2025.07

Vol.10

글로벌 시장동향보고서

사이버보안

(Cybersecurity)

과학기술정보통신부 서울특별시 서울테크노파크 SEOULTECHNOPARK

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

글로벌 시장동향보고서

사이버보안
(Cybersecurity)

목차

1. 개요

1.1 시장 정의

사이버보안(cybersecurity)은 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 및 개인 정보 보호(privacy)를 제공하고 유지하는 프로세스

- 사이버 보안은 사실상 모든 회사가 해결해야할 주제로 자동화된 프로세스, 클라우드 기반 도구 및 소프트웨어 지원 등 운영 활동의 성공적인 디지털 변환을 강화함
- 디지털 공격 및 중단(digital attacks and disruptions)과 같은 모든 사이버 범죄 사건을 예방하고 대응하기 위하여 컴퓨터 시스템, 네트워크, 프로그램 등에 대한 보호 조치 및 개인 자산 및 파일, 산업 및 정부 정보 등의 데이터 보호 조치가 포함됨
- 사이버 보안 시장은 인터넷 보급률 증가에 따라 확대될 것으로 예상되며, 디지털 기술의 발전과 함께 클라우드 컴퓨팅 인프라, 데이터 센터와 같은 가상화된 IT 환경의 확대에 따라 사이버 보안 시장의 성장도 가속화되고 있음
- 더욱이, 다양한 유형의 사이버 공격이 존재하여 기업과 운영, 매출, 그리고 직원에 대한 피해를 방지하기 위해 고유한 접근 방식을 요구하고 있으며, 사이버 위협의 심각성에 대한 인식이 높아지고 이에 대한 강력한 보호 필요성이 커짐에 따라 글로벌 사이버 보안 시장은 지난 몇 년간 성장세를 보임
- 이전에는 사이버 보안을 IT 부서의 업무로 부여하는 것이 일반적이었지만, 이제는 최고 전략 계획(top-level strategic planning)에서 더욱 핵심적인 역할을 하고 있음

사이버 보안은 크게 사이버 솔루션(cyber solutions)과 보안 서비스(security services) 두 가지 주요 시장으로 구분됨

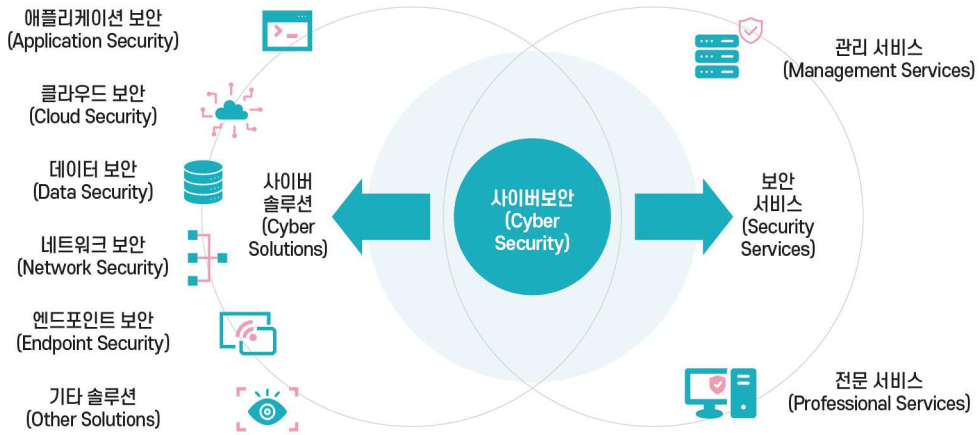
- 사이버 솔루션은 조직의 특정 사이버 보안 요구 사항에 맞춰 설계된 다양한 제품 또는 서비스를 의미하며, 조직의 위험 환경 및 보안 전략에 효과적으로 부합
- 보안 서비스는 피싱(phishing), 맬웨어(malware), 랜섬웨어(ransomware)와 같은 일반적인 사이버 범죄로부터 조직의 보호 및 보안 전략을 강화하는 포괄적인 처리 또는 광범위한 서비스를 의미

〈표 1〉 사이버보안 시장 범위

구분	내용
범위 내 (In scope)	• Cisco Security, SentinelOne, Check Point Software Technologies 등의 **보안 솔루션**(security solutions) • Secureworks, IMB Security Services, Rapid7 등 **사이버 보안 전문 관리 서비스**(professional and managed cybersecurity services) • CrowdStrike Services, Fortinet Professional Services, Symantec Professional Services 등의 **지원 및 구축**(support and deploy)

구분	내용
범위 외 (Out of scope)	• Quantum Corporation Backup and Recovery Solutions, HP Enterprise(HPE) Business Continuity and Recovery Services, IBM Resilience Services 등 **비즈니스 연속성**(business continuity) **및 재해 복구**(disaster recovery) • ADT Security Services, G4S Secure Solutions, Allied Universal 등의 **물리적 보안**(physical security) • **회사 내부 사이버 보안 조치**(company-internal cybersecurity measures)

출처 : Statista (2024)



출처 : Statista (2024)

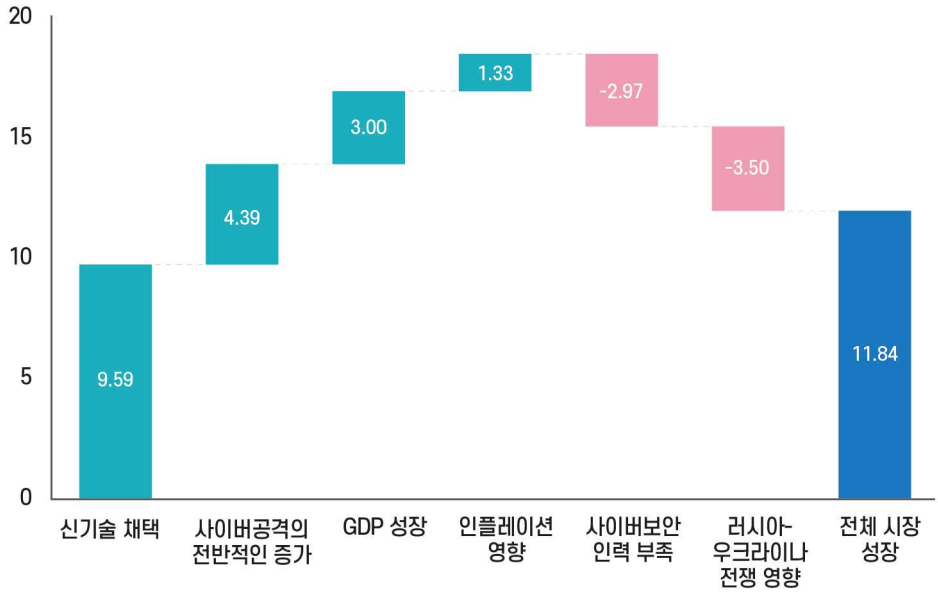
[그림 1] 사이버보안 시장 분류

1.2 시장 동인

» 새로운 기술의 빠른 도입은 2023년 글로벌 사이버보안 시장의 수익 변화에 가장 큰 영향을 미쳤으며, 사이버공격의 전반적인 증가와 새로운 기술 및 IT 투자는 사이버보안 시장을 성장하게 하는 주요 동인

- 사이버 공격의 증가, GDP 성장, 인플레이션 영향, 사이버 보안 노동력 부족 등이 사이버 보안 시장의 주요 동인
- 연간 실질 GDP의 백분율 변화로 추정되는 GDP 성장은 2023년 사이버보안 시장 성장에 약 3%의 영향을 미침
- 명목 GDP와 실질 GDP의 백분율 변화의 차이로 계산되는 인플레이션 영향은 2023년 사이버보안 시장 성장에 약 1.33%의 영향을 미쳤으며, 인플레이션이 상승하면 비용이 증가하여 조직에서 사이버 보안에 더 많은 지출을 하게 됨

- 러시아-우크라이나 전쟁으로 인해 글로벌 경제에 혼란이 오고 불확실성이 증가하여 IT 지출이 감소할 수 있어 해당 요인은 시장 성장에 -3.5% 정도의 영향을 미침
- 클라우드, AI/ML, 제로 트러스트 아키텍처, IoT, 빅데이터와 같은 신기술의 성장과 채택은 전 세계 기업에 상당한 이점을 제공하지만 사이버공격 위험도 증가시켜 사이버보안 시장 확장을 촉진하며, 2023년 사이버보안 시장 성장에 약 9.59%의 영향을 미침
- 사이버공격의 전반적인 증가는 사이버보안 시장의 성장을 가져오며 2023년 시장 성장의 약 4.39%의 영향을 미친 것으로 분석됨
- 사이버보안의 인력 부족은 최근 몇 년 동안 기업이 직면한 가장 심각한 문제 중 하나로 전문가 부족으로 인해 시장 성장이 -2.97%만큼 저해된 것으로 분석됨



출처 : Statista (2024)

[그림 2] 사이버보안 시장 영향 요인 (2023년)

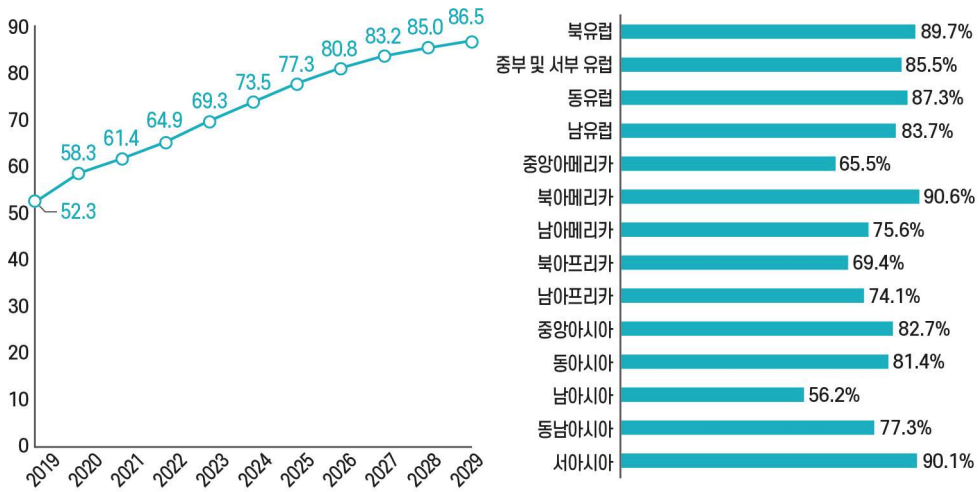
〈표 2〉 사이버보안 시장 동인

구분	내용
글로벌 지표 (Global indicators)	• 사이버보안 시장은 글로벌 경제 동향과 국가 경제 상황을 포함한 거시경제적 요인에 의해 영향을 받음 • 인터넷 보급률은 특히 주요 동인으로 작용하는데, 온라인 연결성이 증가함에 따라 다양한 부문에서 민감한 데이터와 중요한 인프라를 보호하기 위한 강력한 사이버보안 조치에 대한 수요가 증가하기 때문

구분	내용
IT 투자 (IT invesstment)	• 팬데믹 이후 기업들은 사이버공격이 증가하는 상황에 직면하였는데, 이는 주로 IT 시스템에 대한 의존도가 높아졌기 때문 • 원격작업과 관련된 취약성으로 인해 사이버 범죄자들이 활동을 확대하고, 점점 더 진보한 전술을 활용할 것으로 예상됨
하이브리드 및 멀티 클라우드로의 대대적인 전환 (A massive shift to hybrid and multi-cloud)	• 클라우드 데이터 스토리지의 중앙 집중화된 특성이 사이버 범죄자에게는 표적이 될 수 있어 보안은 여전히 중요한 문제로 남아있으며, 잠재적으로 데이터 침해 및 기타 사이버 공격의 위험을 증가시킬 수 있음
사이버공격 및 사이버위협의 증가 (Increase of cyberattacks/ The growth of cyber threats)	• 현대 사이버범죄는 전문적이고 고급 전술을 사용하여 취약점을 악용하며, 이는 기업, 정부 및 개인에게 상당한 과제를 안겨주지만 가까운 미래에는 개선되지 않을 전망
사이버전쟁 (Cyber warfare)	• 러시아-우크라이나 전쟁 이후 현대전은 전통적인 육지, 바다, 공중의 영역을 넘어 사이버공간까지 확대되고 있음

출처 : Statista (2024)

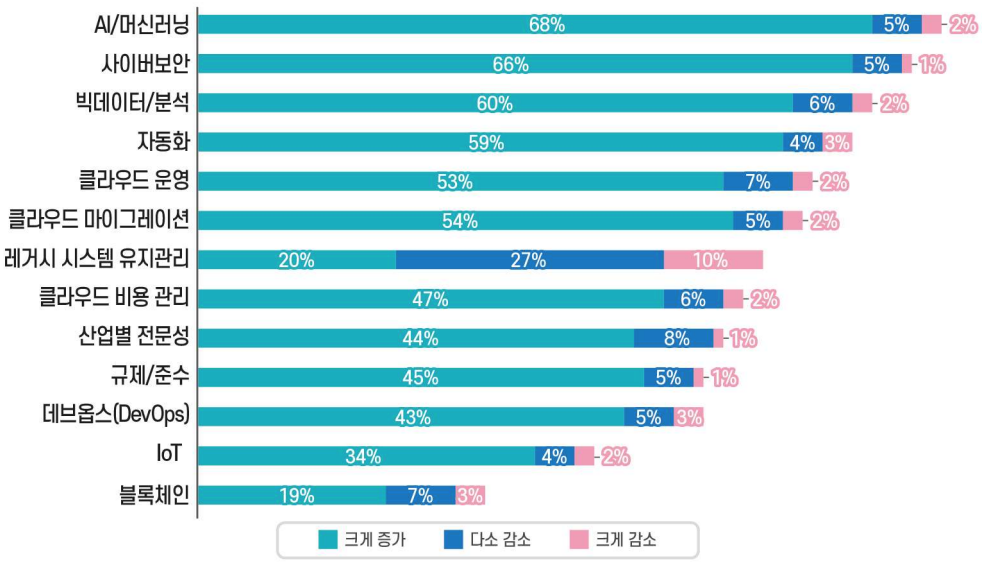
• 전 세계 인터넷 보급률은 완만하지만 일관적으로 증가 패턴을 보여주고 있으며, 사이버보안 시장은 개발도상국과 선진국에서 인터넷 보급이 확대됨에 따라 계속 성장하고 있음



출처 : Statista (2024)

[그림 3] 글로벌 인터넷 보급률 전망(2019~2029)(좌) 및 지역별 인터넷 보급률(2023년)

• 조직은 AI와 사이버 보안에 대한 투자를 중심으로 기술 예산을 재분배하고 있으며, 2023년 외부 IT 리소스 활용에서 사이버보안을 크게 증가시킬 예정이라는 응답이 66%로 집계됨



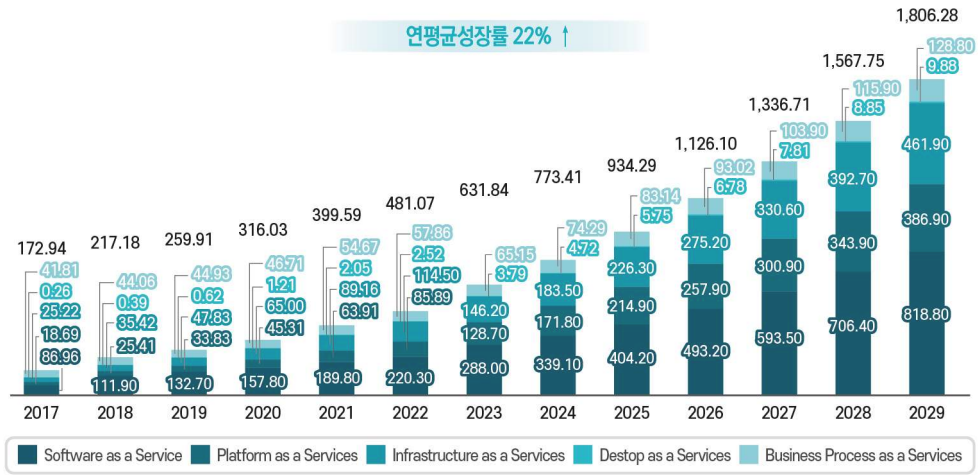
출처 : Statista (2024), Flexera 2023 재인용

※ 응답자 n=506

[그림 4] 외부 IT 리소스 활용 계획 변경 (2023년)

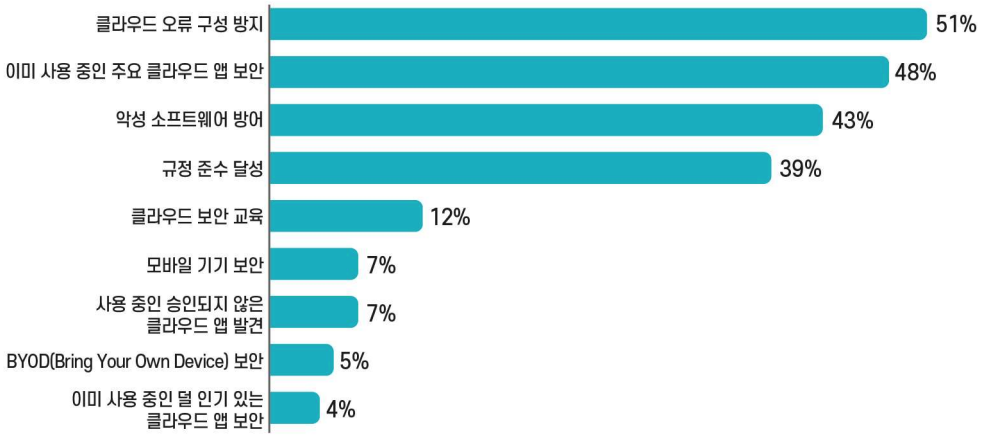
• 클라우드의 도입은 안정적으로 연간 성장하고 있으며, 2023년에는 클라우드 오류 구성 방지가 기업의 최우선 클라우드 보안 우선순위를 차지

(단위: 10억 US$)



출처 : Statista (2024)

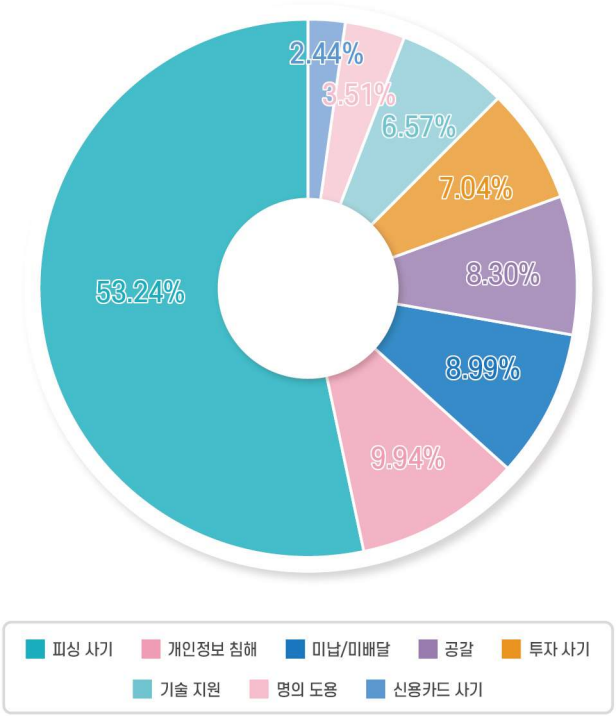
[그림 5] 글로벌 퍼블릭 클라우드 서비스 시장 수익 (2017~2029)



출처 : Statista (2024), Cybersecurity Insiders; Fortinet 재인용

[그림 6] 글로벌 클라우드 보안 우선순위 (2023년)

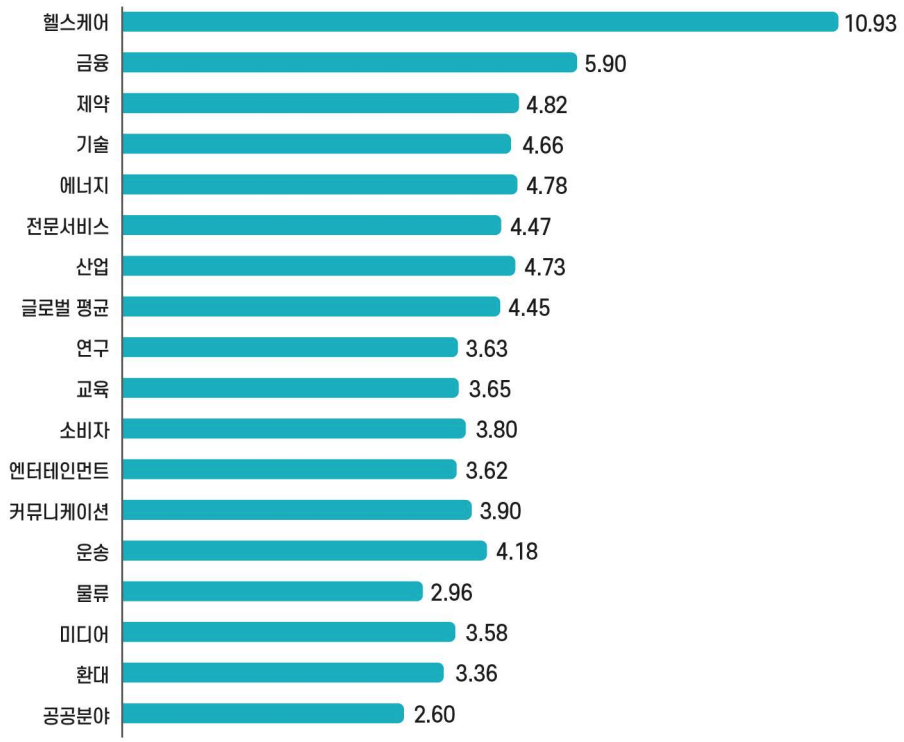
- 최근 몇 년 동안 온라인 활동에서의 팬데믹 급증으로 인해 범죄자들에게 사이버공격이 수익성 있는 수단으로 부상하였으며, 2023년 기준 피싱(phishing) 사기가 가장 빈번하게 일어남



출처 : Statista (2024)

[그림 7] 글로벌 사이버공격 점유율 (2023년)

• 다양한 산업군에서 사이버공격이 일어나고 있으며, 특히 헬스케어에서는 2022년~2023년 데이터 침해에 따른 평균 비용이 천만 달러를 상회함



출처 : Statista (2024), NordVPN 재인용

[그림 8] 산업별 글로벌 데이터 침해 평균 비용 (2022~2023)

• 사이버전쟁의 위협과 그로 인한 영향은 전 세계 정부와 군대에 큰 우려를 불러일으키고 있으며, 다양한 사이버전쟁 사건이 일어나고 있음

〈표 3〉 사이버전쟁 사건 (2015~)

2015	• 러시아 해커가 독인 연방의회의 컴퓨터 네트워크에 침투 • 중국 해커가 미국 재무부의 2,150만 건의 인사관리 기록을 훔침
2016	• 러시아가 우크라이나에 두 번째 정전을 유발
2017	• WannaCry : 랜섬웨어 Cryptowarm • Not Petya : 무기화된 랜섬웨어의 첫 번째 주요 사례
2018	• 34억 달러 상당의 비밀과 데이터가 훔쳐진 사건이 이란의 마브나(Mabna) 연구소와 관련이 있는 것으로 밝혀짐

2019	• 트럼프 행정부는 이란이 미국의 무인기를 격추한 것에 대하여 유조선 공격을 계획하는 데 사용된 혁명수비대(Revolutionary Guard' IRGC) 데이터베이스를 사이버 공격하는 것으로 보복
2020	• 러시아 정부의 지원을 받는 조직이 미국 연방 정부의 여러 부서를 포함하여 전 세계적으로 수천 개의 조직에 침투하여 데이터 침해
2021	• 2021년 후반 러시아 사이버 엔지니어로 의심되는 사람들이 우크라이나 에너지 및 IT 공급업체의 네트워크에 접근
2022	• 러시아의 우크라이나 침공
2023	• 우크라이나 해커가 러시아 정부 웹사이트를 3월과 10월 두 차례 훼손 • 로이터에 따르면 중국 해커들이 케나 정부 부서와 대통령실을 포함한 정부 기관을 표적으로 사이버공격을 시도 • 2023년 2월 우크라이나 공무원을 표적으로 삼은 사기성 피싱 공격이 국방부 이메일을 가장하여 우크라이나의 상황을 악용하고 러시아 활동에 대한 허위 정보 유출 • 2023년 3월 우크라이나 정부와 기반 시설을 겨냥한 치명적인 와이퍼(wiper) 공격이 발생하였으며, 이는 러시아 국영 해킹 단체인 샌드웜(Sandworm)의 소행으로 추정

출처 : Statista (2024)

2. 사이버보안 시장 현황 및 전망

2.1 글로벌 사이버 보안 시장 트렌드

» 사이버보안 시장에는 매년 새로운 트렌드가 등장하고 있으며, AI 및 머신러닝 기술, 제로 트러스트 모델, 사물 인터넷의 진화, 숙련된 전문가의 부족 등이 주요 트렌드

〈표 4〉 사이버보안 시장 동인

구분	내용
 AI 및 머신러닝 기술	• 인공지능과 머신러닝이 발전함에 따라 진화하는 사이버위협을 감지하고 대응하는 데 점점 더 중요한 역할을 하게 되었으며, 전반적으로 사이버보안이 크게 향상하는 데에 기여
 제로 트러스트 모델	• 증가하는 사이버공격에 대비하기 위한 보안 전략 수요가 증가하면서 수년간 제로 트러스트 보안 시장이 확대되었으며, 특히 2020년 초 COVID-19 팬데믹이 선포되었을 때 많은 기업이 원격 작업으로 전환하고 데이터를 클라우드에 저장함에 따라 시장이 번창함

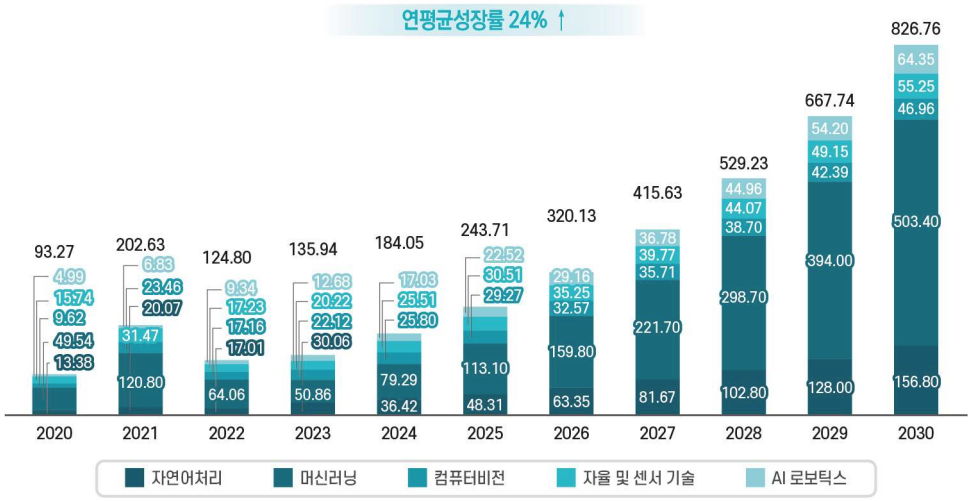
구분	내용
사물인터넷의 진화	• 2028년까지 전 세계적으로 200억 개가 넘는 IoT 연결 기기가 설치될 것으로 전망되며, 원격 근무 추세는 이러한 증가를 촉진시키는 요인 중 하나임. 사물인터넷(IoT)의 확장은 사이버범죄의 기회를 더욱 확대시킴
사이버보안 인력 부족	• 사이버보안 인력의 상당한 증가에도 불구하고, 글로벌 IT 산업은 350명이 넘는 인력 부족에 직면해 있으며, 이러한 지속적인 추세는 사이버보안 문제를 해결하고자 하는 조직에 심각한 과제가 됨

출처 : Statista (2024)

AI의 급속한 발전과 머신러닝의 광범위한 적용은 사이버위협에 대한 지속적인 모니터링 및 신속한 탐지의 자동화, 데이터 침해에 대한 효과적인 대응을 가능케 함

- AI 시장은 산업 전반에서 AI 기술이 증가함에 따라 2030년까지 상당한 성장과 발전을 이룰 것으로 예상됨

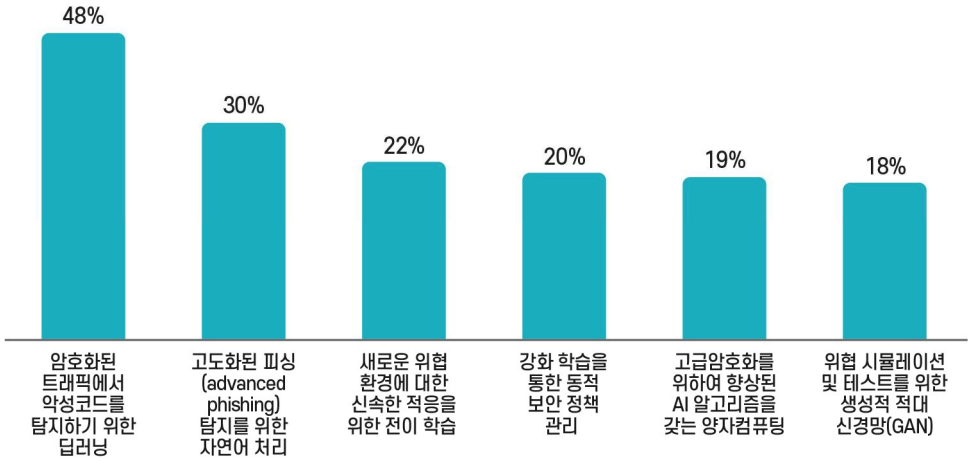
(단위: 10억 US$)



출처 : Statista (2024)

[그림 9] 글로벌 인공지능 수익 전망 (2020~2030)

- 2023년 설문조사결과에 따르면, 전 세계 응답자의 절반가량이 딥러닝을 사이버 보안 강화하는데 가장 유망한 신흥 AI 또는 머신러닝 기술로 꼽았으며, 이는 특히 암호화된 트래픽에서 맬웨어(malware)를 탐지하는 데 주목할 만함

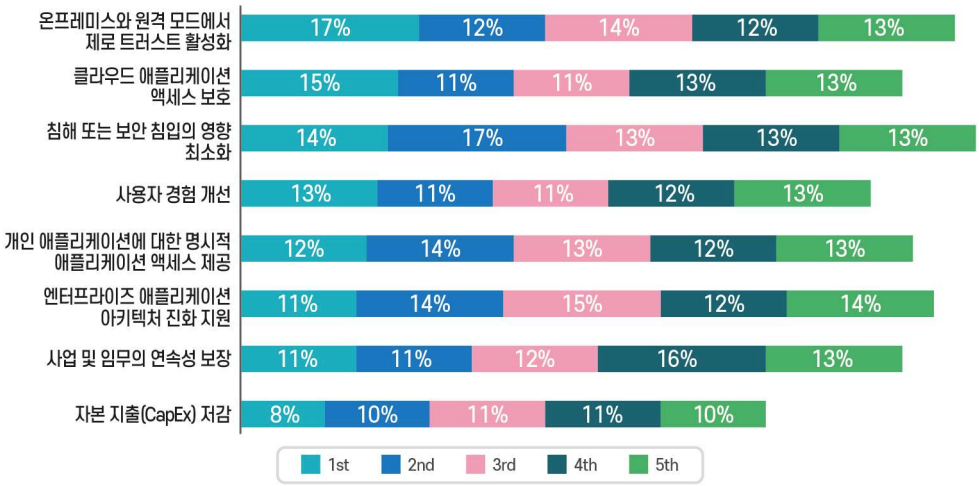


출처 : Statista (2024)

[그림 10] 사이버보안 강화를 위한 유망한 AI 및 머신러닝 기술 (2023년)

제로 트러스트는 데이터 손실을 줄이고 데이터 침해를 방지하는 효과적인 방법으로 여겨지고 있으며, 조직은 사이버보안 위험을 줄이기 위해 제로 트러스트를 수용 중

- '절대 신뢰하지 말고 항상 확인하라'는 핵심 원칙을 따르는 제로 트러스트는 조직 네트워크 내외부의 모든 사용자가 애플리케이션 및 데이터에 대한 액세스 권한을 부여받고 유지하기 전에 보안 구성 및 포스처에 대해 인증, 권한 부여 및 지속적으로 검증을 받아야 하는 보안 프레임워크
- 전 세계적으로 제로 트러스트의 최우선 순위는 침해 영향을 줄이고 온프레미스(on-premises)와 원격을 포함한 모든 환경에 제로 트러스트를 배포하는 것



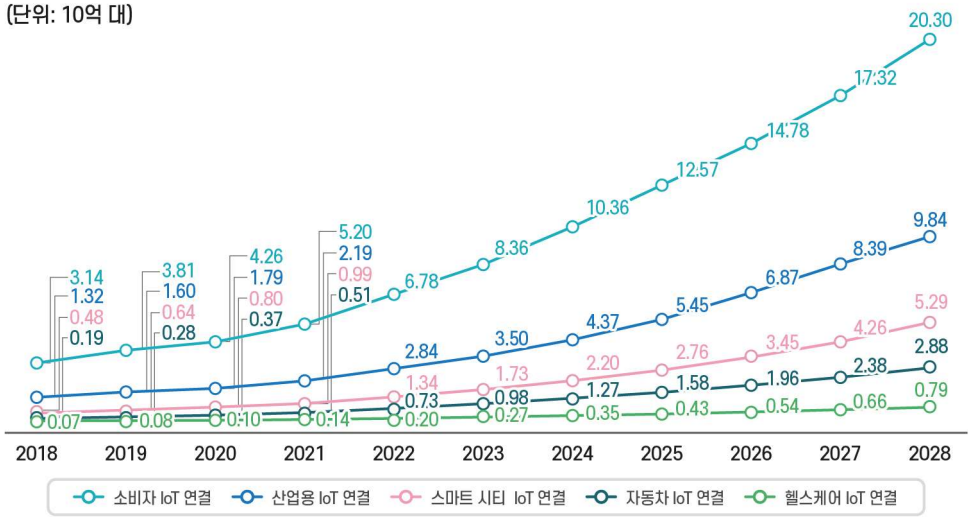
출처 : Statista (2024)

[그림 11] 글로벌 제로 트러스트 전략 우선순위 (2023년)

다양한 부문에서 사물인터넷(IoT) 기술과의 연결이 증가하고 있으며, IoT의 확대로 기업에 대한 사이버 공격이 급증하고, IoT 보안 시장이 발전하고 있음

- 광역 및 단거리 IoT 기술에 연결된 기기의 총 수는 2028년까지 급격히 증가할 것으로 전망되며, 특히 소비자 IoT 연결은 전 세계적으로 사물인터넷을 주도할 것으로 예상

(단위: 10억 대)

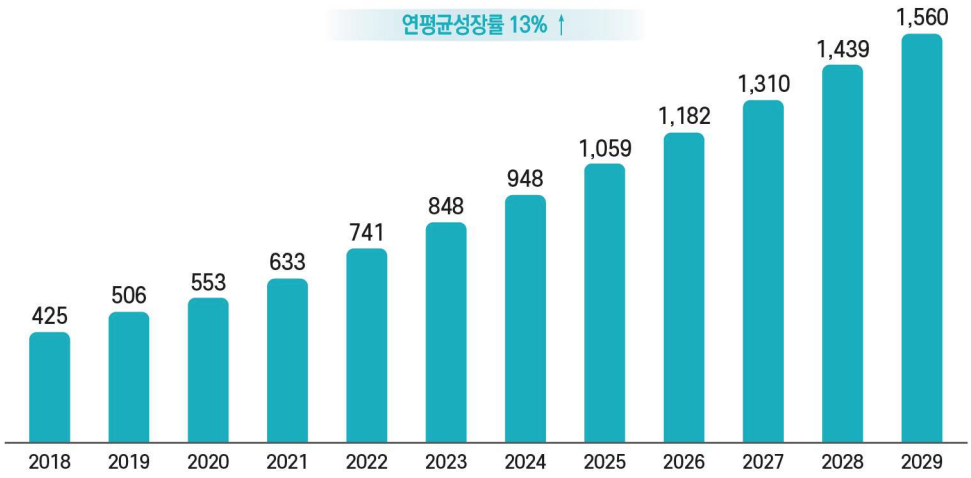


출처 : Statista (2024)

[그림 12] 글로벌 IoT 연결 수 (2018~2028)

- IoT는 지난 10년 동안 꾸준히 확대되어 왔으며, 2029년에는 1조 5,599억 달러 규모에 도달할 것으로 예상됨

(단위: 10억 US$)



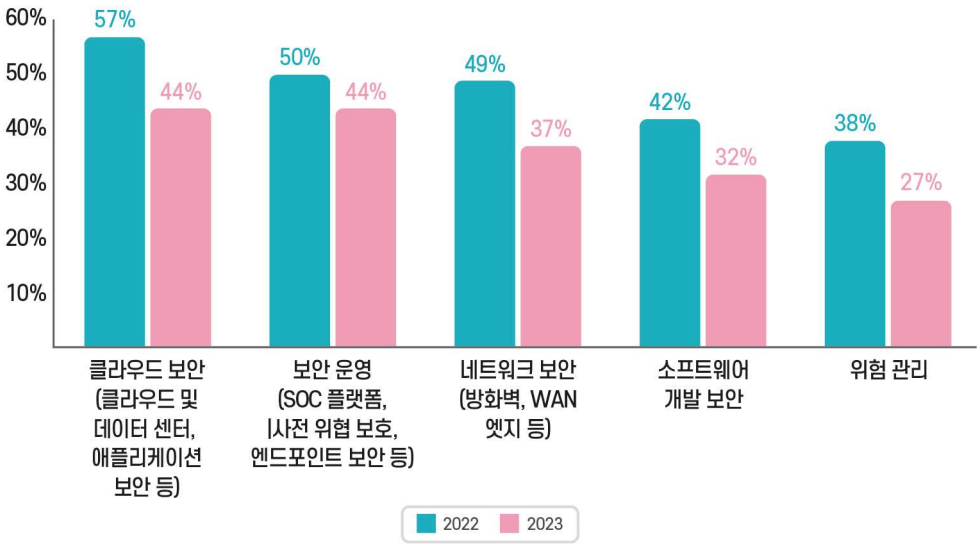
출처 : Statista (2024)

[그림 13] 글로벌 IoT 연간 수익 (2018~2029)

- IoT의 이러한 성장은 조직 내 사이버공격의 증가도 촉진시키므로 기업은 관련 정보 보안 정책 및 절차를 수립하고 연결된 기기에 대한 관행을 개선해야 하며, 사고에 대응하기 위해 기기를 보다 면밀히 모니터링하고 패치해야 함
- 기업 환경에서 IoT 기기에는 산업 기계, 스마트 에너지 네트워크, 빌딩 자동화, 직원 소유 IoT 기기 등이 포함되며, 이러한 모든 기기는 보안 위험을 초래할 수 있어 IoT 기기와 연결된 네트워크의 보안인 IoT 보안의 중요성이 커지고 있음

사이버보안 인식이 높아지고 있으나 사이버보안 인력은 점점 부족해지고 있으며, 전 세계적으로 채용이 가장 어려운 분야는 2023년 기준 클라우드 보안 및 보안 운영 분야로 나타남

- 조직 내에서 사이버범죄를 경험하는 경우가 매우 많고, 사이버보안 전문가의 57%가 보안 인력 부족으로 인하여 사이버보안 공격을 경험할 위험에 노출되어 있다고 응답
- 다양한 보안 및 IT 네트워크 관련 역할과 전문 분야에 대한 다양한 기술을 갖춘 인력을 모집하기 위해 노력이 필요하나 인재의 채용과 유지에 어려움을 겪는 상황
- 사이버 보안 인식 제고를 위한 교육 프로그램들이 시행되고 있으나, 여전히 필요한 지식이 부족하다고 느껴지고 있어 프로그램의 효과성에 대한 의문이 제기되고 있음
- 전 세계적으로 가장 인력이 부족하다고 느껴지는 분야는 클라우드 및 데이터 센터, 애플리케이션 보안 등을 포함하는 클라우드 보안 분야와 SOC 플랫폼, 사전 위협 보호, 엔트포인트 보안 등을 포함하는 보안 운영 분야



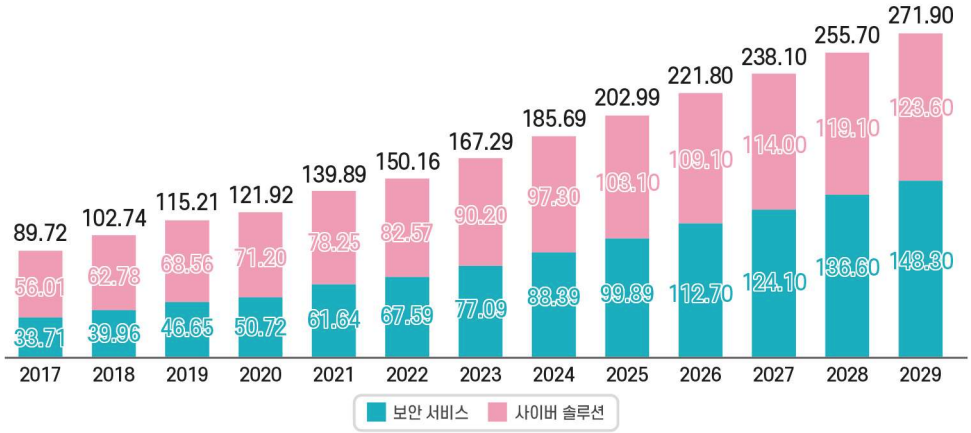
출처 : Statista (2024)

[그림 14] 전 세계적으로 채용이 가장 어려운 사이버보안 분야

2.2 글로벌 사이버보안 시장 규모

›› 글로벌 사이버보안 시장 규모는 2029년 2,719억 달러에 이를 것으로 예상되며, 2024년 기준 보안 서비스 시장이 사이버보안 시장을 지배

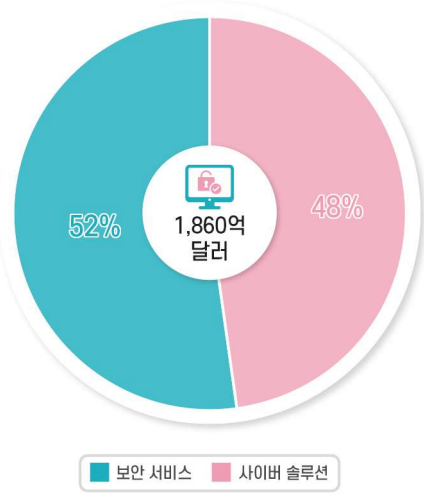
- 글로벌 사이버보안 시장은 2024년에 1,857억 달러 규모로 앞으로도 안정적인 성장세를 유지하며 2024년부터 2029년까지 연평균성장률 7.92%를 보이며 2029년에는 2,719억 달러의 시장 규모에 달할 것으로 전망



출처 : Statista (2024)

[그림 15] 글로벌 사이버보안 시장 규모 (2017~2029)

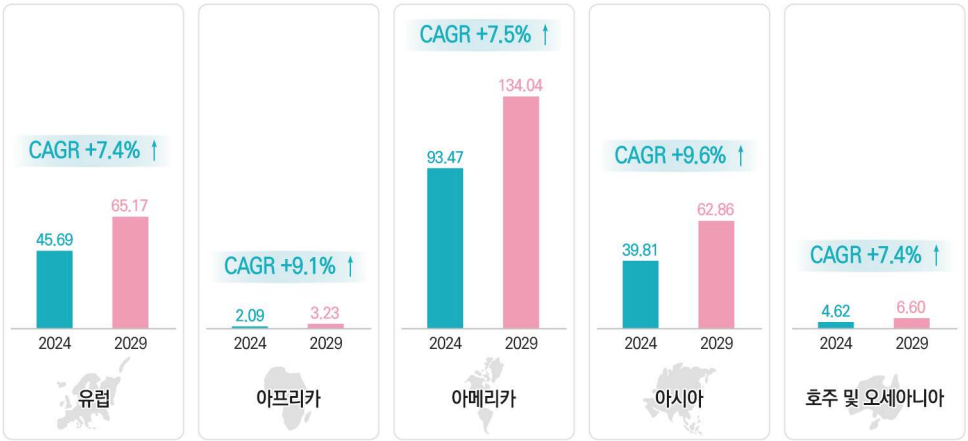
- 2024년 기준 보안 서비스는 973억 달러의 시장을 보이며 사이버보안 시장의 52%를 차지



출처 : Statista (2024)

[그림 16] 글로벌 사이버보안 시장 분야별 매출 점유율 (2024)

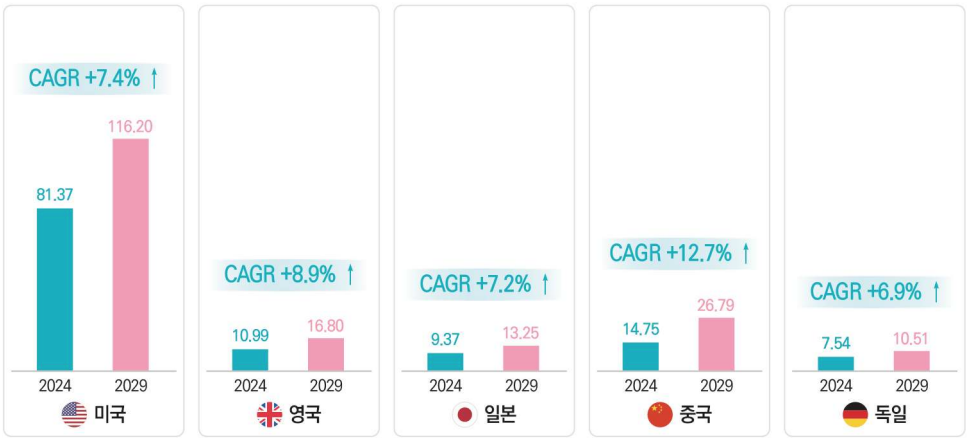
» 지역별로는 미주 지역이 2024년에 935억 달러 규모의 매출을 기록하며 가장 큰 시장으로 나타났으며, 국가별로는 미국이 매출 813억 달러로 2024년 분석 대상 국가 중 가장 큰 규모의 시장으로 나타남



출처 : Statista (2024)

[그림 17] 지역별 사이버보안 시장 규모 예측 (2024년 및 2029년)

- 미주 지역은 연평균성장률 7.5%로 2029년 1,340억 달러의 규모로 성장할 것으로 전망되며, 유럽이 7.4% 성장세를 보여 652억 달러, 아시아가 9.6%의 성장세를 보여 629억 달러의 규모에 달할 것으로 예측
- 국가별로는 미국이 813억 달러, 중국이 268억 달러로 2024년 사이버보안 시장에서 가장 높은 수익을 창출하였으며, 2029년까지의 연평균성장률은 중국이 12.7%로 가장 큰 성장률을 보일 것으로 전망

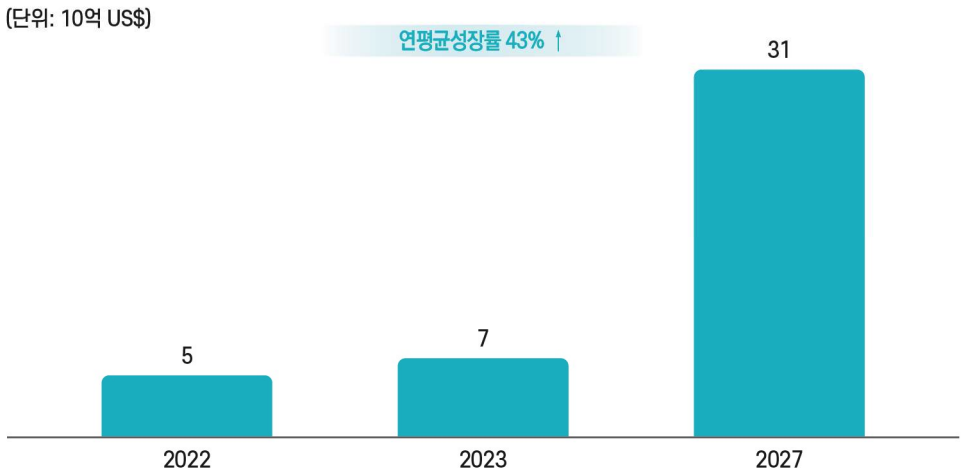


출처 : Statista (2024)

[그림 18] 주요국 사이버보안 시장 규모 예측 (2024년 및 2029년)

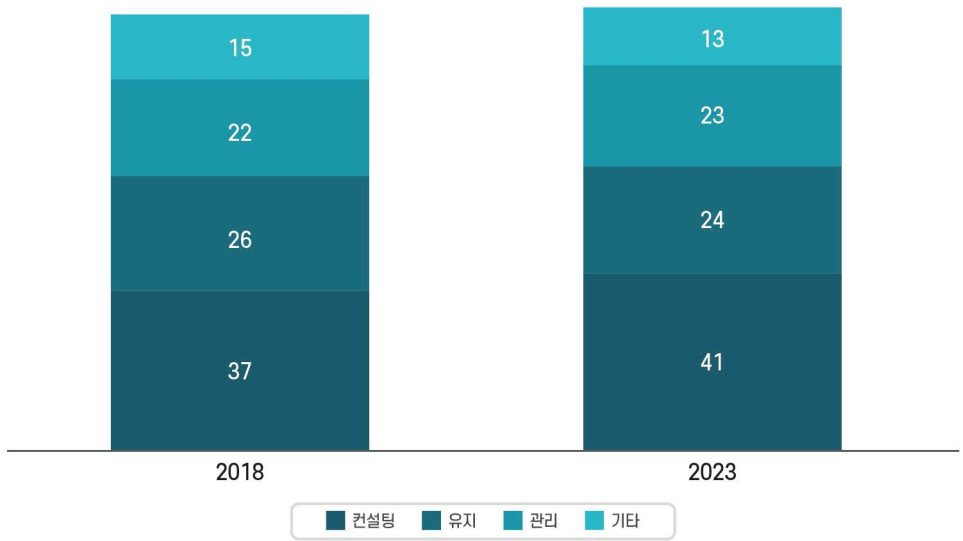
글로벌 IoT 보안 시장 규모는 2027년에 310억 달러에 도달할 것으로 예상되며, 2023년 기준 컨설팅 부문이 가장 많은 시장 점유율을 보임

- 글로벌 IoT 보안 시장 규모는 2022년 70억 달러에 달했으며, 2027년까지 연평균성장률 43%를 보이며 310억 달러 규모로 성장할 것으로 전망



출처 : Statista (2024), BRC (2023.01) 재인용

[그림 19] 글로벌 사물인터넷(IoT) 보안 시장 규모 (2022~2027)

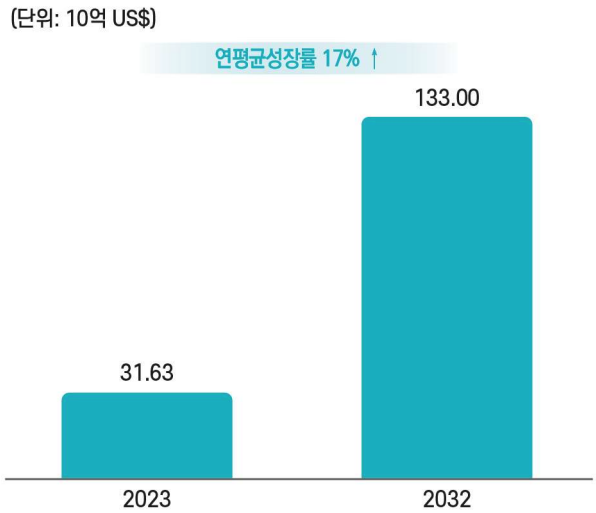


출처 : Statista (2024), BRC (2023.01) 재인용

[그림 20] 서비스 유형별 글로벌 IoT 보안 시장 점유율 (2018년 및 2023년)

글로벌 제로 트러스트 보안 시장의 가치는 2032년에 1,330억 달러에 달할 것으로 전망

- 제로 트러스트를 채택하면 비즈니스 사용자는 모든 환경 및 모든 기기에서 모든 애플리케이션과 안전하게 상호작용할 수 있으며, 이 모델은 COVID-10 팬데믹이 발발한 이후 비즈니스 혁신 이니셔티브의 클라우드 마이그레이션과 분산된 작업 환경의 가속화로 인해 극적으로 성장함
- 글로벌 제로 트러스트 시장 규모는 2023년 316억 달러에 달했으며, 2032년까지 연평균 성장률 17%를 보이며 1,330억 달러 규모로 성장할 것으로 전망



출처 : Statista (2024)

[그림 21] 글로벌 제로 트러스트 보안 시장 규모 (2023년 및 2032년)

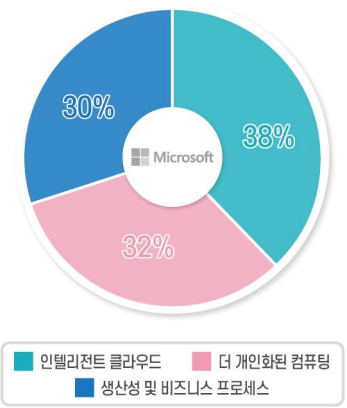
3. 주요 기업

3.1 Microsoft

퍼블릭, 프라이빗, 하이브리드 서버 제품과 클라우드 서비스를 포함하는 Microsoft의 인텔리전트 클라우드 부문은 2023년 총 매출의 35%를 차지

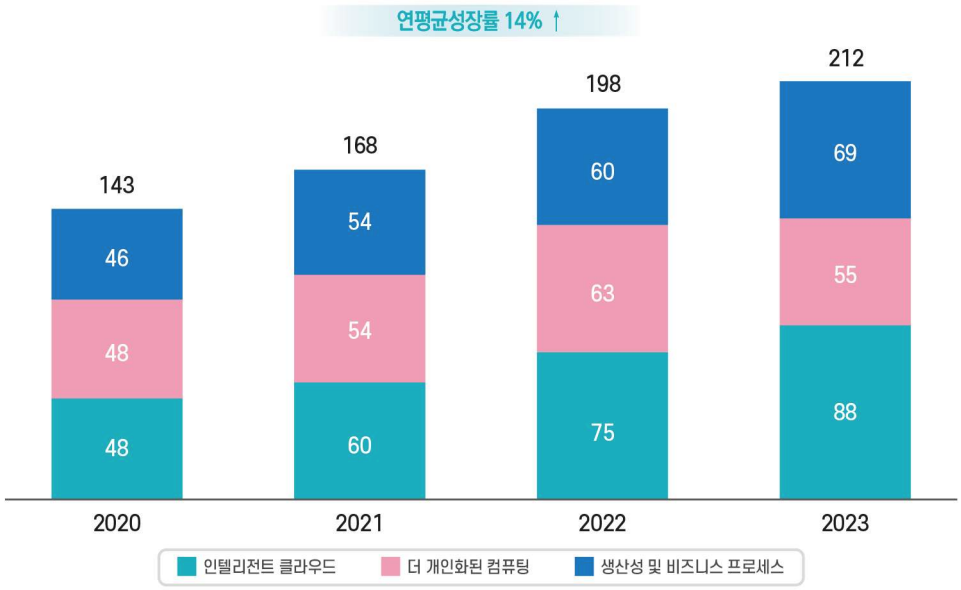
- Microsoft는 소프트웨어, 서비스, 기기 및 솔루션의 개발 및 지원에 참여하며, 생산성 및 비즈니스 프로세스(business process), 인텔리전트 클라우드(intelligent cloud), 그리고 더 개인화된 컴퓨팅(More Personal Computing)이라는 사업 부문을 통해 운영

〈표 5〉 Microsoft 기업 개요 (2023년 기준)

구분	내용	2023년 부문별 수익 점유율
주요 산업	기술 및 통신	
본사	레드먼드, 미국 (Redmond, U.S.)	
2023년 수익	2,120억 US$	
2023년 직원	221,000 명	
2023년 직원당 매출	96만 US$	

출처 : Statista (2024)

- 2020년부터 2023년까지 Microsoft의 글로벌 수익 규모는 연평균성장률 14%를 기록하며 2023년 2,120억 달러를 돌파하였으며, 인텔리전트 클라우드 부문은 2023년 880억 달러의 수익을 창출



출처 : Statista (2024)

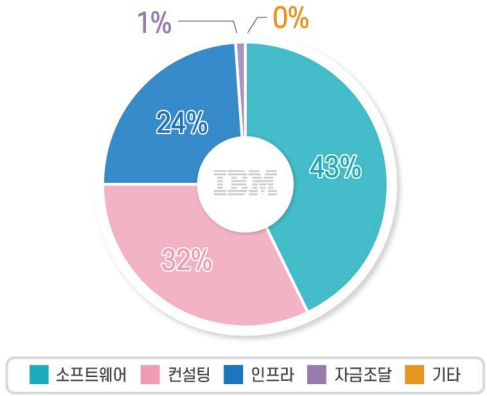
[그림 22] Microsoft 글로벌 수익 규모 (2020~2023)

3.2 IBM

IBM의 사업 부문 중 소프트웨어는 2023년 전체 매출의 43%를 차지했으며, 컨설팅 부문은 32%, 인프라 부문은 24%를 차지

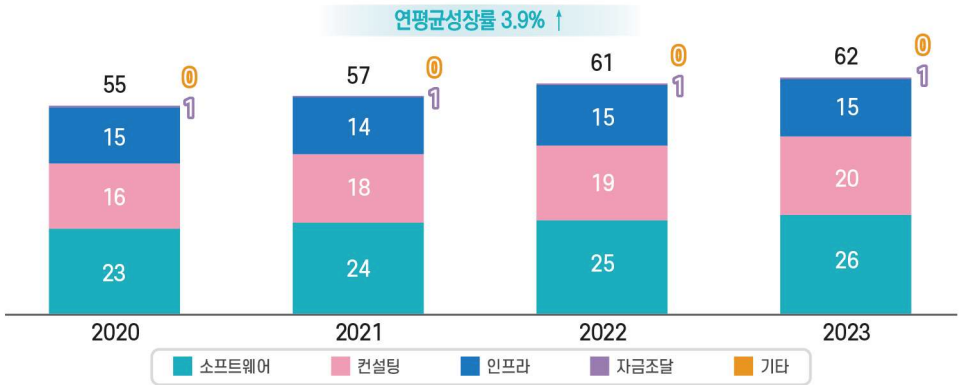
- IBM은 정보 기술과 비즈니스 프로세스에 대한 지식을 활용하는 통합 솔루션을 제공하는 정보 기술 회사로, 하이브리드 클라우드 플랫폼 및 소프트웨어 솔루션, 비즈니스 자동화 소프트웨어, AIOps 및 관리, 통합, 보안 소프트웨어 및 위협, 데이터 및 ID 서비스를 제공하는 소프트웨어 부문이 매출의 가장 많은 부분을 차지

〈표 5〉 IBM 기업 개요 (2023년 기준)

구분	내용	2023년 부문별 수익 점유율
주요 산업	기술 및 통신	
본사	아몬크, 미국 (Armonk, U.S.)	
2023년 수익	620억 US$	
2023년 직원	282,200 명	
2023년 직원당 매출	22만 US$	

출처 : Statista (2024)

- 2020년부터 2023년까지 IBM의 글로벌 수익 규모는 연평균성장률 3.9%를 기록하며 2023년 620억 달러를 돌파하였으며, 인텔리전트 클라우드 부문은 2023년 880억 달러의 수익을 창출



출처 : Statista (2024)

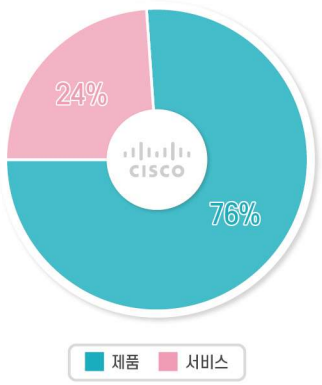
[그림 23] IBM 글로벌 수익 규모 (2020~2023)

3.3 Cisco

Cisco의 사업 부문 중 스위치, 라우터, 방화벽 및 소프트웨어 정의 네트워킹(SDN) 솔루션을 포함한 제품 부문은 2023년 전체 매출의 76%를 차지

- Cisco Systems Inc(Cisco)는 네트워킹, 보안, 협업, 애플리케이션 및 클라우드 전반에 걸쳐 의도 기반 기술을 통합하는 기업
- 제품들은 가상 LAN(VLAN), 보안 영역, 액세스 제어 목록(ACL) 및 기타 세분화 기술을 만드는 데 사용할 수 있으며, 서비스 부문은 조직이 네트워크 세분화를 수행할 수 있도록 돕는 네트워크 세분화 솔루션 컨설팅, 설계, 구현 및 관리 등을 포함

〈표 6〉 Cisco 기업 개요 (2023년 기준)

구분	내용	2023년 부문별 수익 점유율
주요 산업	컴퓨터, 주변 장비 및 소프트웨어	
본사	샌호세, 미국 (San Jose, U.S.)	
2023년 수익	570억 US$	
2023년 직원	84,899 명	
2023년 직원당 매출	67만 US$	

출처 : Statista (2024)

- 2020년부터 2023년까지 Cisco의 글로벌 수익 규모는 연평균성장률 5.0%를 기록하며 2023년 570억 달러를 돌파하였으며, 제품 부문은 2023년 430억 달러의 수익을 창출

출처 : Statista (2024)

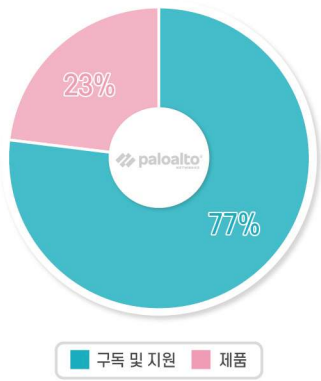
[그림 24] Cisco 글로벌 수익 규모 (2020~2023)

3.4 Palo Alto Networks

Palo Alto Networks의 사업 부문 중 구독 및 지원이 2023년 기준 50억 달러 규모로 전체 매출의 77%를 차지

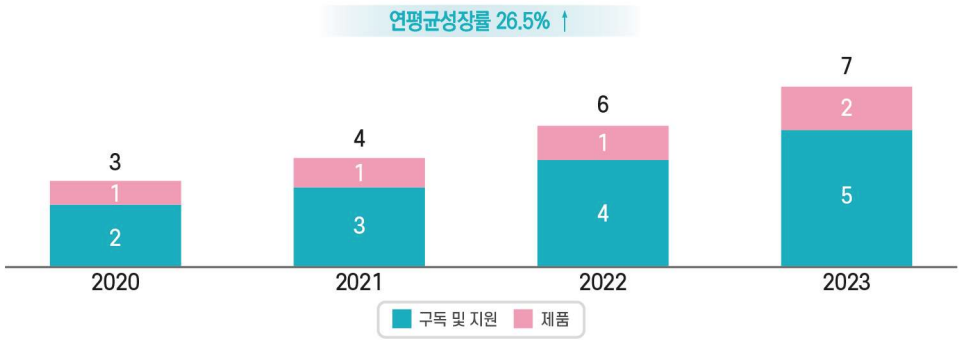
- Palo Alto Networks는 기업, 정부 및 서비스 제공업체에 사이버보안 서비스를 제공하는 기업으로 제품 및 서비스 포트 폴리오에는 방화벽 어플라이언스 및 소프트웨어, 지원 및 유지 관리 서비스, 보안 관리 솔루션, 가상 시스템 업그레이드 등이 포함
- 구독 상품에는 위협 방지 구독, URL 필터링, IoT 보안, DNS 보안, WildFire, GlobalProtect, 데이터 손실 방지 및 SD-WAN 등이 포함

〈표 7〉 Palo Alto Networks 기업 개요 (2023년 기준)

구분	내용	2023년 부문별 수익 점유율
주요 산업	컴퓨터 프로그래밍	
본사	산타클라라, 미국 (Santa Clara, U.S.)	
2023년 수익	70억 US$	
2023년 직원	13,948 명	
2023년 직원당 매출	49만 US$	

출처 : Statista (2024)

- 2020년부터 2023년까지 Palo Alto Networks의 글로벌 수익 규모는 연평균성장률 26.5%를 기록하며 2023년 70억 달러를 돌파



출처 : Statista (2024)

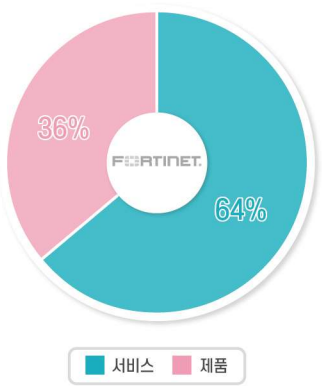
[그림 25] Palo Alto Networks 글로벌 수익 규모 (2020~2023)

3.5 Fortinet

Fortinet의 서비스 수익은 주로 FortiGuard 보안 구독 및 FortiCare 기술 지원에서 발생하며, 2023년 전체 매출의 64%가 제품 부문에서 발생

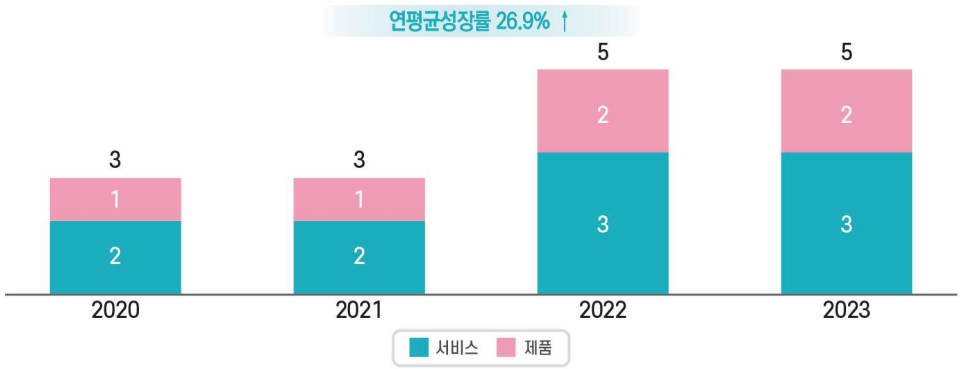
- Fortinet은 중소기업, 대기업 및 정부 기관에 제품, 지원 및 서비스를 판매하는 사이버보안 공급업체로 네트워크 보안 어플라이언스, 소프트웨어 및 구독 서비스를 제공
- Fortinet의 시스템은 방화벽, VPN, 바이러스 백신, 침입 방지(IPS), 웹 필터링, 스팸 방지 및 트래픽 셰이핑을 포함한 업계에서 가장 광범위한 보안 기술을 통합

〈표 8〉 Fortinet 기업 개요 (2023년 기준)

구분	내용	2023년 부문별 수익 점유율
주요 산업	컴퓨터 및 주변 장비	
본사	서니베일, 미국 (Sunnyvale, U.S.)	
2023년 수익	53억 US$	
2023년 직원	13,568 명	
2023년 직원당 매출	39만 US$	

출처 : Statista (2024)

- 2020년부터 2023년까지 Fortinet의 글로벌 수익 규모는 연평균성장률 26.9%를 기록하며 2023년 40억 달러를 돌파하였으며, 서비스 부문은 2023년 30억 달러의 수익을 창출



출처 : Statista (2024)

[그림 26] Fortinet 글로벌 수익 규모 (2020~2023)

참고문헌

- Statista. (2024.08). Cyber security : market data & analysis