Global X ETFs 리서치

Global X Cybersecurity ETF (BUG) 소개

작성자:

Pedro Palandrani
리서치 애널리스트

날짜: 2019년 10월 29일

주제: 기술

세계가 디지털화됨에 따라 중요하고 민감한 데이터를 보호하는 것은 점점 더 필수적인 일이 되어가고 있습니다. 기술은 형태가 있는 사물을 디지털화하고 수작업을 자동화함으로써 생산성을 향상시킵니다. 하지만 더 많은 사물과 과정이 실물 세계를 벗어나 디지털 세계로 이전됨에 따라 새로운 형태의 범죄가 나타났습니다. 2021년까지 사이버 범죄로 인한 전 세계의 피해가 6조 달러에 이르러 개인, 회사 및 정부는 독점 데이터를 보호할 수 있는 정교한 소프트웨어와 서비스를 제공하는 사이버 보안 회사를 고용하는 데 거금을 지출하고 있습니다.[1] 따라서 사이버 보안은 머신 러닝, 클라우드 컴퓨팅 및 사물 인터넷과 같이 데이터를 산출하고 활용하거나 연결해주는 접점 분야가 성장함에 따라 더욱 추진력을 얻게 될 유망한 테마입니다.

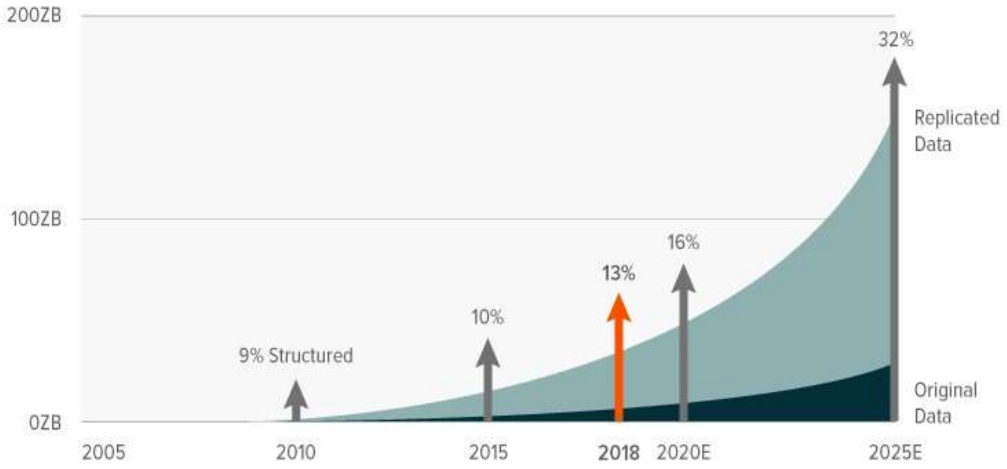
빅데이터의 증가

얼마 전까지만 해도 알파벳순으로 정리된 폴더로 가득 찬 파일 캐비닛에 주소, 건강 기록이나 재무제표와 같은 아주 중요한 정보를 저장했었습니다. 이제는 컴퓨터와 인터넷이 도입되어 1과 0을 통해 방대한 양의 정보를 파악하고 저장하는 새로운 패러다임이 구축되었습니다. 순식간에 기술을 통해 마우스를 한 번만 클릭하면 데이터를 얻을 수 있게 되었습니다. 하지만 여기서 멈추지 않았습니다. 실제로 기록되었던 오래된 데이터를 디지털 데이터로 전환시키는 것이 첫 번째 단계였지만 이제는 우리가 하는 모든 것 예를 들어 무엇을 구매하고 무엇을 시청하며 누구와 대화를 나누고 어디를 방문하는지 등이 다양한 플랫폼을 통해 데이터로 남겨집니다. 한 추산에 의하면 전 세계적으로 매일 250경(2.5×10^{18}) 바이트 이상의 데이터가 만들어지며 이는 지난 2년 동안 만들어진 데이터의 90%에 해당하는 양입니다.[2] 다른 관점에서 보면 2020년에는 매일 관측 가능한 우주에 있는 별의 수보다 40배 많은 바이트의 데이터가 만들어 졌습니다.[3]

이렇게 데이터가 폭발적으로 늘어나자 1) 식기 세척기부터 TV에 이르는 일상 기기를 인터넷에 연결하여 데이터를 수집, 전송하는 사물 인터넷, 2) 저렴하고 확장성이 있으며 효율적인 데이터 인프라 서비스를 제공하여 회사들이 더 많은 데이터에 의존하도록 만드는 클라우드 컴퓨팅, 3) 광범위한 데이터로부터 유의미한 정보를 도출하여 데이터를 그 어느 때보다 더욱 가치 있게 변화시킨 머신 러닝 및 인공 지능과 같은 몇몇 디지털 기술이 출현하게 되었습니다.

NEW DATA CAPTURED / CREATED / REPLICATED, PER IDC (DATA VOLUME, ANNUAL, GLOBAL (ZB))

Source: Bondcap, Internet Trends 2019. Note: 1 petabyte= 1 million gigabytes; 1 zeta (ZB) byte= 1 million petabytes. Structured data indicates data that has been organized so that it is easily searchable. Replicated data= data that is sourced from the original.



데이터 급증 = 사이버 위협 급증

그러나 귀중한 데이터가 더 많이 생성됨에 따라 사이버 범죄자들이 이를 훔쳐 암시장에서 팔거나 보유하여 대가를 요구하거나 개인정보를 유출하는 사례도 같이 증가하였습니다. 가장 흔한 경우는 사이버 범죄자들이 디지털 수단을 사용하여 독점적인 개인 데이터, 지적재산과 금전을 훔치는 것입니다. 기술이 발전함에 따라 사이버 위협 역시 발전할 것입니다. 예를 들어, 사물 인터넷이 일상적인 기기를 인터넷에 연결함에 따라 사이버 범죄자들이 활동할 새로운 공간이 만들어집니다. 실제로 교통신호 해킹, 차량 절도 또는 개인 건강 기기의 조작 모두가 이제 가능합니다.

한 사이버 보안 회사가 매일 1억 건 이상의 위협을 차단할 수 있습니다.[4] 이는 1초마다 1천 건 이상의 위협을 차단하는 것입니다. 그러나 한 건의 침해라도 발생하게 되면 회사와 사용자는 심각한 피해를 입게 됩니다.

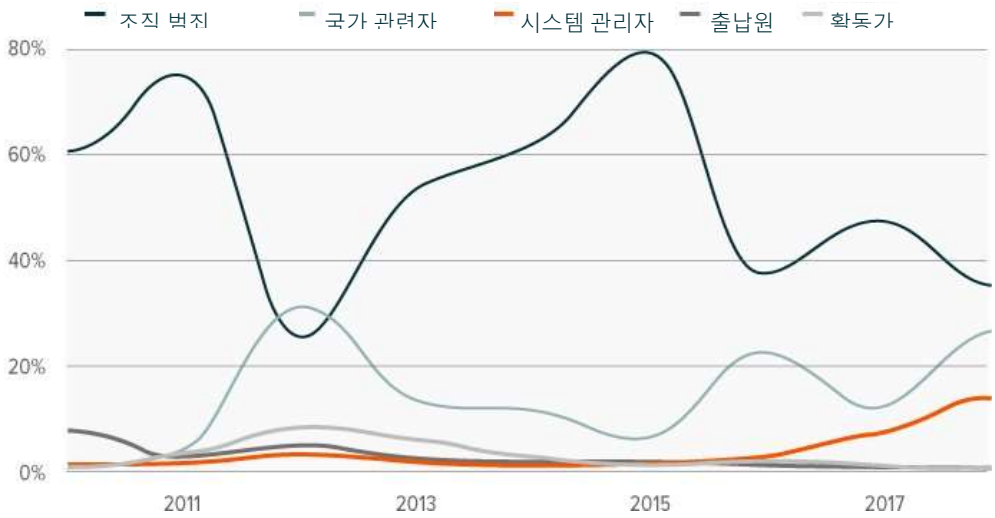
2013~2014년에 야후는 두 건의 개별 공격에서 30억 개의 계정 모두가 해킹을 당했는데, 이는 아마도 21세기 최악의 데이터 침해 사건일 것입니다. 이러한 침해로 인해 사용자의 이름, 이메일 주소, 생년월일, 전화번호, 비밀번호 및 보안 질문이 노출되었습니다.
더 걱정되는 부분은 실제 사건이 발생된 지 3~4년 후인 2017년에야 해당 공격을 확인했다는 점입니다.
2017년, 미국의 최대 신용조사 회사 중 하나인 Equifax는 사회보장번호, 생년월일 및 운전면허증 번호를 포함하여 1억 4,300만 소비자에게 영향을 끼친 데이터 침해 사건을 발표했습니다. 2018년 말에 Marriott International은 여권번호와 같은 개인정보를 포함하여 5억 개의 계정을 위태롭게 한 데이터 침해 사건을 발표하였습니다.

일반적으로 사이버 범죄는 외부인이 저지릅니다. 야후의 경우 범인은 국가의 지원을 받았는데, 이는 드문 경우입니다. 외국 정부의 지원을 받는 해커들의 비중은 전 세계 침해의 약 23%를 차지합니다.[5] 조직 범죄는 데이터 침해 사건의 39%를 차지합니다.

그러나 외부 행위자만 걱정거리는 아닙니다. 개인적인 이득 또는 금융상의 이득을 얻기 위해 내부 침해가 발생하는데, 때로는 인간의 단순한 실수에 의해 발생하는 경우도 있습니다.

데이터 급증 = 사이버 위협 급증(침해)

출처: Verizon, 2019년 데이터 침해 조사 보고서.



솔루션 생태계가 필요

사이버 위협에 대해 방어하는 것은 하나의 산업입니다. 사이버 보안은 게이트웨이, ID, 이메일, 클라우드, 웹 보안 및 엔드포인트를 포함한 모든 레벨의 네트워크를 보호하는 데 중점을 둡니다. 사이버 보안 회사가 무단 활동과 악의적인 활동을 방지하기 위해 사용하는 기법은 다양하며 다음과 같은 기법 중 하나 또는 그 이상을 조합하여 사용합니다.[6]

- 인증 및 승인: 사용자 활동을 확인 및 인증하기 위하여 사용하는 허가 프로세스.
- 암호작성술: 수학적 함수를 사용하여 통신의 보안을 확보하는 프로세스.
- 합법적인 사용 패턴에 대한 자동 분석: 관리자에게 비정상적인 행동을 경고하기 위하여 사용되는 사용 패턴에 대한 자동 분석.
- 침입 탐지 및 리스크 완화: 악의적인 행위자들이 시스템 침투를 하지 못하도록 하는 적극적인 접근법.
- 데이터 무결성 검증: 데이터의 무결성 상태를 검증하고 피해 또는 변경 범위를 평가하기 위한 분석.
- 컴퓨터 포렌식: 사이버 위협과 범죄를 추적하여 사건 발생 방법 및 이유를 확인하는 대응 메커니즘.

적극적인 예방 메커니즘이 진화하여 인공 지능 및 머신 러닝 접근법을 포함하게 되리라 예상합니다. 인공 지능 및 머신 러닝은 피싱을 탐지하고, 합법적인 것으로 보이려 시도하는 가짜 웹사이트와 링크를 찾아내는 데 도움이 될 수 있습니다. 인공 지능과 머신 러닝이 차세대 기술 사이버 보안 회사의 잠재적 위협 탐지에 도움을 줄 수 있는 다른 분야는 시각 인식 기술의 진전입니다. 물론, 인공 지능 및 머신 러닝 메커니즘이 발전하려면 훈련 목적으로 멀웨어와 같은 악성 데이터를 포함한 엄청난 양의

데이터에 접속해야 합니다.

사이버 보안을 확보하려면 더 많은 지출이 필요

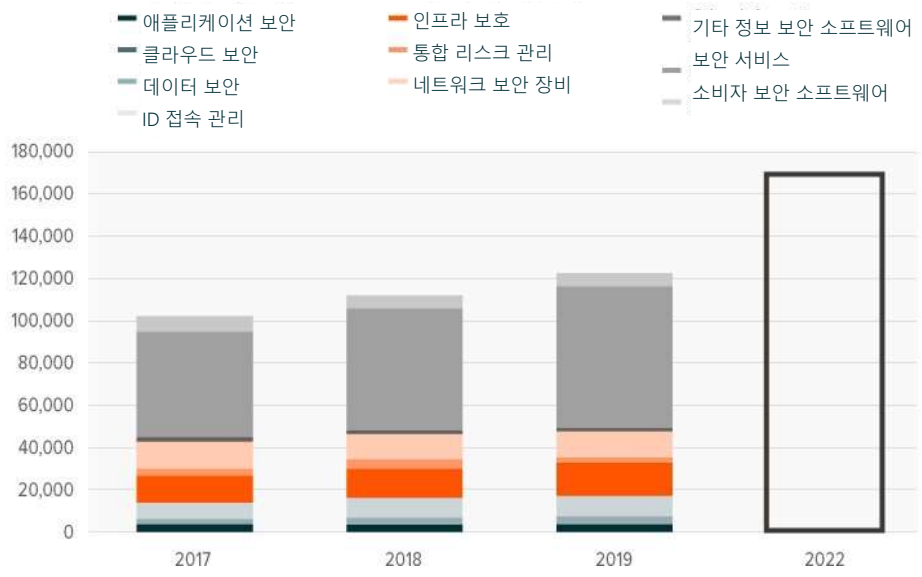
사이버 보안은 가장 빨리 증가하는 IT 지출 분야 중 하나입니다. 미국 전역의 최고정보책임자(CIO)는 사이버 보안에 대한 예산에 지속적으로 가장 많은 금액을 책정합니다.[7] 2019년 회사들이 사이버 보안에 수백만 달러를 지출하는 이유를 이해할 수 있습니다. 한 회사에서 데이터 침해 사건으로 발생하는 평균 총 비용은 390만 달러로, 고객 신뢰 상실에서 발생하는 비용의 36%에 해당합니다.[8]

보안 관련 소프트웨어, 하드웨어 및 서비스에 대한 전 세계의 지출액은 2021년 말까지 1,240억 달러에 이르고 등록된 악성 프로그램의 수는 9억 2,500만 개에 달하리라 예상됩니다.[9, 10] 2022년까지 전 세계의 총 지출액은 1,704억 달러에 이르고 5년 연평균 성장률이 10.9%에 달하리라 예상합니다.[11] 사이버 위협이 급증하는 점을 고려하면 이제 사이버 보안은 종종 침해로 인한 비용과 그로 인한 악영향을 두려워하는 조직이 비용을 절약하는 수단으로 간주됩니다.

마찬가지로, 사이버 보안 실행에 대한 정부 지출 역시 계속 증가하고 있습니다. 2018년 5월에 발효된 유럽연합의 일반 데이터 보호 규정(GDPR)은 개인 데이터에 대한 보안과 보호 및 투명성을 확보할 수 있는 방법으로 처리할 것을 요구하고 있습니다.

미국에서는 사이버 보안에 우선순위를 두고 있으며 규제 당국은 GDPR과 같은 법률을 제정하기 위해 지속적인 노력을 기울이고 있습니다. 2019년 연방 예산에 사이버 보안으로 150억 달러가 책정되었었는데, 이는 2018년 대비 5억 8,340만 달러 또는 4.1%가 증가한 금액입니다.[12] 사이버 보안은 주 차원에서 다루어야 할 문제이기도 합니다.
캘리포니아는 2018년 디지털 개인정보보호법을 통과시켜 사람들이 자신의 데이터를 관리할 수

2017~2022년 분야별 글로벌 보안 지출액(단위: 백만 달러)
출처: Gartner. 2019~2022년 데이터는 추정치임.



결론

모든 산업에 걸친 디지털 변환은 사이버 보안 역량이 단순히 대응하는 수준에 그치면 안 된다는 점을 시사합니다. 적극적인 보안이 필수적입니다. 데이터 침해 발생을 방지하면 원하지 않는 정치경제적 파문을 완화할 수 있습니다. 매일 수백만 건씩 발생하는 사이버 위협은 점점 복잡해지고 있기에 사이버 보안 회사의 서비스에 대한 수요가 지속적으로 성장할 기회를 제공합니다. 전 세계의 회사, 소비자 및 정부 기관을 보호하는 중요한 역할을 고려할 때, 사이버 보안은 더 강력한 보안과 더불어 개인정보보호의 수단과 정책을 활용할 수 있는 위치에 있습니다.

---

1. Cybercrime Magazine, "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021(2017~2021년 동안 글로벌 사이버 보안 지출이 1조 달러를 초과할 것으로 예상)", 2019년 6월 10일.
2. Domo, "Data Never Sleeps 5.0(잠들지 않는 데이터 5.0)", 2017년.
3. Domo, "Data Never Sleeps 7.0(잠들지 않는 데이터 7.0)", 2019년.
4. 참고: Zscaler 클라우드 활동 대시보드에서 파악한 숫자(2019년 10월 11일 접속) - 이는 라이브 툴이므로 데이터는 지속적으로 변함.
5. Verizon, 2019 Data Breach Investigations Report(2019년 데이터 침해 조사 보고서)", 2019년.
6. 참고: 카네기 멜론 대학교의 언어 기술 연구소가 개발한 사이버 보안 분류 체계. 분류 목적상 사이버 보안의 기술적 측면만이 고려되었음. 2019년 10월 15일 접속.
7. IDC, "Developing Your Security Fabric: A Transformational Approach for State Government(보안 패브릭 개발: 주 정부를 위한 혁신적인 접근법)", 2019년 5월.
8. IBM, "Cost of a Data Breach Report 2019(2019년 데이터 침해 비용 보고서)", 2019년.
9. Gartner, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019(Gartner, 글로벌 정보 보안 지출액이 2019년에 1,240억 달러를 초과할 것으로 예측하다)", 2018년 8월 15일.
10. Palo Alto Networks, "2019 Analyst Meeting(2019년 애널리스트 회의)", 2019년 9월 4일.
11. Gartner, "Forecast Analysis: Information Security, Worldwide, 2Q18 Update(예측 분석: 전 세계 정보 보안, 2018년 2분기)", 2018년 9월 14일.
12. Whitehouse, Cybersecurity Funding(사이버 보안 자금조달). 2019년 10월 24일 접속.