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.

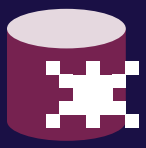
Dell PowerProtect Cyber Recovery는 랜섬웨어, 파괴적인 사이버 공격 및 예기치 않은 이벤트로부터 조직이 데이터와 애플리케이션을 보호하도록 지원하는 데이터 관리, 보호 및 복구 솔루션이다. 이 솔루션은 다중 복제 접근 방식을 사용한다. 즉, 백업을 생성한 후 보호 및 분석을 위해 이러한 백업을 격리된 스토리지에 복사한다. PowerProtect Cyber Recovery는 하나 이상의 스토리지 볼트를 비롯하여 여러 구성 요소로 구성되며, PowerProtect DD(이전 명칭 Data Domain) 어플라이언스의 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 중요하다. 다음과 같은 기능이 제공됩니다.

1. **불변성**
   변경 불가능한 데이터는 수정하거나 삭제할 수 없으며 쓰기만 가능하다. DD 시스템은 운영 시스템과 사이버 볼트 모두에 변경 불가능한 백업을 쓸 수 있다. 즉, 악의적인 행위자가 어떻게든 백업 시스템에 액세스하더라도 기존의 보호된 복제본은 수정 또는 삭제하거나 손상시킬 수 없다.[2] DD 시스템이 운영 환경에서 생성하는 모든 백업은 즉시 변경 불가능해지며, IT 담당자가 보안을 강화하기 위해 볼트에 복사할 수 있다. 이 보고서의 다음 섹션에서는 불변성에 대해 자세히 알아본다.

2. **보존 잠금**
   DD 보존 잠금 기능을 사용하면 미리 정해진 기간 동안 데이터가 변경 불가능해진다. 이 솔루션을 통해 데이터가 보존 잠금 상태로 전환되면 잠금 기간이 만료될 때까지 어떤 사용자나 시스템도 해당 데이터를 변경, 삭제 또는 수정할 수 없다.[3]

   보존 잠금에는 거버넌스 및 규정 준수 모드가 있다. 규정 준수 모드에서는 고객이 다양한 규제 표준을 충족할 수 있다. 한 독립적인 타사에서 DD 보존 잠금이 SEC 규칙 17a-4(f)(2) 및 240.18a-6(e)(2)과 FINRA 규칙 4511(c)에 지정된 스토리지 요구 사항을 충족한다는 것을 증명한 바 있다.[4] 이 기능은 FDA 21 CFR Part11, Sarbanes-Oxley Act, IRS 98025 및 97-22, ISO 표준 15489-1, MoREQ2010을 준수하기 위한 조직의 노력을 지원하는 데에도 도움이 될 수 있다.[5]

   공격자가 시스템 클록을 변경하여 보존 잠금을 우회하려고 시도할 수 있고, 그러면 솔루션이 파일을 예상보다 일찍 삭제하게 되므로 DD에는 내부 보안 클록이 있다. 시스템은 보안 클록과 시스템 클록의 시간을 정기적으로 비교한다. 단일 역년 내에 두 클록 간의 누적된 시간 차이가 2주에 이르면 시스템은 데이터 액세스를 방지하기 위해 DDFS(DD File System)를 자동으로 비활성화한다.[6]

3. **DDBoost를 통한 전송 중인 데이터 암호화**
   전송 중인 데이터는 상당한 보안 위험을 초래할 수 있다. DDBoost는 백업 서버 또는 애플리케이션 클라이언트에서 모든 데이터가 아닌 고유한 데이터 세그먼트만 네트워크를 통해 DD 어플라이언스로 전송할 수 있도록 함으로써 전송 중인 데이터의 양을 제한한다. 또한 조직은 인증서 유무에 관계없이 데이터 인증 및 암호화에 DDBoost 프로토콜을 사용할 수 있다. 인증서가 있으면 데이터 전송 기능의 보안이 강화된다. 전송 중 암호화를 사용하면 애플리케이션이 시스템에서 LAN을 통해 전송 중인 백업을 암호화하거나 데이터를 복원할 수 있다. 클라이언트는 TLS(Transport Layer Services)를 사용하여 클라이언트와 시스템 간의 세션을 암호화할 수 있다.[7]

4. **DD OS(DD Operating System) 보안**
   DD 보안 기능은 운영 체제로도 확장된다. DD OS는 보안을 위해 Bash 셸에 맞춤형 액세스 제어 및 제한을 구현한다. 제한된 Bash 셸 모드에서는 사용자가 자신의 역할과 작업에 필요한 미리 정의된 명령 집합만 수행할 수 있다. DD OS는 시스템에 대한 무단 또는 의도치 않은 수정을 수행하는 정의되지 않은 명령을 차단하여 데이터 무결성을 강화한다.[8]

5. **RBAC(Role-Based Access Control) 및 DDFS(DD Filesystem) 보안**
   DD 시스템은 파일 시스템 내의 파일과 데이터를 보호하기 위해 여러 가지 방법을 사용한다. 첫째, DD 시스템은 관리자가 특정 권한을 가진 역할을 정의하고 사용자를 해당 역할에 할당할 수 있도록 하는 RBAC를 제공한다. 적절한 권한을 가진 권한이 부여된 사용자만 어플라이언스와 해당 데이터에 액세스할 수 있다. 이를 통해 사용자는 작업을 수행하는 데 필요한 기능과 데이터에만 액세스할 수 있으므로 무단 액세스나 우발적인 데이터 유출의 위험이 감소한다.

   DDFS는 또한 데이터 무결성 검증에 해싱을 사용한다. 해싱은 주어진 키나 문자열을 다른 값으로 변환한다. 어플라이언스는 논리적 스토리지 컨테이너에 고유한 데이터 청크를 저장하고, 파일 시스템은 데이터 청크와 컨테이너를 모두 해시한다. 시스템이 데이터를 검색하면 DDFS에 저장된 해시 값과 일치하도록 데이터의 해시 값을 다시 계산하며, 이는 데이터가 변조되거나 손상되지 않았는지 확인하는 데 도움이 된다.[9]

6. **이중 역할 권한 부여**
   조직에서 DD 보존 잠금 규정 준수 모드를 활성화하면 DD 시스템은 이중 로그온 형태로 추가적인 관리 보안을 제공한다. 즉, 시스템 관리자와 권한이 부여된 두 번째 사용자(예: 보안 책임자)가 함께 로그온해야 한다. DD 보존 잠금 규정 준수 모드의 이중 로그온 메커니즘은 보존 기간이 만료되기 전에 잠긴 파일의 무결성을 저해할 수 있는 행위를 방지하는 기능을 한다.[10]

7. **DIA(Data Invulnerability Architecture)**
   DD OS는 하드웨어 및 소프트웨어 오작동으로 인한 데이터 무결성 문제를 방지하기 위해 포괄적인 검증, 장애 방지 및 억제, 지속적인 장애 감지 및 복구, 파일 시스템 복구 가능성을 제공한다. DD 시스템이 백업 소프트웨어로부터 쓰기 요청을 받으면 먼저 데이터 세그먼트의 지문을 계산하고 시스템에 저장된 기존 지문과 비교하여 이중화에 대해 데이터 세그먼트를 분석한다. 고유한 데이터 세그먼트와 해당 지문만 디스크에 저장된다. 그런 다음 DD는 디스크에서 연속적으로 데이터를 다시 읽고, 읽은 지문을 다시 계산하고, 디스크의 지문과 일치하는지 확인한다. DD 시스템은 손상된 데이터를 재구성하고, 이 프로세스 중에 손상을 감지하면(즉, 다시 읽은 내용이 기록된 내용과 일치하지 않는 경우) 데이터를 올바른 상태로 복원하는 자가 복구 프로세스를 수행한다. 또한 자가 복구 프로세스는 플랫폼의 무결성에 영향을 미칠 수 있는 다른 변경 사항으로부터 시스템을 보호하는 데 도움이 된다.

불변성*

백업을 변경 불가능한 읽기 전용으로 만들면 조직이 복구를 위해 이러한 백업을 신뢰할 수 있게 된다. 운영 측면에서 불변성은 데이터의 진정성과 신뢰성을 유지하는 데 도움이 된다.

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

운영 방식

DD 시스템은 MTree를 사용하여 데이터를 저장하는 방식에 불변성을 제공한다. MTree는 파일 시스템의 논리적 파티션이다. 애플리케이션이 MTree에 데이터를 쓸 때 DD 시스템은 Fast Copy라는 기능을 사용하여 원래 MTree의 시점 복제본을 새 MTree에 생성한다. 새 MTree 내에서 DD는 보존 기간에 정의된 기간 동안 사용자 또는 프로세스가 새 MTree를 삭제할 수 없도록 보존 잠금을 적용한다. 새 MTree는 변경 불가능한 데이터 복제본이며 원래 MTree와 독립적이다.[11]

또한 PowerProtect Cyber Recovery 솔루션은 MTree 복제를 사용하여 DDBoost 프로토콜을 통해 운영 DD에서 볼트의 다른 DD로 변경 불가능한 데이터 복제본을 복제한다.[12] 두 DD 간의 초기 동기화에서 솔루션은 모든 데이터를 볼트 DD에 복제한다. 이후에 동기화할 때는 매번 새 데이터 세그먼트와 변경된 데이터 세그먼트만 복제한다. 이 보고서의 뒷부분에서 설명할 CyberSense는 볼트의 모든 변경 불가능한 복제본을 검사하여 잠재적인 손상이 있는지 확인한다.

불변성에 대한 접근 방식

변경 불가능한 백업을 삭제해야 하는 경우는 드물지만 그러한 시나리오는 발생할 수 있다. 조직에서는 삭제할 수 없는 변경 불가능한 백업이 누적되면 용량 및 그에 따른 비용 문제에 직면하게 될 수 있다. 백업을 저장하려면 막대한 용량이 필요할 수 있으며, 이로 인해 초기 하드웨어 투자 외에도 지속적인 운영, 관리 및 모니터링 비용이 소요된다. 변경 불가능한 백업을 주기적으로 삭제하면 이러한 문제를 해결하는 데 도움이 될 수 있다.

앞서 언급했듯이 Dell PowerProtect Cyber Recovery는 보존 잠금 및 기타 툴을 활용하여 불변성을 제공한다. 보존 잠금은 두 가지 모드인 규정 준수와 거버넌스를 통해 고객이 불변성을 구현하는 방식에 약간의 수정을 가할 수 있으므로 어느 정도 유연성을 제공한다. 불변성은 사용자나 악의적인 행위자가 백업을 삭제할 수 없음을 의미하지만, 스토리지 용량 문제와 같은 특정한 경우에는 PowerProtect Cyber Recovery를 통해 고객이 보존 잠금 - 거버넌스 모드를 통해 백업을 삭제할 수 있다.

PowerProtect Cyber Recovery와 비교했을 때, 다른 회사의 유사한 제품은 어떠한가? Cohesity Cyber Recovery, Veeam, Rubrik 및 Veritas NetBackup에 대해 공개된 정보를 살펴보았다. Cohesity Cyber Recovery를 제외한 모든 솔루션은 온프레미스 또는 오프프레미스에 상주할 수 있다. Cohesity는 AWS에서 지원하는 클라우드 기반 솔루션이다. 4개 솔루션에 대한 설명서에서는 불변성을 제공한다고 주장하지만, Rubrik과 NetBackup은 PowerProtect Cyber Recovery와 몇 가지 차이점이 있다.

Rubrik의 경우 관리자는 백업을 삭제할 수 있지만 클라이언트 측에서는 삭제할 수 없고, 특정 제어 기능이 적용된 경우에만 삭제할 수 있다. 또한 모든 쓰기는 "위치 외"로 수행된다. 즉, 새로운 쓰기는 이전에 쓰여진 데이터에 영향을 미치지 않는다.[13]

불변성을 제공함에도 불구하고 NetBackup WORM 지원 스토리지 내의 백업에 대해서는 관리자나 악의적인 행위자가 잠금을 삭제할 수 있다. 그런 다음 bpexpdate 명령을 사용하여 이미지를 삭제할 수 있다.[14]

격리

데이터 격리는 무단 액세스를 방지하기 위해 장벽 또는 경계에 의해 생성된 데이터에 대한 액세스를 분리하고 제한하는 것을 말한다. 격리에는 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 운영 에어 갭 형태로 물리적 및 논리적 격리를 모두 제공하여 데이터를 보호하는 데 도움이 될 수 있다. PowerProtect Cyber Recovery는 백업 데이터가 운영 네트워크에서 물리적으로 분리되어 격리된 위치에 저장되는 물리적 에어 갭과 논리적으로 분리된 백업 복제본을 운영 환경에서 분리하기 위해 네트워크 액세스 제어를 사용하는 논리적 에어 갭을 모두 사용할 수 있다. 논리적 에어 갭만으로는 볼트에 대한 네트워크 액세스 권한이 있는 내부 사용자가 데이터에 액세스하고 데이터를 손상시키는 것을 막을 수 없기 때문에 두 가지 유형의 에어 갭을 모두 사용하는 것이 중요하다.

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.[15] 운영 네트워크에서 복구 환경에 대한 액세스 권한을 제거함으로써 조직은 공격 노출 지점을 줄일 수 있다. 앞서 언급했듯이, 격리된 데이터에 액세스하려면 별도의 보안 자격 증명과 MFA(Multi-Factor Authentication)가 필요하다.[16]

격리에 대한 접근 방식

Gartner는 "IDV(Immutable Data Vault)가 포함된 IRE(Isolated Recovery Environment)는 내부자 위협, 랜섬웨어 및 기타 형태의 해킹에 대한 최고 수준의 보안 및 복구 기능을 제공한다"고 말한다.[17] 또한 "IDV가 포함된 IRE는 기존 백업 및 DR(Disaster Recovery) 시스템을 대체하는 것이 아니라, 영향을 받은 시스템을 복구하기 위한 모든 툴, 프로세스 및 리소스를 갖춘 IRE에서 변경 불가능한 3차 백업 복제본을 제공함으로써 이를 보완한다"고 언급한다.[18]

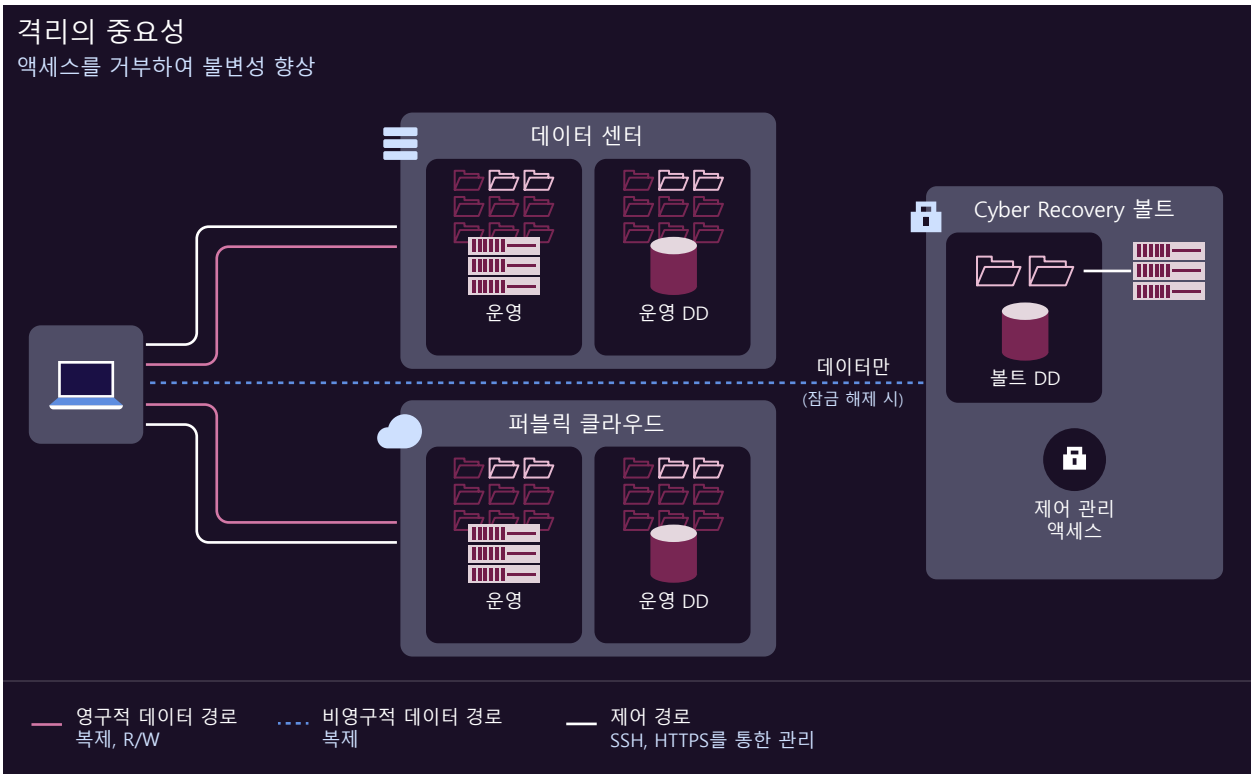
Cohesity, Veeam, Rubrik 및 Veritas 솔루션에 대해 공개된 정보를 검토하는 동안 각 솔루션이 IRE에 대해 PowerProtect Cyber Recovery와는 최소한 약간씩 다른 접근 방식을 취한다는 사실을 발견했다. Dell 솔루션을 통해 고객은 DD 볼트를 운영 환경에서 물리적 또는 논리적으로 격리하여 운영 환경의 제어 및 데이터 플레인을 볼트와 분리할 수 있다. 또한 PowerProtect Cyber Recovery는 다른 모든 솔루션과는 달리 에어 갭을 자동화한다.

문서에 따르면 다음과 같다.

- Cohesity Cyber Recovery는 AWS 기반 FortKnox 볼트에 대해 동적으로 자동화된 논리적 에어 갭만 제공한다.[19]
- Veeam은 Veeam Cloud Connect를 통해 퍼블릭 및 프라이빗 클라우드 공급업체를 위한 자동화되지는 않은 논리적 에어 갭을 지원한다. Veeam은 또한 솔루션을 위한 온프레미스 볼트 역할을 하고 조직이 물리적 에어 갭을 갖도록 구성할 수 있는 Veeam Hardened Repository도 제공한다.[20]
- Rubrik은 Rubrik Cloud Vault에 자동화된 에어 갭을 제공하지 않지만, 고객이 Microsoft와의 제3자 파트너십을 통해 논리적 에어 갭을 추가할 수 있다.[21]
- NetBackup 고객은 논리적 에어 갭을 수동으로 활성화해야 하며, 온프레미스 또는 오프프레미스 솔루션을 통해 물리적 에어 갭을 생성할 수 있다.[22]

운영 방식

그림 1에는 격리된 Cyber Recovery 볼트의 네트워킹 경로가 나와 있다. 볼트에는 공격 지점을 줄이기 위한 운영 환경에 대한 관리 또는 제어 경로가 없다.



1: Cyber Recovery 볼트의 개략적인 데이터 및 제어 경로 아키텍처이다. 출처: Principled Technologies

Cyber Recovery 볼트에 필요한 유일한 연결은 주기적인 데이터 동기화를 위한 데이터 경로이다. 동기화란 Cyber Recovery 솔루션이 복제를 위해 짧은 정책 기반 간격으로 데이터를 수집하는 것을 말한다.[23] PowerProtect Cyber Recovery 솔루션 가이드에 따르면, "기본 수준의 Cyber Recovery 솔루션 아키텍처는 PowerProtect DD 시스템 쌍과 Cyber Recovery 관리 호스트로 구성된다. 이 기본 수준 구성에서는 관리 호스트에서 실행되는 Cyber Recovery 소프트웨어가 Cyber Recovery 볼트의 PowerProtect DD 시스템에서 복제 컨텍스트와 함께 복제 이더넷 인터페이스를 활성화 및 비활성화하여 운영 환경에서 볼트 환경으로의 데이터 흐름을 제어한다."[24] Dell Technologies는 조직이 데이터 경로를 보호하고 격리할 수 있는 추가적인 방법을 제안한다. 테스트 과정에서는 복제 도중 및 복제 후에 Cyber Recovery가 볼트를 잠금 해제하고 잠그는 것이 관찰되었다.

볼트의 물리적 구현을 위한 Dell Technologies의 권장 사항에 따르면, "물리적 액세스 제어 기능이 있는 전용 룸 또는 케이지에 Cyber Recovery 볼트 장비를 설치하는 것이 좋다. 이 보안 룸에는 키 로그아웃 또는 2인 키 액세스가 포함된 제한된 액세스 목록이 있어야 한다. 케이지 또는 룸으로 들어가는 진입 지점 및 장비에 대한 영상 관제가 마련되어 있어야 한다. 최고 수준의 보안을 위해 Cyber Recovery 소프트웨어는 Cyber Recovery 관리 서버에 대한 물리적 액세스 및 해당 키보드와 마우스를 통해서만 액세스할 수 있어야 한다."[25]

관리 경로와 제어 경로를 분리함으로써 Cyber Recovery의 물리적 및 논리적 에어 갭 격리 옵션은 다른

솔루션과 차별화된다. 일부 솔루션은 운영 환경 인터페이스에서 볼트 데이터에 액세스할 수 있도록 허용한다. 그러면 볼트 데이터가 운영 데이터와 동일한 공격 노출 지점에 배치되어 악의적인 행위자가 손상된 자격 증명을 사용해 백업 복제본에 액세스할 가능성이 있다.

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. CyberSense는 AI 기반 ML 분석 알고리듬을 사용하여 볼트의 백업과 백업 내 파일의 사용자 콘텐츠에 대한 무결성을 검사하고 검증하는 분석 엔진이다.

CyberSense는 운영 환경에서 격리된 볼트 내에서 실행된다. 볼트 내의 파일, VM 이미지 및 데이터베이스를 모니터링하고 데이터의 무결성을 분석하여 공격이 발생했는지 확인한다. Cyber Recovery 솔루션이 백업 복제본을 볼트에 복제하고 보존 잠금 기능을 적용하면 CyberSense는 자동으로 복제본을 검사하여 파일, 데이터베이스 및 핵심 인프라스트럭처에 대한 시점 관찰 정보를 생성한다. 분석 엔진은 메타데이터뿐만 아니라 파일의 전체 콘텐츠와 각 데이터베이스 페이지를 검사한다. 다른 솔루션이 데이터 임계값 또는 메타데이터의 변경 사항을 찾는 반면, CyberSense는 파일의 콘텐츠를 살펴보고 데이터 무결성을 검증한다. 이러한 관찰을 통해 CyberSense는 파일과 데이터베이스가 시간이 지남에 따라 어떻게 변경되는지 추적하고 숨겨진 다양한 고급 공격 유형을 밝혀낼 수 있다. 그런 다음 CyberSense는 파일 암호화, 삭제, 생성 또는 난독 처리 등 악의적인 행위자 활동을 나타낼 수 있는 손상 패턴을 탐지하는 분석을 생성한다.[26] 다른 솔루션은 분석을 클라우드로 푸시하여 공격 노출 지점을 넓힐 수 있는 반면, 조직은 CyberSense를 온프레미스에서 또는 Cyber Recovery가 지원하는 여러 클라우드 옵션 중 하나에서 실행하도록 선택할 수 있다.

CyberSense는 200개 이상의 분석과 데이터 관찰 결과를 결합하여, 시간이 지남에 따라 관찰이 축적될수록 더 유용한 정보를 제공한다. ML 알고리듬은 수천 건의 멀웨어 감염에 대한 정보를 사용하여 비정상적인 동작 패턴을 찾고 사용자 활동을 랜섬웨어와 구분하는 동시에 거짓 양성 및 거짓 음성을 최소화한다. 이 알고리듬은 지속적인 연구를 통해 공격 변형 등의 새로운 사항에 대한 교육을 받는다. 또한 ML 알고리듬은 기존 CyberSense 고객의 실제 데이터를 기반으로 업데이트를 받는다.[27]

아울러 CyberSense는 Dell, IBM, CommVault 및 Veritas의 공통 디스크 백업 형식으로 데이터를 인덱싱할 수 있도록 지원한다.[28] Dell Technologies는 다른 공급업체의 백업 형식을 지원함으로써 데이터 백업 측면에서 고객의 요구에 부응하려는 의지를 보여준다.

본 연구에서는 두 가지 턴키 엔터프라이즈 데이터 보호 및 사이버 복구 솔루션의 ML 기반 지능형 분석 소프트웨어를 테스트했다. 하나는 Dell PowerStore™ 7000T에서 구동되는 Dell PowerProtect Cyber Recovery용 CyberSense이고, 다른 하나는 유사한 크기의 어플라이언스에 대해 유사하게 작동하는 경쟁업체("공급업체 X") 데이터 관리 플랫폼의 툴이다.

테스트 방법

모든 테스트를 원격으로 진행했으며 테스트 베드에 대한 완전한 통제권과 제한 없는 액세스 권한을 확보했다. Dell 솔루션(CyberSense, PowerProtect Data Manager 백업 애플리케이션, APEX Protection Storage(이전 DD Virtual Edition) 및 PowerProtect Cyber Recovery 솔루션 등)과 공급업체 X 솔루션은 모두 오프사이트 데이터 센터 랩에 있었다.

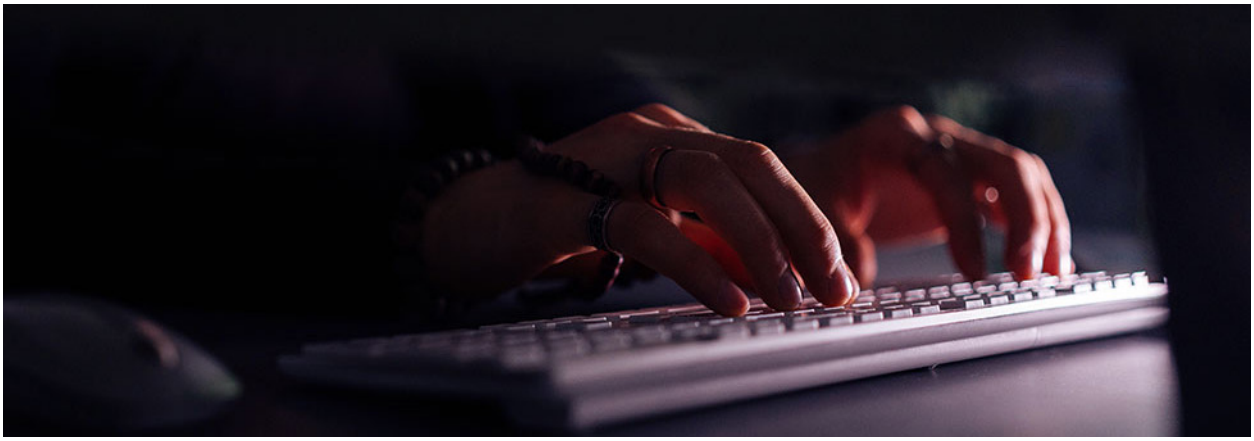
두 솔루션 모두에서 백업을 타겟으로 하는 스크립트 기반의 악의적인 이벤트 시나리오 세 가지를 실행했다.

그림 2: 테스트 시나리오. 출처: Principled Technologies.

두 솔루션 모두에서 처음 두 시나리오는 동일한 일반 절차를 따랐다. 먼저, Dell PowerProtect Data Manager 및 공급업체 X 스토리지 어플라이언스에서 모든 클린 VM의 전체 백업을 생성하고, 스캔을 위한 증분 백업을 생성하고, 타겟 솔루션이 위협을 감지하지 못하는지 확인했다. 이를 통해 공격 스크립트를 실행할 수 있는 기준 백업 세트가 제공되었다.

다음으로, 운영 체제와 애플리케이션 유형이 서로 다른 4개의 VM에서 랜섬웨어 시뮬레이션 스크립트를 실행하고, 타겟 어플라이언스에서 새로운 증분 백업을 수행하고, 타겟 분석 소프트웨어가 암호화 위협을 감지했는지 확인했다.

세 번째 시나리오(SQL Server 페이지 감염)에서는 다른 두 시나리오와 유사한 절차를 따르되, 대신 SQL VM에 초점을 맞추고 암호화 스크립트가 아닌 페이지 손상 스크립트를 사용했다. 단일 VM에서 스크립트를 실행했다.



연구 결과

시나리오 1: 난독 처리된 파일 이름의 암호화된 파일 탐지

이 시나리오에서는 파일을 암호화하고 이름을 난독 처리하여 파일의 내용뿐만 아니라 메타데이터도 변경하는 악의적인 이벤트를 시뮬레이션했다. 이러한 유형의 공격은 일반적으로 랜섬웨어라고 하며, 시스템 소유자 또는 사용자가 미리 정해진 금액을 지불할 때까지 악성 소프트웨어가 컴퓨터 시스템에 대한 액세스를 차단하는 보안 이벤트이다. 미국 CISA(Cybersecurity and Infrastructure Security Agency)에 따르면, "랜섬웨어와 데이터 갈취로 인한 경제적 영향과 평판에 미치는 영향은 모든 규모의 조직에 초기 중단 기간과 때로는 장기적인 복구 기간 동안 곤란과 막대한 비용을 끼치는 것으로 검증되었다."[29] 지능형 분석 소프트웨어를 사용하여 백업의 암호화를 탐지하면 조직의 데이터 보호 전략을 강화하고, 중요한 기밀 정보를 보호하며, 사이버 공격으로 인한 비용이 많이 드는 다운타임 가능성을 줄일 수 있다.

테스트에서는 두 지능형 분석 애플리케이션 모두 파일 이름이 변경된 암호화된 파일을 찾아냈다. 공급업체 X 솔루션은 감염을 탐지하기 전에 15개의 기준 백업(전체 백업 1개와 증분 백업 14개)이 필요한 반면, CyberSense는 전체 백업 1개만으로 감염을 탐지했다. 즉, 공급업체 X 솔루션은 CyberSense와 대조적으로 14개의 추가 백업이 필요했다.

공급업체 X 솔루션은 의심스러운 활동에 대해 알렸을 때 많은 파일이 제거되고 동일한 수의 파일이 추가되었다는 것만을 지적했는데, 이는 백업의 엔트로피 등급을 기준으로 볼 때 의심스러운 활동이었다.[30] 공급업체 X 솔루션은 파일이 암호화되었거나 파일 이름이 변경되었음을 지적하지 않았다. 반면 Cyber Recovery with CyberSense는 파일 이름이 암호화되고 난독 처리되었음을 알려주었다.

공급업체 X의 결과는 거짓 양성을 나타낼 수 있다. 즉, 조직이 공급업체 X 솔루션을 사용해 일일 백업을 실행한다고 가정하면, 이상 징후가 탐지되기 전에 14일 분의 감염된 파일을 수집했을 수 있는 것이다. 반면 CyberSense는 감염 및 그 세부 사항에 대한 정보를 알리는 데 하나의 기준 백업만 필요했다. 예시의 이 단계에서 Cyber Recovery를 사용한 복구는 격리된 볼트에서 수행되며, 조직은 공급업체 X 솔루션과는 달리, 감염된 14개 백업에 운영 네트워크가 노출되지 않았음을 확신할 수 있다.

그림 3: 각 솔루션에서 손상을 감지하기 위한 기준을 생성하는 데 필요한 백업 수.
출처: Principled Technologies.

시나리오 2: 원래 파일 이름의 암호화된 파일 탐지

이 시나리오는 첫 번째 시나리오와 유사하지만, 스크립트는 암호화된 파일의 원래 파일 이름을 그대로 유지했다. 이 변경 사항은 파일의 메타데이터에는 영향을 주지 않고 파일 자체에만 영향을 주었다. 이러한 행위는 일정 기간 잠복한 뒤 활성화되는 시한폭탄 랜섬웨어일 수 있다. 시한폭탄 랜섬웨어는 탐지를 회피하고 백업을 타겟으로 하기 때문에, 조직에 백업이 필요할 때 감염된 백업은 무용지물이 될 수 있다.[31] 메타데이터에 변화가 없으면 파일이 표면적으로는 감염되지 않은 것처럼 보일 수 있어 잠복해 있는 공격을 계속 숨길 수 있다.

테스트에서는 두 지능형 분석 애플리케이션 모두 암호화된 파일을 찾아냈다. 이 시나리오에서도 공급업체 X 솔루션은 이상 징후를 탐지하기 전에 14개의 증분 백업을 포함하여 15개의 기준 백업이 필요했다. CyberSense는 이상 징후를 탐지하기 전에 하나의 기준 전체 백업만 필요했다.

첫 번째 시나리오에서와 마찬가지로, 공급업체 X 솔루션은 많은 파일이 변경되었다는 것만 알렸는데, 이는 백업의 엔트로피 등급을 기준으로 볼 때 의심스러운 활동이었다. 이 솔루션은 파일이 암호화되었다는 것을 지적하지 않았지만, Cyber Recovery with CyberSense는 이를 알려주었다. 이러한 방식으로 손상을 감지한다는 것은 CyberSense가 표면 수준의 메타데이터만이 아니라 파일의 내용을 살펴본다는 것을 의미한다. 이러한 유형의 검사는 백업에 대한 보안을 한층 더 강화하여 디지털 인프라스트럭처나 자산 전체의 보안을 강화한다. CyberSense는 "진정한" 지능형 분석 애플리케이션이라고 할 수 있다. 또한 CyberSense를 사용하면 솔루션이 기준을 생성하는 데 필요한 백업이 훨씬 적기 때문에 조직은 손상을 더 빨리 감지할 수 있다. 조직의 백업 일정에 따라 며칠 더 빨라질 수 있다.

그림 4: 각 솔루션에서 손상을 감지하는 데 필요한 백업 수. 출처: Principled Technologies.

시나리오 3: SQL Server 페이지 손상 감지

이 시나리오에서는 SQL Server 페이지를 손상시키는 악의적인 이벤트를 시뮬레이션했다. SQL Server에서 데이터 스토리지의 기본 단위는 페이지이며, 데이터베이스는 전체 데이터 페이지를 읽거나 쓴다.[32] 이 시나리오에서도 이 변경 사항은 메타데이터에는 영향을 주지 않고 파일 자체에만 영향을 주었다. 이러한 유형의 공격은 일반적으로 SQL 삽입으로 알려져 있으며, 공격자는 웹 페이지 입력을 통해 SQL 문에 악성 코드를 삽입하여 SQL 데이터 기반 애플리케이션을 타겟으로 한다.[33] 감염되었더라도 데이터베이스는 계속 실행될 수 있다. 데이터 도난 외에도 SQL Server 페이지가 손상되면 데이터 무결성 문제, 데이터 손실 및 데이터베이스 기능 중단이 발생할 수 있다. 이러한 결과는 조직의 평판을 훼손하고, 운영 워크플로를 중단시키고, 금전상의 손실을 초래하고, 심지어 법적 책임을 초래할 수도 있다.

처음 두 시나리오에서는 CyberSense와 Vendor X 솔루션 모두 암호화를 탐지했지만, 세 번째 시나리오에서는 CyberSense만 SQL Server 페이지의 손상을 탐지할 수 있을 만큼 심층적으로 검사할 수 있었다. 이는 두 솔루션이 어느 정도 수준에서 유사한 탐지 기능을 제공하는 반면, CyberSense는 잠재적으로 비즈니스 크리티컬 SQL Server 기반 애플리케이션의 백업에 대한 심층 검사를 제공한다는 것을 보여준다. 이러한 방식으로 CyberSense는 심층 검사와 더 포괄적인 보호를 통해 보안 회복탄력성을 한층 더 강화한다.

SQL Server는 금융, 소매, 의료 및 기타 산업의 많은 애플리케이션을 구동한다. SQL Server는 개발 아키텍처의 백엔드 역할을 할 수 있기 때문에, SQL Server 공격은 다운타임 및 작업 중단을 초래할 수 있으며, 이러한 애플리케이션이 창출하는 매출에 위협이 될 수 있다.

Dell PowerProtect Cyber Recovery를 사용한 복원 및 복구

Dell 사이버 회복탄력성 전략은 광범위한 복구 기능을 제공한다. 이러한 복구 옵션에는 인스턴트 액세스나 운영 환경에서 유지되는 변경 불가능한 백업으로부터의 기존 복구와 같은 일반적인 업계 기능이 포함된다. 또한 Dell Technologies는 PowerProtect Cyber Recovery 솔루션의 고유한 복구 기능을 지원한다. PowerProtect Cyber Recovery는 복제본을 격리된 상태로 유지하고 CyberSense를 통해 무결성을 검사하므로, 조직은 공격 직후 복제본에 액세스하고 이를 사용해 복구 단계를 시작하거나 클린룸과 같은 대체 복구 플랫폼으로 즉시 복원할 수 있다.

이 즉각적인 활용 사례를 운영 환경이나 퍼블릭 클라우드에서만 데이터에 액세스할 수 있는 조직과 비교해 보겠다. 조직은 근본 원인을 파악하여 해결하고, 악의적인 행위자의 존속을 차단하고, 보험사와 법무 부서를 위한 포렌식 이미지를 생성하고, 데이터를 다시 검사하고, 백업 인프라스트럭처에 액세스할 수 있는 충분한 가용 인프라스트럭처(AD, DNS)를 확보할 때까지는 손상된 영역에 저장된 데이터에 안전하게 액세스할 수 없다. 공격의 범위와 교묘함에 따라 이 프로세스는 며칠 또는 몇 주가 걸릴 수 있다.

운영 방식

정상적인 운영 중에는 PowerProtect Cyber Recovery가 복구 및 보안 분석을 위한 복원 지점을 자동으로 생성한다. 사이버 공격 발생 시에는 Cyber Recovery가 자동화된 복원 및 복구 절차와 이러한 복원 지점을 사용하여 비즈니스 크리티컬 시스템을 다시 온라인 상태로 전환한다. CyberSense 및 포렌식 보고서는 사이버 보안 및 복구 팀이 공격의 영향을 진단하는 데 도움이 된다. 운영 환경이 정상화되고 복구 준비가 완료되면 Cyber Recovery는 실제 데이터 복구를 수행하는 툴과 기술을 제공한다.

사이버 공격 후에는 복구 속도(CRT(Cyber Recovery Time))와 파괴적인 공격 후 사용자가 복귀할 수 있는 시점(CRP(Cyber Recovery Point))을 결정하기 위해 여러 가지 데이터 보호 지표가 작용한다. Cyber Recovery 솔루션의 경우 이러한 지표에는 다음이 포함된다.

- **DDO(Destruction Detection Objective):** 공격이 발생한 후 공격이 탐지될 때까지 걸리는 시간을 기준으로 하는 이동 구간이다. 분석 및 기타 Cyber Recovery 메커니즘은 이 기간 내에 작동해야 한다.
- **DAO(Destruction Assessment Objective):** 손상 범위와 잠재적 대응을 결정하기 위해 침입 후 사이버 보안 팀에 할당된 시간이다.
- **Cyber Recovery 동기화 간격:** Cyber Recovery 솔루션이 운영 환경에서 볼트로 데이터를 복제하는 빈도이다. 타이밍은 솔루션에 대해 이전에 설정된 RPO(Recovery Point Objective)를 기준으로 한다. 복제본 보존 기간은 솔루션에 따라 다르지만 일반적으로 1주~1개월이다.
- **Cyber Recovery 데이터 복제본 수:** Cyber Recovery 볼트에 보관된 데이터 복제본 수이다. 이 지표를 동기화 간격과 함께 사용하면 조직이 데이터를 얼마나 과거로 복구할 수 있는지에 대한 대략적인 측정값이 도출된다. 예를 들어, 24시간 간격과 7개의 복제본을 결합하면 사용자는 최대 1주 전의 데이터를 복구할 수 있다.

복구 요구 사항 외에 솔루션이 보호하는 데이터 유형도 데이터 동기화 간격과 보존 시간을 결정하는 데 도움이 될 수 있다. Cyber Recovery 솔루션 가이드에 따르면, 복구 유연성을 극대화하기 위해 사용자는 솔루션이 보호하는 데이터를 다음 백업 스트림 중 하나로 분류할 수 있다.[34]

- 기본 수준 운영 체제 배포 및 애플리케이션 빌드를 포함한 바이너리 및 실행 파일 백업

- 이미지 및 애플리케이션별 데이터를 포함한 전체 애플리케이션 및 파일 시스템 백업

이러한 별도의 백업 스트림은 두 가지 복구 전략으로 이어진다.

1. **Cyber Recovery 볼트에서 데이터 및 애플리케이션 바이너리 복원**
   이 솔루션은 가용 복원 지점과 멀웨어 및 멀웨어가 지속된 위치를 식별하고, 백업 이미지에서 멀웨어를 제거할지, 아니면 Cyber Recovery 볼트 복제본을 사용하여 재구축할지를 결정한다. 보안 패치를 적용한 후 솔루션은 애플리케이션에 대한 DR 운영 지침을 사용하여 복구 호스트에 데이터를 복원한 후 복구 프로세스가 멀웨어의 영향을 제거했는지 여부를 확인한다. 그런 다음 볼트 컴퓨팅을 사용하여 애플리케이션에서 테스트 실행을 수행하고, 운영 환경을 정리하거나 재이미징한다. 마지막으로 Cyber Recovery는 복구 호스트를 운영 환경에 연결하고 애플리케이션과 데이터를 운영 환경에 다시 복제한다. 그림 5에 이 프로세스가 나와 있다.

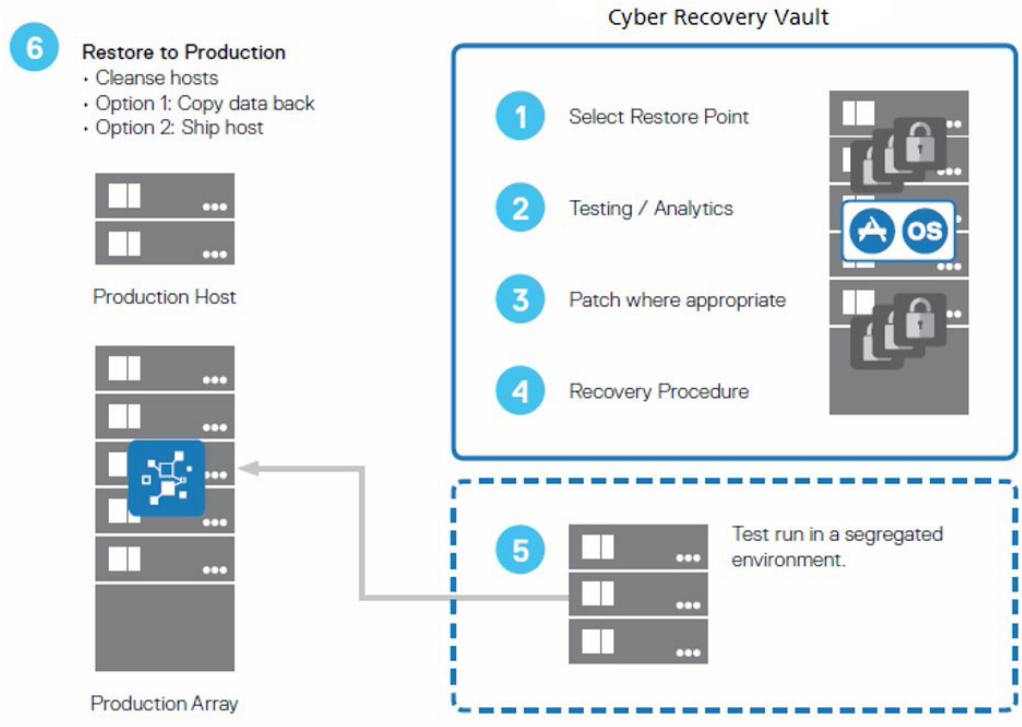
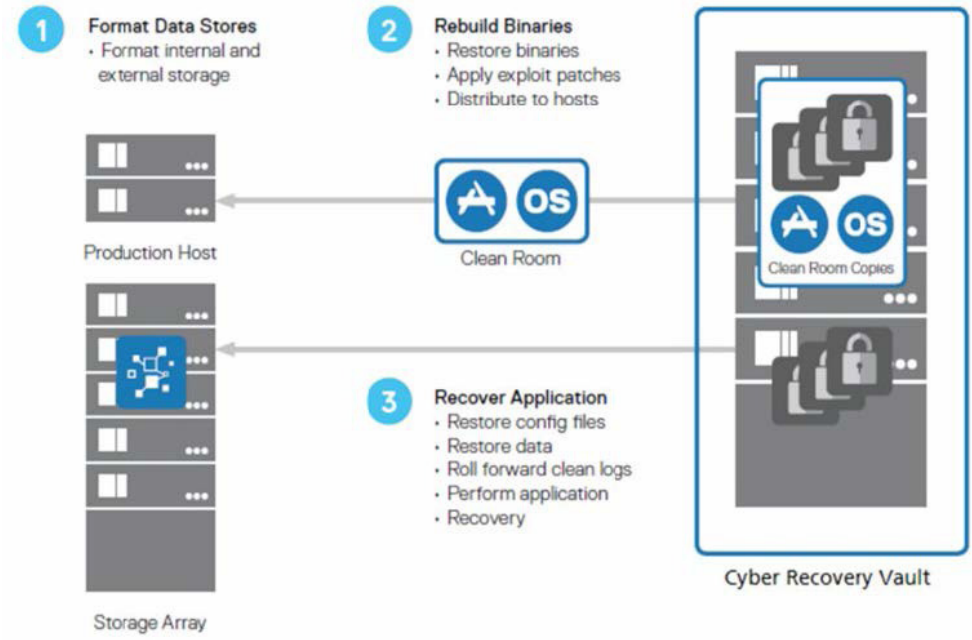


그림 5: 데이터 및 애플리케이션 바이너리를 복원하는 프로세스. 출처: Dell Technologies.[35]

2. **Cyber Recovery 볼트에서 완전히 재구축**
   이 접근 방식에서 Cyber Recovery 솔루션은 인시던트 대응 중 포렌식 평가를 통해 확인된 손상 수준에 따라 운영 시스템을 다시 포맷한다. 그런 다음 솔루션은 Cyber Recovery 볼트의 복제본을 통해 바이너리를 재구축하고 사용 가능한 보안 패치를 적용한다. 마지막으로 애플리케이션에 대한 관련 DR 운영 지침을 사용하여 애플리케이션, 데이터 및 구성 파일의 적절한 복제본을 운영 환경에 복원한다. 그림 6에 이 프로세스가 나와 있다.



6: Cyber Recovery 볼트에서 완전히 재구축하는 프로세스. 출처: Dell Technologies.[36]

Cyber Recovery 솔루션에는 Cyber Recovery 소프트웨어가 복구에 사용할 수 있는 물리적 또는 가상 복구 호스트(또는 둘 다)가 포함된다. 이러한 호스트에는 백업 애플리케이션 및 백업 애플리케이션 카탈로그가 복구되는 지정된 서버인 백업 애플리케이션 복구 서버와 애플리케이션 복구 서버가 모두 포함된다. 조직은 솔루션의 복구 요구 사항에 따라 여러 서버를 구축할 수 있다. Cyber Recovery 소프트웨어는 샌드박스(새로운 소프트웨어 또는 테스트되지 않은 소프트웨어를 안전하게 실행하기 위한 테스트 환경) 데이터 복제본을 호스트에 노출시켜 볼트 내 데이터(예: 파일 시스템 데이터, IBM, CommVault 및 Veritas 백업 데이터)나 Dell NetWorker, Dell Avamar, Dell PowerProtect DP Series Appliance 또는 Dell PowerProtect Data Manager 소프트웨어로 보호되는 데이터의 복구를 수행할 수 있다. 볼트 내에서 백업 애플리케이션을 복구한 후 솔루션은 해당 데이터를 볼트의 추가 복구 호스트에 복원할 수 있다.

조직은 사용자가 Cyber Recovery 솔루션이 보호하는 모든 백업 애플리케이션을 복구할 수 있도록 백업 애플리케이션 복구 서버를 미리 사이징한다. 마찬가지로 애플리케이션 복구 서버는 솔루션이 애플리케이션을 복구하는 지정된 서버이다. 일부 애플리케이션의 경우 고객이 먼저 다른 종속 애플리케이션을 복구해야 할 수도 있다. 볼트 내의 인프라스트럭처는 솔루션이 보호하는 가장 큰 운영 애플리케이션의 복구를 지원할 수 있다.

결론

조직은 데이터 보호 계획을 수립할 때 다양한 공격 벡터를 고려해야 한다. 여기에는 모든 데이터에 대한 보호가 포함되지만, 운영에 필수적인 중요한 데이터를 보호하는 것이 무엇보다 중요하다. PowerProtect Cyber Recovery는 중요한 데이터를 격리하고 사이버 공격 발생 시 적절한 데이터 복구에 도움이 된다. Cyber Recovery는 CyberSense의 ML 기반 분석을 사용하여 볼트에 있는 데이터의 무결성을 확인하고 복구할 클린 백업 데이터를 식별한다. 테스트 결과, PowerProtect Cyber Recovery는 SQL 데이터베이스 페이지에서 감염을 탐지한 것으로 확인되었는데, 이는 경쟁 솔루션은 탐지할 수 없는 것이었다. 또한 PowerProtect Cyber Recovery는 경쟁 솔루션보다 데이터 손상을 파악하는 데 필요한 백업 횟수가 적었다. 이 모든 것 외에도 Cyber Recovery 솔루션은 볼트에 저장된 손상되지 않은 데이터를 활용하여 효율적이고 원활하게 운영을 재개할 수 있는 다양한 복구 옵션을 제공한다.

---

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, "Dell PowerProtect Cyber Recovery Solution Guide", 2023년 8월 23일 액세스, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
4. Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", 2023년 10월 27일 액세스, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, "Data Domain: Retention Lock 자주 묻는 질문", 2023년 9월 12일 액세스, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, "Data Domain: Retention Lock 자주 묻는 질문."
7. Dell, "Encryption types offered by DD series encryption appliance", 2023년 9월 8일 액세스, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, "Dell EMC Data Domain – Security Configuration Guide", 2023년 9월 11일 액세스, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, "Role based access control (RBAC) in Data Domain", 2023년 9월 11일 액세스, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, "Dell EMC Data Domain – Security Configuration Guide."
11. Dell, "MTree replication"(2023년 9월 11일 액세스), https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and limits", 2023년 9월 11일 액세스, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", 2023년 12월 13일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, "NetBackup™ Security and Encryption Guide", 2023년 12월 13일 액세스, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack"(2023년 8월 21일 액세스), http://facts.pt/rkew01n.
16. Dell, "Dell PowerProtect Cyber Recovery", 2023년 9월 12일 액세스, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman & Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware", 2023년 12월 14일 액세스, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman & Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware."
19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era", 2023년 12월 13일 액세스, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, "How to protect your data from ransomware and encryption Trojans", 2023년 12월 13일 액세스, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, "Rest easy with immutable, off-site data storage", 2023년 12월 13일 액세스, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, "NetBackup Isolated Recovery Environment", 2023년 12월 13일 액세스, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)", 2023년 8월 23일 액세스, https://youtu.be/ej5nZzWNRM0.
24. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
25. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
26. Dell, "CyberSense® for PowerProtect Cyber Recovery"
27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines", 2023년 9월 13일 액세스, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, "CyberSense for Dell Cyber Recovery", 2023년 9월 25일 액세스, https://indexengines.com/csmatrix.
29. CISA, "#StopRansomware Guide", 2023년 8월 1일 액세스, https://www.cisa.gov/stopransomware/ransomware-guide.
30. "In security, most people use Shannon Entropy—a specific algorithm that returns a value between 0 and 8. The higher the number, the more random the data, and many times, a higher value means that the data is either packed or encrypted." Mueller, Clint, "How to Use Entropy Analysis in Penetration Testing", 2023년 8월 28일 액세스, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, "How to Protect your Backups from Ransomware in 2023", 2023년 8월 1일, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, "페이지 및 익스텐트 아키텍처 가이드", 2023년 8월 3일 액세스, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, "SQL Injection", 2023년 8월 3일 액세스, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
36. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"

이 보고서에 숨겨진 과학 확인 ▶

▶ 이 보고서의 원본(영문) 보기: https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

이 프로젝트는 Dell Technologies의 의뢰로 진행되었습니다.