위험 대비 또는 위험 노출

COHESITY

의료 산업의 사이버 레질리언스 격차

사이버 공격은 더 이상 고립된 사건이 아니라 디지털 세계의 지속적인 특징입니다. 전 세계의 의료 기관들이 점점 더 자주 공격의 표적이 되면서, 우리는 이에 대한 경종을 매일 다시금 듣게 됩니다. 어떤 조직도 안전지대에 있지 않으며, 위협의 빈도와 정교함이 증가함에 따라 재정, 운영, 평판에 측정 가능한 피해를 초래하는 중대한 사이버 공격이 급증하고 있습니다.

전 세계 의료 기관의 IT 및 보안 운영 의사결정자 약 400명을 대상으로 실시한 설문조사에서 이러한 현실이 드러납니다.

85%
의료 기관의 85%가 중대한 사이버 공격을 경험한 것으로 나타났습니다.

66%
는 지난 12개월 동안 공격을 받은 것으로 나타났습니다.

3곳 중 1
곳은 여러 차례 공격을 경험했습니다.

피해의 상처는 깊게 파고들며 **비용은 급격히 쌓여갑니다.**

92% 매출 손실

59% 가 환자 또는 고객을 상실

80% 상장 의료 기관이 재무 전망을 수정해야 했음

97% 가 규제 또는 법적 결과에 직면함

94% 지난 12개월 동안 88%가 몸값을 지불함

명백한 증거가 있음에도 불구하고, 많은 조직들이 자사의 레질리언스를 과대평가합니다.

49%
는 자사의 사이버 레질리언스 전략에 대해 완전한 신뢰를 가지고 있음

대부분은 대응과 복구라는 동등하게 중요한 기능보다 예방과 탐지를 여전히 우선시합니다.

NIST 사이버 보안 프레임워크에 기반한 순서.
박스 크기는 사이버 레질리언스 투자 비율이 높은 순서부터 낮은 순서로 표시됩니다.

#2 식별 ····· **#1** 보호 ····· **#3** 탐지 ····· **#4** 대응 ····· **#5** 복구

신뢰도와 소비 패턴은 이야기의 **일부에 불과합니다.**

진정한 레질리언스는 이를 뒷받침하는 실천과 역량에 달려 있습니다. 실제 성능 기준에 따라 평가했을 때, **데이터 보호, 데이터 복구, 위협 탐지 및 조사, 애플리케이션 레질리언스, 데이터 위험 최적화라는** 다섯 가지 핵심 영역에서 성숙도를 보여주는 조직은 단 2%에 불과합니다.

11% 가장 미성숙한

17% 신흥

64% 개발 중

7% 진보하는

2% 가장 성숙한

레질리언스 강화의 필요성에 대한 인식이 자동화와 AI를 동력으로 하는 차세대 진화를 주도하고 있습니다. 위협이 더욱 빠르고 복잡해짐에 따라 자동화는 탐지 가속화, 대응 효율화, 복구 강화의 핵심 요소입니다.

61%

는 사이버 공격 이후 얻은 주요 교훈 중 하나로 탐지, 대응, 복구 전반에 걸친 자동화 개선을 꼽음

37%

는 자율적 의사결정을 비롯하여 위협 탐지 및 대응 과정에서 AI가 핵심적인 역할을 할 것이라고 생각함

99%

2026년까지 99%가 데이터 보안 운영을 지원하기 위해 AI를 사용할 계획임

위험에 대비하고 계십니까?

- 자세한 결과를 확인하려면 사이버 레질리언스 의료 산업 보고서를 다운로드하세요.
- 랜섬웨어 레질리언스 워크숍 예약하기.
- “**사이버 레질리언스를 위한 5단계**” eBook을 받아 오늘부터 성숙도를 높여 보세요.

Vanson Bourne은 2025년에 북미, 아시아태평양, 유럽, 라틴아메리카 지역에서 직원 수 1,000명 이상의 조직을 대표하는 IT 및 보안 리더 3,200명을 대상으로 설문조사를 실시했습니다. 이 가운데 371명은 의료 기관 소속 응답자였습니다.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200028-001-KO 4-2026