451 Research | 비즈니스 영향 요약

결코 쉽지 않은 멀티클라우드의 레질리언스 구현

451 핵심 요약

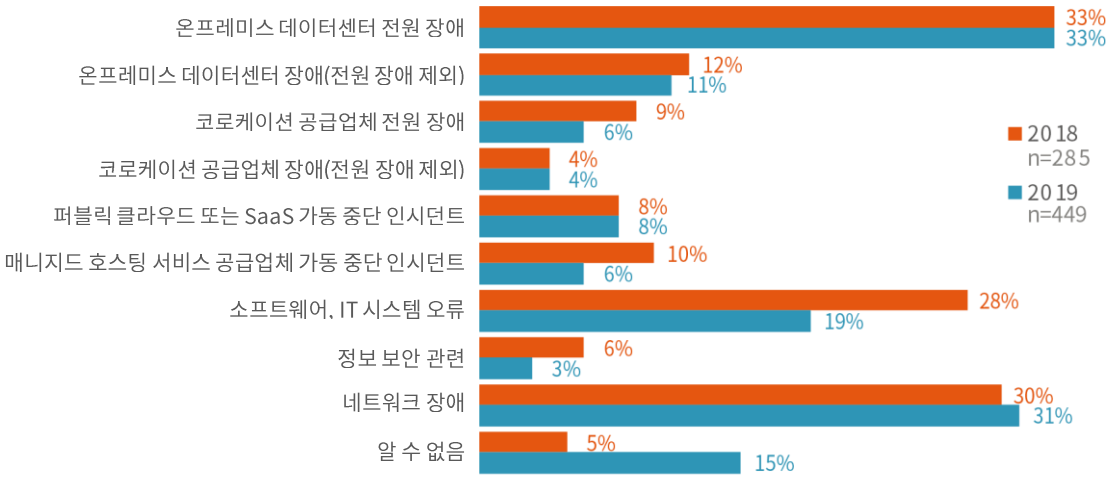
조직에서 하이브리드 및 멀티클라우드 배포를 고려하는 경우 데이터가 여러 위치에 있는 것이 낫다고 생각할 수 있습니다. 하지만 실제 상황은 매우 다릅니다. 장애가 매우 규칙적인 패턴으로 발생하며 확장된 인프라 및 분산된 데이터 리소스의 관리를 위한 협력이 이루어지지 않을 경우 중요한 애플리케이션의 가용성이 저하되어 비즈니스 운영을 위협할 위험이 있습니다. 비즈니스 연속성이 보장되도록 조직은 다양한 장애 시나리오에서 허용 가능한 시간 안에 애플리케이션 및 데이터를 복구할 수 있는 방법을 고려해야 합니다. 데이터의 보안, 가용성, 복구 가능성에 대한 신뢰를 확보하는 프로세스는 기업이 활용하는 전체 실행 환경에서 데이터가 사용되는 방식 그리고 합리적인 보호가 무엇인지를 이해하는 것에서부터 시작합니다. 클라우드 공급업체에서 제공하는 다양한 서비스에 솔깃할 수 있으나 하이브리드 및 멀티클라우드 환경의 실제 애플리케이션 보호는 저절로 이뤄지는 것이 아닙니다.

위험 관리는 복잡한 프로세스입니다. 조직에서는 발생 가능한 모든 위험과 해당 위험을 관리하는 방법을 파악하는 것이 가장 큰 과제인 경우가 많습니다. 오늘날 대부분의 조직에서 지원하는 인프라를 사용하는 경우에는 더욱 그렇습니다. 오늘날의 인프라는 온프레미스에도 있고 오프프레미스에도 있으며 매우 다양한 기능과 사용 패턴, 의존도를 가지고 있습니다. 이렇게 복잡하기 때문에 애플리케이션 그리고 애플리케이션에서 사용하는 데이터에 어떤 위험이 있는지 파악하기가 매우 어려울 수 있습니다. 기존의 BC/DR(비즈니스 연속성 및 재해 복구) 접근 방식에서는 하이브리드 및 멀티클라우드 환경 규모로 확장하는 데 어려움이 있습니다. 하이브리드 환경에서 실제 애플리케이션 레질리언스를 구현하려면 보다 통합된 BC/DR 계획이 필요합니다.

가동 중단의 원인이 대부분 알려져 있음에도 비교적 일정한 발생 빈도 유지

출처: Uptime Institute의 IT 및 데이터센터 관리자 대상 글로벌 설문조사 2019

질문: 조직에서 발생했던 가장 큰 규모의 가동 중단 또는 가장 최근 가동 중단의 주요 원인은 무엇인가요? 해당하는 경우 원인을 여러 개 선택할 수 있습니다.



또 다른 과제로는 정보 보안 환경을 위협하는 여러 복잡한 상황을 들 수 있습니다. 사이버 공격의 본질이 계속 진화하면서 사이버 공격으로 인한 위험의 유형도 변하고 있습니다. 공격자는 시스템을 전복하고 데이터를 빼돌리던 방식에서 데이터를 볼모로 잡고 금전을 요구하는 랜섬웨어를 사용하거나 단순히 데이터를 손상 또는 파괴하는 '와이퍼' 멀웨어를 사용하는 새로운 전략을 채택하는 방식으로 공격을 변화시켰습니다. 이러한 새로운 환경에서 진화된 공격을 이겨내려면 데이터 보호에도 변화가 필요합니다.

451 Research | 비즈니스 영향 요약

451 핵심 요약(계속)

동시에 애플리케이션 아키텍처의 해체로 인해 데이터 레질리언스에 대한 보다 포괄적인 접근 방식도 필요하게 되었습니다. 이를테면, 마이크로 서비스 아키텍처 및 서버리스 컴퓨팅과 같은 패턴의 경우, 데이터의 사용 방법과 데이터가 상주해야 하는 위치를 변화시킵니다.

조직에서 효과적인 애플리케이션 보호 계획을 수립하려면 레질리언스가 우수한 설계와 효율적인 운영의 산물이라는 점을 이해해야 합니다. 다시 말해, 레질리언스는 최신 BC/DR 프로세스의 논리적인 결과에 해당합니다. 하이브리드 환경에서 다양한 인프라와 구성 요소를 융합하여 애플리케이션과 서비스가 구축되므로, 가동 중단을 일으킬 수 있는 원인을 파악하려면 여러 위치뿐만 아니라 해당 위치 간 상호연결 부분까지 포괄적으로 살펴야 합니다. 따라서 데이터 보호 기능 외에 복구 작업의 일환으로 대안 위치에 데이터를 보낼 수 있는 기능의 중요성도 더욱 커지게 되었습니다.

하이브리드 및 멀티클라우드 환경이 안고 있는 가장 큰 과제 중 하나는 확장입니다. 효과적인 방식으로 데이터를 보호하기 위해서는 운영 간소화를 통해 확장 문제를 해결해야 합니다. 운영 간소화는 어떤 접근 방식을 선택하든 이질적인 위치에서도 일관된 데이터 서비스를 이용할 수 있어야 하고 운영 워크로드를 관리하기 위한 자동화가 효과적으로 이루어져야 한다는 2가지 중요한 측면의 목표를 달성함으로써 그 실현을 촉진할 수 있습니다.

하이브리드 환경에는 특히 보안 및 비즈니스 연속성에 대한 과제가 분명히 존재합니다. 하이브리드 환경을 채택하려는 기업이라면 더 제한된 상황에서 효과를 얻었던 보안 방식은 재고해야 합니다. 조직에서 하이브리드 인프라를 활용하려면 핵심 비즈니스 자산을 보호하는 방법이 보다 포괄적으로 평가되도록 바뀌어야 합니다. 이러한 변화에 대처하기 위해서는 비즈니스 가치의 근본적인 측면에 대해 충분한 레질리언스를 보장해야 합니다.

비즈니스에 미치는 영향

강력한 데이터 가용성. 효과적인 계획은 하이브리드 및 멀티클라우드 환경이 가져오는 추가적인 위험을 줄일 수 있으므로 해당 계획을 조직에서 자신 있게 활용할 수 있습니다. 하이브리드 시대에 비즈니스 연속성을 유지하기 위해서는 더욱 광범위한 지원이 필요합니다.

일관된 데이터 관리. 애플리케이션 소유자가 광범위한 실행 환경에서 일관된 데이터 서비스를 활용할 수 있습니다.

사이버 공격으로부터 보호. 중요한 데이터는 최근 들어 새로운 방식으로 데이터를 탈취 또는 파괴하는 데 주력하고 있는 공격자의 시도를 이겨낼 수 있어야 합니다. 따라서, 해결해야 할 과제가 많기는 하나 레질리언스는 매우 중요합니다.

전체 데이터 라이프사이클 관리. 클라우드 및 호스팅 공급업체에는 현대의 비즈니스가 필요로 하는 맞춤형의 조정된 데이터 라이프사이클 관리가 부족합니다. 효과적인 보호가 이루어지면 비즈니스 성장을 지원하는 동시에 위험도 관리할 수 있습니다.

향후 전망

인프라의 안정적인 미래는 원동력이 될 핵심 리소스의 레질리언스와 밀접하게 연계되어 있습니다. 컴퓨팅 성능과 연결성도 중요하지만 데이터는 항상 조직의 생명선 역할을 해 왔습니다. 시장에서 성공을 거두고 발전을 이루도록 조직의 역량을 유지하기 위해서는 데이터 인프라가 진정한 레질리언스를 갖춘 액세스를 제공해야 합니다. 하이브리드 및 멀티클라우드 환경은 새로운 과제를 제시하기는 하지만 그 과제가 극복할 수 없는 수준은 아닙니다. 조직은 세심한 계획 수립을 통해 복잡한 하이브리드 환경이 제시하는 과제를 해결하고 기존 모델을 확장하여 요구사항을 충족할 방법도 찾을 수 있습니다.