AKAMAI SOLUTION BRIEF

Akamai API Security for API Asset Management

APIs are growing in scope, scale, and value as organizations become increasingly cloud-centric and digital. They also present a fast-growing risk.

Exposed or misconfigured APIs are prevalent, easy to compromise, and are not only unprotected but often unseen and unmanaged, including highly vulnerable "shadow APIs." And their proliferation makes it difficult to locate and inventory every API across your enterprise.

To help organizations gain the visibility they need, Akamai API Security provides automated classification and inventory of APIs for both internal and external users.

As input for building a comprehensive inventory, the Akamai API Security solution uses various sources like API gateways, web application firewalls (WAFs), public cloud services, network traffic, API documentation, etc. This ensures that API changes are tracked and that the latest version is reflected in the API library.

The Akamai API Security solution

Akamai API Security consists of four integrated modules, providing API asset management and end-to-end security.

Discovery
Locate and inventory your APIs and related risk, from both the inside out and outside in

Posture
Uncover vulnerabilities and misconfigurations to speed remediation and ensure compliance

Runtime
Detect and block API attacks with real-time traffic analysis powered by machine learning

Testing
Find and remediate vulnerabilities during the development lifecycle

Benefits

API catalog
Identify systems, services, and applications exposing your APIs, with a detailed taxonomy

Query catalog
Explore and manage your API inventory aligned to use cases or regulatory frameworks

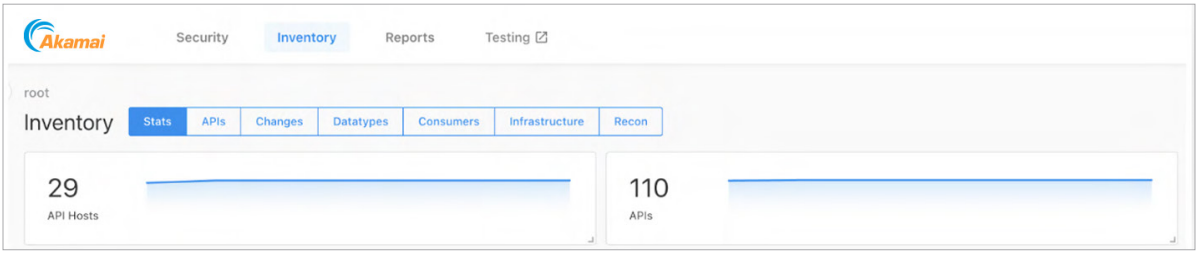
API standards
Upload, view, and analyze your OpenAPI Spec files and linting r ules files

API reusability
Locate existing APIs that perform required tasks instead of coding new ones

For asset management, the starting point is the discovery module. By analyzing traffic sources in your environment, the solution determines how many APIs you have and automatically classifies them based on various frameworks.

API catalog

Akamai API Security presents a comprehensive catalog of your existing APIs. This catalog identifies the systems, services, and applications exposing these APIs and provides a detailed taxonomy of each individual API.

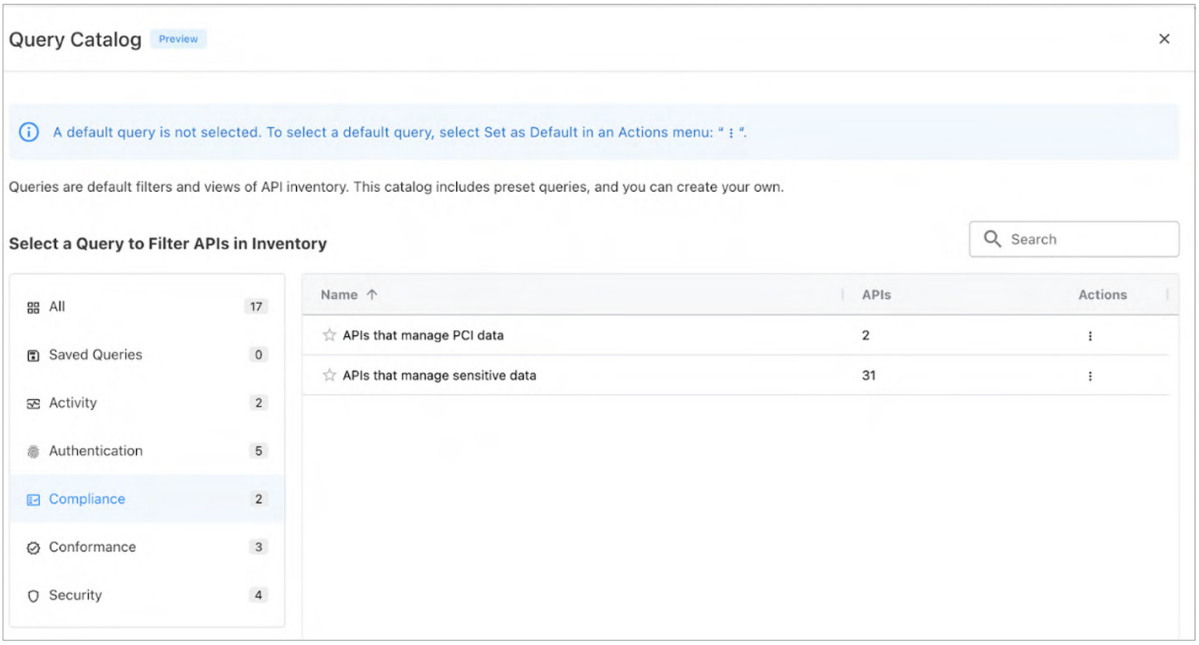


Akamai API Security tracks all changes made to APIs, allowing users to export up-to-date documentation as an OpenAPI Spec file based on these changes. Additionally, the system can notify users if new APIs are added to their environment.

In addition, you can use the management API built into Akamai API Security to extract information from the API library to create a centralized API CMDB (configuration management database).

Query catalog

Akamai API Security provides a built-in query catalog, which lets you easily explore and manage your inventory according to your specific use cases or regulatory frameworks.



For each API, the system will provide the:

- API owner, type, and call flows
- Types of data processed
- Supported authentication methods
- Source and location of the API
- Validation if the detected API matched the API specification/documentation
- Infrastructure behind the API
- Full network graph showing the API dependencies

Leverage API standards

The solution also allows you to upload, view, and analyze your own OpenAPI Spec files and/or linting rules files. Linting is the process of making sure that APIs are technically correct and comply with a set of additional constraints that often are documented in the form of API guidelines. Akamai includes a default set of linting rules for Spectral, an open-source tool that allows developers to create, document, and maintain APIs. In addition, you can upload three formats of spec files:

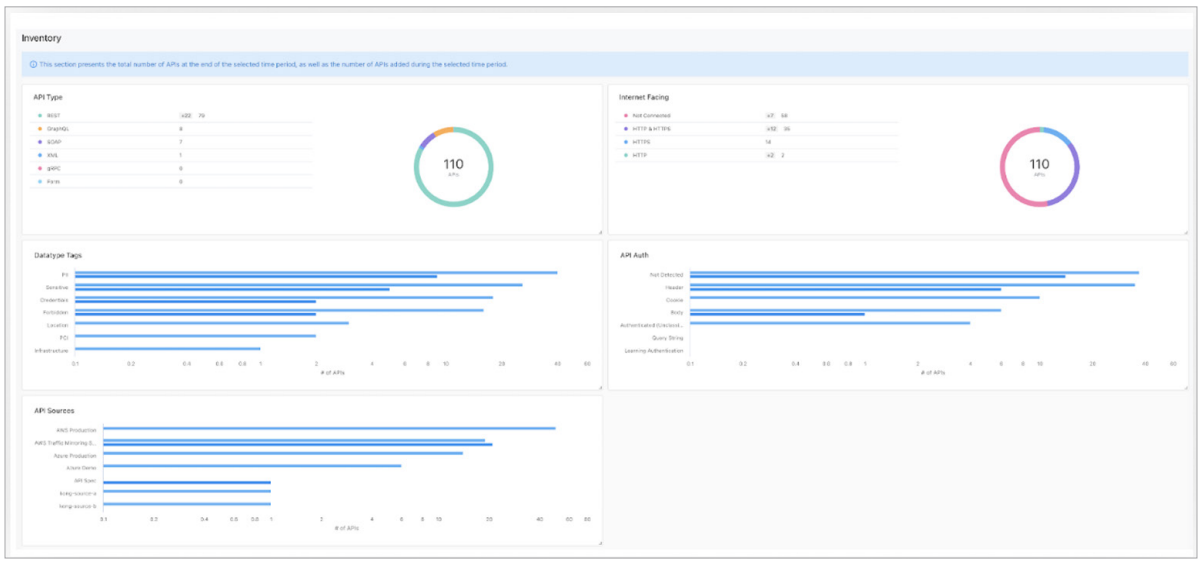
- RESTful API Modeling Language
- Web Services Description Language
- Web Application Description Language

This allows you to leverage existing API standards or define your own and enforce them in your environment. These standards can be sector-specific, for example, standard open banking APIs for the financial services industry on the basis of the Banking Industry Architecture Network.

In addition, our API Security solution will also detect drift from the standard and allow you to define remediation policies to address these types of detections. The system will also detect and import APIs from your Spec files, and compare those with actual network traffic. Using Akamai API Security recon, we can also detect and import external APIs on the basis of simple domain name information.

Drive API reusability

With a comprehensive API library that's easy to search and navigate, developers will be able to locate existing APIs that perform the required task instead of coding new ones from scratch. By using our API inventory and catalog, you can easily drive better reuse of your APIs, as you limit any visibility gaps in your environment for developers and security professionals alike.



Learn more

APIs are a key component of organizations' ability to serve customers, generate revenue, and operate efficiently. However, their continuous growth, proximity to sensitive data, and lack of security controls make APIs an appealing target for today's attackers. Organizations can reduce risk and secure against API attacks with a comprehensive API security solution that provides capabilities for discovery, posture management, runtime protection, and security testing.

Learn more about how Akamai API Security can help your organization.

 | Published 11/24