Global Data Protection Index 2021

주요 연구 결과 – 2021년 7월

VansonBourne

DELL Technologies

주요 연구 결과의 중점 사항

1
데이터 보호의 위험 환경

2
사이버 공격으로 인한 위협

3
새로운 기술 및 첨단 기술 지원

4
클라우드 환경의 데이터 보호 취약성

5
As a Service의 성장

6
데이터 보호 간소화

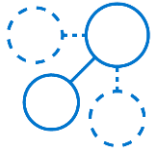
5가지 핵심 내용

광범위한
재택 근무 도입으로
데이터 보호 및 사이버 위험 증가

사이버 위협으로부터
충분히 방어하고 복구할 수 있는 **조직의 데이터 보호 역량을 확신하지 못하는 경우가 많음**

첨단 기술 및
클라우드에 대한
지속적인 투자는
데이터 보호 과제를 가중시킬 수 있음

많은 조직이 데이터
보호의 편의성과
유연성을 높이기 위해
As a Service 활용에 관심을 갖고 있음



협력하는 **데이터 보호 솔루션 공급업체의 수가 적을수록 더 효과적인 데이터 보호 성과로 이어진다는 증거가 있음**

인터뷰 대상

1,000명의 IT 의사 결정권자를 대상으로 2021년 2월, 3월, 4월에 인터뷰 진행

다양한 공공 및 민간 부문 업계의 조직

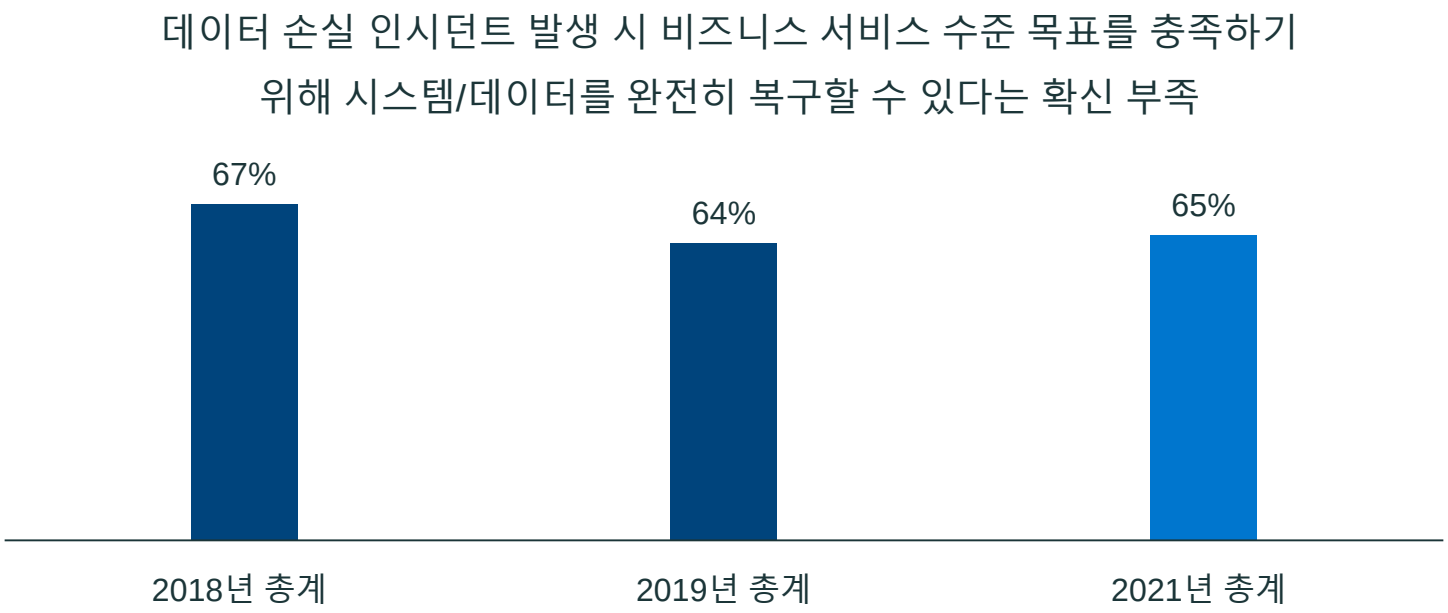
250명 이상의 직원을 보유한 조직

4개 지역:

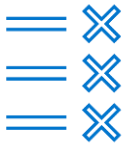
아메리카(200)
EMEA(450)
APJ(250)
중국(100)

1. 데이터 보호의 위험 환경

IT 의사 결정권자들은 조직의 복구 SLO 충족 역량을 확신하지 못함



또한 데이터 보호 역량이 내부 및 외부 표준에 부합한다는 확신이 낮고, 조직의 3분의 2가 내년 중에 운영 중단 사고를 경험할 것으로 예상하는 등 우려가 더욱 가중됨



58%

조직이 **백업 및 복구 서비스 수준 목표를 충족**한다고 그다지 확신하지 못하는 비율

63%

조직의 현재 데이터 보호 인프라스트럭처와 프로세스가 **지역 데이터 거버넌스 규정을 준수**한다고 그다지 확신하지 못하는 비율

64%

앞으로 12개월 이내에 **운영 중단 사고를 경험할 것으로 우려**하는 비율

이러한 우려 사항 외에도, 데이터 손실 및 시스템 다운타임 문제가 조직에 계속해서 심각한 재정적 영향을 미치고 있음

$959,493

지난 12개월의 평균
데이터 손실 비용(USD)

$513,067

지난 12개월의 평균
예상치 못한 다운타임
비용(USD)

2. 사이버 공격으로 인한 위협

조직은 현재 데이터 보호 수단으로 사이버 공격의 영향을 완화시킬 수 있다고 확신하지 못함. 또한 대부분의 조직은 직원들의 재택 근무로 인해 위험에 대한 노출이 증가한다고 판단함.

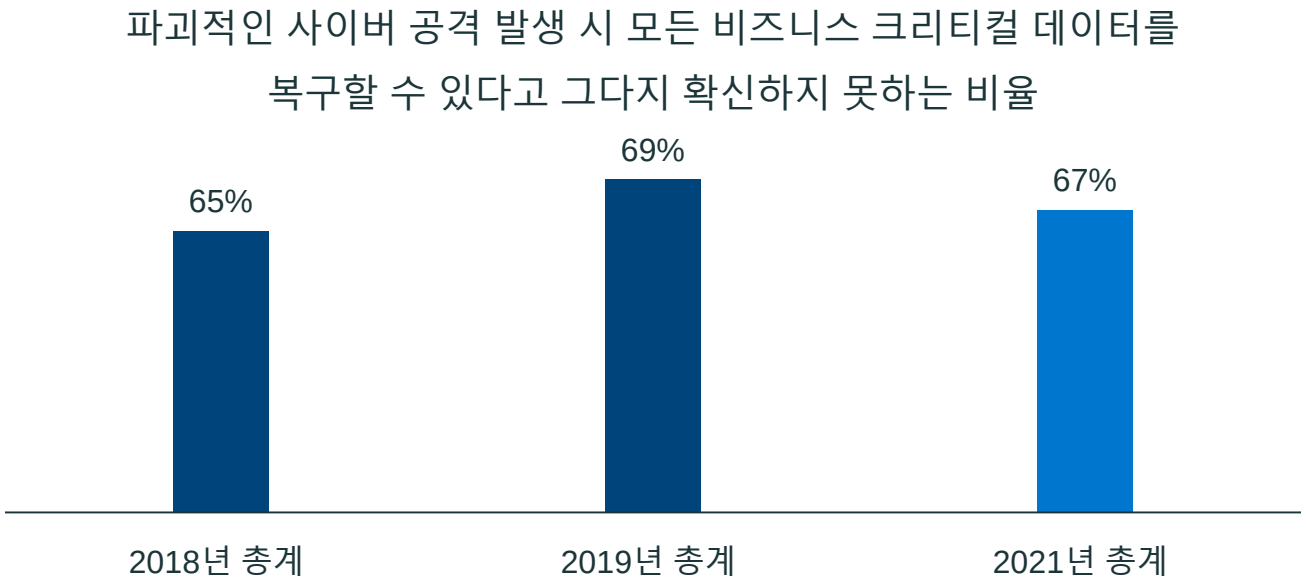
62%

조직의 기존 데이터 보호 수단이 **멀웨어 및 랜섬웨어 위협에 대처하기에 충분하지 않을 수 있음을 우려한다**고 답한 비율

74%

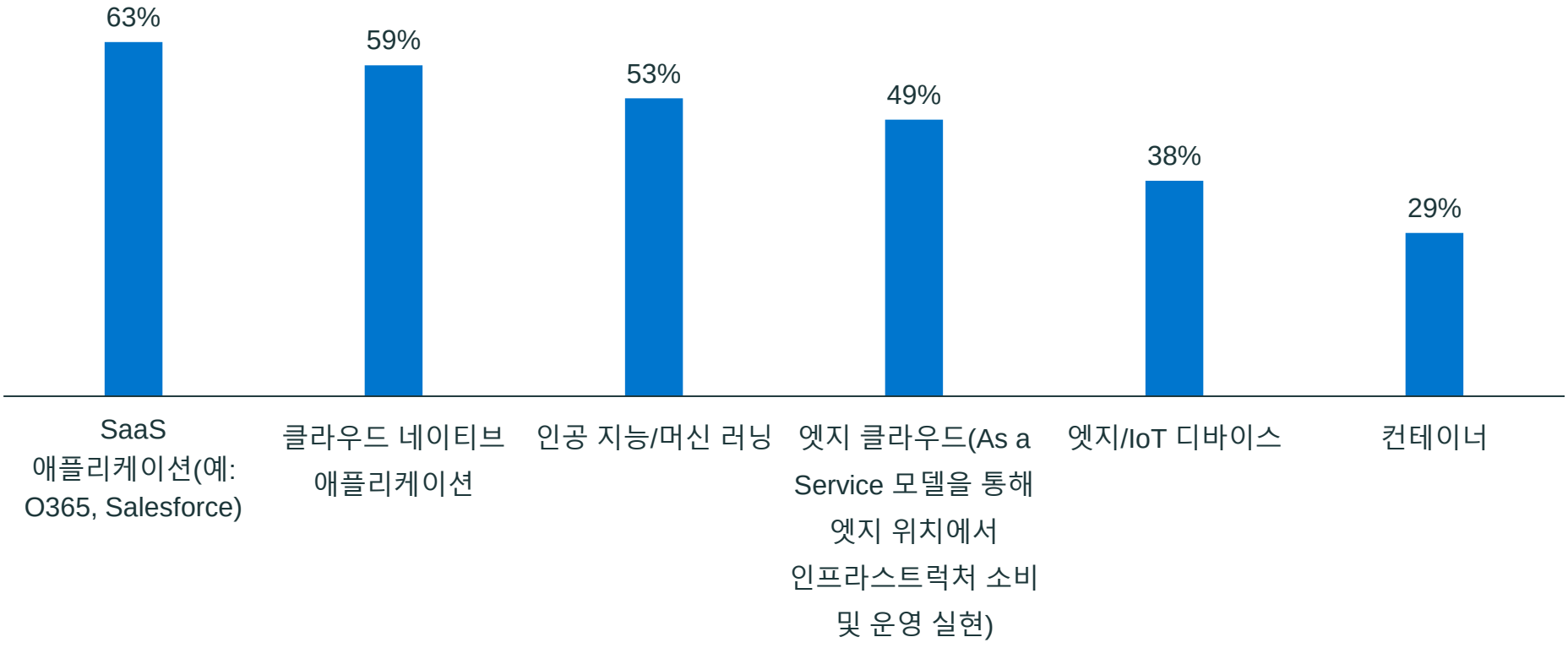
직원 재택 근무의 증가로 인해 사이버 위협으로 인한 **데이터 손실 위험에 더 많이 노출되었다**는 데 동의한 비율

멀웨어 및 랜섬웨어 위협에 맞설 수 있는 조직의 대처 역량에 대한 우려와 함께, 파괴적인 사이버 공격 발생 시 비즈니스 크리티컬 데이터를 모두 복구할 수 있다는 확신이 부족한 경우가 많음

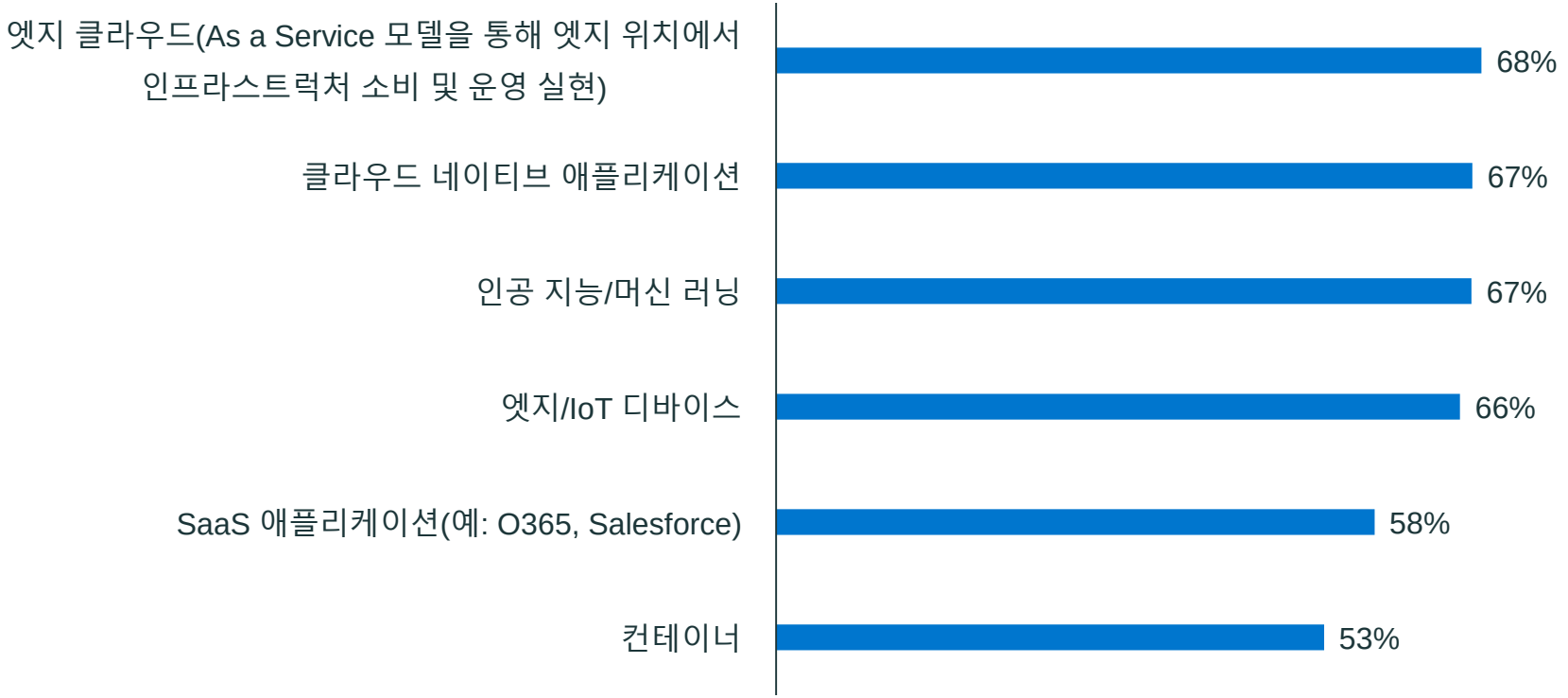


3. 새로운 기술 및 첨단 기술 지원

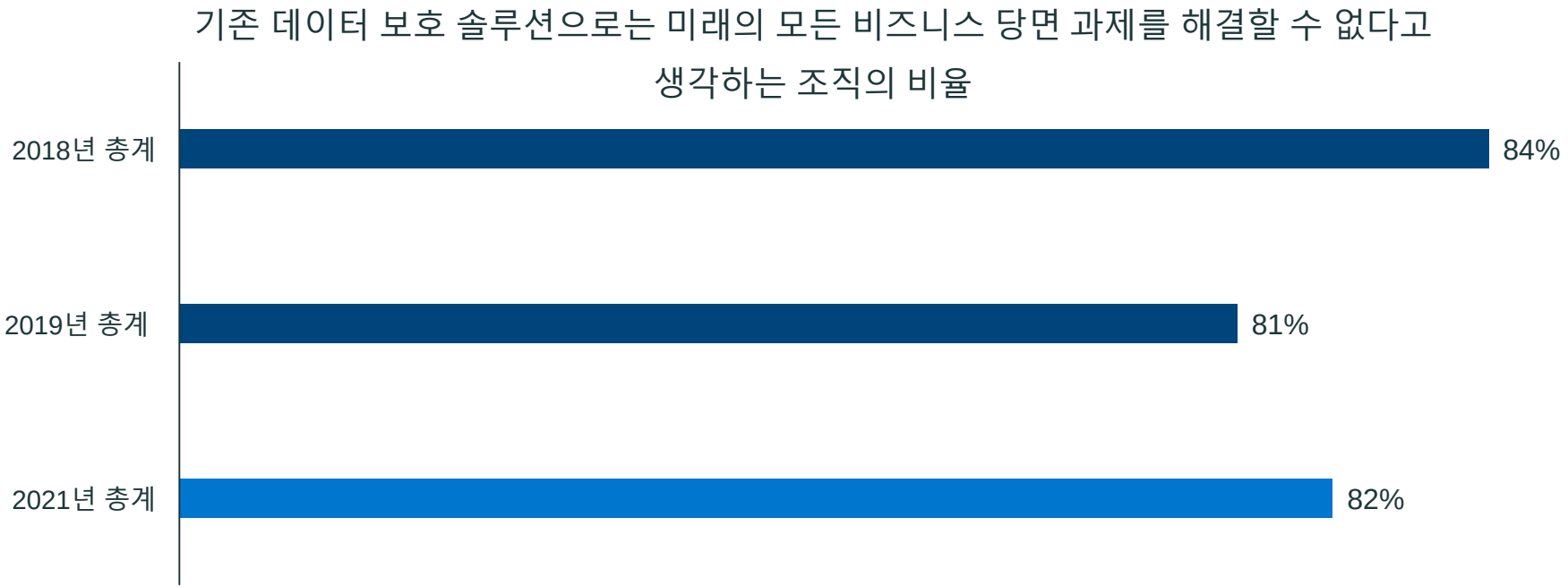
조직은 다양한 새로운 기술에 투자하고 있으며, 이로 인해 데이터 보호 과제가 더욱 복잡해질 수 있음



많은 조직이 최신 기술을 보호하는 데 어려움을 겪음



새로운 기술과 첨단 기술은 보호하기 어렵다는 점이 데이터 보호 솔루션의 미래 대비 관련 확신이 부족한 이유 중 하나임



많은 사람들이 첨단 기술을 데이터 보호 위험 요소로 보고 있으며, 특히 여러 데이터 보호 공급업체를 이용하는 경우 미래의 운영 중단 사고에 대한 우려가 큼

데이터 보호 측면에서 위험 요소가 되는 첨단 기술(예: AI, IoT, 엣지)

하나의 데이터 보호 공급업체 이용

57%

여러 데이터 보호 공급업체 이용

64%

12개월 이내에 운영 중단 사고(예: 데이터 손실, 시스템 다운타임 등)를 겪을 것으로 우려함

하나의 데이터 보호 공급업체 이용

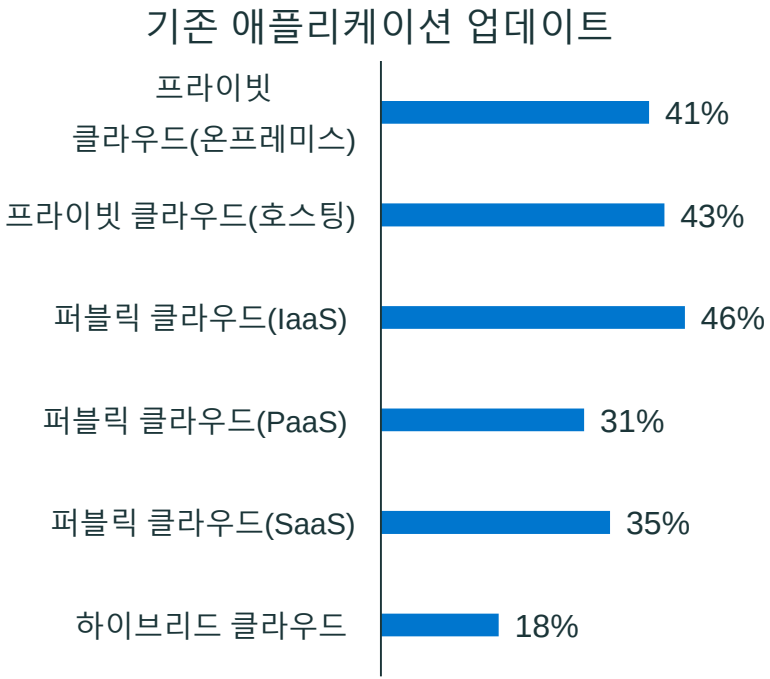
54%

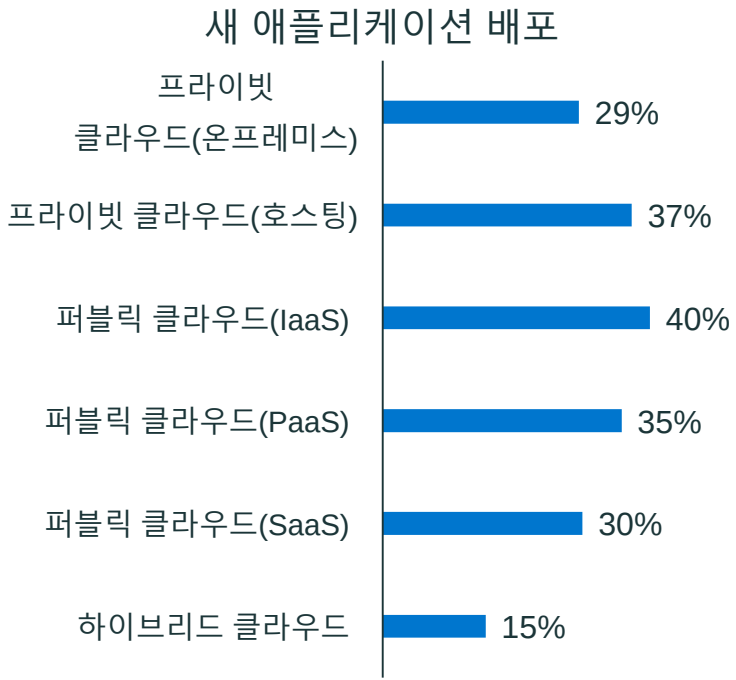
여러 데이터 보호 공급업체 이용

68%

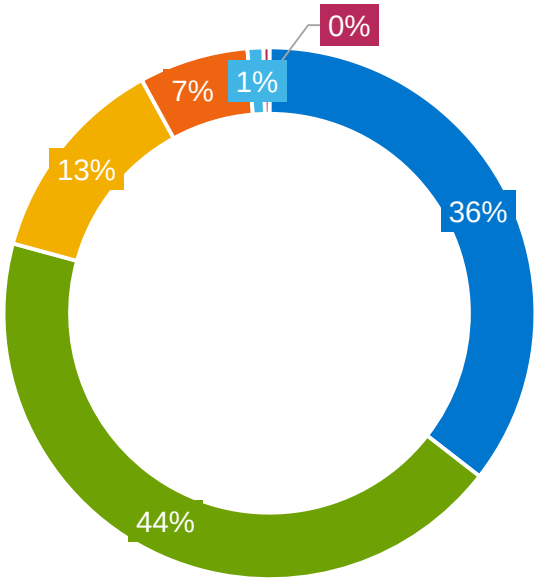
4. 클라우드 환경의 데이터 보호 취약성

조직 IT 인프라스트럭처의 광범위한 환경에 걸쳐 애플리케이션이 업데이트 및 배포됨



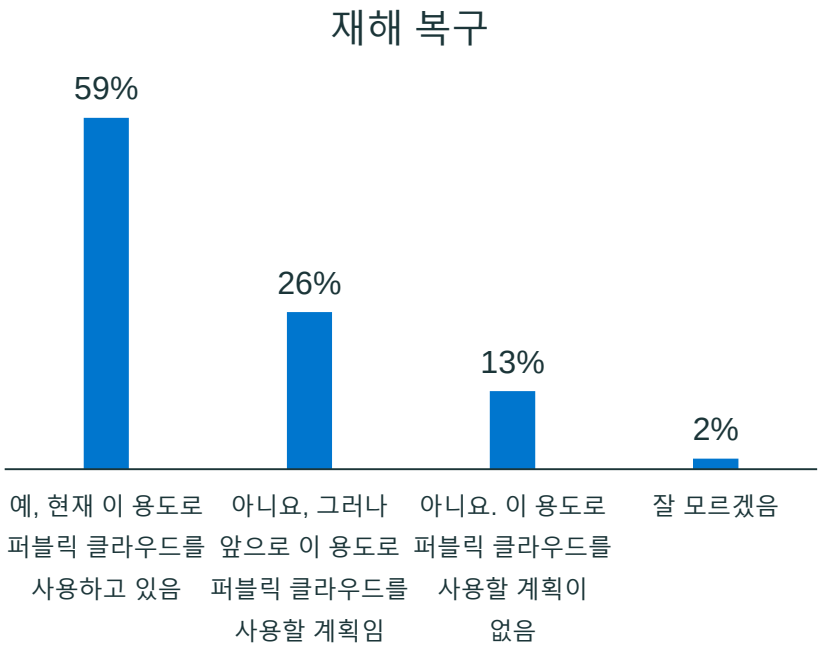


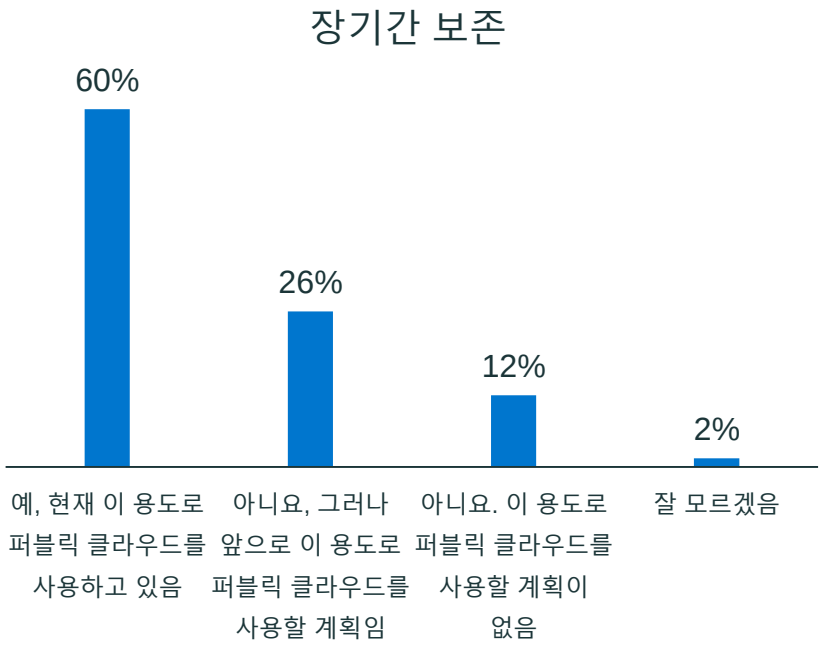
그러나 퍼블릭 클라우드 환경 전반에 걸쳐 데이터를 보호할 수 있는 조직의 역량을 확신하지 못하는 경우가 많음



- 매우 확신함 - 퍼블릭 클라우드 전반에 걸쳐 모든 데이터를 보호함
- 보통 수준으로 확신함 – 퍼블릭 클라우드 전반에 걸쳐 중요 데이터는 모두 보호하지만 모든 데이터를 보호하지는 못함
- 다소 의심스러움 – 퍼블릭 클라우드 전반에 걸쳐 대부분의 중요 데이터를 보호함
- 그다지 확신하지 못함 – 퍼블릭 클라우드 전반에 걸쳐 중요 데이터 일부를 보호함
- 전혀 확신하지 못함 – 퍼블릭 클라우드 전반에 걸쳐 데이터를 보호하지 못함
- 잘 모르겠음

조직의 재해 복구 및 장기간 보존 전략에서 퍼블릭 클라우드의 역할이 확대되고 있음

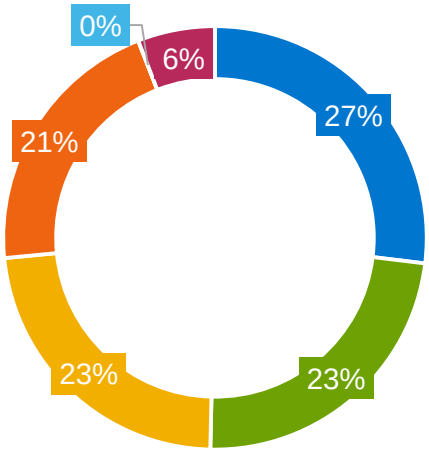




멀티 클라우드 환경을 사용하는 여러 조직이 이 환경을 보호하기 위한 특정 솔루션을 사용하지 않고 있음

21%

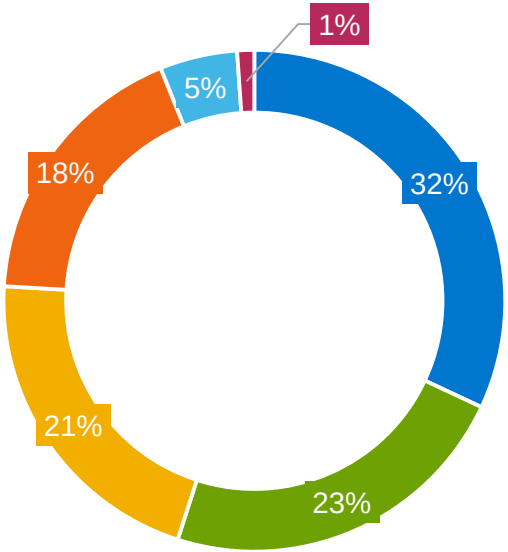
멀티 클라우드 환경을 사용할 때 **각 클라우드 서비스 공급업체**가 **워크로드 보호**를 담당한다고 생각하는 비율



- 멀티 클라우드 전반에 걸쳐 워크로드의 백업을 지원하기 위해 데이터 보호 솔루션을 업그레이드할 계획임
- 현재의 백업 솔루션으로 멀티 클라우드에서 실행되는 워크로드를 보호할 수 있음
- 멀티 클라우드에서 실행 중인 워크로드를 보호하기 위해 다양한 백업 툴을 사용함
- 각 클라우드 서비스 공급업체가 워크로드 보호를 담당함
- 기타
- 멀티 클라우드 환경에서 워크로드를 실행하고 있지 않음

클라우드에서 VMware를 사용하여 가상화된 워크로드 보호를 고려 중인 경우에도 비슷함

- VMware 워크로드의 하이브리드 클라우드 백업을 지원하기 위해 데이터 보호 솔루션을 업그레이드할 계획임
- 클라우드 서비스 공급업체가 워크로드 보호를 담당함
- 현재 온프레미스에서 사용 및 운영되는 백업 툴을 사용함
- 클라우드 서비스 공급업체 시장에서 구매 가능한 백업 툴을 사용함
- 클라우드에서 VMware를 사용하여 가상화된 워크로드를 실행하고 있지 않거나 실행할 계획이 없음
- 잘 모르겠음

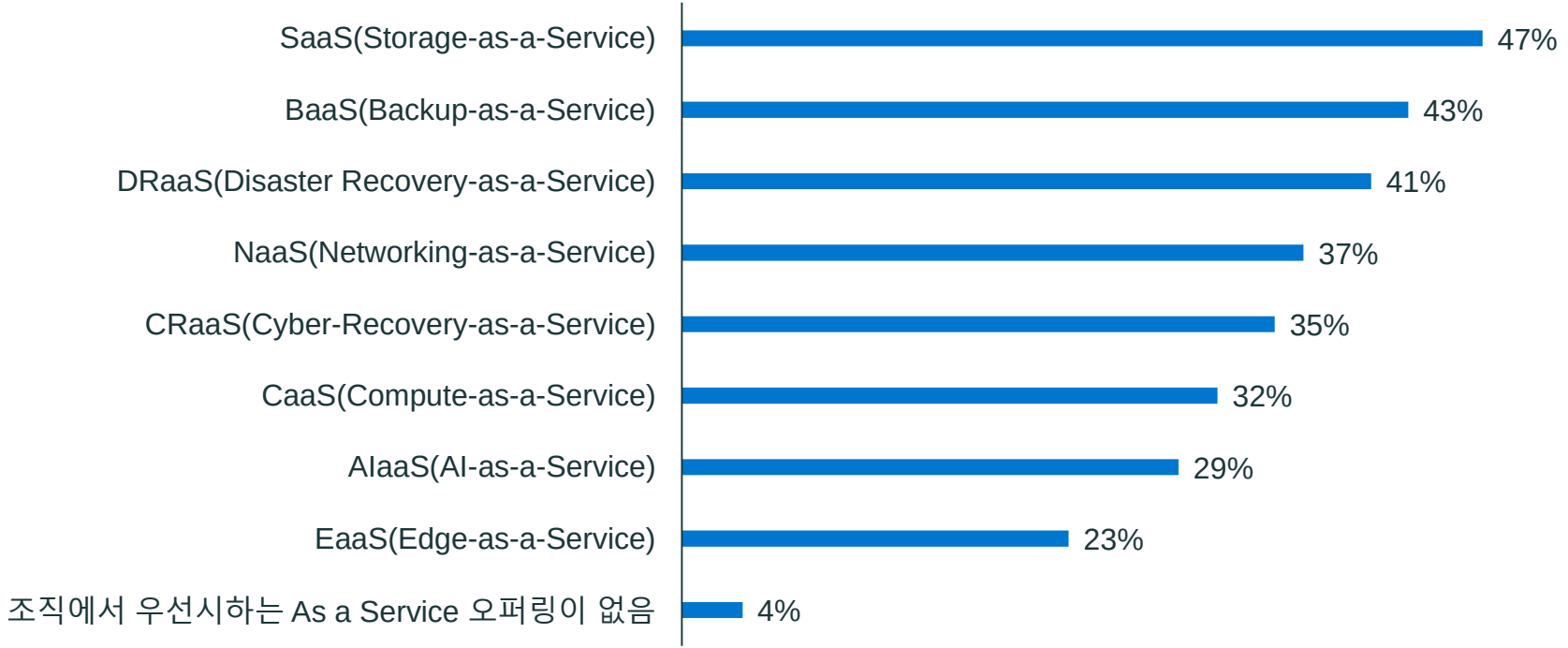


23%

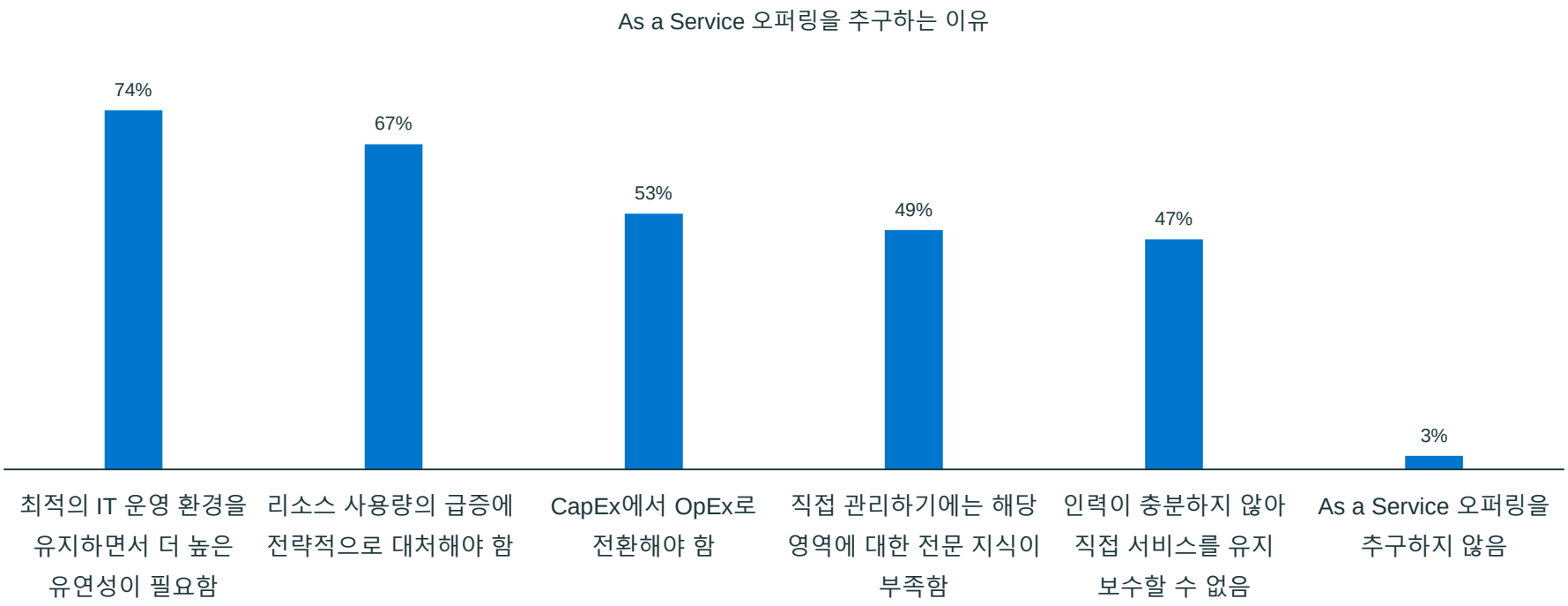
이용 중인 **클라우드 서비스 공급업체**가 **가상화된 워크로드 보호를 담당**한다고 생각하는 비율

5. As a Service의 성장

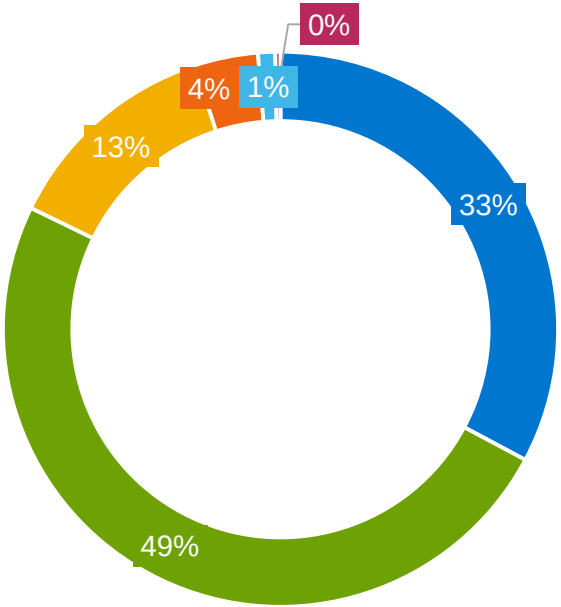
As a Service 오퍼링은 대부분의 조직에서 우선시되고 있으며, BaaS(Backup-as-a-Service)와 DRaaS(Disaster Recovery-as-a-Service)가 가장 일반적으로 우선시됨



As a Service 오퍼링의 대중성은 보통 유연성에 기인함



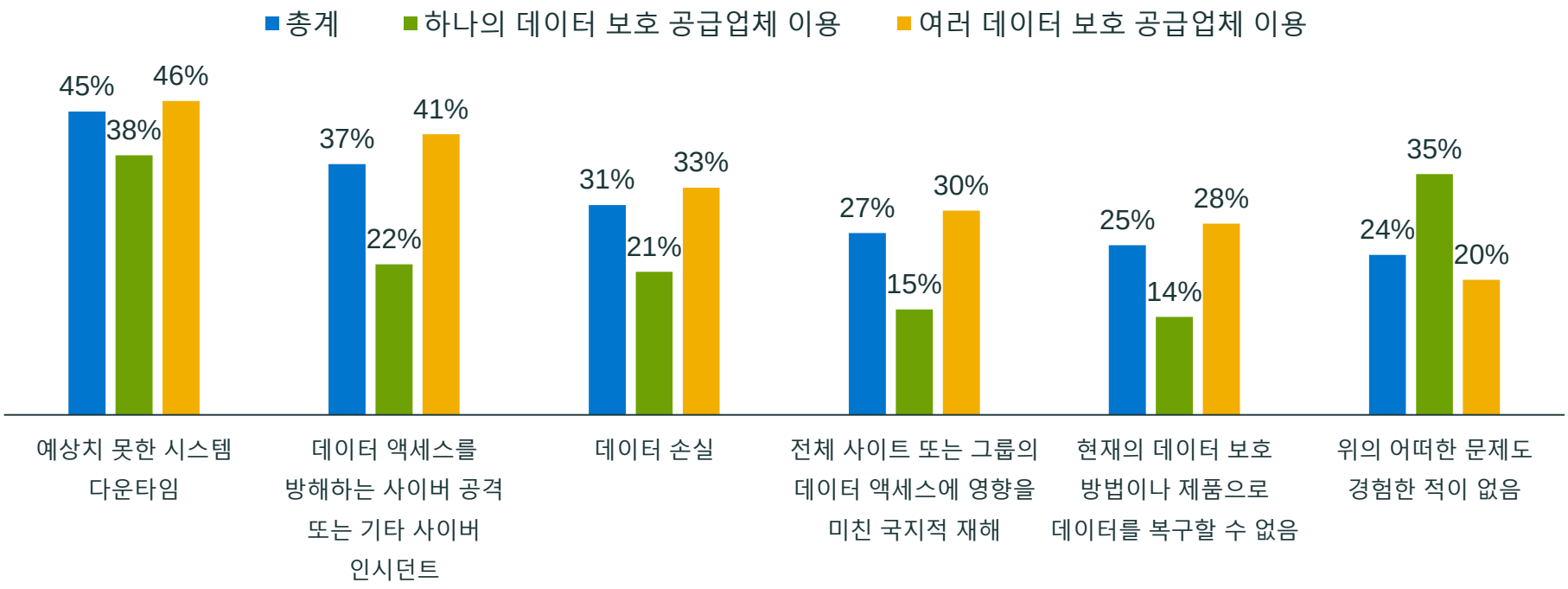
대다수는 여러 As a Service 오퍼링을 갖춘 공급업체와 협력하는 편을 선호하는데, 이는 더 적은 수의 공급업체로 워크로드를 통합하고자 하는 바람을 시사함



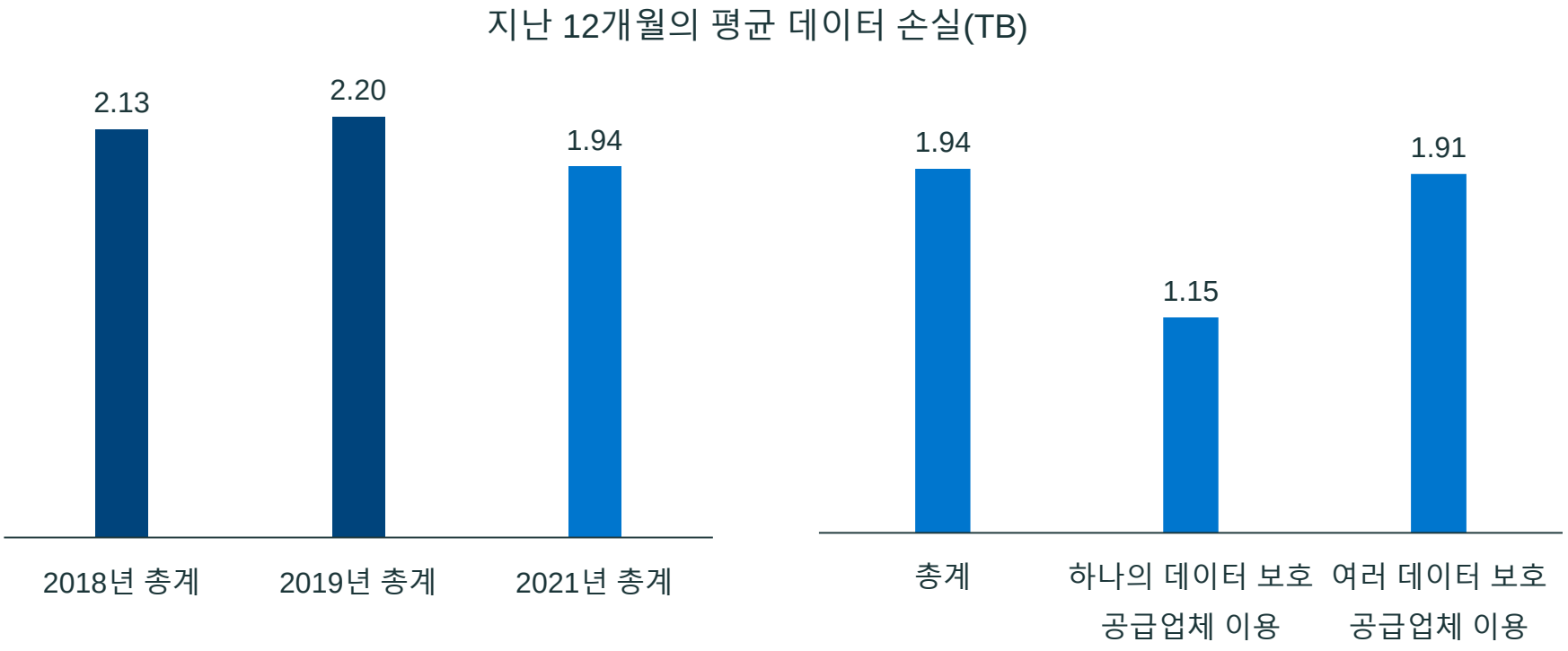
- 여러 As a Service 오퍼링을 갖춘 공급업체를 모색할 가능성이 매우 높음
- 여러 As a Service 오퍼링을 갖춘 공급업체를 모색할 가능성이 다소 높음
- 공급업체가 여러 As a Service 오퍼링을 갖추고 있는지 여부에 관심 없음
- 여러 As a Service 오퍼링을 갖춘 공급업체를 모색할 가능성이 다소 낮음
- 여러 As a Service 오퍼링을 갖춘 공급업체를 모색할 가능성이 매우 낮음
- 잘 모르겠음

6. 데이터 보호 간소화

여러 데이터 보호 공급업체를 이용하는 조직은 하나의 공급업체만 이용하는 조직에 비해 작년에 데이터 손실, 데이터 액세스 또는 시스템 다운타임과 관련된 많은 문제를 겪었을 가능성이 높음



여러 데이터 보호 공급업체를 이용하는 조직은 하나의 공급업체를 사용하는 조직에 비해 평균적으로 더 많은 데이터를 손실함



주요 연구 결과 – 요약(1/2)

데이터 보호의 위험 환경

- 데이터 손실 인시던트 발생 시 SLO를 충족하도록 모든 시스템/데이터를 복구할 수 없을 것으로 우려하는 경우가 많음
- 조직이 앞으로 12개월 내에 운영 중단 사고를 경험하고 이러한 운영 중단 사고가 재정적으로 심각한 영향을 미칠 것이라는 우려가 팽배함
- 조직은 이러한 사고가 발생할 경우 대응할 수 있도록 준비해야 함

사이버 공격으로 인한 위협

- 조직이 멀웨어와 랜섬웨어 위협으로부터 보호하지 못할 것으로 우려하며, 재택 근무의 증가로 인해 사이버 공격 위험이 증가했다는 데 대부분이 동의함
- 조직이 공격을 받더라도 모든 비즈니스 크리티컬 데이터를 복구할 수 있다고 확신하는 경우는 매우 적음

새로운 기술 및 첨단 기술 지원

- 조직은 SaaS 애플리케이션, AI/ML, 엣지/IoT 디바이스 등 다양한 새로운 기술 및 첨단 기술에 투자하고 있지만, 이러한 기술에 맞춰 데이터를 보호하는 데는 어려움을 겪는 경우가 많음
- 다수는 이러한 기술이 데이터 보호 측면에서 위험을 야기한다고 생각하며, 이러한 위험은 조직이 미래에 대한 대비가 되지 않았고 12개월 이내에 운영 중단을 경험할 위험을 안고 있다는 우려의 원인이 됨
- 첨단 기술에 대한 투자는 바람직하고 장려해야 할 일이지만, 조직은 데이터 보호 인프라스트럭처가 이러한 기술을 지원하도록 해야 함

주요 연구 결과 – 요약(2/2)

클라우드 환경의 데이터 보호 취약성

- 애플리케이션은 다양한 클라우드 환경에 걸쳐 업데이트 및 배포되고 있지만, 데이터가 얼마나 적절히 보호되고 있는지에 관해서는 확신이 부족한 경우가 많음
- 클라우드는 재해 복구 및 장기간 보존 전략에서 중요한 역할을 함
- 일부 조직은 여전히 클라우드 공급업체에 데이터 보호의 책임이 있다고 생각하지만, 조직은 멀티 클라우드 및 가상화된 워크로드의 데이터를 보호하기 위한 구체적인 솔루션을 준비해야 함

As a Service의 성장

- As a Service 솔루션은 대부분의 조직이 관심을 갖고 있으며, 향후 많은 조직에서 데이터 보호 솔루션의 일부가 될 가능성이 높음. 이러한 관심의 주된 이유는 유연성임
- 대부분이 선호할 방식은 여러 오퍼링을 갖춘 공급업체의 As a Service 솔루션을 사용하는 것이며, 이 경우 조직의 데이터 보호를 간소화하는 데 도움이 됨

데이터 보호 간소화

- 하나의 데이터 보호 공급업체를 이용하는 조직은 여러 공급업체를 이용하는 조직에 비해 작년 한해 데이터 손실, 데이터 액세스 문제, 예상치 못한 시스템 다운타임을 경험했을 가능성이 낮음
- 또한 하나의 공급업체를 이용하는 조직에서 발생하는 데이터 손실은 여러 솔루션을 이용하는 조직에 비해 평균적으로 더 적음
- 조직은 새로운 솔루션에 투자하는 방법으로 데이터 보호 역량을 확장하고자 할 수 있지만, 솔루션을 하나의 공급업체로 통합하는 편이 데이터 손실과 다운타임과 관련하여 더 효과적으로 보호할 가능성이 높음

위험 최소화 및 경쟁 우위 확보

Dell Technologies의 관점

데이터 보호
역량 점검을
정기적으로 수행

사이버
회복탄력성을
최우선으로 고려

Dell
Technologies와의
협력으로 데이터 보호
이니셔티브 통합

자세한 정보: DellTechnologies.com/GDPI


DELL Technologies