핵심 요약

격리된 볼트, AI 기반 ML 분석 소프트웨어 등을 사용하여 사이버 랜섬웨어 위협으로부터 데이터를 보호하고 사이버 회복탄력성 강화

Dell Technologies PowerProtect Cyber Recovery with CyberSense 사용

사이버 위협의 빈도가 지속적으로 증가하고 공격 방법이 진화함에 따라 데이터 보호 계획은 가장 표면적인 것부터 가장 심층적인 범위에 이르기까지 모든 IT 구성 요소를 보호하고 분석하는 접근 방식을 취해야 한다. Dell PowerProtect Cyber Recovery는 가장 중요한 기밀 데이터를 보호하는 동시에 사이버 공격이나 기타 운영 중단 이벤트에 대비하여 적절한 복구를 보장하는 데 도움이 될 수도 있다.

Dell PowerProtect Cyber Recovery는 랜섬웨어, 파괴적인 사이버 공격 및 예기치 않은 이벤트로부터 조직이 데이터와 애플리케이션을 보호하도록 지원하는 데이터 관리, 보호 및 복구 솔루션이다. 이 솔루션은 다중 복제 접근 방식을 사용한다. 즉, 백업을 생성한 후 보호 및 분석을 위해 이러한 백업을 격리된 스토리지에 복사한다. PowerProtect Cyber Recovery는 하나 이상의 스토리지 볼트를 비롯하여 여러 구성 요소로 구성되며, PowerProtect DD(이전 명칭 Data Domain) 어플라이언스의 온프레미스 또는 소프트웨어 정의 Dell APEX Protection Storage for Public Cloud(이전 명칭 DD Virtual Edition)를 통해 클라우드에 위치할 수 있다. 두 경우 모두 볼트는 운영상 에어 갭, 즉 운영 환경과 격리되어 있다. 온프레미스 환경의 경우 물리적으로 격리되어 있을 수 있고, APEX 환경의 경우 논리적으로 격리되어 있을 수 있다. 따라서 악의적인 행위자나 권한이 없는 사용자가 로그인하여 백업 복제본을 훼손하기가 매우 어렵다.

PowerProtect Cyber Recovery에는 랜섬웨어 공격으로 인한 손상 징후를 확인하기 위해 볼트의 데이터, 파일, 데이터베이스 및 이미지를 자동으로 검사하는 완전 자동화된 통합 지능형 보안 분석 엔진인 CyberSense도 포함되어 있다. CyberSense는 전체 콘텐츠 분석을 제공하고, 파일에서 관찰한 내용을 가져와 AI(Artificial Intelligence) 기반 ML(Machine Learning) 모델의 입력으로 사용하고, 랜섬웨어 또는 파괴적인 공격을 나타낼 수 있는 핵심 인프라스트럭처(Active Directory 및 DNS 포함), 사용자 파일 및 중요한 운영 데이터베이스의 대량 삭제, 암호화 및 기타 의심스러운 변경 사항을 포함한 악의적인 활동을 탐지한다. CyberSense가 손상 패턴을 탐지하면 PowerProtect Cyber Recovery 대시보드에 알림이 생성되어 공격의 규모 및 영향에 대한 추가 정보를 제공한다.[1]

PowerProtect Cyber Recovery는 조직이 사이버 공격을 완화하고, 여러 위치에서 여러 데이터 백업 복제본을 사용하여 데이터 회복탄력성을 강화하고, 다운타임을 줄이고, 비즈니스 연속성을 유지하는 데 도움이 된다. 이 보고서에서는 공개된 데이터를 사용하여 주요 데이터 보호 기능을 강조하고 CyberSense의 경쟁 분석 결과를 제시한다.

기밀 데이터 보호

물리적 및 논리적으로 격리된 볼트로 백업 복제 중에 전송 중인 변경 불가능한 데이터 암호화

SQL Server 페이지 손상 감지

CyberSense는 경쟁 솔루션으로는 찾을 수 없었던 감염을 발견

손상되지 않은 백업 복제본 식별

CyberSense는 복구를 위한 감염되지 않은 최신 백업 복제본을 식별

보안

Dell PowerProtect Cyber Recovery는 랜섬웨어 및 기타 정교한 위협으로부터 중요한 데이터를 보호하고, 권한이 없는 사용자가 기밀 정보에 액세스하는 것을 방지하며, 조직이 정상 운영을 재개할 수 있도록 신속하게 복구할 수 있는 여러 가지 보안 기능을 제공한다.

PowerProtect DD 어플라이언스의 특징과 기능은 PowerProtect Cyber Recovery 솔루션이 제공하는 보안, 무결성 및 복구에 매우 중요할 수 있다. 이러한 기능에는 Retention Lock, DDBoost, RBAC(Role-Based Access Control), 이중 권한 부여 등이 있다.

격리

데이터 격리는 무단 액세스를 방지하기 위해 장벽 또는 경계에 의해 생성된 데이터에 대한 액세스를 분리하고 제한하는 것을 말한다. 격리에는 종종 영구 연결 대신 임시 네트워크 연결이 사용된다.

데이터 격리는 악의적인 행위자가 구성 수정, 데이터 삭제, 정책 변경 또는 사용자 자격 증명을 위한 네트워크 트래픽 스니핑을 시도할 수 있는 감염된 네트워크에서 중요한 데이터가 연결되지 않은 상태로 유지되는 데 도움이 된다. 격리는 공격 노출 지점을 축소하여 악의적인 행위자가 액세스하고 제어권을 얻을 수 있는 기회를 줄이는 데에도 도움이 된다. 또한 조직에서는 권한이 있는 직원에게만 액세스를 제한하여 권한이 없는 사용자가 데이터를 덮어쓰는 것을 방지할 수 있다.

앞서 언급한 기능 외에도 PowerProtect Cyber Recovery는 에어 갭 형태로 물리적 및 논리적 격리를 제공하여 데이터를 보호하는 데 도움이 될 수 있다. 물리적으로 격리된 온프레미스 PowerProtect DD는 볼트 역할을 할 수 있으며, 이 경우 운영 환경의 사용자 또는 시스템은 구성 요소에 액세스할 수 없고, 볼트는 운영 네트워크에서 물리적으로 분리된다.[2] 운영 네트워크에서 복구 환경에 대한 액세스를 제거함으로써 조직은 공격 노출 지점을 축소할 수 있다.

불변성*

백업을 변경 불가능한 읽기 전용으로 만들면 조직이 복구를 위해 이러한 백업을 신뢰할 수 있도록 하는 데 도움이 된다. 운영 측면에서 불변성은 데이터의 진정성과 신뢰성을 유지하는 데 도움이 된다. PowerProtect Cyber Recovery 솔루션에 포함된 DD 시스템은 MTree라는 파일 시스템의 논리적 파티션을 사용하여 데이터를 저장하는 방식에 불변성을 제공할 수 있다. 또한 이 솔루션은 MTree 복제를 사용하여 DDBoost 프로토콜을 통해 운영 DD에서 볼트의 다른 DD로 변경 불가능한 데이터 복제본을 복제한다.[3]

*Dell 제품은 중요한 데이터를 보호하려는 고객의 노력을 지원하도록 설계되었습니다. 다른 전자 제품과 마찬가지로 데이터 보호, 스토리지 및 기타 인프라스트럭처 제품에도 보안 취약성이 발생할 수 있습니다. 고객은 Dell에서 보안 업데이트를 제공하는 즉시 설치하는 것이 중요합니다.

CyberSense

데이터를 효과적으로 보호하려면 모든 수준에서 보안을 제공하는 포괄적인 전략이 필요하다. Dell PowerProtect Cyber Recovery 솔루션의 모든 자가 복구, 보안, 불변성 및 격리 기능에도 불구하고, 명확하지 않은 공격이 여전히 데이터 백업 수준 등 엔터프라이즈 인프라스트럭처에 더 깊이 침투하여 운영 데이터나 전체 사용자 그룹이 손상될 때까지 탐지되지 않을 가능성이 있다. Dell PowerProtect Cyber Recovery 솔루션은 사이버 공격에 대한 마지막 방어선과 CyberSense를 통한 신속한 복구에 도움이 되는 효율적인 접근 방식을 제공한다.

본 연구에서는 CyberSense와 유사한 크기의 어플라이언스에 대해 유사하게 작동하는 경쟁업체(이하 "공급업체 X") 데이터 관리 플랫폼의 툴을 테스트했다. 테스트에서 PowerProtect Cyber Recovery가 SQL 데이터베이스 페이지에서 감염을 탐지한 것으로 확인되었고, 이는 공급업체 X 솔루션은 탐지할 수 없는 것이었다. PowerProtect Cyber Recovery는 공급업체 X 솔루션보다 데이터 손상을 파악하는 데 필요한 백업 횟수도 적었다.

1. Dell, "CyberSense® for PowerProtect Cyber Recovery"(2023년 9월 8일 액세스), https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, "MTree replication"(2023년 9월 11일 액세스), https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3
3. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack"(2023년 8월 21일 액세스), http://facts.pt/rkew01n.

▶ 이 요약의 원본 영어 버전 확인

보고서 보기 ▶

Principled Technologies®

Facts matter.®