데이터 시트

네트워크 포렌식

고성능 패킷 캡처 및 조사 분석을 통해 네트워크 공격으로 인한 영향 최소화

조직이 침해 사고 범위 및 영향을 판단하여 위협을 효과적으로 억제하고 네트워크의 보안을 재구축하기 위해서는 사고에 대한 조기 탐지 및 신속한 조사가 필요합니다 .

FireEye Network Forensics 솔루션은 업계에서 가장 빠르고 손실이 없는 네트워크 데이터 캡처 및 검색 솔루션과 중앙 집중화된 분석 및 시각화 기능을 결합했습니다 . 이 솔루션은 조사를 간소화하고 위험을 줄여주는 단일 워크벤치를 사용하여 네트워크 포렌식 프로세스를 가속화합니다 .

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

조사 분석 어플라이언스는 FireEye Network Forensics 솔루션의 일부로 , 사용하기 쉬운 분석 인터페이스가 포함된 중앙 집중식 워크벤치를 추가함으로써 숨겨진 위협을 밝혀내고 사고 대응을 가속화합니다 .

분석가들은 공격 전 , 중 , 후에 특정 네트워크 패킷 및 세션을 검토할 수 있습니다 . 악성코드 다운로드 또는 콜백을 유발하는 이벤트를 재구성 및 시각화하는 기능을 갖춘다면 보안팀은 재발을 방지하기 위해 효과적이고 빠르게 대응할 수 있습니다 . 또한 네트워크 내부에서 공격을 분산하는 데 일반적으로 사용되는 프로토콜을 해독하여 공격자 활동에 대한 가시성을 확장할 수 있습니다 .

이처럼 고성능 패킷 캡처와 심층 분석을 독보적으로 조합함으로써 공격의 모든 요소를 빠르게 인식하고 모니터링할 수 있습니다 .

그림 1. 패킷 캡처 및 분석을 위한 FireEye Network Forensics 어플라이언스

패킷 캡처 주요 기능

- **고성능:** 최대 20Gbps의 기록 속도로 타임 스탬프를 사용하여 지속적이고 손실이 없는 패킷 캡처 제공
- **높은 정확도:** 타임 스탬프와 연결 속성을 사용하여 캡처된 모든 패킷의 실시간 인덱스화. JSON 형식으로 플로우 인덱스 및 연결 메타데이터 내보내기. 플로우 인덱스는 NetFlow v9, IPFIX 및 Silk Tools 데이터 형식으로 변환할 수 있습니다.
- **빠른 결과:** 특허받은 인덱싱 아키텍처를 사용하여 표적 연결 및 패킷에 대한 초고속 조사 및 검색
- **풍부한 상황 정보:** 패킷, 연결 및 세션의 검색 및 검사를 위한 웹 기반의 드릴다운 GUI
- **광범위한 가시성:** 웹, 이메일, FTP, DNS, 채팅, SSL 연결 세부 사항 및 첨부 파일을 확인 및 검색하기 위한 세션 디코더 지원
- **지능형 캡처:** 캡처된 트래픽의 선택적 필터링을 통해 스트리밍 비디오, 대용량 파일 전송, 암호화된 페이로드 등 제거
- **향상된 효율성:** 독점적인 알고리즘을 사용하여 비정상적인 네트워크 행동을 진단함으로써 데이터 도난을 파악하는 자동화된 프로세스

표 1. 사용 가능한 패킷 캡처 어플라이언스

모델	캡처 포트 설정	관리 포트	최대 기록 속도	총 온보드 스토리지	크기	전원/일반 작동 부하
PX 1004S-6	1 x 2GigE	1 x 1GbE	500Mbps	6TB	1U 17.2인치(437mm) x 19.7인치(500mm) x 1.7인치(44mm) 18파운드(8.2kg)	AC, 고정 AC 100-240V @ 50-60Hz, IEC60320-C14 인렛
PX 2060ESS-96	4 x 10GE SFP+	2 x 1GbE	2Gbps	96TB, 확장 가능한 SAS 연결 스토리지	2U 17.24인치(438mm) x 24.41인치(620mm) x 3.48인치(88.4mm) x 57.3파운드(26.0kg)	중복(1+1) 800와트, 100-240VAC 10.5-4.0A, 50-60Hz IEC60320-C14 인렛, FRU
PX 2060ESS-120	4 x 10GE SFP+	2 x 1GbE	7.5Gbps	120TB, 확장 가능한 SAS 연결 스토리지	2U 17.24인치(438mm) x 24.41인치(620mm) x 3.48인치(88.4mm) x 57.3파운드(26.0kg)	중복(1+1) 800와트, 100-240VAC 10.5-4.0A, 50-60Hz IEC60320-C14 인렛, FRU
PX 1004EXT-4G	4 x 1Gbps, 10/100/1000 BaseT, SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	4Gbps	온보드 스토리지 없음. 외부 SAN 스토리지에 Fiber HBA 연결	1U 랙 마운트 1.7인치(4.3cm) x 43.7cm(17.2") x 65.0cm(25.6") 20.9 kg(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	온보드 스토리지 없음. 외부 SAN 스토리지에 Fiber HBA 연결	1U 랙 마운트 1.7인치(4.3cm) x 43.7cm(17.2") x 65.0cm(25.6") 20.9 kg(46lbs)	650W 고효율(1+1) 중복 AC 전원 100-240 VAC, 60-50Hz 자동 범위 조정 230-280W 일반
PX 4000SX440	해당 없음	해당 없음	해당 없음	440TB 기본 스토리지 셸프	17.2인치(437mm) x 27.5인치(698mm) x 7인치(178mm) 34kg(76lbs)	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.

FireEye 조사 분석 어플라이언스는 단일 노드와 분산된 아키텍처에 대한 여러 구성을 지원하여 메타데이터 집계 , 쿼리 및 분석의 대역폭 및 성능을 최적화합니다 .

조사 분석 주요 기능

- **시각화 기능:** 생성하기 쉬운 맞춤형 대시보드를 통해 네트워크 메타데이터 및 활동의 확인 및 공유 가능
- **신속한 응답:** 모든 경보, 캡처된 플로우 및 메타데이터에 대한 중앙 집중식 애플리케이션 수준 키워드, 정규식 및 와일드카드 쿼리 수행
- **민첩한 인터페이스:** 관심 있는 세션에 대한 개별 또는 대량 PCAP 데이터의 즉각적인 피벗 및 다운로드
- **강력한 검색:** HTTP, SMTP, POP3, IMAP, SSL, TLS, DNS, FTP 등의 프로토콜에서 인덱스된 메타데이터를 사용하여 검색 가속화
- **IOC 집계:** 경보에서 세션 데이터로의 즉각적인 "원 클릭" 피벗을 통해 단일 워크벤치에 모든 네트워크 메타데이터와 함께 FireEye 네트워크 보안, 이메일 보안 및 엔드포인트 보안 제품 경보 통합
- **소급적인 위협 헌팅:** FireEye 위협 인텔리전스, STIX 및 OpenIOC 피드를 자동화된 IA 검색 기능과 통합함으로써 "과거의" IOC 위협 분석. 며칠 또는 몇 주 전에 네트워크에 있던 IOC 위협을 자동으로 알림
- **한 번의 클릭으로 파일 복구:** 추가 분석을 위해 의심스러운 파일, 웹 페이지 및 이메일을 빠르고 안전하게 복구

표 2. 사용 가능한 조사 분석 어플라이언스

모델	총 온보드 스토리지	크기	전원/일반 작동 부하
IA 1000 DIR	6TB	17.2인치(437mm) x 19.7인치(500mm) x 1.7인치(44mm)	AC, 고정 AC 100-240V @ 50-60Hz, IEC60320-C14 인렛
IA 2100-48	48TB	17.2인치(437mm) x 19.7인치(500mm) x 1.7인치(44mm)	중복(1+1) 800와트, 100-240VAC 10.5-4.0A, 50-60Hz IEC60320-C14 인렛, FRU

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.