

헬스케어 업계

API 인시던트가 증가하고 있습니다. 헬스케어 업계가 API 보안 문제를 어떻게 해결하고 있는지, 그리고 변화하는 위협을 방어하기 위해 무엇을 할 수 있는지 알아보세요.

환자 및 회원의 신뢰가 매우 중요한 헬스케어 업계 기업들은 점점 심각해지는 보안 도전과제에 직면해 있습니다. 바로 API 취약점입니다.

전자 건강 기록, 원격 헬스케어, 커넥티드 헬스케어 디바이스는 사이버 범죄자들의 주요 표적이 되었습니다. 그리고 보호되지 않은 API를 통해 접속된 PHI(Protected Health Information)는 HIPAA 위반, 환자 개인정보 유출뿐 아니라 회복에 수년이 걸리는 신뢰 하락으로 이어집니다.

이 문제의 규모는 상당합니다. Akamai가 실시한 포괄적인 설문 조사에 따르면, 헬스케어 전문가의 84.7%가 지난 1년 동안 API 보안 인시던트를 경험했다고 답했는데, 이는 업계 전체 평균인 84%보다 약간 높은 수치입니다.

그러나 가장 우려되는 것은 신뢰에 미치는 영향입니다. 헬스케어 전문가 응답자들은 API 인시던트 이후 가장 우려되는 사항으로 '신뢰와 평판 손실'(28.7%)을 꼽았습니다. 환자들이 기존에 이용하던 공급업체를 다른 곳으로 쉽게 바꿀 수 있는 세상에서, 이러한 평판 손실은 즉각적인 비용 이상의 지속적인 영향을 미칠 수 있습니다.

업계 인사이트를 얻으려면 [2024년 API 보안 영향 연구](#)를 확인하세요.

공격이 증가하면서 가시성에 대한 관심 증가

헬스케어 기업들이 이러한 인시던트를 해결하는 데 평균 51만 600달러를 지출하는 등 API 공격으로 인한 재정적 피해는 상당합니다.

이러한 리스크에도 불구하고, 데이터는 우선순위에 있어 우려할 만한 격차가 있음을 보여줍니다. 향후 12개월 동안의 주요 사이버 보안 우선순위에 대해 질문했을 때, 헬스케어 기업은 12가지 옵션 중 '공격자로부터 API 보호'를 11번째(16.7%)로 꼽았습니다. 대신, 직원들의 시스템 접속 인증 보안(24.7%)과 개발자 비밀번호 관리(22.7%)에 집중하고 있습니다.

헬스케어 서비스 공급업체가 정상적인 API 활동과 악성 API 활동을 구분하기는 여전히 어렵습니다. 업계 동료의 65%가 전체 API 인벤토리를 보유하고 있다고 답했지만, 그중 24%만이 민감한 데이터를 처리하는 API를 알고 있었습니다. 이는 2023년의 40%에서 많이 감소한 수치입니다. 데이터 프라이버시가 좋은 관행이 아니라 법으로 규정되어 있는 헬스케어 분야의 경우, 이러한 가시성 격차는 상당한 리스크를 초래합니다.

중요 IT 또는 보안팀의 적절한 감독 없이 임상 부서에서 배포된 API에 어떤 일이 발생할 수 있는지 생각해 보세요. API는 다음과 같은 상태일 수 있습니다.

- HIPAA 규정을 준수하는 적절한 통제 없이 환자 기록을 공유하도록 설계됨
- 시스템 업그레이드 후에도 활성 상태로 남아, 알려지지 않은 접속 지점을 생성함
- 기존의 보안 톨은 관리되지 않는 API를 탐지하도록 설계되지 않음
- PHI에 접속하기 위해 공격자가 악용함
- 의도하지 않은 사용 사례에 엔드포인트를 사용해 인증된 파트너가 악용함

이것은 단순한 가설이 아닙니다. 헬스케어 데이터 유출이 사상 최고치를 기록하고 데이터 유출로 인한 비용이 평균 488만 달러에 달하는 상황¹에서, API 취약점은 갈수록 커지는

헬스케어 기업의 **84.7%**가 지난 12개월 동안 API 관련 인시던트를 경험했습니다.

헬스케어 기업의 **65%**가 전체 API 인벤토리를 보유하고 있지만, 그중 24%만이 민감한 데이터를 반환하는 API를 알고 있습니다.

지난 12개월 동안 API 보안 인시던트로 인해 헬스케어 기업이 받은 재정적 영향은 **51만 600달러**입니다.

상위 3대 영향

1. **신뢰와 평판 손실** (28.7%)
2. **생산성 저하** (28.7%)
3. **내부 조사 증가** (27.3%)

출처:
Akamai, 'API 보안 영향 연구', 2024년



컴플라이언스 및 보안 리스크를 의미합니다. 또한, 이러한 시나리오는 업계 동료들이 API 인시던트의 가장 큰 원인으로 꼽는 것을 반영합니다.

API 인시던트가 컴플라이언스, 비즈니스 비용, 팀 스트레스에 미치는 영향

2024년 5월 Gartner®의 API 보안 시장 가이드²에는 ‘현재 데이터에 따르면, 평균적인 API 유출 사고에서 유출되는 데이터는 평균적인 보안 유출에서보다 10배 이상 더 많은 것으로 나타났다.’라고 언급되어 있습니다.

HIPAA 컴플라이언스가 API 보안에 점점 더 집중하는 것은 당연한 일입니다. HIPAA는 API를 명시적으로 언급하지는 않지만 직원의 업무에 따라 PHI 접촉을 제한하도록 요구합니다. 이를 위해서는 환자 데이터를 전송하는 API에서 인증과 접속 제어가 필요합니다. 헬스케어 서비스 공급업체와 구매자, 규제 당국은 자신들의 API뿐만 아니라 파트너와 공급업체의 API를 통해 어떤 종류의 데이터가 이동하는지 알아야 합니다. 이는 헬스케어 부문의 써드파티 리스크 관리에 또 다른 과제를 추가합니다.

규제 당국의 신뢰를 잃으면, 컴플라이언스를 준수하기 위해 노력하는 팀의 업무 부담이 증가하고, 이에 대한 감시가 강화될 수 있습니다. 또한 고액의 벌금형으로 이어질 수도 있습니다. 이를 염두에 두면, 헬스케어 관련 회사들이 API 위협으로 인한 재정적 결과에 대해 잘 알고 있다는 것을 알 수 있습니다. 처음으로 설문 조사에 참여한 3개국의 응답자들에게 지난 12개월 동안 경험한 API 보안 인시던트로 인한 예상 비용을 공유해 달라고 요청했습니다.

	헬스케어 업계	모든 업계 평균
 미국	\$510,600	\$591,404
 영국	£363,885	£420,103
 독일	€643,884	€403,453

Q3. API 보안 인시던트를 경험한 경우, 해당 인시던트로 인해 발생한 총 재정적 영향은 얼마였나요? 시스템 수리, 다운타임, 법률 비용, 벌금, 기타 관련 비용 등 모든 관련 비용을 포함해 주세요.

재정적 영향도 상당하지만, 연구 참여자들은 그 비용이 수익에 미치는 영향은 훨씬 더 크다는 점을 강조했습니다. API 보안 인시던트의 가장 큰 영향을 나열해 달라는 질문에 응답자들은 비용이 아니라고 답했습니다. 앞서 언급한 바와 같이, 응답자들은 ‘신뢰와 평판 손실’(28.7%)과 ‘생산성 저하’(28.7%)를 강조했습니다. 이러한 결과는 장기적인 영향을 미칩니다. 환자의 신뢰가 손상되면 향후 매출에 악영향을 미칠 수 있으며, 이미 과중한 업무에 시달리는 헬스케어 종사자의 생산성 저하는 번아웃과 직원 이탈을 가속할 수 있습니다.

¹ IBM 데이터 유출 비용 보고서, 2024년
² Gartner, API 보안 시장 가이드, 2024년 5월 29일. GARTNER는 Gartner, Inc. 및/또는 미국 내외에 있는 Gartner 계열사의 등록 상표 및 서비스 마크이며, 이 문서에의 사용 허가를 받았습니다. All rights reserved.

선제적인 API 보안을 통해 리스크와 스트레스 줄이기

헬스케어 기업을 대상으로 한 API 공격은 범위, 규모, 정교함, 비용 면에서 증가하고 있습니다. 여기에는 기존 API 보안 툴 및 기타 경계 방어 체계를 우회하기 위해 빠르게 적응하는 GenAI 기반 봇 공격이 포함됩니다. 업계의 많은 보안팀이 이러한 위협을 직접 경험하고 있으며 금전적, 인적 피해를 입고 있습니다. 하지만 기업이 API 위협의 심각성을 이해하더라도 여전히 '무엇을 할 수 있을까?'라는 의문이 남습니다.

기업은 지금, API와 API가 교환하는 데이터의 보안을 강화하기 위한 조치를 취해 매출을 보호하고 보안팀의 부담을 덜어주는 동시에 이사회와 고객 모두의 어렵게 얻은 신뢰를 유지할 수 있습니다. 기업이 취할 수 있는 조치에는 지능형 API 위협에 대한 팀의 지식과 이를 방어하는 데 필요한 기능을 구축하는 것이 포함됩니다.



보고서 전문을 읽고 API 가시성 및 보안을 위한 모범 사례에 대해 알아보려면 **2024년 API 보안 영향 연구**를 다운로드하세요.

현재 직면한 도전 과제 해결을 Akamai가 어떻게 지원할 수 있는지 궁금하신가요?

[맞춤 Akamai API 보안 데모 신청하기](#)



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, akamai.com/blog를 확인하거나 X, LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2025년 3월 발행.