AKAMAI 제품 설명서

Akamai와 Apiiro가 함께 제공하는 코드부터 런타임까지의 보안

API는 최신 애플리케이션을 강화하고, 혁신을 주도하고, 원활한 디지털 경험을 가능하게 합니다. 그러나 API를 노리는 공격 기법이 증가하고 있기 때문에 API를 제대로 보호하지 않으면 기업이 심각한 리스크에 노출될 수 있습니다. Akamai와 Apiiro는 이 문제를 해결하기 위해 Akamai API Security를 Apiiro의 ASPM(Application Security Posture Management) 플랫폼과 통합했습니다. 이 통합 솔루션은 기업이 코드에서 런타임에 이르기까지 API를 보호할 수 있도록 지원해, 보안에 영향을 미치지 않으면서 리스크를 줄이고, 문제 해결을 간소화하고, 혁신의 속도를 높입니다.

API 기반의 리스크를 효과적으로 관리하기 위해서는 가시성이 필수입니다. 취약점을 신속하게 파악하고 대응하는 것이 중요합니다. 보안팀은 문제를 탐지하면 개발자와 협력해 리스크가 높은 취약점을 최대한 빨리 해결해야 합니다. 그러나 대부분의 솔루션은 식별된 리스크를 코드 소스와 연결하지 못하기 때문에 보안팀과 개발팀은 어려움을 겪습니다. Akamai와 Apiiro의 통합은 엔드투엔드 가시성과 맥락을 제공함으로써 이러한 단절을 해결합니다.

Akamai API Security는 트래픽에서 API를 발견하고, 공격으로 이어질 수 있는 잘못된 설정과 취약점을 분석합니다. 각 취약점에 대해 개발자에게 발생한 상황, 리스크를 초래하는 이유, 문제 복제 방법 등 자세한 인사이트를 제공합니다. 이러한 실행 가능한 정보는 코드에 대한 심층 분석을 통해 발견된 API의 포괄적인 목록을 유지 관리하는 Apiiro 플랫폼으로 전달됩니다. Apiiro의 플랫폼은 Akamai가 식별한 API와 취약점을 기존 API 라이브러리와 자동으로 매칭해 각 취약점을 관련 저장소, 특정 코드 라인, 책임 있는 코드 소유자에 매핑합니다.

이렇게 원활한 통합을 통해 Akamai API Security가 탐지한 API 리스크의 근본 원인까지 동적으로 추적할 수 있습니다. 개발자는 취약점을 신속하게 해결하는 데 필요한 모든 정보를 갖고 있기 때문에 해결 프로세스의 속도와 효율성을 모두 높일 수 있습니다. 또한, 이 접근 방식은 보안팀과 개발팀 간의 원활한 소통과 협업을 강화해 API 보안 워크플로우에서 중요한 간극을 메워줍니다.

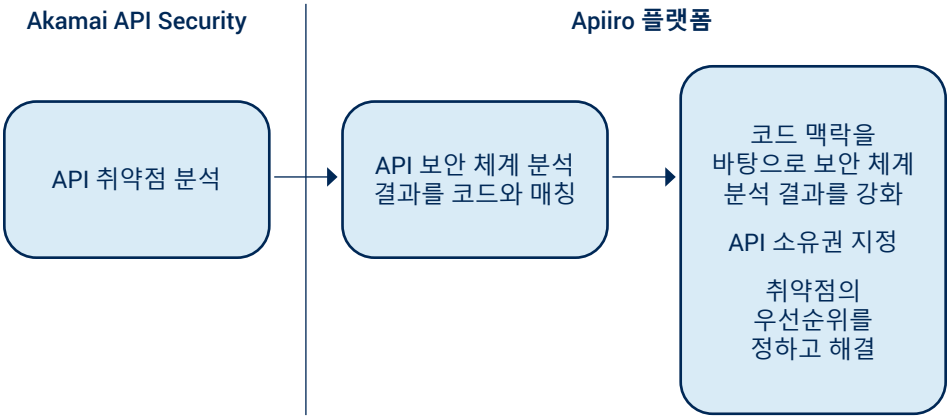
기업이 누릴 수 있는 장점

가시성 강화
API 취약점 맥락을 통해 코드 분석 강화

문제 해결 시간 단축
API 취약점을 소스 코드에 자동으로 매핑하고 개발팀 소유자 지정

리스크 프로필 감소
API 트래픽을 코드와 연관시키고 잠재적 영향을 기반으로 취약점의 우선순위를 지정해 취약점 조사 간소화

작동 방식



주요 사용 사례

- 리스크 평가 자동화: API와 관련 코드를 지속적, 종합적으로 분석해 리스크를 식별합니다.
- 리스크 방어 가속화: API 취약점의 우선순위를 정하고, 이를 소스 코드에 매핑한 뒤 담당자를 지정해 평균 문제 해결 시간(MTTR)을 단축합니다.
- 사전 프로덕션 보호 장치: 보안 조치를 개발 워크플로우에 통합해 API 변경 사항을 선제적으로 모니터링하고 관리합니다.

결론

Akamai–Apiiro 서비스는 엔드투엔드 가시성과 유용한 정보를 제공하는 독자적인 API 보안 접근 방식을 제시합니다. 이번 통합으로 Apiiro 고객은 코드를 넘어 런타임까지 보호 범위를 확장해 보다 포괄적인 API 보안을 실현할 수 있습니다. 동시에 Akamai 고객은 API 리스크를 코드상의 근본 원인까지 추적하고 적절한 팀에 할당해 문제 해결의 효율성을 높일 수 있습니다. Akamai와 Apiiro는 복잡성이 지속적으로 증가하는 API 환경에서 기업이 보다 안전하고 자신 있게 혁신할 수 있도록 지원합니다.

©2025 Akamai Technologies | 지원 | | 2025년 2월 발행