

Global Data Protection Index - 2024년 특별 에디션

주요 결과 - 2023년 10월



VansonBourne



주요 연구 결과의 중점 사항

1

데이터 보호의 위험 환경

2

증가하는 사이버 공격 위협

3

멀티클라우드 사용

4

클라우드 환경 보호

5가지 핵심 내용



사이버 공격은
계속 증가하고
있습니다.



사이버 공격으로 인한
피해액이 증가하고
있습니다.



공격으로 인해
부담해야 하는 비용을
보험으로 충분히
충당하지 못하고
있습니다.



GenAI 사용 증가로
인해 가치 높은
데이터가 증가할 수
있습니다.



사이버 공격의
위험이 증가하고
재정적 영향이
높아지고 있습니다.

인터뷰 대상



2023년 9월과 10월에 IT
및 IT 보안 의사 결정권자
1,500명 인터뷰



다양한 공공 및 민간
업계의 조직



직원 수가 250명 이상인
조직



4개 지역:
미주(300명)
EMEA(675명)
APJ(375명)
중국(150명)

1. 데이터 보호의 위험 환경

데이터 보호 조치에 대한 우려가 널리 확산되고 있으며, 확신이 부족한 상태에서 많은 조직이 취약한 상황에 놓여 있습니다



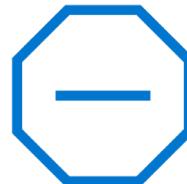
60%

조직이 백업 및 복구
SLO(Service Level
Objective)를 충족한다고
그다지 확신하지 못하는 비율



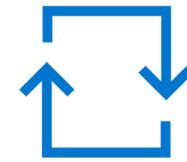
79%

앞으로 12개월 이내에 운영
중단 사고를 경험할 것으로
우려하는 비율



75%

조직의 기존 데이터 보호
수단이 멀웨어 및 랜섬웨어
위협에 대처하기에 충분하지
않을 수 있음을 우려하는
비율

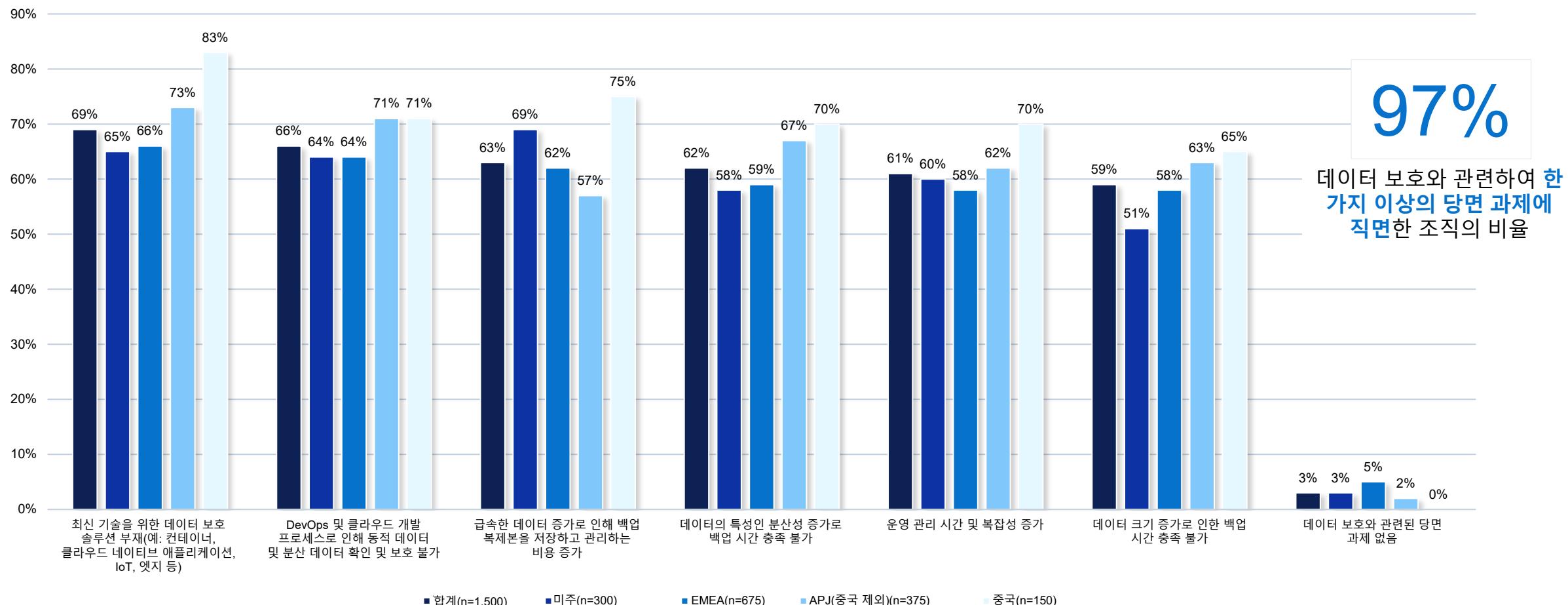


65%

데이터 손실 인시던트 발생
시 조직이 모든 플랫폼에서
시스템/데이터를 완전히
복구할 수 있다고 확신하지
못하는 비율

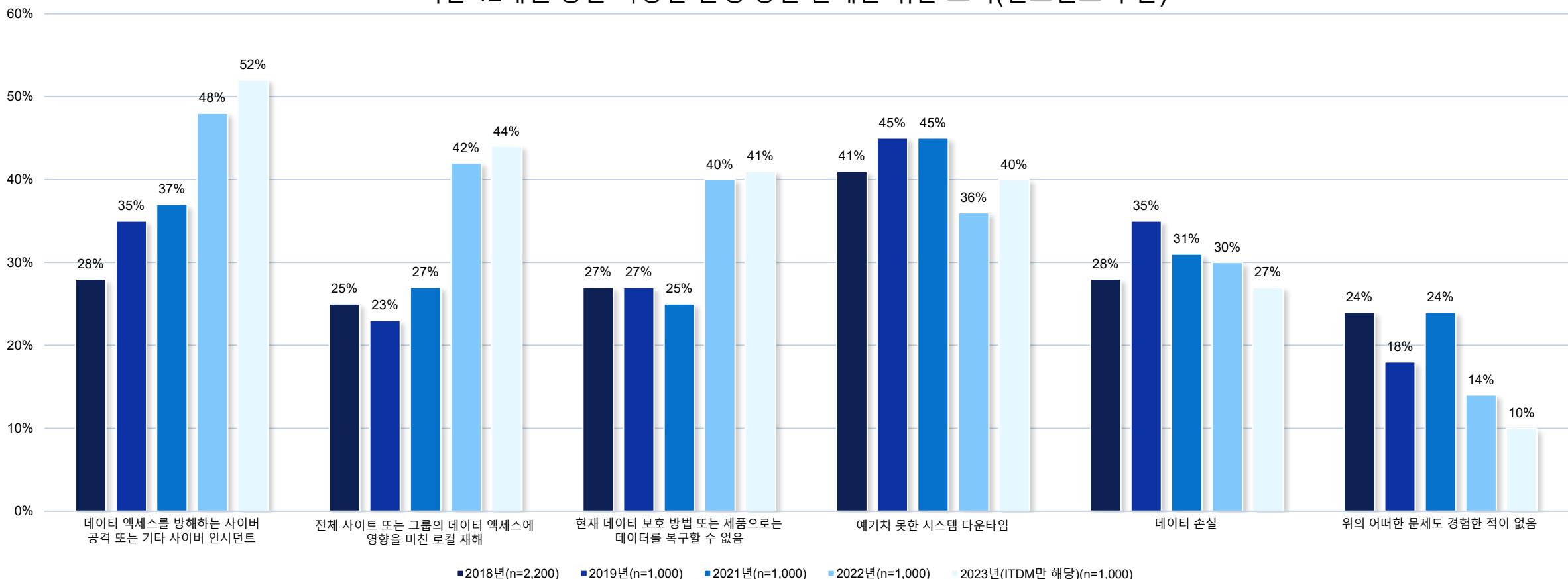
데이터 보호에 대한 우려 외에도 많은 조직이 여러 당면 과제에 직면하고 있습니다

데이터 보호 관련 당면 과제 중 상위 5위(지역별로 구분)



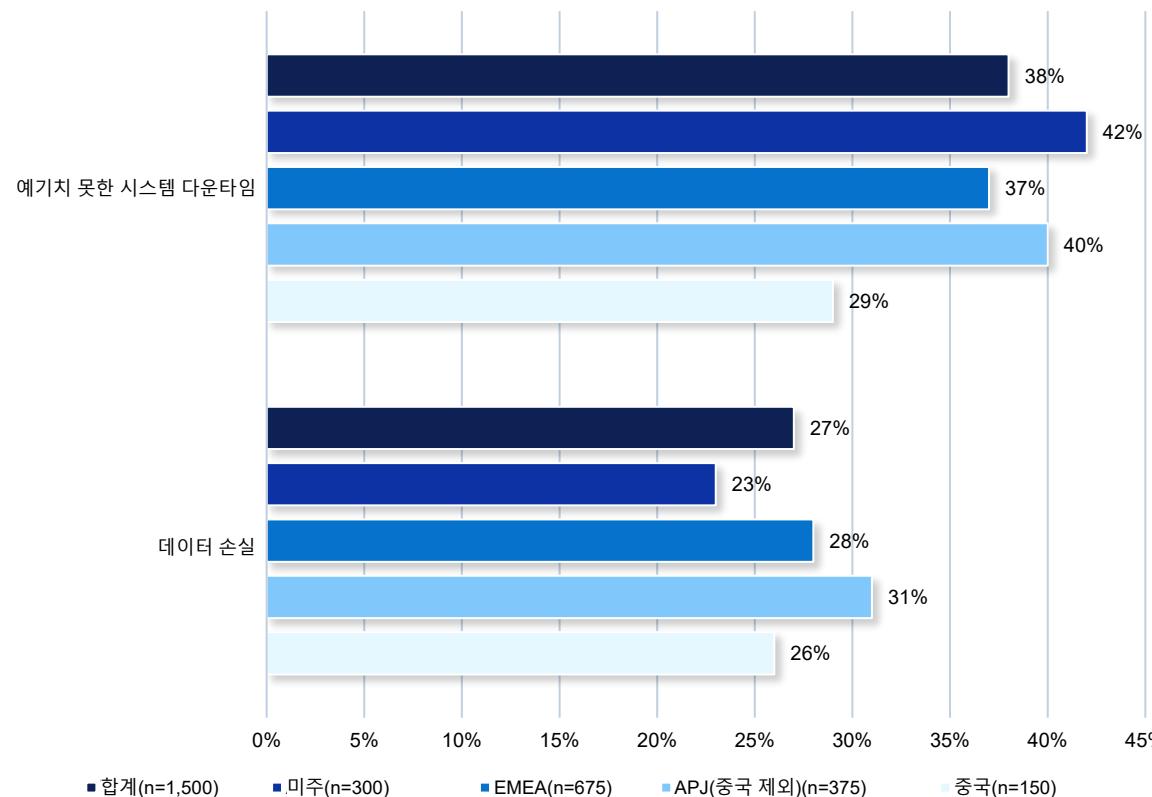
지난 12개월 동안 사이버 공격이 점차 늘어나며 끊임없이 위협을 가하는 상황에서 많은 조직이 심각한 운영 중단 사태에 직면했습니다

지난 12개월 동안 다양한 운영 중단 문제를 겪은 조직(연도별로 구분)



데이터 손실은 운영 중단의 원인이 되었을 뿐만 아니라 수익에도 영향을 미쳤습니다

지난 12개월 동안 예기치 못한 시스템 다운타임 또는 데이터 손실을 경험한 조직의 비율(지역별로 구분)



지난 12개월 동안 발생한 피해

26시간

예기치 못한 시스템 다운타임(평균)

2.45TB

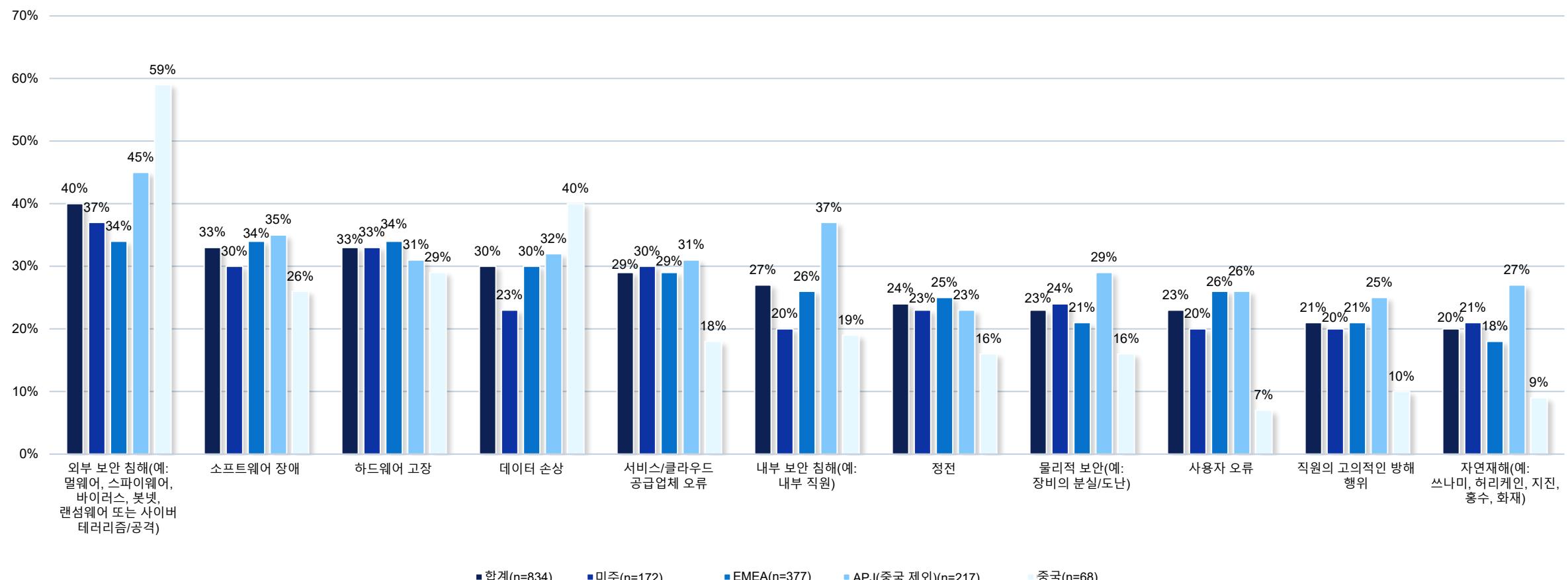
손실된 데이터의 양(평균)

\$261만

(평균) 데이터 손실에 따른 비용

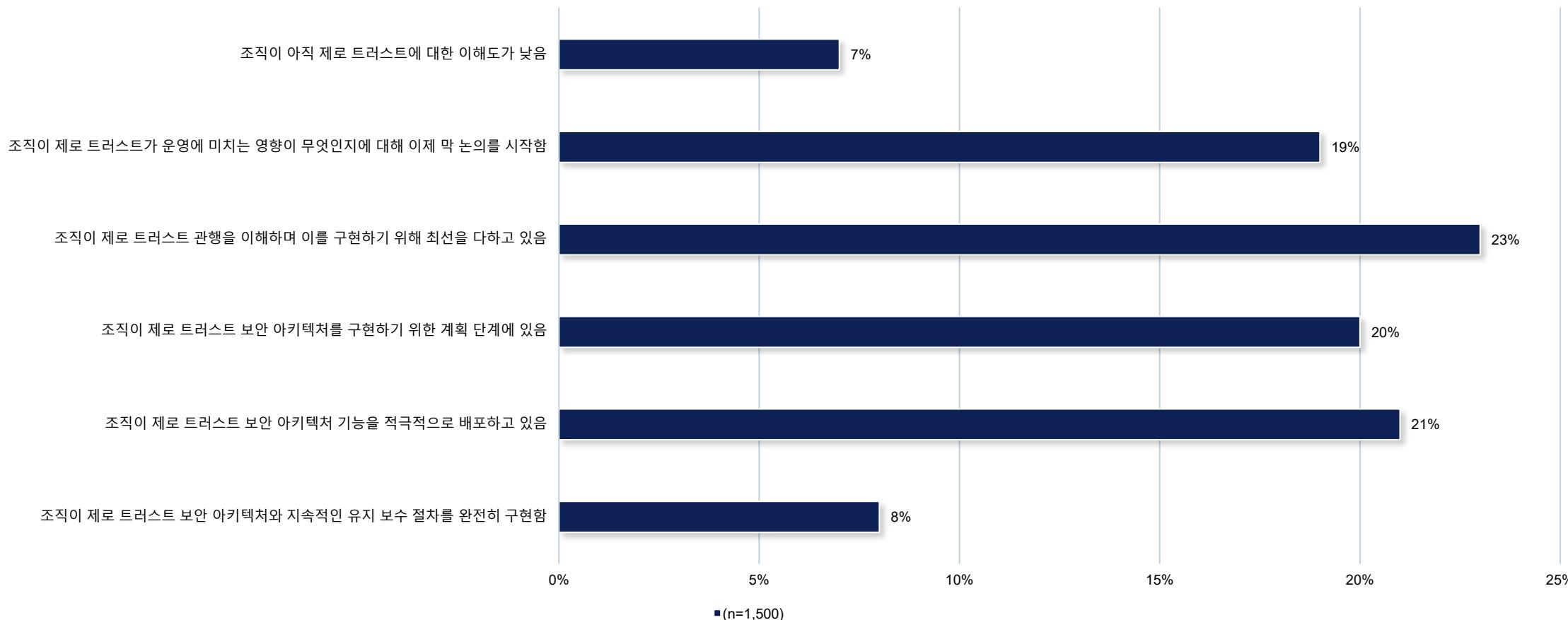
외부 보안 위협은 지난 12개월 동안 데이터 손실 및/또는 예기치 못한 시스템 다운타임의 가장 일반적인 원인이었습니다

지난 12개월 동안의 데이터 손실 및/또는 시스템 다운타임에 대한 원인



데이터 보호 관련 당면 과제와 우려에도 불구하고 제로 트러스트 보안을 완전히 구현한 조직은 거의 없습니다

제로 트러스트 보안을 구현하기 위한 조직의 여정

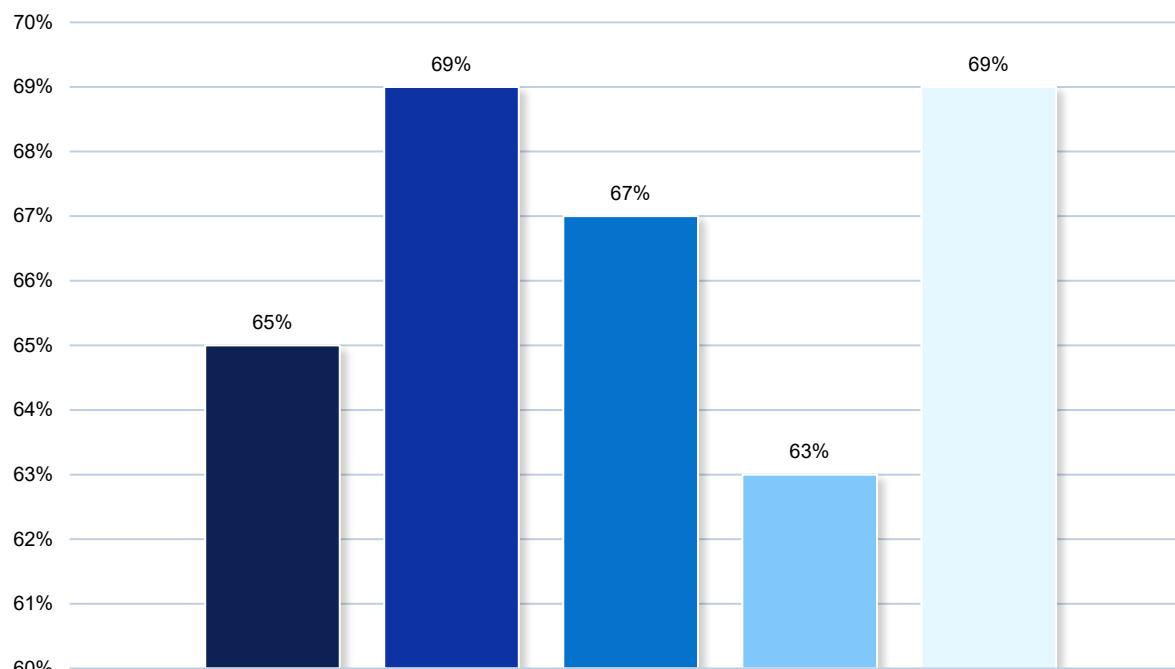


필터: 데이터 분할: 지역 = 합계

2. 증가하는 사이버 공격 위협

데이터 보호 조치에 대한 우려가 널리 확산되고 있으며, 확신이 부족한 상태에서 많은 조직이 취약한 상황에 놓여 있습니다

파괴적인 사이버 공격 발생 시 모든 비즈니스 크리티컬 데이터를 안정적으로 복구할 수 있다는 데 대해 "매우 확신함"이라고 답하지 않은 비율(연도별로 구분)



■ 2018년(n=2,200) ■ 2019년(n=1,000) ■ 2021년(n=1,000) ■ 2022년(n=1,000) ■ 2023년(ITDM만 해당)(n=1,000)



81%

직원 재택근무의 증가로 인해
사이버 위협으로 인한 데이터
손실 위험에 더 많이
노출되었다는 데 동의한 비율



74%

백업 데이터가 랜섬웨어
공격으로 인해 손상될 수
있다고 우려하는 비율

랜섬웨어 공격의 결과를 둘러싼 잘못된 자신감으로 인해 위험이 가중되고 있습니다



72%

조직 내 업무와 직원들이
**랜섬웨어 공격의 영향을 받지
않을 것이다**는 데 동의하는
비율



74%

조직이 랜섬웨어 공격을 당할
경우 **공격자에게 비용을
지불하면 모든 데이터를
되돌려받아** 비즈니스를
재개할 수 있을 것이라는 데
동의하는 비율

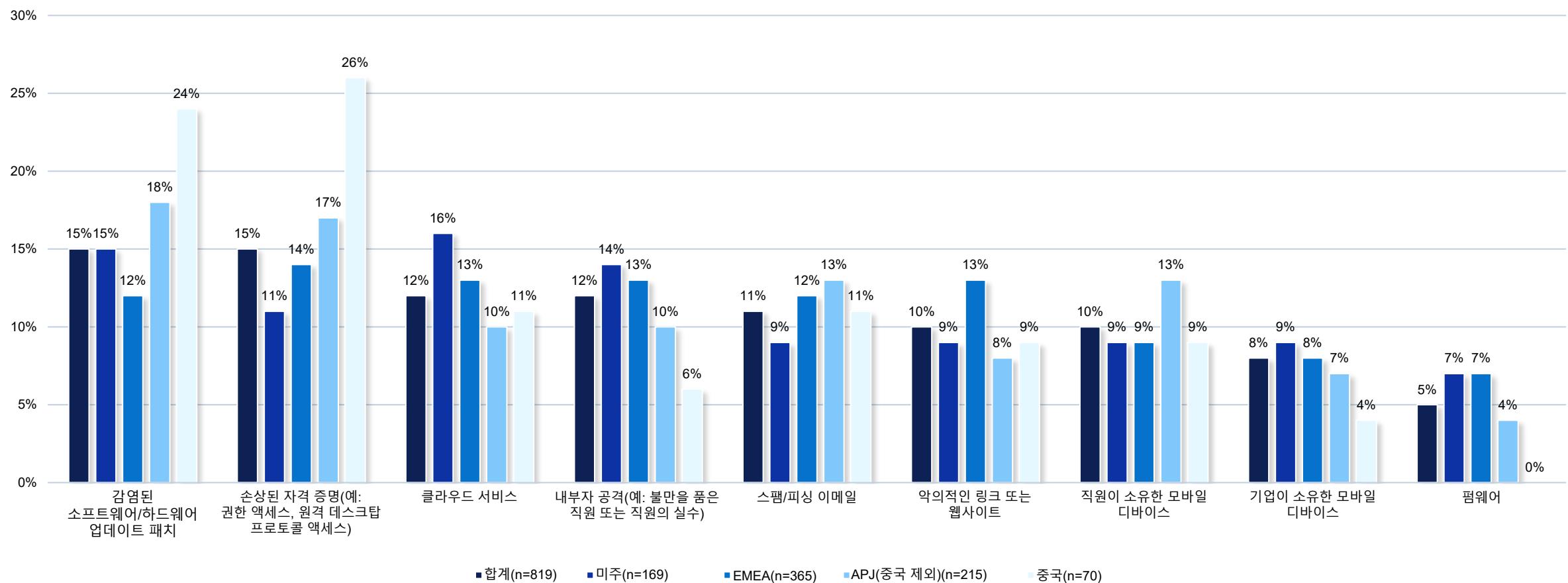


66%

조직이 랜섬웨어 공격을 당할
경우 **공격자에게 비용을
지불하면 다시는 공격을 받지
않을 것이라는** 데 **동의하는**
비율

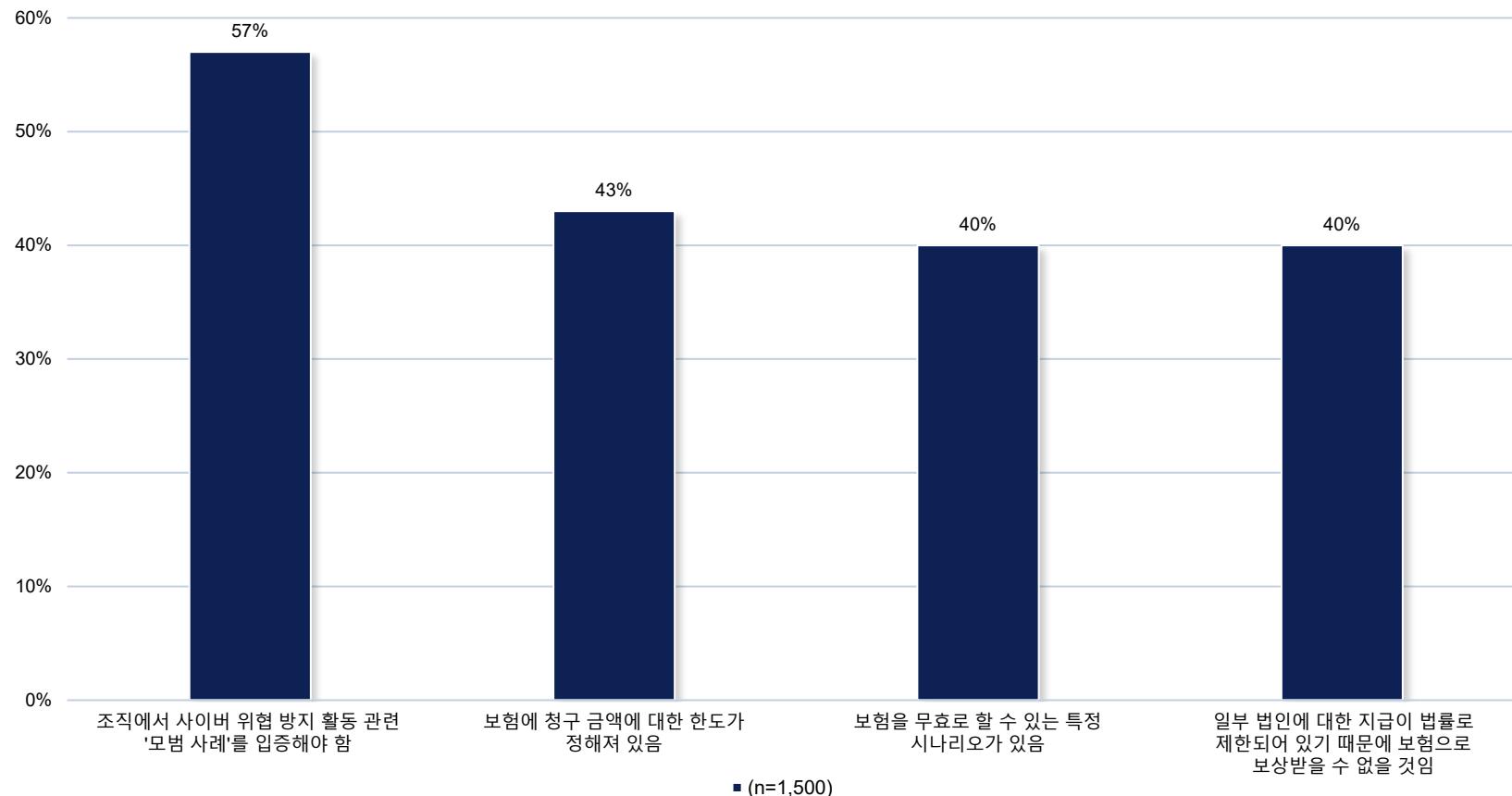
사이버 범죄자는 다양한 진입점을 표적으로 삼지만, 공격은 외부 소스로부터 발생할 가능성이 높습니다

조직이 최근에 받은 사이버 공격의 진입점(지역별로 구분)



랜섬웨어 보험은 조직에 보편화되어 있지만 제한 사항을 다수 포함합니다

조직의 랜섬웨어 보험 조건

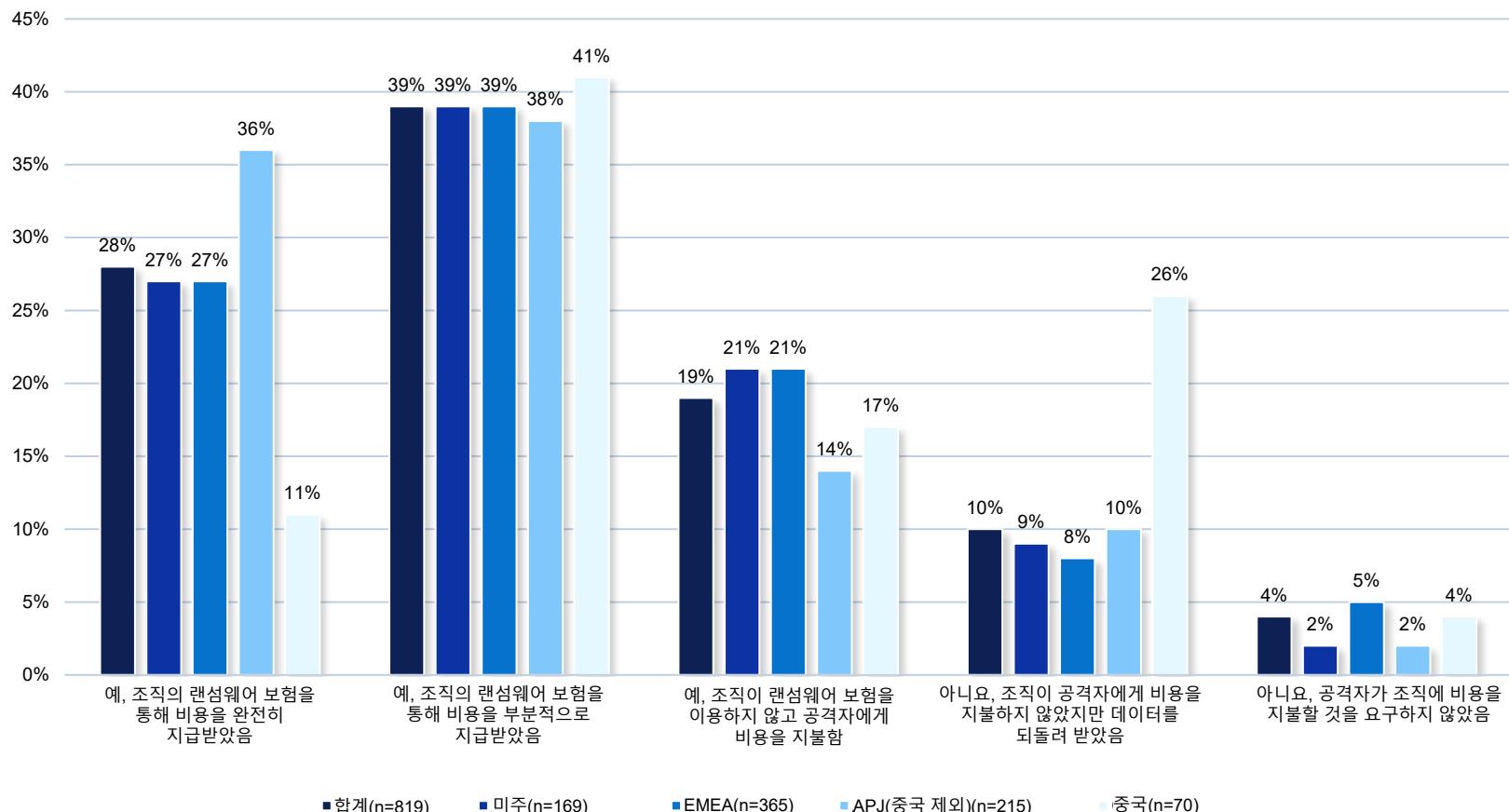


93%

랜섬웨어 보험을 보유한
조직의 비율

많은 조직이 랜섬웨어 보험을 보유하고 있지만 여전히 재정적 취약성을 안고 있습니다

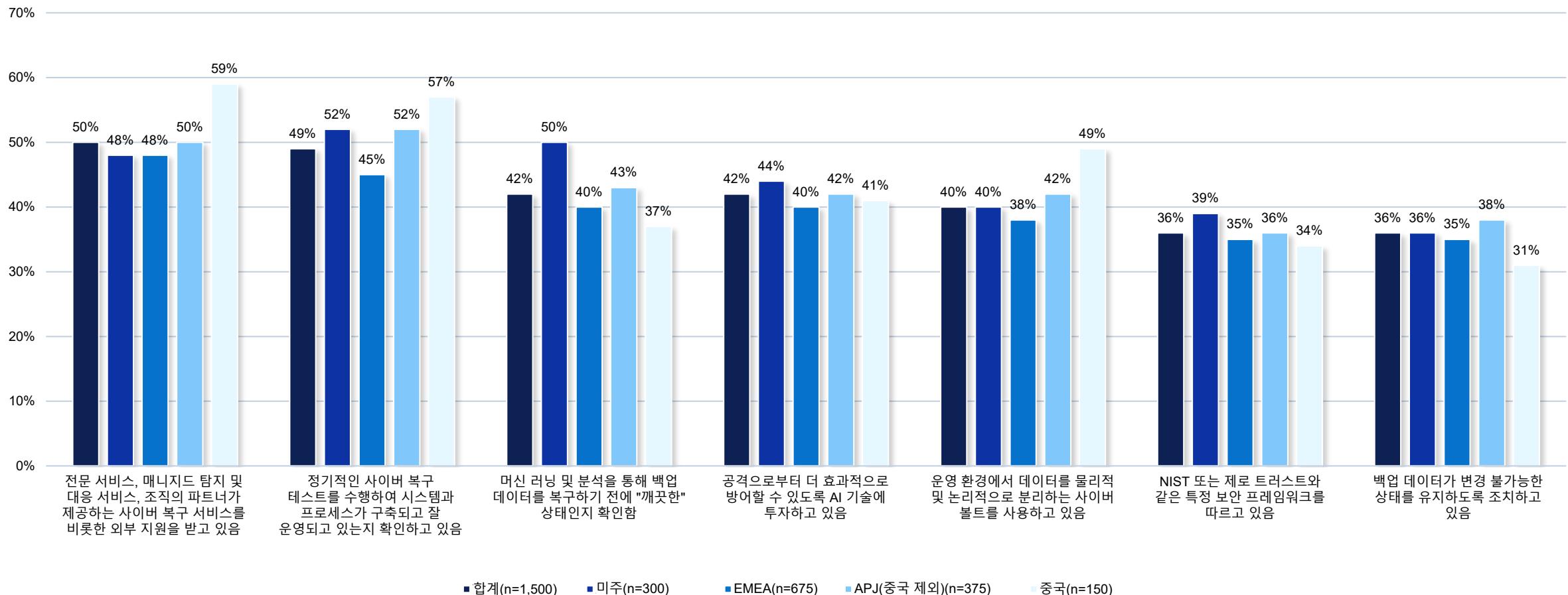
조직의 데이터에 액세스하기 위해 공격자에게 비용을 지불했는지 여부(지역별로 구분)



지난 12개월 동안 사이버 공격 및 기타 사이버 관련 인시던트로 인해 조직이 지불한 평균 비용

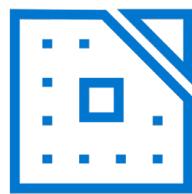
다행히도 많은 조직이 사이버 회복탄력성을 향상하기 위한 조치를 취하고 있습니다

조직이 사이버 회복탄력성을 개선하기 위해 취하고 있는 조치(지역별로 구분)



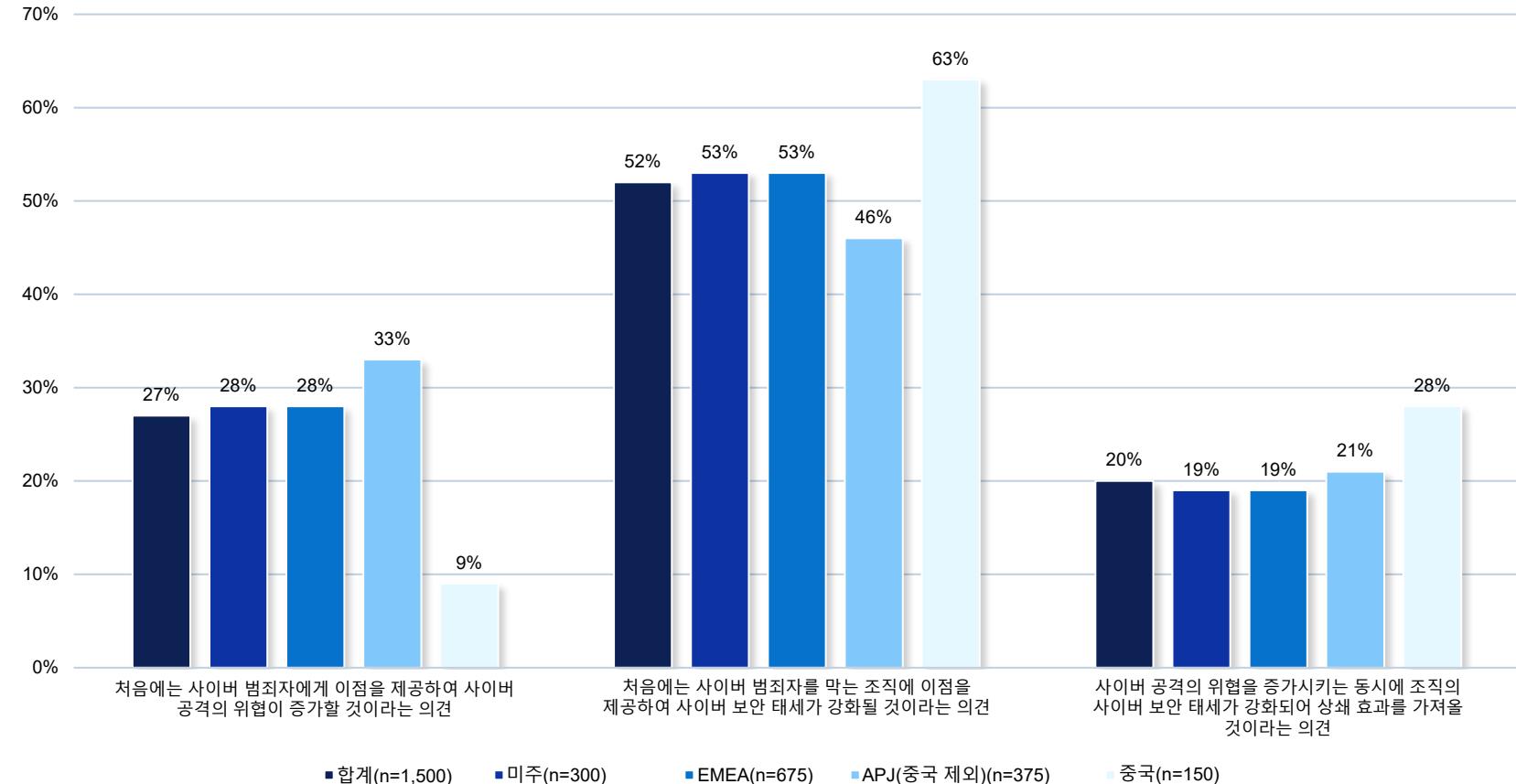
그러나 모든 조직이 Generative AI가 사이버 회복탄력성에 도움이 된다고 생각하는 것은 아닙니다

Generative AI가 사이버 위협과 데이터 보안에 미치는 영향(지역별로 구분)

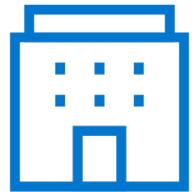


81%

새로운 기술(예: AI, IoT,
엣지)이 데이터 보호
측면에서 위험 요소가 된다는
데 동의하는 비율



실제로 조직들이 이미 데이터 보호에 대해 우려하고 있는 가운데
많은 조직에서 Generative AI로 인해 새로운 당면 과제가 발생할
것이라 믿고 있습니다



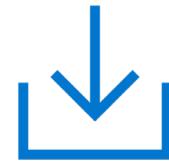
88%

Generative AI로 인해 대량의
새로운 데이터가 생성되고
이러한 데이터에 **보호 기능**
및 보안이 필요할 것이라는
데 동의하는 비율



88%

Generative AI로 인해 특정
데이터 유형의 가치가 높아져
더 높은 데이터 보호 서비스
수준이 필요하게 될 것이라는
데 동의하는 비율



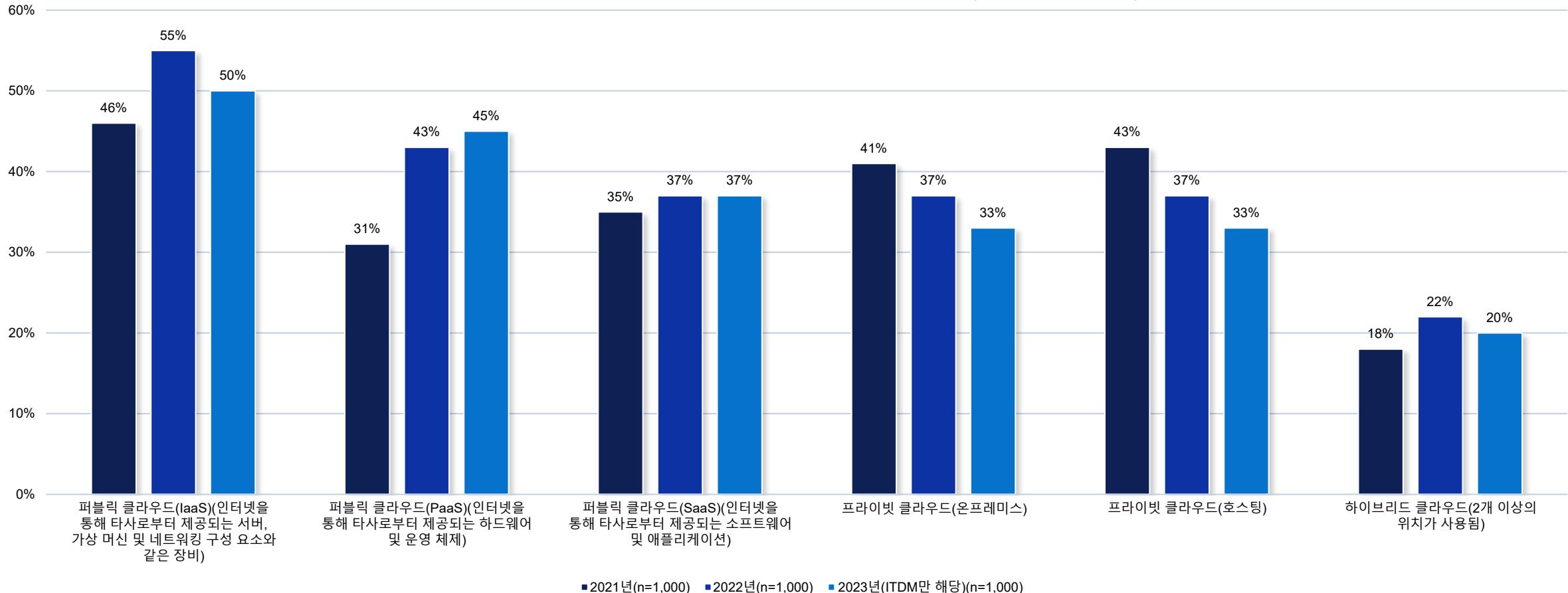
85%

Generative AI에 사용되는
데이터 세트가 **손상되면**
Generative AI 출력에 영향을
미칠 것이라는 데 동의하는
비율

3. 멀티클라우드 사용

퍼블릭 클라우드는 기존 애플리케이션을 업데이트할 때 여전히 인기 있는 옵션이지만 프라이빗 클라우드에 대한 선호도는 감소하고 있습니다

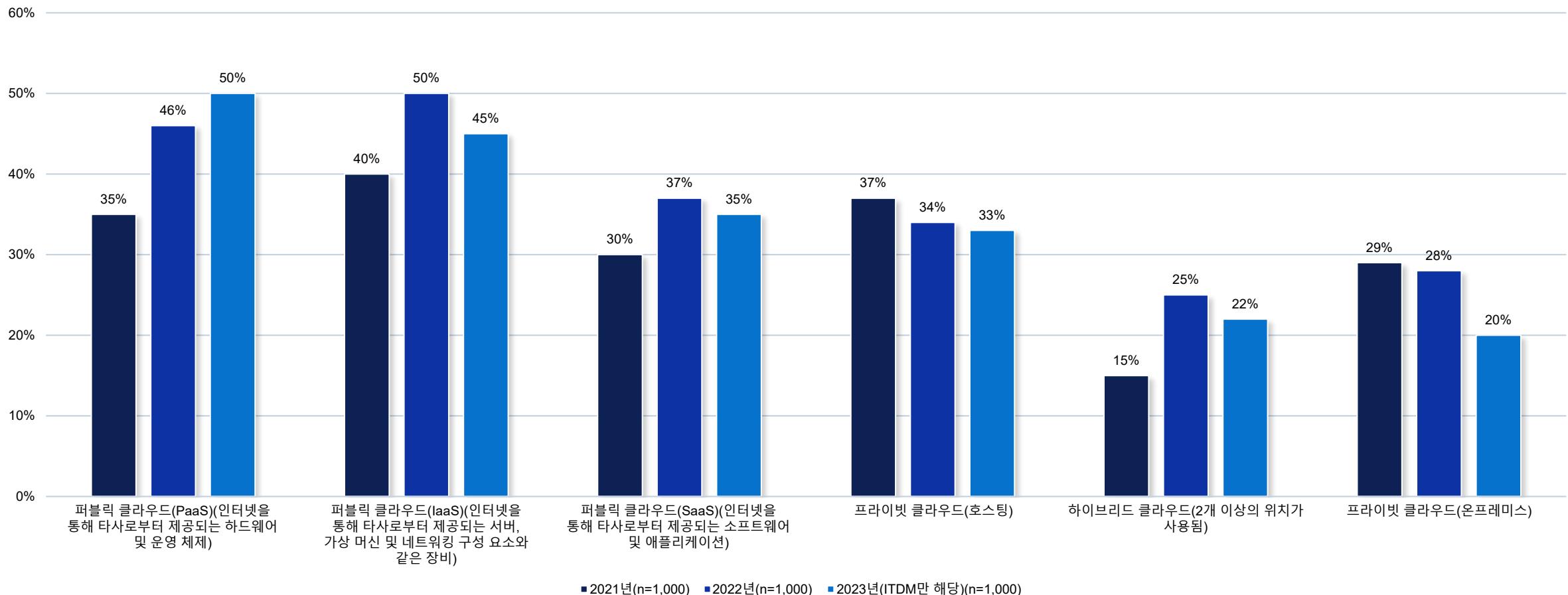
기준 애플리케이션을 업데이트할 때 취하는 방법(연도별로 구분)



■ 2021년(n=1,000) ■ 2022년(n=1,000) ■ 2023년(ITDM만 해당)(n=1,000)

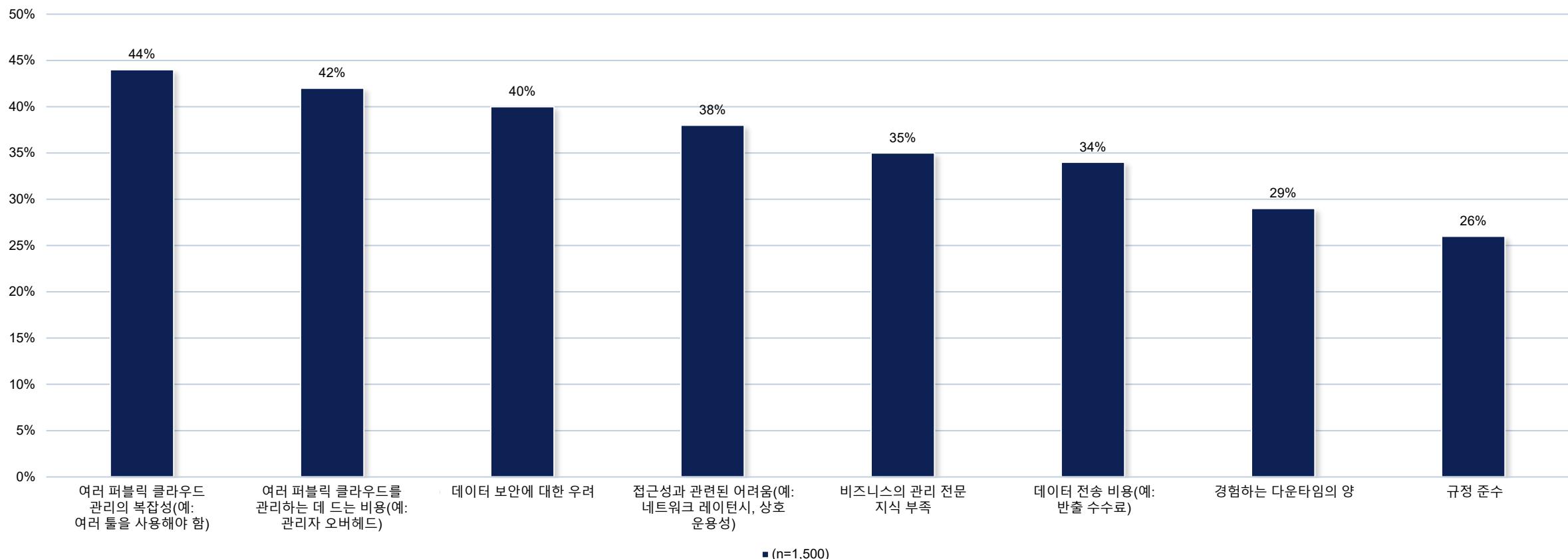
또한 퍼블릭 클라우드는 새로운 애플리케이션을 배포할 때 여전히 인기 있는 옵션이지만 지원은 감소하고 있을 수 있습니다

새로운 애플리케이션을 배포할 때 취하는 방법(연도별로 구분)



퍼블릭 클라우드의 인기에도 불구하고 많은 조직이 데이터를 유지할 때 어려움을 겪습니다

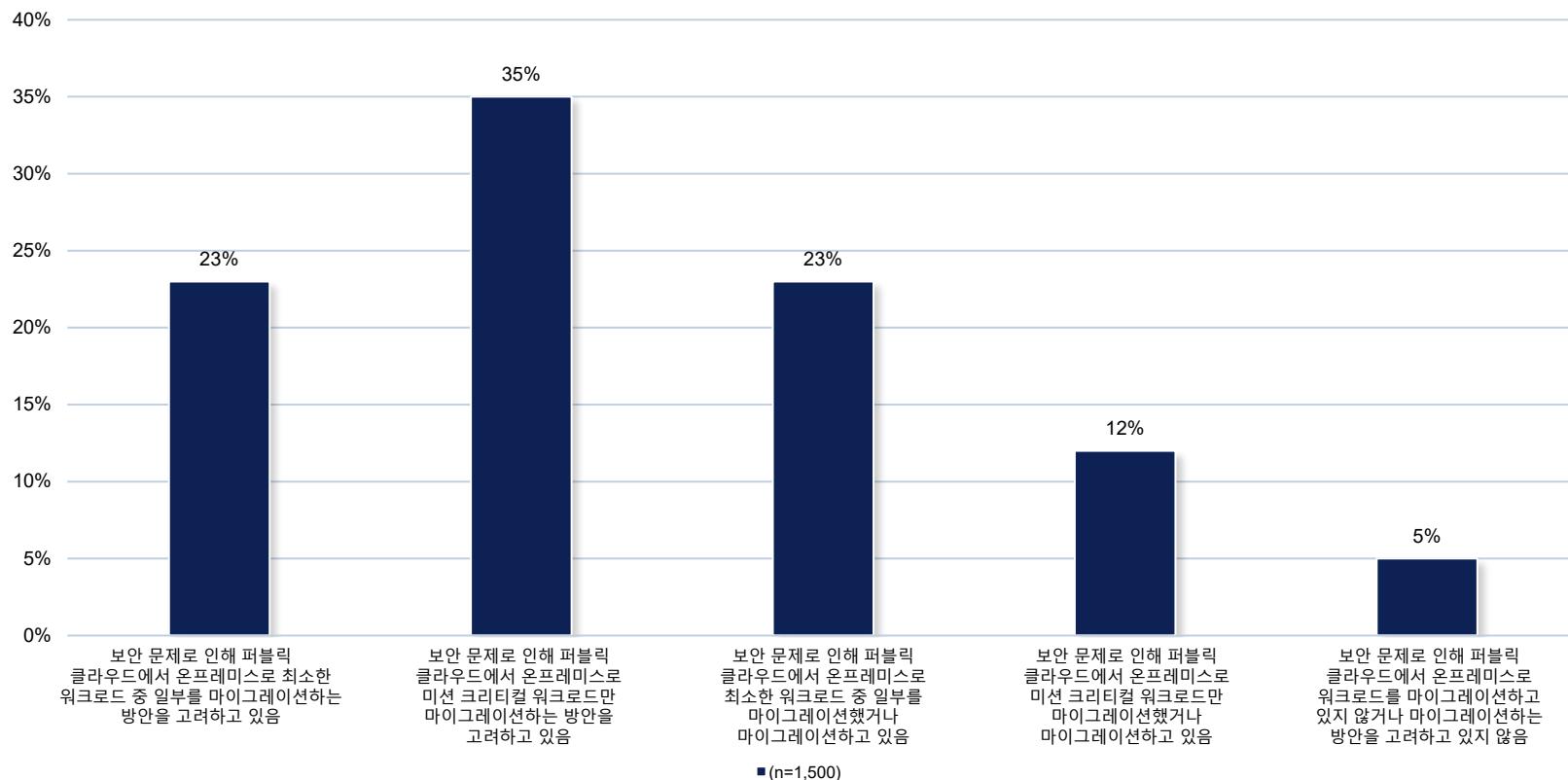
퍼블릭 멀티클라우드 환경에서 데이터를 유지할 때 조직이 직면하는 당면 과제



필터: 데이터 분할: 지역 = 합계

보안 문제로 인해 많은 조직이 퍼블릭 클라우드에서 온프레미스로 워크로드의 일부를 마이그레이션하고 있거나 마이그레이션을 고려하고 있습니다

조직이 퍼블릭 클라우드에서 온프레미스로 마이그레이션하려는 워크로드의 범위



필터: 데이터 분할: 지역 = 합계

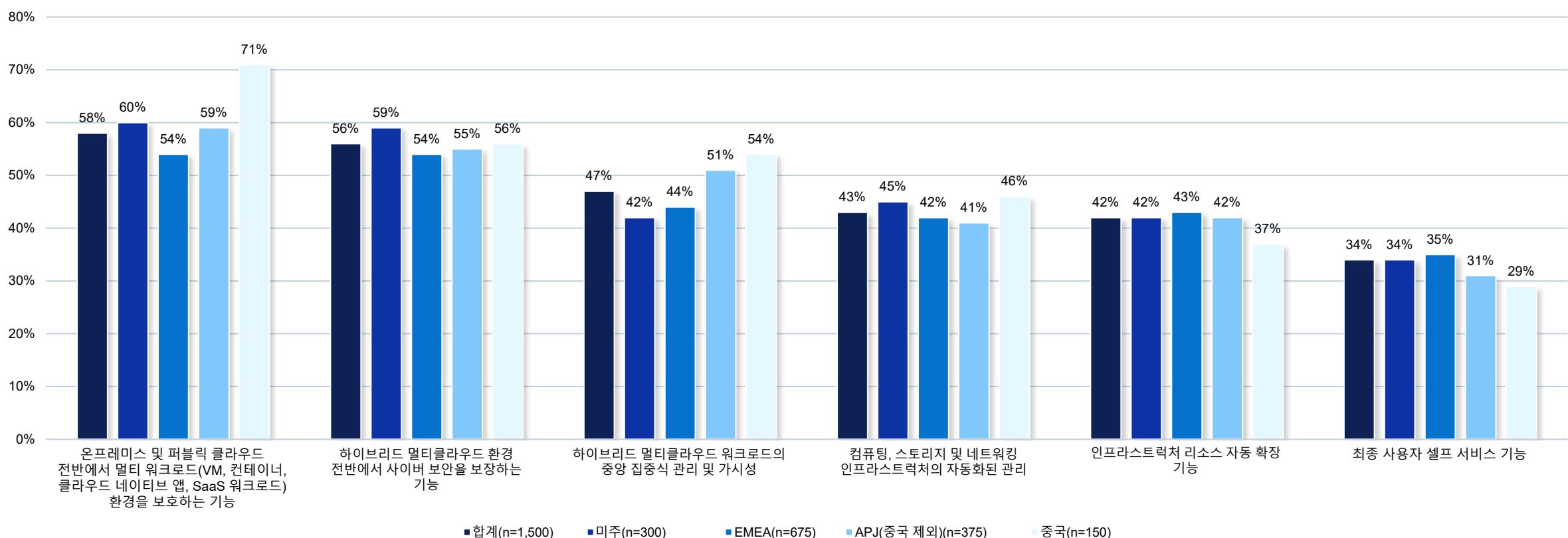


79%

조직이 퍼블릭 클라우드 환경 전반에서 **모든 데이터를 보호할 수 있다고 확신하지 않는** 비율

사이버 관련 인시던트 증가와 데이터 보호 전략에 대한 신뢰가 낮은 상황에서 하이브리드 멀티클라우드 운영을 활성화할 때 보안이 가장 중요한 기능으로 인식되는 경우가 많습니다

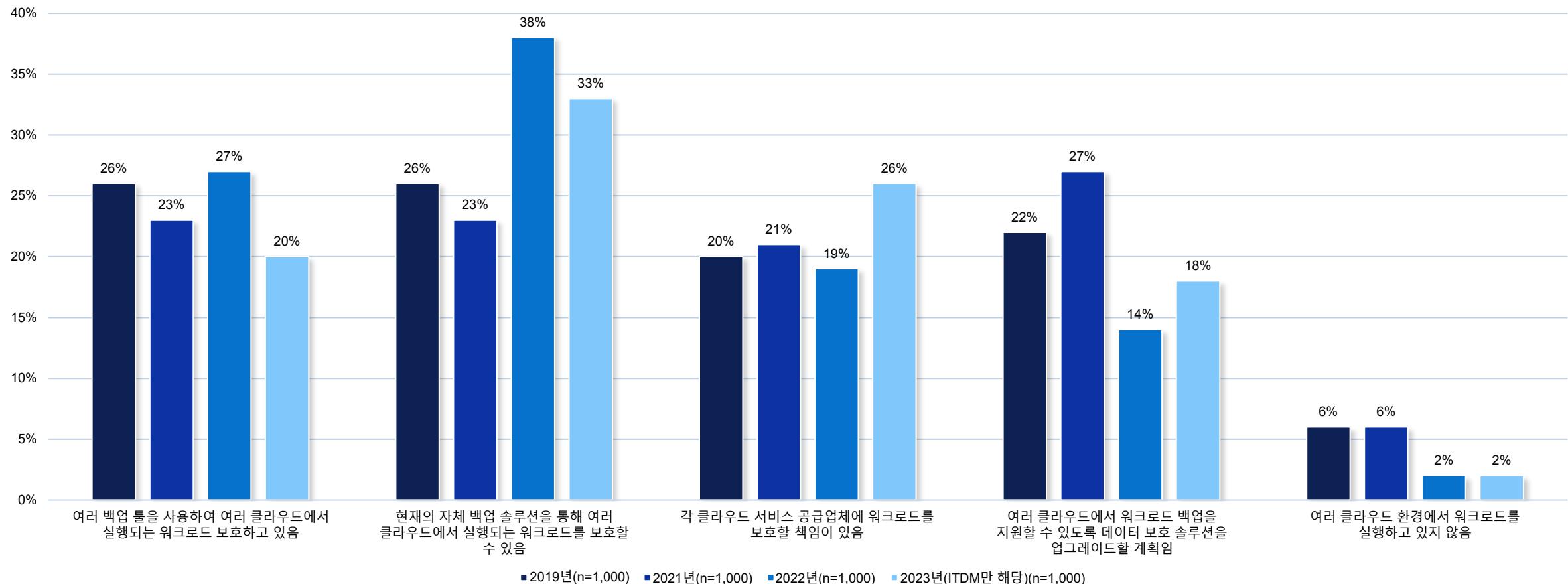
하이브리드 멀티클라우드 운영을 활성화할 때 가장 중요한 기능(지역별로 구분)



4. 클라우드 환경 보호

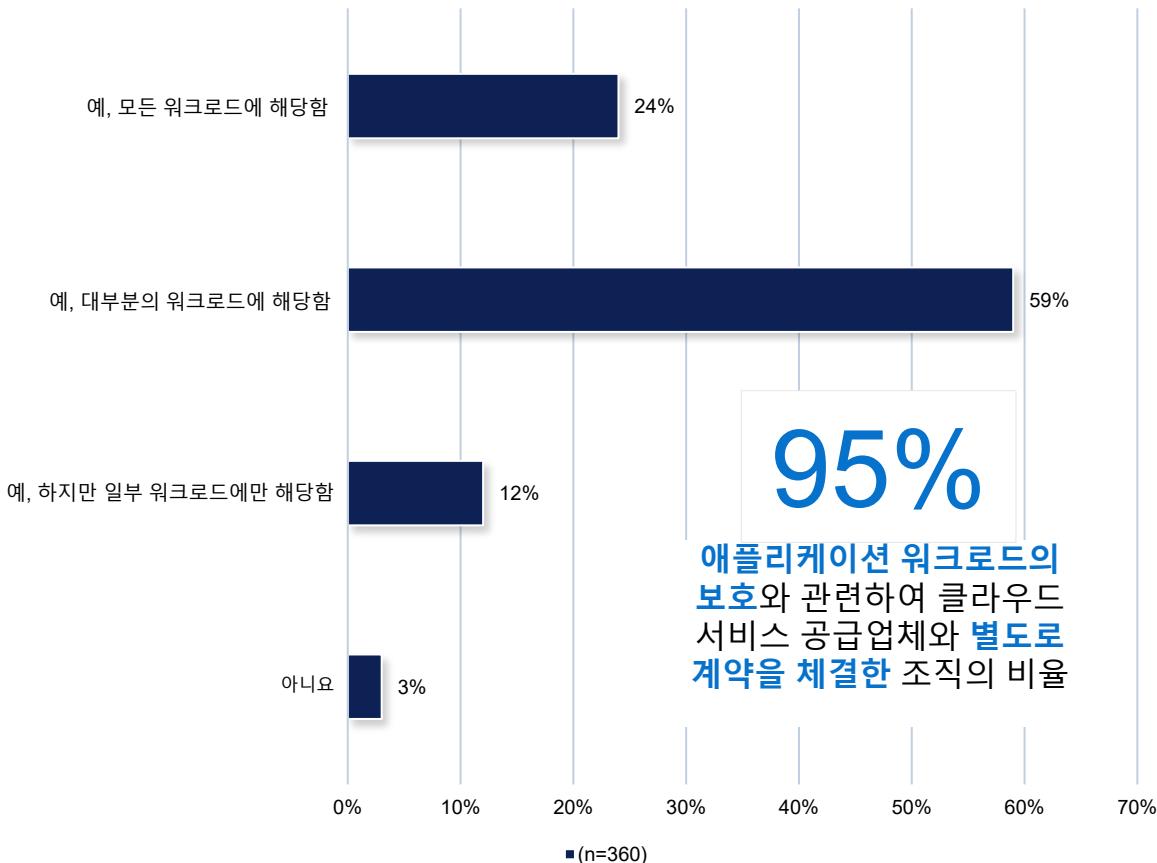
많은 조직이 현재 워크로드를 보호하기 위해 다양한 백업 툴과 솔루션을 사용하고 있지만 업그레이드의 필요성이 대두되고 있습니다

클라우드 보호 툴 및 솔루션(연도별로 구분)



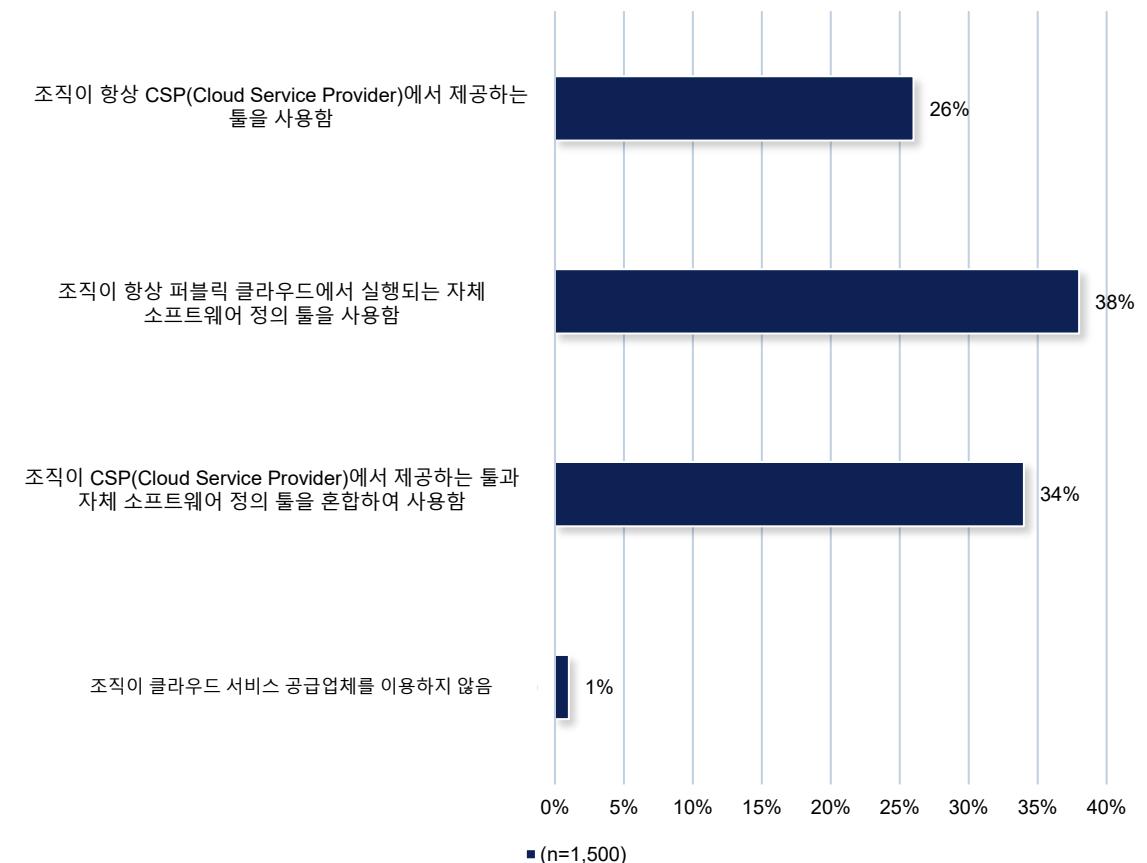
많은 조직이 클라우드 환경 전반에서 워크로드를 보호하기 위해 클라우드 서비스 공급업체에 점점 더 의존하고 있습니다

애플리케이션 워크로드 보호를 위해 CSP와 별도로 계약



필터: 데이터 분할: 지역 = 합계

클라우드 서비스 공급업체가 제공하는 백업 및 복구 툴



필터: 데이터 분할: 지역 = 합계

주요 연구 결과 – 요약

데이터 보호의 위험 환경

- 데이터 보호 조치에 대한 우려가 널리 확산되고 있으며, 확신이 부족한 상태에서 많은 조직이 취약한 상황에 놓여 있습니다.
- 거의 모든 조직이 데이터 보호와 관련하여 어려움을 겪고 있으며, 지난 12개월 동안 많은 조직이 데이터 손실 및/또는 예기치 못한 시스템 다운타임으로 인해 상당한 운영 중단 사태를 경험했습니다.
- 외부 보안 위협은 지난 12개월 동안 데이터 손실 및/또는 예기치 못한 시스템 다운타임의 가장 일반적인 원인이었습니다.
- 데이터 보호 관련 당면 과제와 우려에도 불구하고 제로 트러스트 보안을 완전히 구현한 조직은 거의 없습니다.

증가하는 사이버 공격 위협

- 지난 12개월 동안 사이버 공격이나 인시던트를 경험한 조직이 증가하여 비즈니스에 평균 192만 달러의 비용이 발생했습니다.
- 많은 조직이 백업 데이터가 랜섬웨어 공격으로 인해 손상될 수 있다고 우려합니다.
- 랜섬웨어 공격의 결과를 둘러싼 잘못된 자신감으로 인해 위험이 가중되고 있습니다.
- 랜섬웨어 보험은 보편화되어 있지만 제한 사항을 다수 포함합니다. 이에 따라 조직은 재정적 취약성을 안고 있습니다.

멀티클라우드 사용

- 퍼블릭 클라우드는 기존 애플리케이션을 업데이트하고 새로운 애플리케이션을 배포할 때 여전히 인기 있는 옵션이지만 데이터 보안에 대한 우려가 존재합니다.
- 보안 문제로 인해 많은 조직이 퍼블릭 클라우드에서 온프레미스로 워크로드의 일부를 마이그레이션하고 있거나 마이그레이션을 고려하고 있습니다.
- 사이버 관련 인시던트 증가와 데이터 보호 전략에 대한 신뢰가 낮은 상황에서 하이브리드 멀티클라우드 운영을 활성화할 때 보안이 가장 중요한 기능으로 인식되는 경우가 많습니다.

클라우드 환경 보호

- 많은 조직이 현재 워크로드를 보호하기 위해 다양한 백업 툴과 솔루션을 사용하고 있지만 업그레이드의 필요성을 인정하고 있습니다.
- 많은 조직이 클라우드 환경 전반에서 워크로드를 보호하기 위해 클라우드 서비스 공급업체에 점점 더 의존하고 있습니다.

