Le guide ultime de gestion de la posture de sécurité des API

Table des matières

Pourquoi la sécurité des API est devenue un impératif

Les API permettent aux développeurs d'une entreprise de construire un réseau efficace, dans un secteur où la vitesse n'est pas négociable. Cependant, bien que les API soient conviviales pour les développeurs, et essentielles pour l'interopérabilité des logiciels et des ressources de données, leur sécurité n'a pas suivi le rythme de l'innovation.

84 % des entreprises ont connu un incident de sécurité des API au cours des 12 derniers mois, contre 78 % en 2023[1]. Cela s'explique en partie par le fait que les attaquants tirent aussi parti de ces API. En effet, de nombreuses API comportent des erreurs de configuration, des erreurs de codage et un manque de contrôles d'authentification. Par conséquent, une attaque d'API peut être assez simple à réaliser et peut constituer un moyen direct de voler des données.

En ce qui concerne les données, seulement 27 % des entreprises disposant d'inventaires d'API complets savent quelles API renvoient des données sensibles (des données clients à la propriété intellectuelle), contre 40 % en 2023[2]. Les attaques ne cessant de s'intensifier et la visibilité diminuant, les entreprises ont besoin d'un moyen d'évaluer et d'améliorer leur stratégie de sécurité des API.

1, 2. Akamai, « Étude de l'impact sur la sécurité des API », 2024

Ce à quoi ressemble une sécurité complète des API

Plus votre entreprise utilise des API, plus votre surface d'attaque s'étend, ce qui crée de nouveaux défis en matière de sécurité.

Lorsqu'il s'agit de sécuriser les API, les outils que les entreprises ont l'habitude d'utiliser, comme les passerelles d'API et les pare-feux d'applications Web, peuvent fournir une certaine protection. Mais à mesure que votre parc d'API devient plus complexe (par exemple, avec une prolifération d'API non gérées difficiles à voir et à sécuriser), le système de sécurité doit changer.

Les API méritent d'occuper une place importante dans le programme de sécurité des entreprises. De plus, une solution de sécurité des API dédiée, conçue pour prendre en charge les risques et les méthodes d'attaque actuels des API, peut fournir la visibilité et les capacités nécessaires à l'exécution de ce programme. C'est assez semblable au concept de défense en profondeur, où les outils sont complémentaires pour couvrir chaque étape du chemin d'attaque.

Une plateforme complète de sécurité des API, conçue pour assurer la découverte des API, la gestion de la posture, la protection de l'exécution et les tests de sécurité, peut vous aider à voir les risques cachés liés aux API, à identifier les chemins d'attaque que présentent les API et à atténuer les menaces que vous découvrez en temps réel.

Dans notre livre numérique connexe, le guide ultime de la découverte des API, nous expliquons le premier élément essentiel à la sécurité des API, à savoir la localisation de vos API. Une fois que vous avez découvert toutes les API utilisées à l'échelle de votre entreprise et avoir réalisé un inventaire complet, l'étape suivante consiste à améliorer votre posture globale de sécurité des API.

La gestion de la posture peut s'avérer particulièrement importante pour les entreprises qui achètent les applications d'un fournisseur tiers et qui les utilisent, les personnalisent et les vendent comme si c'était les leurs. Par exemple, presque toutes les voitures neuves des cinq dernières années partagent des fonctionnalités télématiques presque identiques. Si un attaquant détecte des vulnérabilités dans les points de terminaison des API d'un fabricant, il obtient un point d'entrée facile pour les attaques par piratage de compte à distance et les violations de données.

Ce que couvre ce guide

La gestion de la posture des API vous fournit les outils pour gérer, surveiller et maintenir la sécurité de vos API tout au long de leur cycle de vie. Ce guide ultime se concentre sur les principales exigences en matière de gestion de la sécurité des API, y compris la détection des vulnérabilités et la protection des données sensibles. Il explore les méthodes de gestion des postures et présente les capacités de gestion des postures de la solution Akamai API Security.

Pourquoi s'intéresser à la gestion de la posture ?

La gestion de la posture des API vous permet d'avancer en toute sérénité en matière de sécurité des API. Elle vous aide à comprendre le risque lié aux API découvertes en identifiant les types de données qui circulent, en repérant les vulnérabilités ou les configurations incorrectes, en vous assurant de la bonne authentification des API, etc. La capacité à identifier les vulnérabilités des API et à les corriger rapidement vous permet de prendre des mesures correctives avant qu'une attaque ne se produise.

La gestion de la posture complète offre une visibilité sur toutes les activités autour des API, ce qui vous permet d'appliquer des stratégies de sécurité, de garantir la conformité aux réglementations et d'auditer les modifications apportées à votre écosystème d'API. Elle protège et sécurise vos API contre les

Seules 27 % des entreprises disposant d'un inventaire complet de leurs API savent lesquelles renvoient des données sensibles, contre 40 % en 2023.[3]

3. Akamai, « Étude de l'impact sur la sécurité des API », 2024

attaques malveillantes, les utilisateurs non autorisés et les violations de données, autant d'éléments qui peuvent entraîner d'importantes atteintes à la réputation, une perte d'activité et des sanctions réglementaires.

La mise en œuvre des meilleures pratiques de gestion de la posture permet de réduire la surface d'attaque des API et d'atténuer bon nombre des risques liés à vos API. La création d'inventaires complets des API et des magasins de données sensibles de votre entreprise est essentielle pour une bonne gestion de la posture. Sur la page suivante, nous allons aborder d'autres éléments de la gestion de la posture des API, à savoir la détection des vulnérabilités, la surveillance des API et la résolution des problèmes.

- ## Détection des vulnérabilités

  Analyse : inspectez le code source pour détecter les faiblesses courantes, comprenez comment une API interagit avec les systèmes externes et évaluez ses fonctionnalités d'autorisation et d'authentification.

  Observation : inspectez le trafic vers et depuis une API pour identifier les erreurs de configuration, détecter les vulnérabilités et comprendre le comportement de base de l'API.

La gestion de la posture n'est qu'une partie d'un vaste programme de sécurité des API. Il est également essentiel d'utiliser des tests complets de préproduction pour empêcher les vulnérabilités d'atteindre la production.

- ## Surveillance des API

  Identifiez et surveillez les appels d'API en production, suivez les demandes d'API, détectez les écarts par rapport à l'utilisation de référence et créez des alertes lorsque l'utilisation de l'API dépasse les seuils prédéfinis.

- ## Correction

  Corrigez les faiblesses ou vulnérabilités identifiées pour renforcer la sécurité et la conformité d'une API en modifiant le code, en ajustant les paramètres de sécurité ou en appliquant des correctifs sur les failles de l'API. Une bonne gestion de la posture permet de résoudre les problèmes avant qu'une vulnérabilité ne puisse être exploitée.

Fonctionnalités de gestion de la posture dont vous ne pouvez pas vous passer

Vous savez peut-être déjà (ou vous soupçonnez fortement) que votre stratégie de sécurité des API n'est pas aussi solide qu'elle pourrait l'être. Voici quelques fonctionnalités clés que doivent offrir vos outils de gestion de la posture.

- **Classification des données sensibles**
  Une API qui fournit des données météorologiques à partir de sources publiques est beaucoup moins préoccupante qu'une API qui transmet des informations de carte de crédit. Les outils de gestion de la posture des API doivent être en mesure d'identifier rapidement le nombre d'API pouvant accéder aux données de carte de crédit, aux numéros de téléphone, aux numéros de sécurité sociale et à d'autres données sensibles, ainsi que le nombre d'utilisateurs ayant accédé à des données sensibles par l'intermédiaire de vos API.
- **Évaluation de la configuration**
  De nombreuses cyberattaques aboutissent en raison d'une simple mauvaise configuration des réseaux, des passerelles d'API ou des pare-feux qui assurent le courtage et la protection du trafic des API. Une gestion rigoureuse de la posture nécessite la capacité d'analyser régulièrement les configurations de l'infrastructure et des logiciels, y compris les fichiers journaux et les fichiers de configuration. Une analyse régulière permet de découvrir les mauvaises configurations et les vulnérabilités, et d'identifier les risques ainsi engendrés.
- **Indice de confiance de l'attaquant**
  Recherchez un moteur d'évaluation de la confiance des attaquants qui utilise des algorithmes avancés d'apprentissage automatique formés pour évaluer les signaux externes et internes, y compris le comportement des API, les modèles de trafic réseau, les données de géolocalisation, les

renseignements sur les menaces et d'autres facteurs contextuels. Vous pouvez ainsi savoir quelle est la probabilité (niveau de confiance) qu'un incident d'exécution détecté soit le résultat d'une activité malveillante. Cette fonctionnalité unique permet aux clients de se concentrer rapidement sur les menaces critiques et de créer automatiquement des flux de correction et de notification pour les attaques à haute probabilité malveillante.

- **Flux de travail personnalisés**
  En plus de la gravité personnalisable, vous devez être en mesure de créer des flux de travail pour prendre des mesures immédiates lorsque des vulnérabilités sont identifiées. Les flux de travail personnalisés peuvent aller de la création de tickets d'incident à la notification des parties prenantes clés en passant par la mise à jour des configurations réseau.

- **Documentation générée automatiquement**
  La documentation sur les API indique aux utilisateurs d'une API ce qu'elle fait et comment l'utiliser. Les API sécurisées doivent être évaluées pour vérifier leur conformité par rapport aux spécifications et documentées avec précision. Une documentation médiocre ou inexistante rend les tests de sécurité plus difficiles et augmente le risque qu'une API parvienne en production avec une vulnérabilité non détectée.

Ce problème est souvent exacerbé par l'externalisation du développement des API. Quelle que soit la source du problème, une documentation obsolète, incomplète ou manquante est inacceptable si vous voulez que votre programme de sécurité des API soit efficace.

La spécification OpenAPI (anciennement Swagger) définit les descriptions d'interface standard. Les outils de gestion de la posture doivent être en mesure de générer automatiquement une documentation OpenAPI complète basée sur l'état actuel et futur des API pour vous assurer que toutes les API sont correctement documentées et que la documentation est à jour.

Un leader de l'assurance améliore la posture de la sécurité de ses API avec Akamai

Alors que les consommateurs abandonnent les magasins pour se tourner vers le virtuel, les entreprises de services financiers doivent innover à un rythme effréné. Comme bon nombre de ses pairs, Aflac, premier fournisseur d'assurance maladie complémentaire aux États-Unis, a été confronté à un nombre grandissant de défis en matière de sécurité des API.

Pour répondre à ses besoins, Aflac s'est tourné vers la plateforme Noname de sécurité des API (désormais intégrée à Akamai API Security). Le module de gestion de la posture aide l'équipe à identifier les types de données qui passent par les API de l'entreprise, en offrant une visibilité sur les API qui accèdent aux données sensibles et en identifiant toute anomalie dans l'accès aux données.

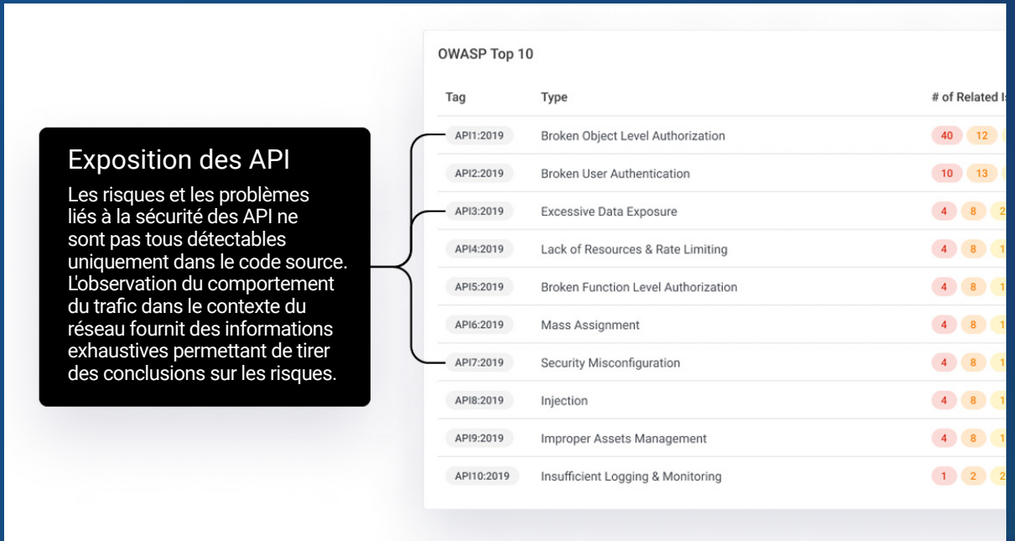
Lisez l'étude de cas complète d'Aflac pour en savoir plus.

> Nous savions que l'empreinte de nos API était importante, et nous voulions être totalement sûrs que chaque API était prise en compte, que nous avions une visibilité totale sur leur fonctionnement et qu'elles étaient continuellement testées pour évaluer les risques de sécurité.
>
> — DJ Goldsworthy, Vice-président, Opérations de sécurité et gestion des menaces, Aflac

L'approche d'Akamai en matière de gestion de la posture

Le module de gestion de la posture de la solution Akamai API Security fournit une vue complète du trafic, du code et des configurations pour évaluer la posture de sécurité des API de votre entreprise. Akamai détermine l'étendue de votre véritable surface d'attaque à l'échelle de vos API et applications Web, et découvre toutes les formes de données sensibles qui transitent par vos API, pour ainsi mieux les sécuriser.

De simples erreurs de configuration d'API peuvent vous laisser sans défense face aux cybercriminels. Une fois à l'intérieur, les attaquants peuvent accéder rapidement à vos données sensibles et les exfiltrer. Le module de gestion de la posture de la solution Akamai API Security offre les fonctionnalités clés suivantes :



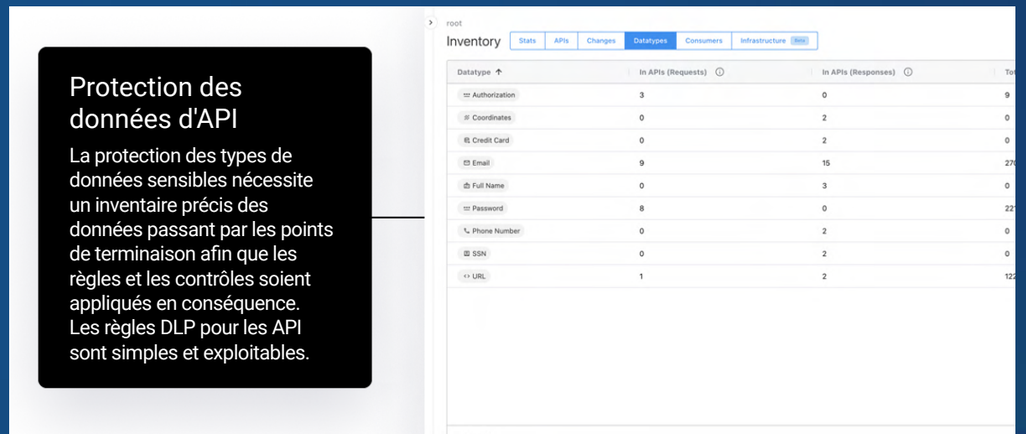
- Intégration hors bande pour la découverte continue des API sur site et dans les clouds hybrides et publics
- Inventaire d'API simple et consultable qui inclut des détails sur le schéma, le positionnement du réseau et les types de données
- Génération automatisée de documentation sur les API (OAS/Swagger)
- Analyse contextuelle des erreurs de configuration des API et des vulnérabilités avec hiérarchisation
- Détection de toutes les vulnérabilités figurant dans les 10 principaux risques pour la sécurité des API selon l'OWASP
- Découverte et classification automatisées des données sensibles et des modifications des API

Exposition des API

Outre la découverte des risques au sein du code d'une API, il est également important d'observer le trafic des API en surveillant leur comportement (typique ou atypique) dans le contexte du réseau.

Le module de gestion de la posture de la solution Akamai API Security examine l'ensemble le plus large possible de sources pour détecter les vulnérabilités, notamment les fichiers journaux, les relectures de l'historique du trafic, les fichiers de configuration et bien plus encore. La solution détecte toutes les vulnérabilités dans les 10 principaux risques pour la sécurité des API selon l'OWASP et protège les API contre les fuites de données, les problèmes d'autorisation, les abus, les utilisations abusives et la corruption des données.

Akamai identifie et hiérarchise intelligemment les vulnérabilités potentielles. Celles-ci peuvent être corrigées manuellement, de manière semi-automatique ou de façon entièrement automatique grâce à des intégrations dans les WAF, les passerelles d'API, les outils SIEM et ITSM, les outils de flux de travail et d'autres services.



Protection des données d'API

La protection des types de données sensibles nécessite un inventaire précis des données passant par les points de terminaison afin que les règles et les contrôles soient appliqués en conséquence. Les règles DLP pour les API sont simples et exploitables.

La conformité prend une toute nouvelle dimension avec la croissance de l'utilisation des API. Une vague de réglementations a vu le jour en réponse à l'augmentation de la surface d'attaque. Les industries réglementées doivent désormais intégrer les API dans leurs plans de conformité.

Le module de gestion de la posture de la solution Akamai API Security identifie toutes les formes de données sensibles qui passent par vos API, y compris toutes les informations personnelles identifiables telles que les cartes de crédit, les numéros de sécurité sociale, les adresses, les informations d'assurance, etc. En réduisant l'accès à ces types de données et en mettant en œuvre un cadre de gestion des données, nous vous aidons à vous assurer que les données sensibles sont là où elles doivent être et bien protégées contre les menaces malveillantes.

Comment la gestion de la posture des API peut vous aider

Chaque fois qu'un client, un partenaire ou un fournisseur interagit avec votre entreprise par la voie numérique, une API facilite l'échange rapide de données (souvent sensibles). L'obtention d'une visibilité sur toutes les API de votre entreprise et l'évaluation de leurs attributs de risque (par exemple, quelles API renvoient des données sensibles) peuvent vous aider à protéger votre entreprise contre un vecteur d'attaque à croissance rapide. La gestion de la posture de sécurité des API peut également vous aider à assurer la conformité avec les réglementations internationales visant à prévenir les violations de données.

Découvrez les réglementations en matière de protection des données qui exigent de voir et de sécuriser toutes les API.

Découvrez comment nous pouvons vous aider en planifiant une démonstration personnalisée d'Akamai API Security.

La solution de sécurité d'Akamai 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 abonnez-vous à Akamai Technologies sur **X** (anciennement Twitter) et **LinkedIn**. Publication : 12/24.

Akamai