Akamai 고객 사례

혁신적인 의료 서비스의 원동력인 API를 보호하는 Novant Health

가시성, 데이터 보호, 시프트 레프트 테스팅을 통한 API 리스크 발견 및 완화

보안 취약점 식별 | 선제적 리스크 완화 | 개발자의 효율성 개선

포괄적이고 지역사회 중심의 헬스케어 시스템을 통해 얼마나 많은 생명을 개선할 수 있을까요? Novant Health는 이 질문에 다음과 같은 놀라운 답변을 제공합니다.

- 개인병원 방문 680만 건
- 입원 환자 수 15만 5964명
- 응급실 방문 60만 2590건
- 2만 2082명 출생

또한 이러한 수치를 통해 의료 기관에서는 API 침해를 통해 민감한 데이터를 노리는 위협 행위자로부터 누구와 무엇을 보호해야 하는지를 명확하게 파악할 수 있습니다.

위험 요소 파악

Novant Health는 900개 이상의 지역에 걸쳐 16개의 의료 센터에서 1,900명 이상의 의사가 근무하고 있는 비영리 통합 시스템입니다. 3만 6000여 명의 팀원과 협력 의사를 보유하고 있으며 윈스턴세일럼에 기반을 두고 노스캐롤라이나와 사우스캐롤라이나에서 의료 서비스를 제공하고 있습니다.

다양한 디지털 이니셔티브를 통해 환자 진료를 더욱 효과적이고, 개인맞춤화하며, 효율적으로 만듭니다. API는 이러한 혁신의 핵심적인 역할을 하고 있으며 애플리케이션, 디바이스, 시스템 간의 원활한 환자 데이터 교환을 가능하게 합니다. 실제로 API는 매우 중요한 요소이기 때문에 Novant는 동급 최고의 API 제품 개발을 보장하기 위해 인력, 지식, 리소스로 구성된 우수 센터(COE)를 구축했습니다.

NOVANT HEALTH

위치

노스캐롤라이나주
윈스턴세일럼
novanthealth.org

업계

헬스케어 및 생명과학

솔루션

API Security

Akamai

팀은 처음부터 API 보안을 최우선 순위로 생각했고, API 중심 공격이 의료 서비스 제공업체에 미치는 영향을 연구했습니다. 이들이 발견한 업계 통계는 부정적인 의미로 놀라웠습니다. 예를 들어, 의료 데이터 유출의 평균 비용은 970만 달러입니다. 또한 의료 기관의 79%가 지난 12개월 동안 API 보안 인시던트를 경험했습니다.

문제 파악

API COE는 첫 번째 업무로 Novant의 전체 조직에 걸쳐 API 보안 수준을 개선해야 한다고 결정했습니다. Novant가 가지고 있던 유일한 솔루션은 웹 애플리케이션 방화벽(WAF)이었습니다. 이런 툴은 이미 알려진 공격은 방어합니다. 하지만 오늘날의 의료 조직은 다음을 포함한 API 보안에 대해 보다 포괄적인 접근 방식을 필요로 합니다.

- 조직의 IT 환경 내에 존재하는 API의 수에 대한 가시성
- 처리되는 데이터 유형과 같은 각 API의 위험 속성에 대한 통찰력
- 설정 오류와 같이 공격자가 악용하는 부분을 밝혀내는 것을 포함한 조직의 API 보안 태세에 대한 심층 분석
- API 비즈니스 로직의 결함을 악용하는 공격 차단

Novant COE 팀은 또한 시프트 레프트 또는 개발 초기 단계에 보안을 포함시키려는 조직의 노력에서 주요 격차를 파악했습니다. Docker 컨테이너를 테스트할 수 있는 툴이 있었지만 API 개발을 위한 솔루션이 필요했습니다. 환자 기록과 같은 민감한 데이터가 걸려있는 상황에서, Novant COE 팀은 API 보안에 100% 집중하는 인력 및 제품을 보유한 벤더를 찾아야 한다는 데 동의했습니다.

자각하는 순간

Novant COE는 API 보안에 대한 포괄적인 접근 방식을 알게 된 후 Noname Security(Akamai가 인수함)와 회의를 시작했습니다. Novant의 IT 환경에 있는 모든 API에 대해 심층적인 보안 태세 관리 분석을 함께 진행했습니다. Novant COE는 Noname API 보안 플랫폼(현재 Akamai API Security의 일부)을 사용해 중대한 보안 영향을 끼칠 수 있는 Azure 취약점을 식별했습니다.

> “Akamai는 Novant Health의 상당한 격차를 해소해주었으며, 공격자들이 가장 자주 노리는 자산 중 하나에 대해 더 명확한 가시성을 제공했습니다. API 생태계에서 발견된 조치 가능한 보안 취약점들은 이미 그 가치를 입증했습니다. Novant Health에서 데이터 자산의 보호는 우리의 최우선 순위입니다. Akamai는 이러한 가치와 부합하며, 우리의 전반적인 데이터 보안 스택 내에서 기본적인 역량으로 자리잡았습니다.
>
> - **저스틴 P. 버드(Justin P. Byrd)**
> Novant Health 데이터 플랫폼 및 통합 부사장

플랫폼의 API 보안 태세 관리 솔루션은 Novant의 클라우드 환경에서 일부 API 요청이 WAF 툴을 통해서가 아니라 WAF 툴을 우회해 들어오고 있다는 것을 밝혀냈습니다. WAF가 보호할 수 없는 '열린 문'을 통해 위협 공격자들이 WAF를 우회해 Novant의 API를 반복적으로 공격하고 있었습니다. Novant는 이 공격에 노출된 상태였는데, 이를 인지하지 못하고 있었습니다.

Akamai가 제공한 인사이트는 충격적이었고 즉각적으로 큰 도움이 되었습니다. Novant Health의 API를 안전하게 개발하고 유지하려면 완전하게 보호된 클라우드 작업 공간이 필요합니다. Novant의 부사장인 저스틴 P. 버드(Justin P. Byrd)와 그의 팀은 Akamai 가 적극적으로 API 보안 태세 관리 솔루션을 적용하고 발견된 보안 격차를 찾아 완화하는 것에 깊은 인상을 받았습니다.

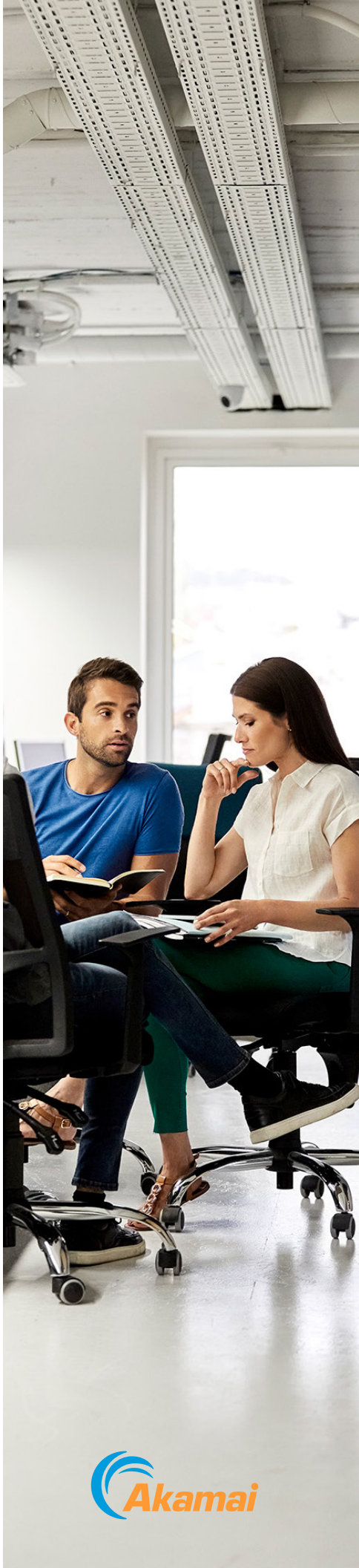
COE 팀은 초기 발견을 토대로 이제 API의 설정 오류와 숨겨진 위험을 지속적으로 확인하는 Akamai API 보안 태세 관리 솔루션의 자동화 기능을 사용하게 되면서 이를 사전에 완화하기 위한 조치를 취할 수 있습니다. 여기에는 어떤 API와 내부 사용자가 민감한 데이터에 접근할 수 있는지 식별하는 기능이 포함됩니다.

수백만 건의 환자 상호작용을 포함해 건강 데이터를 관리하는 Novant와 같은 기업에게 어떤 API가 민감한 정보와 관련되어 있는지 파악하는 것은 환자, 의료 제공자, 규제 기관과의 신뢰를 구축하고 유지하는 데 매우 중요합니다.

보안과 비즈니스 가치를 모두 실현

실무 경험이 있는 엔지니어링 리더들로 구성된 Novant COE의 또 다른 우선순위는 조직의 API 테스팅에 보안을 포함시키는 것이었습니다. 개발 속도는 모든 API에 필수적이며, 특히 환자 치료에서 API가 중요한 역할을 하는 Novant와 같은 기업에는 더욱 중요합니다. 하지만 빠른 개발에 대한 압박으로 인해 개발자들이 프로덕션으로 서두르는 과정에서 취약점이나 설계 결함이 발견되지 않은 채 넘어가기 쉽습니다.

COE는 모든 API에 구현된 보안 조치를 평가하기 위한 신뢰할 수 있는 API 테스팅 기능을 찾고 있었습니다. 이는 인증 메커니즘, 권한 부여 제어, 데이터 무결성 및 암호화 프로토콜과 같은 변수들의 취약점을 식별하기 위한 포괄적인 테스트를 수행하는 것을 포함합니다.



물론 새로운 보안 툴을 구축할 때 성공 여부는 기능뿐만 아니라 주요 이해관계자의 참여에 달려 있습니다. 개발자는 보안의 중요성을 잘 알고 있지만, 속도를 중요하게 생각하기 때문에 일반적으로 익숙하지 않은 툴로 인해 속도가 느려지는 것을 경계합니다.

Novant Health도 처음에는 마찬가지였습니다.

Novant 팀은 Akamai와 더 많이 협력하면서, 개발자들이 업무를 안전하게 수행하고 효율성을 높이는 방식으로 일할 수 있도록 도와주는 여러 기능들을 파악했습니다. 예를 들어, Akamai API Security의 Active Testing은 프로세스에서 나중에 문제해결에 시간이 많이 소요될 수 있는 중대한 실수들을 사전에 발견합니다.

또한, COE는 이 솔루션을 활용해 개발자들에게 효율성을 높이기 위한 간략한 방법을 제공할 수 있었습니다. 이 솔루션이 비보안 QA 검사도 진행한다는 사실을 몰랐던 COE 팀원들은 놀라워했습니다. 예를 들어, 빌드된 API가 실제로 제공하는 사양과 API의 사양이 서로 일치하는지 여부를 확인할 수 있습니다. 처음에는 미온적이었던 개발자들이 COE 팀과 함께 보안 및 효율성의 장점을 깨닫고 Akamai API Security와 열정적으로 협력하기까지는 오랜 시간이 걸리지 않았습니다.

"Akamai는 첫날부터 코딩부터 프로덕션까지 모든 단계에 걸쳐 API를 검색, 보호, 테스트하는 방법에 대해 신뢰할 수 있는 조언자로서의 역할을 해왔습니다. 이를 통해 저희 센터는 조직 전체에 어떻게 보안과 효율성을 동시에 달성할 수 있는지 보여줄 수 있게 되었습니다."라고 Byrd는 설명했습니다. "이 파트너십은 제품 이상의 의미가 있습니다. Noname(현재 Akamai) 팀원들은 저희 세계와 API를 개발하는 이유가 무엇인지 이해하고 있습니다."

Novant의 리더십 또한 Akamai API Security가 '문제가 되기 전에 문제점을 포착할 수 있는' 능력을 언급하며 동의했고, API 보안을 조직의 시프트 레프트 노력에 확고히 자리잡게 했습니다.

API 보안을 활용해 성장

현재 Novant는 Akamai API Security를 사용해 API와 모든 디지털 이니셔티브에 대한 '자동 보호'를 제공합니다. Novant의 API 검색, 인벤토리 구축, 평가 및 테스트에서 얻은 이점을 바탕으로 COE 팀은 이제 Novant가 개발하는 새로운 API에 플랫폼의 포괄적인 보호 기능을 적용하고 있습니다. 이 팀은 Novant 개발자가 조정된 모범 사례를 기반으로 API를 구축하면 각 API가 자동으로 보호될 것이라고 생각하고 있습니다.

앞으로 COE 팀은 기업 내 다른 팀으로 Akamai API Security의 사용을 확대할 계획입니다. CEO는 API 보호를 위한 전사적 협업 모델을 목표로 CEO와 Novant Health 보안 팀, 조직의 기반 구조 팀이 Akamai API Security를 사용하는 파트너십을 구상하고 있습니다.

NOVANT HEALTH

Novant Health는 19개의 의료 센터와 900개 이상의 지역에서 근무하는 2000명 이상의 의사들로 구성된 비영리 통합 의료 시스템으로, 외래 수술 센터, 의료 플라자, 재활 프로그램, 진단 영상 센터, 지역사회 보건 지원 프로그램 등 다양한 의료 서비스를 제공합니다. Novant Health의 약 4만 여명의 직원들과 파트너 의사들은 노스캐롤라이나와 사우스캐롤라이나의 환자들과 지역사회를 돌보고 있습니다.

Akamai