FORTINET

3세대 샌드박스를 통한 AI 기반 보안 침해 방지

목차

FORTINET

종합 요약

급격히 진화하는 위협 동향으로 인해 지난 5년 사이에 보안 침해 빈도는 67% 증가하였고 기업당 사이버 범죄 비용 합계는 72%가 늘어났습니다.[1] 이제 멀웨어는 다양한 변종, 인공 지능(AI)과 같은 지능적 전략을 동원해 오래된 도구(예: 이전 세대의 샌드박스 기기)의 탐지를 회피합니다. 알려지지 않은 위협에서 발생하는 데이터 침해를 예방하려면 기업에서는 샌드박스에 대한 전략을 다시 평가해야 합니다. 답은 3세대 샌드박스 솔루션에 있습니다. 3세대 샌드박스 솔루션은 관리와 보고 기능을 단순화하는 공통적인 보안 용어를 사용할 뿐만 아니라 보안 통합, 실시간 위협 인텔리전스 공유, 지능적 AI를 통한 정적 분석 및 동작 분석 기능을 통해 기업 전체의 자동화된 방어를 지원할 수 있습니다.

오래된 샌드박스로 인한 보안 침해 취약성 발생

위협 동향에서 고유한 공격 횟수와 목표를 실행하기 위한 기술 수준이 나날이 진화하고 있습니다. 그 증거로, 작년의 평균 데이터 침해 비용은 392만 달러로 상승했습니다. 여기에는 성공한 공격을 찾아내서 억제하기까지 평균 279일이 걸린다는 점이 많은 영향을 미쳤습니다.[2] 각종 변종이 나오는 요즘의 최신 멀웨어는 AI를 사용하여 동시다발적으로 새로운 맞춤형 공격을 만듭니다.[3] 언제나 새로운 멀웨어 중 제로데이거나 알려지지 않은 위협인 비율이 40%까지 존재하기 때문에[4] 보안 시스템에서 공격을 탐지해 차단하기가 더욱 어려워졌습니다.

오래된 보안 솔루션(방화벽, 2세대 샌드박스 기기 포함)은 모든 새로운 위험을 커버하기에는 한계가 있어서 많은 보안 담당자가 서로 다른 공급업체의 포인트 보안 제품들을 이용해 방어할 수밖에 없는 실정입니다. 따라서 보안 팀은 여러 가지 비표준 보안 용어를 배우고 여러 보안 콘솔을 관리해야 할 뿐만 아니라, 관리와 보고 기능에 수동 워크플로를 사용해야 합니다. 일반적으로는 이런 복잡성으로 인해 종합적인 위협 인텔리전스 공유가 불가능해지면서 기업 전체적으로 위협에 대해 실시간으로 자동화된 대응을 할 수 없게 됩니다.

설상가상으로 보안 담당자는 제로데이와 다른 알려지지 않은 공격을 차단해 보안 침해를 예방해야 하는 현실에 처해 있습니다. 이를 위해서는 보안 담당자는 지능적 AI 기능을 제공하고 기업의 전반적인 보안 아키텍처와 통합되는 3세대 샌드박스 솔루션을 구현해야 합니다.

샌드박스의 발전

- **1세대 샌드박스는 지능적 위협을 탐지하는 데 사용하는 독립형 물리적 기기였습니다.**
- **2세대 샌드박스는 광범위한 보안 아키텍처의 다른 기기와 통합되어 기업 전체의 지능적 위협을 탐지합니다.**
- **3세대 샌드박스에는 정적 분석과 동작 분석이 모두 가능한 안정적인 AI 기능까지 포함되었습니다.**

3세대 샌드박스의 구성 요소

1세대와 2세대 샌드박스는 보호 기능이 오래되고 매우 제한적이지만 여전히 다양한 종류가 시장에 나와 있습니다. 보안 담당자가 샌드박스 간의 차이를 알아내기는 매우 어려울 수 있습니다. 기본적으로 효과적인 3세대 샌드박스 솔루션에는 3가지 중요한 기능이 포함되어야 합니다.

- **정적 분석과 동적 분석이 모두 가능한 AI**를 활용하여 제로데이 위협에 대한 탐지 효율을 높여서 진화하는 위협 동향에 대응해야 합니다.
- **보편적 보안 언어**로 된 보고에 읽기 쉬운 표로 모든 멀웨어 기술을 분류한 표준화된 프레임워크를 활용해야 합니다(예: MITRE ATT&CK 프레임워크).
- **완전히 통합된 보안 아키텍처에서 위협 인텔리전스를 공유**하고 자동적인 보안 침해-보호-대응을 제공해야 합니다. 실시간으로 제로데이에 맞서기 위해서는 필요한 기능입니다.

보안 담당자는 이런 3세대의 필수 기능 외에도 5가지 영역에서 샌드박스 솔루션의 효과를 평가해야 합니다.

보안 효율성

샌드박스는 보안 이벤트에 즉시 대응해야 위험 노출을 최소화할 수 있습니다. 이 경우, 솔루션의 평가 기준은 유효 위협 탐지율뿐만 아니라 기업의 투자수익률(ROI)에 영향을 미치는 탐지 시간 지표도 포함해야 합니다.[5] 위협을 빠르게 찾아 침해를 억제할수록 복구 비용이 감소합니다.

샌드박스에서는 시기적절하게 감염을 차단하고 보고하는 기능과 모니터링 대상 네트워크의 보안과 기능을 유지하는 것이 중요합니다.[6]

기업에서는 대부분 네트워크를 안전하게 지키는 보안 솔루션의 기능과 트래픽을 대량으로 처리하는 네트워크 기능 중에서 선택해야 합니다. 그러나 오늘날과 같이 인프라가 진화하는 시대에는 그 두 가지가 균형을 이루어야 합니다. 샌드박스의 보안 효과는 성능을 고려하여 평가해야 하고, 그 반대도 필요합니다.[7] 또한, 국제적 조사에서 얻은 위협 인텔리전스, 지역적으로 공유되는 컨텍스트 인식, (그중에서도 특히) 자체적인 AI 기반 분석 도구를 적용하여 알려지지 않은 위협을 탐지해야 합니다.

이 점을 염두에 두고 제3자 테스트 기업(예: NSS Labs)에서 보안 효과와 탐지 시간 측면에서 "추천" 등급을 받은 샌드박스를 찾아야 합니다. 따라서 구매할 샌드박스의 효과를 평가하려면 보안 담당자는 다음을 고려해야 합니다.

- **통합**. 샌드박스는 기업 전체의 방어 아키텍처에서 다른 보안 솔루션과 연결되어 더 나은 가시성과 관리 기능을 제공해야 합니다. 샌드박스를 통합하면 위협 정보를 즉시 공유하는 기능을 통해 기업 전체 보안 에코시스템에서 자동적인 위협 완화 대응이 가능해집니다. 이는 보안 침해를 예방하는 데도 도움이 됩니다.
- **지능적 AI 분석**. 현재 시장에 나와 있는 대부분 샌드박스는 AI 기능이 전혀 탑재되어 있지 않습니다. AI를 사용한다고 주장하는 샌드박스의 경우에도 정적 분석만 가능할 뿐입니다. 그러나 진정한 AI 기반 샌드박스 솔루션이라면 정적 분석과 동적 분석을 모두 적용하고 멀웨어가 실행되는 동안 보안 침해 지표(IOC)를 찾아내, 알려진 위협과 새로운 동작을 모두 발견할 수 있어야 합니다. AI 분석은 새로운 동작이 점점 더 많은 빈도로 나타나게 되면서 중요 보안 우려 사항과의 관계를 자동으로 추적하고 판단 할 수 있게 됩니다.
- **탐지 + 예방**. 효과적인 멀웨어 침입 탐지는 신속하고 정확하게 이루어져야 관리자들이 감염을 억제하고 네트워크에 미치는 영향을 최소화할 수 있습니다.[8] 따라서 보안 담당자는 보안 침해 방지 및 탐지 기능을 지원하는 샌드박스를 찾아야 합니다. 이전 세대의 샌드박스 솔루션은 위협 탐지는 제공합니다. 그러나 보안 침해의 횟수와 비용을 낮추려면 보안 침해가 일어나기 전에 방지하는 데 도움을 주는 샌드박스가 필요합니다. 이제 잠재적 위협을 시기적절하게 차단하고 보고하는 샌드박스의 예방 기능이 매우 중요해졌습니다.
- **자체 기술**. 시중에 나와 있는 가장 효과가 뛰어난 샌드박스 솔루션은 대개 사내에서 개발된 독창적 기술을 기반으로 합니다. 일반적으로 이런 기업들이 제품을 최신으로 유지하고, 완전히 패치를 적용하고, 현재 위협 동향에 가장 알맞은 최신 기능을 도입합니다.

간소화된 운영

CISO의 절반 이상(57%)이 가장 큰 문제점으로 "지나치게 많은 수동 프로세스"를 꼽았고 그다음으로 "멀웨어 및 공격 누락"을 꼽았습니다."[9]. 그러나 그와 동시에 대부분(65%) 기업이 사이버 보안 인력이 부족하다고 보고했습니다.[10] 빠듯한 예산 제약에도 직면하는 경우가 많아서 필요에 따라 리소스를 확대하기 어렵습니다.

- **자동화된 보안 관리**. 제로데이 인텔리전스를 다른 인라인 보안 관제로 공유하는 통합 샌드박스를 사용하면 네트워크 전체를 자동으로 보호할 수 있습니다. 이런 안정적인 보안 자동화는 수동 프로세스를 제거하는 데 도움이 됩니다. 직원에 대한 부담을 덜어주는 동시에 보안을 개선하고 운영 경비(OpEx)를 절감해주기 때문입니다.
- **자동 멀웨어 보고**. 통합적 샌드박스는 통합 프레임워크를 사용한 보편적 보안 용어로 보고하고, 모든 멀웨어 기술을 읽기 쉬운 표로 분류합니다. 보안 관리가 간단해지면서도 수동 프로세스를 사용해야 할 필요가 없습니다. 즉, 사고와 관련된 알림과 컨텍스트 정보를 조사하고 실천 가능한 위협-완화 프로세스로 변환할 수 있게 됩니다. 이런 보편적 언어의 예시로는 MITRE ATT&CK가 있습니다. 이는 실제 관측 결과를 기반으로 한 공격 전술과 기술을 모은 국제적인 기술 자료로, 민간 부문과 정부, 사이버 보안 제품과 서비스 커뮤니티에 널리 도입되어 있습니다.[11]

CISO는 "지나치게 많은 수동 프로세스"와 "멀웨어 공격 누락"을 가장 큰 보안 문제로 꼽았습니다.

38%의
기업이 현재 자동화, 인공 지능, 기계 학습을 효과적으로 활용하고 있습니다. 따라서 기존의 보안 모델로는 해결할 수 없는 지능적 위협도 대비 할 수 있습니다.[12]

확장성

3세대 샌드박스는 디지털 혁신이 도입되면서 일어나는 트래픽 증가와 인프라 변화에 맞게 확장을 지원해야 합니다. 충분한 성능 용량, 유연한 라이선스, 다양한 배포 옵션도 제공해야 합니다. 핵심적 기능에는 다음이 포함됩니다.

- **클러스터링**. 보안 담당자는 클러스터링을 지원하는 솔루션을 찾아야 합니다. 예를 들어, 향후 네트워크 확장, 트래픽 수요 증가, 보안 요구 사항의 확대를 뒷받침할 만큼 클러스터당 노드 개수가 충분해야 합니다.
- **배포**. "온프레미스 전용" 폼팩터(가상 머신(VM), 클라우드 기반 옵션 포함)에서 벗어난 샌드박스 솔루션은 배포 위치와 방식에 유연성을 제공합니다. 예를 들어 클라우드 기반 샌드박스 폼팩터는 서비스형 인프라(IaaS)의 탄력적 성격을 이용해 분산된 인프라에서 운영 확장성을 개선할 수 있습니다.

비용 관리

대부분 샌드박스 솔루션은 여러 기기 및/또는 구독이 필요하고, 따라서 총소유비용(TCO)이 증가합니다. 주로 고려해야 할 사항은 다음과 같습니다.

- **통합 보호**. 3세대 샌드박스는 추가적인 라이선스와 비용 없이도 전체 공격 면(네트워크, 엔드포인트, 웹, 이메일, 클라우드)에 적용되어야 합니다. 또한, 보안 에코시스템 전체에서 다른 중요한 솔루션(예: 차세대 방화벽(NGFW))과 통합되어 보안 소켓 계층(SSL)/전송 계층 보안(TLS) 암호화 트래픽에 숨은 공격을 발견할 수도 있어야 합니다. 이런 종류의 통합 기능이 없는 샌드박스는 암호화/복호화 기능을 구매해야 할 수도 있어서, 자본 지출(CapEx)과 운영 복잡성이 늘어나게 됩니다.
- **보호된 Mbps당 비용**. 대부분 기업에서는 비용을 걱정하기 마련이고, 샌드박스는 보호된 Mbps당 비용(NSS Labs 등의 제삼자 테스트 기업 측정 기준)을 낮추고 추가적인 구독 비용을 제거해야 합니다.

배포, 유지관리, 유지하는 전반적 비용에 여러 가지 요소가 영향을 미치기 때문에 샌드박스는 구현이 복잡할 수 있습니다.[13]

진화하는 위협 동향에 맞추어 설계된 AI 기반 보안

지능적 AI 기반 멀웨어 변종이 배로 늘어나고 제로데이 위협의 위험으로 인해 보안 침해의 가능성이 커지고 있기 때문에, 기업에서는 오래된 샌드박스를 오늘날의 위협 동향에 맞게 설계된 솔루션으로 대체할 방안을 생각해야 합니다. 통합적인 3세대 샌드박스는 보안 효과, 관리 기능, 확장성, 비용을 개선하여 보안 리더들에게 보안 침해를 탐지하고 예방하는 능력을 제공합니다.

1 "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, 2019년 3월 6일.

2 "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, 2019년 7월.

3 "AI-driven Cyber Crime Brings New Challenges to CISOs: Too Fast, Too Agile, Too Dangerous for Traditional Security Approaches," Fortinet, 2019년 6월 21일.

4 FortiGuard Labs 내부 데이터.

5 "NSS Labs Announces 2018 Breach Detection Systems Group Test Results," NSS Labs, 2018년 10월 11일.

6 Jessica Williams, et al., "Breach Prevention Systems Test Report," NSS Labs, 2019년 8월 7일.

7 상게서.

8 상게서.

9 "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, 2019년 4월 26일.

10 "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.

11 "MITRE ATT&CK," MITRE, 2019년 11월 25일에 액세스.

12 "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, 2019년 3월 6일.

13 Jessica Williams, et al., "Breach Prevention Systems Test Report," NSS Labs, 2019년 8월 7일.

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 전화: 080-559-8989 Email: kr-callcenter@fortinet.com

483924-0-0-EN