WAVEMED / RADCARD

최후의 방어선

The Last Line of Defense

AI로 가속화되는 병원 사이버 공격 시대의
환자 소유·오프라인 우선 건강 데이터

WaveMed / RadCard 포지셔닝 백서

2026

목차

1. 핵심 요약

보건의료는 전 세계에서 가장 많은 공격을 받는 단일 부문이 되었습니다. 2025년 보건의료는 금융 서비스를 제치고 랜섬웨어와 데이터 탈취의 최우선 표적이 되었으며, 보건의료 데이터 유출 한 건의 평균 비용은 이제 다른 어떤 산업보다 높습니다. 2025-2026년에는 위협의 성격 자체도 바뀌었습니다. 인공지능이 숙련된 인간 공격자의 작업을 자율적으로 수행하기 시작하면서, 공격의 규모·속도·정밀도가 사후 대응형 방어로는 따라잡을 수 없는 수준으로 높아졌습니다.

병원이 계속 패배하는 이유는 부주의가 아닙니다. 디지털 헬스의 지배적인 아키텍처, 즉 수백만 건의 환자 파일을 네트워크로 연결된 하나의 저장소에 집중시키는 대규모 중앙집중식 기록 시스템이 구조적으로 공격자에게 최적화되어 있기 때문입니다.

중앙집중화는 두 가지 치명적인 속성을 동시에 만들어 냅니다. 첫째, **허니팟**을 만듭니다. 단 한 번의 침해로 수천만 건의 기록이 한꺼번에 노출될 수 있습니다. 둘째, **단일 장애점**을 만듭니다. 중앙 시스템이 랜섬웨어에 의해 암호화되면 기관 전체가 마비되고 진료가 중단됩니다. 그 대가는 더 이상 프라이버시와 금전에 그치지 않습니다. 진단이 지연되고, 치료가 연기되며, 기록으로 확인된 사례에서는 환자 사망으로까지 이어집니다. 이제 AI는 이 두 속성을 더욱 위험하게 만듭니다. 자율 에이전트가 어떤 인간 팀의 대응보다 빠르게 허니팟을 찾아내고 인력이 부족한 방어자를 공략할 수 있게 되고 있기 때문입니다.

WaveMed와 RadCard 플랫폼은 이 아키텍처를 뒤집습니다. 데이터를 중앙 저장소에 집중시키는 대신, 환자의 필수 의료 기록은 **환자 자신에게** 존재합니다. 암호화되고, 오프라인에서도 사용할 수 있으며, 환자가 소유하는 형태로 RadCard(USB + NFC MicroEHR)와 RadPatch(수동형 NFC 응급 태그)에 저장됩니다. 국가 단위의 집계 데이터는 정부가 보유하기로 선택한 경우 해외의 허니팟이 아닌 **국내 주권 클라우드(iSAVE)** 안에 보관됩니다.

이를 통해 패치나 경계 보안으로는 도달할 수 없는 방어 태세가 만들어집니다.

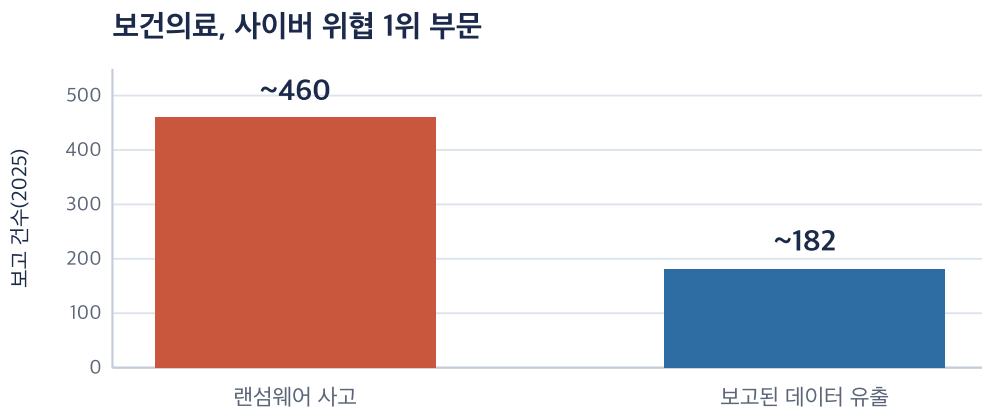
- **몸값을 노릴 중앙의 '대박' 표적이 없습니다.** 환자 한 명의 카드를 탈취해도 얻는 것은 수백만 건이 아니라 기록 한 건입니다. 대규모 공격을 부추기는 경제적 동기가 사라지며, 허니팟의 부재는 AI 공격 에이전트가 결코 찾아낼 수 없는 단 하나의 표적입니다.
- **병원이 공격받는 중에도 진료는 계속됩니다.** 기관의 네트워크가 암호화되어 오프라인 상태가 되더라도, 환자는 혈액형, 알레르기, 복용 약물, 영상 등 자신의 암호화된 기록을 지니고 내원하며, 이 기록은 인터넷 없이도 진료 현장에서 판독할 수 있습니다. 이것이 바로 최후의 방어선입니다. 모든 중앙 시스템이 실패하더라도 환자는 여전히 자신의 데이터를 보유하고 있습니다.
- **국가 보건 데이터의 주권이 유지됩니다.** 정부는 침해되거나, 소환장의 대상이 되거나, 접속이 차단될 수 있는 해외 클라우드에 의존하는 대신, 국가 인프라로 귀속된 자체 인스턴스를 호스팅할 수 있습니다.

이 백서의 논지는 단순하며, 시점에 관한 논거는 결정적입니다. 중앙집중식 시스템을 겨냥하는 공격이 특징인 위협 환경에서, 그리고 이제는 일단 공격이 시작되면 결코 앞지를 수 없는 AI로 가속화된 환경에서, 가장 지속 가능한 보호책은 허니팟 주위에 더 튼튼한 벽을 쌓는 것이 아닙니다. 기록의 보관 권한을 환자와 국가에 되돌려 줌으로써 허니팟 자체를 없애는 것이며, 이는 공격이 닥치기 전에 갖춰져 있어야 합니다.

2. 글로벌 위협 환경(2024-2026)

보건의료 부문의 노출 수준을 보여 주는 데이터는 더 이상 모호하지 않습니다.

보건의료는 1순위 표적입니다. 미국 연방수사국(FBI)의 2025년 인터넷 범죄 보고에서 보건의료 및 공중보건 부문은 사이버 위협 측면에서 모든 부문 중 1위를 기록했습니다. 랜섬웨어 사고 약 460건과 보고된 데이터 유출 182건으로, 그 뒤를 이은 금융 부문보다 전체 사건 수가 많았습니다.



출처: 미국 FBI 2025년 인터넷 범죄 보고(AHA 인용).

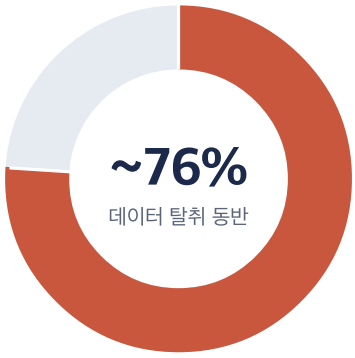
그림 1. 2025년 보고된 사이버 사건 수에서 보건의료가 모든 부문 중 1위를 차지했습니다.

재정적 부담은 모든 산업 중 가장 큽니다. 2025년 보건의료 데이터 유출의 평균 비용은 건당 약 742만 달러로, 대부분의 산업 추적 기관 기준으로 전 부문 중 가장 높았습니다. 부문 전반에서 500명 이상에게 영향을 미친 유출이 대규모로 계속 발생했으며, 건당 평균 수만 건의 기록이 관련되었습니다.

최대 규모의 사고는 이제 인구 전체 규모에 이릅니다. 2024년 2월 Change Healthcare 공격으로 약 1억 명의 보호 대상 건강 정보가 침해되었고, 전국적으로 보험 청구와 진료 제공이 중단되었으며, 대응 비용은 24억 달러로 추산되었습니다. 의료기관, 청구 대행업체, 검사기관, 클라우드 호스팅 헬스 플랫폼 전반에서 발생한 2025년의 다른 사고들은 수백만 건의 기록을 추가로 노출시켰으며, 병원 자체보다는 제3자 및 공급망 업체를 통한 경우가 많았습니다.

공격자의 목적은 업무 마비에서 탈취로 바뀌었습니다. 2025년 한 해 동안 보건의료 사고의 약 4분의 3에서 암호화 이전에 또는 암호화 대신 데이터 유출이 발생했습니다. 이른바 이중 갈취입니다. 데이터를 잠그는 능력이 아니라 데이터 자체가 전리품이 된 것입니다. 이러한 변화는 중앙 시스템의 가용성에 의존하기보다 저장 상태의 기록을 환자에게서 보호해야 한다는 논거를 직접적으로 강화합니다.

공격 목적, 업무 마비에서 데이터 탈취로 이동



2025년 보건의료 사고 중 데이터 유출(이중 갈취)이 발생한 비율.

그림 2. 이중 갈취: 이제 목표는 단순한 업무 마비가 아니라 데이터 탈취입니다.

위협은 광범위하고 지속적입니다. 보안 연구자들은 12개월 동안 보건의료를 겨냥한 서로 다른 랜섬웨어 조직을 88개가량 추적했으며, Qilin, INC, RansomHub, Medusa 같은 변종이 번갈아 가며 이 부문을 공격했습니다. 이는 개별적으로 억제할 수 있는 소수의 행위자가 아니라, 탈취된 건강 데이터를 거래하는 구조화·산업화된 시장입니다.

신뢰할 수 있는 모든 출처가 같은 그림을 보여 줍니다. 보건의료는 빠르게 디지털화되고 있고, 가장 가치 있는 개인 데이터를 보유하고 있으며, 여전히 가장 공략하기 쉬운 고가치 표적입니다.

3. AI 변곡점: 다음 공격의 물결이 대비하지 않은 이들을 응징하는 이유

2장은 현재 시점의 위협을 설명합니다. 오늘 내리는 모든 결정에 더 중요한 사실은 위협이 움직이는 방향이며, 2025-2026년에 그 방향의 성격이 바뀌었습니다. 이제 AI가 작업의 상당 부분을 자율적으로 수행하기 때문에, 공격은 더 이상 숙련된 인간 운영자의 공급에 제약받지 않습니다.

증거는 더 이상 추측이 아닙니다. 2025년 9월, 연구자들은 최초로 확인된 완전 자율형 AI 주도 사이버 공격을 기록했습니다. 이 공격에서 AI는 작전의 약 80-90%를 독립적으로 처리했으며, 국가 연계 조직이 주요 상용 언어 모델의 에이전트 기능을 이용해 침투를 수행한 사례도 기록되었습니다. 이후 기존 랜섬웨어 조직들은 AI 에이전트를 공격 파이프라인에 직접 통합했습니다. 자율적 취약점 스캐닝, 즉석 익스플로잇 생성, 그리고 템플릿 기반 시도보다 몇 배 더 효과적인 것으로 보고된 스피어피싱이 그 예입니다. 한 유력 조직은 의료 데이터 저장소를 찾아내고, 병원이 얼마나 심각하게 마비될지를 좌우하는 운영 기술(OT) 의존 관계를 파악하도록 특별히 훈련된 에이전트를 배치하는 것이 관찰되었습니다. 2026년에 대한 업계 전망은 같은 방향으로 수렴합니다. 단 한 명의 운영자나 소규모 조직이 생태계가 한 번도 경험해 보지 못한 규모로 다수의 표적을 동시에 공격할 수 있게 하는 완전 자율형 랜섬웨어 파이프라인이 등장할 것이며, 이미 대다수 조직이 AI로 강화된 공격의 속도를 따라잡을 수 없고 기존 방어 체계가 실패하고 있다고 보고하고 있습니다.

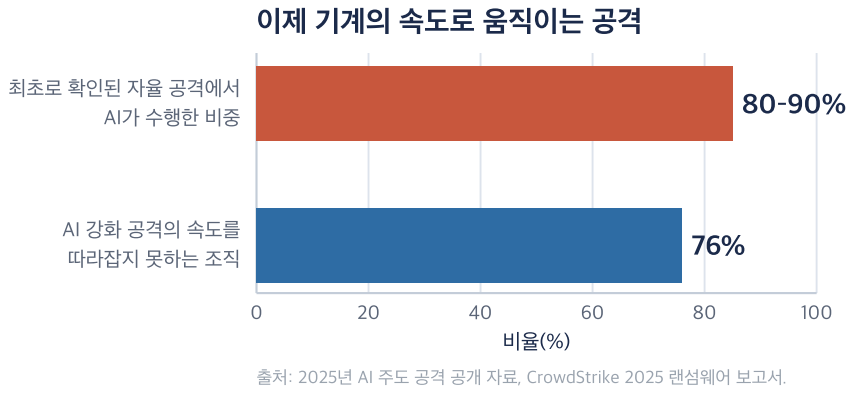


그림 3. 자율 공격이 인간 방어자를 앞지르고 있습니다.

여기서 세 가지 결과가 도출되며, 각각은 사후 대응형 보안 강화보다 사전에 배치된 아키텍처 차원의 방어가 유리함을 보여 줍니다.

1. 공격의 양과 속도가 인간의 대응 능력을 넘어섭니다. AI 에이전트를 갖춘 운영자 한 명이 팀 전체의 일을 해내고 여러 표적을 동시에 공격할 수 있게 되면, 공격 건수는 늘어나고 침투에서 피해 발생까지의 간격은 급격히 짧아집니다. 인간 팀이 제때 알아차리고 대응하는 데 의존하는 방어는 처음부터 구조적으로 뒤처질 수밖에 없습니다.

2. 방어자의 가장 약한 지점이 바로 AI가 파고드는 지점입니다. 보건의료 랜섬웨어 공격이 성공하는 가장 흔한 요인은 보안 인력 부족입니다. AI 공격자는 바로 그 격차를 넓힙니다. 어떤 기관도 자율형 공격자보다 더 많은 인력을 투입할 수는 없으며, 자원이 부족한 시스템(5장)은 시도조차 할 수 없습니다.

3. AI는 허니팟을 찾는 능력이 점점 더 뛰어나집니다. 최신 공격 에이전트는 의미론적 이해를 활용해 가장 가치 있는 파일을 찾아내고, 기관을 붕괴시키는 의존 관계를 파악합니다. 중앙집중식 기록 저장소는 그 어느 때보다 찾기 쉽고 우선 표적으로 삼기 쉬워졌습니다. AI가 극복할 수 없는 단 하나의 방어는 찾아낼 허니팟 자체가 없는 것입니다.

이것이 지금 내리는 모든 결정의 핵심입니다. **AI로 가속화된 공격은 시작된 뒤에는 대응할 수 없습니다.** 기계의 속도로 진행되는 자율 침투 중에는 데이터 아키텍처를 재설계하거나, 보관 권한을 분산하거나, 오프라인 기능을 구축할 시간이

없습니다. 피해를 제한하는 유일한 요소는 공격이 닥치기 전에 이미 갖춰져 있던 것뿐입니다. 분산형이면서 오프라인에서도 사용할 수 있는 환자 보유형 기록을 사전에 배치한 보건의료 시스템은 손실을 줄일 것이고, 기다린 시스템은 타격을 고스란히 받게 될 것입니다.

이러한 관점에서 WaveMed는 여유롭게 도입해도 되는 보안 제품이 아닙니다. **다음 물결보다 앞서 갖춰야 하는 사전 대비책입니다.** WaveMed의 보호 효과는 바로 사전에 설치되어 있기 때문에 실현됩니다. 환자는 이미 자신의 기록을 보유하고 있고, 데이터는 이미 중앙 표적에서 벗어나 있으며, 시스템은 이미 네트워크 없이 작동합니다. 사전 배치는 부수적인 이점이 아니라 핵심 그 자체입니다.

4. 병원이 계속 무너지는 이유: 중앙집중화의 함정

위협이 이토록 잘 알려져 있는데 왜 병원은 계속 패배할까요? 취약점이 고칠 수 있는 설정 오류가 아니라 시스템 설계 그 자체이기 때문입니다.

허니팟의 경제학. 중앙집중식 EHR / HIS / PACS는 바로 데이터를 집적하기 위해 존재합니다. 이러한 집적은 임상적으로는 유용하지만 경제적으로는 파국적입니다. 전체 환자 집단의 기록을 하나의 자격 증명 체계와 하나의 네트워크 경계 뒤에 집중시키기 때문입니다. 그 경계를 뚫은 공격자는 기록 한 건을 훔치는 것이 아니라 기관 전체를 훔칩니다. 침투에 성공했을 때의 수익은 데이터베이스 규모에 비례하며, 바로 이 때문에 대형 보건의료 시스템과 데이터가 풍부한 공급업체가 가장 집요하게 표적이 되고, AI 에이전트도 이제 이들을 찾도록 조정되고 있습니다.

단일 장애점. 데이터를 보관하는 중앙 시스템이 병원 운영도 담당합니다. 랜섬웨어가 이 시스템을 암호화하면 임상의는 기록, 영상, 검사 결과, 처방, 일정 관리에 대한 접근을 한꺼번에 잃습니다. 기관은 종이 기록으로 돌아가거나 운영을 중단하며, 복구에는 몇 시간이 아니라 몇 주가 걸립니다. 2024년 영국의 한 검사 서비스 업체에 대한 공격은 한 지역 전체의 혈액 검사 결과를 지연시켰고, 그로 인한 진료 지연은 한 환자의 사망에 부분적으로 기여한 것으로 공식 인정되었습니다. 이것이 가장 중요한 지점입니다. 중앙집중화는 데이터 보안의 실패를 환자 안전의 실패로 바꿔 놓습니다.

방어자의 구조적 불리함. 병원은 임상 업무의 특성상 모든 문, 즉 모든 워크스테이션, 모든 연결 기기, 모든 원격 접속 경로, 모든 제3자 연동을 열어 두어야 합니다. 공격자에게는 그중 하나만 있으면 됩니다. 보건의료 분야의 자체 사고 분석은 반복적으로 같은 근본 원인을 지목합니다. 사이버 보안 인력 부족, 알려졌지만 패치되지 않은 취약점, 레거시 운영 체제, 자격 증명 탈취입니다. 이는 태만의 징후라기보다, 자원이 부족한 의료기관에 끊임없이 확장되는 중앙집중식 공격 표면을 이제는 기계의 속도로 움직이는 공격자에 맞서 방어하라고 요구한 데 따른 예측 가능한 결과입니다.

결론은 자명합니다. 아키텍처가 데이터와 기능을 한곳에 집중시키는 한, 모든 방어적 개선은 점진적일 뿐이고 모든 침해는 전면적입니다. 유일한 구조적 탈출구는 집중을 멈추는 것입니다.

사례 연구

루마니아, 2024년 2월: 한 국가가 펜과 종이로 돌아가다

위에서 설명한 위험은 이론이 아닙니다. 2024년 2월, 공격자들은 부쿠레슈티의 한 소프트웨어 회사를 침해하고, 루마니아 전역에서 입원 관리, 검사 결과, 약국 물류, 급여 관리에 사용되던 의료 플랫폼 Hippocrates에 BackMyData 랜섬웨어를 심었습니다. 100곳이 넘는 병원이 동일한 신뢰 시스템에 의존하고 있었기 때문에, 감염은 그 단일 공유 채널을 통해 확산되었고 병원들의 파일은 사용할 수 없는 무의미한 데이터로 뒤섞였습니다. 공격자들은 약 160,000유로 상당의 비트코인을 요구했으나, 루마니아는 지불하지 않기로 결정했습니다.

확산을 막을 유일한 방법은 극단적이었습니다. 국가 사이버 보안국은 피해를 입은 모든 병원에 인터넷 연결을 완전히 차단하라고 명령했습니다. 임상의들은 디지털 차트, 검사 결과, 영상의학 자료, 처방전, 의약품 물류를 한꺼번에 잃었습니다. 한 외과의가 표현했듯이 IT 기록은 단순한 환자 명단이 아니며, 그 모든 것이 한순간에 사라졌습니다. 병원들은 환자 등록을 계속하기 위해 펜과 종이, 오프라인 스프레드시트에 의존해야 했습니다.

루마니아의 대응은 성공으로 평가받는 것이 마땅합니다. 최근 백업과 범국가적 협력 덕분에 대부분의 병원이 약 5일 만에 운영을 재개했으며, 이 공격으로 인한 사망자는 보고되지 않았습니다. 그러나 그 성공의 본질이 바로 교훈입니다. 가능했던 유일한 방어는 시스템 전체를 오프라인으로 전환하고 19세기 방식의 대비책으로

돌아가는 것이었으며, 그 대가로 이후 몇 주 동안 수작업 재입력이 필요했고 일부 데이터는 영구적으로 손실되었습니다. 게다가 이 방법이 통한 것은 루마니아에 최근 백업, 국가 사이버 보안 기관, 그리고 100개 병원을 동시에 조율할 자원이 있었기 때문이며, 이는 자원이 부족한 보건의료 시스템(5장)에는 없는 이점입니다.

바로 이 격차를 WaveMed가 메웁니다. 루마니아는 살아남기 위해 병원을 오프라인으로 만들어야 했습니다. WaveMed는 설계 단계부터 데이터를 오프라인에서 사용할 수 있게 만듭니다. 따라서 시스템이 멈추더라도 임상의가 종이 노트 한 권만 든 채 아무런 정보 없이 남겨지지 않습니다. 환자는 여전히 구조화되고 암호화된 기록(혈액형, 알레르기, 복용 약물, 영상)을 지니고 있으며, 이 기록은 진료 현장에서 몇 초 만에 판독할 수 있습니다. 이것이 기록을 잃는 대비책과 기록을 지키는 대비책의 차이입니다.

5. 신흥 시장의 관점: 같은 위협, 더 적은 방어

저소득 및 중간소득 국가의 보건의료 시스템에서는 중앙집중화의 함정이 더욱 심각합니다. 이들 시스템을 공격에 취약하게 만드는 바로 그 조건이 방어를 불가능하게 하고 복구를 더디게 만들기 때문입니다.

대륙 단위의 데이터는 냉혹합니다. 2025년 아프리카 보건의료 기관은 **주당 평균 약 3,575건의 사이버 공격**을 받았으며, 이는 **전년 대비 38% 증가**한 수치입니다. 그 이유는 명백히 구조적입니다. 공공 부문 보건의료 시스템은 레거시 소프트웨어, 파편화된 인프라, 자원이 부족한 IT 팀으로 운영되고 있습니다. 최근 사고는 대륙 전역에 걸쳐 있습니다. 전국 규모의 검사 서비스 중단으로 수백만 명의 검사 처리가 지연되었고, 지역 디지털 헬스 플랫폼이 침해되었으며, 민간 의료기관 부문은 이제 세계에서 가장 많이 표적이 되는 곳 중 하나로 꼽힙니다.

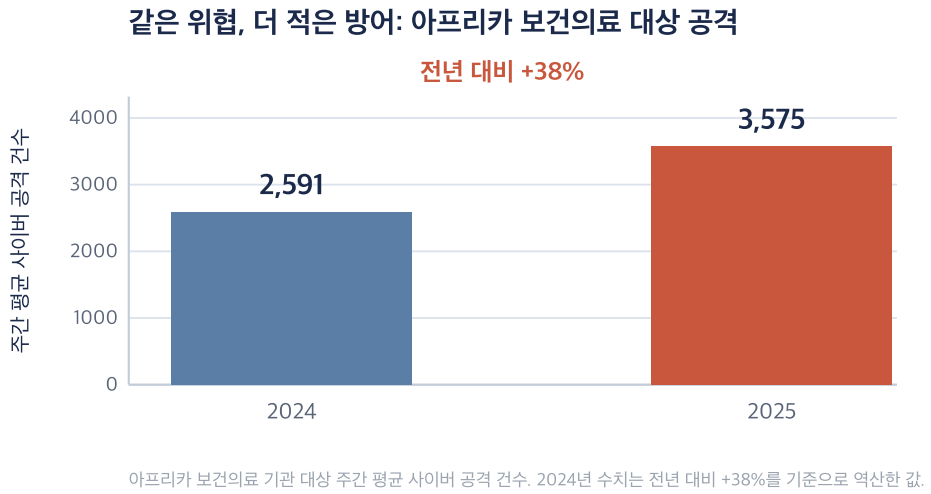


그림 4. 아프리카 보건의료 기관에 대한 공격이 전년 대비 38% 증가했습니다.

이 환경은 세 가지 구조적 격차로 정의됩니다.

1. **통신 음영 지역.** 넓은 지역에서 통신이 불안정하거나 아예 없습니다. 클라우드에 의존하는 온라인 전용 시스템은 네트워크가 닿지 않는 곳에서 작동할 수 없습니다.
2. **IT 인력 부족.** 모니터링, 패치, 대응을 수행할 보안 전문가가 충분하지 않습니다. 전 세계적으로 보건의료 랜섬웨어 공격이 성공하는 가장 흔한 단일 요인이 바로 이러한 인력과 역량의 부족이며, 이 문제는 이 지역에서 가장 심각합니다.
3. **자본 및 인프라 부족.** 부유한 시스템이 중앙집중식 모델을 방어하기 위해 사용하는 엔터프라이즈급 하드웨어, 이중화된 데이터 센터, 상시 보안 운영은 재정적으로 감당할 수 없는 수준입니다.

핵심 통찰은 이 세 가지 격차가 단순히 취약성의 원인에 그치지 않는다는 것입니다. 이는 기존의 중앙집중식·클라우드 의존형 보건의료 IT가 갖추지 못하면 작동할 수 없는 바로 그 필수 요건입니다. 상시 연결, 보안 팀, 자본 인프라를 필요로 하는 시스템은 이 세 가지 중 어느 것도 없는 환경에서 실패할 수밖에 없습니다. 그리고 AI로 가속화된 공격 앞에서는 이들 시스템이 결코 메울 수 없는 인력 격차가 결정적인 요인이 됩니다.

바로 여기서 아키텍처 논거가 결정적인 힘을 갖습니다. 이 지역에서 중앙집중식 시스템을 방어 불가능하게 만드는 세 가지 격차는, WaveMed와 RadCard가 그것 없이도 작동하도록 설계된 바로 그 격차입니다.

6. WaveMed의 역발상: 방어로서의 아키텍처

WaveMed의 방어력은 기존 시스템에 덧붙인 기능이 아닙니다. 데이터가 어디에 존재하고 누가 이를 통제하는지를 뒤집은 결과입니다. 다섯 가지 아키텍처 선택이 이를 실현합니다.

1. 탈중앙화 — 데이터는 환자에게 있습니다. 환자의 필수 기록은 RadCard(지갑 크기의 USB + NFC MicroEHR, 8-64 GB)에, 응급 상황용으로는 RadPatch(손톱 크기의 수동형 NFC 태그)에 담겨 환자와 함께 이동합니다. 모든 환자의 전체 기록을 단일 표적으로 보관하는 중앙 데이터베이스는 존재하지 않습니다. 한 인구 집단의 데이터를 훔치려면 공격자는 그 인구의 카드를 하나하나 물리적으로 탈취해야 하며, 이는 대규모 공격의 경제성을 무너뜨리고 AI 에이전트가 찾아낼 중앙 저장소를 남기지 않습니다.

2. 오프라인 우선 — 인터넷 의존성이 없습니다. RadCard는 자동 실행(auto-run)을 통해 카드에서 직접 자체 MicroEHR와 내장 DICOM 뷰어(iQ-VIEW Lite)를 구동하며, 설치나 네트워크가 필요하지 않습니다. RadPatch는 최신 휴대폰으로 태그하기만 하면 완전한 오프라인 상태에서 판독됩니다. 이 시스템은 연결을 전제하지 않습니다. 연결이 없는 상황을 전제로 하며 그래도 작동합니다. 지리적 이유로든 공격으로 인해서든 클라우드에 접속할 수 없는 곳에서도 기록은 여전히 사용할 수 있습니다.

3. 엣지 암호화 — 보호가 데이터와 함께 이동합니다. 기록은 독자적인 WMSD(WaveMed Security Data) 형식 안에서 AES-256으로 저장 시 암호화됩니다. NFC 계층은 사전 프로비저닝 방식으로만 운용됩니다. 제3자 앱은 페이로드를 해독할 수 없으며, WaveMed가 프로비저닝한 인증된 태그에만 쓰기가 가능합니다. 편집은 PIN으로 보호됩니다. 위기 상황에서는 누구나 응급 데이터를 읽을 수 있지만, 변경은 소유자만 할 수 있습니다. 암호화는 데이터가 우연히 놓여 있는 서버의 속성이 아니라, 데이터가 가는 모든 곳에서 유지되는 데이터 자체의 속성입니다.

4. 중앙 허니팟이 없습니다. 기관 운영을 위해 항상 온라인 상태를 유지해야 하는 단일한 전체 기록 집적 저장소가 없으므로, 몸값을 노릴 '대박' 표적도 없고 암호화되면 진료가 멈추는 단일 시스템도 없습니다. 현대 보건의료 공격의 결정적 표적이자 AI 에이전트가 찾도록 훈련받은 대상이 이 모델에는 아예 존재하지 않습니다.

5. 환자 보관 — 소유권이 곧 보안입니다. 환자는 자신의 기록에 대한 보관 소유권을 가집니다. 이는 윤리적·규제적 입장에 그치지 않고 하나의 보안 아키텍처입니다. 보관 권한을 개인에게 분산하면 공격자가 의존하는 집중이 사라지고, 기록의 가용성이 어떤 기관의 정상 운영 여부에도 좌우되지 않게 됩니다.

그 위에, 국가가 선택하는 경우 **iSAVE 주권 클라우드**가 계층으로 더해집니다. 이는 동기화, 백업, 국가 집계 데이터를 위한 국내 인스턴스이며 8장에서 다룹니다. 두 계층의 관계는 의도적으로 설계되었습니다. 개인 기록은 환자가 소유하고 휴대하는 반면, 선택 사항인 국가 인스턴스는 주권적 통제하에 집계 인프라를 보유합니다. 두 계층은 서로 구별되며 상호 보완적이고, 같은 데이터를 두 번 보관하는 것이 아닙니다.

7. 공격 속의 회복력: 진료의 연속성

이러한 역발상의 가치를 가장 명확하게 확인하는 방법은, 같은 날 같은 랜섬웨어 공격이 기존 병원과 WaveMed를 갖춘 병원에 각각 닥쳤을 때 어떤 일이 벌어지는지 비교하는 것입니다.

기존 병원. 랜섬웨어가 중앙 HIS/EHR/PACS를 암호화합니다. 임상의는 기록, 영상, 검사, 처방을 동시에 잃습니다. 병원은 종이 기록으로 돌아가고, 구급차를 다른 병원으로 돌리며, 시술을 취소하고, 몇 주가 걸리는 복구에 들어갑니다. 환자의 병력에는 접근할 수 없고, 알레르기와 복용 약물은 환자가 말을 할 수 있는 상태라면 문진을 통해 다시 파악해야 합니다. 침해는 전면적이며 업무 중단은 기관 전체에 미칩니다. 루마니아의 100개 병원(4장 사례 연구 참조)이 교과서적인 사례입니다. 유일한 탈출구는 모든 연결을 끊고 펜과 종이를 드는 것이었습니다.

WaveMed를 갖춘 환경. 병원 자체 시스템은 여전히 공격받을 수 있습니다. WaveMed는 병원 네트워크를 침해 불가능하게 만든다고 주장하지 않습니다. 그러나 환자는 RadCard와 RadPatch를 지니고 내원합니다. 응급 대응 요원이나 임상의가 패치를 태그하거나 카드를 판독하면, **오프라인 상태에서 2초 이내에** 혈액형, 알레르기, 현재 복용 약물, 만성 질환, 비상 연락처, 과거 영상을 확인할 수 있습니다. 중증도 분류가 진행되고, 치료 결정은 실제 데이터를 바탕으로 이루어집니다. 기록은 애초에 암호화된 서버에 있지 않았으므로, 그 서버에 대한 공격이 기록을 앗아 가지 못했습니다.

이것이 "최후의 방어선"이 갖는 실제 운영상의 의미입니다. 환자가 보유한 기록은 모든 중앙 계층이 실패했을 때에도 살아남는 계층입니다.

표 1. 같은 공격, 두 가지 결과.

구분	공격받는 중앙집중식 EHR	공격받는 RadCard / WaveMed
기록 가용성	시스템이 암호화된 동안 손실	환자에게 있어 오프라인으로 사용 가능
피해 범위	전체 환자 집단	물리적으로 탈취된 경우 카드 한 장
진료 연속성	중단, 종이 기록으로 복귀	진료 현장에서 계속 유지
복구 시간	수 주	기록 복구 단계 불필요
인터넷 의존성	필요	불필요
공격자 / AI 에이전트의 유인	높음 — 한 번의 침해로 수백만 건의 기록 확보	낮음 — 찾아낼 집적된 '대박' 표적 없음

진료 연속성을 지키는 동일한 논리가 일상적인 회복력도 지켜 줍니다. 이 플랫폼의 시범 도입 사례에서는 오프라인 모드에서의 사실상 완전한 데이터 가용성, 환자 식별 오류의 거의 완전한 제거, 그리고 훨씬 빨라진 환자 접수가 보고되었습니다. 이러한 이점은 공격이 있는 날뿐 아니라 평범한 모든 날에 유효합니다.

8. 주권 계층: iSAVE

정부에게 사이버 문제는 주권 문제와 분리될 수 없습니다. 국가의 건강 데이터는 어디에 있으며, 누가 접근할 수 있는가? 기존의 디지털 헬스 도입 사례는 이 질문에 제대로 답하지 못합니다. 국가 건강 기록은 흔히 해외에서 운영되는 클라우드 인프라에 보관되며, 자국이 통제할 수 없는 침해, 역외 법적 절차, 외부 제공업체에 의한 서비스 중단 위험에 노출됩니다.

iSAVE 아키텍처는 이 질문에 다르게 답합니다. 국가는 해외 기기나 서비스가 아닌 국가 디지털 인프라로 귀속된 **자체 국내 인스턴스**를 호스팅할 수 있습니다. 동기화, 장기 백업, 국가 집계 데이터는 해당 국가의 관할권과 통제 안에 머뭅니다.

두 계층은 서로 다른 소유자를 위해 존재하므로 반드시 구분되어야 합니다.

- **개인 기록은 환자가 소유합니다.** 각 시민의 개인 의료 데이터는 본인의 PIN과 보관 아래 본인의 RadCard와 RadPatch에 담겨 이동합니다. 이것이 프라이버시와 연속성의 계층입니다.
- **국가 집계 인스턴스는 주권 인프라입니다.** 비식별화된 인구 수준의 데이터 레이크와 호스팅 환경은 국가 거버넌스하에 보유되는 국가 자산이며, 국가가 지정한 분석 또는 AI 역량과 연결될 수 있습니다.

이러한 계층화는 자칫 모순이 될 수 있는 문제, 즉 환자의 기록 소유권과 국가의 건강 데이터 관리 책임 사이의 긴장을 각각을 알맞은 계층에 배정함으로써 해결합니다. 시민은 자신의 기록을 소유하고, 국가는 인프라를 소유합니다. 어느 쪽도 해외의 허니팟에 의존하지 않으며, 어느 쪽도 2장과 3장에서 설명한 공격이 노리도록 만들어진 단일·중앙집중·전체 기록 표적을 제공하지 않습니다.

따라서 국가 의사결정권자에게 제안하는 바는 “해외 의료기기를 구매하라”가 아닙니다. “모든 시민이 각자 회복력 있는 기록을 휴대하는, 공격에 강한 주권적 국가 보건 인프라를 구축하라”는 것입니다.

9. 결론 및 행동 제안

지난 3년간의 증거는 하나의 결론을 가리킵니다. 보건의료의 사이버 위기는 지나가기를 기다리면 되는 일시적 급증이 아니며, 중앙집중식 모델을 점진적으로 강화하는 것으로는 해결되지 않습니다. 데이터와 기능이 한곳에 집중되어 있는 한, 공격자의 경제성과 방어자의 불리함은 그대로 유지되고 모든 침해는 여전히 전면적입니다. AI 기반 자율 공격의 등장은 대응을 미룰 마지막 이유마저 없앱니다. 다음 물결이 시작되면 그 속도는 어떤 기관의 대응보다 빠르며, 이미 갖춰져 있던 것만이 피해를 제한할 것입니다.

지속 가능한 해답은 아키텍처에 있습니다. 기록의 보관 권한을 환자에게 돌려주고, 기록이 어디로 이동하든 암호화되고 오프라인에서 사용할 수 있는 상태로 유지하며, 국가 집계 데이터를 주권 인프라 안에 보관하는 것. 이 세 가지가 함께 현대 보건의료 공격이 의존하는 허니팟과 단일 장애점을 제거합니다. WaveMed와 RadCard는 동일한 취약 설계를 둘러싼 더 튼튼한 벽이 아닙니다. 세계에서 가장 많이 공격받는 자산이 더 이상 한곳에 모여 탈취되기를 기다리지 않는, 전혀 다른 설계입니다.

사전 배치가 핵심인 만큼, 권장 경로는 다음 사고 이후가 아니라 지금 시작하는 단계적 접근입니다.

1. **시범 도입** — 특정 시설이나 지역에서 시행하며, 오프라인 데이터 가용성, 식별 오류 감소, 네트워크 장애 모의 상황에서의 진료 연속성을 측정합니다.
2. **주권 인스턴스 구축** — 국내 iSAVE 환경을 국가 보건 인프라로 구축하고, 환자 소유 기록과 국가 집계 데이터를 분리하는 명확한 거버넌스를 마련합니다.
3. **전 국민 발급** — 의료기관, 클리닉, 정부 채널을 통해 RadCard와 RadPatch를 단계적으로 배포하여, 필요한 순간이 오기 전에 환자 보유형 회복력 계층이 시스템 전반으로 확산되도록 합니다.

보건의료 시스템이 공격을 받을지가 아니라 언제 받을지가 문제인 시대, 그리고 공격자가 점점 더 어떤 팀의 대응보다 빠르게 공격하는 기계가 되어 가는 시대에, 국가가 확보할 수 있는 가장 강력한 입지는 공격이 닥치더라도 기록을 빼앗기지 않는 입지입니다. WaveMed는 바로 그 입지를 제공하기 위해 만들어졌습니다.

참고문헌

1. U.S. Federal Bureau of Investigation — 2025 Internet Crime reporting; healthcare ranked top sector (via AHA, Apr 2026).
2. Comparitech — Healthcare Ransomware Roundup: 2025.
3. HIPAA Journal — healthcare breach statistics and largest breaches of 2025.
4. JAMA Network Open (Jiang et al., 2025) — ransomware attacks and data breaches in US healthcare; Change Healthcare scale and cost.
5. Sophos — State of Ransomware in Healthcare 2025 (shift to data extortion; staffing as top contributing factor).
6. Trend Micro — 2026 security predictions (autonomous / agentic AI ransomware).
7. CrowdStrike — 2025 ransomware report (76% of organizations unable to keep pace with AI-enhanced attacks).
8. Malwarebytes / Cybersecurity Dive — first AI-orchestrated attacks (2025); autonomous ransomware pipelines forecast (2026).
9. ISACA — AI-driven ransomware and new threat groups (2026); documented state-linked LLM-agent intrusion.
10. Microsoft / Intelligent CIO Africa / ITWeb Africa — Africa healthcare cyberattack volume (~3,575/week, +38%).
11. INTERPOL — African Cyberthreat Assessment (healthcare breach trend).
12. BBC World Service — How 100 Romanian hospitals switched to pen and paper to defeat a national cyber-attack (Feb 2024 Hippocrates / BackMyData incident), June 2026.
13. WaveMed / RadCard Concept Paper v50 and iDataMap Product Portfolio (내부 원천 문서 / internal source documents).