

2022 년에도 지속될 사이버 보안 위협

기관, 소비자 및 데이터를 노리는 사이버 범죄자 사이의 쫓고 쫓기는 게임이 올해에는 더 심해질 것으로 예상됩니다. 최근에는 전 세계 수억 개의 시스템에 피해를 줄 수 있는 Log4j 로 알려진 인터넷 소프트웨어의 취약점에 대한 우려가 있었습니다. 미국 동부 전역에 위치한 Colonial Pipeline 의 연료 공급을 위태롭게 했던 랜섬웨어 공격과 같은 위협을 비롯해 2021년에는 세간의 이목을 끄는 여러 건의 침해가 있었습니다. 이와 같은 사이버 사건은 더 자주 발생하고 있으며 그에 따른 손해도 커지고 있는데, 특히 주요 인프라 및 공급망에 대한 공격의 경우 더욱 그렇습니다. 글로벌 경제가 계속 온라인으로 이동함에 따라 위협의 수준은 더 심각해지고 있으며 종종 민감한 데이터가 노출될 위험에 처하곤 했습니다. 이에 대한 결과로 사이버 보안에 대한 인식이 높아지고 보안에 대한 지출이 늘어나면서 장기적으로 사이버 보안 테마는 순풍을 맞을 것으로 예상합니다.

주요 요약:

- 2021 년에 사이버 공격이 만연하여 상당한 규모의 피해가 발생하였으며 이러한 추세는 2022 년에도 계속될 가능성이 있습니다. 평균 데이터 침해 비용이 2020 년 386 만 달러에서 2021 년 424 만 달러로 증가하였는데, 이는 IBM 이 데이터 침해 비용 보고서 2021 에서 발표한 바와 같이 17 년 중에서 가장 높은 총비용입니다.ⁱ
- 기업, 정부 및 소비자는 사이버 보안에 대한 노력을 기울이고 있으며 소비자 역시 자신을 보호하기 위한 조치를 취하고 있습니다. 기업은 2022 년에 1,720 억 달러를 지출할 것으로 예상됩니다.ⁱⁱ
- 사이버 보안은 ID, 네트워크 및 엔드포인트 보안에 지속적으로 중점을 두고 이루어 질 것으로 보이며 이 중에서도 네트워크 보안이 2021 년과 2026 년 사이에 24%로 가장 빠르게 성장할 것으로 예상됩니다.ⁱⁱⁱ

2021 년에 취약점이 드러난 디지털 세계

현재 세계적으로 매일 약 250 경 바이트의 데이터가 생성되고 있습니다.^{iv} 따라서 해커 입장에서는 그 어느 때보다 민감한 데이터에 진입할 수 있는 여지가 많으며 세계가 계속 디지털화되고 데이터 양이 증가함에 따라 더 많은 기회가 생길 것입니다. 특히 사물인터넷(IoT) 기기가 데이터 풀이 커지는 데 있어 큰 역할을 하게 될 것입니다. 2021 년 말 기준으로 커넥티드 기기는 146 억 대였습니다.^v 2022 년 그 수는 거의 18% 증가하고 2027 년까지 두 배 이상이 될 가능성이 있습니다.^{vi}

작성자:
Pedro Palandrani 및
Alec Lucas

날짜: 2022 년 1 월 24 일
주제: 테마



경제가 재택근무로 바뀌고 있는 점 역시 사이버 범죄자들에게는 상당한 기회가 되고 있습니다. 2021년 미국에서 팬데믹으로 인해 도입되었던 봉쇄조치가 완화되었지만 정규직의 45%는 최소 일부 시간 동안 아직도 가정에서 계속 근무하고 있습니다.^{vii} 새로운 변이 때문이든 직원이 선호하기 때문이든, 재택근무 이니셔티브는 계속될 가능성이 있어 가까운 장래에 데이터가 취약해질 위험에 놓일 수 있습니다. IBM 보고서에 의하면 2021년 원격 근무에 의한 데이터 침해가 보고 건수의 17.5%를 차지하였습니다.^{viii} 이러한 침해의 평균 비용 역시 원격 근무가 실시되기 전에 비해 16.6% 증가하였습니다.^{ix}

2021년, 잘 알려진 일부 기업들이 사이버 공격의 희생양이 되어 상당한 규모의 피해를 입었습니다. Colonial Pipeline에 대한 랜섬웨어 공격으로 인해 공격자들에게 4백만 달러를 지급해야 했습니다.^x CNA Financial은 해커들에게 4천만 달러를 지급하고 회사의 접근이 차단되었던 디지털 인프라의 일부에 대한 암호를 풀었습니다.^{xi} 세계 최대의 육류 가공업체인 JBS는 사이버 공격으로 공장 여러 곳을 폐쇄했습니다.^{xii} 이러한 사례는 지난해 회사를 상대로 수백만 달러의 손실을 입었던 주요 공격 중 일부에 불과합니다.

2021년 주요 사이버 공격	산업	날짜	지급 또는 요청 금액(백만)
Microsoft Exchange	기술	2021년 1월 5일	\$50.00*
기아자동차	자동차	2021년 2월 13일	\$20.00*
Bombardier	제조(항공)	2021년 2월 23일	
CNA Financial	금융	2021년 3월 21일	\$40.00
Harris Federation	교육	2021년 3월 29일	8.00*
Colonial Pipeline	에너지	2021년 3월 7일	\$4.40
Brenntag	화학	2021년 5월 11일	\$4.40
JBS	식품	2021년 5월 30일	\$11.00
Kaseya	정보 기술	2021년 7월 2일	\$70.00*
Accenture	기술	2021년 8월 12일	\$50.00*
Acer	기술	2021년 10월 5일	\$50.00*

*요청 받았으나 전액 지급하지 않음.



최근의 공격으로 인해 늘어나는 사이버 보안 지출

최첨단 솔루션이라 해도 모든 취약점을 제거하는 것은 불가능하겠지만 많은 위협을 막고 최악의 결과는 피할 수 있습니다. 2021 년 기업, 미국 정부와 소비자들의 사이버 위협에 대한 의식이 높아졌으며 이들 모두 예방 조치에 대해 더 많은 노력을 기울였습니다.

- **기업:** 랜섬웨어 공격의 희생양, 그들의 공급업체, 고객 및 경쟁사들은 보안 침해로 인해 발생할 수 있는 혼란을 이해하고 있습니다. 피해액은 종종 적절한 솔루션에 대한 투자 비용을 능가합니다. 통상적으로 대기업은 매년 사이버 보안에 2~5 백만 달러를 지출하는 반면에 단일 랜섬웨어 침해로 인해 회사가 입는 비용은 평균 462 만 달러에 달합니다.^{xiii,xiv} 이러한 비용 때문에 3,000 명 이상의 임원을 대상으로 실시한 최근의 설문조사에서 응답자의 69%가 2022년에는 사이버 보안 지출이 늘어날 것으로 예상했습니다.^{xv} 한 추정에 따르면, 데이터 보호 및 리스크 관리에 대한 지출이 2021년부터 11% 증가하여 2022년에 1억 7,200만 달러에 이를 것이라고 합니다.^{xvi}
- **정부:** 2021년 5월, 바이든 대통령은 연방 사이버 보안 역량을 현대화하고 사이버 공격에 대한 대응 전략을 표준화하며 정부 계약업체에 대한 정보 공유 요건을 강화하려는 목적의 행정명령에 서명했습니다. 그후 7월, 바이든 대통령은 전력, 용수 및 교통과 같은 중요 인프라에 대한 사이버 공격을 막기 위한 국가 보안 각서에 서명했습니다. 이러한 조치는 인프라 투자 및 일자리 법에서 실제 지출로 반영되었습니다. 동 법은 국가의 사이버 보안을 개선하기 위해 17억 달러의 전용 지출 및 약 70억 달러의 예비 지출을 담고 있습니다.^{xvii}

또한 지난해, 상원은 백악관의 첫 국가 사이버 국장 임명을 만장일치로 인준했습니다. 의회는 2021년 국가방위수권법의 일환으로 이 자리를 신설하였는데, 이는 앞으로 행정부 내에서 사이버 보안에 더욱 중점을 두겠다는 신호입니다.

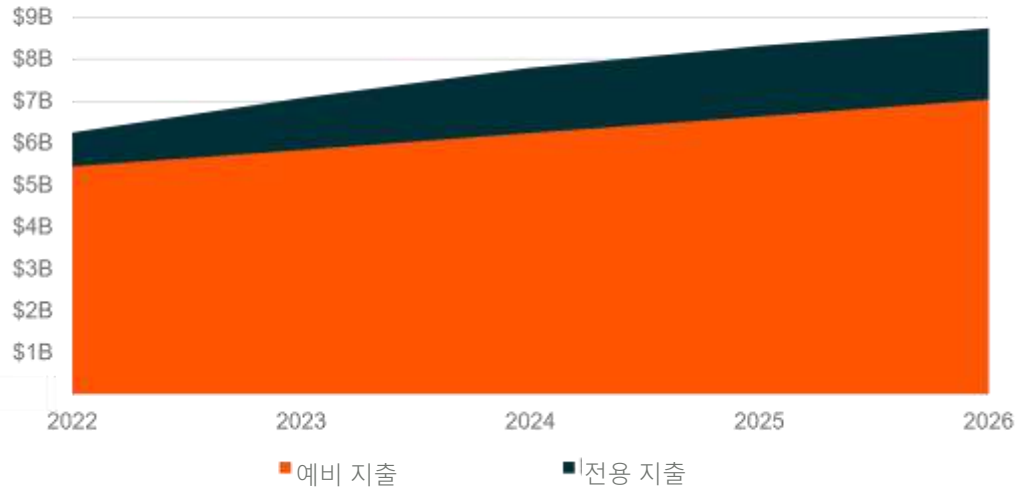
전용 및 예비 사이버 보안 지출에 거의 90억 달러를 승인한 최근 미국 인프라 법안

인프라 투자 및 일자리 법이 승인한 전용 및 예비 사이버 보안 지출(단위: \$10억)



THE RECENT U.S. INFRASTRUCTURE BILL AUTHORIZES ALMOST \$9B IN DEDICATED & POTENTIAL CYBERSECURITY SPENDING

DEDICATED & POTENTIAL CYBERSECURITY SPENDING AUTHORIZED BY INFRASTRUCTURE INVESTMENT AND JOBS ACT (\$ BILLIONS)



출처: 117 차 의회(2021-2022 년), "H.R. 3684 - 인프라 투자 및 일자리 법", 2021 년 6 월, Global X 분석.

- 소비자:** 소비자는 사이버 보안 지출 중에서 적지만 점점 커지고 있는 부분을 차지하고 있습니다. 소비자의 약 53%가 최소 한번은 사이버 범죄를 당한 경험이 있기 때문에 많은 사람들이 개인 VPN, 이중 요소 인증, ID 도난 방지 서비스와 같은 예방책을 취하고 있습니다.^{xviii} 팬데믹으로 소비자들이 온라인에서 사용하는 시간이 늘어남에 따라 대담해진 사기꾼들이 이를 이용하면서 개인에 대한 위협이 악화되었습니다. 2021 년 10 월 기준으로 미국인은 코로나 관련 사기로 인해 5 억 8,600 만 달러를 잃었습니다.^{xix} 하지만 소비자들은 높아진 위협에 대해 인지하고 있습니다. 지난해, 성인의 거의 40%가 팬데믹으로 활발해진 온라인 활동을 보호하기 위한 조치를 취했습니다.^{xx} 팬데믹 기간 동안 습득한 이와 같은 디지털 보안 습관은 소비자들의 사이버 보안 서비스 채택을 가속화할 수 있습니다.

주시해야 할 주요 사이버 보안 분야

- ID 보안:** 원격 근무가 폭발적으로 늘어나면서 중요한 데이터, 자원 및 앱에 접속하는 사람들에게 대한 보안 확보는 기관 입장에서는 필수 사항입니다. 이러한 수직적인 사이버 보안 하위 부문에는 ID 및 접속 관리(Identity and Access Management, IAM), 특전 계정 관리(Privileged Account Management, PAM), ID 거버넌스 및 관리(Identity Governance & Administration, IGA)가 포함됩니다. 이러한 하위 부문은 2021 년과 2026 년 사이에 연평균 19% 성장하리라 예상됩니다.^{xxi}
- 네트워크 보안:** 이 수직적 하위 부문에 속하는 회사들은 네트워크의 완벽성, 기밀성 및 오용 또는 침해로부터의 접근 가능성을 보호할 책임을 집니다. 네트워크에 대한 접근을 과도하게 허용한



상태에서 한 개인이 위험에 빠지면 사이버 공격이 수평으로 퍼지게 됩니다(즉, 사용자에서 사용자로). 예를 들어, 제로 트러스트 네트워크(Zero Trust Network)는 회사의 네트워크에 연결하거나 사용자들을 인터넷에 노출시킬 필요 없이도 사용자들에게 내부 앱 접속권한을 제공합니다. 이러한 수직적인 사이버 보안 하위 부문에는 제로 트러스트 네트워크 액세스(ZTNA), 소프트웨어 정의 네트워킹(SDWAN), 네트워크 탐지 및 대응(NDR), 방화벽/NGFW/통합 위협 관리(UTM), 안전한 액세스 안전한 예지(SASE)가 포함됩니다. 이러한 하위 부문은 2021 년과 2026 년 사이에 연평균 24% 성장하리라 예상됩니다.^{xxii}

- 엔드포인트 보안:** 인터넷으로 연결된 아주 많은 기기들은 해커들에게는 새로운 진입점으로 작용하여 회사와 개인 입장에서 보안을 효과적으로 관리하기가 어려워지고 복잡해졌습니다. 사물인터넷을 성공적으로 배치하기 위해서는 전면에 설치된 보안 요건에서부터 지속적인 관리와 기계가 산출하는 민감한 데이터의 보호에 이르는 엔드 투 엔드 보안이 필요합니다. 이러한 수직적인 사이버 보안 하위 부문에는 엔드포인트 보호 플랫폼(EPP), 엔드포인트 탐지 및 대응(EDR), 데이터 분실 방지(DLP)가 포함됩니다. 수직적 엔드포인트 보안은 대체로 2021 년과 2026 년 사이에 연평균 8% 성장하리라 예상됩니다.^{xxiii}

이러한 주요 분야 외에, 사이버 보안 회사들은 점점 더 통합을 고려하고 있습니다. 일반적으로 사이버 보안 제공업체는 제한적인 제품에 특화되어 있으므로 고객은 여러 제공업체들을 이용하여 자신의 데이터를 지켜야 합니다. 이러한 구조로 인해 비용이 많이 들면서도 지연 문제가 발생하여 비효율적인 측면이 있습니다. 실제로 2021 년 데이터 침해를 파악하고 차단하는 데 평균 287 일이 걸렸습니다.^{xxiv} 엔드 투 엔드 보호 역량을 개선하기 위한 노력의 일환으로 여러 뛰어난 사이버 보안 제공업체들이 2021 년 인수 합병을 실시하였습니다. 주목할 만한 활동은 CrowdStrike Holdings 의 3 억 5,200 만 달러 규모의 Humio 인수와 Rapid7 의 3 억 3,500 만 달러 규모의 IntSights 인수로서, 이를 통하여 통합된 위협 탐지 및 치료 제품이 나오게 되었습니다.^{xxv, xxvi} 안티 바이러스 및 VPN 서비스 제공업체인 Norton 과 Avast 가 80 억 달러 규모의 합병을 시작한 가운데 이러한 통합 활동의 증가는 2022 년에도 계속될 가능성이 있습니다.^{xxvii}

결론

2021 년은 최근에 가장 영향력이 컸던 사이버 침투가 발생하였고, 세계는 지속적으로 디지털화되고 있기 때문에 향후 상당한 공격이 발생할 가능성이 커지고 있습니다. 하지만, 이 기간 동안 배운 디지털 보호에 대한 교훈으로 인해 사이버 보안 서비스 채택이 가속화될 것으로 생각합니다. 사이버 범죄를 방지하려는 최근의 재정적 노력은 2022 년 사이버 보안 회사들에게는 순풍으로 작용할 수 있고 사이버 보안 테마에 대한 장기적인 투자를 강화하게 될 것이라 생각합니다.

투자에는 원금 손실 가능성을 포함한 리스크가 수반됩니다. 사이버 보안 회사들은 개인정보보호/사이버 보안 우려와 관련해 중첩되는 규제기관의 감독과 관련된 리스크가 있습니다. 제품/서비스 사용 갱신의 감소 또는 변동성이나 지적재산권의 상실 또는 침해가 이익에



부정적인 영향을 줄 수 있습니다. BUG가 투자할 수 있는 회사의 투자 가능 유니버스는 제한적일 수 있습니다. 정보기술 업종의 회사 주식은 급속한 제품 퇴화 및 극심한 업계 경쟁으로 인해 영향을 받을 수 있습니다. 국제 투자에는 통화 가치의 불리한 변동, 일반회계원칙의 차이, 또는 다른 국가의 사회적, 경제적 또는 정치적 불안정으로 인한 자본 손실 리스크가 수반됩니다.

ⁱ IBM, "Cost of a Data Breach Report 2021," July 2021.

ⁱⁱ Soffid, "Cybersecurity Trends for 2022, December 29," 2021.

ⁱⁱⁱ Metric derived from average CAGRs featured in the following sources: Markets and Markets, "Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026," February 2021., Research and Markets, "SD-WAN - Global Market Trajectory & Analytics," April 2021., Market Growth Reports, "Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026," July 2021., Expert Market Research, "Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments," 2021., Markets and Markets, "Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026," August 2021., Global X Analysis.

^{iv} CloudTweaks, "Infographic: How Much Data is Produced Every Day?," accessed on Nov 15, 2021.

^v Ericsson Mobility Visualizer, "Connected Devices," accessed on Nov 15, 2021.

^{vi} 같은 출처.

^{vii} Gallup, "Remote Work Persisting and Trending Permanent," October 13, 2021.

^{viii} IBM, (각주 1).

^{ix} IBM, (각주 1).

^x CNBC, "Colonial Pipeline paid \$5 million ransom one day after cyberattack, CEO tells Senate," June 8, 2021.

^{xi} Bloomberg, "CNA Financial Paid \$40 Million in Ransom After March Cyberattack," May 20, 2021.

^{xii} CNBC, "Meat supplier JBS paid ransomware hackers \$11 million," June 9, 2021.

^{xiii} PCH Technologies, "Cost of Cyber Attacks vs. Cost of Cyber Security in 2021," July 7, 2021.

<https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/>

^{xiv} IBM, "Cost of a Data Breach Report 2021," July 2021.

^{xv} PwC, "Global Digital Trust Insights 2022," October 2021.

<https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html#findings>

^{xvi} Gartner, "Gartner IT Symposium/Xpo Americas," October 2021.

<https://www soffid.com/cybersecurity-trends-for-2022/>

^{xvii} Infrastructure Investment and Jobs Act, H.R. 3684, 117th Cong. 2021.



^{xviii} Norton, "2021 Norton Cyber Safety Insights Report Global Results," May 2021.

^{xix} CNBC, "Covid-related scams have bilked Americans out of \$586 million," October 18, 2021.

^{xx} Norton, "2021 Norton Cyber Safety Insights Report Global Results," May 2021.

^{xxi} Metric derived from average CAGRs featured in the following sources: Technavio, "Privileged Access Management Solutions Market by Deployment and Geography - Forecast and Analysis 2022-2026," January 2022., Mordor Intelligence, "Identity Governance And Administration Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)," January 2022., Technavio, "Consumer Identity and Access Management (IAM) Market by Deployment and Geography - Forecast and Analysis 2022-2026," December 2021.

^{xxii} Metric derived from average CAGRs featured in the following sources: Markets and Markets, "'Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026," February 2021., Research and Markets, "SD-WAN - Global Market Trajectory & Analytics," April 2021., Market Growth Reports, "Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026," July 2021., Expert Market Research, "Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments," 2021., Markets and Markets, "Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026," August 2021., Global X Analysis.

^{xxiii} Mordor Intelligence, "Endpoint Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)," January 2022.

^{xxiv} IBM, (각주 1).

^{xxv} CrowdStrike, "CrowdStrike Completes Acquisition of Humio," March 5, 2021.

^{xxvi} VentureBeat, "Rapid7 acquires threat intelligence platform IntSights for \$335M," July 19, 2021.

^{xxvii} Norton, "NortonLifeLock and Avast to Merge to Lead the Transformation of Consumer Cyber Safety," August 10, 2021.

