FICHE PRODUIT AKAMAI

API Security

API Security d'Akamai est la solution intelligente pour protéger vos API contre les abus de logique métier et le vol de données

Les menaces liées aux API ne cessent d'évoluer

Les API sont le moteur de votre activité au quotidien et vous permettent de collaborer avec vos partenaires, fournisseurs et clients. Toutefois, chaque API élargit également votre surface d'attaque, et les acteurs malveillants le savent. Les attaques contre les API se multiplient et évoluent rapidement, et elles prennent souvent des formes que votre application Web et votre protection des API ne peuvent pas détecter. Sans un inventaire complet de vos API, un angle mort subsiste pour votre équipe et les API de votre entreprise ne sont pas protégées.

Pourquoi choisir API Security d'Akamai ?

Notre plateforme protège les API tout au long de leur cycle de vie, du développement à la production. Conçue pour les entreprises qui exposent des API à des partenaires, des fournisseurs et des utilisateurs, API Security détecte vos API, comprend leur niveau de risque, analyse leur comportement et empêche les menaces de pénétrer dans votre réseau.

Les capacités stratégiques d'API Security

Découverte

Il n'est pas rare d'avoir des API dont personne ne connaît l'existence. Or, sans inventaire précis, votre entreprise est exposée à toute une série de risques de sécurité. N'avancez plus à tâtons ! Laissez-nous vous aider à :

- localiser et inventorier toutes vos API, quel que soit leur configuration ou leur type, y compris RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC ;
- détecter les API inactives, héritées et zombies ;
- identifier les domaines oubliés, négligés ou autrement inconnus ;
- éliminer les angles morts et déceler les voies d'attaque potentielles.

Test

Les applications sont développées à un rythme plus rapide que jamais. Il est donc plus facile pour une vulnérabilité de sécurité ou un défaut de conception de passer inaperçu. Profitez de notre suite de tests API Security pour :

- exécuter automatiquement plus de 150 tests qui simulent le trafic malveillant, y compris les 10 principaux risques pour la sécurité des API selon l'OWASP ;
- découvrir les vulnérabilités avant que les API n'entrent en production afin de réduire le risque d'une attaque réussie ;
- inspecter les spécifications de vos API par rapport aux politiques et règles de gouvernance établies ;
- exécuter des tests de sécurité axés sur les API à la demande ou dans le cadre d'un pipeline CI/CD.

AVANTAGES POUR VOTRE ENTREPRISE

Découverte
Comprenez la surface d'attaque de vos API. Réduisez les coûts des inventaires d'API et des mises à jour de la documentation. Améliorez la conformité avec les exigences réglementaires et les politiques internes.

Test
Réduisez les coûts de correction en détectant les problèmes plus tôt. Améliorez la qualité du code sans sacrifier la vitesse. Augmentez vos revenus en accélérant la mise sur le marché.

Détection
Obtenez le contexte métier stratégique en apprenant exactement ce qui s'est passé. Déterminez pourquoi il s'agit d'un problème et découvrez son impact potentiel. Déterminez comment remédier au problème.

Réponse
Réduisez les risques en stoppant immédiatement les attaques. Réduisez les coûts en remédiant aux vulnérabilités avant qu'elles ne soient exploitées. Réduisez les pertes de revenus dues aux temps d'arrêt.

Détection

De simples erreurs de configuration d'API peuvent vous laisser sans défense face aux cybercriminels. Une fois à l'intérieur, les pirates peuvent rapidement accéder à vos données sensibles et les exfiltrer. Utilisez notre plateforme pour :

- analyser automatiquement l'infrastructure et découvrir les erreurs de configuration ainsi que les risques cachés ;
- créer des workflows personnalisés pour informer les principales parties prenantes des vulnérabilités ;
- identifier les API et les utilisateurs internes capables d'accéder aux données sensibles ;
- attribuer des niveaux de gravité aux problèmes détectés afin de hiérarchiser les mesures correctives

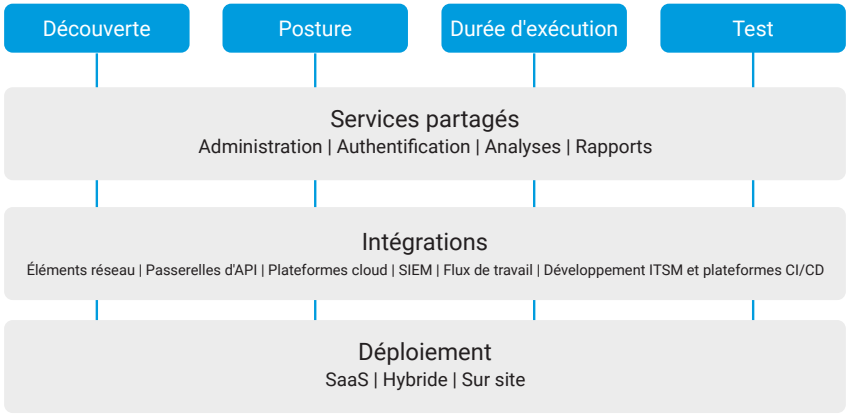
Réponse

La question n'est plus de savoir si votre entreprise sera attaquée, mais quand, ce qui signifie que vous devez être en mesure de détecter et de bloquer les attaques en temps réel. Utilisez notre système de détection des anomalies basé sur l'intelligence artificielle/l'apprentissage automatique pour :

- surveiller la falsification et la fuite de données, les violations de règles, les comportements suspects et les attaques d'API ;
- analyser le trafic API sans modifications supplémentaires du réseau ni agents difficiles à installer ;
- intégrer les flux de travail existants (système de tickets, gestion des informations et des événements de sécurité [SIEM], etc.) pour alerter les équipes chargées de la sécurité/des opérations ;
- prévenir les attaques et les abus en temps réel grâce à une correction partielle ou entièrement automatisée.

La différence Akamai : bloquer les menaces en bordure de l'Internet

Akamai App & API Protector détecte et déjoue les menaces liées aux API pour les applications et les API exécutées dans Akamai Connected Cloud, et peut bloquer en ligne tout trafic présentant une menace potentielle découverte par API Security. Lorsqu'elles sont déployées ensemble, les protections de l'API d'Akamai proposent une visibilité complète et continue des API et vous permettent de constater, d'auditer, de détecter et de résoudre les problèmes de sécurité des API sur l'ensemble de vos applications.



Vous souhaitez savoir comment fonctionne API Security ? Rendez-vous sur akamai.com/apisecurity et planifiez un rendez-vous avec notre équipe.

| Publication : 06/24