DELL Technologies

AI 보안 및 회복탄력성 서비스

AI 사용에 대한 신뢰 확보

AI 도입 관련 과제 해결

AI(Artificial Intelligence)는 획기적인 혁신과 더 빠른 의사 결정을 지원하여 비즈니스의 판도를 바꿀 수 있습니다. 하지만 잠재력이 큰 만큼 과제도 상당합니다. AI 도입 시 보안, 신뢰, 규정 준수에 대한 고유한 우려가 생기며, 이는 조직에 새로운 압박이 되고 있습니다. Dell Technologies에서는 새로운 AI 보안 작동 방식을 정립했습니다. 이러한 독보적인 접근 방식을 통해 데이터 관리, 인프라스트럭처 보안, AI 모델 보호를 통합하여 포괄적인 맞춤형 솔루션을 제공합니다. AI를 처음 접하든 기존 솔루션을 확장하든 관계없이 Dell Technologies의 포괄적인 서비스는 더 빠르고 안전하며 안정적으로 AI를 도입하도록 설계되었습니다.

IT 담당자를 포함해 모두가 책임지는 보안

최신 AI 관련 보안에는 팀 간의 협업이 필요합니다. AI 보안은 단체 스포츠와 마찬가지로 조직 전체에 걸친 의견 수렴과 의사 결정이 필요합니다. 기존의 사일로화된 IT 운영 모델은 이렇게 진화하는 환경에 적합하지 않습니다. Dell Technologies의 고유한 접근 방식은 데이터, 인프라스트럭처, 애플리케이션, 모델을 특정 비즈니스 요구 사항에 맞게 조정되는 하나의 일관된 전략에 통합하여 앞서 나가는 데 도움이 되는 포괄적인 솔루션을 제공합니다.

AI의 고유한 보안 과제 해결

AI 도입에는 다음과 같이 잠재적 이점을 위협할 수 있는 복잡한 보안 및 규정 준수 고려 사항이 있습니다.

- 미흡한 데이터 보호 또는 무단 액세스로 인한 데이터 침해 및 IP(Intellectual Property) 손실
- 적대적 공격, 모델 조작 또는 훈련 데이터 오염과 같은 AI 기반 위협
- 지원 에이전트 등 현재 중요한 AI 툴의 지속적인 운영 가능성 문제
- 상호 연결된 시스템에서 발생하는 타사 공급망 취약성
- 하이브리드 및 멀티클라우드 환경에서 AI 애플리케이션의 확장에 따른 공격 표면의 확대
- 환각 현상으로 인한 사용자의 오해(순전히 보안 문제라고 보기는 어려움)

주요 이점

신뢰성 및 투명성 향상: 데이터, 지식재산, AI 무결성을 보호하여 이해관계자 간의 신뢰를 유지합니다.

운영 회복탄력성: 미션 크리티컬 AI 시스템이 지속적으로 운영되고 위협에 저항할 수 있도록 합니다.

규정 준수: 업계 및 정부 규정을 준수하여 처벌에 관련된 높은 비용과 평판 손상을 방지하도록 지원합니다.

확장 가능한 솔루션: 조직과 기술 스택에 따라 확장되는 적응형 AI 보안 조치를 적용합니다.

전문가 지원 및 지침: 검증된 보안 전문가와 협력하여 솔루션을 맞춤화하고 측정 가능한 결과를 제공합니다.

맞춤형 보안 아키텍처를 제공하는 포괄적인 서비스

Dell Technologies에서 개발한 보안 아키텍처는 고객의 고유한 요구 사항을 충족하도록 설계되어 유연하고 신뢰할 수 있는 기반을 제공합니다. Dell AI Factory와 원활하게 통합되고 제로 트러스트(Zero Trust) 원칙을 적용하며 파트너 기술을 전문적으로 통합하여 안전하고 미래 지향적인 혁신을 추진합니다.

	기능
자문 조직의 요구 사항 및 규정 준수 요구 사항에 부합하도록 AI 보안 설정 지원	• **AI의 보안 및 회복탄력성을 위한 자문 서비스**에는 포괄적인 보안 및 가용성 전략을 개발하기 위한 비즈니스 및 기술 워크숍이 포함됩니다. • **AI용 CISO 어드바이저**를 통해 AI 보안 전략 수립을 시작하기 위해 AI 전문가인 가상 CISO를 제공합니다. • **AI용 데이터 보안**으로 사용자의 데이터에 대한 데이터 보안 위협과 위험을 낮출 수 있습니다.
구현 AI 스택 가시성 향상을 위한 보안 소프트웨어 설계 및 구현	• **보안 소프트웨어 설계 및 구성**을 통해 액세스 관리, 애플리케이션, 네트워크를 보호하는 툴을 통합할 수 있습니다.
관리 스택 전반에 걸쳐 심층적인 가시성을 지원하여 위협을 신속하게 탐지하고 대응	• **MDR(Managed Detection and Response)**을 통해 데이터, 인프라스트럭처, 애플리케이션, 모델 전반에 걸쳐 연중무휴 위협을 탐지합니다. • **매니지드 AI 방화벽**은 격리된 AI 기반 가드레일 세트를 적용하고 프롬프트 및 출력을 검사하여 정책을 준수합니다. • **AI용 침투 테스트**를 통해 적대적 공격을 시뮬레이션하고 약점을 파악합니다. • **인시던트 대응 및 복구 서비스**를 통해 신속하게 복구하고 운영 중단을 최소화하면서 비즈니스를 재개하도록 지원합니다.

안심하고 안전한 AI 미래 구축

Dell의 AI 보안 및 회복탄력성 서비스는 조직에 AI를 도입하는 것과 관련된 새로운 위험을 해결하도록 개발되었습니다. 팀과 협업하여 최대한 빠르게 AI를 온보딩하도록 설계된 Dell Technologies의 서비스는 전략 기획, 솔루션 구현, 매니지드 보안 서비스와 관련한 전문 지식을 제공함으로써 운영 부담을 줄이고 AI를 통해 안전하게 혁신하도록 지원합니다.

Dell 보안 및 회복탄력성 서비스 알아보기

Dell Technologies 전문가에게 문의

대화에 참여: #DellTechnologies