# 보호, 보안 및 AI 융합되어야 하는 이유

COHESITY

# 보호, 보안 및 AI가 융합되어야 하는 이유

수년 동안 조직은 데이터 보호, 데이터 보안 및 AI 이니셔티브를 별도의 우선순위로 취급해 왔습니다. 백업 팀은 복구에 집중했습니다. 보안 팀은 위협 예방에 집중했습니다. AI 팀은 분석, 자동화 및 혁신에 집중했습니다. 각 팀은 자체 도구, 목표 및 아키텍처로 운영되었습니다.

**이제 이 파편화된 모델을 다시 구상해 볼 시간입니다.**

그 이유는 현실적입니다. 사이버 공격은 점점 더 표적화되고 있으며, 이제 온프레미스, 클라우드, SaaS 등 모든 곳에 데이터가 존재합니다. 동시에, 기업은 AI 결과를 개선하기 위해 데이터에 액세스하는 데 어려움을 겪고 있습니다. 이러한 데이터는 종종 서로 다른 시스템에 분산되어 복잡성과 사각지대가 늘어나게 합니다.

더 많은 도구를 추가해도 그 문제는 해결되지 않습니다. 오히려 더 악화됩니다.

앞서 나가는 조직은 더 많은 계층을 추가하지 않습니다.

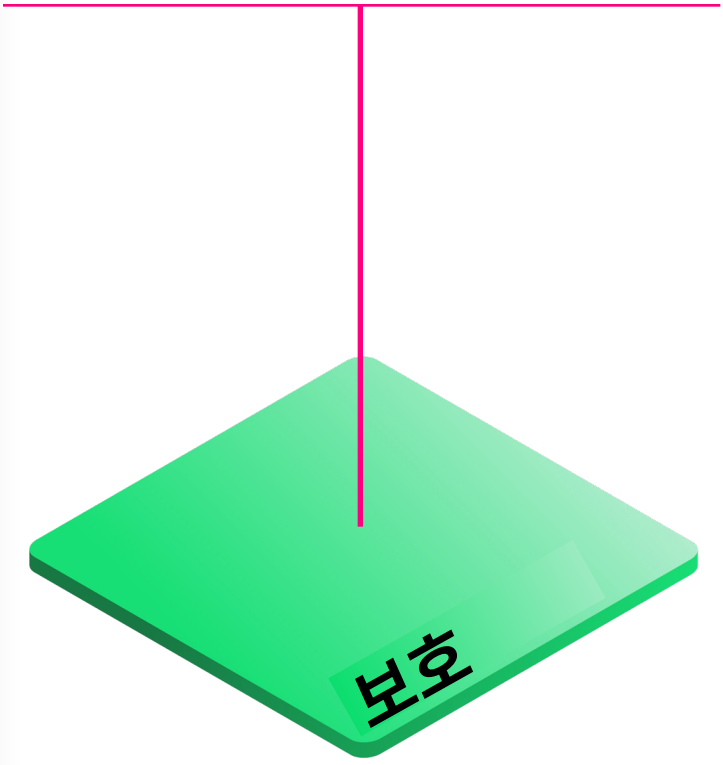
**사람들은 기반에 대해 다시 생각하고 있습니다.**

# 보호는 기반입니다

보호는 사이버 레질리언스를 향한 첫 번째 단계입니다. 이는 가상 머신, 데이터베이스, 파일 시스템 및 비정형 워크로드를 아우르는 전체 데이터 자산에 대한 포괄적인 적용 범위로 시작됩니다.

보호는 이러한 모든 데이터를 일관성 있게 그리고 격차 없이 다루어야 합니다. 복구가 이에 달려 있습니다. 보호가 불완전하거나, 파편화되거나, 일관성이 없는 경우, 안전하고 신속한 복구를 기대할 수 없습니다. 보호가 포괄적이고 일관적인 경우, 손상, 손실 또는 잔여 위험 없이도 복구가 가능합니다.

## 사이버 레질리언스는 이러한 기반 수준의 보호에서 시작됩니다.



# 보안은

# 데이터 계층에 통합되어야 합니다

보호가 확립되면 그 다음 과제가 명확해집니다.

백업 시스템이 손상되거나 암호화되거나 부적절하게 액세스될 수 있는 경우 복구 데이터 자체가 또 다른 공격 표면이 됩니다. 보안은 외부 오버레이로 남아 있으면 안 됩니다. 데이터 계층에서 직접 작동해야 합니다.

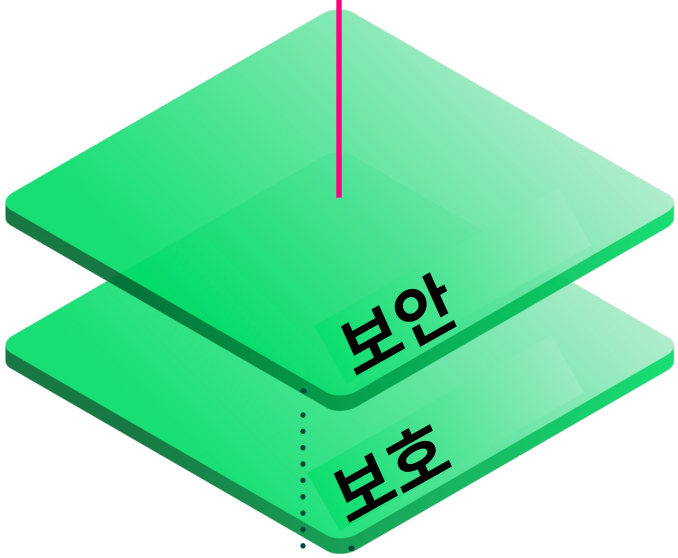
그 의미는 다음과 같습니다.

- 백업 환경 내에서 비정상적인 활동 감지
- 소스에서 ID 및 액세스 제어 적용
- 데이터 자산 전반에 걸쳐 일관되게 거버넌스 적용

보호와 보안이 별도의 시스템에서 작동하는 경우, 팀은 종종 압박이 심한 상황에서 도구 전반에 걸쳐 신호와 정책을 조정해야 합니다. 격차는 기능이 존재하지 않기 때문이 아니라 이러한 기능이 통합되지 않았기 때문에 나타납니다.

데이터 보호 계층에 보안을 포함하면 이러한 격차가 좁아져 보안과 복구가 서로 강화됩니다. 위협 탐지는 깨끗한 복구를 지원하며 거버넌스는 한 번 적용되어 어디서나 시행됩니다.

이것들은 함께 신뢰할 수 있는 데이터 기반을 구축합니다.




**보호**
는 레질리언스를 확립합니다.

**보안**은 이를 강화합니다.

# 엔터프라이즈 규모에서 AI를 실용적으로 구현

데이터를 안정적으로 보호하고 보안을 확보한 후에야 새로운 기회가 완전히 모습을 드러냅니다.

AI가 영향력을 발휘하게 하려면 조직은 다음을 수행해야 합니다,

- 환경 전반의 비정형 데이터를 통합
- 과거 변경 사항 캡처
- 일관된 거버넌스, 역할 기반 액세스 및 감사 가능성 유지
- 중복 및 의도하지 않은 노출 위험 감소

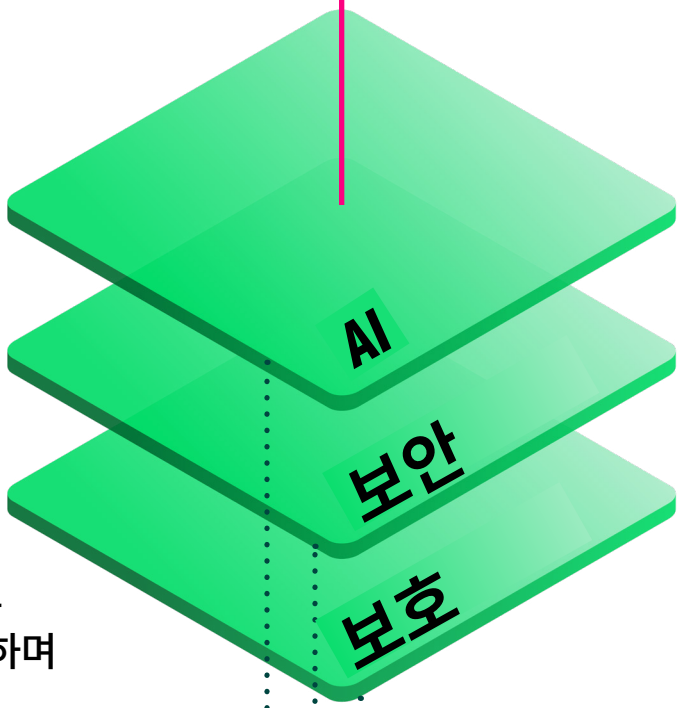
많은 팀이 데이터를 별도의 분석 또는 AI 플랫폼으로 복사하여 이를 해결하려고 합니다. 그 결과 비용이 증가하고 복잡성이 커지며 공격 표면이 확대됩니다.

**통합된 기반이 판도를 바꿉니다. 이를 통해 조직은 AI 지원 데이터에 액세스하여 이를 안전하고 정확하며 완전하게 사용할 수 있습니다.**

보호 및 보안이 이미 통합되어 있으면 거버넌스 모델을 훼손하거나 데이터 및 인프라를 복제하지 않고도 똑같이 신뢰할 수 있는 데이터 자산을 검색 가능하고 사용 가능하도록 만들 수 있습니다. 연속성을 보호하는 데이터는 인사이트를 이끌어내는 AI 지원 데이터가 됩니다.

이 모델에서 AI는 두 가지 역할을 합니다. 자동화와 더 스마트한 탐지를 통해 기본 플랫폼을 강화합니다. 또한 관리되는 엔터프라이즈 데이터를 소스로 사용하여 생산성 어시스턴트부터 전문 에이전트에 이르는 하위 애플리케이션을 지원합니다.

**각 계층은 그 앞에 있는 계층을 기반으로 만들어집니다.**




**보호**는 데이터를 복구 가능하게 만듭니다.

**보안**은 신뢰할 수 있게 만듭니다.

**AI**는 가치 있게 만듭니다.

# 통합이 합리적인 방안

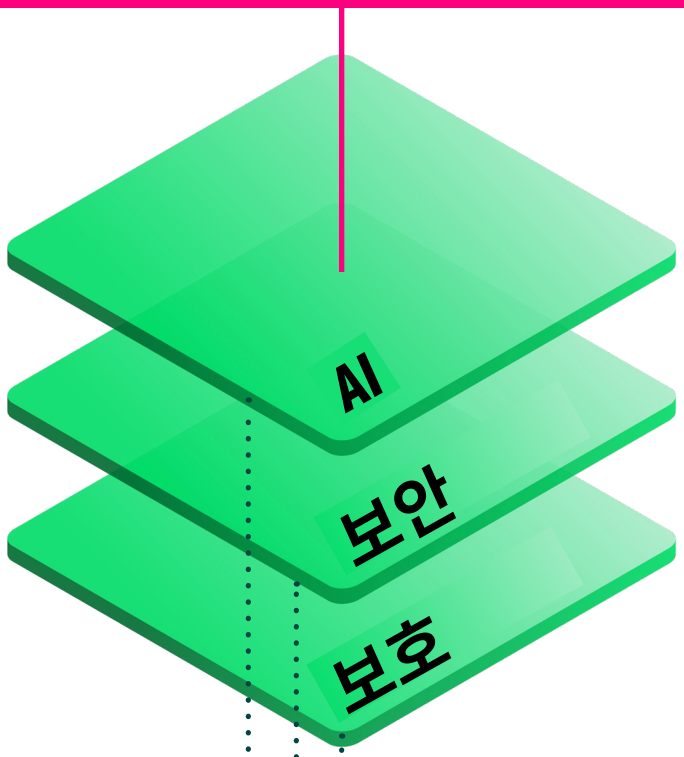
보호, 보안 및 AI 준비성이 단일 기반으로 통합되면 데이터는 다음과 같게 됩니다.

- 한 번의 거버넌스로 여러 번 사용됨
- 어디에 있든 보호됨
- 소스에서 보안 유지됨
- 중복 없이 AI 지원 가능.

어느새, 가장 안전한 데이터 사본이 가장 스마트한 데이터 사본이 되었습니다.

사이버 리스크와 AI 채택 가속화로 정의되는 세상에서 아키텍처 선택의 기준은 분명합니다. 하나의 데이터 자산은 단일하고 확장 가능한 시스템으로 관리되며, 중단을 견디는 동시에 인사이트를 생성하도록 구축되었습니다.

## 그것이 COHESITY DATA CLOUD입니다.




**보호**는 복구 가능성을 보장합니다.

**보안**은 노출을 줄입니다.

**AI**는 가치를 추출합니다.

## 엔터프라이즈 규모에서 입증됨

**Cohesity Data Cloud**는 사이버 레질리언스를 강화하고 데이터에서 더 많은 가치를 추출하기 위해 구축된 유일한 통합 플랫폼입니다.

온프레미스, 클라우드 및 SaaS 전반에서 **1,000개 이상의** 워크로드를 보호하며,

최대 **18배** 더 빠른 백업,

**97%** 더 빠른 복원과 즉각적인 AI 가치 실현 시간,

**50%** 적은 스토리지와

전체 비용에서 **최대 40%** 절감 효과를 제공합니다.

자세한 내용은 cohesity.com/DataCloud



COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6300010-001-IT 03-2026