Security Engine et tester les mises à jour ou les nouvelles règles/stratégies. Les clients peuvent voir les nouvelles mises à jour ou modifications avant de choisir de les activer en fonction de leur environnement d'application Web spécifique. Pour une modernisation efficace de la sécurité, Akamai estime que les tests sur le trafic en temps réel améliorent les résultats de sécurité par rapport aux tests sur le trafic passé. Le mode d'évaluation s'apparente à l'application d'une règle fantôme où vous pouvez voir les résultats en temps réel comme si la règle était appliquée, mais sans que cela n'ait d'incidence sur les utilisateurs finaux actuels. Les organisations peuvent opter pour ce mode de fonctionnement manuel/d'évaluation afin de minimiser l'impact inattendu sur les faux positifs et les faux négatifs.

Intégration de protections modernisées

Les équipes de sécurité et DevOps peuvent également mettre en œuvre la sécurité en intégrant des appels aux API d'Akamai à l'aide de l'interface de ligne de commande, d'Akamai Terraform ou des scripts dans leur pipeline d'automatisation CI/CD. La flexibilité de la configuration et de l'automatisation garantit une sécurité performante qui n'entrave jamais la vitesse de développement. Ces intégrations peuvent :

- permettre une intégration rapide des applications ;
- assurer une gestion uniforme des règles de sécurité sur de grands portefeuilles d'applications ;
- centraliser l'application de la sécurité dans les infrastructures hybrides et multicloud ;
- améliorer la collaboration entre les équipes DevOps et de sécurité dans un flux de travail GitOps pour une couverture optimale.

De plus, la gestion des informations et des événements de sécurité (SIEM) vous permet de collecter les événements de sécurité qui se produisent sur la plateforme Akamai. À son tour, notre solution d'intégration SIEM permet de transmettre les événements SIEM à des outils d'analyse SIEM sur site et dans le cloud, tels que Splunk et QRadar afin que vous puissiez intégrer les événements de sécurité Akamai à votre infrastructure globale d'événements et de sécurité en quatre étapes de base.

Vous pouvez protéger et contrôler votre flux de données grâce aux fonctionnalités suivantes :

- **Filtrage des événements**
  Utilisez la configuration et la règle de sécurité pour vous concentrer sur les menaces réelles.
- **Conservation des données**
  Le collecteur stocke les données pendant 12 heures afin que vous puissiez enregistrer les événements manqués.
- **Protection contre les surcharges SIEM**
  Dans votre connecteur SIEM, vous pouvez définir le nombre maximal d'événements de sécurité récupérés dans chaque requête. Cela vous permet d'éviter de surcharger l'application SIEM.
- **Intervalle de récupération**
  Vous pouvez définir la fréquence à laquelle les connecteurs SIEM appellent l'API SIEM pour récupérer les données d'événements de sécurité.

Sécurité des applications et défense contre les attaques DDoS

La sécurité des applications est un aspect crucial de la cybersécurité d'aujourd'hui, car elle garantit que les applications restent résistantes à un large éventail de menaces et de vulnérabilités. Son importance réside dans plusieurs domaines clés. L'intégrité et la confidentialité des données sont primordiales, car la sécurité des applications garantit que les données sensibles sont protégées contre tout accès non autorisé et toute falsification. Elle joue également un rôle essentiel dans la continuité des activités en protégeant les applications contre les perturbations causées par des incidents de sécurité, garantissant ainsi une disponibilité constante des services. De plus, la sécurité des applications est essentielle pour la gestion de la réputation, car elle empêche les violations susceptibles de nuire à la réputation d'une organisation et d'ébranler la confiance des clients. Enfin, elle aide les organisations à se conformer aux exigences réglementaires, évitant ainsi les sanctions juridiques et financières.

Sur le plan fonctionnel, une solution WAAP filtre et surveille le trafic HTTP entre les applications Web et Internet. Cela assure une protection contre les attaques Web courantes telles que les attaques XSS, les injections SQL et les attaques DDoS.

App & API Protector est reconnu pour sa protection DDoS leader sur le marché, conçue pour contrer les attaques volumétriques visant à submerger les ressources. La solution permet de lutter contre les attaques DDoS des manières suivantes :

- **Protection contre les attaques DDoS en bordure de l'Internet**
  En tirant parti de la plateforme périphérique d'Akamai, distribuée à l'échelle mondiale, App & API Protector peut instantanément bloquer les attaques DDoS avant qu'elles n'atteignent l'origine de l'application. Cette approche en bordure de l'Internet garantit une latence minimale et une protection maximale sans affecter les performances de l'application.
- **Limitation du débit**
  App & API Protector inclut une limitation adaptative du débit pour se défendre contre les attaques DDoS distribuées au niveau de la couche applicative. Ces contrôles peuvent être configurés pour limiter le débit des requêtes entrantes en fonction de divers critères, notamment l'IP, la géolocalisation, les contrôles de réputation IP, divers en-têtes HTTP et les conditions de correspondance.
- **Protection des URL avec délestage de charge intelligent**
  Adopte une approche différente de la limitation du débit. Avec la protection des URL, vous pouvez protéger votre origine contre les demandes excessives en fonction du débit de demande acceptable (RPS maximum) selon la capacité d'origine. Elle est spécialement conçue pour protéger les URL à forte charge de calcul, les points de terminaison API, etc. contre les attaques DDoS de la couche applicative hautement distribuées.

- **Behavioral DDoS Engine**
  Nouveau dans App & API Protector, Behavioral DDoS Engine est un outil puissant pour une stratégie de défense en profondeur. Il introduit une approche à distance de la gestion et de la mitigation des événements DDoS en utilisant l'IA pour établir des références de trafic et identifier les anomalies par rapport aux normes. Le moteur fonctionne en comprenant les changements de modèles de trafic et permet aux utilisateurs de définir la façon dont le système réagit aux différentes anomalies sans fixer de seuils explicites, ce qui réduit la charge opérationnelle de gestion et de réglage du système.

- **Mises à jour automatiques et réglage automatique adaptatif**
  Grâce à la stratégie à deux moteurs d'Akamai, Adaptive Security Engine et Behavioral DDoS Engine, App & API Protector s'adapte en permanence aux nouvelles menaces par le biais de mises à jour automatiques et d'un réglage automatique basé sur l'apprentissage automatique afin de réduire la charge opérationnelle.

Behavioral DDoS Engine : fonctionnement

Au cœur de Behavioral DDoS Engine se trouve un modèle avancé d'apprentissage automatique qui surveille en permanence le trafic en temps réel, établissant des références pour un comportement normal et détectant instantanément les écarts qui indiquent une attaque. En analysant les modèles de trafic à travers de multiples dimensions dynamiques (telles que le pays d'origine, les modèles TLS, l'IP et les empreintes TLS) ce moteur peut rapidement identifier les anomalies et prendre des mesures.

Voici certains composants principaux de Behavioral DDoS Engine :

- **Surveillance du comportement en temps réel**
  Le moteur analyse en permanence le trafic pour établir des références d'activité normale et détecter instantanément les écarts qui signalent des attaques DDoS potentielles.

- **Apprentissage automatique pour plus de précision**
  Les modèles d'apprentissage automatique avancés renforcent la capacité du moteur à identifier les anomalies subtiles dans les modèles de trafic, garantissant une atténuation précise sans bloquer les utilisateurs légitimes.

- **Atténuation proactive**
  En exploitant les informations du réseau mondial d'Akamai (1 056 To de trafic par jour), le moteur prédit et neutralise les attaques, souvent avant qu'elles n'aient une incidence sur les entreprises.

- **Analyse multidimensionnelle**
  Le trafic est évalué sur plusieurs aspects, notamment l'adresse IP, le pays et les modèles TLS, offrant ainsi une protection robuste adaptée aux besoins de chaque application

Architecture avancée pour une meilleure défense
Behavioral DDoS Engine fonctionne grâce à une architecture sophistiquée qui comprend plusieurs composants essentiels :

- **Moteur de détection**
  Utilise des dimensions dynamiques et des données historiques sur les attaques pour identifier les attaques DDoS en temps réel.
- **Moteur d'atténuation**
  Contre automatiquement les attaques en utilisant les renseignements du générateur de référence et les signaux de menace, réduisant ainsi les frais généraux opérationnels pour les équipes de sécurité.
- **Réduction du bruit/des faux positifs**
  Les modèles d'apprentissage machine filtrent les données non pertinentes, garantissant que le trafic propre est utilisé pour l'analyse et l'atténuation.
- **Générateur de référence**
  Il affine en permanence les profils de trafic en traitant les données nettoyées sur une période de deux semaines, ce qui permet au moteur de rester à jour avec les stratégies d'attaque les plus récentes.
- **Validateur de référence**
  Grâce à l'IA, ce composant crucial évalue des centaines d'attaques DDoS chaque mois pour affiner la solution.

Ce cadre automatisé garantit que les équipes de sécurité peuvent compter sur le moteur pour ajuster dynamiquement les défenses sans intervention manuelle. La solution détecte les activités anormales du trafic, telles que le trafic généré par des bots ou les tentatives DDoS, et les filtres pour protéger efficacement les applications.

Précision de la sécurité des applications

Une solution de sécurité applicative (WAF ou WAAP) qui n'est pas précise nécessite davantage de ressources internes pour gérer le nombre croissant d'alertes quotidiennes. L'inexactitude peut entraîner un grand nombre de faux positifs (une requête est signalée comme malveillante alors qu'elle ne l'est pas) et de faux négatifs (une requête est signalée comme non malveillante alors qu'elle l'est), ce qui entraîne une perte de compétences et de temps précieux en matière de sécurité pour la recherche et l'analyse de ces types d'alertes.

Les organisations sont souvent confrontées aux alertes incessantes, mais restent sans solution en raison de contrôles trop larges ou de capacités qui corrigent trop ou trop peu. Cela conduit souvent l'organisation à mettre son WAF hors ligne ou pire, à ignorer les alertes et les mises à jour de version. Si cette solution permet d'apaiser les inquiétudes des organisations concernant le blocage accidentel d'utilisateurs légitimes, elle réduit aussi considérablement la protection contre les attaques Web et d'API. De nombreuses organisations manquent également de granularité des contrôles pour équilibrer avec précision l'accès au trafic légitime et le blocage du trafic malveillant.

L'avantage d'une solution WAAP efficace est qu'elle réduit à la fois les faux positifs et les faux négatifs pour augmenter la précision et minimiser l'impact sur les utilisateurs légitimes grâce à un ensemble complet de contrôles et de capacités WAAP.

Comprendre la précision

La précision mesure la capacité d'un WAF ou WAAP à bloquer simultanément les attaques sans bloquer par inadvertance les utilisateurs légitimes. Elle prend en compte quatre variables :

- **Vrais positifs (TP) :** attaques réelles correctement identifiées comme malveillantes
- **Faux positifs (FP) :** demandes légitimes identifiées à tort comme malveillantes
- **Vrais négatifs (TN) :** demandes légitimes transmises à l'application
- **Faux négatifs (FN) :** attaques réelles transmises de manière inappropriée à l'application

Scores de réputation du client

La réputation du client utilise un moteur d'analyse des risques sophistiqué pour calculer un ensemble de « scores de risque » pour chaque adresse IP qui tente d'accéder à votre site. Il analyse les adresses IP entrantes et utilise divers facteurs tels que la persistance de l'attaquant, le nombre d'applications ciblées, la gravité de l'attaque, l'ampleur, le secteur d'activité et les attaques précédentes visant les applications d'un client pour déterminer un score qui spécifie la probabilité que cette adresse IP se livre à une attaque Web, notamment les suivantes :

- **DOSATCK**
  Utilise des botnets pour lancer des attaques par déni de service (DoS). L'objectif d'une attaque DoS est d'inonder un site de demandes frauduleuses, jusqu'à le rendre insupportablement lent, voire le faire planter. Dans une attaque par déni de service distribué (DDoS), ces requêtes proviennent de milliers d'endroits (généralement des ordinateurs ou des téléphones infectés par des logiciels malveillants), ce qui rend impossible l'arrêt de l'attaque par le simple blocage d'une adresse IP donnée.

- **SCANTL**
  Les outils d'analyse peuvent identifier les risques potentiels pour la sécurité tels que l'injection SQL, la falsification de requête intersite (CSRF), les redirections non valides et d'autres vulnérabilités. Il est judicieux d'exécuter un outil d'analyse Web sur votre propre site. Il est moins judicieux de demander à un malfaiteur d'utiliser un outil d'analyse sur votre site Web.

- **WEBATCK**
  Utilise des techniques telles que l'injection SQL, l'inclusion de fichiers à distance ou les attaques de type cross-site scripting pour installer des logiciels malveillants ou voler des données utilisateur. Un attaquant peut être en mesure de récupérer toutes vos données utilisateur, y compris les mots de passe, les numéros de carte de crédit, les numéros de sécurité sociale et toute autre information que vous auriez pu stocker dans la base de données utilisateur.

- **WEBSCRP**
  Utilise des outils automatisés pour télécharger une copie d'une page Web, puis « extraire » (c'est-à-dire copier) tout le contenu de cette page. Le contenu peut être réutilisé à des fins illégales ou contraires à l'éthique.

Avec la réputation du client, vous pouvez protéger votre organisation de manière proactive contre les sources de menaces suspectes grâce aux renseignements cumulatifs sur les menaces fournis par Akamai Connected Cloud.

Protection contre les logiciels malveillants

Les acteurs malveillants utilisent couramment les logiciels malveillants. Pour une protection complète des applications, Akamai propose une solution de protection contre les logiciels malveillants. Les organisations de toutes tailles autorisent le téléchargement de fichiers pour des raisons d'efficacité interne et externe, notamment pour les usages courants suivants :

- CV pour les candidatures à des emplois
- Contrats de travail, intégration, vérification électronique, configuration de dépôt direct, etc.
- Demandes, y compris les prêts, la configuration de compte et les demandes de crédit
- Estimations d'assurance ou de réparation pour les voitures, les maisons, etc.
- Dossiers médicaux pour l'assurance ou la configuration de compte patient
- Avis de clients sur les produits ou les expériences, y compris les images

La protection contre les logiciels malveillants dans la sécurité des applications et des API détecte et isole les menaces de logiciels malveillants en bordure de l'Internet avant qu'elles n'atteignent le système d'entreprise cible. Les organisations peuvent protéger leur temps, leur budget et leur productivité, ainsi que les données internes et celles de leurs clients, grâce aux avantages de la protection contre les logiciels malveillants pour les applications et les API :

- **Détecter et bloquer les logiciels malveillants en bordure de l'Internet**
  Évitez les risques liés à l'analyse sur les serveurs, au cours de laquelle le logiciel malveillant aurait déjà pu se propager.
- **Éviter la complexité et libérer du temps**
  Analysez les fichiers une seule fois au lieu de configurer individuellement la protection dans chaque système, comme vous le faites avec les analyses ICAP et basées sur un agent.
- **Positionner la stratégie de sécurité pour favoriser la croissance**
  En choisissant une approche préventive et en couches, les organisations peuvent adapter leur protection à la croissance de l'activité, en fournissant une protection supplémentaire en bordure de l'Internet et la possibilité d'effectuer une nouvelle analyse au point d'origine.
- **Assurer la cohérence de vos applications**
  Les entreprises n'ont pas besoin de configurer ou de modifier le code d'application. La protection contre les logiciels malveillants est entièrement hébergée sur Akamai Connected Cloud.

Analyse de la sécurité des applications

App & API Protector comprend le produit Akamai le plus apprécié (et le plus utilisé) : Web Security Analytics. Cette solution WAAP d'Akamai vous permet d'enregistrer les événements de sécurité qui se produisent sur votre application Web et vos API sur la plateforme Akamai et de les visualiser dans les outils d'analyse de sécurité fournis.

Web Security Analytics est un composant essentiel de la cybersécurité d'aujourd'hui, offrant un aperçu complet du trafic Web et des menaces potentielles. En analysant un large éventail de points de données, y compris les modèles de trafic, le comportement des utilisateurs et les événements de sécurité, il fournit une visibilité détaillée de la stratégie de sécurité des applications Web. Cette approche proactive permet aux organisations de détecter les menaces et d'y répondre plus efficacement, en atténuant les risques avant qu'ils ne puissent causer des dommages importants. Web Security Analytics permet non seulement d'identifier les activités malveillantes, telles que les attaques de bots, les injections SQL et les attaques de type cross-site scripting, mais aussi de comprendre et de corriger les vulnérabilités au sein des applications Web. De plus, il soutient les efforts de conformité en générant des rapports qui démontrent le respect des règles de sécurité et des exigences réglementaires.

Détection et profilage automatiques des API

Les API permettent aux organisations de créer des expériences Web et mobiles puissantes, souvent en exposant des données et une logique back-end pour développer des offres nouvelles et innovantes. Les API élargissent également la surface d'attaque. Les organisations doivent savoir quels points de terminaison API se trouvent dans leur environnement, quelles sont les fonctions de l'API et quels sont leurs profils de trafic. La fonctionnalité de détection et de profilage des API d'Akamai fait tout cela, et bien plus encore, automatiquement et en continu.

La fonctionnalité de découverte des API alerte les équipes de sécurité de la présence d'applications et d'API nouvelles, souvent non protégées, connectées par différents secteurs d'activité dans une entreprise au sein d'une organisation. Cette technologie de détection automatisée est une nouvelle fonctionnalité de la solution WAAP d'Akamai qui permet d'assurer la cohérence entre les équipes de développement, les responsables des secteurs d'activité et les équipes de sécurité.

Adaptive Security Engine décèle automatiquement des API toutes les 24 heures sur la base d'un mécanisme de notation qui prend en compte le type de contenu de réponse, les caractéristiques de chemin et les modèles de trafic. Les données de découverte comprennent des informations sur les spécifications des API observées, avec les détails suivants :

- Nom d'hôte
- Chemin de base
- Chemin de ressource
- Paramètres et leur type de données
- Méthodes
- Format de l'API

Les chemins de base et de ressource sont déterminés sur la base d'un algorithme qui prend en compte la profondeur du chemin, le nombre d'enfants et les frères et sœurs du trafic observé sur un nom d'hôte spécifique avec le trafic d'API. Dans le chemin de ressource, si un paramètre est observé pour une méthode spécifique, il est marqué et le type de données de ce paramètre est identifié.

Le profil de trafic des points de terminaison API contient des informations qui donnent un aperçu de l'objectif de l'API et du niveau de menace actuel. Voici quelques-uns des points de données inclus :

- Nombre total de requêtes depuis la découverte de l'API, à la fois au cours des dernières 24 heures et au fil du temps
- Date à laquelle l'API a été découverte pour la première fois et vue pour la dernière fois
- Nombre de requêtes pour différentes méthodes, telles que GET, PUT, POST, DELETE et OPTIONS
- Nombre de requêtes générant des réponses 2xx, 3xx, 4xx et 5xx
- Identification du client final basée sur l'agent utilisateur
- Erreurs de réponse telles que le pourcentage de trafic entraînant des erreurs côté client et côté serveur
- Les attaques provenant d'acteurs hostiles connus, y compris le pourcentage du trafic total provenant d'acteurs malveillants connus vers la plateforme Akamai, réparties par attaquants Web, outils d'analyse Web, extracteurs Web et attaquants DoS

La protection des API peut constituer un obstacle important sans visibilité. Comment une entreprise peut-elle protéger ce qu'elle ne voit pas ? Avec Akamai, les entreprises peuvent découvrir et profiler automatiquement et en continu les API, y compris leurs points de terminaison, leurs définitions et les caractéristiques de leurs ressources et de leur trafic. Une fois les API identifiées, Akamai fournit une protection étendue pour gérer les attaques DoS, les injections malveillantes, les attaques par vol d'identifiants et les violations des spécifications API. L'approche indépendante du cloud et de l'origine d'Akamai permet une détection aisée des API sur l'ensemble des applications, sans configuration supplémentaire pour l'utilisateur final. Cette visibilité permet aux développeurs, aux propriétaires d'applications et aux équipes de sécurité de garder une longueur d'avance sur les API nouvelles, inconnues ou en évolution, et de les enregistrer facilement pour les protéger.

Visibilité et atténuation des bots

Étant donné que les bots contribuent à plus de la moitié du trafic des sites Web, il peut être difficile de savoir lesquels aident votre organisation à atteindre ses objectifs et lesquels ont l'intention de lui nuire. Les bots légitimes créent des gains d'efficacité dans l'organisation en automatisant les évaluations, les conversations ou les recommandations. Les bots malveillants peuvent bloquer les chemins de trafic et avoir un impact sur l'expérience client et opérationnelle, ce qui a un impact négatif sur les revenus. Dans App & API Protector, la visibilité et l'atténuation des bots permettent de détecter efficacement les bots légitimes et de les laisser passer, tout en bloquant les bots malveillants. Cela permet aux organisations d'effectuer les actions suivantes :

- **Observer les bots et comprendre leur impact**
  La visibilité du trafic des bots est essentielle pour les entreprises digitales d'aujourd'hui, étant donnée l'utilisation omniprésente des bots pour des opérations telles que la recherche, la vérification des performances du site et l'interaction avec les partenaires commerciaux.
- **Améliorer le contrôle opérationnel**
  Le blocage des bots malveillants permet d'améliorer l'efficacité, de réduire les risques commerciaux et financiers et de mieux contrôler les dépenses informatiques.
- **Prendre des décisions plus rationnelles et éclairées**
  Des analyses et des rapports détaillés permettent de faire des choix créatifs et efficaces en ce qui concerne les parcours clients, la stratégie de sécurité, la tolérance au risque et les opérations informatiques.

Visibilité et atténuation des bots intrinsèques à App & API Protector

App & API Protector offre des détections de bots et des contrôles du trafic de bots qui peuvent avoir un impact négatif sur les performances et la sécurité des propriétés Web. Il offre une visibilité précoce pour surveiller de manière proactive les anomalies et les menaces liées aux bots qui se développent au fil du temps.

Utilisation de la solution de bots d'Akamai fournie dans App & API Protector :

- Accédez à plus de 1 700 bots définis connus d'Akamai
- Bénéficiez d'une visibilité en temps réel sur le trafic des bots
- Créez des définitions de bots personnalisées
- Autorisez les bots légitimes et refusez les bots malveillants
- Consultez les rapports de visibilité et de tendances des bots

Pour les sites confrontés à des problèmes de bots avancés, Akamai propose Bot Manager, qui inclut des protections avancées contre les bots pour une sécurité accrue du commerce électronique et du digital. Bot Manager fournit des actions plus nuancées pour les bots persistants et conflictuels comme ceux utilisés pour les attaques telles que les suivantes :

- Credential stuffing
- Accaparement de stocks
- Extraction de contenus et extraction de tarifs
- Abus de logique métier

Principales capacités du bot

Akamai reconnaît l'évolution des besoins en matière de gestion des bots via WAAP et a amélioré ses outils de visibilité et d'atténuation des bots pour inclure de nouvelles fonctionnalités telles que les suivantes :

- **Détection de l'usurpation d'identité des navigateurs**
  Cette fonctionnalité d'Akamai Bot Manager, très appréciée des clients, utilise des modèles de notation dynamiques et l'apprentissage automatique pour discerner et contrer les activités des bots dans le navigateur, et est incluse dans App & API Protector.
- **Actions de réponse conditionnelles**
  Les clients ont désormais une meilleure compréhension des activités des bots dans le navigateur et peuvent réagir par des actions conditionnelles pour appliquer différentes stratégies de réponse contre les bots malveillants.
- **Actions de défi**
  Traitez les bots à l'aide d'une série d'actions de défi différentes, y compris des défis interstitiels qui, lorsqu'ils ne sont pas résolus, permettent de bloquer l'accès au contenu.

Plus qu'un simple WAF : avantages de la solution Akamai

L'approche d'Akamai en matière de WAAP a abouti à la solution App & API Protector. Les avantages dont bénéficient nos clients WAAP ne se limitent pas à un seul produit. Construit sur la plateforme mondiale la plus distribuée et alimentée par des centaines d'experts en menaces humaines, Akamai Connected Cloud offre des performances, une disponibilité, une intelligence, une expertise et des résultats de sécurité efficaces.

Renseignements sur les menaces et détection des menaces

Le fait de disposer d'une capacité interne solide en matière de renseignements sur les menaces améliore la capacité d'un fournisseur de WAAP à répondre aux menaces en développement. Cependant, la qualité, la rapidité et la capacité d'action des renseignements fournis détermineront l'impact sur l'efficacité de la sécurité des applications. Akamai analyse en permanence les données disponibles via Akamai Connected Cloud afin d'identifier les tendances actuelles dans l'écosystème des menaces, les nouveaux vecteurs d'attaque dès leur apparition et les attaquants actuellement actifs. Akamai intègre ensuite ces renseignements dans notre solution WAAP de plusieurs manières.

La technologie Akamai Adaptive Security Engine, présentée plus haut dans ce document, combine deux niveaux de renseignements approfondis sur les menaces pour créer un moteur puissant et exclusif permettant de gérer automatiquement les dernières protections pour nos clients. Outre l'apprentissage automatique et l'adoption automatisée des règles, Adaptive Security Engine s'appuie sur les renseignements sur les menaces provenant de la plateforme mondiale d'Akamai et d'une importante équipe d'experts en recherche sur les menaces.

Intelligence de la plateforme Akamai

Le fait de disposer de l'une des plus grandes plateformes mondiales fournit à Akamai le mécanisme permettant d'analyser en temps utile le trafic d'attaque à l'échelle mondiale contre chaque client Akamai. Notre base de données de renseignements comprend en moyenne 1 056 To de données d'attaque chaque jour. Elle exploite la visibilité d'Akamai sur le trafic Web de milliers d'entreprises en ligne parmi les plus importantes, les plus fréquentées et les plus fréquemment attaquées pour acquérir des données pertinentes et de haute qualité à des fins d'analyse par l'équipe de recherche sur les menaces d'Akamai :

- **Déclencheurs WAP**
  Ils intègrent des données directement à partir des déploiements WAAP mondiaux d'Akamai, capturant les attaques réelles qui ciblent chaque client de sécurité d'Akamai.
- **Journaux de réseau de diffusion de contenu (CDN)**
  Ils intègrent l'analyse hors ligne effectuée sur les journaux d'événements de chaque client Akamai, y compris ceux qui n'ont pas déployé leur solution WAAP.

La base de données de renseignements d'Akamai abrite l'un des plus grands ensembles de données au monde (9 Po). Pour les organisations qui accordent la priorité à la sécurité de leurs activités et de leurs clients, les renseignements sur les menaces d'Akamai sont une référence pour les fournisseurs de solutions WAAP.

Recherche sur les menaces et réponse aux incidents

Les organisations de recherche sur les menaces et de réponse aux incidents fournissent des renseignements et des analyses humaines pour compléter et élargir la couverture des attaques d'une solution WAAP. Akamai emploie plusieurs équipes ayant des chartes différentes pour soutenir nos clients WAAP, ainsi que pour identifier de nouveaux vecteurs d'attaque qui peuvent nécessiter des protections supplémentaires.

Recherche sur les menaces

L'équipe de recherche sur les menaces d'Akamai effectue des analyses régulières des tendances des attaques Web sur l'ensemble de la clientèle d'Akamai, ainsi que des analyses personnalisées pour des clients individuels, selon les besoins. L'équipe conçoit et met également en œuvre des méthodes heuristiques pour rechercher des renseignements exploitables afin de soutenir la création et les mises à jour de la logique des règles WAF de base et de la réputation du client.

Intervention en cas d'incident

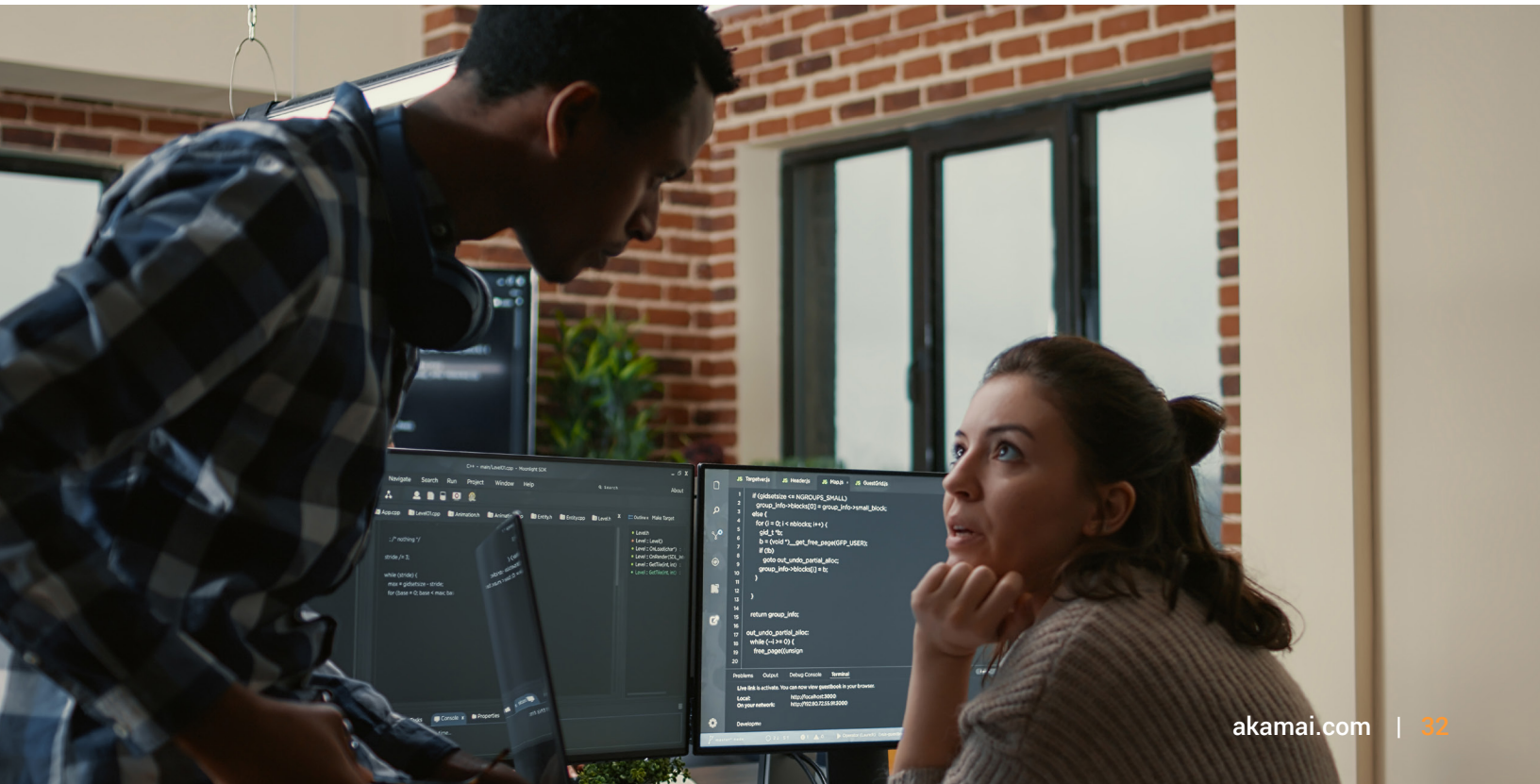
Akamai dispose de deux équipes d'intervention en cas d'incident : l'équipe d'intervention en cas d'incident de sécurité informatique (CSIRT) et l'équipe d'intervention en cas d'incident de sécurité (SIRT). Toutes deux travaillent avec le centre d'opérations de sécurité (SOC) mondial d'Akamai et fournissent des analyses et des réponses aux incidents pour les clients individuels lorsqu'ils subissent une attaque. De plus, la CSIRT surveille les clients d'Akamai fréquemment attaqués, représentant un large éventail de secteurs, en tant qu'indicateur avancé des nouveaux vecteurs ou des nouvelles tendances d'attaque.

Détection rapide des menaces

Nos nouvelles capacités permettent un déploiement rapide des protections contre les menaces émergentes et les CVE de premier plan. Les mises à jour automatiques et la possibilité d'actions « gérées par Akamai » vous permettent de gérer vos défenses avec agilité.

Protection contre les CVE

L'équipe de recherche sur les menaces d'Akamai continue de surveiller les vulnérabilités et expositions communes et veille à ce que la solution WAAP soit mise à jour pour protéger les applications des clients et fournir les confirmations nécessaires via l'outil de recherche CVE d'Akamai. Cet outil fournit des informations détaillées sur les CVE, y compris les niveaux de menace et des informations sur les protections actuelles d'Akamai. Le catalogue de protection contre les CVE d'Akamai vous offre une visibilité qui vous permet de hiérarchiser les mesures de sécurité en fonction des protections d'Akamai et vous permet d'effectuer des recherches dans la base de données des CVE afin de déterminer les mesures de protection actives d'Akamai contre une vulnérabilité, ainsi que d'évaluer le niveau de menace et d'accéder aux informations relatives aux CVE.



Plateforme en bordure de l'Internet distribuée mondialement

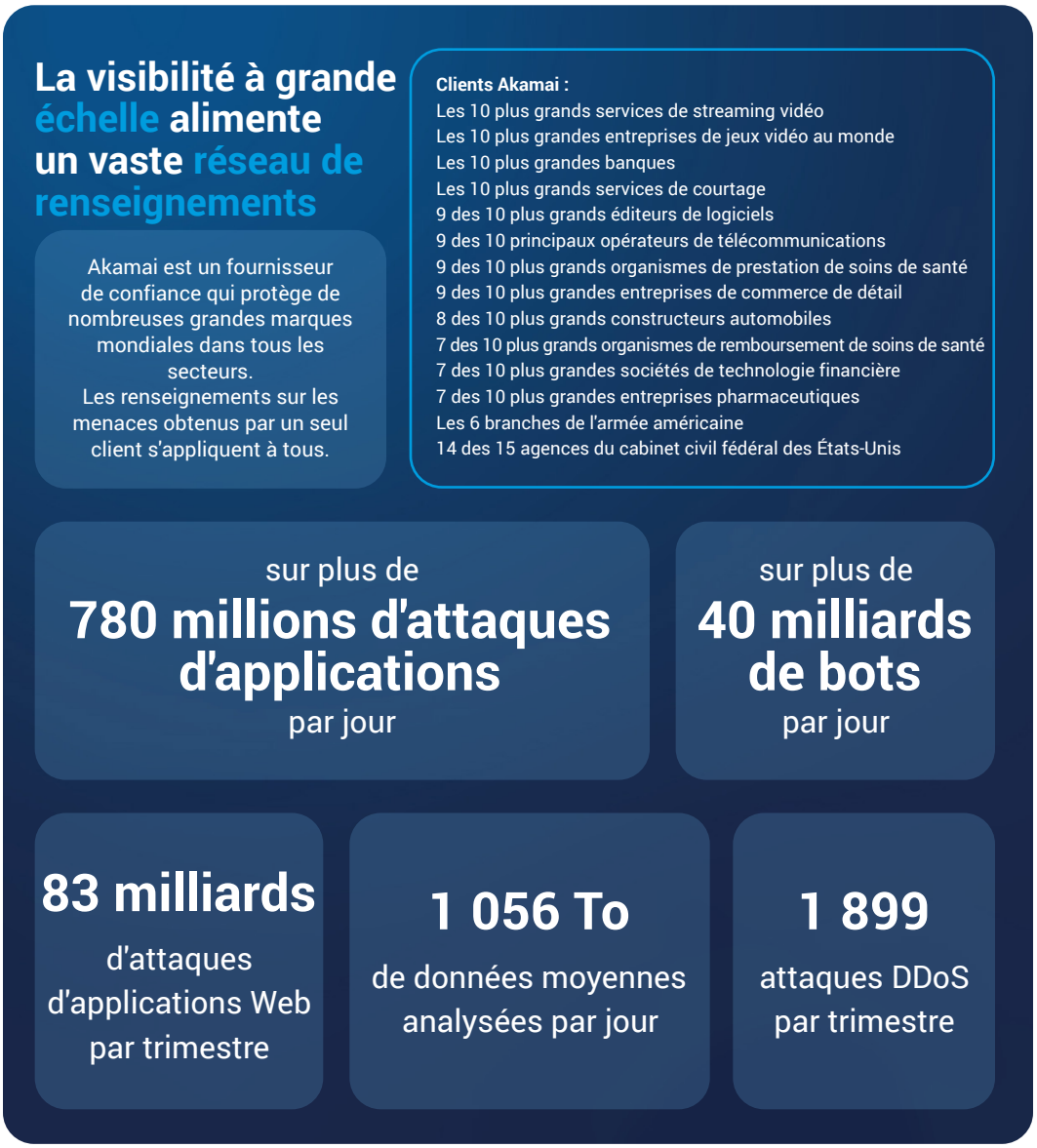
Fiabilité et résilience

Les solutions WAAP haut de gamme reposent sur des réseaux étendus et puissants qui ne limitent pas le bon trafic des clients, même lors des cyberattaques les plus importantes. La qualité, la capacité et l'aptitude d'exécution éprouvées de la plateforme mondiale d'un fournisseur WAAP devraient être tout aussi importantes que les fonctionnalités de la solution. Lorsqu'un fournisseur WAAP ne parvient pas à fournir un bon trafic lors d'une attaque active, les clients doivent évaluer s'ils ont investi dans une solution ou simplement dans un outil.

Akamai s'engage à fournir à ses clients des performances et une protection de pointe. Cette mission n'est possible qu'en construisant des services sur la base la plus solide : Akamai Connected Cloud. Akamai a construit la plateforme cloud la plus distribuée au monde, composée de plus de 4 200 points de présence en bordure de l'Internet dans plus de 130 pays.

Parmi les clients d'Akamai figurent les 10 plus grands courtiers, les 10 plus grandes banques, les 10 plus grands services de streaming vidéo et les 10 plus grandes entreprises de jeux vidéo. Notre clientèle s'étend de la plupart des plus grandes entreprises automobiles, des prestataires de soins de santé, des détaillants et des opérateurs de télécommunications à un nombre important d'agences gouvernementales et de forces armées.

Ces clients font confiance aux capacités d'Akamai pour les alimenter et les protéger contre les 40 milliards de bots par jour, les 780 millions d'attaques d'applications par jour et les 1 889 attaques DDoS par trimestre qui menacent de détruire leurs réseaux. Akamai assure la sécurité avec succès, car les renseignements sur les menaces obtenus par un client bénéficient à tous les clients et leur permettent de bénéficier de protections. L'envergure de la plateforme mondiale d'Akamai fournit à la fois la quantité et la qualité de données nécessaires pour sécuriser les organisations qui entrent dans l'ère de l'IA.



Déploiement à l'échelle mondiale

Pour un WAF, la question de l'échelle dépend à la fois de sa capacité à inspecter le volume requis de trafic Web, initialement et au fur et à mesure qu'il augmente avec le temps, et du nombre de règles WAF nécessaires pour évaluer ce trafic. Les solutions WAF matérielles traditionnelles souffrent souvent d'une mauvaise échelle car elles sont limitées aux ressources CPU et mémoire disponibles dans le terminal et peuvent être en concurrence avec d'autres solutions sur le même terminal.

Le déploiement d'une solution WAAP intégrée sur la plateforme cloud d'Akamai élimine le problème d'échelle en exploitant les ressources de serveurs distribués d'Akamai pour inspecter le trafic Web entrant. Les utilisateurs et les attaquants se connectent aux sites Web protégés via le serveur Akamai le plus proche, qui inspecte ensuite le trafic à la recherche d'attaques et bloque toute requête malveillante détectée. Cela permet à la solution WAAP d'Akamai de s'adapter en toute transparence à toute augmentation du trafic des applications Web, qu'il s'agisse de pics de trafic soudains ou d'une croissance à long terme, ainsi qu'aux nouveaux emplacements des utilisateurs dans le monde.

Performances

De mauvaises performances peuvent entraver le déploiement d'une solution de sécurité, en particulier d'une solution WAAP déployée en ligne devant une application. La réduction des performances des sites Web essentiels à l'activité peut entraîner une baisse de productivité, une mauvaise expérience utilisateur, un délai de mise sur le marché plus long et une réduction des revenus.

L'envergure mondiale de la plateforme cloud d'Akamai permet au WAAP de protéger les applications Web sans réduire les performances. Le WAAP, distribué à l'échelle mondiale, inspecte le trafic HTTP dès son arrivée sur la plateforme, en répartissant les ressources de processeur et de mémoire nécessaires à l'inspection de ce trafic sur tous les serveurs de la plateforme. Cela élimine le problème des performances en tant que source de friction intra-organisationnelle et d'obstacle au déploiement.

Plateforme en bordure de l'Internet pour assurer la protection

Les solutions de sécurité applicative Web d'Akamai, indépendantes du cloud, fonctionnent de manière fluide sur l'ensemble de la plateforme pour se défendre contre un large éventail d'attaques basées sur les applications et les API. L'image ci-dessous illustre l'ensemble des mécanismes de sécurité et contrôles multicouches d'Akamai utilisés pour éloigner les menaces de l'origine tout en améliorant les performances et l'accès pour les utilisateurs légitimes.

Akamai App & API Protector comprend un large éventail de mécanismes et de contrôles de sécurité intégrés automatiquement (représentés en bleu) pour une défense complète prête à l'emploi, tandis que des produits et services Akamai supplémentaires sont ajoutés pour une protection complète de la couche 7.

Assistance gérée en cas d'attaque

En plus de la gestion continue du WAAP, Akamai fournit également à ses clients une assistance gérée en cas d'attaque, avec une surveillance 24 h/24, 7 j/7 des sites Web protégés et une réponse gérée à toute attaque détectée.

L'assistance gérée en cas d'attaque fait appel au personnel du centre d'opérations de sécurité (SOC) mondial d'Akamai pour répondre aux incidents de sécurité dès qu'ils se produisent via les actions suivantes :

- Répondre aux alertes WAAP et aux demandes des clients et approfondir l'analyse des problèmes
- Déterminer une signature d'attaque appropriée et déployer des mesures d'atténuation supplémentaires
- Travailler avec les équipes d'application des clients pour mesurer l'efficacité et la précision des mesures d'atténuation déployées, en ajustant les mesures d'atténuation si nécessaire
- Examiner la réponse globale avec les équipes d'application des clients après l'incident
- Fournir des boutons d'alerte d'attaque dans l'interface pour lancer une demande d'assistance d'urgence

Centre de commande des opérations de sécurité (SOCC)

Le SOCC d'Akamai contribue à atténuer un grand nombre des plus grandes attaques dans le monde depuis plus de 10 ans, protégeant ainsi les clients d'un écosystème des menaces en constante évolution.

La surveillance et l'atténuation d'une attaque malveillante nécessitent quatre fonctionnalités :

- Visibilité mondiale
- Surveillance et émission d'alertes proactives
- Atténuation agile des attaques
- Service de conseil continu par une équipe de sécurité expérimentée

Le SOCC d'Akamai offre ces capacités en exploitant la plus grande infrastructure de sécurité au monde. Tout le trafic réseau transite par notre plateforme de sécurité unifiée, qui recueille des renseignements en temps réel. Par exemple, Akamai a recueilli des tendances en matière de sécurité, telles qu'une forte augmentation récente des attaques par injection SQL.

Tout cela aide l'équipe de sécurité d'Akamai à atténuer rapidement les menaces pesant sur les clients avec une efficacité maximale et un impact minimal.

Conclusion

Outre la protection contre les attaques DDoS au niveau du réseau et des applications, les nouvelles formes de bots automatisés et d'attaques ciblées via les API et les composants côté client obligent les organisations à protéger l'ensemble de leurs applications Web, points de terminaison d'API, navigateurs et infrastructures grâce à une approche de sécurité complète et approfondie. Les responsables et les professionnels de la sécurité ont besoin d'une sécurité applicative Web qui identifie et atténue rapidement les menaces provenant de multiples vecteurs d'attaque et qui étend les protections traditionnelles au-delà du pare-feu aux technologies de sécurité adjacentes pour une défense optimale.

L'approche d'Akamai en matière de WAAP consiste à proposer un ensemble de solutions d'une ampleur et d'une efficacité inégalées, en fournissant toutes les technologies de sécurité nécessaires à une stratégie de sécurité de pointe. Nous pensons que la meilleure solution de sécurité ne devrait pas être réservée aux marques les plus grandes ou les plus populaires du monde. Notre portefeuille de protections d'applications et d'API met la sécurité efficace des applications Web à la disposition de toute organisation qui donne la priorité à la sécurité grâce à un portefeuille à plusieurs niveaux.

Avec une solution de sécurité qui évolue et s'adapte en permanence, en s'appuyant sur des renseignements approfondis et étendus sur les attaques, Akamai s'associe à des entreprises mondiales pour moderniser et améliorer continuellement les résultats en matière de sécurité. Nous nous efforçons de doter les équipes de sécurité de votre organisation des renseignements, de la visibilité, de l'automatisation et des orientations nécessaires pour faire avancer les initiatives internes tout en empêchant les adversaires d'accéder aux systèmes de votre entreprise. C'est pourquoi nous sommes reconnus pour protéger les marques les plus exigeantes qui soutiennent la vie en ligne.

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X et LinkedIn. Publication : 02/25.