작성자:

Pedro Palandrani
리서치 애널리스트

날짜: 2021년 2월 2일
주제: 테마

Global X ETF 리서치

사이버 보안 발전을 선도하는 4개의 기업

오늘날 기업들은 언제라도 해킹 위험에 노출되어 있습니다. 소프트웨어 관리 기업인 SolarWinds는 2020년 12월에 대형 해킹 문제에 봉착했습니다. 일부 사람들이 미국 역사상 최대 사이버 공격이라고 일컫는 사건에서 가해자는 소프트웨어가 구동되는 서버에 치명적인 바이러스를 Orion 소프트웨어에 심었습니다. 무서운 점은 이 공격이 주요 연방기관 및 조직에 영향을 주어 국가 안보를 위태롭게 할 가능성이 있었다는 것입니다. 조기 추정에 따르면 약 250개 조직이 이 해킹에 영향을 받았습니다.

미국과 전 세계에서 발생하는 사이버 위협은 점점 만연하고 정교해지고 있습니다. 사이버 공격의 증가로 인해 전 세계 보안 지출이 2020년 약 1,250억 달러에서 2024년까지 1,750억 달러로 늘어날 것으로 예상됩니다.[1] 이러한 증가세는 클라우드 기술로의 이전 가속화 때문입니다. 현재 총 워크로드의 3분의 1만이 클라우드 컴퓨팅 기술을 사용하고 있습니다. 그 수가 늘어남에 따라 악성 공격을 방지하려면 사이버 보안에 대한 지출을 늘려야 할 것입니다.[2] 마찬가지로, 인터넷을 이용하는 기기를 더 많이 그리고 빠르게 전환함으로써 데이터를 훔치거나 데이터를 인질로 대가를 요구하는 해커들의 새로운 타겟이 되고 있습니다.

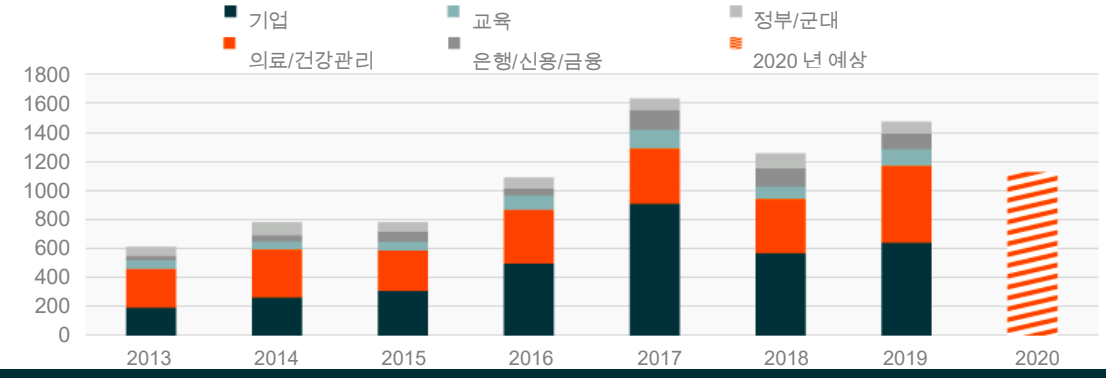
이 보고서에서는 사이버 보안 테마에서 키 플레이어인 4개 기업을 집중 조명합니다.

- CrowdStrike: 선도적인 엔드포인트 보호 플랫폼
- Zscaler: 안전한 웹 게이트웨이를 제공하는 클라우드 네이티브 플랫폼
- Okta: ID 접속 관리의 키 플레이어
- Mimecast: 악성 이메일을 탐지하여 차단하는 최고의 솔루션 제공업체

3억 8천만 명 이상의 개인이 2020년에 데이터 침해를 경험한 것으로 예상.[3]

미국의 데이터 해킹 수

출처: Identity Theft Resource Center, 2020 년.



CrowdStrike: 선도적인 엔드포인트 보호 플랫폼

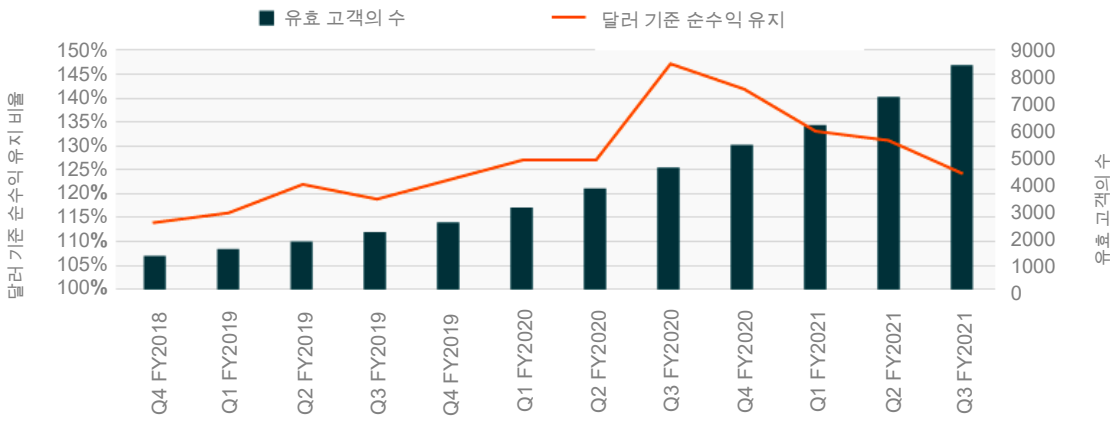
CrowdStrike는 고객이 모바일 기기, 노트북 및 서버와 같은 최종 사용자 기기를 안전하게 지키는 데 도움을 주는 엔드포인트 보호 플랫폼(EPP)의 선도적인 사이버 보안 기업 중 하나입니다. CrowdStrike의 솔루션은 위협을 지속적으로 탐지하고 분석하는 서비스형 소프트웨어입니다. 솔루션은 100% 클라우드 기반 아키텍쳐로서 CrowdStrike가 기존의 비-클라우드 기반 기업에 비해 경쟁 우위를 확보할 수 있도록 해줍니다. 동사는 많은 상이한 IT 환경에서 빠르고 효과적으로 솔루션을 설정할 수 있습니다. 예를 들면, 2020 회계연도 4분기에 동사는 Target을 10일 만에 새로운 고객으로 맞이했습니다.

과거에 사내 안티-바이러스 소프트웨어는 엔드포인트 파일에서 알려진 위협을 모니터링하고 스캐닝함으로써 해킹을 막았습니다. 그러나 그러한 보안 장벽은 대부분 사후 반응적입니다. 오늘날 최고 수준의 제품은 AI를 활용합니다. CrowdStrike의 AI 제품은 Threat Graph라 불리는데, 이는 동사의 AI를 활용한 사이버 보안 솔루션의 두뇌 역할을 수행합니다. CrowdStrike는 Threat Graph를 통해 매주 4조 건의 사이버 사건을 처리하고 분당 5천만 건의 결정을 내릴 수 있습니다.[4] 데이터 세트는 CrowdStrike의 클라우드에서 처리되어 고객 전체서 더 많은 데이터가 분석될 수록 Threat Graph AI 기술이 더 좋아지는 네트워크 효과를 만들어 냅니다.

클라우드 기반 솔루션은 반복적 구독 매출로 이어질 수 있습니다. 2020년 4분기 기준으로 CrowdStrike는 총수익의 92%를 구독 매출로 받았습니다.[5] CrowdStrike는 2019 회계연도 1분기 이후 120% 이상의 달러 기준 순수익 유지(Net Revenue Retention, NRR) 비율을 유지해왔습니다.[6] 비율이 100% 이상이라는 것은 가격 인상 또는 연쇄 판매를 통하여 기존 고객 기반으로부터의 순수익이 증가되었다는 것을 의미합니다.

CROWDSTRIKE 의 순수익 유지 비율(왼편) 및 유효 고객(오른편)

출처: Global X ETF, CrowdStrike 회사 제출 서류.



Zscaler: 보안 웹 게이트웨이의 최고 플레이어

Zscaler는 또 하나의 100% 클라우드 기반 사이버 보안 플랫폼입니다. 따라서 구입하거나 관리할 하드웨어는 없으며 플랫폼은 항상 최신으로 유지됩니다. Zscaler는 매일 175,000건의 보안 클라우드를 업데이트합니다.[7] Zscaler의 보안 웹 게이트웨이(SGW) 솔루션은 Zscaler Private Access(ZPA)를 통해 주로 고객이 내부적으로

관리되는 애플리케이션에 안전하게 접속하도록 돕는 데 중점을 둡니다. 또한 Zscaler는 Zscaler Internet Access(ZIA)를 통해 고객 관계 관리(CRM) 소프트웨어와 같은 외부 애플리케이션용 솔루션을 제공합니다. 보안 웹 게이트웨이는 외부 웹 애플리케이션을 통해 안전하지 않은 트래픽이 내부 네트워크에 진입하는 것을 방지합니다. Zscaler는 네트워크를 연결이 아닌 사용자들을 직접 애플리케이션에 연결하는 중개인과 같습니다.

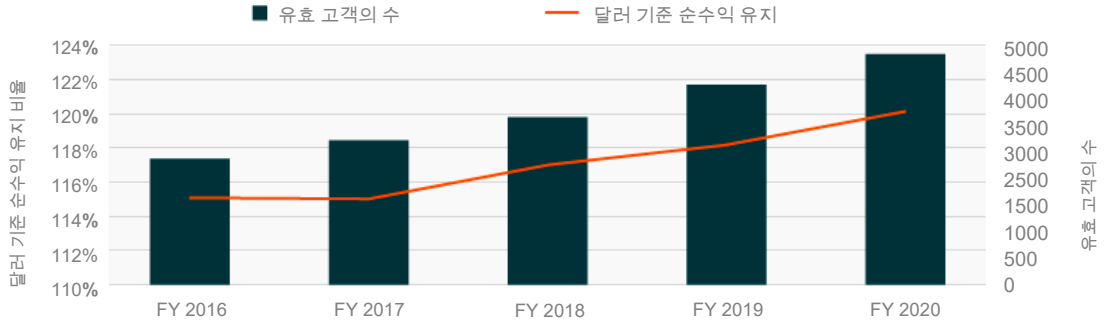
Zscaler는 궁극적으로 가상 사설 통신망(VPN) 기술을 쓸모가 없게 만드는 역량을 제공합니다. 동사의 ZPA 솔루션은 구축 및 관리가 용이하고, 전통적인 VPN 솔루션보다 더 안전합니다. ZPA는 사용자들에게 내부 앱 접속권을 제공하므로 기업 네트워크에 연결하거나 그러한 사용자들을 인터넷에 노출시킬 필요가 없습니다. 또한 이 아키텍쳐는 침해 중에 네트워크를 횡단하는 사이버 공격의 능력을 완전히 제한합니다. 네트워크를 모든 사용자들에게 확장하지 않으므로 동사는 이 아키텍쳐를 Zero Trust Network라고 부릅니다. 한 마디로 네트워크의 중요성이 하락하며 인터넷이 기업의 네트워크가 됩니다.[8]

노트북, 스마트폰 및 기타 사물인터넷(IoT) 기기에 있는 내외부 앱에 대한 접속 확보는 특히 원격 및 하이브리드 작업이 대세가 됨에 따라 조직에 있어서 최고의 우선순위입니다. 리서치 회사 Gartner에 따르면, 2023년까지 기업의 60%가 대부분의 원격 접속 VPN을 단계적으로 폐지하게 되는데, 이는 Zscaler가 제공하는 Zero Trust Networks에 유리하게 작용할 것으로 예상됩니다.[9]

Zscaler의 달러 기준 순수익 유지 비율은 2020 회계연도 말 기준으로 120% 수준에 이르며 이는 기존의 사용자 기반에서 지속적으로 성장하고 있음을 보여줍니다.[10] 중요한 점은, 동사는 ZIA와 ZPA만으로도 기존의 고객으로부터 6배 업셀링 기회가 있다고 생각한다는 것입니다.[11]

ZSCALER 의 달러 기준 순수익 유지 비율(왼편) 및 유효 고객(오른편)

출처: Global X ETF, Zscaler 회사 제출서류.



Okta: ID 접속 관리(IAM) 기업중 가장 빠르게 성장하는 회사

Okta는 ID 접속 관리(IAM) 부문에서 선도적인 사이버 보안 회사입니다. 이 기업은 권한을 가진 개인 및 직원이 특정 자원 또는 정보를 필요시에만 접근을 허락해주는 시스템을 구축하는데 중점을 둡니다.[12] 다중 요소 인증(MFA), 애플리케이션 프로그래밍 인터페이스(API) 및 싱글 사인 온(SSO)은 허락된 사용자가 여러 애플리케이션에 접속할 권한이 부여되도록 하기 위해 점차 널리 활용되고 있는 대표적인 ID 솔루션입니다.

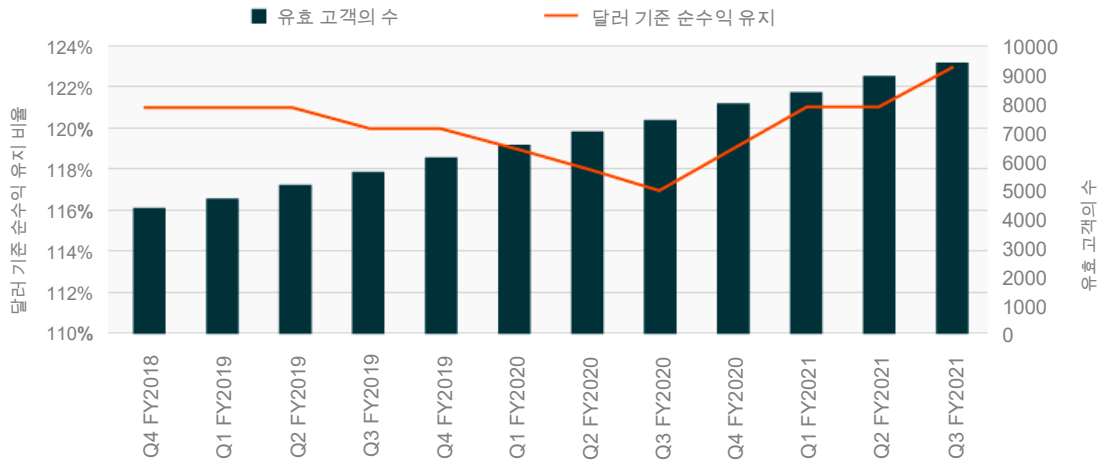
또한 IAM 부문의 회사들은 원격 및 하이브리드 근무 환경으로의 이동에서 혜택을 볼 것으로 기대됩니다. 직원들이 여러 장소에서 근무하고 서로 다른 기기로 연결함에 따라 IAM은 IT 부서로 하여금 누가 주어진 시간에 특정한 앱에 접속하는지 모니터링하도록 해줍니다. 또한 IAM은 일정한 내부 애플리케이션에 접속해야 하는 계약업체 또는 고객에게 제공한 접속 포인트를 모니터링하고 안전을 유지하는 데 도움을 줍니다.

Okta의 IAM 솔루션은 최종 사용자 관점에서 단일 포털 내의 모든 애플리케이션에 대한 접속권을 제공합니다. 이러한 특징은 로그인 관련 헬프데스크 통화량을 50% 줄여주고 새로운 앱으로의 로그인 및 사용을 50% 더 빠르게 만들어 줍니다.[13] Okta는 처리 가능한 직원 ID 총 시장을 300억 달러, 고객 ID 시장을 250억 달러로 추정합니다.[14]

CrowdStrike 및 Zscaler와 마찬가지로 Okta의 솔루션은 클라우드 네이티브입니다. 이 기업의 수익은 서비스 사용에서 나오기 때문에 94%가 반복적입니다. Okta는 달러 기준 순수익 유지 비율이 견고한 회사로서, 2021 회계연도 3분기에 12개월을 추적한 결과 123%를 기록하여 지난 분기 대비 2% 성장했습니다.

OKTA 의 달러 기준 순수익 유지 비율(왼편) 및 유효 고객(오른편)

출처: Global X ETF, Okta 기업 제출서류.



Mimecast: 최고의 이메일 보안 제공업체

Mimecast는 아마도 가장 잘 알려진 유형의 사이버 보안 부문, 보안 이메일 게이트웨이의 최고 플레이어입니다. 사이버 공격의 95%가 기회를 틈탄 타겟 공격의 선호 채널로 이메일을 활용합니다.[15] 전 세계 비즈니스 이메일 사용자 10억명을 고객으로 두고 있는 Mimecast의 성장 가능성은 상당합니다.[16] 현재 동사는 약 1,500만 명의 사용자, 즉 총 글로벌 시장의 1.5%를 고객으로 두고 있습니다.[17]

대량 피싱과 타겟 스피어 피싱 공격의 목표는 이메일 메시지를 보내 수신자가 특정 행동을 취하게 만드는 것입니다.[18] 이때 공격자는 돈이나 지적재산과 같이 매우 중요한 데이터를 해킹하려 합니다. FBI는 2013년 10월과 2018년 5월 사이에 이메일 침해에 의해 총 120억 달러의 피해가 발생한 것으로 추정됩니다.[19] 이메일 피싱 및 사칭 사기는 오늘날 언제든 존재하지만, 코로나19 대유행으로 인해 더 많은 시간을 온라인에서

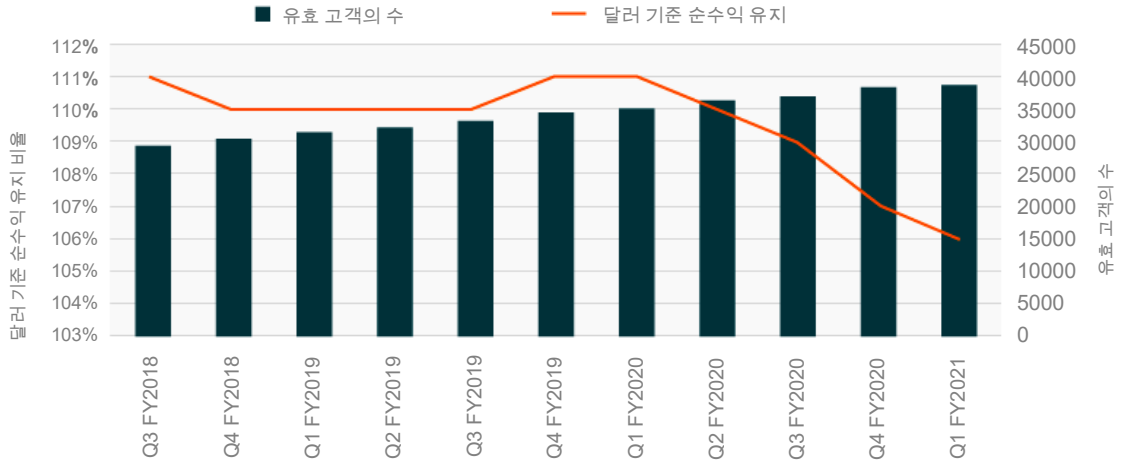
보내는 사람들로 인해 그러한 행동을 하기에 더욱 좋은 환경이 조성되었습니다. 사실, 이메일 피싱 및 사칭 사기는 코로나19가 대유행한지 첫 100일 동안에만 30% 증가했습니다.[20]

Mimecast는 알려지거나 알려지지 않은 멀웨어, 악성 URL, 그리고 직원이나 은행, 연방기관 또는 고객 및 공급업체와 같은 제3자 조직의 사칭이 담긴 이메일을 탐지하여 차단하는 솔루션을 제공합니다. Mimecast는 안전하지 않은 이미지와 로고를 식별하기 위한 딥 러닝, 이메일의 변칙적이고 위험한 패턴을 탐지하기 위한 머신 러닝, 고위험 링크를 분류하기 위한 지도 학습과 같은 AI 기능으로 전통적인 탐지 기법을 보완합니다.

또한 Mimecast는 클라우드 네이티브 아키텍쳐를 구현함으로써 매력적인 비즈니스 모델에 민첩성을 부여합니다. 동사는 지난 수 년 동안 달러 기준 순수익 유지 비율을 100% 이상 유지하고 사이버 보안 비즈니스 모델의 강점을 늘려왔습니다.[21]

MIMECAST 의 달러 기준 순수익 유지 비율(왼편) 및 유효 고객(오른편)

출처: Global X ETF, Mimecast 회사 제출서류.



결론

사이버 보안은 기업의 예산의 많은 부분을 차지합니다. 점점 많은 수의 사이버 공격 및 해킹으로 인한 전 세계 여러 부문과 정부에 대한 잠재적인 영향으로 인해 사이버 보안 도구는 조직이 여러 업무 기능을 안전하게 운영하는 데 필수적인 요소가 되었습니다. 이메일이든, ID 관리든, 내외부 앱 접속이든, 최종 사용자 기기 보호든, 여기에서 살펴본 4개 회사는 이렇듯 커지는 디지털 세상을 더 안전하게 유지하는 데 키 플레이어로서 사이버 보안 업계의 다면적인 성격을 잘 보여줍니다.

각주:

1. IDC, “새로운 IDC 지출 가이드에 따르면, 지속적인 수요로 인해 보안 제품 및 서비스가 견조한 성장을 이룰 것이다”, 2020년 8월 13일.
2. IDG, “2020년 IDG 클라우드 컴퓨팅 설문조사”, 2020년 6월 8일.
3. Identity Theft Resource Center, “Identity Theft Resource Center의 2020년 3분기 데이터 침해 분석 및 주요한 배울 점” 2020년 10월 14일.
4. CrowdStrike, “기업 개요”, 2020년 12월.
5. 같은 출처.
6. CrowdStrike, (n4).
7. Zscaler, “투자자 관계: 클라우드 통계”, 2021년 1월 19일에 접속.
8. Zscaler, “Zero Trust Network 접속 소개”, 2021년 1월 19일 접속.
9. Zscaler, “VPN 대안”, 2020년 6월.
10. Zscaler, “Zscaler 2021년 분석가의 날”, 2021년 1월 11일.
11. 같은 출처.
12. Gartner, “ID 및 접속 관리(IAM)”, 2021년 1월 19일 접속.

13. Okta, “싱글 사인 온”, 2021년 1월 19일 접속.
14. Okta, “2021 회계연도 3분기 실적”, 2020년 12월 2일
15. Mimecast, “이메일 보안에 대한 2020 Gartner 시장 가이드”, 2021년 1월 19일 접속.
16. Mimecast, “Mimecast 투자자 프레젠테이션”, 2020년 11월.
17. 같은 출처.
18. Mimecast, “귀사를 보호하는 이메일 보안”, 2021년 1월 19일 접속.
19. FBI, “업무 이메일 침해 120억 달러 스캠”, 2018년 7월 12일.
20. Mimecast, “이메일 보안 상태: 다운로드 허브”, 2021년 1월 19일 접속.
21. Mimecast, (n16).

.