# Guide ultime de la protection de l'exécution des API

# Table des matières

# Introduction

## Pourquoi la sécurité des API est indispensable

Dans la course à la satisfaction des besoins des clients, les entreprises doivent rapidement développer, produire et améliorer les applications, les services et les outils d'IA générative. Ce besoin de vitesse entraîne malheureusement un risque caché : les API qui fonctionnent en arrière-plan pour toutes ces innovations comportent souvent des erreurs de configuration et de codage, et leurs contrôles de sécurité sont insuffisants. Et lorsque ces API atteignent la phase de production, elles n'interagissent plus uniquement avec des utilisateurs finaux ; les attaquants cherchent constamment des moyens de compromettre les API et d'accéder aux données qu'elles échangent.

Les API mal configurées et compromises constituent de plus en plus un facteur clé de violations de données importantes. Pourtant, peu d'entreprises sont en mesure de suivre les milliers d'appels d'API qui ont lieu au sein de leurs écosystèmes digitaux. Et encore moins d'entre elles sont entièrement protégées contre les menaces ciblant l'exécution des API.

Par exemple, en 2021, une entreprise de commerce de détail spécialisée dans la remise en forme a trouvé un bogue dans une API pour les données de compte utilisateur permettant à quiconque de faire des requêtes non authentifiées de données, notamment l'âge, le sexe, la ville, le poids et la date de naissance. Si dans ce cas précis, cette vulnérabilité a été détectée et signalée à l'entreprise par un chercheur en sécurité, les bogues comme celui-ci peuvent passer inaperçus et être exploités pendant des semaines ou des mois.

Lorsqu'il s'agit de sécuriser les API, les outils sur lesquels les entreprises ont l'habitude de s'appuyer (par exemple, les passerelles d'API et les pare-feux d'applications Web) peuvent fournir une base de protection. Cependant, les équipes de sécurité d'aujourd'hui ont besoin de couches de sécurité supplémentaires, à mesure que les attaques d'API augmentent en nombre et en sophistication. La clé consiste à renforcer les contrôles existants avec des informations plus détaillées sur les vulnérabilités, les chemins d'attaque éventuels, les activités malveillantes et le comportement des API.

Les entreprises peuvent atteindre ces capacités grâce à une solution complète de sécurité des API, couvrant quatre domaines :

1. Découverte des API
2. Gestion de la posture des API
3. Protection de l'exécution des API
4. Tests de sécurité complets des API

## Ce que couvre ce guide

La protection de l'exécution des API est le processus de sécurisation des API lorsqu'elles traitent et gèrent les requêtes pendant leur fonctionnement normal. Ce guide décrit les principales exigences en matière de protection de l'exécution des API, notamment la surveillance des API pour éviter les erreurs de configuration et d'exploitation, et la prévention des attaques d'API. Il explore les bases de la prévention de l'exécution et présente les fonctionnalités de prévention de l'exécution proposées par Akamai API Security.

# Pourquoi protéger l'exécution ?

La protection de l'exécution des API sécurise les API tout au long de la phase de production de leur cycle de vie, lorsque l'API est opérationnelle et disponible pour interagir avec les utilisateurs finaux prévus et avec les attaquants. Grâce à des fonctionnalités qui aident les entreprises à identifier et à traiter rapidement les requêtes d'API malveillantes, des fonctionnalités efficaces de protection de l'exécution peuvent sécuriser les API contre tout un éventail de menaces après le déploiement, notamment les suivantes :

- Extraction de grands volumes de données sensibles par un attaquant à partir d'une API
- Attaques par élévation des privilèges qui exploitent les bogues de sécurité
- Déploiement d'API non autorisées en dehors des processus normaux

Le blocage des menaces ciblant l'exécution des API nécessite de comprendre le contexte de fonctionnement de chaque API, y compris l'accès, l'utilisation et le comportement des API. Pour commencer, vous devez connaître la portée de votre parc d'API. Notre guide ultime de la découverte des API explique l'importance d'un inventaire des API. Grâce à un inventaire complet des API, vous pouvez surveiller tout le trafic des API et établir une compréhension de base du comportement « typique » de chaque API. Cette référence peut être utilisée pour reconnaître les comportements anormaux. La protection de l'exécution des API doit détecter les éléments suivants :

- Fuite de données
- Violations des politiques de données
- Attaques de sécurité des API
- Falsification de données
- Comportement suspect

En outre, cette protection de l'exécution doit consigner le trafic d'API, surveiller l'accès aux données sensibles, détecter les menaces et bloquer ou corriger les attaques.

# Surveillance du trafic d'API pour détecter les attaques

Il est essentiel d'observer le comportement du trafic des API pour identifier les risques. Le déploiement d'une solution de surveillance sans une image précise de votre parc d'API n'offre qu'une visibilité limitée. Une fois que vous avez terminé l'inventaire de vos API, la protection de leur exécution doit surveiller en permanence le trafic et leur consommation, et rechercher les vulnérabilités et les erreurs de configuration.

# Détection des comportements anormaux

Le fait de disposer d'une référence de comportement normal des API permet d'identifier tout ce qui est inhabituel. La lecture des données historiques peut aider à identifier les comportements anormaux, ce qui peut également révéler l'intention d'un attaquant.

Toute anomalie potentielle doit être examinée plus en détail dans le cadre d'autres actions ayant eu lieu au sein de l'application ou du réseau. Par exemple, si les requêtes de données sont généralement d'une certaine taille et qu'un appel d'API demande des données en dehors de la plage habituelle, cet appel doit être signalé. Il n'est pas forcément malveillant, mais l'anomalie nécessite une inspection plus approfondie.

# Détection de l'exposition des données

Certaines des API de votre parc envoient et reçoivent probablement des données sensibles. Les informations sensibles exposées en raison d'une vulnérabilité de sécurité permettent à un attaquant d'élever les privilèges ou d'autres configurations de contrôle d'accès inappropriées. L'IA et l'apprentissage automatique peuvent jouer un rôle déterminant dans l'analyse du trafic et la détection des anomalies en temps réel, en fournissant des informations contextuelles sur les fuites de données, la falsification de données, les violations de règles de données, les comportements suspects et les attaques de sécurité des API.

Pour leurs attaques, il est de plus en plus fréquent que les cybercriminels se procurent des clés d'API valides. Une fois qu'un attaquant dispose de clés valides, la seule façon de se protéger contre une utilisation inappropriée des API et une violation potentielle des données consiste à détecter et bloquer les comportements anormaux et l'exposition des données.

# Audit de sécurité des API

Les outils d'audit de sécurité des API doivent surveiller le trafic en temps réel et vous alerter des attaques et autres intentions malveillantes. Au minimum, l'audit de sécurité des API doit :

- Fournir une surveillance continue pour identifier les attaquants et les requêtes malveillantes
- Analyser les API de façon passive, en interne et en externe, pour détecter les erreurs de configuration et les oublis susceptibles d'ouvrir la voie vers une violation, l'aggravation de celle-ci ou l'affaiblissement des défenses
- Appliquer des règles sur les données qui doivent (et ne doivent pas) être envoyées ou reçues par les API

La protection de l'exécution des API doit également être complétée par la gestion de la posture des API, qui identifie les erreurs de configuration et les vulnérabilités connues. Consultez notre **guide ultime sur la gestion de la posture des API** pour en savoir plus.

# Des fonctionnalités de protection de l'exécution dont vous ne pouvez pas vous passer

Si votre entreprise développe et déploie activement des API, votre programme de sécurité des API doit comprendre une protection robuste de leur exécution. Voici les principales fonctionnalités que vos outils de protection de l'exécution doivent inclure.

## Surveillance hors bande en temps réel

La surveillance de la sécurité des API ne doit pas avoir de conséquences sur la latence du trafic d'API. C'est-à-dire qu'elle ne doit, ni le ralentir ni l'accélérer. Elle doit fonctionner entièrement hors bande, sans modification du réseau et sans agents encombrants et difficiles à installer. Les outils de protection de l'exécution doivent refléter le trafic provenant de sources de données identifiées et effectuer une analyse de ces données de trafic en arrière-plan, avec des alertes en temps réel à chaque fois qu'un problème est détecté.

Akamai fonctionne hors bande et sans agent par défaut, mais nous proposons des options de détection basée sur agent et de blocage en ligne si nécessaire.

## Détection des anomalies des API et des tentatives d'exploitation

La collecte passive de données ne suffit pas, d'autant plus que le nombre d'API et le volume total de trafic API continuent d'évoluer. L'activité des API doit être analysée en permanence pour détecter les événements anormaux et alerter les équipes de sécurité et d'exploitation. Les outils de plateforme de pointe intègrent des fonctionnalités d'IA et d'apprentissage automatique pour analyser le trafic en temps réel et tirer parti des informations contextuelles sur les fuites de données, la falsification de données, les violations de règles de données, les comportements suspects et les attaques de sécurité des API.

## Prévention des attaques d'API et mesures correctives en matière de risques

Une fois qu'une anomalie ou un autre problème a été identifié et qu'une alerte a été générée, il est essentiel d'agir rapidement. Les mouvements non autorisés de données sensibles via des API ou toute autre utilisation abusive présumée des API doivent être détectés et corrigés. La protection de l'exécution ne doit pas seulement empêcher l'utilisation abusive des API par le biais de l'intégration avec vos pare-feux et passerelles d'API existants, elle doit aussi fournir des options de correction, automatisées lorsque cela est possible. Recherchez des fonctionnalités comprenant l'évaluation de la confiance des attaquants. Cela aide votre équipe à déterminer si les alertes d'abus, d'attaques ou de violations sont avérées et si elles doivent être transmises au niveau supérieur.

## Intégrations pour la réponse aux incidents

En règle générale, les outils de protection de l'exécution doivent s'intégrer facilement aux autres outils de sécurité, de surveillance et de gestion utilisés par votre organisation. Par exemple, lorsqu'un incident se produit, les outils de protection de l'exécution doivent inclure les intégrations nécessaires pour s'assurer que les tâches de correction sont attribuées aux équipes appropriées. Si des erreurs de configuration, des violations des politiques de données ou des comportements suspects sont détectés, ils doivent être signalés à la passerelle d'API, au système SIEM et à d'autres moteurs de sécurité de l'information afin de garantir le niveau approprié de prise de conscience. La capacité d'évaluation de la confiance des attaquants peut permettre aux équipes de filtrer les alertes et de se concentrer sur les véritables priorités de sécurité des API.

Rapyd

Rapyd, société internationale de traitement des paiements et de technologie financière, gère des systèmes de paiement dans plus de 100 pays. En l'absence d'une visibilité granulaire sur l'utilisation et le comportement des API, l'entreprise avait besoin d'un meilleur moyen de sécuriser les API publiques (et des centaines d'API internes) dans un système mondial extrêmement complexe fonctionnant à partir du cloud AWS. Rapyd avait besoin d'un inventaire granulaire de toutes ses API, d'une visibilité sur les erreurs de configuration et les vulnérabilités, et d'alertes hiérarchisées intelligemment pour adopter une approche de correction plus logique.

Akamai API Security a répondu aux besoins de Rapyd en offrant une visibilité complète et une protection d'exécution qui utilise l'apprentissage automatique pour créer un trafic de référence pour chaque API, avec une détection et une correction automatisées des anomalies.

Lire le témoignage client dans son intégralité

> Nous pouvons désormais évaluer les risques de manière précise et contrôler notre avenir.

– Nir Rothenberg
RSSI, Rapyd

# Protection de l'exécution avec Akamai API Security

La capacité à identifier et déjouer les attaques des API au fur et à mesure qu'elles se produisent doit faire partie intégrante de votre programme d'évaluation de la conformité et des risques. Il s'agit de votre dernière ligne de défense si les autres contrôles de sécurité ne sont pas à la hauteur.

Le module de protection de l'exécution d'Akamai API Security inclut toutes les fonctionnalités décrites dans la section précédente. Sa fonction principale consiste à détecter et bloquer les attaques d'API en temps réel. La surveillance basée sur l'apprentissage automatique permet d'analyser le trafic et de fournir des informations contextuelles sur les fuites de données, la falsification de données, les violations de politiques de données, les comportements suspects et les attaques de sécurité des API. Les outils de protection de l'exécution détectent les anomalies et les menaces potentielles dans votre trafic d'API et facilitent la correction en fonction de règles de réponse aux incidents présélectionnées.

La protection de l'exécution s'intègre aux WAF, aux passerelles d'API, aux ITSM, aux SIEM et à d'autres outils de flux de travail pour offrir une défense globale contre les attaques. Vous pouvez choisir d'automatiser entièrement la correction des menaces ou d'exiger différents niveaux d'intervention manuelle pour une visibilité et un contrôle accrus. La solution Akamai API Security s'intègre également de manière native à la plateforme Akamai, ce qui nous permet de bloquer les adresses IP des attaquants directement à la bordure de l'Internet.

## Génération du problème

Grâce à l'apprentissage automatique, Akamai crée un modèle pour chaque API. Cette base de référence du comportement normal est ensuite utilisée pour détecter les attaques de logique métier des API telles que l'autorisation brisée au niveau de l'objet, lorsqu'un individu accède aux données auxquelles

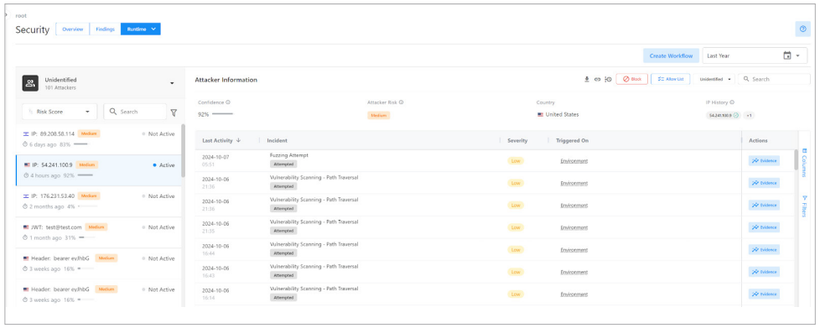
il ne devrait pas avoir accès. Akamai génère un problème en temps réel chaque fois que le trafic d'API s'éloigne du comportement normal. Un problème ressemble beaucoup à une alerte et est généré chaque fois qu'un comportement anormal ou une mauvaise configuration est détectée au niveau d'une API. Au fur et à mesure que les problèmes sont générés, les alertes peuvent être envoyées automatiquement à un SIEM tel que Splunk ou Qradar. Les alertes peuvent également être envoyées automatiquement à un système de tickets tel que ServiceNow ou Jira.

# Détails du problème

Chaque problème généré par le module de protection de l'exécution d'Akamai API Security inclut la gravité, l'état, une correspondance avec les 10 principales vulnérabilités des API selon l'OWASP, ainsi que des informations relatives à l'attaquant, le cas échéant.

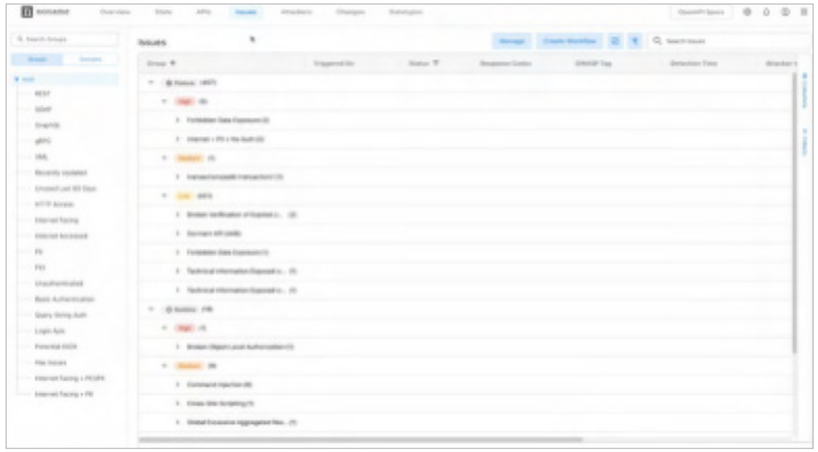
Les pages d'informations sur le problème comprennent une description du problème et de son impact potentiel sur votre entreprise, et fournissent des recommandations de résolution. Akamai API Security permet également aux entreprises de voir les types d'actions entreprises par les attaquants sur une période donnée, avec un historique de chaque attaque et la possibilité de prendre des mesures contre les acteurs malveillants.

**Exemple : Visibilité sur les actions des attaquants**

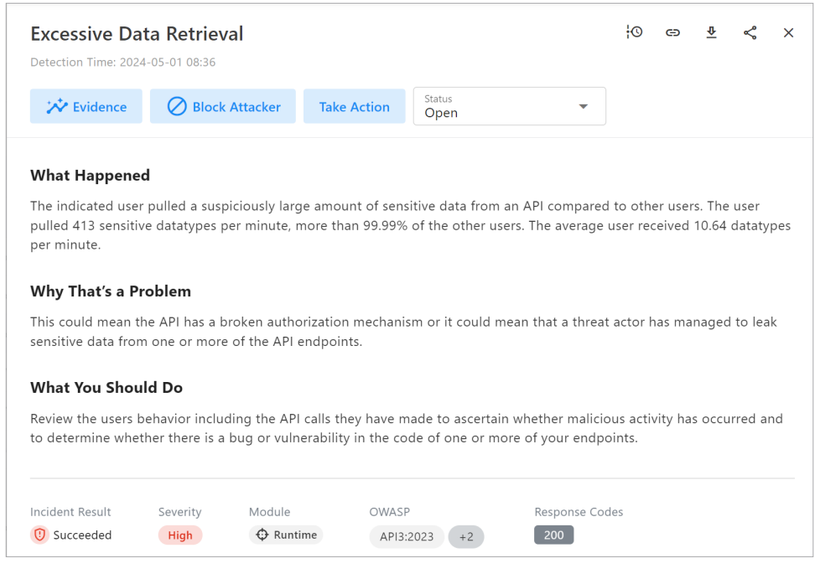



Chaque problème comprend des preuves. Les preuves sont les détails de la session de l'attaquant qui ont conduit à la génération du problème, ainsi qu'une copie de la requête et de la réponse de l'API (en-têtes et corps) pour faciliter le tri et la résolution rapide du problème. Grâce à des tableaux de bord intuitifs, des fonctions de filtrage, des alertes et des fonctionnalités de création de rapports, le module de protection de l'exécution de la solution Akamai API Security peut aider les entreprises à déterminer ce qui s'est passé, pourquoi, et ce qui doit être fait exactement.

## Exemple : Création de rapports sur les problèmes d'API avec preuves



## Exemple : Informations sur la récupération excessive de données




## Actions de la règle

Akamai API Security offre la possibilité de prendre une action de règle semi-automatisée pour chaque problème généré. Les actions peuvent inclure l'ouverture d'un ticket, l'envoi d'informations à un SIEM ou l'envoi d'un webhook à un système tiers. Elles peuvent également inclure le blocage d'un attaquant. Les types d'actions disponibles sont déterminés par les types d'intégrations configurés sur la plateforme Akamai.

La solution comprend de nombreuses règles prédéfinies prêtes à l'emploi pour la détection des attaques et des configurations erronées d'API. Akamai API Security inclut également plus de 20 types de données préconfigurés pour vous aider à créer les règles de données dont vous avez besoin afin de détecter et de prendre des mesures lorsque des données sensibles traversent vos API.

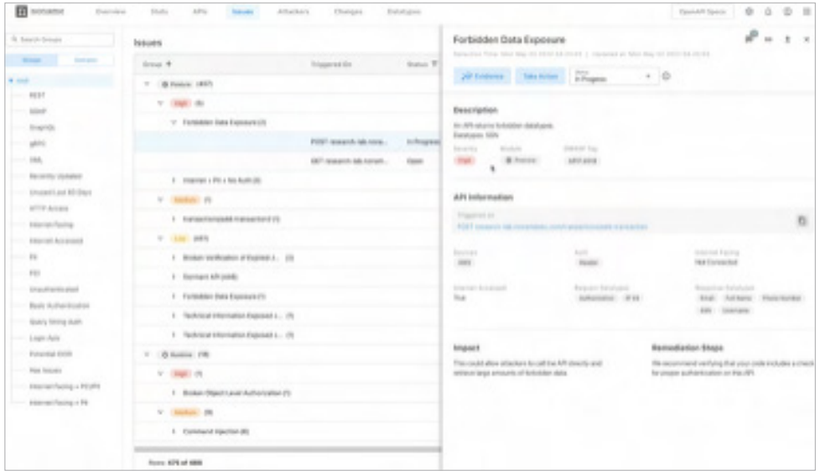
En résumé, le module de protection de l'exécution de la solution Akamai API Security offre une détection et une prévention en temps réel des attaques d'API, ainsi qu'une détection continue des erreurs de configuration d'API, en plus de nombreuses intégrations de flux de travail populaires qui simplifient les opérations et la correction.

## Anatomie d'un incident de sécurité d'API

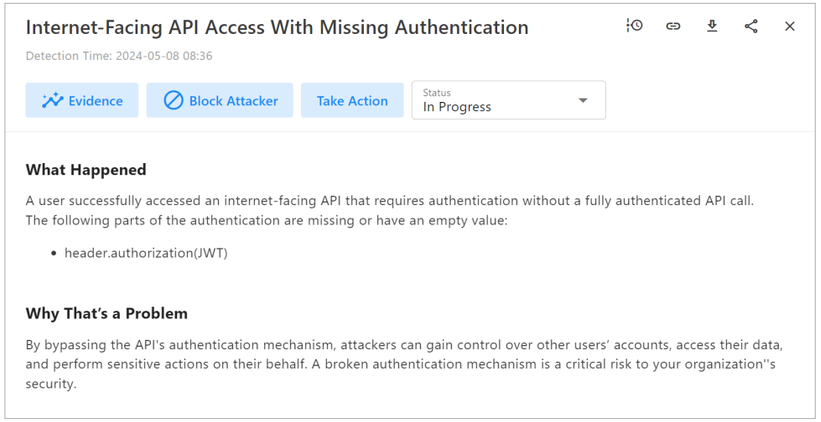
Examinons de plus près un exemple de divulgation interdite de données. Cet exemple illustre un problème de posture interne à une API. La plateforme Akamai connaît les types de données et les valeurs associées à chaque API grâce au contexte.

Dans la figure ci-dessous, des données interdites sont exposées par une API. La plateforme Akamai a détecté le type de données en cours de transmission, en l'occurrence un numéro de sécurité sociale, et a compris que ce type de données avait précédemment été marqué comme interdit. Akamai peut également détecter les erreurs de configuration externes à l'API, telles que les API qui sont accessibles sur Internet, mais qui ne sont pas enregistrées avec une passerelle d'API.

### Exemple : Informations sur l'exposition interdite des données



### Exemple : Identification des API sans authentification



# Étapes suivantes pour obtenir une protection efficace de l'exécution des API

Chaque fois qu'un client, un partenaire ou un fournisseur interagit avec votre entreprise par la voie digitale, une API facilite l'échange rapide de données (souvent sensibles). La mise en œuvre de fonctionnalités clés de protection de l'exécution des API (par exemple, la surveillance des API pour se défendre contre les erreurs de configuration et d'exploitation, et la prévention des attaques d'API) peut vous aider à protéger votre entreprise contre un vecteur d'attaque à croissance rapide.

Découvrez comment évaluer les fournisseurs de sécurité des API pour vous assurer qu'ils offrent des fonctionnalités essentielles de protection de l'exécution.

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