글로벌 시장동향보고서

2025.08
Vol.13

사이버 보안 內 인공지능

(Artificial intelligence (AI) in cybersecurity)

1. 사이버 보안에 대한 AI의 영향

» 사이버 보안에서 AI는 반복적이고 시간이 많이 소요되는 작업을 자동화함으로써 분석가가 더 빠르고 적은 노력으로 더 나은 정보에 기반한 의사 결정을 하도록 지원하며 보안 수명 주기 전반에 걸쳐 성능을 향상시킴

- AI 사이버보안 자동화는 최소한의 개입으로 위협을 탐지, 격리, 해결할 수 있는 적응형 자체 복구 시스템을 만드는 통합 기술에 의존하며, 위협을 탐지하고 대응하는 능력뿐만 아니라 위협으로 인해 피해가 발생하기 전에 이를 예측하고 예방하는 능력을 포함

〈표 1〉 AI 보안의 이점

구분	내용
향상된 위협 탐지	• AI 알고리즘은 대량의 데이터를 실시간으로 분석하여 잠재적인 사이버 위협을 탐지하는 속도와 정확성을 향상시킬 수 있으며, AI 도구는 기존 보안 조치에서 놓칠 수 있는 정교한 공격 경로도 식별할 수 있음
더 빠른 사고 대응	• AI는 보안 사고의 탐지, 조사 및 대응에 필요한 시간을 단축하여 조직이 보다 신속하게 위협을 해결하고 잠재적 피해를 줄일 수 있도록 지원
운영 효율성 향상	• AI 기술은 일상적인 작업을 자동화하여 보안 운영을 간소화하고 비용을 절감 • 사이버 보안 운영 최적화 시 인적 오류를 줄이고 보안 팀이 보다 전략적인 프로젝트에 집중 가능
사이버 보안에 대한 사전 예방적 접근 방식	• AI 보안을 통해 조직은 과거 데이터를 사용하여 미래의 사이버 위협을 예측하고 취약성을 식별함으로써 사이버 보안에 대한 보다 사전 예방적 접근 방식을 취할 수 있음

구분	내용
새로운 위협에 대한 이해	• AI 시스템은 새로운 데이터로부터 지속적으로 학습함으로써 새로운 위협에 적응하고 새로운 공격 방법에 대해 사이버 보안 방어를 최신 상태로 유지할 수 있도록 함
사용자 환경 개선	• AI는 사용자 환경을 손상시키지 않으면서 보안 조치를 강화할 수 있음/ 예를 들어, 생체 인식 및 행동 분석과 같은 AI 기반 인증 방법은 사용자 인증을 보다 원활하고 안전하게 만들 수 있음
자동화된 규정 준수	• AI는 규정 준수 모니터링, 데이터 보호 및 보고를 자동화하여 조직이 규정 요구 사항을 일관되게 충족할 수 있도록 지원
확장성	• AI 사이버 보안 솔루션은 대규모의 복잡한 IT 환경을 보호하도록 확장할 수 있도록 하며, 또한 보안 정보 및 이벤트 관리(SIEM) 플랫폼과 같은 기존 사이버 보안 도구 및 인프라와 통합하여 네트워크의 실시간 위협 인텔리전스 및 자동화된 대응 기능을 강화

출처 : IBM (2024.06.05.)

사이버 공격이 점점 정교해짐에 따라, 사이버 보안에 반응적 방어에서 사전 예방적 방어로 AI 자동화를 도입하고 있는 추세로 특히 트래픽 모니터링, 침해 예측, 사고 대응 등에서 높은 활용률을 보이고 있음

- AI 도구가 더욱 발전하고 접근성이 높아짐에 따라 사이버 보안에 AI를 적용하는 방식은 다양하고 지속적으로 발전하고 있음

〈표 2〉 AI 보안 활용 사례

구분	내용
데이터 보호	• 데이터 보호는 민감한 정보를 보호하여 데이터 손실 및 손상으로부터 데이터를 보호하고 가용성을 보장하고 규정 요구 사항을 준수하는 것을 포함 • AI 도구는 조직이 민감한 데이터를 분류하고, 데이터 이동을 모니터링하고, 무단 액세스 또는 유출을 방지하여 데이터 보호를 개선하는 데 도움이 될 수 있으며, AI는 저장 중인 데이터와 전송 중인 데이터를 보호하기 위해 암호화 및 토큰화 프로세스를 최적화할 수도 있음 • 또한 AI는 위협 환경에 자동으로 적응하고 24시간 내내 위협을 지속적으로 모니터링할 수 있으므로 조직은 새로운 사이버 위협에 앞서 나갈 수 있음
엔드포인트 보안	• 엔드포인트 보안에는 컴퓨터, 서버, 모바일 디바이스와 같은 엔드포인트를 사이버 보안 위협으로부터 보호하는 것이 포함 • AI는 엔드포인트에서 의심스러운 행동과 이상 징후를 지속적으로 모니터링하여 실시간 보안 위협을 탐지함으로써 기존 엔드포인트 탐지 및 대응(EDR) 솔루션을 개선 • 또한 머신 러닝 알고리즘은 파일리스 멀웨어 및 제로 데이 공격과 같은 지능형 엔드포인트 위협이 피해를 입히기 전에 식별하고 완화하는 데 도움이 될 수 있음
클라우드 보안	• AI는 섀도 데이터를 자동으로 식별하고, 데이터 접근의 이상 징후를 모니터링하고, 위협이 발생하면 사이버 보안 전문가에게 경고함으로써 하이브리드 클라우드 환경에서 민감한 데이터를 보호하는 데 도움이 될 수 있음

구분	내용
지능형 위협 헌팅	• 위협 헌팅 플랫폼은 조직의 네트워크 내에서 악의적인 활동의 징후를 사전에 검색 • AI 통합을 통해 이러한 도구는 대규모 데이터 세트를 분석하고, 침입 징후를 식별하고, 고급 위협을 보다 신속하게 탐지하고 대응할 수 있게 되면서 훨씬 더 발전되고 효율적이 될 수 있음
사기 탐지	• 사이버 공격과 신원 도용이 보편화됨에 따라 금융 기관은 고객과 자산을 보호할 수 있는 방법이 필요하며 AI는 사기를 나타내는 패턴에 대한 거래 데이터를 자동으로 분석하여 이러한 기관을 지원 • 또한 머신 러닝 알고리즘은 새롭고 진화하는 위협에 실시간으로 대응할 수 있으므로 은행은 사기 탐지 기능을 지속적으로 개선하고 위협 행위자보다 앞서 나갈 수 있음
사이버 보안 자동화	• AI 보안 도구는 조직의 기존 보안 인프라와 통합될 때 가장 효과적인 경우가 다수 • 예를 들어, 보안 오케스트레이션, 자동화 및 대응(SOAR)은 많은 조직이 보안 운영을 간소화하는 데 사용하는 소프트웨어 솔루션으로. AI는 SOAR 플랫폼과 통합되어 일상적인 작업과 워크플로를 자동화할 수 있으며 이 통합을 통해 사고 대응 속도가 빨라지고 보안 분석가가 더 복잡한 문제에 집중할 수 있음
ID 및 액세스 관리(IAM)	• AI 기반 IAM 솔루션은 역할, 책임, 행동에 따라 세분화된 액세스 제어를 제공하여 권한이 있는 사용자만 민감한 데이터에 액세스할 수 있도록 함으로써 이 프로세스를 개선할 수 있음 • 또한 AI는 머신 러닝을 사용하여 사용자 행동 패턴을 분석하고 개별 사용자의 위험 수준에 따라 변경되는 적응형 인증 조치를 지원함으로써 인증 프로세스를 개선 가능
피싱 탐지	• ChatGPT와 같은 LLM은 피싱 공격을 더 쉽게 수행하고 인식하기 어렵게 만들었으나 AI는 피싱 퇴치를 위한 중요한 도구로도 부상 • 머신 러닝 모델은 조직에서 피싱 징후가 있는지 이메일과 기타 커뮤니케이션을 분석하여 탐지 정확도를 높이고 피싱 시도를 줄이는 데 도움을 줄 수 있으며, AI 기반 이메일 보안 솔루션은 실시간 위협 인텔리전스와 자동화된 대응 기능을 제공하여 피싱 공격이 발생했을 때 이를 포착할 수 있음
취약성 관리	• 취약성 관리는 조직의 IT 인프라 및 소프트웨어의 보안 취약점을 지속적으로 발견하고, 우선순위를 정하고, 완화하고, 해결하는 것으로, AI는 잠재적인 영향과 악용 가능성에 따라 취약성의 우선순위를 자동으로 지정하여 기존 취약성 스캐너를 개선할 수 있으며 이를 통해 조직은 가장 중요한 보안 위험을 먼저 해결할 수 있음 • 또한 AI는 패치 관리를 자동화하여 사이버 위협에 대한 노출을 즉시 줄일 수 있음

출처 : IBM (2024.06.05.)

- CompTIA의 설문조사*에 따르면 기업들은 네트워크 트래픽 모니터링(54%)에 AI를 가장 많이 적용하고 있으며, 침해 예측(50%)과 방어 테스트 생성(50%), 사고 대응 자동화(49%) 등도 주요 활용 분야

  * 2024년 3분기 기술 및 비즈니스전문가를 대상으로 설문조사를 실시하였으며 1,181명 응답

출처 : Statista (2024), CompTIA 재인용

[그림 1] 전 세계 사이버 보안 분야의 주요 AI 활용 사례 (2024년)

- IBM의 설문조사*에 따르면 대다수의 기업이 보안 기능에 AI 자동화를 도입하거나 도입을 고려하고 있는 것으로 나타났으며, 응답자의 64%는 보안 수명 주기 프로세스 중 하나 이상에 AI 보안 기능을 구현하고 있으며, 29%는 도입을 고려

  * 2022년 5개 지역의 16개 산업에 종사하는 조직의 it 및 운영 기술 사이버 보안을 총괄하는 임원 1,000명을 대상으로 실시

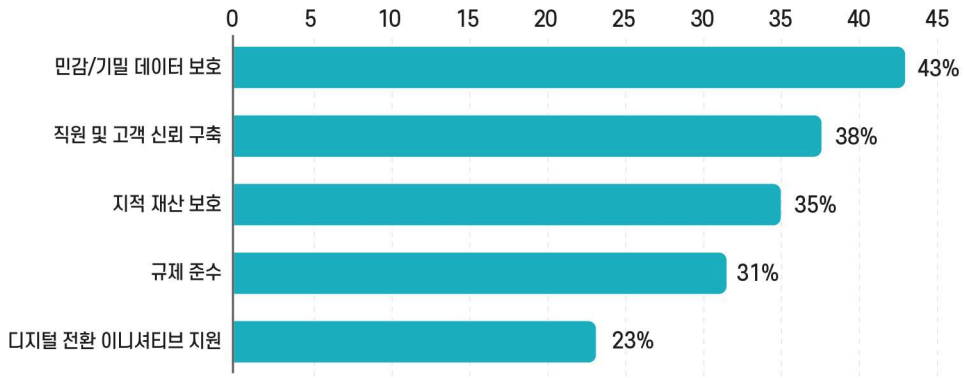
- AI를 도입한 보안 조직들이 보안 운영 성과를 향상시킨 핵심 AI 활용 영역으로는 Tier 1 위협 분류가 67%로 1위로 나타났으며, 제로데이(Zero-day) 공격 및 위협 탐지(66%), 미래 위협 예측(65%), 거짓 양성 및 노이즈 감소(65%) 등의 순으로 나타남

출처 : IBM (2022)

* Q: Which of the following AI applications has had the greatest impact on your security operations (select the top 5)?

[그림 2] 보안 성과 향상에 기여한 AI 적용 분야 (Top 5)

- 기업들은 민간/기밀 데이터를 보호하고 직원 및 고객 신뢰를 구축하기 위해서 보호와 예방에 중점을 둔 AI를 도입

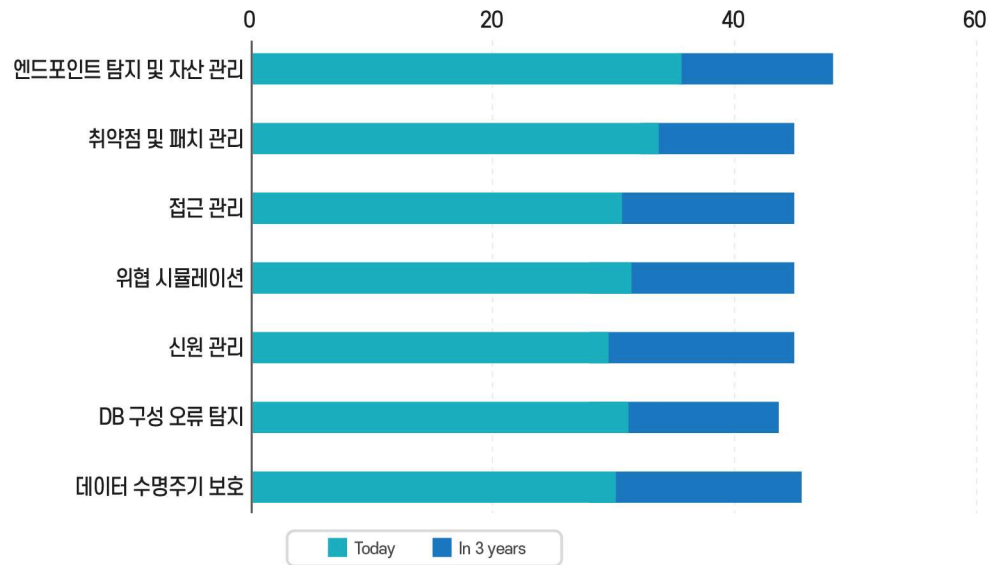


출처 : IBM (2022)

* Q: What are the primary drivers of AI in your organization? (Objectives focused on protection and prevention)

[그림 3] 보안을 위한 AI 도입 목적

- AI 도입 기업들은 엔드포인트 검색 및 자산 관리를 주요 AI 활용 사례로 꼽았으며, 35%는 현재 이 기능에 AI와 자동화를 적용하고 있고, 3년 안에 활용률을 거의 50%까지 늘릴 계획으로 AI 기반 보호 및 예방 중심 보안이 확대될 전망

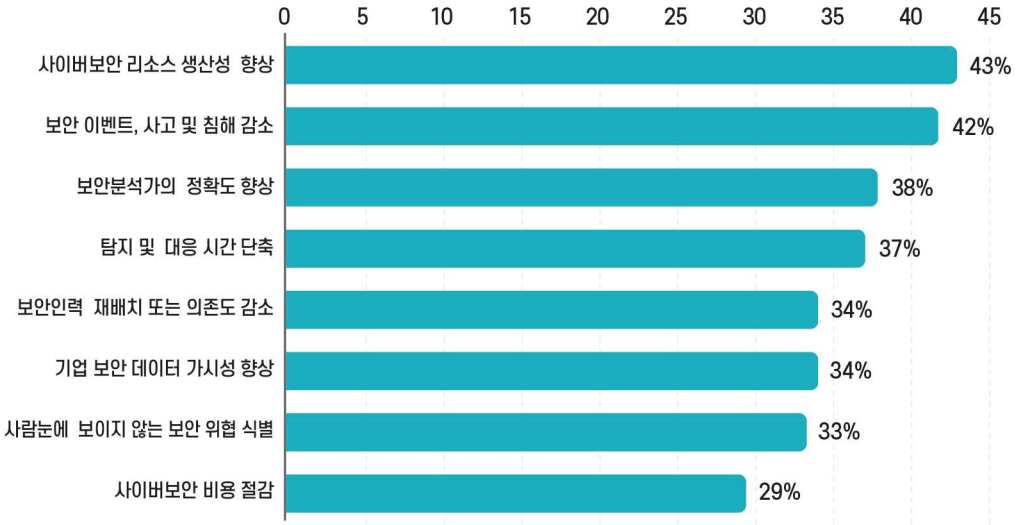


출처 : IBM (2022)

* Q: What use cases for AI automation are being implemented today? And in 3 years? (Use cases focused on protection and prevention.)

[그림 4] 보안을 위한 AI 자동화 활용 분야 (현재 vs 향후 3년)

• 기업들은 AI를 활용해 사이버보안 업무의 생산성과 정확성을 동시에 개선하고 있으며, 특히 인력 활용 효율화와 위협 탐지의 신속성·정확성 측면에서 큰 효과를 보고 있음



출처 : IBM (2022)

* Q: What are the primary drivers of AI in your organization? (Objectives focused on operations, detection, and response.

[그림 5] AI 기반 사이버보안 업무 개선 목적

IBM의 보고서*에 따르면, 사이버 보안 운영에 AI 자동화를 광범위하게 활용하는 조직은 침해 비용이 평균 220만 달러 감소한 것으로 나타남

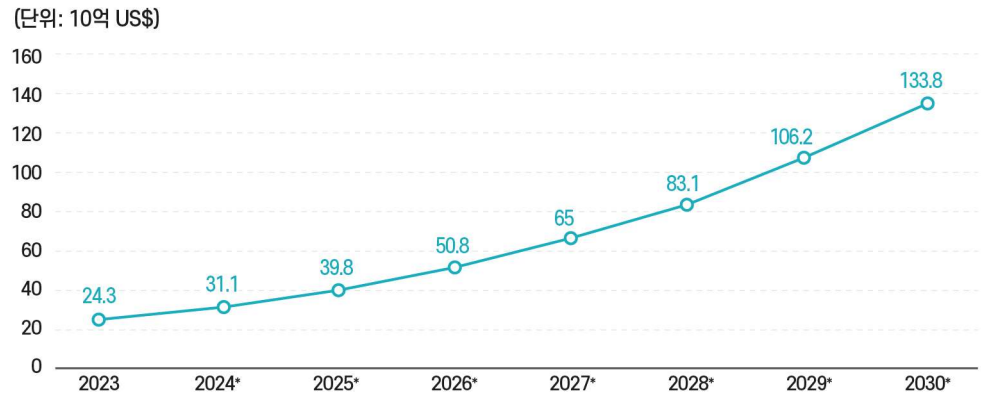
* 2024년 16개 국가 및 지역의 17개 산업에 종사하는 604개 기업을 대상으로 2,100개에서 113,000개에 달하는 침해 사례를 조사

- IBM의 "2024 데이터 유출 비용 연구 보고서(2024 Cost of a Data Breach Report)"에 따르면 2024년 전세계 2024년 전세계 데이터 유출 사고 한 건 당 평균 비용이 488만 달러(한화 약 67억 6,100만원)에 달하며, 데이터 유출로 인해 상당한 또는 매우 심각한 업무 중단을 겪었다고 응답한 기업은 70%에 달함
- AI와 관련해서는 보안 AI 및 자동화 솔루션을 도입한 기업이 67%로 전년 대비 10% 가까이 증가했으며, 20%는 차세대 AI 보안 툴을 사용한다고 밝힘
- 보안 AI 솔루션을 완벽하게 구축한 조직에 영향을 미치는 침해 사고의 경우, 솔루션을 구축하지 않은 기업보다 평균 220만 달러의 비용이 감소함
- AI 사이버 보안을 도입한 조직은 데이터 침해가 발생했을 때 이를 식별하고 격리하는 데 걸리는 시간이 그렇지 않은 조직보다 평균 98일 단축된 것으로 나타남
- 전 세계 평균 데이터 유출 사고 수명 주기(침입 감지부터 봉쇄, 최종 해결까지 걸리는 시간)는 전년도 277일에서 7년 만에 최저치인 258일을 기록했으며, AI 기술이 위협 완화 및 대응 활동을 개선해 방어자들이 시간을 확보하는 데 도움이 될 수 있음을 시사

2. 글로벌 사이버 보안 분야 AI 시장 규모 및 전망

2023년 243억 달러규모였던 AI 사이버 보안 시장은 2026년까지 두 배로 성장할 것으로 예상되며, 2030년에는 약 1,340억 달러 규모에 달할 것으로 전망

- Technopedia는 글로벌 AI 사이버 보안 시장 규모가 2023년부터 2030년까지 27.6% 연평균 성장률을 보이며 1,330억 달러를 넘어설 것으로 예상



출처 : Statista (2024), Technopedia 재인용

[그림 6] 글로벌 AI 사이버보안 시장 가치 (2023~2030)

- 2023년 AI 사이버보안 시장은 북미(40%)가 최대 지역이며, 아시아 태평양은 가장 빠르게 성장 중으로 아시아태평양 지역은 예측 기간 동안 글로벌 시장 성장의 44%를 차지할 것으로 추정되며, 아시아태평양 지역의 AI 및 ML 기반 사이버 AI 시장은 특히 중국, 일본, 한국에서 상당한 성장을 경험하고 있음
- AI 사이버보안 시장의 확장은 행동 생체인식 및 ML 알고리듬과 같은 AI 기반 사이버보안 솔루션을 활용하는 BFSI 및 핀테크 부문을 포함한 IT 부문의 급속한 발전에 기인

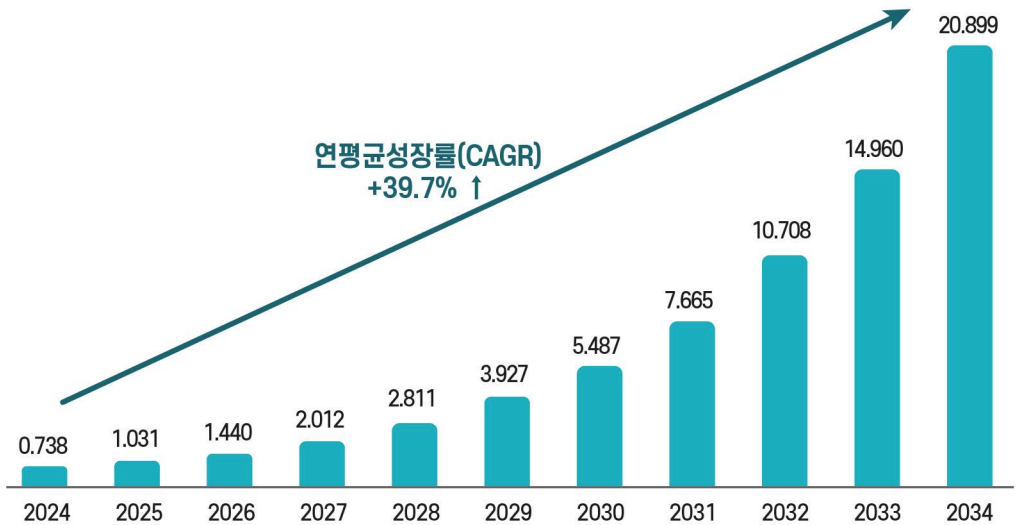
기술별로는 머신러닝(45%)이 시장을 주도하나, 딥러닝은 복잡한 위협 분석 역량으로 가장 빠르게 성장하고 있으며, 중소기업 부문도 비용 효율적 솔루션 수요 증가로 빠르게 확대되고 있음

- Verified Market Reports에 따르면 AI 기술 유형별로는 2023년 기준 머신 러닝이 약 45%로 가장 큰 시장 점유율을 차지하고, 딥 러닝이 30%, 자연어 처리가 15%, 기타가 10%를 차지했으며, 머신 러닝은 위협 탐지 분야에서 널리 적용 가능하기 때문에 가장 빠르게 성장하는 것으로 분석됨
- 대기업은 AI 기반 사이버 보안 솔루션 도입률이 높아 시장 점유율 60%로 대부분의 시장을 차지하고, 중소기업은 30%, 나머지 10%는 기타 기업들이 차지하였으며, 가장 빠르게 성장하는 애플리케이션 부문은 중소기업 부문으로, 사이버 위험이 커짐에 따라 저렴한 AI 사이버 보안 솔루션 도입이 증가하고 있음
- AI 유형별로는 딥 러닝이 방대한 데이터 세트를 분석하고 복잡한 위협을 보다 효과적으로 식별하는 능력에 힘입어 가장 빠르게 성장하는 하위 세그먼트로 나타남

글로벌 사이버 보안 분야의 에이전트 AI 시장(agentic AI market)은 2034년까지 약 208억 9천만 달러 규모로 성장할 것으로 예상

- 에이전트 AI는 인간의 개입 없이 스스로 결정을 내리고 작업을 실행할 수 있는 자율 시스템을 의미하며, 사이버 보안에서 에이전트형 AI는 독립적인 감시자 역할을 하며, 네트워크를 지속적으로 모니터링하고, 데이터를 분석하며, 시스템을 사전에 보호
- 사전 정의된 규칙과 수동 감독에 의존하는 기존 보안 조치와 달리, 에이전트 AI는 새롭게 발생하는 위협에 실시간으로 적응하고, 주변 환경을 학습하여 방어 전략을 강화하여 이러한 역동적인 접근 방식을 통해 AI는 위험이 확산되기 전에 이를 예측하고 완화함으로써 조직이 정교한 사이버 공격에 더욱 효과적으로 대응할 수 있도록 지원
- 글로벌 사이버 보안 분야의 에이전트 AI 시장은 2024년 7억 3,820만 달러 규모에서 2025년부터 2034년까지 연평균 성장률 39.70%로 성장하여 2034년 약 208억 9천만 달러에 달할 것으로 전망

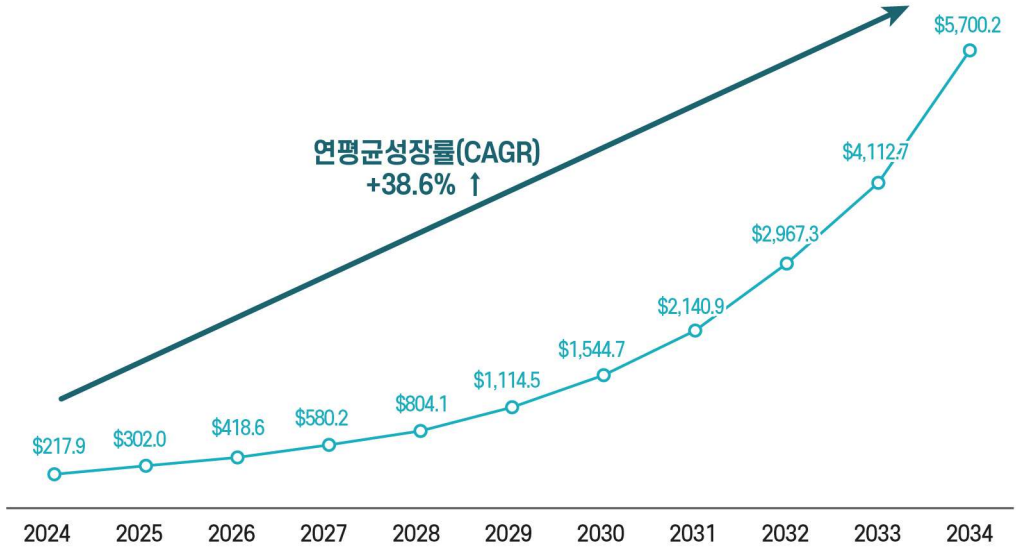
(단위: 10억 US$)



출처 : Market.us (2025.02)

[그림 7] 글로벌 에이전트 AI 사이버보안 시장 규모 (2024~2034)

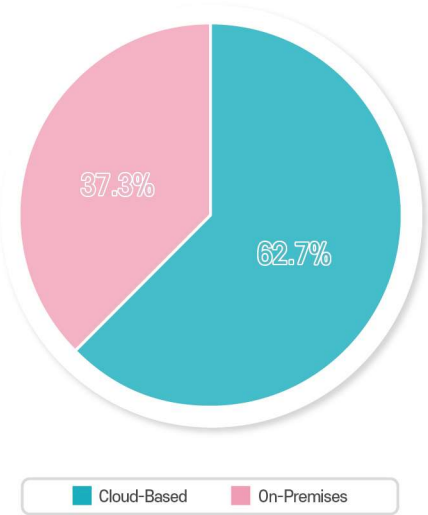
- 2024년 북미 시장은 32.8% 이상의 점유율을 기록하며 2억 4,210만 달러의 매출을 달성하며 시장 지배력을 유지했으며, 미국은 2억 1,790만 달러로 시장을 장악하고 38.6%의 연평균 성장률(CAGR)을 기록하며 꾸준히 강력한 입지를 유지



출처 : Market.us (2025.02)

[그림 8] 미국의 에이전트 AI 사이버보안 시장 규모 (2024~2034)

- 배포 모드별로는 2024년 클라우드 기반 부문이 시장 점유율 62.7% 이상을 기록하며 압도적인 시장 지위를 차지했으며, 온프레미스(On-Premises) 부문은 높은 비용 및 유지 관리 요구 사항과 클라우드 기반 유연성에 대한 선호도 증가로 인해 시장 점유율이 낮게 나타남



출처 : Market.us (2025.02)

[그림 9] 배포모드별 에이전트 AI 사이버보안 시장 규모 (2024)

2024년 주요 사이버보안 기업들은 생성형 AI 기술을 통합하여 위협 탐지와 대응 자동화를 강화하고 있으며, 클라우드 플랫폼과의 협력을 통해 보안 솔루션의 확장성과 실효성을 높이고 있음

〈표 3〉 AI 사이버 보안 관련 최근 개발 사항

구분	내용
SentinelOne	• 2024년 10월, 미국 사이버 보안 기업 SentinelOne, Inc.는 AWS와의 협력을 확대하여 자사의 사이버 보안 솔루션에 생성 AI를 통합하고, Amazon Bedrock을 활용하여 Purple AI 사이버 보안 분석가를 지원 • 이 협력을 통해 AWS Marketplace에서 SentinelOne의 Singularity Platform이 강화되어 고객은 AI 기반 보안 기능을 활용하고, 조사를 간소화하며, 위협 탐지 및 대응을 개선
IBM	• 2024년 8월, IBM은 자사의 위협 탐지 및 대응 서비스(Threat Detection and Response Services)에 생성형 AI 기반 사이버 보안 어시스턴트(Cybersecurity Assistant)를 도입 • IBM의 Watsonx 플랫폼을 기반으로 구축된 이 어시스턴트는 과거 상관관계 분석과 대화형 엔진을 통해 위협 조사 및 대응을 강화하도록 설계되었으며, 위협 조사를 가속화하고 운영 작업을 자동화
IBM	• 2024년 7월, IBM은 Microsoft와의 협력을 강화하여 고객의 보안 운영 현대화 및 네트워크 보안 클라우드 ID 보호를 지원했으며, 이는 고객 솔루션에 AI 기반 보안 기술을 통합함으로써 가능 • IBM의 위협 탐지 및 대응(TDR) 클라우드 네이티브 서비스와 같은 AI 도구를 활용하여 위협 탐지 기능을 강화하고, 복구를 자동화하며, 고객의 클라우드 보안을 최적화
CROWDSTRIKE	• 2024년에 CrowdStrike은 AI 기반 위협 인텔리전스를 자사의 주력 플랫폼인 Falcon에 통합하여 AI 기반 사이버보안 역량을 더욱 확장 • 고객의 특정 환경 및 산업 특성을 기반으로 위협 우선순위를 자동 조정하고 맞춤화된 인텔리전스를 제공할 수 있도록 함
DARKTRACE	• 2024년 3월 Darktrace는 Xage Security와 전략적 제휴를 체결하여 기업이 중요 인프라를 대상으로 한 내부자 위협 및 사이버 공격을 효과적으로 방지할 수 있도록 지원 • 이번 파트너십을 통해 Darktrace의 AI 기반 위협 탐지 기술과 Xage의 제로 트러스트 보안 솔루션이 결합되어, 보안 위반을 보다 신속하게 식별하고 대응할 수 있는 역량이 강화되었습니다.
ACALVIO AI-POWERED DECEPTION	• 2023년 3월, 아칼비오 테크놀로지스는 미국 소프트웨어 회사인 카라소프트 테크놀로지(Carahsoft Technology Corp.)와 파트너십을 맺고 카라소프트의 공공 부문 계약을 통해 섀도플렉스 액티브 디펜스 플랫폼(ShadowPlex Active Defense Platform)을 포함한 첨단 사이버 기만 기술을 미국 정부 기관에 제공 • 이 파트너십을 통해 정부 기관은 AI 기반 위협 탐지, 차단 및 인텔리전스 기능을 통해 사이버 보안 태세를 강화

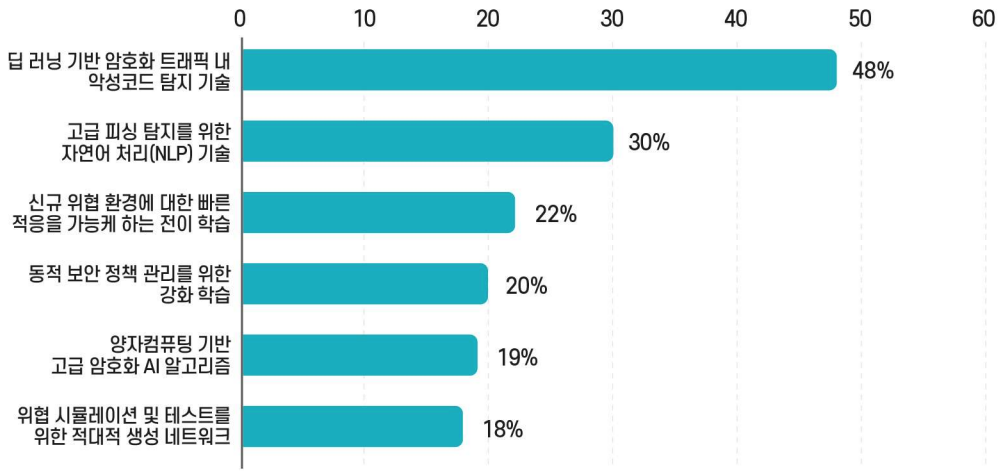
출처 : Grand view research (2024.11.27.), Market.us (2025.02)

암호화된 데이터 분석, 피싱 대응, 위협 적응력 향상 등 실질적인 보안 운영 강화를 위한 AI 기술에 높은 기대를 두고 있으며, 딥 러닝 기반의 암호화 트래픽 내 악성코드 탐지 기술, 고급 피싱 탐지를 위한 자연어 처리 기술 등이 높게 평가되고 있음

- Cybersecurity Insiders가 실시한 글로벌 조사*에 따르면, 보안 전문가들은 다양한 AI 및 머신러닝(ML) 기술 중 딥 러닝 기반의 암호화 트래픽 내 악성코드 탐지 기술이 사이버 보안 방어 강화에 가장 큰 가능성을 가진 기술로 평가(응답자의 48%)

  * 2023년 9월 다양한 산업의 글로벌 사이버 보안 전문가를 대상으로 한 설문조사에 457명 응답

- 다음으로 고급 피싱 탐지를 위한 자연어 처리(NLP) 기술이 30%로 두 번째로 높은 비중을 차지했으며, 이어 신규 위협 환경에 대한 빠른 적응을 가능케 하는 전이 학습(Transfer Learning)이 22%, 동적 보안 정책 관리를 위한 강화 학습(Reinforcement Learning)이 20%를 기록
- 한편, 양자컴퓨팅 기반 고급 암호화 AI 알고리즘(19%), 위협 시뮬레이션 및 테스트를 위한 적대적 생성 네트워크(GANs, 18%)도 주목받고 있으나, 상대적으로 기술 성숙도와 현실 적용 가능성 측면에서 우선 순위가 낮게 평가



출처 : Statista (2024), Cybersecurity Insiders. 재인용

[그림 10] 사이버 보안 강화를 위한 유망 AI/ML 기술 트렌드 (2023)

참고문헌

- Statista. (2024.02). Artificial intelligence (AI) in cybersecurity
- IBM (2022.06) AI and automation for cybersecurity
- IBM (2024.06.05.) AI 보안이란 무엇인가요? (https://www.ibm.com/kr-ko/think/topics/ai-security)
- Techopedia. (February 2, 2024). Value of the artificial intelligence (AI) cybersecurity market worldwide from 2023 to 2030 (in billion U.S. dollars) [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/
- Techopedia. (July 2, 2025). Self-Healing Networks: AI's Role in Autonomous Cybersecurity
- Nutanix. (November 13, 2023). Key artificial intelligence (AI) application and infrastructure upgrade drivers in businesses worldwide as of 2023 [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1449087/drivers-of-ai-applications-infrastructure-upgrades/
- Tech.co. (January 3, 2024). Does your organization use artificial intelligence for the following purposes? [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1440900/us-organizations-use-of-ai-for-selected-purposes/
- Cybersecurity Insiders. (October 4, 2023). Which emerging AI and ML techniques hold the most promise for enhancing cybersecurity defenses? [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1425598/top-ai-and-ml-techniques-to-improve-cybersecurity/
- Verified Market Reports (Feburary, 2025) AI and Machine Leaing in Cybersecurity Market Insights
- Grand view research (2024.11.27.) AI In Cybersecurity Market Size, Share & Trend s Analysis Report By Type (Network Security, Endpoint Security), By Offering, By Technology (Machine Learning, Natural Language Processing), By Application, By Vertical, By Region, And Segment Forecasts, 2025 – 2030
- Market.us (2025.02) Global Agentic AI in Cybersecurity Market Size, Share, Statistics Analysis Report By Component (Solutions, Services), By Deployment Mode (Cloud-Based, On-Premises), By Application (Threat Detection and Response, Vulnerability Management, Others), By Industry Vertical (BFSI, IT & Telecom, Government, Healthcare, Retail, Others), Region and Companies - Industry Segment Outlook, Market Assessment, Competition Scenario, Trends and Forecast 2025-2034

본 보고서는 과학기술정보통신부에서 시행하는 연구개발지원단 육성·지원사업의 일환으로 과학기술정보통신부와 서울특별시의 지원을 받아 서울연구개발지원단(서울테크노파크 전략기획팀)에서 작성한 연구보고서입니다.

본 보고서는 글로벌 시장정보 전문업체(statista 등)에서 제공되는 내용을 기반으로 작성된 보고서로 서울연구개발지원단의 공식적 견해는 아님을 알려드립니다.

본 보고서는 서울과학기술정보시스템(https://www.stis.or.kr/)에서 다운로드 가능하며, 본 보고서의 내용을 인용할 경우 출처를 명시하여 주시기 바랍니다.

과학기술정보통신부 서울특별시 서울테크노파크 SEOULTECHNOPARK