네트워크 포렌식 (PX 시리즈)

요약

제대로 관리된 경계선 방어는 모든 보안 전략의 핵심입니다. 조직들은 공격을 조사하고 분석하기 위해 경계선 방어를 강력한 포렌식 기능으로 보완해야 한다는 것을 점점 인식하고 있습니다. 공격을 받았을 때 기업은 위협을 효과적으로 억제하고 네트워크 보안을 지키기 위해 이를 신속하게 조사하고 사고의 범위와 피해를 판단할 수 있어야 합니다.

FireEye Network Forensics을 사용하면 풀 패킷을 매우 빠른 속도로 캡처 및 인덱스화하여 보안 사고를 더욱 신속하게 식별하고 해결할 수 있습니다. Network Forensics를 통해 광범위한 보안 사고를 탐지하고, 대응의 질을 개선하며, 각 보안 사고의 영향을 정확하게 정량화할 수 있습니다.

Network Forensics는 FireEye의 종합적인 위협 방어 기능을 보완합니다. 분석가들은 정확한 경보 및 관계가 있는 위협 정보를 받을 수 있을 뿐만 아니라 공격 전, 중, 후에 특정한 패킷과 세션에 대한 세밀한 분석 결과를 입수하여 무엇이 악성코드 다운로드 또는 콜백을 유발했을지 확인하고, 신속하고 효과적으로 대응하며, 이러한 정보를 적용하여 향후의 방어 전략을 강화할 수 있습니다.

킬 체인 복원 가속화 및 영향의 정량화

사용자들이 보안 이벤트 전, 중, 후에 트래픽 및 세션을 신속하게 파악하고 해독하도록 지원함으로써, Network Forensics는 이벤트 관련 활동에 대해 뛰어난 가시성을 제공합니다. 또한 신속한 사고 대응 조사에 매우 중요할 수 있는 가시성을 더욱 향상시켜 줍니다.

네트워크의 과거 데이터에 초고속으로 접근하는 것은 사고를 해결하는 평균 시간을 줄일 뿐만 아니라 '침해가 존재했던 기간', '네트워크로부터 이미 유출된 데이터의 종류', '침해를 당한 다른 호스트들의 수' 등과 같은 중요한 질문들에 답변하기 위해 반드시 필요합니다.

빠른 패킷 캡처, 인덱싱 및 검색

최대 20Gbps의 기록 속도의 나노초 타임 스탬프를 사용하여 지속적이고 손실이 없는 패킷 캡처를 제공합니다. 나노초 타임 스탬프와 연결 속성을 사용하여 캡처된 모든 패킷의 실시간 인덱스화로 즉각적인 포렌식을 위한 데이터를 제공합니다.

업계 표준 데이터 저장 및 내보내기 기능

다양한 온보드 스토리지 구성 및 SAS 또는 SAN에 연결된 스토리지 옵션을 통해 기업들은 유연성과 확장을 위한 공간을 확보할 수 있습니다. 모든 패킷은 가능한 모든 지원 분석 플랫폼에 유연성을 제공하기 위해 표준 PCAP 형식으로 저장됩니다.

주요 기능

- 최대 20Gbps의 기록 속도의 나노초 타임 스탬프를 사용하여 지속적이고 손실이 없는 패킷 캡처 제공
- 타임 스탬프와 연결 속성을 사용하여 캡처된 모든 패킷의 실시간 인덱스화. 다른 플로우 분석 툴과 함께 사용하기 위해 NetFlow v5, v9 및 IPFIX 포맷으로 플로우 지수 익스포트
- 특허 출원 중인 인덱싱 아키텍처를 사용하여 표적 연결과 패킷에 대한 초고속 조사 및 검색
- 패킷, 연결 및 세션의 검사를 위한 웹 기반의 드릴다운 GUI
- 웹, 이메일, FTP, DNS, 채팅, SSL 연결 세부 사항 및 첨부 파일을 관찰하고 검색하기 위한 세션 디코더 지원
- 정규 표현식을 사용하여 패킷 페이로드 검색
- 분석을 위해 PCAP 형식으로 가져오고 내보내는 기능을 제공하는 업계 표준의 데이터 저장 공간
- 이벤트 기반 캡처를 사용하여 보다 심층적인 조사가 필요한 의심스러운 세션을 파악하는 신속한 조사 프로세스
- 독점적인 알고리즘을 사용하여 잠재적으로 비정상적인 네트워크 행동을 진단함으로써 데이터 도난을 식별하는 자동화된 프로세스

실시간 위협 인텔리전스 시그니처 분석

Network Forensics는 FireEye iSIGHT Intelligence 네트워크와 통합되어 새로운 위협 시그니처 다운로드와 실시간 위협 시그니처 분석의 프로세스를 자동화합니다. 위협이 탐지되면 Network Forensics는 분석가가 위협을 신속하게 조사할 수 있도록 경보를 작동합니다.

FireEye 위협 방지 솔루션과 통합된 워크플로

FireEye 솔루션과의 완전한 통합은 가장 규모가 크고 사용량이 많은 네트워크에서 캡처, 인덱스화, 저장된 연결 및 패킷 정보에 대한 접근을 통해 네트워크 트래픽과 활동에 대한 심층적인 드릴다운 분석을 제공합니다. 사용자들이 보안 이벤트 전, 중, 후에 트래픽 및 세션을 신속하게 파악하고 해독하도록 지원함으로써, Network Forensics는 이벤트 관련 활동에 대해 뛰어난 가시성을 제공합니다. 또한 신속한 사고 대응 조사에 매우 중요할 수 있는 가시성을 더욱 향상시켜줍니다.

의심스러운 세션 강조

사용자들은 조사 프로세스를 가속화하고, 의심스러운 세션 데이터에 플래그를 지정하는 사용자 지정 가능한 규칙을 생성함으로써 시간이 지남에 따라 발생하는 이벤트들의 상관관계를 파악할 수 있습니다. 이를 통해 심층적인 조사와 장기적인 보존을 확보할 수 있습니다. 지정 이벤트에 결합된 조사들은 하나의 사례로 관리될 수 있습니다.

기술 사양

	캡처 포트 설정	관리 포트	최대 기록 속도	총 온보드 스토리지	크기	전원/일반 작동 부하
PX 004S	4 x 1Gbps SFP	2 x 10/100/1000 BASE-T	500Mbps	6TB	4.3 x 42.67 x 35.56cm (1.7" x 16.8" x 14") 5kg(11lbs)	200W 낮은 노이즈의 AC 전원 100-240V, 60-50Hz 자동 범위 조정
PX 1004ESS-16	4 x 1Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000 BASE-T	1.5Gbps	16TB, 확장 가능한 SAS가 연결된 저장 공간	1U 랙 마운트 4.3 x 43.7 x 65.0cm (1.7" x 17.2" x 25.6") 20.9kg(46lbs)	650W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정 230-280W 일반
PX 1020ESS-16	2 x 10Gbps, SFP+	2 x 10/100/1000/10G BASE-T	1.5Gbps	16TB, 확장 가능한 SAS가 연결된 저장 공간		
PX 2004ESS-48	4 x 1 Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000/ 10G BASE-T	4Gbps	48TB, 확장 가능 SAS가 연결된 저장 공간		
PX 2020ESS-48	2 x 10Gbps, SFP+	2 x 10/100/1000/ 10G BASE-T	5Gbps, 20Gbps로 업그레이드 가능	48TB, 확장 가능한 SAS가 연결된 저장 공간	2U 랙 마운트 8.9 x 43.7 x 64.8cm (3.5" x 17.2" x 25.5") 23.6kg(52lbs)	1280W 고효율 (1+1) 중복 AC 전원 100-240 VAC 60-50Hz 자동 범위 조정
PX 2040ESS-48	4 x 1/10Gbps SFP/SFP+	2 x 10/100/1000/ 10G BASE-T	5Gbps, 20Gbps로 업그레이드 가능	48TB, 확장 가능한 SAS가 연결된 저장 공간		
PX 1004EXT-4G	4 x 1Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	4Gbps	온보드 스토리지 없음. 외부 SAN 스토리지에 섬유 HBA 연결	1U 랙 마운트 4.3 x 43.7 x 65.0cm (1.7" x 17.2" x 25.6") 20.9kg(46lbs)	650W 고효율(1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정 230-280W 일반
PX 1040EXT-20G	4 x 1Gbps,	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	20Gbps			
PX 2000SX-24	해당 없음	해당 없음	해당 없음	ESS 모델을 위한 24TB 스토리지 선반 확장	2U 랙 마운트 8.9x43.7x64.8cm (3.5"x17.2"x25.5") 23.6kg(52lbs)	500W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정
PX 2000SX-48	해당 없음	해당 없음	해당 없음	ESS 모델을 위한 48 TB 스토리지 선반 확장		
PX 4000SX-264	해당 없음	해당 없음	해당 없음	ESS 모델을 위한 264 TB 스토리지 선반 확장	4U 랙 마운트 17.8 x 43.7 x 64.8cm(7" x 17.2" x 27.5") 34kg(75lbs)	1280W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정

주: 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다.

FireEye에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오.

www.FireEye.com

FireEye, Inc. 소개

FireEye는 인텔리전스 기반 SaaS(Security-as-a-Service)의 리더입니다. FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 맨디언트 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 간소화합니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함해 67개국의 5,000여 기업을 고객으로 보유하고 있습니다.

FireEye Korea |
서울특별시 강남구 테헤란로 534 글라스타워 20층 |
02.2092.6580 | korea.info@fireeye.com | www.fireeye.kr

www.FireEye.com

FireEye