# API 보안 체계 관리 최종 가이드

# 목차

# API 보안이 필수 과제가 된 이유

API를 사용하면 속도가 생명인 분야에서 기업 개발자들이 효율적으로 구축할 수 있습니다. 그러나 API는 개발자에 친화적이고 소프트웨어와 데이터 자산의 상호 운용성을 위한 핵심 요소이기는 하지만, API 보안은 혁신의 속도를 따라가지 못하고 있습니다.

기업의 84%가 지난 12개월 동안 API 보안 인시던트를 경험했으며, 이는 2023년의 78%에서 증가한 수치입니다.[1] 이는 부분적으로 API가 공격자에게도 효율성을 제공하기 때문입니다. 많은 API가 설정 오류, 코딩 오류, 인증 제어 능력 부족 상태에서 구축됩니다.

결과적으로, API 공격은 매우 간단하게 수행할 수 있으며 데이터를 훔치는 직접적인 방법이 될 수 있습니다.

그리고 데이터와 관련해, 전체 API 인벤토리를 보유한 기업의 27%만이 고객 데이터에서 지적 재산에 이르기까지 민감한 데이터를 반환하는 API를 알고 있는 것으로 나타났으며, 이는 2023년의 40%에서 감소한 수치입니다.[2] 공격이 증가하고 가시성이 감소함에 따라 기업은 API 보안 체계를 평가하고 개선할 수 있는 방법이 필요합니다.

1, 2. Akamai, 2024년 API 보안 영향 연구

# 포괄적인 API 보안의 모습

기업의 API 사용이 확대됨에 따라 공격 표면도 확대되어 새로운 보안 문제가 발생합니다.

API 보안과 관련해, 기업이 전통적으로 사용하는 툴(예: API 게이트웨이 및 웹 애플리케이션 방화벽)은 어느 정도 보호 기능을 제공할 수 있습니다. 확인 및 보호하기 어려운 관리되지 않는 API가 무분별하게 확장되는 현상 등 API 자산의 복잡성이 심화됨에 따라 이에 대응하여 변화가 필요하기도 합니다.

API는 기업 보안 계획에서 중요한 위치를 차지합니다. 그리고 오늘날의 API 리스크와 공격 방법을 해결하기 위해 설계된 전용 API 보안 솔루션은 그 계획을 실행하기 위한 가시성과 기능을 제공할 수 있습니다. 공격 경로의 모든 단계를 지원하기 위해 툴이 서로를 보완하는 심층 보안 개념과 유사합니다.

API 검색, 체계 관리, 런타임 보호, 보안 테스트를 제공하도록 구축된 포괄적인 API 보안 플랫폼은 숨겨진 API 리스크를 파악하고, API 공격 경로를 식별하고, 발견된 위협을 실시간으로 방어하는 데 도움이 될 수 있습니다.

관련 e-Book인 'API 검색에 대한 최종 가이드'에서는 API 보안의 첫 번째 핵심 요소인 API 위치 파악에 대해 설명합니다. 기업 전체에서 사용 중인 모든 API를 발견하고 목록을 작성한 다음, 다음 단계는 전반적인 API 보안 체계를 강화하는 것입니다.

써드파티 공급업체의 애플리케이션을 구매해 자체 애플리케이션으로 사용하고, 브랜드를 적용해 판매하는 기업에서는 체계 관리가 특히 중요할 수 있습니다. 예를 들어, 지난 5년 동안 출시된 거의 모든 신차에는 거의 동일한 텔레매틱스 기능이 탑재되어 있습니다. 공격자가 제조업체의 API 엔드포인트에서 취약점을 발견하면, 원격 계정 탈취 공격과 데이터 유출을 위한 쉬운 진입 지점을 확보하게 됩니다.

## 이 가이드에서 다루는 내용

API 체계 관리는 API 수명 주기 전반에 걸쳐 API 보안을 관리, 모니터링, 유지하는 툴을 제공합니다. 이 최종 가이드는 취약점 탐지와 민감한 데이터 보호를 포함해 API 보안 체계 관리의 핵심 요구 사항에 초점을 맞추고 있습니다. 이 가이드에서는 체계 관리 방법을 살펴보고 Akamai API Security 솔루션의 체계 관리 기능을 소개합니다.

# 왜 체계 관리가 필요하나요?

API 체계 관리는 API 보안과 관련해 최선의 노력을 기울일 수 있도록 해줍니다. 어떤 종류의 데이터가 이동하고 있는지, 취약점이나 설정 오류가 있는지, API가 제대로 인증되었는지 등을 확인함으로써 발견된 API의 리스크를 파악할 수 있도록 도와줍니다. API 취약점을 식별하고 신속하게 해결할 수 있는 기능을 통해 공격이 발생하기 전에 시정 조치를 취할 수 있습니다.

포괄적인 체계 관리로 API와 관련된 모든 활동에 대한 가시성을 확보할 수 있으므로 보안 정책을 시행하고, 컴플라이언스를 보장하고, API 생태계의 변경 사항을 감사할 수 있습니다. 체계 관리는 악성 공격, 무단 사용자, 데이터 유출로부터 API를 보호하고 보안을 유지합니다. 이러한 모든 공격은 심각한 평판 손상, 비즈니스 손실, 규제 관련 처벌로 이어질 수 있습니다.

전체 API 인벤토리를 보유한 기업의 27%만이 민감한 데이터를 반환하는 API를 알고 있는 것으로 나타났으며, 이는 2023년의 40%보다 낮은 수치입니다.[3]

3. Akamai, 2024년 API 보안 영향 연구

체계 관리 모범 사례를 구축하면 API 공격 표면을 최소화하고 API 리스크를 크게 줄일 수 있습니다. 체계 관리를 잘 하려면 기업의 API와 민감한 데이터 저장소에 대한 철저한 목록을 작성해야 합니다. 다음 페이지에서는 API 체계 관리의 추가 요소인 취약점 탐지, API 모니터링, 문제 해결에 대해 설명합니다.

- ## 취약점 탐지

  **분석:** 소스 코드의 일반적인 취약점을 검사하고, API가 외부 시스템과 상호 작용하는 방식을 이해하고, 권한 확인 및 인증 기능을 평가합니다.

  **관찰:** API와의 트래픽을 검사해 설정 오류를 식별하고, 취약점을 탐지하고, 기본 API 행동에 대한 이해를 높입니다.

체계 관리는 완전한 API 보안 프로그램의 한 요소에 불과합니다. 또한 포괄적인 사전 제작 테스트를 사용해 취약점이 프로덕션에 도달하지 못하게 하는 것도 중요합니다.

- ## API 모니터링

  프로덕션에서 API 호출을 식별 및 모니터링하고, API 요청을 추적하고, 기준 사용량과의 편차를 탐지하고, API 사용량이 사전 정의된 임곗값을 초과할 때 알림을 생성합니다.

- ## 문제 해결

  코드 변경, 보안 설정 미세 조정 또는 API 결함 패치 적용을 통해 식별된 약점이나 취약점을 해결해 API 보안을 향상하고 규정을 준수하도록 합니다. 우수한 체계 관리는 취약점이 악용되기 전에 해결합니다.

# 필수적인 체계 관리 기능

여러분은 여러분의 API 보안 체계가 충분히 강하지 않다는 것을 이미 알고 있거나 강력하게 의심하고 있을지 모릅니다. 다음은 체계 관리 툴에 반드시 포함되어야 하는 몇 가지 핵심 기능입니다.

- **민감한 데이터 분류**
  퍼블릭 소스에서 제공하는 날씨 데이터를 제공하는 API는 신용카드 정보를 전송하는 API보다 훨씬 덜 중요한 우려 대상입니다. API 체계 관리 툴은 신용카드 정보, 전화번호, SSN(사회 보장 번호), 기타 민감한 데이터에 접속할 수 있는 API의 수와 API를 통해 민감한 데이터에 접속한 사용자 수를 신속하게 파악할 수 있어야 합니다.

- **설정 평가**
  많은 사이버 공격은 네트워크, API 게이트웨이 또는 API 트래픽을 중개하고 보호하는 방화벽의 단순한 설정 오류로 인해 발생합니다. 강력한 체계 관리를 위해서는 로그 파일과 설정 파일을 포함해 인프라와 소프트웨어 설정을 정기적으로 스캔할 수 있는 능력이 필요합니다. 정기적인 스캔은 설정 오류와 취약점을 발견하고 설정의 변화로 인해 발생하는 리스크를 식별하는 데 도움이 됩니다.

- **공격자 신뢰도 점수**
  API 행동, 네트워크 트래픽 패턴, 지리적 위치 데이터, 위협 인텔리전스 피드, 기타 상황에 따른 요인을 포함해 외부 및 내부 신호를 평가하도록 훈련된 고급 머신 러닝 알고리즘을 사용하는

공격자 신뢰도 점수 엔진을 찾아보세요. 이를 통해 탐지된 런타임 인시던트가 악성 활동의 결과인지에 대한 신뢰도를 판단할 수 있습니다. 이 고유한 기능을 통해 고객은 중요한 위협을 신속하게 파악하고, 확률이 높은 공격에 대한 자동적인 문제 해결 및 알림 흐름을 만들 수 있습니다.

- **맞춤형 워크플로우**
  취약점이 확인되면 즉시 조치를 취할 수 있도록 맞춤화 가능한 심각도와 함께 워크플로우를 생성할 수 있어야 합니다. 맞춤형 워크플로우는 문제 티켓 생성부터 주요 이해관계자에게 알림 보내기, 네트워크 설정 업데이트에 이르기까지 다양합니다.

- **자동 생성 문서**
  API 문서는 API의 기능과 사용 방법을 사용자에게 알려줍니다. 보안 API는 사양을 기준으로 컴플라이언스 여부를 평가하고 정확하게 문서화해야 합니다. 문서가 부실하거나 존재하지 않으면 보안 테스트가 더 어려워지고, 탐지되지 않은 취약점이 있는 API가 프로덕션 환경에 도달할 리스크가 높아집니다.

이 문제는 종종 API 개발을 아웃소싱함으로써 악화됩니다. API 보안 프로그램의 성공을 원한다면 문제의 원인과 상관없이 오래된 문서, 미완료 문서 및 문서 누락을 허용하지 말아야 합니다.

OpenAPI Specification(이전 명칭: Swagger)은 표준 인터페이스 설명을 정의합니다. 체계 관리 툴은 모든 API가 적절하게 문서화되고 최신 상태의 문서를 유지할 수 있도록 API의 현재 상태와 미래 상태를 기반으로 완전한 OpenAPI 문서를 자동으로 생성할 수 있어야 합니다.

# 보험 업계 리더, Akamai를 통해 API 보안 체계 강화

소비자들이 오프라인에서 디지털로 이동함에 따라 금융 서비스 기업들은 빠른 속도로 혁신을 이루어야 합니다. 많은 동종 기업과 마찬가지로, 미국의 선도적인 보충 건강 보험 서비스 공급업체인 Aflac도 증가하는 API 보안 문제에 직면했습니다.

Aflac은 이러한 요구사항을 충족하기 위해 Noname API Security Platform(현재 Akamai API Security의 일부)을 선택했습니다. 체계 관리 모듈은 팀이 기업의 API를 통과하는 데이터 종류를 식별하는 데 도움을 주어, 어떤 API가 민감한 데이터에 접속하는지 파악하고 데이터 접속에서 발생하는 모든 비정상을 식별할 수 있도록 합니다.

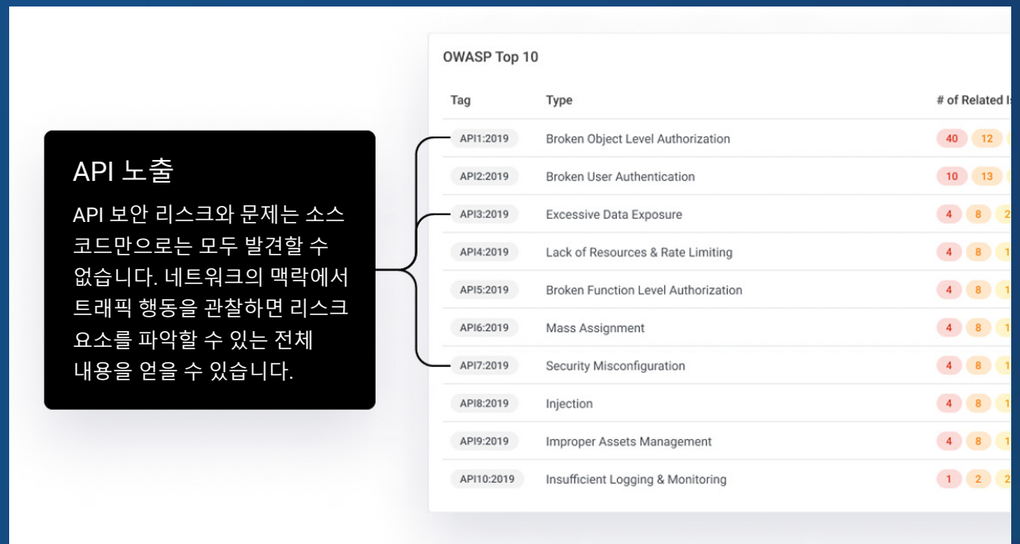
자세한 내용은 Aflac 사례 연구 전문을 통해 확인하세요.

> "API 풋프린트가 크다는 것을 알고 있었기 때문에 모든 API를 완벽하게 파악하고, 운영 현황에 대한 완벽한 가시성을 확보하고, 보안 리스크를 지속적으로 테스트하고 있다는 확신을 갖고 싶었습니다.
>
> — DJ 골즈워디(DJ Goldsworthy), Aflac, 보안 운영 및 위협 관리 부문 부사장

# 체계 관리에 대한 Akamai의 접근 방식

Akamai API Security 솔루션의 체계 관리 모듈은 트래픽, 코드, 설정에 대한 포괄적인 시각을 제공해 기업의 API 보안 체계를 평가합니다. Akamai는 API와 웹 애플리케이션 전반에 걸쳐 실제 공격 표면이 어떤 모습인지 파악하고, API를 통해 이동하는 모든 형태의 민감한 데이터를 찾아내어 민감한 데이터를 보호할 수 있도록 도와줍니다.

간단한 API 설정 오류 때문에 사이버 범죄에 무방비 상태로 노출될 수 있습니다. 해커는 일단 침입하면 빠르게 민감한 데이터에 접속해 이를 유출할 수 있습니다. Akamai API Security 솔루션의 체계 관리 모듈은 다음과 같은 주요 기능을 제공합니다.



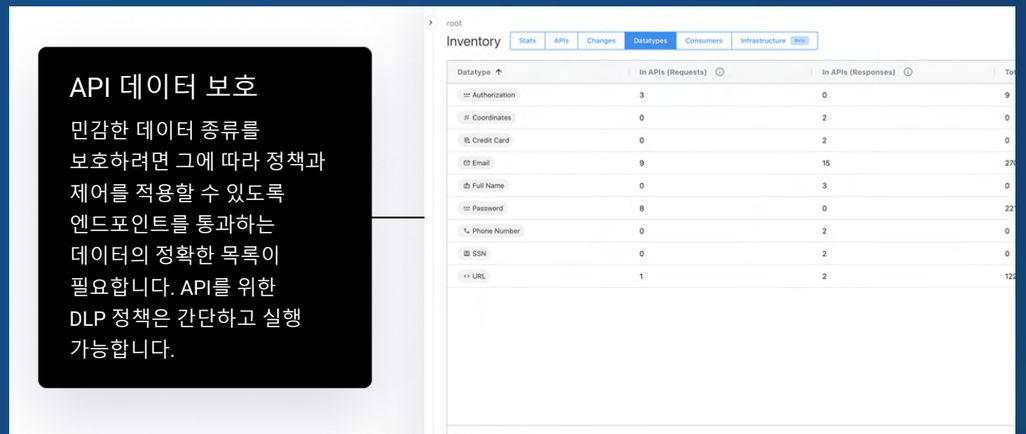

- 온프레미스, 하이브리드, 퍼블릭 클라우드에서 아웃오브밴드 통합으로 지속적인 API 검색 지원
- 스키마, 네트워크 배치, 데이터 종류에 대한 세부 정보를 포함하는 검색 가능한 간단한 API 인벤토리
- 자동화된 API 문서 생성(OAS/Swagger)
- 우선순위 지정을 통한 API 설정 오류 및 취약점에 대한 맥락 인식 분석
- OWASP API 보안 상위 10개 항목의 모든 취약점 탐지
- 민감한 데이터와 API 변경 사항의 자동 검색 및 분류

## API 노출

API 코드 내의 리스크를 발견하는 것 외에도, 일반적인 행동과 비정상적인 행동을 구분하고 네트워크의 맥락 내에서 API 트래픽을 관찰하는 것도 중요합니다.

Akamai API Security 솔루션의 체계 관리는 로그 파일, 과거 트래픽의 리플레이, 설정 파일 등을 포함하여 가능한 한 가장 광범위한 소스 집합을 조사해 취약점을 탐지합니다. 이 솔루션은 OWASP API 보안 상위 10개 항목에 포함된 모든 취약점을 탐지하고, 데이터 유출, 권한 확인 문제, 남용, 오용, 데이터 손상으로부터 API를 보호합니다.

Akamai는 잠재적 취약점을 지능적으로 식별하고 우선순위를 지정합니다. 취약점은 WAF, API 게이트웨이, SIEM 및 ITSM 툴, 워크플로우 툴, 기타 서비스와의 통합을 통해 수동, 반자동 또는 완전 자동 방식으로 해결할 수 있습니다.




## API 데이터 보호

민감한 데이터 종류를 보호하려면 그에 따라 정책과 제어를 적용할 수 있도록 엔드포인트를 통과하는 데이터의 정확한 목록이 필요합니다. API를 위한 DLP 정책은 간단하고 실행 가능합니다.

컴플라이언스는 API 사용의 증가와 함께 완전히 새로운 차원으로 발전하고 있습니다. 증가하는 공격 표면에 대응하기 위해 일련의 규제가 등장했습니다. 규제를 받는 산업은 이제 컴플라이언스를 위한 계획에 API를 고려해야 합니다.

Akamai API Security 솔루션의 체계 관리 모듈은 신용카드, SSN, 주소, 보험 정보 등과 같은 모든 PII(개인 식별 정보)를 포함해 API를 통해 이동하는 모든 형태의 민감한 데이터를 식별합니다. Akamai는 이러한 데이터 종류에 대한 접속을 줄이고 데이터 관리 프레임워크를 구축함으로써, 민감한 데이터가 필요한 곳에 있고 악성 위협으로부터 안전하게 보호받도록 도와드립니다.

# API 체계 관리가 지원하는 방법

고객, 파트너 또는 벤더사가 디지털 방식으로 기업과 소통할 때마다, (종종 민감한) 데이터의 신속한 교환을 촉진하는 API가 배후에서 작동합니다. 기업 전체의 모든 API에 대한 가시성을 확보하고 리스크 속성을 평가하는 것(예: 민감한 데이터를 반환하는 API가 무엇인지 확인)은 빠르게 증가하는 공격 기법으로부터 기업을 보호하는 데 도움이 될 수 있습니다. 또한, API 보안 체계 관리는 데이터 유출을 방지하기 위한 글로벌 규정을 준수하는 데 도움이 될 수 있습니다.

# 모든 API를 보고 보호할 것을 요구하는 데이터 보호 규정을 알아보세요.

## 맞춤형 Akamai API Security 데모를 예약해 Akamai가 어떻게 도움을 드릴 수 있는지 알아보세요.

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 **akamai.com** 및 **akamai.com/blog**를 확인하거나 **X**(기존의 Twitter), **LinkedIn**에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 12월 발행.

Akamai