DELL Technologies

NVIDIA

GenAI(Generative AI)를 위한 5가지 주요 보안 고려 사항

Dell AI Factory with NVIDIA를 통해 안전하고 확장 가능한 인프라스트럭처 기반 도입 가속화

GenAI의 혁신적인 잠재력

GenAI는 아직 상상하지 못한 방식으로 판도를 바꿀 수 있는 잠재력이 있습니다.

76%

GenAI가 조직에 혁신적인 가치를 제공할 것이라고 생각하는 IT 및 비즈니스 리더의 비율.[1]

AI

이벤트를 해석하고 의사 결정과 행동을 지원하고 자동화하는 고급 분석 및 논리 기반 기술.

GenAI

대량의 데이터를 활용하여 자연어 프롬프트 또는 기타 비코드 및 비일반적 입력에서 새로운 콘텐츠를 생성하는 기술 및 기법.

시뮬레이션

- 디지털 트윈
- 합성 데이터
- 설계 프레임워크
- 예측

콘텐츠 검색

- 자연어 검색
- 대규모 데이터 세트 분석
- 지식 관리
- 개인화된 교육 및 훈련

콘텐츠 제작

- 코딩
- 수학
- 글쓰기/말하기
- 이미지/비디오
- 오디오

사용자 경험

- 70개 이상의 언어를 실시간 번역
- 자연스러운 얼굴 표정과 몸짓을 사용한 개인화된 상호 작용

1 Dell Technologies Innovation Catalysts Study, 2024년 2월.

커지는 잠재력, 증가하는 위험

비즈니스 리더는 데이터, 규정 준수, 거버넌스 및 기타 위험과 관련된 영향을 피하고 빠르게 움직이기를 원합니다. 그러나 GenAI는 보안과 관련하여 양날의 검입니다.

이점

- 공격 탐지 기능 향상
- 운영 효율성 향상
- 맞춤형 보안 인식 교육

단점

- 공격의 정교함 향상
- 강화된 소셜 엔지니어링
- 섀도우 AI

33%

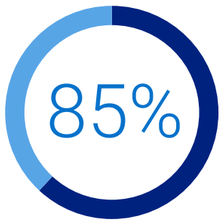
조직이 완화하기 위해 노력하고 있는 주요 GenAI 위험으로 사이버 보안을 꼽은 응답자의 비율.[2]

2 AI에 대한 McKinsey 글로벌 설문조사: The state of AI in early, 2024년 5월

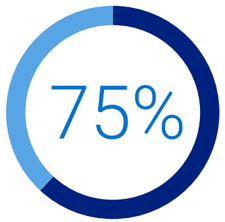
고려 사항 1

새로운 위협 환경

GenAI로 얻을 수 있는 이점과 함께 따라오는 냉철한 현실: 공격자들은 기존 방어 체계를 우회할 수 있는 새롭고 더 복잡한 공격을 시도하고 있어 사이버 보안 팀이 이를 따라잡기 어렵습니다.



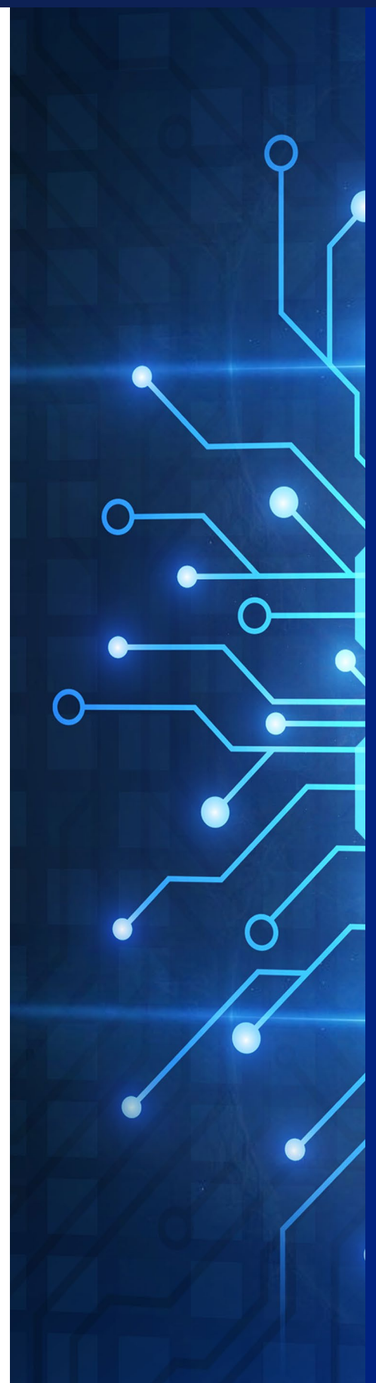
AI가 사이버 보안 공격을 더욱 정교하게 만들었다고 생각하는 응답자의 비율.[3]



지난 12개월 동안 공격 수가 증가하는 경향을 목격한 보안 전문가의 비율.[4]

이러한 새로운 위협으로부터 보호하기 위해 기업은 침투 테스트, 모니터링, 감사 등을 통해 공격 노출 지점을 최소화하는 데 집중해야 합니다.

3 2024 Human Risk in Cybersecurity Survey, EY, 2024년 5월
4 Voice of SecOps Report "Generative AI and Cybersecurity: Bright Future or Business Battleground?" 2023



새로운 공격 벡터

고급 멀웨어
GenAI를 사용하여 "자체 발전"하는 점점 더 정교해지는 멀웨어로, 서명 기반 탐지와 같은 기존 보안에 의해 탐지되지 않도록 코드를 지속적으로 변경합니다.

고도로 개인화된 피싱 이메일 및 캠페인
일반적인 사기 징후가 없는 실제 악성 이메일의 빈도가 증가합니다.

설득력 있는 딥 페이크 데이터
글쓰기, 말하기, 이미지 또는 영상과 같은 인간의 행동을 모방할 수 있어 신원 도용, 금융 사기, 잘못된 정보의 전달이 더 쉬워집니다.

자동화된 정찰
정보 수집을 통해 잠재적인 타겟 네트워크 또는 시스템의 취약성과 약점을 파악하여 더 구체적으로 표적을 공격합니다.

고려 사항 2

배포 및 구현 위험

GenAI의 잠재적 이점을 활용하려는 조직들은 대량의 고품질 데이터, 즉 모델이 최상의 성과를 생산하는 데 사용할 수 있는 입력이 필요합니다. 하지만 데이터의 활용에는 위험이 따릅니다. 기업은 정보를 활용하기 전에 고유한 요구 사항, 입력, 위험을 신중하게 평가하고 고려해야 합니다.

LLM(Large Language Model) 취약성

GenAI 서비스는 프롬프트 인젝션 공격에 취약합니다. 이는 공격자가 출력을 조작하여 보안 가드레일을 우회하거나 모델을 개선하는 데 사용되는 파일에 대한 무단 액세스 권한을 얻는 공격입니다.

데이터 오염

공격자는 훈련 단계 동안 의도적으로 변경된 데이터를 LLM에 제공할 수 있습니다. 따라서 모델은 데이터 내부에 숨겨진 백도어를 통해 공격을 받는 취약성을 가질 수 있습니다. 실제 사례로 스팸 이메일을 학습하여 스팸 필터를 공격하고 악용하는 경우가 있습니다.

복잡한 규제

전 세계 규제 기관은 GenAI의 안전성을 이해하고 제어하며 보장하기 위해 경쟁하고 있습니다. GenAI 모델에는 데이터의 저장, 처리 및 사용 방식을 결정하는 현재의 데이터 주권 규칙이 적용되지만, 여전히 관리 기관이 IP와 저작권 정보에 대한 감독을 정의하고 있습니다. 규정 준수에는 비용이 많이 들 수 있지만, 확립된 새로운 규정을 준수하지 않으면 벌금과 기타 불이익이 발생할 수 있습니다.

고려 사항 3

섀도우 AI

오늘날 많은 직원들이 이미 ChatGPT와 같은 공용 텍스트, 이미지 및 비디오 생성기를 사용하여 일상적인 작업 흐름을 보완하고 있습니다. 그러나 이러한 툴을 적절한 관리 감독 없이 사용하면 기업의 지적 재산과 데이터를 보호하는 데 심각한 위협이 됩니다. 이렇게 GenAI를 무단으로 사용하는 것을 섀도우 AI라 부릅니다.

지적 재산 손실

이미 기업은 공용 GenAI 툴에서 기밀 정보를 공유하는 직원으로 인한 지적 재산 손실을 겪고 이에 대처하고 있습니다.

소스 코드 데이터 유출

ChatGPT를 사용하여 소스 코드를 최적화하려는 개발자가 데이터 유출을 일으킬 수 있습니다.

섀도우 AI의 당면 과제를 해결하기 위해 기업은 안전한 AI 거버넌스와 관련된 의사 결정을 내릴 수 있는 권한이 있는 전사적 협의회 또는 이사회를 구성해야 합니다.

데이터가 어디에 있습니까? 워크로드를 어디에 배치해야 합니까?

AI는 데이터가 어디에 있든 이와 결합했을 때 가장 큰 효율을 발휘합니다. 인프라스트럭처 및 LLM을 완벽하게 제어하면 IP 손실이나 소스 코드 데이터 유출의 위험이 없습니다.

비용

온프레미스 구현을 활용하면 3년 동안 TCO를 최대 75%까지 절감할 수 있습니다.[5]

보안 및 개인 정보 보호

온프레미스 워크플로와 운영을 통해 조직 전반에 안전한 AI/GenAI 환경을 구축합니다. 기밀 데이터를 취급하는 산업에서는 특히 엄격한 데이터 보안 조치를 취하고 규정 준수를 강조하여 데이터의 안전을 확보해야 합니다.

5 Dell Technologies의 의뢰로 온프레미스 Dell 인프라스트럭처와 네이티브 퍼블릭 클라우드 IaaS(Infrastructure as-a-Service)를 비교한 Enterprise Strategy Group 연구 기준, 2024년 4월. 분석된 모델에 따르면, 사용자 5천 명 규모의 조직에서 RAG를 활용하는 70억 매개변수 LLM은 최대 38% 더 비용 효율적이고, 사용자 5만 명 규모의 조직에서 RAG를 활용하는 700억 매개변수 LLM은 최대 75% 더 비용 효율적인 것으로 나타났습니다. 실제 결과는 달라질 수 있습니다. 경제 요약

고려 사항 4

평가 기준

지난 한 해 동안 AI 커뮤니티는 책임 있는 개발 및 배포, 영향 평가, 위험 완화라는 세 가지 주요 문제에 점점 더 집중하고 있습니다. 기업은 GenAI 모델을 평가할 때 다음과 같은 몇 가지 중요한 주의 사항을 고려해야 합니다.

일관된 보고 요구 사항 없음

선도적인 개발자들은 서로 다른 AI 벤치마크를 기준으로 모델을 테스트합니다. 보고의 표준화가 크게 부족하기 때문에 주요 AI 모델의 위험과 한계를 체계적으로 비교하기 어렵습니다.

출력에 저작권이 있는 자료

인기 있는 LLM의 출력에는 저작권이 있는 자료가 포함되어 있을 수 있으며, 이는 법률을 위반하고 해당 자료를 사용하는 회사에 불이익이 발생할 위험이 있습니다.

점점 더 복잡해지는 취약성

연구자들은 모델이 무작위 단어를 무한히 반복하도록 만드는 것과 같이 LLM이 유해한 행동을 하도록 하는 덜 명백한 전략을 발견하고 있습니다.

투명성이 부족한 개발자

AI 개발자들은 교육 데이터와 방법론에 대한 정보를 공개하지 않는 경우가 많습니다. 이는 AI 시스템의 견고성과 안전성을 더 깊이 이해하려는 노력에 방해가 됩니다.

고려 사항 5

보안 이점

GenAI에는 보안 위험과 함께 잠재적인 보안 이점도 있습니다. GenAI는 사이버 보안의 중요한 지원군이 되어 새로운 보호 기회를 열어주고 있습니다.

이제 더 풍부한 통찰력과 자동 위협 탐지를 더 빠르게 활용하여 확장 가능한 보안 운영을 수행할 수 있으므로 효율성을 높이고 인력이 부족한 보안 팀을 보완할 수 있습니다.

Threat Detection and Response

GenAI는 과거 데이터를 분석하고 패턴 및 이상 징후를 식별하여 새로운 위협과 진화하는 위협을 실시간으로 인식할 수 있습니다. 네트워크 트래픽, 시스템 로그 및 사용자 동작을 지속적으로 모니터링하고 보안 위협이 될 수 있는 비정상적인 활동을 즉시 식별할 수 있습니다.

덕분에 변화하는 공격 벡터에 대한 신속한 대응과 새로운 사이버 위협에 대한 사전 예방적 방어 기능을 가진 강력한 적응형 위협 탐지 체계를 갖출 수 있습니다.

위협 시뮬레이션 및 교육

GenAI를 통해 기업은 통제된 환경에서 다양한 사이버 보안 위협 및 공격 시나리오를 시뮬레이션할 수 있습니다. 결과적으로 팀은 짧은 시간 내에 사이버 위협을 식별, 대응 및 완화할 수 있도록 더 잘 준비할 수 있습니다.

심층 분석 및 요약

GenAI를 통해 팀이 서로 다른 소스 또는 모듈에서 데이터를 조사할 수 있으므로 기존에는 시간이 많이 걸리던 지루한 데이터 분석을 더 빠르고 정확하게 수행할 수 있습니다. 또한 팀은 인시던트 및 위협 평가에 대한 자연어 요약을 생성하여 효율성을 개선하고 팀 성과를 높일 수 있습니다.

맞춤형 보안 인식 교육

GenAI에 대화형 AI를 추가하고 AI 아바타를 사용자 인터페이스에 통합함으로써 조직은 자연스러운 얼굴 표정과 몸짓 언어를 사용하여 개인화된 상호 작용(24/7 대규모 이용 가능)을 제공할 수 있습니다. 이를 보안 훈련 및 교육을 위해 사용하여 더 자연스럽고 맞춤화된, 상호작용적인 학습 경험, 자동 평가 등 다양한 이점을 가질 수 있습니다.

Dell AI Factory with NVIDIA

업계 최초의 종합 턴키 AI 솔루션을 통해 AI 여정을 가속하고 데이터에서 통찰력을 안전하게 도출하십시오. Dell AI Factory with NVIDIA는 AI와 GenAI를 활용하고자 하는 엔터프라이즈의 복잡한 니즈를 해결합니다. 최고 수준의 인프라스트럭처 및 서비스를 NVIDIA AI 소프트웨어와 함께 활용하면 개발과 배포를 간소화함으로써 프로젝트의 가치 실현 시간을 개선할 수 있습니다.

- RoT(Root of Trust) 및 기타 주요 기능을 포함하여 내재적 보안을 갖춘 인프라스트럭처를 구축하여 위협의 위험을 최소화합니다.
- 통제할 수 있는 온프레미스 AI 솔루션으로 지적 재산의 손실을 방지하고 데이터 유출을 예방합니다.
- 안전한 액세스 방식으로 AI를 데이터에 활용하여 엄격한 규정 준수 및 데이터 주권 요구 사항을 충족합니다.
- 데이터에 액세스할 수 있는 위치와 사용자를 제어하여 이해 관계자의 개인 정보를 보호합니다.

Dell AI Factory with NVIDIA

Dell 최초의 포괄적인 엔터프라이즈 AI 솔루션

AI Factory와 활용 사례의 동력인 데이터

가장 가치 있는 데이터는 온프레미스와 엣지 환경에 있습니다. Dell Technologies는 가치 있는 데이터에 AI를 활용할 수 있도록 지원하며, 이러한 데이터를 저장, 보호, 관리하는 분야에서 선도적인 기업입니다.

성과를 위한 활용 사례

AI Factory는 우선순위가 가장 높은 활용 사례로 비즈니스 성과를 창출합니다. Dell Technologies는 검증된 솔루션과 맞춤형 서비스를 통해 가장 중요한 AI 활용 사례의 배포를 간소화합니다.

보안 위험이 혁신의 걸림돌이 되지 않도록 대비

Dell Technologies와 함께 AI와 GenAI의 세계를 살펴보고 그 혜택을 누리십시오.

전략 계획

GenAI를 위한 무료 Accelerator Workshop

- 성공적인 전략 개발을 위한 여정 시작
- 당면 과제 및 부족한 역량 해결, 세부 목표의 우선순위 지정, 기회 파악
- 인프라스트럭처 요구 사항, AI 모델, 운영 통합 등에 대한 심층 분석을 위한 준비 상태 진단

기술 준비

즉시 사용할 수 있는 모바일 랩

성공을 향한 여정을 시작하십시오. NVIDIA GPU가 탑재된 Dell Mobile Precision Workstation 5690/7780과 2일간의 컨설팅 서비스가 포함되어 있습니다.

- GenAI 테스트 및 데모를 위한 휴대용 샌드박스 환경
- 개발자를 위한 NVIDIA AI Workbench 플랫폼으로 사전 검증됨
- 데이터로 구현된 초기 챗봇 활용 사례
- GenAI 기술을 실험하고 체득하기 위한 비용 효율적이고 위험성이 낮은 접근 방식

NVIDIA GPU를 탑재한 DELL MOBILE PRECISION WORKSTATION 5690/7780

지금 시작하십시오

DELL Technologies AI Factory WITH NVIDIA