

비즈니스 복원력 구축

비즈니스 연속성 및 재해 복구를 위한 퍼블릭 클라우드 활용



소개

점점 더 치열해지는 시장에서 민첩성을 유지하기 위해 노력하는 조직은 고객과 이해관계자에게 유연하게 대응할 수 있는 IT 솔루션과 인프라를 선택하는 것이 그 어느 때보다 중요해졌습니다. 대부분의 현대 조직은 이러한 민첩성과 유연성을 염두에 두고 애플리케이션 및 기타 워크로드를 퍼블릭 클라우드로(많은 경우 여러 퍼블릭 클라우드로) 이전하고 있습니다.

온프레미스, 여러 프라이빗 또는 퍼블릭 클라우드 및 엣지를 포함한 인프라 환경을 관리하고 유지보수하는 일은 매우 복잡하고 매우 빠르게 진행될 수 있습니다. 단순히 인프라를 관리하는 것도 어렵다면, 시스템의 일부가 다운되거나 악의적인 공격으로 인해 침해되면 어떻게 될까요? 하이브리드 멀티클라우드 환경에서 비즈니스 연속성 및 재해 복구는 어떻게 작동하나요?

이 eBook에서는 오늘날 기업들이 더 많은 퍼블릭 클라우드 제공업체와 협력하는 이유와 최악의 시나리오가 현실화되었을 때 직면하게 되는 재해 복구 문제를 살펴봅니다. 또한 성공적인 기업들이 다운타임의 위험과 현실을 완화하고 더 나은 비즈니스 연속성을 보장하여 더 성공적으로 경쟁하고 번창하기 위해 어떤 노력을 기울이고 있는지도 살펴볼 것입니다.

목차

기업 성공의 핵심인 비즈니스 복원력.....	03
오늘날의 하이브리드 멀티클라우드는 BCDR에 대한 과제를 제시할 수 있습니다.	04
변화하는 위협 환경으로 인해 BCDR은 필수.....	05
데이터가 어디에 있는 비즈니스 복원력 보장.....	06
BCDR 전략의 일부로 퍼블릭 클라우드 사용.....	07
클라우드 기반 BCDR 솔루션에서 살펴봐야 할 사항	08
비즈니스 연속성 및 재해 복구를 간소화하는 NC2.....	09



비즈니스 복원력은 기업의 성공에 필수적입니다.

계속 운영하거나 가능한 빨리 온라인 상태로 복구하는 것은 오늘날 비즈니스의 필수 과제입니다. 고객은 민첩하고 편리한 서비스와 지원은 물론 대부분의 비즈니스와 옴니채널로 상호 작용하기를 기대합니다. 오늘날과 같이 빠르게 변화하는 디지털 환경에서는 리테일 웹사이트가 다운되면 고객이 몇 분 안에 다른 곳에서 필요한 것을 찾을 가능성이 높습니다. 애플리케이션이 작동하지 않는 경우 많은 고객이 소셜 미디어 포럼에 불만을 토로합니다.

다운타임이 영향을 미치는 것은 고객뿐만이 아닙니다. 조직의 이해관계자, 공급업체, 파트너, 내부 직원도 데이터와 시스템에 대한 일관된 액세스를 필요로 합니다. 직원들이 업무를 수행하거나 회사 또는 담당자와 효율적으로 소통할 수 없다면 비즈니스에 큰 타격을 입게 됩니다. 비즈니스 연속성이 없으면 브랜드 평판, 수익, 고객 경험 및 만족도, 브랜드 충성도 등이 위험해질 수 있습니다.

최근 [연구](#)에 따르면 계획되지 않은 IT 다운타임으로 인해 매년 총 4,000억 달러의 기업 손실이 발생한다고 합니다. 이러한 금전적 손실은 거래 손실이나 고객 손실로 인한 것뿐만 아니라 법적 벌금이나 벌금으로 인한 것일 수도 있습니다. 다운타임을 방지하거나 신속하게 복구하지 못하면 오늘날 기업의 존립 자체가 위협받고 있습니다.

기업은 비즈니스 연속성 외에도 강력한 재해 복구 전략, 즉 예기치 않은 중단이 발생한 후 시스템을 복구하고 정상 운영을 복원하는 방법에 대한 계획을 수립해야 합니다. 재해 복구 계획은 비즈니스 연속성을 유지하는데 도움이 됩니다.

재해 복구는 비즈니스 연속성이라는 포괄적인 개념에 속합니다. 비즈니스 연속성에는 데이터 보호도 포함되며, 여기에는 미사용 데이터를 백업하고 악의적인 공격이나 기타 예기치 않은 이벤트 발생 시 복원할 프로덕션 데이터를 복제하는 것이 포함됩니다. 데이터 보호 및 재해 복구는 전반적인 비즈니스 복원력, 즉 운영, 직원, 서비스, 자산 또는 고객에게 위협이 되는 갑작스럽고 예기치 않은 변화에 얼마나 빨리 복구하거나 적응할 수 있는지에 대한 중요한 요소입니다.

BCDR

비즈니스 연속성 및 재해 복구를 의미하며 데이터 보호 및 재해 복구의 모든 측면을 포괄하는 용어로 사용됩니다.

비즈니스 연속성

잠재적인 위협과 취약성을 예방 및 복구하고 합리적인 시간 내에 최소한의 피해로 평소와 같이 비즈니스로 복귀할 수 있는 조직의 역량입니다.

재해 복구

도구, 정책 및 절차를 구현하고 중요한 비즈니스 운영을 재구축하여 미션 크리티컬 IT 기능을 복원하는 능력입니다.

데이터 보호

예기치 않은 중단 중에 손실되거나 손상된 데이터를 다시 마이그레이션하는 작업을 처리합니다.



오늘날의 하이브리드 멀티클라우드는 BCDR에 도전 과제 제시 가능

오늘날 IT 인프라의 사실상 표준은 하이브리드 멀티클라우드입니다. Nutanix의 최근 연구에 따르면 설문조사에 참여한 조직의 80% 이상이 하이브리드 IT 환경이 애플리케이션 및 데이터 관리 능력에 가장 큰 도움이 된다고 생각하는 것으로 나타났습니다. 또한 응답자의 거의 절반이 하이브리드 IT가 CIO의 최우선 순위가 되었다고 답했습니다.

하이브리드 멀티클라우드 인프라는 기업에 데이터와 애플리케이션 배포를 위한 다양한 옵션을 제공하며, 다양한 컴퓨팅 비용 및 청구 모델을 지원합니다. 이러한 이유로 많은 조직이 이를 선호합니다. 각 워크로드나 애플리케이션이 가장 잘 작동할 수 있는 환경에 최적의 위치를 찾을 수 있기 때문입니다.

하지만 이러한 다양한 옵션에는 단점도 조금 있습니다. 환경이 많아질수록 복잡성도 증가하기 때문입니다. 하이브리드 멀티클라우드에서는 많은 조직이 여러 공급자의 솔루션을 사용하고 있으며, 각 솔루션이나 환경마다 고유한 도구, 기술, 보안 절차가 필요합니다. IT 부서가 하이브리드 멀티클라우드 인프라를 관리하고 모니터링하며, 각 환경을 상호 운영 가능하고 연결된 상태로 유지하는 것은 상당한 도전 과제가 될 수 있습니다.

고의적인 공격이나 자연재해로 인해 데이터가 손실되거나 손상되는 최악의 시나리오가 발생했을 때보다 더 심각한 문제는 없을 것입니다. 하이브리드 멀티클라우드 에코시스템 전반에서 재해 복구 및 비즈니스 연속성 유지는 특히 복잡해질 수 있습니다. 시스템을 백업하고 데이터를 복원할 수 있는 기능이 없다면 기업은 심각한 영향을 받을 수 있습니다.

하이브리드

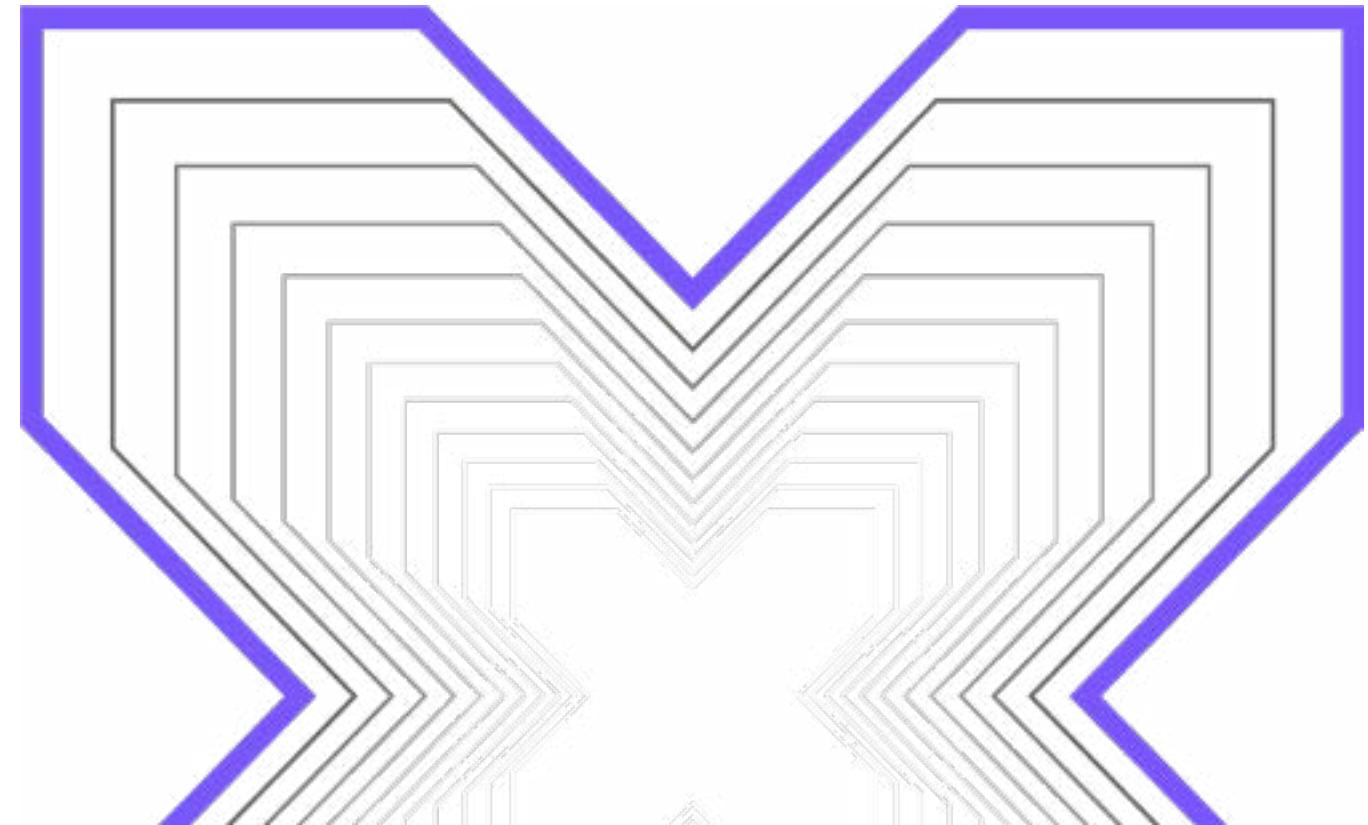
IT 모델은 온프레미스, 호스팅, 프라이빗 클라우드, 퍼블릭 및 서비스 제공업체 클라우드, 엣지 위치 등 다양한 환경에 걸쳐 있는 워크로드와 애플리케이션으로 구성됩니다.

멀티클라우드

조직이 둘 이상의 퍼블릭 클라우드에 데이터와 애플리케이션을 보유하고 있음을 의미합니다.

환경이 많아질수록 복잡성도 증가하기

때문입니다. IT 부서가 하이브리드 멀티클라우드 인프라를 관리하고 모니터링하며, 각 환경을 상호 운영 가능하고 연결된 상태로 유지하는 것은 상당한 도전 과제가 될 수 있습니다. 하이브리드 멀티클라우드도 BCDR을 복잡하게 만듭니다.



진화하는 위협 환경으로 인해 BCDR은 필수 요소가 되었습니다.

하이브리드 멀티클라우드 인프라의 복잡성 증가는 관리 및 유지 관리에만 적용되는 것이 아닙니다. 또한 BCDR로 확장됩니다. 하이브리드 멀티클라우드는 온프레미스, 엣지, 퍼블릭 클라우드 환경에 걸쳐 있기 때문에 각 환경에서 데이터를 보호하고 복원하는 방식이 다를 수 있습니다.

데이터와 애플리케이션을 보호하고 필요할 때 신속하게 복원할 수 있는 것은 비즈니스의 필수 요소이자 성공의 핵심입니다. 오늘날 끊임없이 진화하는 위협 환경으로 인해 랜섬웨어, 외부 침입자, 정전 등의 형태로 예기치 않은 다운타임이 발생할 가능성이 높기 때문입니다. 이는 '만약'이 아니라 '언제'의 문제입니다.

다운타임의 원인은 단순한 장비 오작동부터 내부 직원의 실수나 부정행위, 화재, 홍수, 지진과 같은 자연재해로 인한 정전이나 네트워크 손실에 이르기까지 다양합니다.

오늘날 기업에게 가장 시급한 위협 중 하나는 랜섬웨어 및 기타 사이버 공격입니다. 최신 [Nutanix 엔터프라이즈 클라우드 인덱스 보고서](#)에 따르면 응답 기업들은 랜섬웨어 보호 및 데이터 보안을 조직의 가장 큰 데이터 관리 과제로 꼽았습니다. 또한 랜섬웨어 공격을 경험한 응답자의 71%는 전체 운영을 복구하는 데 며칠 또는 몇 주가 걸렸다고 답했습니다. 비즈니스에 따라 단 한 순간의 다운타임도 재앙이 될 수 있습니다.

랜섬웨어는 쉽게 사라지지 않을 것입니다. 실제로 공격 빈도는 점점 더 증가하고 있습니다. 2024년 1월 [시만텍의 연구](#)에 따르면 "랜섬웨어 공격은 2023년 10월에 급증했으며 2023년 10월 랜섬웨어의 영향을 받은 조직의 수는 1년 전보다 66% 증가했습니다."라고 합니다.

랜섬웨어 공격 및 기타 예기치 않은 다운타임의 원인이 증가하는 상황에서 기업은 복원력을 높이기 위한 강력한 BCDR 계획을 수립하는 것이 그 어느 때보다 중요합니다.

랜섬웨어 공격을 경험한 조직의 71%는 전체 운영을 복구하는 데 며칠 또는 몇 주가 걸린다고 답했습니다.

[\(6차 연례 Nutanix 엔터프라이즈 클라우드 인덱스\)](#)



데이터가 어디에 있든 비즈니스 복원력 보장

효과적인 BCDR 계획은 다운타임이 발생했을 때 기업의 큰 힘이 될 수 있습니다. 데이터 복구와 비즈니스 연속성 유지는 반드시 대규모 작업일 필요는 없습니다. BCDR은 간단한 백업부터 종합적인 재해 복구에 이르기까지 모든 과정을 포함하는 일련의 프로세스로 생각할 수 있습니다. 때로는 시스템을 최신 스냅샷으로 복원하거나 데이터를 가능한 최신 상태로 유지하는 것만으로도 충분할 수 있습니다.

오늘날의 악의적인 행위자들과 랜섬웨어는 기본 데이터뿐만 아니라 온프레미스 백업까지도 표적으로 삼고 있습니다. 이는 조직이 백업에 접근하지 못할 경우 몸값을 지불할 가능성이 높아져 더 큰 위험에 노출되게 만듭니다. 이러한 이유로 운영 체제와 애플리케이션 같은 데이터와 컴퓨팅 환경의 오프사이트 복사본을 생성하고 저장하는 것이 중요합니다.

오랫동안 IT 업계는 3-2-1 백업 규칙에 의존해 왔으며, 이는 오늘날에도 여전히 유효합니다. 이 규칙에 따르면 조직은 최소 **두 곳** 이상의 위치에 데이터 사본을 **3개** 이상 보관해야 하며, 그 중 **한 곳**은 오프사이트에 보관해야 합니다.

하이브리드 멀티클라우드 인프라의 한 가지 장점은 다양한 환경에서 데이터와 애플리케이션을 이미 보유하고 있다는 점입니다. 각 환경은 시스템의 다른 곳에 위치한 데이터 및 애플리케이션에 대한 백업 역할도 할 수 있습니다.

탄탄한 BCDR 전략을 달성하는 것은 쉽지 않습니다. 여기에는 모범 사례, 정기적인 IT 리소스 백업, 빈번한 재해 복구 계획 테스트가 신중하게 혼합되어 있습니다.

비즈니스 연속성 및 재해 복구는 데이터가 손상, 손실 또는 손상되지 않도록 보호해야 합니다. 데이터 보호의 두 가지 하위 범주는 다음과 같습니다.

백업

데이터 사본을 만드는 과정입니다. 대부분의 백업 솔루션은 가끔씩 전체 백업을 수행하며, 이전 백업 이후 변경된 데이터만 복사하는 정기적인 야간 증분 백업으로 보완합니다. 조직은 충분한 복구 지점을 확보하고 규정을 준수하기 위해 백업 빈도 및 보존 정책을 설정합니다.

복제

회사 사이트 간에 데이터를 복사한 다음 이동하는 행위입니다. 일반적으로 복구 시간 목표(RTO)와 복구 지점 목표(RPO)로 측정합니다. 재해 발생 후에도 미션 크리티컬 및 고객 대면 애플리케이션을 중단 없이 운영할 수 있습니다. 재해 발생 시 가동 중단 시간과 데이터 손실을 최소화하려면 복제를 장애 조치 및 장애 복구 기능으로 보완해야 합니다.



BCDR 전략의 일부로 퍼블릭 클라우드 활용하기.



3-2-1 백업 규칙의 경우, 오늘날 많은 조직이 퍼블릭 클라우드를 온프레미스 데이터의 오프사이트 백업 위치로 사용하고 있습니다. 실제로 IDC의 2023년 설문조사에 따르면 하이브리드 및/또는 멀티클라우드 인프라를 보유한 기업 중 67%가 클라우드 기반 BCDR을 사용하고 있는 것으로 나타났습니다.

같은 설문조사에서 클라우드 투자와 관련하여 가장 고려해야 할 두 가지 사항은 (1) 포괄적인 보안과 (2) 재해 복구 및 백업이라고 답했습니다. 또한 오늘날 가장 일반적인 방법이 온프레미스 프라이빗 클라우드에서 데이터를 백업하여 퍼블릭 클라우드에 저장하는 것이라는 사실을 발견하면서 백업 및 재해 복구가 하이브리드 전략에 필수적인 요소가 되고 있음을 강조합니다. 두 번째로 가장 일반적인 백업 방법은 호스팅된 프라이빗 클라우드에 온프레미스 데이터센터의 복사본을 저장하는 것입니다.

재해 복구 모델 선택과 관련하여 IDC는 하이브리드 멀티클라우드 인프라를 사용하는 기업이 주로 데이터 보호 혜택, 데이터 검색 속도, 관리 용이성을 고려한다고 보고했습니다.

퍼블릭 클라우드는 재해 복구 전략의 일부로 상당한 이점을 제공할 수 있습니다.

데이터를 신속하게 복구하여 다운타임을 줄이고 공격이나 중단의 영향을 최소화하는 데 도움이 됩니다. 또한 퍼블릭 클라우드는 온프레미스 인프라에는 없는 다양한 기능과 이점을 제공합니다. 여기에는 다음이 포함됩니다.

- **자본** 비용이나 추가 장비가 필요하지 않습니다.
- **관리가 간편한** 자동화된 운영
- 효율성 향상을 위한 **통합 관리** 영역
- **유형 리소스** 및 오래된 백업 제거
- **비용 절감** 및 IT 관리 부담 감소
- **필요할 때마다 빠르고 간편하게 확장 가능**
- 데이터 삭제 또는 변경을 방지하는 데이터 불변성

Penn National Insurance는 확장 중인 온프레미스 가상 데스크톱 인프라(VDI)의 관리를 간소화할 방법이 필요했습니다. 동시에 테이프 기반 재해 복구 시스템에 대한 대대적인 업데이트가 필요했습니다.

Nutanix는 온프레미스 및 AWS에서 실행되는 Nutanix 클라우드 클러스터(NC2)를 통해 이 보험사가 하이브리드 멀티클라우드 모델을 완전히 수용하고 온프레미스 데이터를 클라우드로 쉽게 복제할 수 있도록 지원하여 두 가지 과제를 모두 해결했습니다.

"재해가 발생하면 AWS에서 NC2를 신속하게 가동하고 클라우드에 복제된 데이터를 불러올 수 있습니다."라고 Penn National Insurance의 선임 인프라 시스템 설계자인 Craig Wiley는 말합니다. "재해 복구를 AWS 클라우드로 이전함으로써 복구 시간이 며칠에서 단 몇 시간 이내로 단축되었습니다."

[사례 연구 모두 읽기](#)

클라우드 기반 BCDR 솔루션에서 살펴봐야 할 사항

하이브리드 멀티클라우드는 기업의 IT 복잡성을 증가시킬 수 있지만, 적절한 기능과 성능을 갖춘 솔루션을 선택하면 이러한 위험을 줄일 수 있습니다.

과적인 BCDR(비즈니스 연속성 및 재해 복구) 솔루션의 가장 중요한 특징 중 하나는 온프레미스와 엣지를 포함한 하이브리드 멀티클라우드의 모든 환경을 하나의 단일 시스템처럼 관리하고 모니터링할 수 있도록 하는 것입니다. 상호 운용성은 필수적입니다. 실제로 일부 전문가들은 각 환경이 서로 분리된 상태로 존재하는 분리된 하이브리드 멀티클라우드는 진정한 하이브리드 멀티클라우드가 아니라고 말하기도 합니다. 이 인프라의 장점은 모든 것이 매끄럽게 협력할 때 비로소 발휘됩니다.

다양한 SLA 요구 사항을 충족하는 데 도움이 되는 중요한 기능은 다음과 같습니다.

스냅샷 - 특정 시점의 서버에 대한 빠른 '사진'입니다. 여기에는 파일, 소프트웨어 및 설정이 포함됩니다. 스냅샷은 "특정 시점" 상태를 유지하며 서버의 데이터를 복사하거나 이동할 필요가 없습니다.

복제 - 데이터를 복사하여 기본 소스와 지리적으로 분리된 다른 사이트에 저장하는 것입니다.

재해 복구 티어링 - 티어는 특정 방법을 사용하여 데이터를 얼마나 빨리 복구할 수 있는지를 정의합니다. 티어가 높을수록 복구 속도가 빨라지고 비용도 더 많이 듭니다. 티어는 '오프사이트에 저장된 데이터 없음'(티어 0)부터 '자동화된 재해 복구, 종종 AI를 통한 복구'(티어 7)까지 다양합니다.

AWS 탄력적 재해 복구 통합 - 탄력적 재해 복구는 AWS로 데이터를 복구하는 빠르고 간단한 방법입니다. AWS를 사용하는 경우 BCDR 솔루션과 통합되어야 합니다.

클러스터 최대 절전 모드 - 일부 재해 복구 솔루션에는 클러스터를 종료하거나 최대 절전 모드로 전환할 때 클러스터 데이터를 클라우드(예: AWS 버킷)로 백업하는 기능이 있습니다. 최대 절전 모드는 클러스터를 사용하지 않을 때 유용합니다.

요컨대, 효과적인 복구 솔루션은 다운타임과 데이터 손실을 최소화하면서 평소와 같이 비즈니스로 복귀할 수 있어야 합니다.

동기식 복제

데이터를 기본 저장소에 기록하는 동시에 리포지토리에 복사하는 프로세스입니다.

비동기 복제

정보는 먼저 기본 스토리지에 기록되어 메모리 장치에 저장된 다음 나중에 지정된 시간에 다른 스토리지 위치로 복제됩니다. 동기식 복제보다 대역폭을 적게 사용하여 장거리에서 더 잘 작동하도록 설계되었습니다.

Near-sync 복제

변경된 데이터만 지속적으로 복제하는 상시 프로세스입니다. 예약되지 않았으면 스냅샷이 필요하지 않습니다.



비즈니스 연속성 및 재해 복구를 간소화하는 NC2

NC2를 사용하면 비즈니스 연속성 및 재해 복구 계획을 간단하고 효율적으로 관리할 수 있습니다. 이 솔루션을 통해 조직은 복잡성을 추가하지 않고도 하이브리드 멀티클라우드 아젠다를 가속화할 수 있습니다. 원클릭 재해 복구 기능을 제공하여 많은 재해 복구 사이트를 유지 관리하는 데 드는 비용과 복잡성을 줄일 수 있습니다. 온디맨드 탄력성 및 자동 호스트 수정 기능을 통해 모든 IT 환경에 일관된 단일 관리 포털을 제공합니다. 클라우드에서 데이터 손실이나 공격이 발생하더라도 데이터와 애플리케이션은 계속 사용할 수 있습니다. 이는 오늘날의 경쟁 환경에서 큰 의미가 있습니다.

[Nutanix BCDR 솔루션](#) 및 [NC2에 대해 자세히 알아보십시오.](#)

[무료 체험](#)을 신청하거나 자세한 내용을 [문의](#)할 수도 있습니다.



info@nutanix.com | www.nutanix.com/kr | [@nutanix](https://twitter.com/nutanix)

©2024 Nutanix, Inc. All rights reserved. Nutanix, Nutanix 로고 및 여기에 언급된 모든 제품 및 서비스 이름은 미국 및 기타 국가에서 Nutanix, Inc.의 등록 상표 또는 상표입니다. 여기에 언급된 기타 모든 브랜드명은 구분을 위한 목적으로만 사용되었으며 각 해당 소유주(들)의 상표일 수 있습니다.
eBook-Nutanix-Building-Business-Resilience-FY25Q1-08292024

