AKAMAI 솔루션 설명서

API 자산 관리를 위한 Akamai API Security

기업들이 점점 클라우드 중심적이고 디지털화되는 상황에서 API는 범위, 규모, 가치 면에서 증가하고 있습니다. 동시에 API 리스크 역시 빠르게 증가하고 있습니다.

노출되거나 잘못 설정된 API는 빈번하게 발생하고 감염되기 쉬우며 보호되지 않을 뿐 아니라, 취약한 '섀도 API'를 포함해 종종 보이지 않거나 관리되지 않습니다. 그리고 이러한 확산으로 인해 기업 전체의 모든 API를 찾고 인벤토리를 구축하기가 어려워졌습니다.

Akamai API Security는 기업이 필요한 가시성을 확보하도록 내부 및 외부 사용자 모두를 위한 API의 자동 분류 및 인벤토리를 제공합니다.

Akamai API Security 솔루션은 포괄적인 인벤토리 구축을 위한 기반으로써 API 게이트웨이, 웹 애플리케이션 방화벽(WAF), 퍼블릭 클라우드 서비스, 네트워크 트래픽, API 문서화 등의 다양한 소스를 사용합니다. 이를 통해 API 변경 사항을 추적하고 최신 버전이 API 라이브러리에 반영되게 할 수 있습니다.

Akamai API Security 솔루션

Akamai API Security는 API 자산 관리 및 엔드투엔드 보안을 제공하는 4개의 통합 모듈로 구성됩니다.

검색
내부 및 외부에서 API 및 관련 리스크를 찾고 인벤토리화합니다.

체계
취약점과 설정 오류를 찾아내 문제 해결을 가속하고 컴플라이언스를 보장합니다.

런타임
머신 러닝을 통한 실시간 트래픽 분석으로 API 공격을 탐지 및 차단합니다.

테스트
개발 수명 주기 동안 취약점을 찾고 해결합니다.

장점

API 카탈로그
API를 노출하는 시스템, 서비스 및 애플리케이션을 세밀한 분류 체계를 통해 파악합니다.

쿼리 카탈로그
사용 사례 또는 규제 프레임워크에 맞게 API 인벤토리를 탐색 및 관리합니다.

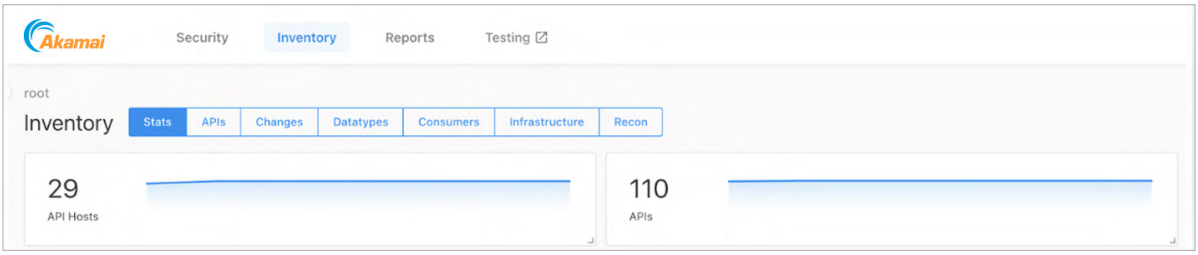
API 표준
OpenAPI Spec 파일과 린팅 룰 파일을 업로드하고 확인하고 분석합니다.

API 재사용
새로운 API를 코딩하는 대신 필요한 작업을 수행하는 기존 API를 찾습니다.

자산 관리는 검색 모듈에서 시작됩니다. 이 솔루션은 사용자 환경에서 트래픽 소스를 분석해 보유한 API 수를 파악하고 다양한 프레임워크를 기반으로 자동으로 분류합니다.

API 카탈로그

Akamai API Security는 기존 API의 포괄적인 카탈로그를 제공합니다. 이 카탈로그는 이러한 API를 노출하는 시스템, 서비스 및 애플리케이션을 파악하고 각 개별 API의 세부 분류 체계를 제공합니다.

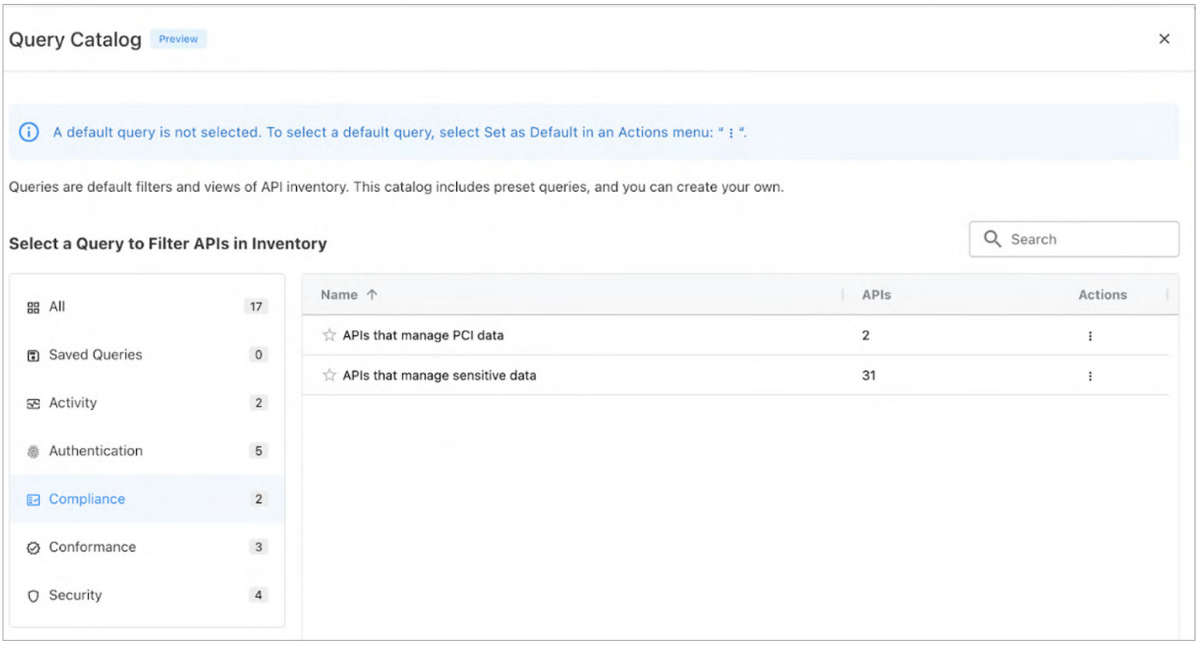


Akamai API Security는 API에 대한 모든 변경 사항을 추적하기 때문에 사용자는 이러한 변경 사항을 기반으로 최신 문서를 OpenAPI Spec 파일로 내보낼 수 있습니다. 또한 새로운 API가 사용자 환경에 추가될 경우 사용자에게 이를 알릴 수 있습니다.

게다가 Akamai API Security에 내장된 관리 API를 사용해 API 라이브러리에서 정보를 추출하여 중앙 집중식 API 설정 관리 데이터베이스(CMDB)를 생성할 수 있습니다.

쿼리 카탈로그

Akamai API Security는 특정 사용 사례 또는 규제 프레임워크에 따라 손쉽게 인벤토리를 탐색 및 관리할 수 있는 쿼리 카탈로그를 제공합니다.



이 시스템은 각 API에 대해 다음을 제공합니다.

- API 소유자, 종류 및 호출 흐름
- 처리된 데이터 종류
- 지원되는 인증 방법
- API의 소스 및 위치
- 탐지된 API가 API 사양 및 문서와 일치하는 경우 검증 진행
- API 이면의 인프라
- API 의존성을 보여주는 전체 네트워크 그래프

API 표준 활용

또한 이 솔루션을 사용하면 자체 OpenAPI Spec 파일 및 린팅 룰 파일을 업로드하고 확인하고 분석할 수 있습니다. 린팅은 API가 기술적으로 옳은지 확인하고 API 가이드라인 형태로 문서화되는 일련의 추가 제약 조건을 준수하는 프로세스입니다. Akamai는 개발자가 API를 생성, 문서화, 유지관리하게 해 주는 오픈 소스 툴인 Spectral에 대한 기본 린팅 룰 세트를 포함했습니다. 또한 다음 3가지 형식의 사양 파일을 업로드할 수 있습니다.

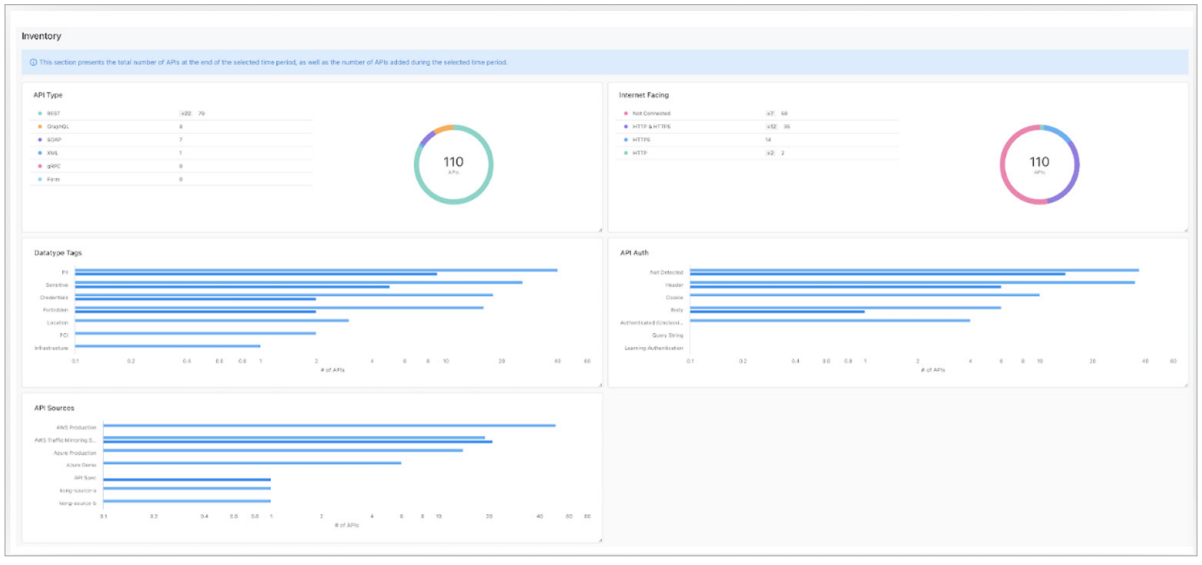
- RESTful API 모델링 언어
- 웹 서비스 설명 언어
- 웹 애플리케이션 설명 언어

이를 통해 기존 API 표준을 활용하거나 사용자 고유의 표준을 정의해 자체 환경에 적용할 수 있습니다. 이러한 표준은 업계별로 구분할 수 있습니다. 예를 들어, 금융 서비스 업계에 대한 오픈 뱅킹 API 표준은 은행 업계 아키텍처 네트워크를 기반으로 합니다.

또한 Akamai의 API Security 솔루션은 해당 표준에서 벗어난 경우를 탐지해 이러한 탐지 종류에 대응하는 문제 해결 정책을 설정할 수 있습니다. 이 시스템은 사양 파일에서 API를 탐지하고 가져오며, 이를 실제 네트워크 트래픽과 비교하기도 합니다. Akamai API Security recon을 사용해 단순한 도메인 이름 정보를 기반으로 외부 API를 탐지하고 가져올 수도 있습니다.

API 재사용 유도

검색 및 탐색이 간편한 포괄적 API 라이브러리를 통해 개발자는 새로운 API를 처음부터 코딩하는 대신 필요한 작업을 수행하는 기존 API를 찾을 수 있습니다. Akamai의 API 인벤토리와 카탈로그를 사용하면 개발자와 보안 전문가 모두의 환경 가시성 격차를 최소화하여 API 재사용을 보다 쉽게 유도할 수 있습니다.



자세히 보기

API는 고객에게 서비스를 제공하고 매출을 창출하며 효율적으로 운영할 수 있게 하는 기업의 핵심 구성요소입니다. 그러나 지속적인 성장, 민감한 데이터에 대한 근접성, 보안 제어의 부재로 인해 API는 오늘날 공격자들에게 매력적인 표적이 되고 있습니다. 기업들은 검색, 체계 관리, 런타임 보호, 보안 테스트를 위한 기능을 제공하는 포괄적 API 보안 솔루션을 통해 리스크를 줄이고 API 공격에 대한 보안을 유지할 수 있습니다.

Akamai API Security가 기업에 어떤 도움을 줄 수 있는지 자세히 알아보세요.