AKAMAI 제품 설명서

API Security

Akamai API Security는 비즈니스 로직 남용과 데이터 유출로부터 API를 보호하는 스마트한 방법입니다

진화하는 API 위협

API는 파트너, 공급업체, 고객과 연결하는 방식으로 매일 기업 성장을 이끕니다. 하지만 모든 API는 또한 공격표면을 확장하며, 공격자는 이를 알고 있습니다. API 공격은 빠르게 성장하고 진화하며, 웹 애플리케이션과 API 보안이 탐지하지 못할 수 있는 방식으로 이루어지는 경우가 많습니다. 또한, API에 대한 포괄적인 인벤토리가 없으면 사각지대가 발생하여 기업의 API를 보호할 수 없습니다.

Akamai API Security를 선택해야 하는 이유

Akamai 플랫폼은 개발부터 프로덕션까지 라이프사이클 전체에서 API를 보호합니다. API Security는 파트너, 공급업체, 사용자에게 API를 노출하는 기업을 위해 구축되었습니다. API를 발견하고, 리스크 체계를 파악하고, 행동을 분석하고, 내부에 숨어 있는 위협을 차단합니다.

API Security의 핵심 기능

탐색

기업에는 아무도 모르는 API가 생각보다 많습니다. 그러나 정확한 인벤토리가 없으면 기업이 다양한 보안 리스크에 노출됩니다. Akamai가 불확실한 상황을 멈출 수 있도록 다음과 같이 도와드리겠습니다.

- 설정이나 종류에 관계없이 RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, gRPC 등 모든 API 탐색 및 인벤토리화
- 휴면, 레거시, 좀비 API 탐지
- 잊히거나, 방치되거나, 알려지지 않은 섀도 도메인 탐지
- 사각지대를 제거하고 잠재적인 공격 경로 발견

테스트

애플리케이션은 전에 없이 빠른 속도로 개발되고 있습니다. 따라서 보안 취약점이나 설계 취약점이 잘 발견되지 않을 수 있습니다. Akamai의 API 보안 테스트 스위트를 활용해 다음과 같은 이점을 얻으세요.

- 악성 트래픽을 시뮬레이션하는 150개 이상의 테스트를 자동으로 실행해 OWASP API 보안 10대 위협을 비롯한 다양한 위협 탐지
- API가 프로덕션 환경에 들어가기 전에 취약점을 발견해 공격 성공 리스크 경감
- 확립된 거버넌스 정책 및 룰에 따라 API 사양 검사
- 온디맨드 또는 CI/CD 파이프라인의 일부로 API 중심 보안 테스트 실행

기업이 누릴 수 있는 혜택

탐색
API 공격표면을 이해합니다. API 인벤토리 및 문서 업데이트 비용을 절감합니다. 규제 요건 및 내부 정책 컴플라이언스를 개선합니다.

테스트
문제를 조기에 발견해 해결 비용을 줄입니다. 속도 저하 없이 코드 품질을 개선합니다. 시장 출시 시간을 단축해 매출을 증대합니다.

탐지
정확히 어떤 일이 발생했는지 파악해 중요한 사업 관련 컨텍스트를 확보합니다. 문제가 발생한 이유를 추론하고 잠재적인 영향을 파악합니다. 해결 방법을 정합니다.

대응
공격을 즉시 차단해 리스크를 줄입니다. 악용되기 전에 취약점을 해결해 비용을 절감합니다. 다운타임으로 인한 매출 손실을 줄입니다.

Akamai

탐지

간단한 API 설정 오류 때문에 사이버 범죄에 무방비 상태로 노출될 수 있습니다. 해커는 일단 내부에 침투하면 민감한 데이터에 빠르게 접속해 유출할 수 있습니다. Akamai 플랫폼을 활용해 다음 성과를 실현하세요.

- 인프라를 자동으로 스캔해 설정 오류와 숨겨진 리스크 발견
- 주요 이해관계자에게 취약점을 알리는 맞춤형 워크플로우 생성
- 민감한 데이터에 접속할 수 있는 API 및 내부 사용자 식별
- 탐지된 문제에 심각도 순위를 할당해 해결 우선순위 지정

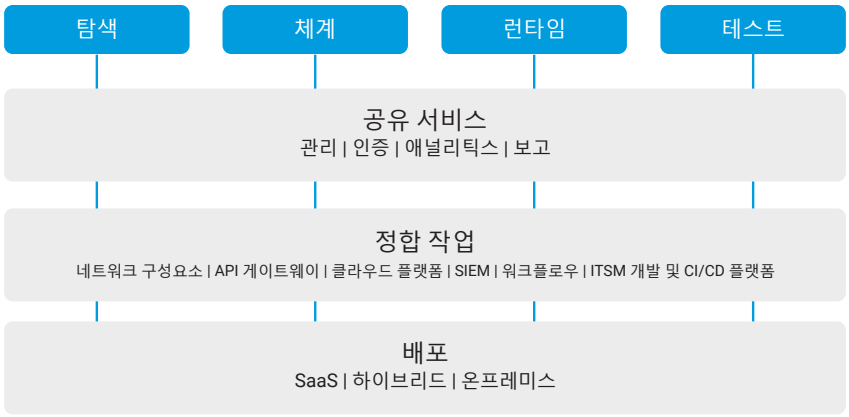
대응

기업은 언제든 공격받을 수 있는 상황이기 때문에, 공격을 실시간으로 탐지하고 차단할 수 있어야 합니다. Akamai의 인공 지능 및 머신 러닝 기반 비정상 탐지 기능을 사용해 다음을 실현하세요.

- 데이터 변조 및 유출, 정책 위반, 의심스러운 행동, API 공격 모니터링
- 추가적인 네트워크 변경이나 설치하기 어려운 에이전트 없이 API 트래픽 분석
- 기존 워크플로우(티켓팅, SIEM[보안 정보 및 이벤트 관리] 등)와 통합해 보안 및 운영팀에 알림 제공
- 부분적으로 또는 완전히 자동화된 해결을 통해 실시간으로 공격 및 오용 방지

Akamai만의 차별화 요인: 엣지에서의 차단

Akamai App & API Protector는 Akamai Connected Cloud를 통해 실행되는 앱과 API에 대한 API 위협을 발견 및 방어하고, API Security에서 발견되지 않은 잠재적인 위협이 포함된 모든 트래픽을 차단합니다. Akamai의 API 보안을 함께 배포하면 API에 대한 포괄적이고 지속적인 가시성을 확보하고 모든 애플리케이션 자산에서 API 보안 문제를 발견, 감사, 탐지, 대응할 수 있습니다.



API Security가 어떻게 작동하는지 궁금하세요? akamai.com/apisecurity에서 Akamai팀과의 일정을 예약하세요.

| 2024년 6월 발행