PRÉSENTATION DE LA SOLUTION AKAMAI

Akamai API Security pour la gestion des ressources API

À mesure que les entreprises deviennent de plus en plus digitales et centrées sur le cloud, la portée, l'échelle et la valeur des API augmentent, mais celles-ci présentent également un risque à croissance rapide.

Les API exposées ou mal configurées sont courantes et faciles à compromettre. Elles manquent non seulement de protection et sont souvent invisibles et non gérées, comme c'est le cas des « API fantômes » très vulnérables. De plus, leur prolifération rend difficiles la localisation et l'inventaire de chaque API au sein de votre entreprise.

Pour aider les entreprises à obtenir la visibilité dont elles ont besoin, Akamai API Security fournit une classification et un inventaire automatisés des API pour les utilisateurs internes et externes.

Afin de constituer un inventaire complet, la solution Akamai API Security utilise diverses sources telles que les passerelles d'API, les pare-feux d'applications Web (WAF), les services de cloud publics, le trafic réseau, la documentation API, etc. Cela garantit un suivi des modifications des API et permet de s'assurer que la dernière version est reflétée dans la bibliothèque d'API.

La solution Akamai API Security

Akamai API Security se compose de quatre modules intégrés, offrant une gestion des ressources API et une sécurité de bout en bout.

Découverte
Localisez et inventoriez vos API, ainsi que leurs risques associés issus de l'extérieur comme de l'intérieur

Posture
Découvrez les vulnérabilités et les erreurs de configuration pour accélérer leur résolution et garantir la conformité

Durée d'exécution
Détectez et bloquez les attaques d'API grâce à l'analyse du trafic en temps réel optimisée par l'apprentissage automatique

Tests
Identifiez et corrigez les vulnérabilités tout au long du cycle de vie du développement

Avantages

Catalogue d'API
Identifiez les systèmes, services et applications exposant vos API, avec une taxonomie détaillée

Catalogue de requêtes
Explorez et gérez votre inventaire d'API en fonction des cas d'utilisation ou des cadres réglementaires

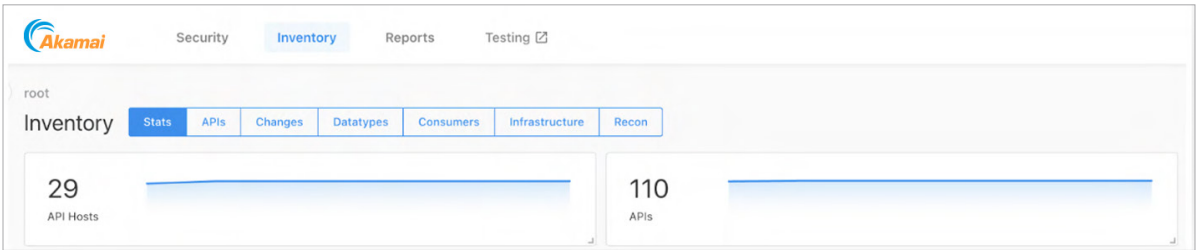
Normes en matière d'API
Téléchargez, affichez et analysez vos fichiers OpenAPI Spec et vos fichiers de règles de linting

Réutilisation des API
Localisez vos API existantes qui effectuent les tâches requises au lieu d'en coder de nouvelles

Le point de départ de la gestion des ressources est le module Découverte. Grâce à une analyse des sources de trafic au sein de votre environnement, la solution détermine le nombre d'API dont vous disposez et les classe automatiquement en fonction de différents cadres de référence.

Catalogue d'API

Akamai API Security établit un catalogue complet de vos API existantes. Ce catalogue identifie les systèmes, services et applications exposant ces API et fournit une taxonomie détaillée de chaque API.

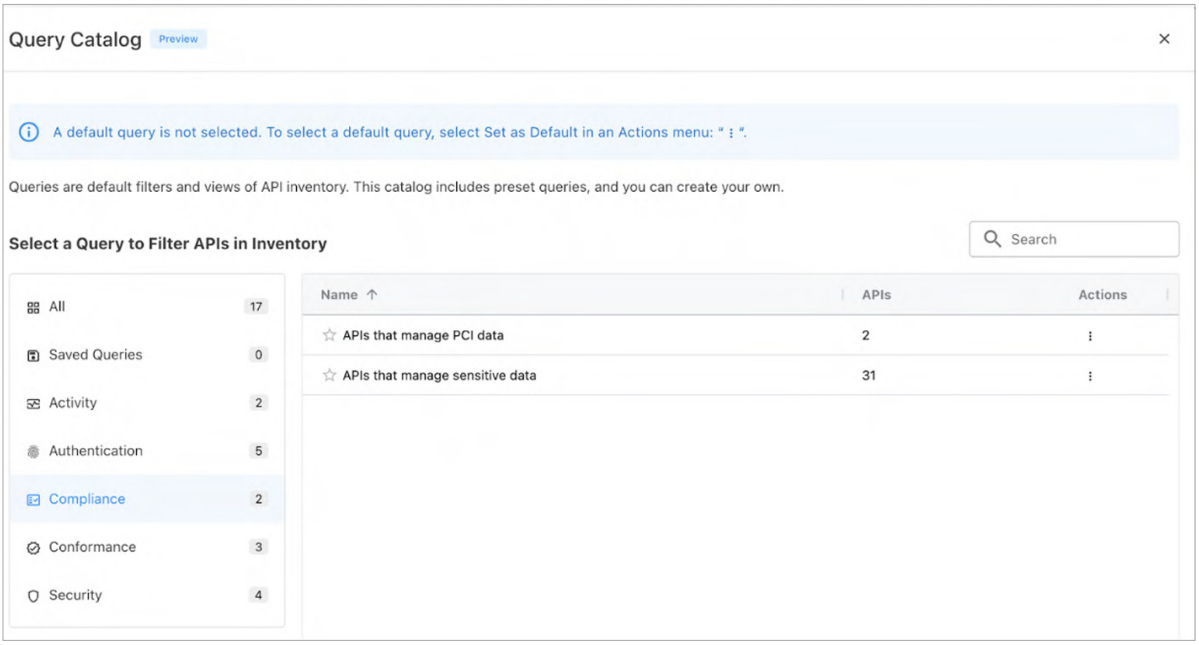


Akamai API Security assure un suivi de toutes les modifications apportées aux API, permettant ainsi aux utilisateurs d'exporter une documentation à jour sous forme de fichier OpenAPI Spec basé sur ces modifications. En outre, le système peut avertir les utilisateurs en cas d'ajout de nouvelles API à leur environnement.

Vous pouvez également utiliser l'outil de gestion d'API intégré à Akamai API Security pour extraire des informations à partir de la bibliothèque d'API, afin de créer une base de données de gestion de configuration (CMDB) API centralisée.

Catalogue de requêtes

Akamai API Security fournit un catalogue de requêtes intégré, qui vous permet d'explorer et de gérer facilement votre inventaire en fonction de vos cas d'utilisation spécifiques ou de vos cadres réglementaires.



Pour chaque API, le système fournit les informations suivantes :

- le propriétaire, le type et le flux d'appels API ;
- les types de données traitées ;
- les méthodes d'authentification prises en charge ;
- la source et l'emplacement de l'API ;
- la confirmation que l'API détectée correspond à la spécification/documentation de l'API ;
- l'infrastructure à l'origine de l'API ;
- un graphique du réseau complet montrant les dépendances des API.

Tirez parti des normes en matière d'API

La solution vous permet également de télécharger, d'afficher et d'analyser vos propres fichiers OpenAPI Spec et/ou fichiers de règles de linting. Le linting est le processus qui consiste à s'assurer que les API sont techniquement correctes et conformes à un ensemble de contraintes supplémentaires, lesquelles sont souvent documentées sous la forme de directives en matière d'API. Akamai inclut un ensemble de règles de linting par défaut pour Spectral, un outil open source qui permet aux développeurs de créer, documenter et gérer des API. En outre, vous pouvez télécharger trois formats de fichiers de spécifications :

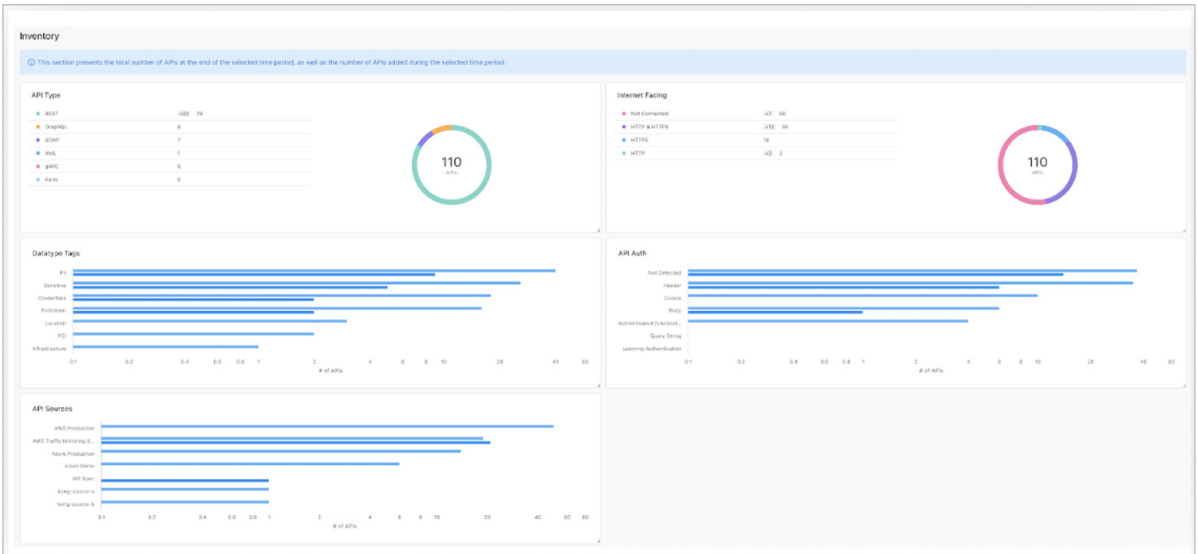
- RESTful API Modeling Language
- Web Services Description Language
- Web Application Description Language

Ainsi, vous pouvez tirer parti des normes existantes en matière d'API ou bien définir les vôtres et les appliquer au sein de votre environnement. Ces normes peuvent être spécifiques à un secteur, telles que les API bancaires ouvertes standard dédiées au secteur des services financiers, qui sont basées sur le Banking Industry Architecture Network (réseau d'architecture du secteur bancaire).

De plus, notre solution API Security détectera également les dérives par rapport à la norme et vous permettra de définir des politiques de résolution pour répondre à ces types de détections. Le système détecte et importe également les API de vos fichiers Spec, et les compare avec le trafic réseau réel. Grâce à Akamai API Security, nous pouvons également détecter et importer des API externes sur la base de simples informations de nom de domaine.

Améliorez la réutilisation de vos API

Grâce à une bibliothèque API complète facilitant les recherches et la navigation, les développeurs pourront localiser les API existantes qui exécutent la tâche requise au lieu d'en coder de nouvelles à partir de zéro. En utilisant notre inventaire et notre catalogue d'API, vous pouvez facilement améliorer la réutilisation de vos API, grâce à une meilleure visibilité au sein de votre environnement pour les développeurs et les professionnels de la sécurité.



En savoir plus

Les API constituent un élément clé de la capacité des entreprises à servir leurs clients, générer des revenus et fonctionner efficacement. Cependant, leur croissance continue, leur proximité avec les données sensibles et l'absence de contrôles de sécurité font des API une cible attrayante pour les pirates d'aujourd'hui. Grâce à une solution complète de sécurité des API comportant des fonctionnalités de découverte, de gestion de posture, de protection de la durée d'exécution et de test de sécurité, les entreprises peuvent réduire leurs risques et se protéger contre les attaques d'API.

En savoir plus sur la façon dont Akamai API Security peut aider votre entreprise.

| Publication 11/24