솔루션 브리프

헬스케어 분야에서 랜섬웨어를 대적하는 5단계 방법

퓨어스토리지의 현대적인 데이터 보호 기능으로 환자와 비즈니스를 보호하세요.

최근 전 세계의 여러 의료 시설들이 랜섬웨어 공격을 받아 업무가 마비되는 사태가 발생했습니다. 미 정부 기관들은 앞으로 수개월 내에 헬스케어 업계에 더 많은 공격이 발생할 것이라고 경고하고 있습니다. Cybersecurity Ventures는 2021년 말까지 매 11초마다 새로운 조직이 랜섬웨어 공격의 피해자가 될 것으로 내다봤습니다. 병원에는 데이터의 잠금 해제 또는 복호화에 드는 비용 일부를 부담해주는 보험 정책이 있긴 하지만, 이러한 정책은 완전한 보장이나 안전망을 제공하지는 못합니다. 또한 대가를 지급하는 것은 사이버 범죄를 더욱 부추길 수 있습니다. 이에 따라 미 재무부는 랜섬웨어 공격자에게 대가를 지불하는 병원이나 대리인에게는 민사 처벌을 내린다는 방침입니다.

환자 치료에 영향을 미치는 랜섬웨어 복구 시간

랜섬웨어 공격으로 병원의 전자 의료 기록(EHR) 시스템을 사용할 수 없게 되면, 문제는 더 커질 수 있습니다. 랜섬웨어 공격으로 인해 EHR 시스템의 가동이 중단되면 임상 결정이 지연되고 의료 과실을 야기할 수 있으며, 심하게는 환자의 사망으로 이어질 수도 있습니다.

헬스케어 조직에 대한 랜섬웨어 공격은 EHR 운영 데이터베이스뿐만 아니라, 공격으로부터 복구하는 데 사용하는 백업 데이터까지 암호화합니다. 이렇게 공격이 정교해짐에 따라, 헬스케어 조직은 현대적인 사이버 보호 전략을 통해 랜섬웨어 방어 및 복구 문제를 해결해야 합니다.

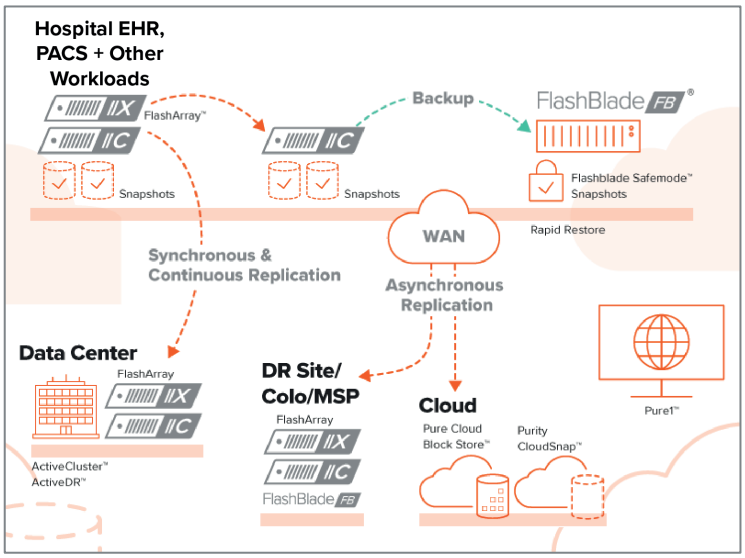
사이버 보호 수준을 한 단계 높여주는 5단계 프레임워크

랜섬웨어 복구
세이프모드(SafeMode™) 스냅샷 기능이 포함된 퓨어스토리지의 플래시블레이드(FlashBlade®)는 데이터 보호 전략을 강화하여 랜섬웨어 복구를 가속화합니다.

데이터 보호
현대적인 데이터 보호를 도입하고 사일로화 된(siloed) 기존 솔루션을 통합합니다.

백업 및 복원
퓨어스토리지의 현대적인 아키텍처는 가장 중요한 데이터를 신속하게 백업하고 복원합니다.

다음은 공격으로부터 데이터를 보호하기 위해 수행할 수 있는 5가지 단계와 퓨어스토리지가 어떤 도움을 줄 수 있는지에 대해 설명합니다.



1단계: 가시성 향상. 이 단계는 보유하고 있는 장비와 그 이유를 파악하는 것입니다. 병원 지하에 아무도 모르게 방치되어 있는 서버는 방어에서 가장 취약한 연결점이 될 수 있습니다. 각 자산의 재고를 관리하고 침입점을 모니터링하여 침입을 나타내는 이상 징후를 찾는 것이 중요합니다.

- 퓨어1 메타(Pure1 Meta®) 분석 플랫폼은 수천 대의 장치로부터 수집된 인텔리전스를 합성합니다.
- 퓨어스토리지의 플래시블레이드에 Splunk나 Elasticsearch를 결합하면 강력한 데이터 분석 및 보안 플랫폼이 구축됩니다.

2단계: 제어 보장. 인프라를 가상 울타리로 둘러싸 액세스를 제어합니다. 직원들이 여러 곳에 분산되어 있고 재택 근무가 보편화되면서, 사이버 보호에 대한 새로운 접근 방식이 요구되고 있습니다. 플래시어레이(FlashArray™)는 처음부터 VDI를 더 빠르게 실행하고 시장에 출시된 다른 어떤 제품보다도 높은 집적도를 제공하도록 설계되었습니다.

3단계: 노출 감소. 이 단계에서 중요한 것은 탐지만이 아닙니다. 지속적으로 유지 관리 및 모니터링되는 환경을 구축해야 합니다. 이를 위해서는 복잡한 분석에 필요한 방대한 양의 데이터를 수집해야 합니다. 신속하게 결과를 제공하도록 설계된 인프라를 갖추는 것이 중요한 이유입니다.

- 평가를 통해 조직이 랜섬웨어 공격에 준비가 되어 있는지 확인해야 합니다.

4단계: 공격 비용 증가. 퓨어스토리지의 세이프모드 스냅샷은 변경 불가능한 백업을 통해 복원성을 제공하므로, 관리자 자격증명이 손상된 경우에도 공격자나 악의적인 내부자가 백업을 삭제할 수 없습니다. 또한 세이프모드 스냅샷은 공격이 발생할 경우 데이터를 보호해줍니다. 암호화를 통합하면 공격하는 것이 더 어렵고 비용이 많이 들게 됩니다. 2019 RSA 컨퍼런스에서 퓨어스토리지와 Thales는 효율적인 스토리지 관리를 위해 Vormetric Transparent Encryption for Efficient Storage 솔루션을 선보였습니다. 이 솔루션은 IT 및 보안 업계 최초로 스토리지 어레이 데이터 절감를 실현하는 엔드 투 엔드 데이터 암호화 프레임워크입니다.

5단계: 대응 및 진화. 공격 발생 후 최대한 신속하게 대응 및 복구하여 진화하는 능력이 매우 중요합니다. 코헤시티(Cohesity®)로 구동되는 퓨어스토리지의 플래시리커버(FlashRecover™)는 업계 최초로 공동 설계된 올플래시 최신 데이터 보호 솔루션으로, 빠른 백업 및 대규모의 신속한 복구 속도를 제공합니다.

- 퓨리티 액티브DR(Purity ActiveDR™)은 빠른 백업을 보장하는 강력한 데이터 복제 기능을 제공하며, 플래시블레이드(FlashBlade)는 시간당 최대 270TB의 빠른 복원 역량을 제공합니다.
- MEDITECH 사용자들을 위해 퓨어스토리지는 BridgeHead Software, AWS, Healthcare Triangle 과 파트너십을 맺고 AWS의 퓨어 클라우드 블록 스토어(Pure Cloud Block Store™)로 MEDITECH 백업의 생성, 저장 및 복제를 자동화하는 서비스형 백업 (Backup as-a-Service, BaaS)을 제공합니다.

purestorage.com/kr
02-6001-3330

PURESTORAGE®

PS1946-01 11/2020