

헬스케어 업계를 위한 API 보안

헬스케어 서비스 공급업체가 API 위협을 식별하고 방어할 수 있도록 Akamai API Security가 어떻게 지원하는지 확인하세요.

API는 시스템, 디바이스, 사람 간에 원활히 데이터가 교환되도록 지원하여 환자 치료를 개선하고 업무를 간소화합니다. 하지만 API를 통해 오가는 데이터는 환자 기록부터 보험 정보까지 매우 민감한 경우가 많아 공격자에게 주요 표적이 됩니다.

API가 리스크에 노출되어 있나요? [2024년 API 보안 영향 연구](#)에서 얻은 다음 결과를 고려해 보세요.

- 2024년에는 헬스케어 기업의 85%가 API 보안 인시던트를 경험했는데, 이는 2023년의 79%보다 증가한 수치입니다.
- 전체 API 인벤토리를 보유한 기업 중 24%만이 민감한 데이터를 교환하는 API를 알고 있으며 이는 2023년의 40%보다 낮은 수치입니다.

한편, 여러 업계의 IT 및 보안 리더들은 API 보안 인시던트를 해결하고 복구하는 데 평균 94만 3000달러 이상을 지출했다고 보고했습니다.

API는 원활한 데이터 교환을 가능하게 해 헬스케어 기관이 상호운용성과 운영 효율성을 크게 높일 수 있도록 지원합니다. 하지만 API는 공격 표면도 확장시킵니다. 애플리케이션, 클라우드 환경, AI 모델 전반으로 API가 확산되면서 그만큼 보안 리스크도 커지고 있습니다. 헬스케어 기관은 설정이 잘못됐거나, 테스트가 제대로 이뤄지지 않았거나, 접속 제어 없이 구축된 API를 의도치 않게 배포하고 있는 경우가 많습니다. 이로 인해 공격자가 보다 쉽게 데이터를 탈취하거나 운영을 방해할 수 있게 됩니다.

Akamai API Security는 공급업체가 보유한 API의 수와 해당 API를 통해 교환되는 데이터 종류를 파악할 수 있도록 지원하며, 공급업체가 언제든지 해당 데이터를 보호할 수 있는 수단을 제공합니다. 문제는 많은 헬스케어 전문가들이 API를 기존 애플리케이션 보안의 연장선으로만 인식한다는 점입니다. 하지만 AppSec과 DevOps 담당자들은 API가 이 두 분야 모두에 가져오는 고유한 보안 과제를 별도로 고려해야 합니다. 최신 헬스케어의 기반 기술인 API는 기존 보안 틀로는 해결할 수 없는 새로운 유형의 리스크를 수반합니다.

강력한 API 거버넌스 및 보안 프로그램을 구축하려면, 기업은 신뢰할 수 있는 API 보안 벤더와 협력해야 합니다. 헬스케어 업계에서 모니터링되지 않는 데이터 흐름은 중대한 리스크를 유발할 수 있지만, 여전히 많은 기업들은 자사 API에 대한 포괄적인 인벤토리를 갖고 있지 않습니다. Akamai API Security는 모든 활성 API를 식별하고 해당 API가 처리하는 데이터 유형을 분석해, 기관이 전체 API 환경에 대한 가시성을 확보할 수 있도록 지원합니다. 이후 자산 관리, 민감한 데이터 분석, 비정상 탐지, API 보안 테스트, CI/CD 통합, 수동 및 자동화된 문제 해결 기능을 통해 지속적인 보호를 제공합니다. 또한 써드파티 워크플로우와도 원활하게 통합됩니다.

도전 과제



API는 공격 표면을 확장합니다.



2024년, 헬스케어 기업의 약 85%가 API 보안 인시던트를 경험한 것으로 나타났습니다.

Akamai API Security가 API 위협을 해결하는 방법

Akamai의 솔루션은 헬스케어 기관이 API 자산을 보호할 수 있도록 특별히 설계되었습니다.

포괄적인 API 발견

RESTful, GraphQL, SOAP, XML-RPC, gRPC를 등 비즈니스 환경에 있는 API를 식별하고 인벤토리를 구축합니다. API 게이트웨이의 보호를 받지 못하는 미관리 또는 노후된 API를 탐지하고, 각 API의 속성과 메타데이터에 대한 가시성을 제공합니다.

API 행동 분석 및 위협 탐지

AI 기반 분석을 활용해 데이터 유출, 무단 접속, 설정 오류, 의심스러운 활동과 같은 보안 리스크를 자동으로 식별합니다. 지속적인 모니터링과 비정상 탐지를 통해 잠재적 위협에 선제적으로 대응합니다.

API 보호 및 보안 격차 해소

공격을 실시간으로 차단하고, 보안 설정의 오류를 수정하고, 방화벽 룰을 자동으로 업데이트해 악성 트래픽을 차단합니다. WAF, 티켓팅 시스템, SIEM 플랫폼 등 기존 보안 생태계와 원활하게 통합해 대응 역량을 강화합니다.

배포 전 API를 선제적으로 테스트

API가 프로덕션 단계에 도달하기 전에, 개발 라이프사이클의 일부로 해당 API를 철저히 테스트해 비즈니스 로직의 결함, 설정 오류, 기타 취약점을 사전에 파악합니다. 기업은 보안 테스트를 초기 단계부터 통합해 리스크를 선제적으로 해결하고 API 방어 체계를 강화할 수 있습니다.

Akamai API Security

API 발견에서 리스크 분석, API 테스트, 컴플라이언스까지



자세한 내용은 [API 보안 페이지](#)를 방문하거나 [Akamai 영업팀](#)에 문의하세요.