McAfee Network Security Platform

포괄적이며 지능적인 고급 위협 보호 플랫폼

McAfee® Network Security Platform는 네트워크 전반의 정교한 악성 프로그램 위협을 탐지하고 차단하는 차세대 IDPS(침입 탐지 및 방지 시스템)입니다. 지능형 감지 및 에뮬레이션 기술을 활용하여 단순한 패턴 매칭을 벗어나서 높은 수준의 정확도로 은폐형 공격을 방어할 수 있습니다. 이 플랫폼은 까다로운 네트워크의 요구 사항을 충족할 수 있도록 단일 장치에서 30Gbps 이상으로 확장할 수 있고 스택 시 최대 100Gbps까지 확장 가능합니다. 통합 McAfee 솔루션 포트폴리오는 실시간 McAfee® Global Threat Intelligence 피드를 사용자, 장치 및 응용프로그램에 관한 다양한 컨텍스트 데이터와 결합함으로써 보안 작업을 간소화하여 네트워크에서 발생하는 공격에 대해 신속하고 정확하게 응답할 수 있습니다.

오늘날의 은폐형 위협으로부터 보호

디지털화로 보안 환경이 크게 변경되었습니다. 클라우드, 모빌리티 및 IoT로 인해 사실상 보호할 '엣지' 또는 경계가 사라진 새로운 수준의 연결이 나타났습니다. 위험의 양과 심각성이 거의 하룻밤 사이에 급속하게 증가하고 있습니다. 많은 기업이 이제 데이터 보호에 집중하고 있습니다. 그 결과, 강한 네트워크 보안 전략은 데이터 보호의 핵심이 되었습니다. 네트워크는 기존의 감지 방법을 회피할 수 있는 지능적인 은폐형 공격에 직면하면서 응용프로그램과 데이터가 심각한 손상을 주는 위반 및 가동 중단에 노출되어 있습니다. 안타깝게도 대다수의 조직은 재정 및 운영 자원이 부족하기 때문에 적절한 방어를 제공하는 데 필요한 도구와 기술의 조합을 구현하거나 관리할 수 없습니다.

McAfee Network Security Platform는 지능형 위협 방지와 직관적인 보안 관리를 결합해 감지 정확성을 개선하고 보안 운영을 간소화합니다. 하나의 악성 프로그램 감지 기술로 모든 공격을 방어할 수 없기 때문에 McAfee Network Security Platform는 원치 않는 악성 프로그램으로 인해 네트워크에 큰 손해가 발생하지 않도록 여러 가지 시그니처 및 무 시그니처 검색 엔진을 통합했습니다. 악성 프로그램 콜백, 서비스 거부(DoS,denial-of-service), 제로 데이 공격 및 기타 고급 위협에 대한 감지 및 보호를 위해 전체 프로토콜 분석, 위협 평판, 동작 분석을 포함하는 고급 기술의 조합을 이용하여 심층적인 네트워크 트래픽 검사를 수행합니다.

통합 보안

McAfee Network Security Platform은 심도 있는 정적 코드 분석, 동적 분석(악성 프로그램 샌드박싱) 및 기계 학습을 결합하여 우회 공격 기술과 랜섬웨어를 사용하는 위협을 포함한 제로 데이 위협을 감지하는 McAfee® Advanced Threat Defense와 통합됩니다. 또한 McAfee Network Security

주요 이점

- 위협을 빠르게 감지하여 차단함으로써 응용프로그램과 데이터를 보호
- 동적 환경을 위한 확장 가능한 고성능 솔루션
- 가시성 및 제어를 위한 중앙 집중식 관리
- 시그니처를 사용하지 않는 악성 프로그램 분석을 포함한 고급 감지
- 네트워크 트래픽 조사를 위한 인바운드 및 아웃바운드 SSL 암호 해독
- 고가용성 및 재해 복구 보호
- 가상 어플라이언스도 사용 가능
- 장치-클라우드 간 보안을 위해 McAfee 솔루션 포트폴리오와 통합

McAfee에 문의

Platform는 McAfee Global Threat Intelligence의 파일 평판을 통합하며 모든 관련 소스 전반의 실시간 네트워크 이벤트 상호 연계를 위해 McAfee® ePolicy Orchestrator® 소프트웨어와 McAfee® Enterprise Security Manager와의 통합을 제공합니다. 조직은 장치 세부 정보, 사용자 정보, 엔드포인트 보안 상태, 취약성 평가를 비롯해 여러 가지 다양한 정보를 통합한 이 통합 솔루션으로 위협 심각도와 비즈니스 위험 요인에 대한 이해도를 높일 수 있습니다.

성능 및 가용성

McAfee Network Security Platform은 보안과 고성능 두 부문의 이점을 모두 제공합니다. 이는 싱글 패스, 프로토콜 기반의 검사 아키텍처와 통신업체급 맞춤 하드웨어를 결합하여 100Gbps 이상의 실제 환경 검사를 실시합니다. 이 효율적인 아키텍처는 보안 설정과 상관없이 성능을 유지하지만, 다른 IPS 솔루션은 성능보다 보안을 중요시하는 정책으로 인해 처리량이 최대 50% 감소될 수 있습니다.

McAfee Network Security Platform는 또한 상태 저장 페일오버를 통한 능동-능동 및 능동-수동을 제공하여 성능이 느린 어플라이언스나 과부하된 독립형 솔루션의 병목 현상을 피하는 동시에 고가용성 SLA를 충족할 수 있도록 돕습니다.

투자 보호를 제공하는 확장 가능한 하드웨어 플랫폼

McAfee NS7500 및 NS9500 시리즈 어플라이언스는 고객에게 유연성을 제공하므로 고객은 지금 필요한 것을 구입하고, 소프트웨어 라이선스를 통해 요구 사항에 필요한 만큼 처리량을 쉽게 확장할 수 있습니다. McAfee NS9500 어플라이언스의 경우, 여러 개의 McAfee NS9500 어플라이언스를 스태킹하여 추가 용량을 더할 수도 있습니다.

가시성 및 제어

네트워크의 응용프로그램과 프로토콜에 대해 정보에 입각한 의사 결정을 내리십시오. McAfee Network Security Platform은 지능형 위협 방지와 응용프로그램 인식 기능을 하나의 보안 의사 결정 엔진에 통합한 최초의 IDPS 솔루션입니다. McAfee는 위협 활동을 2,000개 이상의 응용프로그램과 프로토콜에 대한 계층 7 가시성을 포함한 응용프로그램 사용과 연결하여 네트워크에서 허용할 응용프로그램에 대해 정보에 입각한 의사 결정을 내릴 수 있도록 지원합니다.

McAfee Network Security Platform는 응용프로그램 식별 이외에 사용자 및 장치 가시성을 제공합니다. 네트워크 이상 동작을 식별함으로써 활성 봇네트를 포함해 위험한 호스트와 사용자의 우선 순위를 지정합니다.

확장 가능한 지능형 보안 관리

지능형 네트워크 보안 관리를 통해 보안 투자를 최대한 활용하십시오. McAfee Network Security Manager는 적게는 2개에서 많게는 수백 개의 네트워크 보안 어플라이언스에서 확장 가능한 웹 기반 관리를 제공합니다. 적절한 경보 및 사용하기 쉬운 보안 대시보드를 안내하는 직관적이며, 점진적인 정보 노출 워크플로를 통해 관리자는 경보 심각도와 관련성을 토대로 이벤트의 우선순위를 자동으로 지정할 수 있습니다.

추가 기능

지능형 위협 방지

- 인바운드 SSL(Secure Sockets Layer) 암호 해독은 센서 성능에 영향을 미치지 않는 에이전트 기반 공유 키 솔루션 (특허 출원 중, NS 시리즈용)을 이용하는 DH(Diffie-Hellman) 및 ECDH(Elliptic-Curve Diffie–Hellman) 암호화를 지원
- 아웃바운드 SSL 암호 해독(NS 시리즈)

- McAfee® Gateway Anti-Malware 에뮬레이션 엔진
- PDF JavaScript 에뮬레이션 엔진
- Adobe Flash 동작 분석 엔진
- Microsoft Office 전체 파일 검사 엔진
- 고급 우회 공격 방지
- 모바일 위협 평판 및 클라우드 분석

봇네트 및 악성 프로그램 콜백 보호

- DNS/DGA Fast flux 콜백 감지
- DNS sinkholing
- 휴리스틱 봇 감지
- 다중 공격 상관 관계
- 명령 및 제어 데이터베이스

고급 침입 방지

- IP 조각 모음 및 TCP 스트림 재조립
- McAfee의 사용자 정의 및 공개 소스 시그니처
- Snort 시그니처를 위한 기본 지원(NS 시리즈)
- STIX(Structured Threat Information eXpression) (McAfee NS 시리즈)를 지원하는 허용 목록/차단 목록 개선 사항
- 호스트 격리 및 등급 제한
- 가상 환경 검사
- McAfee Advanced Threat Defense와 통합
- HTTP 응답 압축 풀기 지원

DoS 및 DDoS 방지

- 임계값 및 휴리스틱 기반 감지
- 호스트 기반 연결 제한
- 자체 학습, 프로필 기반 감지

McAfee Global Threat Intelligence

- 파일, IP 및 URL 평판
- 응용프로그램 및 프로토콜 평판
- 위치정보
- McAfee Global Threat Intelligence 범주를 기반으로 한 허용 목록

고가용성

- 상태 저장 페일오버를 통한 능동-능동 및 능동-수동 지원
- 외부 페일오픈(능동)
- 기본 제공되는 페일오픈

프로토콜 터널링 지원

- IPv6
- V4-in-V4, V4-in-V6, V6-in-V4 및 V6-in-V6 터널
- MPLS
- GRE
- Q-in-Q 이중 VLAN

McAfee® Network Security Manager

- 계층적 관리 기능으로 최대 1,000개 센서 지원
- 사용자 인증(RADIUS 및 LDAP)
- 자동 페일오버 및 페일백
- 중요한 구성 데이터의 재해 복구
- 중앙 집중식 계층적 정책 관리
- 장치별 메모리 사용량 세부 정보를 보여주는 메모리 대시보드

자세히 알아보기

더 자세한 내용과 물리적 어플라이언스 옵션에 대해서는 McAfee Network Security Platform 사양 시트를 참조하십시오.

What To Look For in an IDPS(침입 탐지 및 방지 시스템(IDPS)의 요건)에 대해 자세히 알아보십시오.

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr