DELL Technologies

솔루션 브리프

Dell EMC PowerProtect Cyber Recovery

랜섬웨어 및 파괴적인 사이버 공격으로부터 중요한 데이터를 보호하는 것으로 검증된 최신 보호 솔루션

Cyber Recovery를 선택해야 하는 이유

사이버 공격은 백업 등 귀중한 데이터를 파괴하거나 훔치거나 침해하도록 설계되었습니다. 중요한 데이터를 보호하고 무결성이 보장된 상태로 해당 데이터를 복구하는 것은 공격 후 정상적인 비즈니스 운영을 재개하는 데 핵심 요인입니다. 공격을 받은 후에도 비즈니스가 정상적으로 유지될 수 있을까요? 검증된 최신 Cyber Recovery 솔루션의 5가지 구성 요소를 소개합니다.

데이터 격리 및 거버넌스

기업 및 백업 네트워크에서 분리되고 적절한 승인을 거친 사용자 이외의 사용자 액세스를 제한하는 격리된 데이터 센터 환경입니다.

자동화된 데이터 복제 및 에어 갭

프로덕션/백업 환경과 볼트의 운영을 물리적으로 분리하는 프로세스와 안전한 디지털 볼트에 변경 불가능한 데이터 복제본을 생성합니다.

지능형 분석 및 툴

안전한 볼트 내에서 강력한 분석 기능으로 머신 러닝 및 전체 콘텐츠 인덱싱 기능을 제공합니다. 자동화된 무결성 검사를 사용하여 데이터가 멀웨어의 영향을 받았는지 확인하고, 필요한 경우 문제 해결을 지원하는 툴을 제공합니다.

복구 및 문제 해결

동적 복원 프로세스와 기존 DR 절차를 사용하여 인시던트 후 복구를 수행하는 워크플로와 툴을 지원합니다.

솔루션 전략 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 인터넷 경제의 통화이며, 보호되고 기밀로 유지되며 즉시 사용할 수 있어야 하는 중요한 자산입니다. 오늘날의 글로벌 마켓플레이스는 상호 연결된 네트워크 전반의 지속적인 데이터 흐름에 의존하며, 디지털 혁신을 위한 노력은 더 많은 기밀 데이터를 위험에 노출시키고 있습니다.

따라서 조직의 데이터는 사이버 범죄자에게 매력적이고 수익성이 높은 표적이 됩니다.

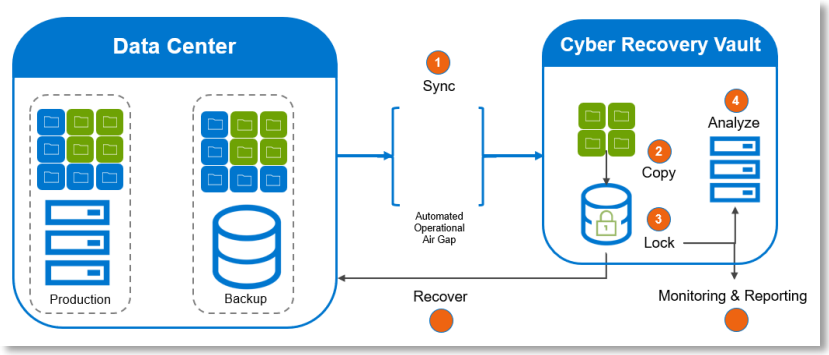
사이버 범죄는 역사상 가장 큰 부(富)의 이전이라고 불려 왔으며, 여기서 가장 중요한 것은 데이터입니다. Accenture에 따르면 향후 5년 동안 전 세계 사이버 범죄 피해액은 5조 2천억 달러에 달할 것으로 예상됩니다.[i]

오늘날에는 업종이나 조직의 규모에 관계없이 사이버 공격으로 인해 기업과 정부에서 데이터 손상, 다운타임으로 인한 매출 손실, 평판 손상, 규제에 따른 거액의 과태료 등의 피해가 지속적으로 발생하고 있다. 2018년 사이버 범죄로 인한 연간 피해 금액은 기업 평균 미화 1,300만 달러까지 증가했으며, 이는 5년 동안 72% 급증된 수치입니다.[ii]

Cyber Recovery 전략을 수립하는 것은 기업과 정부 기관 책임자의 의무가 되었습니다. 2019년 Marsh와 Microsoft의 연구에 따르면 글로벌 경영진의 79%가 사이버 공격을 조직의 가장 높은 위험 관리 우선순위 중 하나로 꼽았습니다.[iii]

그렇다면 조직과 조직의 귀중한 데이터를 보호하려면 무엇을 해야 할까요?

솔루션: PowerProtect Cyber Recovery

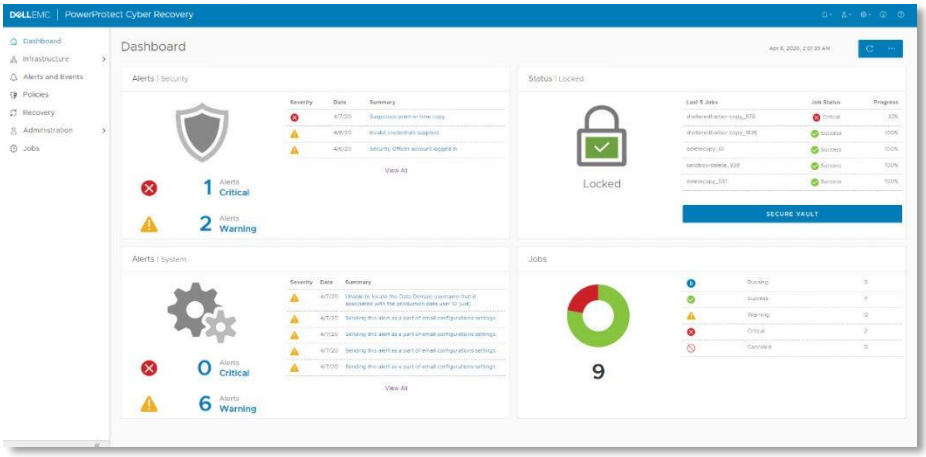


사이버 공격으로 인한 비즈니스 위험을 최소화하고 Cyber Recovery 성능이 뛰어난 데이터 보호 접근 방식을 갖추려면 복구 및 비즈니스 연속성 전략을 현대화 및 자동화하고 최신 지능형 툴을 활용해 사이버 위협을 탐지하고 방어할 수 있어야 합니다.

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

PowerProtect Cyber Recovery – 검증된 최신 지능형 보호 기능으로 사이버 위협으로 인한 비즈니스 위험 최소화

- **Cyber Recovery 볼트** – PowerProtect Cyber Recovery 볼트는 내부자 위협을 포함한 사이버 공격 시 회복탄력성 보장을 위한 여러 보호 계층을 제공합니다. 예를 들어 중요한 데이터를 공격 표면 이외의 위치로 이동하여 데이터 센터의 보호된 위치에서 해당 데이터를 물리적으로 격리하거나, 이 데이터에 액세스하려면 별도의 보안 자격 증명을 제공하고 다단계 인증을 진행하도록 설정합니다. 그 외에도 네트워크를 격리하는 자동화된 운영 에어 갭, 손상 가능성이 있는 관리 인터페이스 제거 등의 보호 기능도 제공됩니다. PowerProtect Cyber Recovery는 운영 시스템과 볼트 간의 데이터 동기화를 자동화하여 변경 불가능한 복제본과 잠금 설정된 보존 정책을 생성합니다. 사이버 공격이 발생하면 사용자는 정상 데이터 복제본을 빠르게 파악하여 중요한 시스템을 복구함으로써 비즈니스 운영을 다시 시작할 수 있습니다.



- **CyberSense** – PowerProtect Cyber Recovery에 완전히 통합된 CyberSense는 사이버 공격이 데이터 센터로 침투하는 경우 데이터 손상을 파악할 수 있는 지능형 보호 계층을 추가로 제공합니다. 이 혁신적인 방식은 전체 콘텐츠 인덱싱 기능을 제공하며, ML(Machine Learning)을 사용해 100가지 이상의 콘텐츠 기반 통계를 분석하여 랜섬웨어로 인한 손상 징후를 탐지합니다. CyberSense의 손상 탐지 신뢰도는 최대 99.5%나 되므로, 사용자는 안전한 볼트 내에서 비즈니스 크리티컬 콘텐츠를 보호하면서 위협을 파악하고 공격 벡터를 진단할 수 있습니다.
- **복구 및 문제 해결** – PowerProtect Cyber Recovery는 자동화된 복원 및 복구 절차를 통해 비즈니스 크리티컬 시스템을 최대한 빨리 안정적으로 온라인 상태로 복구합니다. PowerProtect Data Manager의 일부로 Dell EMC NetWorker Cyber Recovery를 실행하는 고객의 경우 볼트에서 자동화된 복구를 수행할 수 있습니다. Dell EMC와 생태계 파트너는 데이터를 보호하면서 손상 평가 및 포렌식을 수행하여 시스템을 복구하거나 시스템을 공격하는 멀웨어를 제거하고 문제를 해결할 수 있는 종합적인 방법론을 제공합니다.
- **솔루션 전략 및 설계** – 선택 사항으로 제공되는 Dell EMC Advisory 서비스를 이용하면 보호할 비즈니스 크리티컬 시스템을 판단하는 데 도움이 되며, 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 구현 일정과 함께 데이터를 분석, 호스팅 및 보호하는 식별을 식별합니다.

사이버 공격으로부터 중요한 데이터를 보호하려면 검증된 최신 솔루션이 필요합니다. PowerProtect Cyber Recovery를 사용하면 양호한 상태의 데이터를 신속하게 식별 및 복원하고 사이버 공격 후 정상적인 비즈니스 운영을 재개할 수 있다는 확신을 가질 수 있습니다.

Dell EMC PowerProtect Cyber Recovery 에 대한 자세한 정보

Dell EMC 전문가에게 문의

[출처: Accenture, 2019 Cost of Cybercrime 연구]
[출처: Accenture, 2019 Cost of Cybercrime 연구]
[출처: Marsh 및 Microsoft, 2019 Global Cyber Risk Perception 연구