

작성자:

Jon Maier

날짜: 2022. 4. 22

주제: 대화형 알파

알파 추구: 사이버 보안, 있으면 보충적 기술에서 필수 기술로

오늘날 디지털 세계에서 데이터는 돈이고, 많은 악의적 행위자들이 이를 자기 손에 넣으려고 합니다. 얼마 전 두 개의 거물급 대형 기술 회사가 법 집행관으로 위장한 해커에게 고객 데이터를 제공하여 사이버 방어 체계가 생각만큼 튼튼하지 않다는 사실을 증명했습니다.¹ 이러한 우려는 푸틴의 우크라이나 침략 시 동반되었던 사이버 공격으로 더욱 악화되었으며 개인, 기업 및 정부는 자신의 네트워크에 누가 숨어 있지는 않은지 걱정하며 신경을 곤두세우게 되었습니다. 이에 대해 바이든 행정부는 서방이 부과한 제재와 긴장된 지정학적 관계와 관련해 더 높은 수준의 사이버 범죄가 발생할 가능성이 있다고 기업에 경고했습니다.² 이러한 환경에서는 그 누구도 사이버 공격에서 완전히 벗어날 수는 없지만 이를 예방하기 위해 노력할 수는 있습니다. 결과적으로 사이버 보안에 드는 지출이 계속 증가함에 따라 사이버 보안 회사가 반복적인 수익 모델로 투자자의 관심을 끌 것으로 예상합니다. 당사의 견해로 이러한 요인들이 포트폴리오에서 지정학적 리스크를 관리하는 데 도움이 되는 사이버 보안 테마의 기능과 더불어 이러한 익스포저를 필수적으로 만듭니다.

주요 요점

- 사이버 범죄 예방에 도움이 되는 공공 및 민간 행동 계획의 범위가 늘어나 결과적으로 사이버 보안에 관한 지속적인 지출이 커질 것으로 예상합니다. 어느 주요 리서치 회사는 2021년에서 2025년 사이에 전 세계 사이버 보안 지출이 누적 1.75조 달러를 초과할 것으로 예측합니다.³
- 바이든 행정부는 정부, 정부 계약업체 및 민간 기업 모두에 영향을 미치는 사이버 공격으로부터 보호가 필요한 상황의 긴급성을 강조했습니다. 이에 따라 관련 다운스트림 업계는 사이버 보안에 더 많은 지출을 할 것으로 보입니다.
- 사이버 보안 테마에 대한 익스포저는 지속적으로 반복되는 수익 방어력과 점점 더 정교해지는 사이버 범죄 행위에 맞선 공공 및 민간 부문의 대응과 연관된 성장 잠재력을 불러옵니다.

행동을 촉구한 SolarWinds 해킹

2020년 12월에 발견된 Solar Winds 해킹은 사이버 보안의 주축이 되는 순간이었습니다. 이 해킹은 러시아 대외정보국(FIS)의 소행으로 추정됩니다. 여기에는 약 100개 기업과 미 재무부, 법무부, 에너지부, 국방부 등 10여 개의 정부 기관이 피해를 입은 배후 사정이 있습니다.⁴ 이 공격은 특히 공격자가 활용도가 높은 소프트웨어를 손상시킬 때 그 영향이 얼마나 신속히 퍼지고 광범위할 수 있는지에 대한 경고 그 자체였습니다. 바이든 행정부는 사이버 보안 방어를 현대화하고 미국 정부와 계약을 맺은 조직의 보안 요건을 업데이트해야 할 필요성을 이해하고 있습니다.⁵ 러시아의 우크라이나 침략을 고려해 바이든 행정부는 미국 기업들에 사이버 공격으로부터 보호가 필요한 상황의 긴급성을 강조했습니다. 관련 다운스트림 업계는 사이버 보안에 더 많은 지출을 할 것을 시사합니다.



그 후 발발한 전쟁, 사이버 보안에 더 많은 지출 야기

우크라이나 은행과 정부 부처를 겨냥한 최근 사이버 보안 위협은 사이버 보안 테마를 전쟁의 최전선으로 불러왔습니다. 사이버 공격으로부터 우크라이나를 보호하기 위해 유럽 연합은 리투아니아, 크로아티아, 폴란드, 에스토니아, 루마니아 및 네덜란드의 전문가로 이루어진 사이버 신속 대응팀을 제공했습니다. 민간 부문에서도 도움의 손길을 내밀고 있습니다. 푸틴의 침략 직전, Microsoft의 위협 인텔리전스 센터는 우크라이나 정부 부처와 금융 기관을 노리는 비정상적인 활동을 식별하고 신속하게 이를 공개하는 데 관여했습니다.⁶ 또한 Alphabet은 우크라이나의 사이버 공격을 방지하는 데 핵심적인 역할을 했습니다.⁷

이러한 대응은 미국의 전력, 파이프라인 및 수도 부문을 보호하고 정부 권한을 사용하여 새로운 사이버 보안 및 네트워크 방어 조치를 지시하기 위해 바이든 행정부가 시작한 공공 및 민간 행동 계획과 유사합니다.⁸ 사이버 방어체계를 현대화하려는 바이든 행정부의 목표에는 랜섬웨어 공격을 저지하고 사이버 범죄 활동을 공개적으로 지명하기 위해 수많은 국제 동맹국 및 파트너와의 지속적인 협력도 포함됩니다.⁹

우크라이나 정부, 유럽 연합 및 북대서양 조약 기구(NATO)와 기술 부문의 긴밀한 협력은 그 범위와 속도에 있어 전례가 없는 일입니다. 이러한 대응은 사이버 기술의 발전과 사이버 기술이 글로벌 경제에서 수행하는 핵심적인 역할에 관해 이야기합니다. 사이버 범죄는 끊임없이 반복되는 위협이기 때문에 이러한 노력이 계속될 것이며 사이버 보안에 대한 지출이 증가할 것으로 예상합니다.

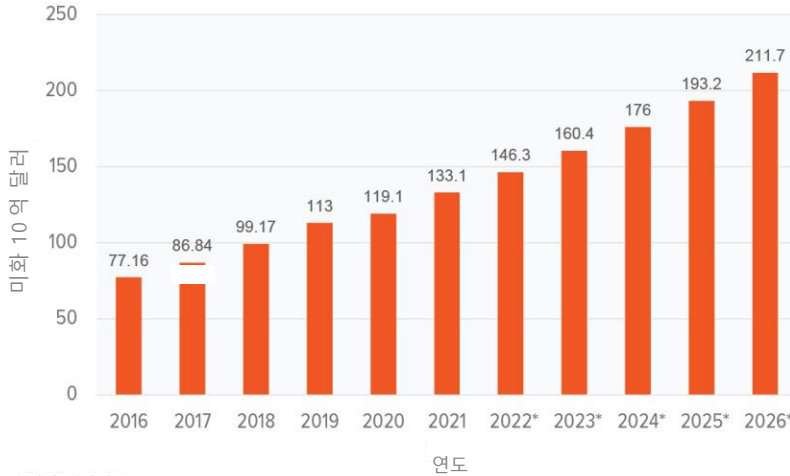
사이버 보안은 높은 성장 기회가 될 수 있다

우크라이나 전쟁과 이와 관련된 지정학적 책략은 강력한 사이버 방어의 중요성에 관한 더 많은 관심을 끄니다. 행정 명령과 백악관의 새로운 사이버 보안 전략은 특히 정부의 감독 계획과 최소 기준을 강제하는 규칙이 있는 경우 채택을 늘릴 것으로 보입니다.¹⁰ 사이버 보안이 기업의 자발적 투자에서 비즈니스 수행에 필요한 규제 대상 투자로 전환되면 미국, 유럽 및 기타 지역에서 급격히 채택이 늘어날 것으로 보입니다.¹¹ 데이터 보안과 접근성 간의 직접적인 상충 관계를 고려할 때 데이터의 절대적인 보호는 지나치게 야심 찬 목표일 수 있으나 계속 늘어날 가능성이 있는 사이버 보안에 대한 지출은 리스크를 완화할 수 있기 때문에 이 테마는 더 광범위한 포트폴리오 측면에서 고려되어야 합니다.



전 세계 사이버 보안 수익

출처: 2022년 3월 기준 Statista 데이터



연도	성장률
2017년	12.55%
2018년	14.20%
2019년	13.95%
2020년	5.40%
2021년	11.75%
2022년*	9.92%
2023년*	9.64%
2024년*	9.73%
2025년*	9.77%
2026년*	9.58%

*예상 데이터

참고: 표시된 데이터는 아직 러시아-우크라이나 전쟁의 시장 영향을 반영하지 않습니다.

사이버 보안 ETF는 포트폴리오에 탄력성을 더할 수 있다

사이버 보안 기술은 잠재적인 공격을 사전에 방어하는 한편, 이미 발생한 사고에 따른 피해를 완화하고 복구합니다. 사이버 공격의 발생 빈도 및 강도는 증가하고 있으며, 이는 사이버 보안 지출에 대한 필요성이 끊이지 않을 것임을 보여줍니다. 사이버 보안 회사에 있어 점점 더 중요해지는 이러한 필요성은 강력한 반복 수익을 생성하는 비즈니스 모델을 창출합니다. 결과적으로 이 테마의 더 넓은 수준에 투자함으로써 투자자는 회사 전반에 걸쳐 익스포저를 다각화할 수 있습니다. 채택에 박차를 가하는 이러한 요인들이 빠른 시일 내에 줄어들 가능성이 작기 때문입니다.

어떤 분야나 테마에서든 항상 승자를 고르는 어렵습니다. 시장을 통제할 수 있는 개별 기업을 효과적으로 선별하려면 자세한 정보가 필요하지만 테마에 투자하는 ETF를 통해 투자자는 리스크를 다각화할 수 있습니다. 사이버 보안 관련 주식은 대규모 해킹 발생 이후 주가 실적에 따라 상승할 수 있고 애플리케이션 개발자가 대규모 침해로 피해를 입을 경우 하락할 수 있으므로 ETF는 다각화된 타당한 솔루션이 될 수 있습니다.

각주:

1 백악관, 팩트 시트: 발생할 수 있는 사이버 공격으로부터 보호하려면 지금 행동하세요, 2022년 3월 21일

2 백악관, 팩트 시트: 발생할 수 있는 사이버 공격으로부터 보호하려면 지금 행동하세요, 2022년 3월 21일

3 Cybersecurity Ventures, 2021년부터 2025년까지 1조 7,500억 달러를 초과하는 전 세계 사이버 보안 지출, 2021년 9월 10일

4 NPR, '최악의 악몽' 사이버 공격: SolarWinds 해킹의 알려지지 않은 이야기, 2021년 4월 16일

5 NPR, '최악의 악몽' 사이버 공격: SolarWinds 해킹의 알려지지 않은 이야기, 2021년 4월 16일

6 사이버 보안 및 인프라 보안국, 우크라이나 기관을 표적으로 한 파괴적인 멀웨어, 2022년 3월 1일



⁷ Chamber Business News, 위협이 커짐에 따라 전문가들이 사이버 공격에 대한 정부 및 민간 부문의 준비를 평가, 2022년 3월 24일

⁸ NYT, 탱크가 우크라이나에 굴러 들어갈 때, 멀웨어도 같이 들어가. 그리고 Microsoft도 전쟁에 들어감, 2022년 2월 28일

⁹ CSIS, 공유된 책임: 사이버 보안을 위한 민간 협력, 2022년 3월 22일

¹⁰ MIT Technology Review, 미국의 끝나지 않는 사이버 보안 실패를 해결하려는 내부 계획, 2022년 3월 18일

¹¹ Reuters, 유럽 연합, 사이버 보안 우려 속에 유럽 연합 기관에 사이버 보안 규칙 제안, 2022년 3월 22일

투자에는 원금 손실 가능성을 포함한 리스크가 수반됩니다. 좁은 범위의 투자에는 변동성이 더 클 수 있습니다.

기술 테마 투자는 기술의 급격한 변화, 치열한 경쟁, 제품과 서비스의 급속한 노후화, 지적재산 보호의 상실, 진화하는 산업 표준 및 빈번한 신제품 생산, 비즈니스 사이클 및 정부 규제의 변화에 영향을 받을 수 있습니다.

ETF 주식은 시장가(순자산가치가 아님)로 매매되며 펀드에서 개별적으로 환매할 수 없습니다. 중개 수수료는 수익률을 떨어뜨립니다.

본 자료는 특정 시점의 시장 환경에 대한 평가를 나타내는 것으로 미래의 사건을 예측하거나 미래의 결과를 보장하려는 것이 아닙니다. 이 정보는 개인 또는 개인 맞춤형 투자 또는 세무 자문이 아니며, 매매 목적으로 이용할 수 없습니다. 본인의 투자 및 세무 상황에 관한 더 자세한 정보는 재무상담사 또는 세무전문가와 상담하시기 바랍니다.

Global X Management Company LLC는 Global X 펀드에 자문사 역할을 수행합니다.

