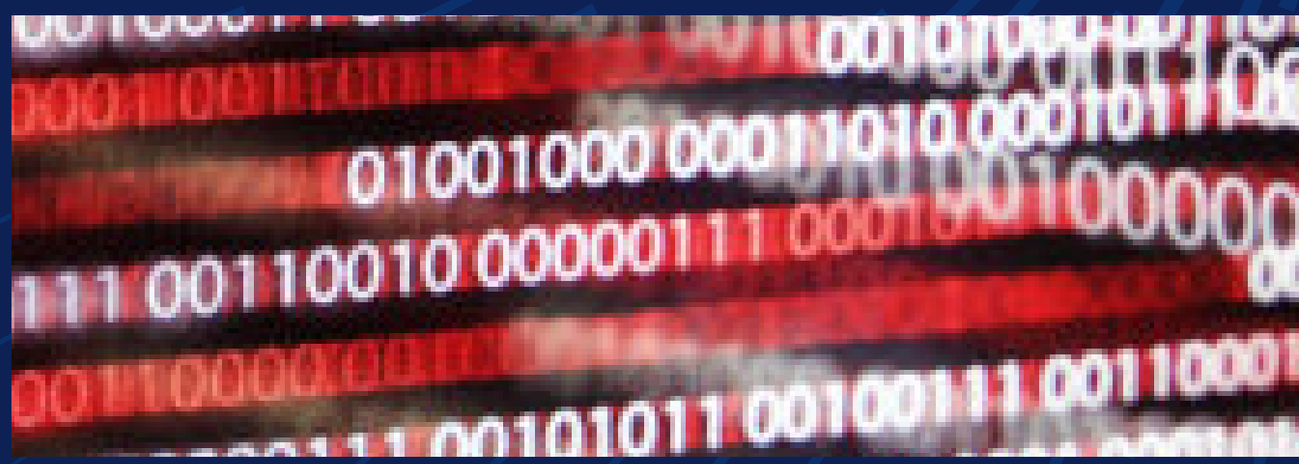
사이버 보안에 대한 잘못된 통념 해소:

AI 보안에 대한 잘못된 통념 해소



AI가 산업에 혁신을 가져오고 있기는 하지만, AI 보안에 관해서는 많은 조직이 AI를 실제보다 복잡해 보이게 만드는 잘못된 통념에 사로잡혀 있습니다. 진실은 무엇일까요? AI 시스템을 보호하기 위해 완전히 처음부터 시작할 필요는 없습니다. 기존 사이버 보안 원칙을 AI의 고유한 과제에 적용하는 것만으로도 큰 효과를 볼 수 있습니다.

Dell Technologies는 AI의 기반이 되는 아키텍처를 이해하고 있으며, 기존 솔루션을 이 새로운 프레임워크에 맞게 조정하도록 지원할 수 있습니다. AI 보안을 둘러싼 가장 흔한 잘못된 통념을 분석하고, 효과적인 시스템 보안을 위한 진실을 밝혀보겠습니다.

잘못된 통념 1: "AI 시스템은 보안이 너무 복잡하다."

진실: AI가 프롬프트 삽입, 데이터 조작, 기밀 정보 유출 등과 같은 새로운 사이버 보안 위험을 야기하는 것은 사실입니다. 또한 에이전틱 AI 시스템은 결과를 조작하거나 권한을 에스컬레이션하는 데 악용될 수 있기 때문에 공격 노출 지점이 더 넓습니다.

그렇긴 해도 이러한 취약성을 인지하고 기존 위협과 AI 관련 위협 모두로부터 AI 시스템을 보호하기 위한 보안 조치를 구현하는 것이 중요하지만, 위험은 관리될 수 있고 AI 모델도 보호될 수 있습니다. AI 시스템에는 입력으로 상당한 양의 데이터가 필요하고 출력으로 많은 양의 데이터가 생성된다는 점을 명심해야 합니다. 따라서 데이터 보호는 핵심 보안 전략 중 하나로 최우선 순위에 있으며, 다음과 같은 사항들이 포함됩니다.

- ID 관리, 역할 기반 액세스, 지속적인 검증과 같은 제로 트러스트 원칙
- 취약성을 파악하기 위한 정기적인 침투 테스트 및 취약성 관리
- 데이터 입력 및 출력 검증을 위한 로깅 및 감사

잘못된 통념 2: "기존 툴로는 AI를 보호할 수 없다."

진실: AI 보안은 처음부터 다시 시작하는 것이 아니라, 이미 보유하고 있는 툴을 더욱 스마트하게 활용하는 것입니다. 대부분의 기존 사이버 보안 툴은 AI 시스템을 효과적으로 보호하도록 조정할 수 있습니다. AI는 본질적으로는 비즈니스를 추진하는 또 하나의 워크로드이지만, 고유한 특성을 가지고 있습니다. ID 관리, 네트워크 세분화 및 모니터링, 엔드포인트 보호, 데이터 보호와 같은 기본적인 사이버 보안 관행은 AI 환경을 보호하는 데 여전히 필수적입니다. 핵심은 학습 데이터 보호, 알고리듬 보안, 적대적 입력과 같은 위험 완화 등 특정 AI 과제를 해결하도록 이러한 관행을 조정하는 것입니다.

강력한 방어는 시스템 패치 적용, 액세스 제어 및 취약성 관리와 같은 효과적인 사이버 보안에서 시작됩니다. 중요한 것은 이러한 관행을 AI 관련 위험을 해결하기 위해 맞춤화하는 것입니다. AI 중심 전략을 기존 보안 접근 방식에 통합하고 적절한 툴을 사용하면 AI 보안을 관리하기 쉽고 효과적으로 만들 수 있습니다.

하지만 업데이트된 하드웨어가 사이버 공격에 대처하는 데 중요한 역할을 할 수 있다는 점을 짚고 넘어가야 합니다. 예를 들어, 최신 AI PC는 주요 공격 벡터인 엔드포인트에 대한 강력한 1차 방어선을 구축합니다. Windows 10 지원이 종료됨에 따라 구형 PC는 위험 요소가 됩니다. 또한 Windows 11에는 암호화, 보안 부팅 및 펌웨어 공격으로부터 보호하는 데 도움이 되는 보안 칩인 TPM(Trusted Platform Module) 버전 2.0이 필요합니다. 많은 구형 PC는 TPM이 전혀 없거나 이전 버전만 지원합니다. Dell은 이러한 개선 사항이 내장된 안전한 AI PC를 제공합니다.

서버 및 스토리지와 같은 AI 인프라스트럭처도 마찬가지입니다. Dell AI Factory에는 AI 보안에 최적화된 하드웨어가 포함되어 있으며, 안전한 공급망, 데이터 불변성, 격리 및 암호화 등 다양한 보안 기능이 내장되어 있습니다.

잘못된 통념 3: "AI 보안은 데이터 보호에만 국한된다."

진실: AI 보안은 기본적인 데이터 보호를 넘어 모델, API, 출력, 시스템 및 디바이스를 포함한 전체 AI 생태계를 보호하는 것을 포함합니다. AI가 중요 애플리케이션에 더욱 통합됨에 따라 오용 또는 악용과 관련된 위험은 심화됩니다. 강력한 보안 조치가 없으면 AI 모델이 변조되어 유해하거나 오해의 소지가 있는 출력을 생성할 수 있고, API가 악용되어 기밀 시스템에 무단으로 접근할 수 있으며, 출력이 의도치 않게 개인 정보 또는 기밀 정보를 노출할 수 있습니다.

포괄적인 AI 보안에는 다층적인 접근 방식이 필요합니다. 여기에는 AI 시스템을 속이기 위해 입력 데이터를 조작하려는 적대적 공격으로부터 모델을 보호하고, 무단 사용을 방지하기 위해 강력한 인증 방법으로 API를 보호하고, **출력을 지속적으로 모니터링**하여 공격이나 오작동을 나타낼 수 있는 비정상적이거나 의심스러운 패턴이 있는지 확인하는 것이 포함됩니다. 효과적인 AI 보안은 AI 시스템의 무결성과 신뢰성을 보장할 뿐만 아니라 악의적인 사용이나 의도치 않은 결과의 위험을 완화하여 사용자 및 이해 관계자와의 신뢰를 구축합니다.

잘못된 통념 4: "AI는 인간의 감독이 필요하지 않다."

진실: AI 시스템이 윤리적이고 예측 가능하며 인간의 가치에 부합하는 방식으로 운영되도록 하려면 거버넌스와 인간의 감독이 필수적입니다. 고급 AI 시스템, 특히 자율적인 의사 결정 기능을 갖춘 에이전틱 AI는 강력한 안전 장치를 요구하는 고유한 과제를 안고 있습니다. 적절한 감독이 없다면 이러한 시스템은 의도한 목표에서 벗어나거나 위험을 초래할 수 있는 의도치 않은 행동을 보일 수 있습니다.

이를 해결하려면 명확한 경계를 설정하고, 계층화된 제어 메커니즘을 구현하며, 중요한 의사 결정 프로세스에 인간의 지속적인 참여를 보장하는 것이 필수적입니다. 정기적인 감사, AI 운영의 투명성, 그리고 철저한 테스트는 책임과 신뢰를 더욱 강화하여 AI 기술의 오용을 방지하고 책임감 있는 배포를 촉진하는 데 도움이 될 수 있습니다.

AI 보안 강화를 위한 모범 사례

AI 관련 보안 격차를 해소하기 위해 조직은 사전 예방적이고 전략적인 접근 방식을 채택해야 합니다.
AI 시스템 보안을 위한 10가지 모범 사례는 다음과 같습니다.

계층형 보안 아키텍처:
세분화, 방화벽 및 강력한 인증을 활용하여 모든 계층에서 인프라스트럭처, 소프트웨어 및 데이터를 보호합니다.

AI 출력 모니터링 및 검증:
이상 징후 탐지, 로깅 및 알림을 사용하여 AI 출력에서 비정상적인 패턴이나 유해한 동작을 모니터링합니다.

공급망 보안:
강력한 공급업체 관리 프로그램을 구현합니다. 공급업체 및 타사 구성 요소를 감사하고, 무결성을 검증하고, 서명된 코드를 사용함으로써 AI 개발 수명주기의 취약성을 예방합니다.

회복탄력성 계획:
데이터를 정기적으로 백업하고 재해 복구 계획을 테스트하여 다운타임을 최소화하고 침해 발생 시 신속한 복구를 보장합니다.

학습 데이터 및 모델 보호:
데이터 무결성을 모니터링하고 강력한 검증 툴을 적용하여 감염된 데이터, 적대적 입력 및 기타 위협으로부터 보호합니다.

강력한 암호화 구현:
강력한 알고리듬을 사용하여 저장 상태 데이터 및 전송 중인 기밀 데이터를 암호화하고, 암호화 키를 안전하게 관리하고 정기적으로 순환합니다.

액세스 제어 강화:
최소 권한 원칙을 시행하고, RBAC(Role-Based Access Control)를 구현하고, 자격 증명을 정기적으로 순환하고, 사용 권한을 감사하여 무단 액세스를 방지합니다.

정기적인 보안 감사 및 침투 테스트 실시:
시스템의 취약성을 자주 평가하고 침투 테스트를 실시하여 악용되기 전에 위험을 파악합니다.

API 보안:
강력한 인증 프로토콜(예: OAuth 2.0)을 사용하고, HTTPS 암호화를 적용하며, API를 정기적으로 업데이트하여 잠재적인 취약성을 차단합니다.

AI 보안 모범 사례에 대한 직원 교육:
보안 개발, 위협 인식, 그리고 보안 침해 방지를 위한 강력한 보안 관행 유지에 대한 교육을 정기적으로 팀원들에게 제공합니다.

DELL Technologies

Dell의 가치 제안: 실용적인 AI 보안 솔루션

AI 보안은 복잡해 보일 수 있지만, 생각보다 어렵지 않습니다. 진실은 무엇일까요? AI 보안은 기존 워크로드 보안과 크게 다르지 않습니다. 아키텍처를 이해하고 적절한 전략을 적용하는 것입니다. Dell Technologies가 바로 이러한 파트너입니다.

Dell Technologies는 기존 솔루션을 활용하고 AI 중심 아키텍처에 원활하게 통합하여 AI 보안의 본질을 명확하게 설명합니다 인프라스트럭처를 완전히 개편하지 않고도 프롬프트 삽입, API 남용, 적대적 공격과 같은 과제를 해결합니다.
Dell Technologies의 전문성은 AI 보안에 대한 잘못된 통념을 불식시키고 그 실현 가능성을 보여주는 데 있습니다. AI 여정을 막 시작했든, 방어 체계를 강화하고 싶든, Dell Technologies는 투자를 보호하고, 시스템을 안전하게 보호하며, 회복탄력성이 뛰어난 디지털 미래를 자신 있게 효과적으로 구축할 수 있도록 지원합니다. 함께 AI 보안을 간소화해 보겠습니다.

도움이 될 수 있는 Dell 제품 및 솔루션

주요 Dell 솔루션	설명
Dell AI Factory	Dell AI Factory는 안전한 공급망을 통해 AI 워크로드를 보호하고, 개발부터 구축까지 신뢰할 수 있는 인프라스트럭처를 보장합니다. 데이터 불변성, 격리, 암호화 등의 기능을 통해 기밀 모델 및 데이터 세트를 보호하고, 사이버 위협으로부터 방어하며, 역동적인 데이터 중심 환경에서 확장 가능하고 효율적이며 원활한 AI 운영을 지원합니다.
사이버 회복탄력성	PowerProtect는 불변성 및 격리와 같은 고급 기능으로 AI 워크로드를 보호하여 데이터 무결성을 보장하고 사이버 위협으로부터 보호합니다. 포괄적인 암호화 및 이상 징후 탐지를 제공하는 동시에 신속한 복구를 지원하여 다운타임을 최소화합니다.
Dell Trusted Work-space(엔드포인트 보안)	AI PC와 해당 PC에서 실행되는 AI 워크로드를 보호하도록 설계된 기본 제공 기능과 선택 사항인 추가 기능의 조합입니다. 안전한 공급망 관리 방식을 기반으로 구축된 기본 제공 기능으로는 SafeBIOS, SafeID with TPM이 있습니다. 선택 사항인 추가 기능으로는 Secured Component Verification, SafeID with ControlVault, 그리고 작업 공간 보안을 극대화하는 파트너 소프트웨어인 CrowdStrike 및 Absolute가 있습니다.
AI 보안 자문 서비스	포괄적인 AI 보안 전략을 개발하고 구현하는 데 도움이 되는 서비스 제품군입니다. 오퍼링에는 자문 서비스, AI vCISO 및 데이터 보안 계획이 포함됩니다.
AI를 위한 관리형 보안 운영	스택 전반에 걸쳐 심층적인 가시성을 지원하여 위협을 신속하게 탐지하고 대응합니다. 기능으로는 Managed Detection and Response, Managed AI Guard, AI용 침투 테스트, 인시던트 대응 및 복구 서비스가 있습니다.
보안 소프트웨어 통합	액세스 관리, 애플리케이션, 네트워크, 클라우드 등을 보호하는 보안 툴을 설계, 설치 및 구성합니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.