

AI 기술 구현의 4가지 핵심 고려 사항

AI(Artificial Intelligence, 인공지능) 기술을 사용하기 시작하거나 사용을 늘리고자 하는 비즈니스 리더에게는 공통적인 질문과 고려 사항이 있습니다. 여기에는 AI를 사용하여 운영 효율성을 개선하고 비즈니스를 성장시키는 동시에 안정성을 유지하고 위험을 완화하는 방법이 포함됩니다. 기업은 AI를 어느 정도 구현했든 간에 다음 4가지 사항을 고려해야 합니다.

1 유연한 플랫폼 선택

이제 막 AI 도입을 시작하든, 기존의 활용 사례를 확장하여 AI를 더 광범위하게 구현하려고 하든 어느 경우에도 확장 가능하고 유연한 플랫폼을 선택하여 AI 배포 성숙도를 높이는 것이 핵심입니다.

AI 도입 초기 단계에서는 팀이 소규모 워크로드를 빌드하고 실행할 수 있는 안정적이면서도 유연한 개방형 인프라가 필요합니다. 기업이 AI 사용을 늘리고 워크로드가 증가함에 따라 사용하는 플랫폼에서 규모에 맞게 모델 훈련을 지원해야 합니다.

안정적인 플랫폼에서는 데이터 사이언티스트와 개발자가 고객에게 실질적인 가치를 제공하는 모델을 구축할 수 있으며, 고객은 자신이 사용하는 플랫폼이 안정적이고 보안에 중점을 두고 있다고 확신할 수 있습니다.

비즈니스가 AI 기능을 비교적 잘 활용하고 있다면 조직이 AI의 잠재력을 최대한 활용할 수 있도록 지원하는 기술이 필요합니다. 이를 위해서는 GPU 및 기타 하드웨어 가속기에 상당한 투자가 필요할 수 있습니다.

확장 가능한 개방형 플랫폼의 이점

- ▶ 기업이 짧은 시간 내에 AI 기반 애플리케이션을 빌드하고 현대화할 수 있는 우수한 기반을 제공합니다.
- ▶ AI 기반 애플리케이션의 배포를 가속화합니다.
- ▶ 빠르게 변화하는 AI 환경에서 경쟁 우위를 선점할 수 있도록 지원합니다.

올바른 인프라를 갖춘 조직은 앞으로 다가올 새로운 AI 혁신을 수용할 준비가 된 것입니다.

2 하이브리드 AI를 위한 준비

생성형 AI(gen AI)로 인해 컴퓨팅 리소스에 대한 수요가 늘고 네트워크 엣지에서도 처리가 이루어지고 있습니다. 생성형 AI 활용 사례에서는 클라우드와 온프레미스의 리소스를 혼합하여 이점을 얻을 수 있지만, 일부 워크로드, 특히 컴플라이언스 문제나 데이터 주권이 영향을 미치는 워크로드는 온프레미스에서만 실행해야 합니다. 하이브리드 AI를 사용하면 팀이 데이터가 생성되는 위치를 포함하여 적합한 장소 어디에서나 워크로드를 실행할 수 있습니다.

하이브리드 AI는 다음을 포함하여 다양한 이점을 제공합니다.

- ▶ **유연성:** 가장 적합한 환경에서 실험적인 워크로드와 프로덕션 워크로드를 실행하여 비용을 절감할 수 있습니다.
- ▶ **제공 가속화:** 엣지에서 소규모 워크로드를 추론하여 사용자에게 정보를 더 신속하게 제공합니다.
- ▶ **위험 감소:** 엣지에서 AI 애플리케이션을 실행하면 대량의 정보를 코어로 전송할 필요성이 줄어들어 데이터 보호 태세가 향상됩니다.

하이브리드 AI를 사용하면 IT 팀이 코어 데이터센터 또는 퍼블릭 클라우드에서 모델을 훈련하여 엔드포인트에 분산할 수 있습니다. 이를 통해 유용한 인텔리전스를 더 신속하게 추론하여 제공할 수 있습니다. 집중적인 워크로드를 중앙 클라우드와 엣지 전반에 분산하여 처리 성능에 대한 요구와 빠르고 정확한 권장 사항에 대한 요구 사이의 균형을 맞출 수 있습니다.

3 모델 빌드 이후의 고려 사항

IT 팀은 최소한의 노력으로 단일 AI 모델을 프로덕션에 투입할 수 있지만 성공 여부는 확장 능력에 따라 결정되는 경우가 많습니다. 비즈니스 가치를 극대화하기 위해서는 팀에서 해당 모델의 여러 버전을 하루에 수백 번 배포할 수 있어야 합니다.

MLOps(Machine Learning Operations, 머신 러닝 운영) 프로세스를 구현하면 팀이 배포를 쉽게 확장하는 데 도움이 될 수 있습니다.

DevOps와 유사하게 MLOps에서는 개발자와 운영 관리자, 데이터 사이언티스트가 모여 AI 기반 애플리케이션의 개발과 성공적인 배포를 가속화합니다. 조직은 MLOps를 통해 애플리케이션 개발을 더욱 쉽게 확장할 수 있어 짧은 시간 내에 고객에게 많은 서비스를 제공할 수 있습니다.

MLOps는 비용 효과적이고 효율적인 개발 수단이 될 수 있습니다. 팀은 공통 플랫폼에서 함께 작업함으로써 효율성을 높이고 이를 통해 조직의 수익에 직접적인 영향을 미치는 시간과 비용을 잠재적으로 절감할 수 있습니다.

4 보안 우선

비용이 많이 드는 사이버 공격에 대응하여 민감한 데이터를 보호하고 위험을 완화할 수 있는 방법을 찾는 기업 경영진이 늘어나고 있습니다. 생성형 AI를 사용하면 기밀 데이터가 노출될 위험이 높아질 수 있으므로 보안 기능 강화가 더욱 시급합니다.

다음과 같은 위협으로부터 조직을 보호하기 위해 강력한 보안 태세를 유지해야 합니다.

- ▶ **데이터 포이즈닝:** 부정확하거나 악의적인 데이터를 AI 모델에 투입하여 부정확한 정보나 허위 권장 정보를 생성하도록 합니다.
- ▶ **모델 도용:** 머신 러닝 모델을 리버스 엔지니어링하고 복사본을 사용하여 데이터를 추출합니다.
- ▶ **백도어 공격:** AI 모델에 악성 코드를 숨겨 공격자가 정보를 훔칠 수 있도록 합니다.

이렇게 악의적인 위협들은 비즈니스에 심각한 위협을 가져와 조직을 재정적 위험과 법적 위험 모두에 노출시킬 수 있습니다. 보안 패치 및 릴리스 처리와 관련해 입증된 실적과 확립된 프로세스를 갖춘, 신뢰할 수 있는 애플리케이션 플랫폼 공급업체의 도움을 받아 AI와 관련된 취약성을 최소화하세요.

자세히 알아보기

AI 전략을 가속화할 때입니다. Red Hat의 AI 솔루션을 [확인해 보세요](#).

한국레드햇 홈페이지 <https://www.redhat.com/ko>



Red Hat 소개

Red Hat은 [권위 있는 어워드를 수상한](#) 지원, 교육, 컨설팅 서비스로 고객이 여러 환경에서 표준화를 진행하고, 클라우드 네이티브 애플리케이션을 개발하고, 복잡한 환경을 통합, 자동화, 보안, 관리할 수 있도록 지원합니다.

f www.facebook.com/redhatkorea
구매문의 02-6105-4390
buy-kr@redhat.com