DELL Technologies

솔루션 브리프

# Dell PowerProtect Cyber Recovery

랜섬웨어 및 파괴적인 사이버 공격으로부터 중요한 데이터를 보호할 수 있도록 회복탄력성을 갖춘 최신 보호 솔루션

**Cyber Recovery를 선택해야 하는 이유**

사이버 공격은 백업 등 귀중한 데이터를 침해하도록 설계되었습니다. 중요한 데이터를 보호하고 무결성이 보장된 상태로 해당 데이터를 복구하는 능력은 공격 후 정상적인 비즈니스 운영을 재개하는 데 핵심 요인입니다.

*사이버 회복탄력성을 갖춘 솔루션의 구성 요소는 다음과 같습니다.*

**데이터 불변성**
변경할 수 없는 데이터 사본을 만들어 보안 및 제어 계층을 통해 데이터 무결성과 기밀성을 유지합니다.

**데이터 격리 및 거버넌스**
기업 및 백업 네트워크에서 분리되고 적절한 권한을 가진 사용자만 액세스 가능한 격리된 복구 환경을 구축하고 있습니다.

**자동화된 데이터 복제 및 에어 갭**
안전한 디지털 볼트(vault)에 변경 불가능한 데이터 복제본을 생성하고 운영/백업 환경과 볼트 간 운영을 물리적으로 분리하는 프로세스를 확립합니다.

**지능형 분석**
안전한 볼트 내에서 강력한 분석 기능과 더불어 AI 기반 머신 러닝 및 전체 콘텐츠 인덱싱을 사용하는 자동화된 무결성 검사를 통해 데이터가 멀웨어의 영향을 받았는지 확인합니다.

**복구 및 문제 해결**
동적 복원 프로세스와 기존 DR 절차를 사용하여 인시던트 후 복구를 수행하는 워크플로와 툴을 지원합니다.

**솔루션 계획 및 설계** RTO 및 RPO를 결정하고 복구를 효율화하기 위해 중요한 데이터 세트, 애플리케이션, 기타 중요한 자산을 선택하는 전문가 지침을 제공합니다.

## 당면 과제: 데이터 중심 비즈니스 환경에서 가장 큰 골칫거리인 사이버 공격

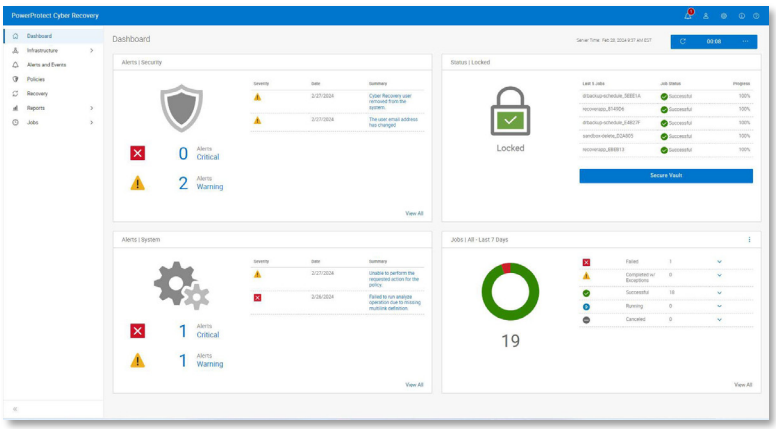
데이터는 디지털 경제의 통화이고, 보호 및 기밀로 유지되면서 즉시 사용할 수 있어야 하는 중요한 자산입니다. 오늘날의 글로벌 마켓플레이스는 상호 연결된 네트워크 전반의 지속적인 데이터 흐름에 의존하며, 디지털 혁신 이니셔티브와 Generative AI의 사용이 증가함에 따라 더 많은 기밀 정보를 위험에 노출시키고 있습니다.

따라서 조직의 데이터는 사이버 범죄자에게 매력적이고 수익성이 높은 표적이 됩니다. 오늘날에는 업종이나 조직의 규모와 관계없이 사이버 공격으로 인해 기업과 정부에서 데이터 손상, 다운타임으로 인한 매출 손실, 평판 손상, 규제에 따른 거액의 과태료 등의 피해가 지속적으로 발생하고 있습니다.

사이버 회복탄력성을 갖춘 전략을 수립하는 것은 기업과 정부 책임자의 의무가 되었지만 아직 많은 조직에서 데이터 보호 솔루션에 대한 확신이 부족한 상황입니다. Global Data Protection Index에 따르면 IT 의사 결정권자의 79%가 향후 12개월 내에 운영 중단 사고를 경험할 것을 우려하고 있으며, 75%는 조직의 기존 데이터 보호 조치가 멀웨어 및 랜섬웨어 위협에 대처하기에 충분하지 않을 수 있다고 우려하고 있습니다[1].

## 솔루션: Dell PowerProtect Cyber Recovery

사이버 공격으로 인한 비즈니스 위험을 최소화하고 사이버 회복탄력성이 뛰어난 데이터 보호 접근 방식을 갖추려면 복구 및 비즈니스 연속성 전략을 현대화 및 자동화하고 최신 지능형 툴을 활용해 사이버 위협을 탐지하고 방어할 수 있어야 합니다.




Dell PowerProtect Cyber Recovery는 회복탄력성이 뛰어나며 검증된 최신 지능형 보호 기능으로 중요한 데이터를 격리하고 의심스러운 활동을 식별하며 데이터 복구 속도를 높여 조직이 중요한 데이터를 더욱 스마트하게 복구하고 정상적인 비즈니스 운영을 신속하게 재개할 수 있도록 지원합니다.

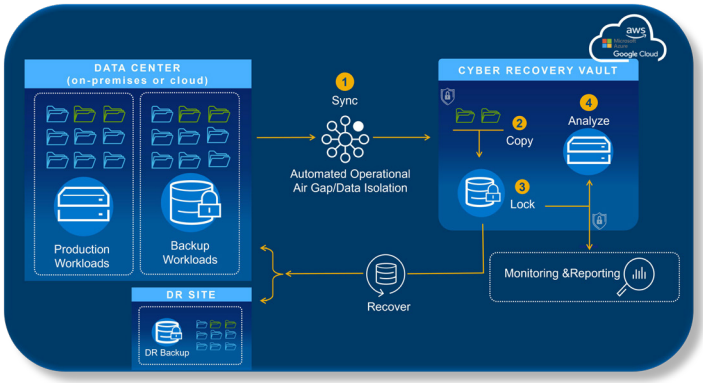
## PowerProtect Cyber Recovery – 불변성, 격리 및 인텔리전스

### 불변성 - PowerProtect Data Domain

PowerProtect Data Domain은 Dell PowerProtect Cyber Recovery의 기반입니다. 여러 계층의 제로 트러스트 보안을 통해 변경 불가능한 백업 복제본을 제공하여 데이터 무결성과 기밀성을 보장합니다. 하드웨어 RoT(Root of Trust), 보안 부팅, 암호화, 보존 잠금, 역할 기반 액세스 제어 및 다단계 인증과 같은 기능은 데이터의 무결성과 복구 가능성을 보장하는 데 도움이 됩니다.

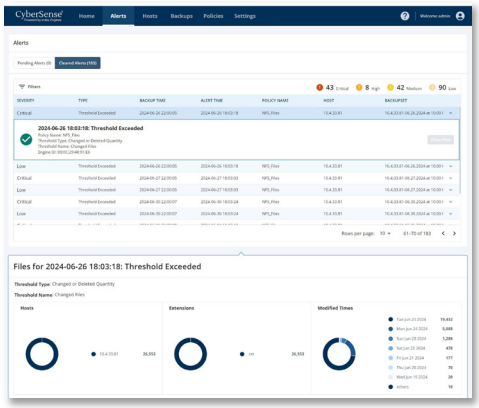
### 격리 - Cyber Recovery 볼트

PowerProtect Cyber Recovery 볼트는 IRE(Isolated Recovery Environment)로, 내부자 위협을 비롯한 사이버 공격 시 회복탄력성을 보장하기 위해 여러 보호 계층을 제공합니다. 운영 에어 갭은 오픈 시스템 및 메인프레임을 비롯한 운영 환경의 공격 표면에서 중요한 백업 데이터 복제본을 물리적으로 격리된 볼트로, 자동으로 이동(동기화)합니다. 중요 데이터가 볼트에 동기화되면 데이터가 수정되지 않도록 변경 불가능한 복제본이 자동으로 생성됩니다. 운영 환경으로부터 독립된 전용 관리, 네트워크 및 서비스를 사용하므로 별도의 보안 자격 증명과 다단계 인증 수단이 있어야 데이터에 액세스하여 복구 및 테스트 작업을 수행할 수 있습니다.




### 인텔리전스 - CyberSense®

PowerProtect Cyber Recovery는 보다 스마트하게 사이버 위협으로부터 복구할 수 있도록 CyberSense®를 완벽하게 통합한 선도적인 솔루션으로, 모든 것이 사이버 복구 볼트의 보안 내에서 이루어집니다. CyberSense는 메타데이터만을 조사하는 솔루션을 넘어서, 전체 콘텐츠분석을 통해 공격 발생 후 99.99%의 정확도[2]로 데이터 손상을 탐지하므로, 지능적이고 신속한 복원이 가능합니다. CyberSense는 변경 불가한 데이터 백업을 활용하여 시간이 지남에 따라 데이터가 어떻게 변하는지 관찰한 다음, AI 기반 머신 러닝을 활용하여 랜섬웨어 공격의 발생을 유추할 수 있는 손상 징후를 탐지합니다. CyberSense는 핵심 인프라스트럭처(Active Directory, DNS 등 포함), 사용자 파일 및 데이터베이스에서 교묘한 공격으로 인한 대량 삭제, 전체 및 부분 암호화 및 기타 의심스러운 변화를 탐지합니다. 맞춤형 임계값 알림을 생성할 수 있으며, 손상의 징후가 탐지될 경우 알림 대시보드 및 공격 후 포렌식 보고서를 통해 주요 시스템을 복구할 수 있는 비감염 데이터 복제본을 식별하는 등 공격의 규모와 영향을 신속하게 진단할 수 있습니다.




## PowerProtect Cyber Recovery – 배포 옵션

### 하이브리드 및 멀티클라우드 환경에서의 사이버 복구

중요 데이터는 온프레미스에 있거나, 서로 다른 데이터 센터에 공동으로 위치하거나, 전 세계의 여러 클라우드와 리전에 위치하는 등 비즈니스 전반에 걸쳐 다양한 곳에 존재할 수 있습니다. 사이버 공격으로부터 데이터를 복구해야 하는 경우, 위치에 상관없이 데이터는 안전하게 보호되며 손상되지 않아야 합니다.

PowerProtect Cyber Recovery는 *AWS*, *Microsoft Azure*, *Google Cloud*의 퍼블릭 클라우드 마켓플레이스를 통해 사용 가능하므로, 빠르게 액세스하여 클라우드 내 사이버 복구 볼트의 데이터를 보호할 수 있습니다. PowerProtect Cyber Recovery는 운영 시스템과 퍼블릭 클라우드의 사이버 복구 볼트 간에 중요 데이터를 자동으로 동기화합니다. 표준 클라우드 기반 백업 솔루션과 달리, 관리 인터페이스에 대한 액세스는 네트워킹 제어를 통해 잠기기 때문에 액세스하려면 별도의 보안 자격 증명과 다단계 인증이 필요합니다. 여러 클라우드에 데이터를 분산하고 복제할 경우 보안 및 규정 준수 위험, 잠재적 동기화 문제, 리소스 비용 증가를 초래할 수 있습니다. 이러한 접근 방식은 다양한 환경 전반에 대한 가시성을 저해하므로 끊임없이 진화하는 사이버 위협에 효율적으로 대응하지 못할 수 있습니다.

Faction 기반의 *Dell PowerProtect Cyber Recovery with MultiCloud Data Services*는 보안 저하 없이 퍼블릭 클라우드 공급업체가 데이터를 동시에 액세스할 수 있도록 하므로, 클라우드 공급업체를 자유롭게 선택할 수 있어 공급업체 종속을 피할 수 있습니다. 이 안전한 데이터 볼팅 서비스는 사이버 공격으로부터 중요한 데이터를 보호하는 안전한 멀티클라우드 지원 인프라스트럭처를 기반으로 구축된 논리적 에어 갭 볼트입니다. 데이터 복구가 필요하면 볼트에서 AWS, Microsoft Azure, Google Cloud, Oracle Cloud 또는 온프레미스 환경으로 데이터를 복원하도록 선택할 수 있습니다.

### Dell APEX Protection Storage All-Flash for Cyber Recovery

중요한 데이터가 계속 늘어나는 가운데, 사이버 이벤트를 신속하고 효율적으로 복구할 수 있는 능력은 비즈니스 연속성과 사이버 회복탄력성을 보장하는 데 매우 중요합니다. 중요 데이터의 관리를 확장하려는 조직은 Cyber Recovery 볼트와 같은 격리된 복구 환경에서 데이터를 효과적으로 검색할 수 있어야 합니다. 소프트웨어 정의 버전의 PowerProtect Data Domain에 기반한 Dell APEX Protection Storage All-Flash는 향상된 CyberSense 분석 및 신속한 복원 기능을 통해 조직 SLA를 준수할 수 있는 간편하고, 에너지 효율적이며, 비용 효율적인 사이버 복구 솔루션을 제공합니다. 하드웨어, 공간 및 에너지를 덜 사용함으로써 데이터 액세스 속도와 운영 효율성을 높이고 데이터 무결성을 보장할 수 있으므로 다운타임과 전체 유지 보수 비용이 줄어듭니다.

## PowerProtect Cyber Recovery – 정상 비즈니스로 복귀

### 복구 및 문제 해결

PowerProtect Cyber Recovery는 자동화된 복원 및 복구 절차를 통해 비즈니스 크리티컬 시스템을 최대한 빨리 안전하게 온라인 상태로 복구합니다. 복구는 인시던트 대응 프로세스와 통합됩니다. 이벤트가 발생한 후 인시던트 대응 팀에서 운영 환경을 분석하여 이벤트의 근본 원인을 확인합니다. CyberSense는 공격 범위를 파악할 수 있도록 공격 후 포렌식 보고서를 제공하며, 손상되기 전 마지막으로 양호한 백업 세트 목록을 제공합니다. 그런 다음, 운영 환경을 복구할 준비가 되면 Cyber Recovery가 실제 데이터 복구를 수행하는 관리 툴 및 기술을 제공합니다.

### 솔루션 전략 및 설계

Dell Professional Services for Cyber Recovery를 이용하면 보호할 비즈니스 크리티컬 시스템을 쉽게 결정할 수 있으며, 관련된 애플리케이션 및 서비스와 이를 복구하는 데 필요한 인프라스트럭처의 종속성 맵을 생성할 수 있습니다. 이 서비스는 또한 복구 요구 사항과 설계 대안을 생성하고, 비즈니스 타당성 및 구축 일정과 함께 데이터를 분석, 호스팅 및 보호하는 기술을 식별합니다.

### 결론

Sheltered Harbor와 같은 산업 이니셔티브는 중요한 시스템에 장애를 일으키는 사이버 공격이 발생할 경우에 대비해 미국 금융 시스템에서 고객, 금융 기관 및 공신력을 보호하고자 PowerProtect Cyber Recovery를 활용하고 있습니다. 여기에는 백업도 포함됩니다. Cyber Recovery with Cyber Sense는 수천 명의 기존 고객을 통해 비즈니스 리더들에게 신뢰감을 주며, 사이버 위협 발생 시 데이터 복구를 가속화하는 것으로 입증되었습니다. Forrester Consulting의 연구에 따르면 사이버 공격 발생 시, PowerProtect Cyber Recovery는 다운타임을 75% 단축하고 복구에 소요되는 시간을 80% 줄이는 데 도움이 됩니다.[3]

PowerProtect Cyber Recovery를 사용하면 정상 데이터를 신속하게 식별 및 복원하고 사이버 공격 후 정상적인 비즈니스 운영을 재개할 수 있다는 확신을 가질 수 있습니다. 이제 정상 비즈니스로 빠르게 복귀할 수 있습니다.

[1] Dell Technologies 의뢰로 Vanson Bourne에서 수행한 연구 "Global Data Protection Index 2024 Snapshot" 기준. 2023년 10월
[2] Index Engines 의뢰로 작성된 ESG 보고서 "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption" 기준. 2024년 6월
[3] Dell Technologies 의뢰로 작성된 Forrester Consulting의 연구 "The Total Economic Impact of Dell PowerProtect Cyber Recovery" 기준, 2023년 8월

Dell PowerProtect Cyber Recovery에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

대화에 참여: #PowerProtect