McAfee Network Threat Behavior Analysis

네트워크 동작 및 위협에 대한 완벽한 가시성 확보

McAfee® Network Threat Behavior Analysis는 네트워크 인프라에 대한 실시간 가시성과 위협 보호를 제공하는 McAfee Network Security Platform의 통합 구성요소입니다. McAfee Network Threat Behavior Analysis는 스위치와 라우터로부터 트래픽을 분석하여 네트워크에서 위험한 동작을 식별하고 은폐형 공격을 효율적으로 방지합니다. 네트워크 수준 위협을 전체적으로 평가하고, 각 네트워크 요소의 전체 동작을 식별하고, 악성 프로그램, 제로 데이 공격, 봇넷 및 웜을 포함한 잠재적인 이상 또는 위협 유형의 즉각적인 추상화를 사용합니다. McAfee Network Threat Behavior Analysis는 또한 시그니처가 없는 악성 프로그램을 식별하는 실시간 에뮬레이션 엔진을 포함하여 McAfee Network Security Platform의 고급 엔진 일부를 내장하고 있습니다.

주요 이점

네트워크 보안을 위한 가시성

- 네트워크 트래픽 분석으로 비정상적인 네트워크 동작을 모니터링 및 보고합니다.
- 동작을 기반으로 하여 사전 예방적으로 위협을 탐지합니다.
- 알 수 없는 위협을 효율적으로 탐지합니다.
- 이상 탐지에는 제로 데이, 스팸, 봇넷 및 정찰 공격이 포함됩니다.

포괄적 악성 프로그램 방지

- 악성 파일에 대한 실시간 에뮬레이션으로 악성 프로그램을 차단합니다.
- 봇넷 활동 탐지를 위해 네트워크 전반에서 고급 상관관계 분석을 수행합니다.
- 네트워크 흐름과 이벤트를 위한 엔드포인트 인텔리전스와 상관관계 분석이 제공됩니다.

오늘날의 은폐형 공격에 대한 지능형 가시성

네트워크는 기존의 탐지 방법을 회피하는 발전된 형태의 은밀한 공격을 직면하고 있으므로 심각한 손상을 주는 위반 및 가동 중단에 노출되어 있습니다. McAfee Network Threat Behavior Analysis는 스위치와 라우터로부터 네트워크 트래픽을 분석하여 비정상적인 동작을 지능적으로 모니터링 및 보고하여 네트워크상의 공격을 식별하고 신속히 대응하도록 돕습니다.

McAfee Network Threat Behavior Analysis 어플라이언스는 NetFlow와 J-Flow 데이터를 활용하여 일반적인 침입 방지 시스템(IPS)의 경계를 벗어난 위협을 구분합니다. 이 어플라이언스는 쿼드 코어 프로세서, RAID 디스크 배열 및 기가비트 이더넷 연결을 모두 갖추고 있습니다. 또한 오프라인 SAN(Storage Area Network) 연결을 제공합니다. 별도의 흐름 용량과 함께 대량의 네트워크 트래픽을 처리하고 보다 빠른 트래픽 분석을 지원할 수 있습니다.

최고 수준의 네트워크 가시성 및 인사이트

McAfee Network Threat Behavior Analysis를 통해 네트워크의 응용프로그램과 프로토콜에 대해 정보에 입각한 의사 결정을 내릴 수 있습니다. 비정상적인 네트워크 동작을 모니터링하고 보고하며 동작 기반 알고리즘을 통해 위협을 식별합니다. 호스트와 응용프로그램 동작을 모두 분석함으로써 제로 데이 공격, 스팸, 봇넷 및 정찰 공격에 대한 이상 탐지를 제공합니다.

포괄적인 흐름 분석을 통해 무단 응용프로그램 사용을 식별하고 문제가 있는 네트워크 구간을 찾아냅니다.

악성 프로그램 아웃브레이크 제어 및 방지

McAfee Network Threat Behavior Analysis는 McAfee Network Security Platform과 연계하여 의심스러운 파일의 고급 검사와 차단을 위한 실시간 에뮬레이션을 제공합니다. 실시간 에뮬레이션 엔진은 의심스러운 파일을 스캔하여 악성 동작을 탐지하고 차단합니다. McAfee Network Threat Behavior Analysis는 여러 IPS와 네트워크 장치에 걸친 고급 상관관계 분석을 통해 기존의 시그니처 기반 방어를 우회하는 은폐형 봇넷를 찾아냅니다. McAfee Endpoint Intelligence Agent와 함께라면 정상적인 네트워크 트래픽으로 위장하여 악성 트래픽을 발송하는 손상된 엔드포인트를 찾아서 제어할 수 있습니다. 엔드포인트 활동에 대한 평판 기반 분석으로 데이터 유출을 제한하고 악성 프로그램 발생을 방지합니다.

보안 운영 간소화 및 비용 절감

McAfee Network Threat Behavior Analysis는 비용 효율적인 보안 관리에 필요한 실행 가능한 인사이트를 제공합니다. 이 어플라이언스는 인시던트 응답 시간을 가속화하고 네트워크 성능을 간소화하는 동시에 비즈니스 운영을 방해하는 네트워크 위협과 취약성 공격을 방지합니다.

추가 기능

- McAfee Global Threat Intelligence(McAfee GTI)와의 통합을 통한 향상된 보안
- 비용 효율적인 구현을 위한 가상 버전
- McAfee ePolicy Orchestrator®(McAfee ePO™) 소프트웨어, McAfee Enterprise Security Manager 및 McAfee Vulnerability Manager 소프트웨어를 통합하여 가시성과 상관관계 분석 확대
- 네트워크 트래픽의 간편한 정렬 및 분석
- 흐름당 메타데이터(App ID, 파일, URL) 대시보드
- 포괄적인 격리 옵션으로 보안 상태 강화
- 자세한 호스트 위협 요소 평가를 통한 외부 호스트 가시성
- Cisco(NetFlow v5 및 v9)와 Juniper(J-Flow v5 및 v9)의 스위치 및 라우터와 호환

	NTBA T-600	NTBA T-1200
사양		
초당 흐름	최대 60,000	최대 100,000
Cisco NetFlow	v5 및 v9	v5 및 v9
Juniper J-Flow	v5 및 v9	v5 및 v9
프로세서	1x Xeon E5-2658	2 x Xeon E5-2658
메모리	46 GB	96 GB
사용 가능한 저장소	4.4TB / Raid 10	8.8TB / Raid 10
네트워크 인터페이스	x4 Copper 10/100/1000	x4 Copper 10/100/1000
환경		
폼 팩터	1U	2U
너비	17.244in(438mm)	17.244in(438mm)
깊이	27.93in(709.37mm)	27.87in(707.8mm)
높이	1.7in(43.2mm)	3.45in(87.6mm)
최대 하중	14.96kg	21.6kg
예상 입력 전원 사용률 (최악의 경우)	402W	667W
중복 전원 공급 장치	750W	750W
시스템 냉각 요구 사항(시간당 BTU)	1370	2280
작동 온도	시간당 10°C를 초과하지 않는 최대 변경 비율로 +10°C에서 +35°C까지	

가상 NTBA 사양	T-VM	T-100VM	T-200VM
권장 RAM	16 GB	8GB	16 GB
권장 CPU	4	4	4
초당 흐름	최대 25,000fps	최대 10,000fps	최대 25,000fps

McAfee
An Intel Company

한국맥아피(주)
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.mcafee.com/kr

60839ds_ntba_0214_ETMG