DELL Technologies

솔루션 브리프

Dell PowerProtect Cyber Recovery for Microsoft Azure

랜섬웨어 및 파괴적인 사이버 공격으로부터 중요한 데이터를 보호하는 안전한 퍼블릭 클라우드 볼트

PowerProtect Cyber Recovery for Azure를 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?

데이터 격리 및 거버넌스 액세스가 제한되고 내부 또는 백업 네트워크와 분리되어 있는 Azure를 사용하는 격리된 데이터 볼트 환경

자동 복제 및 에어 갭 운영 환경과 볼트 환경 간의 운영상의 에어 갭을 통해 보호되는 안전한 디지털 볼트로 데이터 복제본 보호

복구 및 문제 해결 동적 복원 프로세스와 절차를 사용하여 인시던트에서 복구를 수행하는 워크플로 및 툴

솔루션 계획 및 설계 성숙도 높고 신뢰할 수 있는 솔루션을 기반으로 구축된 중요 데이터, 애플리케이션 및 기타 자산을 선택하기 위한 Dell Technologies의 전문가 지침

간소화된 배포

Azure Marketplace를 통한 간편한 구매 및 배포로 퍼블릭 클라우드 볼트에 빠르게 액세스

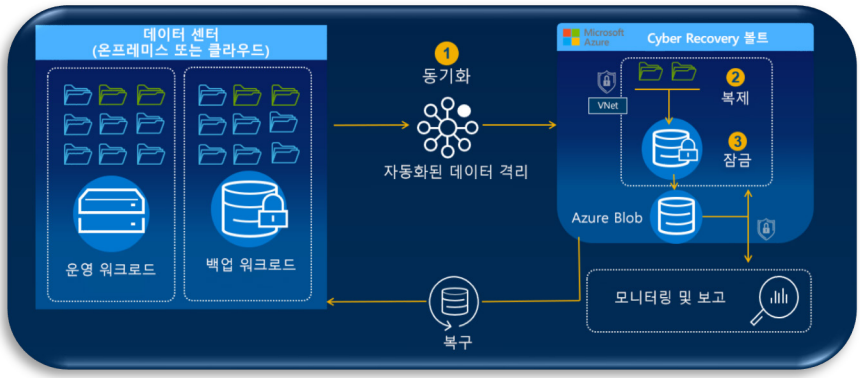
사이버 공격은 데이터 중심 조직의 적

조직 보호는 데이터 보호에서 시작됩니다. 사이버 위협 환경은 끊임없이 변화하고 있으며 기술이 발전함에 따라 계속 성장하고 있습니다. 새로운 공격 전략이 멀웨어와 랜섬웨어에서 디지털 유출로 옮겨가고 있으며, 공격으로 인해 조직의 민감한 내부 데이터가 계속 위험에 노출되고 있습니다. 최근 사이버 공격의 위협에 대응하고 데이터의 기밀성, 가용성 및 무결성을 유지하는 것의 중요성, 특히 오늘날의 데이터 중심 기업, 학교 및 조직에서 중요한 데이터와 시스템을 보호하려면 최신 솔루션과 전략이 필요합니다.

공격이 지속적으로 이루어져 에피소드당 비용은 계속 증가하고 있습니다. 특정 규모의 기업이나 산업만 타겟이 된다고 오해할 수 있지만, 실제로는 규모에 관계없이 모든 업종의 기업이 타겟입니다.

사이버 공격으로 인한 조직의 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.

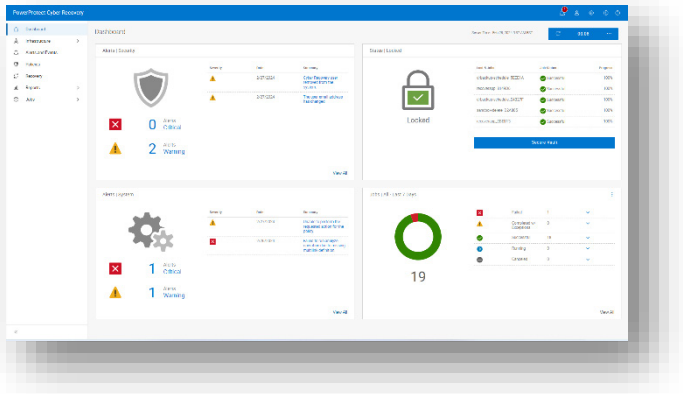
솔루션: PowerProtect Cyber Recovery for Azure



Dell PowerProtect Cyber Recovery for Azure는 검증된 최신 지능형 보호 기능으로 중요한 데이터를 격리하고 데이터 복구 속도를 높여 조직이 정상적인 비즈니스 운영을 신속하게 재개할 수 있도록 지원합니다.

Azure의 Cyber Recovery 볼트

PowerProtect Cyber Recovery for Azure는 여러 보호 계층을 제공하여 사이버 공격 및 내부자 위협에 대한 회복탄력성을 확보할 수 있도록 합니다. 중요 데이터를 공격 노출 지점에서 멀리 옮겨 안전하고 자동화된 운영상의 에어 갭을 통해 물리적이고 논리적으로 액세스할 수 없도록 Azure 내에 격리합니다. 표준 클라우드 기반 백업 솔루션과 달리, 관리 인터페이스에 대한 액세스는 네트워킹 제어를 통해 잠기기 때문에 액세스하려면 별도의 보안 자격 증명과 다단계 인증이 필요할 수 있습니다. PowerProtect Cyber Recovery는 운영 시스템과 Azure의 Cyber Recovery 볼트 간의 데이터 동기화를 자동화하여 잠금 설정된 보존 정책이 적용된 변경 불가능한 복제본을 생성합니다. 사이버 공격이 발생하면 사용자는 정상 데이터 복제본을 빠르게 파악하여 중요한 시스템을 복구함으로써 비즈니스 운영을 다시 시작할 수 있습니다.



사이버 위협으로부터 비즈니스 위험 감소

자동화된 워크플로는 Azure 내에서 비즈니스 크리티컬 데이터를 격리된 환경으로 안전하게 이동합니다. 직관적인 사용자 대시보드를 통해 쉽게 보호 정책을 생성하고 잠재적 위협을 실시간으로 모니터링할 수 있습니다. 볼트는 항상 운영상의 에어 갭을 통해 논리적으로 격리됩니다. 볼트 구성 요소는 운영 환경에서 액세스할 수 없으며 에어 갭 잠금 해제 시 볼트 스토리지에 대한 액세스가 크게 제한되고 안전한 Azure Virtual Network 내에서 보호됩니다.

PowerProtect Cyber Recovery는 운영 시스템과 보안 볼트 간의 데이터 동기화를 처리하여 보호되는 추가 복제본을 생성합니다. 사이버 공격이 이루어지면 권한이 부여된 사용자가 신속하게 데이터에 액세스하여 중요한 시스템을 복구한 다음 조직 운영을 다시 시작할 수 있습니다.

복구 및 문제 해결

PowerProtect Cyber Recovery for Azure는 중요 데이터를 온라인으로 신속하게 복구할 수 있는 유연한 복원 및 복구 옵션을 제공하며 테스트를 마치고 문서화된 복구 프로그램의 지원을 받습니다. Cyber Recovery for Azure를 사용하여 사이버 공격 후 볼트에서 중요 데이터를 복구하거나 복구 테스트 절차를 수행하므로 데이터를 회사 데이터 센터나 대체 데이터 센터 또는 Azure 내에 있는 새로운 VNET 또는 클린 환경으로 복구할 수 있습니다.

솔루션 전략 및 설계

신뢰할 수 있는 Dell Technologies Services를 통해 조직의 요구 사항을 지원할 수 있도록 사이버 복구 프로그램을 전략화하고 구축하며 조정 및 확장할 수 있습니다. 전문 서비스에는 보호 및 복구 조정, 사이버 복구 기술 배포, 사이버 인시던트 대응 또는 팀을 대상으로 한 최신 기술 교육 등이 포함될 수 있습니다. Dell Technologies의 업계 전문가가 팀과 협력하여 보호할 중요 시스템과 데이터는 물론 복구에 필요한 인프라스트럭처를 결정하는 데 도움을 줍니다.

간소화된 배포

PowerProtect Cyber Recovery for Azure는 Azure Marketplace를 통해 거래 가능한 오퍼링으로 제공되므로 사용자가 기존 Azure 구독을 활용할 수 있습니다. Dell Technologies는 간단한 구매 과정을 통해 Azure용 Dell Technologies의 데이터 보호 오퍼링 포트폴리오에 빠르게 액세스할 수 있도록 최선을 다하고 있습니다. 또한 Dell Technologies는 Dell이나 Azure Marketplace를 통해 원하는 방식의 Azure용 Cyber Recovery를 직접 구매할 수 있는 유연성을 제공합니다.

PowerProtect Cyber Recovery는 알려진 양호한 데이터를 보호하고 식별 및 복원하며 사이버 공격 후 정상적인 운영 및 규정 준수를 유지할 수 있는 신뢰성을 제공합니다.

Dell PowerProtect Cyber Recovery 에 대한 자세한 정보	Dell Technologies 전문가에게 문의	Azure Marketplace 오퍼링 보기	대화 참여: #PowerProtect