핵심 인사이트

41%

헬스케어 서비스 생태계에서 결제 기업을 표적으로 삼은 API 공격의 비율

헬스케어 생태계에서 API 공격은 꾸준히 증가하고 있으며, 특히 결제업체와 보험회사가 보유한 보호 건강 정보(PHI), 청구 데이터, 금융 정보 등 풍부한 정보로 인해 이들에 대한 공격이 증가하고 있습니다.

API 스프롤은 데이터에 대한 무단 접속과 같은 심각한 리스크를 초래합니다.

API 스프롤 또는 기업 내에서 규제되지 않은 API의 확산은 가시성 부족과 보안 제어 범위를 벗어난 API의 출현으로 인해 심각한 보안 공백을 야기할 수 있습니다. 결과적으로 API 스프롤은 기업의 공격표면을 확장하고 민감한 데이터에 대한 무단 접속과 같은 리스크를 초래합니다.

88%

EMEA 지역의 제약사를 대상으로 한 레이어 7 DDoS 공격의 비율

EMEA 지역의 제약사는 레이어 7 DDoS 공격을 가장 많이 경험했으며, 북미와 아시아 태평양 및 일본(APJ)이 그 뒤를 이었습니다. 2024년 상반기 데이터를 자세히 살펴보면 EMEA와 북미 지역에 대한 공격 건수가 2023년에 모든 지역의 총합을 넘어설 것으로 예상됩니다.

2100만

헬스케어 공급업체에 대한 월평균 웹 애플리케이션 및 API 공격 건수

데이터 상호 운용성 및 기타 컴플라이언스 요구사항에 대한 압박이 증가하면서 웹 애플리케이션 및 API 사용이 증가했고, 이로 인해 헬스케어 공급업체와 환자 모두에게 보안 리스크가 발생했습니다.

4.15억

헬스케어 공급업체에 대한 월평균 레이어 7 DDoS 공격 건수

헬스케어 업계에서는 핵티비즘과 현재의 지정학적 환경으로 인한 DDoS 공격이 급증하고 있습니다. 이러한 공격은 서비스 중단과 장애를 일으켜 환자의 치료 결과를 위협할 수 있습니다. 2023년, Killnet은 주로 헬스케어 기업에 영향을 미친 대규모 DDoS 캠페인을 시작했습니다.