Microsoft 365

AI 준비 역량 구축을 위한 경영진 플레이북

CIO와 CISO가 AI 비전에서 조직의 준비 역량으로 나아갈 수 있도록 돕는 공동 운영 모델입니다.





03
이 플레이북 활용 방법

04
AI에 대한 야망이 조직의 준비 역량을 앞서가고 있을 수 있습니다.

05
준비 역량 격차: AI 도입을 늦추고 있을 수 있는 요인을 평가합니다.

06
AI에 준비된 안전한 기반 프레임워크

09
AI 준비 역량을 구축하는 데 도움이 되는 세 가지 전환

10
역할별 다음 단계.

11
AI 준비 역량 구축을 시작합니다.

이 플레이북 활용 방법

이 플레이북은 CIO와 CISO가 공유하는 기반을 구축하기 위한 프레임워크를 제공하며, 이는 조직이 AI 준비 역량을 갖추고 비즈니스 혁신을 강화하는 데 도움이 됩니다. 이 프레임워크는 귀하의 조직 내에 격차가 존재할 수 있는 영역을 파악한 다음 이러한 격차를 어떻게 해결할지 결정하는 데 도움이 되도록 고안되었습니다. 이 프레임워크는 다음과 같이 한 가지 핵심 아이디어를 중심으로 구성되어 있습니다. 바로 프론티어 혁신은 생산성, 보안, 데이터, 관리가 하나로 결합되는 안전한 기반을 통해 시작된다는 아이디어죠. 이 플레이북의 정보를 사용하여 다음을 살펴보세요.

1. **정렬.** 준비 역량 격차로 인해 AI의 가치 창출이 지연되는 부분을 논의하고 합의합니다.
2. **평가.** AI 준비가 된 보안 기반 프레임워크의 5단계를 활용하여 조직 내에서 가장 영향이 크고 위험이 가장 높은 영역을 파악하는 것부터 시작하세요.
3. **조치.** 어디서 시작할지, 시간이 지남에 따라 어떻게 확장할지 등 함께 계획을 세우세요.

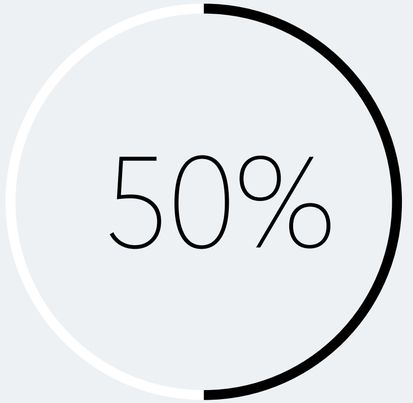


AI에 대한 야망이 조직의 준비 역량을 앞서가고 있을 수 있습니다.

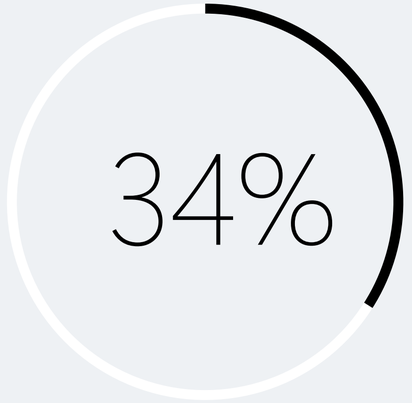
AI는 만연해 있습니다. Deloitte의 2026년 State of AI in the Enterprise 보고서에 따르면, 설문 조사 응답자들은 조직에서 직원들의 AI 접근성을 **50%로** 단 1년 만에[1] 확대했다고 보고했으며, **34%**는 자사의 제품, 프로세스, 비즈니스 모델을 AI를 활용하여 근본적으로 혁신하기 시작했다고 보고했습니다[1]. 직원들이 이미 AI를 활용한 업무 방식의 재구성을 시작하면서 포부가 커지고 있습니다. 이들은 실험하고, 새로운 워크플로를 만들어 내며, 조직이 예상한 것보다 더 빠르게 움직이고 있을 수도 있습니다. 이와 동시에, 직원들을 둘러싼 시스템, 정책, 운영 모델은 여전히 기존의 업무 방식을 강화하는 경향이 있습니다.

Microsoft의 2026년 업무 동향 지수에서는 이를 '전환의 역설'이라고 합니다.[2] 직원들은 업무 방식을 재창조할 준비가 되어 실제로 바꾸기 시작했지만, 이들을 둘러싼 조직 시스템인 지표, 인센티브, 규범은 여전히 이전의 업무 방식을 강화하고 있습니다. AI 채택을 가속화하는 바로 그 요인들이 동시에 AI 채택을 가로막고 있을 수도 있습니다. 이 격차는 단순히 기술 도입에 대한 것이 아닙니다. 매우 특정한 영역에서 조직의 대규모 AI 준비 태세에 따라 이 격차가 더욱 심화될 수 있습니다. 도구, 데이터, ID, 엔드포인트 및 제어, 즉 기본 토대 전반에 걸쳐 확장합니다.

조직이 연결되고 안전한 기반을 바탕으로 운영될 때 AI를 확장할 수 있다는 확신을 갖게 됩니다. 이처럼 강력한 AI 기반은 인프라를 넘어서는 하나의 운영 모델입니다. 사람, 콘텐츠, 커뮤니케이션, 워크플로, ID 및 디바이스를 통합형 플랫폼에서 연결함으로써, 조직은 업무 흐름 속에 보안, 규정 준수, 관리까지 내장할 수 있습니다. 이를 통해 워크플로를 혁신하고 비즈니스 영향력을 창출할 수 있도록 신뢰와 통제 기반을 구축할 수 있습니다. 기회는 단순히 AI의 속도를 따라가는 것을 넘어, 업무 수행 방식을 새롭게 재구상하는 것으로 확대되고 있습니다. 중요한 것은 조직이 AI 환경을 얼마나 빨리 도입하고 확장하느냐가 아니라, 어떻게 안전하게 혁신을 가능하게 하느냐입니다.



설문 조사에 참여한 비즈니스 리더들이 1년 안에 더 많은 근로자가 AI에 접근할 수 있게 될 것이라고 보고한 비율.[1]



설문 조사에 참여한 리더들이 제품, 프로세스 및 비즈니스 모델을 변환하는 데 AI를 활용한다고 보고한 비율.[1]

준비 역량 격차: AI 도입을 늦추고 있을 수 있는 요인을 평가합니다.

직원들은 AI를 활용해 새로운 방식으로 일하고 있으며, 팀들은 새로운 활용 사례를 발굴하고, 초기 파일럿 프로젝트는 잠재적인 생산성 향상 가능성을 입증하고 있습니다. 비즈니스 전반에서 리더들은 더 넓고 대규모의 변혁 가능성을 인식하고 있습니다. 문제는 AI에 대한 열정의 부족이 아닙니다. 문제는 직원들의 업무 방식이 변화한 속도에 맞춰 운영 기반이 항상 함께 발전하지는 않았다는 데 있습니다.

2026년 업무 동향 지수 보고서에 따르면, 조사 대상 AI 사용자 중 **60% 이상이**[2] AI 덕분에 고부가가치 업무에 더 많은 시간을 할애할 수 있게 되었다고 답했으며, **50% 이상은** 1년 전에는 할 수 없었던 업무를 지금은 수행하고 있다고 답했습니다[2].하지만 이와 동시에, AI 사용자 중 **4명 중 한** 명은[2] 자신의 조직 리더십이 AI에 대한 접근 방식에서 일관되게 뜻을 같이하고 있다고 느낀다고 말했습니다.

직원들이 AI 기반 업무 방식을 채택함에 따라, 레거시 프로세스, 분산된 도구, 일관되지 않은 제어, 관리되지 않는 데이터는 진행 속도를 늦출 수 있습니다. AI 도입을 가속하는 동력 자체가 이전 시대에 구축된 시스템의 취약성을 드러낼 수 있습니다. 이것이 바로 준비 역량 격차입니다.

그리고 기반과 관련된 과제로 작용하는 경우가 많습니다. 이러한 기반 관련 과제에 기여할 수 있는 영역은 두 가지입니다. 바로 단절된 경험과 보안 우려죠.

- **설문 조사에 응한 최고 경영진 중 2/3은** 자사 조직이 지나치게 복잡하고 비효율적이라고 말합니다.[3]
- **설문 조사에 참여한 CIO와 CTO 중 90% 이상이** 생성형 AI로 인해 이미 사이버 보안 투자가 늘었거나 앞으로 늘어날 것이라고 말했습니다.[4]

준비 역량 격차가 발생할 수 있는 영역을 파악하기 위해 몇 가지 예시 시나리오를 살펴보겠습니다. 이러한 격차는 직원 환경과 보안 전반에 걸쳐 나타날 수 있습니다. 첫 번째 시나리오는 직원 경험 측면에 대한 시나리오입니다. CIO는 직원들이 정보를 찾거나 업무를 수행하는 데 필요한 모든 앱과 도구에 액세스하는 데 걸리는 시간과 관련된 직원 불만이 더 자주 보고되는 것을 인식하기 시작할 수 있습니다. 이러한 문제는 앱, 워크플로, 디바이스, 데이터 전반에 걸친 단절된 환경에서 비롯된 준비 역량 격차로, AI를 확대 적용할수록 더 큰 문제로 번질 수 있음을 나타낼 수 있습니다.

두 번째 시나리오는 보안 측면입니다. 더 많은 사람이 일상적인 워크플로에서 AI를 실험하고 사용하기 시작함에 따라, CISO는 잠재적으로 과도한 정보를 공유하거나 승인되지 않음 AI 도구의 사용이 증가하는 등 이에 관련된 증가하는 인시던트를 발견할 수 있습니다. 이러한 문제는 데이터 거버넌스 및 액세스 관리와 관련된 준비 역량 격차를 강조할 수 있습니다.

이러한 격차가 함께 작용하면 마찰이 발생하여 엔터프라이즈급 AI 도입 규모 확산이 더 어려워질 수 있습니다. 별개의 생산성, 보안, IT 과제로 시작된 문제가 공유 기반 과제로 발전할 수 있습니다. AI 도입이 증가함에 따라 이러한 준비 역량 격차는 더욱 뚜렷해지고, 그 영향도 더욱 커질 수 있습니다.

이러한 예시는 준비 역량 격차가 어떻게 발생할 수 있는지를 보여주는 가상의 사례이지만, 이는 기회 비용이 단순히 AI 도입에서 뒤처지는 것만을 의미하지는 않는다는 점을 보여줍니다. 이는 직원들이 AI를 통해 달성할 수 있는 것과 조직이 이를 확장할 준비가 되어 있는 수준 사이의 격차를 점점 더 벌어지게 만들고 있습니다. 직원들은 업무를 새롭게 혁신할 준비가 되어 있을 수 있습니다. 문제는 이러한 변화를 규모 있게 강화할 수 있을 만큼 귀사의 기반이 준비되어 있는지에 있습니다.

따라서 AI를 확장한다는 것은 비즈니스, IT, 보안이 공유된 운영 모델을 중심으로 조율되는 것을 의미합니다. AI에서 잠재력을 보고 있는 조직은 단순히 더 많은 AI를 배포하는 것에 그치지 않습니다. 기반을 강화하여 생산성, 보안, 관리 기능이 대규모로 함께 작동하도록 하고 있습니다.

준비 역량 확인

AI를 더 확장하기 전에먼저 두 가지 질문부터 해보세요.

- 조직 내에서 AI 도입이 AI 사용 및 접근과 관련된 정책보다 더 빠르게 진행되는 곳은 어디라고 생각하나요?
- AI는 보안이 유지된 상태에서 충분한 조직 맥락에 액세스하여 업무 수행 방식을 실질적으로 개선할 수 있나요?

CIO는 다음과 같은 질문을 해보세요.

- 운영상 AI를 전사적으로 확장할 수 있는 기반이 마련되어 있나요?

CISO는 다음과 같은 질문을 해보세요.

- AI를 자신 있게 확장할 수 있는 제어 기반을 갖추고 있나요?

AI에 준비된 안전한 기반 프레임워크

안전하고 AI에 대비된 기반을 구축하려면 무엇이 필요할까요? 하나의 프레임워크 접근 방식을 체계적으로 정리하는 데 도움이 됩니다. 5단계를 통해 기반을 구축하기 시작할 수 있도록 설계되어 상호 유기적으로 작동합니다.

각 영역에서 업무 연결, 데이터 준비, 액세스 보호, 대규모 관리, 보호 및 응답 등 이 다섯 단계는 조직이 우선적으로 시작할 영역을 식별한 다음, 구축, 통합, 변환, 확장해 나갈 수 있도록 지원합니다.



1.

업무 연결

사람, 콘텐츠, 대화 및 비즈니스 프로세스를 포괄하는 연결된 업무 그래프를 구축하여, AI가 조직의 실제 업무 진행 방식을 기반으로 조직의 컨텍스트를 파악할 수 있도록 합니다. 도구들이 연결되어 있으면, 직원들은 개별적인 AI 활용 사례에서 벗어나 미팅, 문서, 비즈니스 앱 및 협업 도구 전반에 걸친 AI 지원 워크플로로 전환할 수 있습니다.

시작점
가장 가치가 높은 생산성 도구, 협업 시스템 및 데이터를 파악하여 직원들이 가장 자주 사용하는 것부터 우선적으로 연결합니다.

잠재적 영향
직원들은 정보를 검색하고[1], 애플리케이션 간 전환하며, 상황을 다시 파악하는 데 소요하는 시간이 줄어들고AI는 조직의 실제 업무 방식에 기반한 인사이트, 권장 사항, 실행 방안을 제공하게 됩니다.

준비 역량 확인

CIO는 다음과 같은 질문을 해보세요.
- AI가 인물, 콘텐츠, 대화, 업무 흐름에 직원들이 더 효과적으로 업무를 수행하는 데 필요로 하는 액세스할 수 있나요?

CISO는 다음과 같은 질문을 해보세요.
- AI가 새로운 가시성, 거버넌스 또는 보안 취약점을 만들지 않고 조직의 맥락에 액세스할 수 있나요?

2.

데이터 준비

가치가 높은 데이터를 검색, 분류, 레이블 지정, 보호 및 관리하여 AI가 상황을 인지한 상태로 작동하도록 하고, 민감도가 생성되는 콘텐츠에도 반영되어 보안, 규정 준수 및 비즈니스 정책을 준수하도록 합니다. 데이터가 관리되고, 검색 가능하며, 연결되어 있을 때 AI는 불완전하거나 오래된 정보가 아닌 조직의 지식에 근거하여 응답을 제공합니다.

시작점
완전한 레이블 지정 전략을 기다리지 않습니다. 먼저 DLP(데이터 손실 방지) 정책을 통해 재무, 고객 및 지적 재산과 같은 가장 민감한 정보의 노출을 방지하는 데 집중합니다. 그와 동시에, 가장 큰 비즈니스 가치와 위험을 초래하는 최상위 수준의 민감 데이터를 식별하고 자동으로 레이블을 지정합니다. 그다음에는 조직 전체에서 더 광범위한 데이터 분류 및 거버넌스 프로그램을 구축하도록 확대합니다.

잠재적 영향
직원과 에이전트는 신뢰할 수 있는 민감한 정보를 다루는 동시에, 리더는 데이터가 AI 기반 워크플로에서 사용되고 보호되는 방식에 대해 가시성과 제어력을 유지하고 이에 대한 확신을 가질 수 있습니다. 이러한 지속적인 정책은 조직 내에서 민감한 데이터가 이동하고 저장, 공유 또는 액세스될 때에도 해당 데이터에 부착되어 있습니다.

준비 역량 확인

CIO는 다음과 같은 질문을 해보세요.
- AI 도구와 에이전트가 가장 가치 있는 데이터를 발견되고, 거버넌스가 적용되어, 활용할 수 있나요?

CISO는 다음과 같은 질문을 해보세요.
- AI가 민감한 정보를 다른 정보와 구분하고 적절한 보호 조치를 적용할 수 있나요?

3.

액세스 보호

사용자, 디바이스 및 액세스 요청을 검증하고 사람들이나 AI가 조직 정보에 대해 조치를 취하는 것뿐 아니라 안전하게 검색할 수 있도록 하면서도 위험을 확대하지 않도록 돕는 신뢰 레이어를 구축하세요. ID, 액세스, 권한이 정렬되면 직원과 AI 에이전트는 업무 수행에 필요한 정보에 안전하게 액세스할 수 있으므로, 조직은 팀, 역할, 비즈니스 프로세스 전반에 걸쳐 AI 도입을 확대할 수 있습니다.

시작점
MFA(다중 인증) 및 조건부 액세스 정책을 모든 사용자에게 적용합니다. 이러한 제어는 보호를 제공하는 동시에 승인된 AI 도구에 안전하게 접근할 수 있는 기반을 마련하는 데 도움이 됩니다.

잠재적 영향
직원과 에이전트는 정보와 AI 기반 환경을 안전하게 확보하고 보안 팀은 ID, 디바이스 및 에이전트 전반에 걸쳐 민감한 데이터와 시스템에 대한 접근을 지속적으로 관리할 수 있습니다.

준비 역량 확인

CIO는 다음과 같은 질문을 해보세요.
- 직원들이 불필요한 마찰 없이 필요한 정보와 AI 도구에 안전하게 액세스할 수 있나요?

CISO는 다음과 같은 질문을 해보세요.
- 각 사용자, 디바이스, AI 에이전트가 신뢰할 수 있는지 액세스 권한을 부여하기 전에 검증할 수 있나요?

참고: 이와 같은 다섯 단계는 상호 연계된 역량으로 구성되어 있어, 조직에 맞는 최적의 구현 순서를 자유롭게 선택할 수 있습니다.

4.

대규모 관리

사용자, 디바이스, 앱 및 Cloud PC를 건강하고 규정 준수 상태로 관리하며, 이 관리 범위를 현장 직원, 계약직, 에이전트, 개인 디바이스까지 확장합니다. 예를 들어, 계절성 인력을 보유한 조직은 조직 정책, 애플리케이션, 보호 기능이 이미 내장된 안전한 Cloud PC를 제공함으로써, 이 팀을 직원들이 사용하는 동일한 규정 준수 환경에 신속하게 온보딩할 수 있습니다. 이렇게 하면 각 인력별로 물리적 디바이스를 배송, 관리, 회수할 필요가 없습니다. 엔드포인트가 관리되고 보호되면, 디바이스, 위치 및 업무 방식과 상관없이 전사에 걸쳐 AI를 일관되고 안전하게 배포할 수 있습니다.

시작점
광범위한 관리 기능을 확장하기 전에, 먼저 디바이스 규정 준수 및 애플리케이션 보호 정책을 통해 미관리 디바이스와 개인용 디바이스를 정책 관리 범위에 포함하는 데 집중합니다. 엔드포인트를 공통 관리 프레임워크로 통합하면 즉각적인 보안 및 운영상의 이점을 제공하는 동시에 보다 광범위한 AI 도입을 위한 기반을 마련할 수 있습니다.

잠재적 영향
직원들은 기업용, 현장용, 개인용 디바이스 전반에서 간소화된 환경을 확보합니다. IT 부서는 AI를 안전하게 확장하는 데 필요한 가시성, 제어, 일관성도 확보합니다.

준비 역량 확인

CIO는 다음과 같은 질문을 해보세요.
- 조직 전반에 걸쳐 사용자, 디바이스, 앱을 및 AI 기반 엔드포인트를 일관되게 관리하고 거버넌스를 적용할 수 있을까요?

CISO는 다음과 같은 질문을 해보세요.
- 직원, 계약직, 현장 근로자 및 AI 에이전트 전반에 걸쳐 보안 및 규정 준수 통제가 일관되게 확장될 수 있을까요?

5.

보호 및 대응

조직 전체의 신호를 상관 분석하여 ID, 디바이스, 데이터 및 AI 기반 워크플로 전반의 위협을 탐지하고 조사하며 대응하여 AI 도입이 확대되는 가운데 조직의 회복탄력성을 유지하도록 지원합니다. 보호 제어가 기반에 내장되어 있으면, 조직은 더 많은 사용자, 더 많은 데이터, 더 다양한 비즈니스 시나리오로 AI를 자신 있게 확장할 수 있습니다.

시작점
ID, 엔드포인트, 데이터, 클라우드 리소스 및 애플리케이션 전반에 걸친 전체 노출 위험을 파악하는 것부터 시작합니다. 사고가 발생할 때까지 기다리기보다는, 어떤 영역에서 위험이 가장 높은지와 이러한 위험을 줄이는 데 큰 영향을 미칠 수 있는 조치가 무엇인지 이해해야 합니다. 그 다음에는 AI를 방어 전략에 도입하여 보안 팀이 신호를 연계하고, 대응을 우선순위로 정하며, 위협을 더 신속하게 조사할 수 있도록 지원합니다.

잠재적 영향
직원들은 더 적은 방해를 받으면서 AI를 안전하게 활용해 생산성을 높일 수 있고, 보안 팀은 가시성을 확보하여 위협을 더 빠르게 탐지하고 대응할 수 있습니다.

준비 역량 확인

CIO는 다음과 같은 질문을 해보세요.
- 보안 운영은 AI가 비즈니스에 가져오는 속도와 규모에 발맞출 수 있을까요?

CISO는 다음과 같은 질문을 해보세요.
- 데이터, 운영 및 AI 기반 워크플로에 영향을 미치기 전에 위협을 신속하게 탐지, 조사, 차단할 수 있나요?

참고: 이와 같은 다섯 단계는 상호 연계된 역량으로 구성되어 있어, 조직에 맞는 최적의 구현 순서를 자유롭게 선택할 수 있습니다.

> Microsoft 365로 표준화함으로써 Copilot이 최상의 성능을 발휘할 수 있는 환경을 구축했습니다. 아마 이와 같은 이유로 Copilot의 일일 활성 사용률이 90~95%에 이르는 것일 겁니다.

Elaine Smith

Copilot 프로그램 책임자
PepsiCo

사례 전문 읽어보기: PepsiCo 고객 사례 연구

AI 준비 역량을 구축하는 데 도움이 되는 세 가지 전환.

보안 기반의 각 단계는 운영 환경의 특정 요소를 강화하도록 설계되었으며, 업무를 연결하고, 준비된 데이터를 활용하며, 안전한 액세스를 제공하고, 대규모로 관리하고, 보호와 대응을 수행하도록 합니다.

이러한 단계들을 종합적으로 실행하면 더 광범위한 AI 혁신을 추진할 수 있는 엔터프라이즈급 동력을 강화하고 조직이 준비 역량을 갖출 수 있도록 지원합니다 . 그 결과, 단순히 탄탄한 기반에 그치는 것이 아니라, 조직의 관행을 맥락, 통제, 신뢰를 바탕으로 발전시킬 수 있는 실질적인 변화들을 만들 수 있습니다.

전환 1. 분산된 도구와 정보에서 연결된 업무 인텔리전스로.

AI는 실제로 사람들이 업무를 수행하는 방식(사람, 콘텐츠, 대화, 미팅, 애플리케이션 및 워크플로)을 참조할 수 있을 때 더욱 유용해집니다. 정보가 단절된 도구에 갇혀 있을 때, AI는 부분적인 답변만 제공할 수 있고, 직원들은 여전히 정보를 검색하고, 여러 맥락을 오가며, 배경 정보를 다시 구축하는 데 시간을 허비하게 됩니다. 연결된 업무 기반은 AI가 적절한 인사이트를 도출하고, 진행 중인 업무를 요약하며, 다음 단계의 제안을 하고 및 업무 흐름 전반에서 실행을 지원할 수 있도록 조직의 맥락을 제공합니다. 이와 동일하게 중요한 것은, 업무 환경 자체가 물리적 디바이스, 클라우드 환경, 위치, 팀 등 업무가 이루어지는 모든 곳에서 맥락, 접근성 또는 연속성을 잃지 않고 직원들을 따라야 한다는 점입니다. 정직원이든, 계약직이든, 프로젝트 기반 기여자이든 관계없이, 생산적인 업무를 지원하는 동일한 애플리케이션, 정보, 정책 및 AI 환경에 계속 연결된 상태를 유지할 수 있습니다. 이러한 전환은 조직이 단절된 경험에서 AI 준비가 된 업무 환경으로 나아갈 수 있도록 지원하며, AI가 개별 생산성 향상을 넘어 팀과 비즈니스 프로세스 전반에 걸친 폭넓은 변화를 촉진할 수 있도록 돕습니다.

전환 2. 과도한 공유 및 접근 위험에서 보호된 데이터와 제어로의 전환.

AI 사용이 확대됨에 따라 조직은 민감한 데이터가 검색 가능하고 적절히 관리되며, 적합한 사람, 디바이스 및 에이전트에게만 제공된다는 확신이 필요합니다. 이러한 기반이 없으면 AI는 이미 존재하는 과도한 정보 공유, 액세스, 규정 준수 공백을 더욱 확대할 수 있습니다. 이러한 전환은 보호를 운영 모델의 일부로 만드는 데 있습니다. 가치가 높은 데이터를 분류하고 레이블을 지정하며, DLP 및 액세스 정책을 적용하고, ID와 디바이스 상태를 검증하고, 데이터가 저장, 공유, 액세스, AI 기반 워크플로에서 사용될 때까지 정책이 데이터를 따라가도록 합니다. 그 결과 직원과 에이전트가 관련 비즈니스 컨텍스트를 활용하는 동시에 리더는 가시성과 거버넌스, 제어를 유지할 수 있는 더 신뢰할 수 있는 환경을 조성할 수 있습니다.

전환 3. 파편화된 신호에서 확장 가능한 통합형 방어 체계로.

AI를 확장하면 작업의 속도, 규모, 복잡성이 증가하며, 그로 인해 보안 팀이 이해하고 조치해야 하는 신호의 수도 함께 늘어날 수 있습니다. 더욱 강력한 기반을 통해 팀은 ID, 엔드포인트, 데이터, 앱 및 위협 신호를 상호 연관시켜 위험에 대한 보다 완전한 관점을 확보할 수 있습니다. 이는 또한 AI를 방어 전략에 통합함으로써 조사, 대응, 우선순위 지정을 지원하고, 사용자, 디바이스, Cloud PC, 에이전트, AI 지원 워크플로 전반에 걸쳐 일관된 통제를 유지하는 데 도움을 줍니다. 이러한 전환은 조직이 회복탄력성을 통해 AI를 확장할 수 있도록 돕는 동시에, AI의 배포, 모니터링, 보호 방식에 대해 통제를 강화할 수 있습니다.

역할별 다음 단계.

세 가지 전환을 경영진 워킹 세션으로 활용하여 AI 준비 상태를 단계적인 계획으로 전환하세요. 목표는 모든 기반 격차를 한 번에 해결하는 것이 아니라, CIO와 CISO의 우선순위가 반드시 일치해야 하는 지점, 확장성을 확보하기 위해 CIO가 현대화해야 하는 부분, AI 도입이 확대됨에 따라 신뢰를 유지하기 위해 CISO가 강화해야 하는 부분에 대해 합의하는 것입니다.

함께 시작하세요. AI 지원 기반에 맞추세요.

AI에 대한 공통된 관점을 바탕으로 시작하되 AI 야망이 그 아래의 운영 모델보다 더 빠르게 움직이고 있는 부분이 어디인지부터 살펴보세요. CIO와 CISO 간 조율은 다음 세대 AI 도입에서 가장 중요한 워크플로, 데이터, ID, 디바이스 및 제어 항목에 초점을 맞춰야 합니다.

1. 어떤 AI 지원 워크플로를 다음으로 확장해야 하고, 확장에 나서기 전에 어떤 기반을 먼저 갖춰야 할까요?
2. AI를 유용하고 신뢰받을 수 있게 만들기 위해, 더 긴밀히 연결된 맥락, 더 강력한 거버넌스, 또는 더 명확한 소유권이 필요한 곳은 어디인가요?
3. 어떤 하나의 준비 격차를 먼저 해소하면 가장 큰 신뢰를 비즈니스에 가져올 수 있나요?

CIO 중점 분야. 디지털 인프라를 현대화하세요.

CIO는 개별적인 AI 활용 사례를 엔터프라이즈급 모멘텀으로 전환하고 디지털 환경을 단순화하고 직원들이 의존하는 도구와 워크플로를 연결하며 엔드포인트와 워크스페이스 경험을 현대화함으로써 AI가 조직 전체에서 마찰을 최소화하며 작동할 수 있도록 지원할 수 있습니다 .

1. AI가 일상적인 업무에 내재되고 있는 현재, 우리의 생산성, 협업,엔드포인트 전략은 어떻게 진화해야 하나요?
2. AI가 광범위하게 확장되기 전에, 어떤 직원 그룹, 디바이스 또는 업무 패턴이 더 일관된 환경을 필요로 할까요?
3. 통합과 현대화는 복잡성을 줄이는 동시에 직원들이 AI에서 확보하는 가치를 높일 수 있을까요?

CISO 중점 분야. 신뢰와 제어 범위를 확장하세요.

CISO는 민감한 데이터가 검색 가능하고 보호되며 사용자, 디바이스, 에이전트 전반에 걸쳐 접근이 거버넌스되고 보안 신호가 충분히 통합되어 AI가 위험의 속도와 복잡성을 높일 수 있는 상황에서도 위협을 탐지하고 대응할 수 있도록 돕는 역할을 함으로써 AI를 안심하고 확장할 수 있습니다.

1. AI가 더 많은 워크플로의 일부가 됨에 따라 데이터, ID, 디바이스, 에이전트에는 어떤 통제가 따라야 할까요?
2. AI 액세스 권한을 민감한 정보나 중요 프로세스로 확대하기 전에 어떤 영역에서 가시성을 강화해야 할까요?
3. AI와 에이전트의 업무 범위가 확대될 때 탐지, 대응, 거버넌스 모델은 어떻게 진화해야 할까요?

AI 준비 역량 구축을 시작합니다.

AI 전환은 업무가 연결되고, 데이터가 보호되며, 액세스가 거버넌스로 관리되고, 엔드포인트가 관리되며, 보안 신호가 함께 작동할 때 확장됩니다. 업무가 더욱 분산되고 역동적으로 변화함에 따라, 조직은 물리적 환경과 클라우드 환경 전반에서 애플리케이션, 데이터, 정책 및 경험이 연결된 일관되고 거버넌스가 적용된 업무 환경을 통해 혜택을 얻을 수 있습니다.

업무 경험이 맥락을 잃지 않고 직원들을 따라가면, AI는 더 관련성 높은 인사이트를 제공하고 워크플로 전반에 걸쳐 실행을 지원하며 조직 전체에서 보다 효과적으로 확장하는 데 도움을 줄 수 있습니다. 이것이 바로 Microsoft 365가 조직이 구축할 수 있도록 설계된 기반입니다. 생산성, 보안, 규정 준수, ID, 엔드포인트 관리, AI를 하나의 통합 플랫폼으로 제공하여 CIO, CISO, 비즈니스 리더들이 함께 앞으로 나아갈 수 있도록 지원합니다.

콜투액션 →

1. **함께 시작하세요.** AI 도입의 다음 단계에서 가장 중요한 워크플로, 데이터, ID, 디바이스 및 제어 정책에 대해 합의를 이루세요.
2. **Microsoft 365와 함께 구축하세요.** Microsoft 365 *제품군 및* Microsoft 365 Copilot 및 Windows 365 전반에 걸쳐 통합된 기반을 활용하여 업무를 연결하고, 데이터를 보호하며, 액세스 거버넌스를 수행하고, 대규모로 관리하며, 신뢰를 가지고 대응하세요.
3. **자신 있게 확장하세요.** 모멘텀을 창출할 첫 단계를 순차적으로 구성하세요. 가장 가치가 높은 사용 사례와 가장 위험도가 높은 데이터부터 시작한 후, 기반이 강화됨에 따라 범위를 확장하세요.

소스:
1 Deloitte의 2026 엔터프라이즈급 AI 현황 보고서(PDF), 매일 사용되는 AI를 1개 이상 도입한 조직이 있는 24개국의 비즈니스 및 IT 리더 3,200명 이상을 대상으로 한 설문 조사
2 2026년 업무 동향 지수, Microsoft 365 원격 분석 데이터는 집계 및 익명 처리된 Microsoft 365 생산성 신호와 2026년 2월 18일부터 2026년 4월 7일까지 10개 시장에서 AI를 사용해 업무를 수행하는 정규직 또는 자영업 지식 근로자 2만 명을 대상으로 한 설문 조사 결과를 기반으로 합니다. 조사 대상 글로벌 시장은 다음과 같습니다. 오스트레일리아, 브라질, 프랑스, 독일, 인도, 이탈리아, 일본, 네덜란드, 영국, 미국.
3 McKinsey's the-state-of-organizations 2026 보고서: 전 세계 15개국, 16개 산업 분야의 10,000명 이상의 고위 경영진을 대상으로 한 대규모 리더 설문조사입니다.
4 NTT Data Research Reveals C-Suite Misalignment Over GenAI Adoption, 2025년 6월 20일. 전 세계 34개국에서 1,500명의 경영진급 리더를 포함한 2,300명 이상의 고위 GenAI 의사결정자를 대상으로 진행된 설문조사입니다.

©2026 Microsoft Corporation. All rights reserved. 이 문서는 "있는 그대로" 제공됩니다. URL 및 기타 인터넷 웹사이트 참조를 포함하여 이 문서에 표현된 정보와 견해는 사전 통지 없이 변경될 수 있습니다. 이 문서를 사용하여 발생하는 위험은 사용자가 감수합니다. 이 문서는 Microsoft 제품의 지적 재산권에 대한 어떠한 법적 권리도 귀하에게 제공하지 않습니다. 이 문서는 복사가 가능하며 복사본은 내부 참조용으로만 사용할 수 있습니다.