Network Forensics Platform

활용 가능한 인텔리전스를 가속화하고 신속한 사고 대응을 촉진

데 이 터 시 트

주요 기능

- 최대 20Gbps까지의 기록 속도에서 나노초 타임 스탬프를 사용하여 지속적이고 손실이 없는 패킷 캡쳐를 제공
- 타임 스탬프와 연결 속성을 사용하여 캡쳐된 모든 패킷에 대한 실시간 인덱스화. 다른 플로우 분석 툴과 함께 사용하기 위해 NetFlow v5, v9 및 IPFIX 포맷으로 플로우 지수 익스포트
- 특허 출원 중인 인덱스화 아키텍처를 사용하여 표적 연결과 패킷에 대한 초고속 조사 및 검색
- 패킷, 연결 및 세션의 검색과 검사를 위한 웹 기반의 드릴다운 GUI
- 웹, 이메일, FTP, DNS, 채팅, SSL 연결 세부 사항 및 첨부 파일을 관찰하고 검색하기 위한 세션 디코더 지원
- 일반적인 표현을 사용하는 패킷 페이로드 검색
- 다음과 같은 유연한 스토리지 옵션을 사용하여 저장할 수 있는 산업 표준 데이터 스토리지와 PCAP 포맷의 익스포트: 어플라이언스, SAS 연결 또는 SAN 연결 스토리지.

요약

잘 관리된 경계선 방어는 모든 보안 전략의 핵심입니다. 조직들은 또한 공격을 조사 및 분석하기 위해 경계선 방어를 강력한 포렌식 능력으로 보완해야 한다는 것을 점차적으로 더욱 인식하고 있습니다. 기업은 공격을 받았을 때 이를 신속하게 조사하고 사고의 범위와 피해를 판단하여 위협을 효과적으로 억제하고 네트워크 보안을 재구축할 수 있어야 합니다.

FireEye®Network Forensics Platform (네트워크 포렌식 플랫폼)을 사용하면 풀 패킷을 매우 빠른 속도로 캡쳐 및 인덱스화하여 보안 사고를 신속하게 식별 및 해결할 수 있습니다. Network Forensics Platform은 광범위한 보안 사고를 탐지하고, 대응의 질을 개선하고, 각 사고의 영향을 정확하게 정량화할 수 있는 능력이 있습니다.

Network Forensics Platform은 FireEye의 종합적인 위협 방어 능력을 충분히 보완합니다. 정확한 경보 및 상관 관계가 있는 정보를 받는 것에 추가하여, 분석가들은 또한 공격 전, 중, 후에 특정한 패킷과 세션에 대한 세밀한 분석 결과를 입수하여 악성코드 다운로드 또는 콜백이 무엇을 유발할 수 있는지 확인하고, 공격에 신속하고 효과적으로 대응하고, 이러한 정보를 적용하여 향후의 방어 전략을 강화할 수 있습니다.

킬 체인 복구 및 영향 계량화를 촉진

FireEye 사용자들이 보안 이벤트 전, 중, 후에 트래픽 및 세션을 신속하게 파악하고 해독하게 함으로써, Network Forensics Platform은 이벤트 주위의 활동에 대해 더 뛰어난 가시성을 제공하고, 신속한 사고 대응 조사에 매우 중요한 가시성을 더욱 강화합니다.

과거의 네트워크 데이터에 대한 초고속 접근은 보안 직원이 사고를 해결하는 평균 시간을 줄이는 것은 물론, 다음과 같은 중요한 질문들에 답변하기 위해 반드시 필요합니다: 침해가 존재했던 기간, 네트워크로부터 이미 유출된 데이터의 종류, 침해를 당했을 수도 있는 다른 호스트들의 수.

초고속 패킷 캡쳐, 인덱스화, 검색

Network Forensics Platform은 최대 20Gbps까지의 기록 속도에서 나노초 타임 스탬프를 사용하여 지속적이고 손실이 없는 패킷 캡쳐를 제공합니다. 나노초 타임 스탬프와 연결 속성을 사용하여 캡쳐된 모든 패킷에 대한 실시간 인덱스화로 즉각적인 포렌식을 위한 데이터를 제공합니다.

산업 표준 데이터 스토리지와 익스포트

모든 패킷은 표준인 PCAP 포맷으로 저장되어 선택한 분석 플랫폼에 유연성을 제공할 수 있습니다.

워크플로우를 FireEye Threat Prevention Platform과 통합

FireEye 플랫폼과의 통합은 가장 크고 바쁜 10Gbps 네트워크에서 캡쳐, 인덱스화 및 저장된 연결 및 패킷 정보에 대한 간단한 드릴다운 접근을 통해서 네트워크 트래픽과 활동에 대한 심층적인 통찰력을 제공합니다. FireEye 사용자들이 보안 이벤트 전, 중, 후에 트래픽 및 세션을 신속하게 파악하고 해독하게 함으로써, 네트워크 포렌식 플랫폼은 이벤트 주위의 활동에 대해 더 뛰어난 가시성을 제공하고, 신속한 사고 대응 조사에 매우 중요한 가시성을 더욱 강화합니다.

	캡쳐 포트 설정	최대 기록 속도	총 온보드 스토리지	크기	전원/일반 작동 부하
PX 004S	4 x 1Gbps SFP	500Mbps	2TB	1.7" x 16.8" x 14" (4.3 x 42.67 x 35.56cm)	11lbs (5kg)	200W 저 노이즈 AC 전원 100-240V, 60-50 Hz 자동 범위 조정
PX 1004ESS-16	4 x 1Gbps, 10/100/1000BaseT, SFP	1.5Gbps	16TB, 확장 가능 SAS 연결 스토리지	1U 랙 마운트 | 1.7" x 17.2" x 25.6" (4.3 x 43.7 x 65.0cm) | 46lbs (20.9Kg)	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+	1.5Gbps	16TB, 확장 가능 SAS 연결 스토리지		
PX 2004ESS-24	4 x 1Gbps, 10/100/1000BaseT, SFP	4Gbps	24TB, 확장 가능 SAS 연결 스토리지	2U 랙 마운트 | 3.5" x 17.2" x 25.5" (8.9 x 43.7 x 64.8cm) | 52lbs (23.6Kg)	1280W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정
PX 2004ESS-48	4 x 1Gbps, 10/100/1000BaseT, SFP	4Gbps	48TB, 확장 가능 SAS 연결 스토리지		
PX 2020ESS-24	2 x 10Gbps, SFP+	5Gbps, 20Gbps로 업그레이드 가능	24TB, 확장 가능 SAS 연결 스토리지		
PX 2020ESS-48	2 x 10Gbps, SFP+	5 Gbps, 20Gbps로 업그레이드 가능	48TB, 확장 가능 SAS 연결 스토리지		
PX 2040ESS-48	4 x 10Gbps, SFP+	5Gbps, 20Gbps로 업그레이드 가능	48TB, 확장 가능 SAS 연결 스토리지		
PX 1004EXT-4G	4 x 1Gbps, 10/100/1000BaseT, SFP	4Gbps	온보드 스토리지 없음 외부 SAN/NAS 스토리지를 섬유 HBA로 연결	1U 랙 마운트 | 1.7" x 17.2" x 25.6" (4.3 x 43.7 x 65.0cm) | 46lbs (20.9Kg)	650W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정 230-280W 일반
PX 1020EXT-10G	2 x 10Gbps, SFP+	10Gbps			
PX 1020EXT-20G	2 x 10Gbps, SFP+	20Gbps			
PX 1040EXT-20G	4 x 10Gbps, SFP+	20Gbps			
PX 2000SX-24	해당 없음	해당 없음	ESS 모델에 대한 24TB 스토리지 선반 확장	2U 랙 마운트 | 3.5" x 17.2" x 25.5" (8.9 x 43.7 x 64.8cm) 52lbs | (23.6Kg)	500W 고효율 (1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정
PX 2000SX-48	해당 없음	해당 없음	ESS 모델에 대한 48TB 스토리지 선반 확장		
PX 2000SX-264	해당 없음	해당 없음	ESS 모델에 대한 264TB 스토리지 선반 확장	4U 랙 마운트 | 7" x 17.2" x 27.5" (17.8 x 43.7 x 64.8cm) | 75lbs (34Kg)	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.

더 자세히 알아보십시오

FireEye는 종합적인 서비스 포트폴리오를 제공합니다. 전체적인 세부 내용을 원하시면 services@FireEye.com 또는 +1 855.692.2052로 연락해 주십시오.

왜 FireEye를 선택해야 할까요?

전문성 기술 인텔리전스

FireEye는 공격자들이 표적으로 삼는 전세계에서 가장 귀중한 자산을 보호합니다. 저희는 기술, 인텔리전스, 전문성을 통합하고, 가장 적극적인 사고 대응팀을 보강하여, 보안 침해로 인한 피해를 방지합니다. 저희는 침해의 모든 단계에서 공격자들을 탐지 및 방어합니다. FireEye를 사용하면 공격이 발생하는 즉시 탐지할 수 있습니다. 또한 이러한 공격이 고객의 가장 귀중한 자산에 대해 일으키는 위험을 이해할 수 있습니다. 그리고 사고를 신속하게 억제 및 해결하는 툴과 지원을 제공받습니다. FireEye 글로벌 방어 커뮤니티에는 67개국의 2,700여 고객들이 가입되어 있고, 포춘 500대 기업 중 157개가 넘는 기업들이 포함되어 있습니다.

FireEye Korea | 서울특별시 강남구 테헤란로 440 포스코센터 서관 11층 | 02.559.073 | korea.info@fireeye.com | www.fireeye.kr