



McAfee Network Security Platform

네트워크 보안에 대한 고유한 지능형 접근 방식

McAfee® Network Security Platform은 네트워크에서 복잡한 위협을 발견하고 차단하는 고유한 지능형 보안 솔루션입니다. 지능형 탐지 및 에뮬레이션 기술을 사용하여 단순한 패턴 매칭을 벗어나서 뛰어난 정확도로 은폐형 공격을 방어할 수 있습니다. 이 차세대 하드웨어 플랫폼은 단일 장치로 40Gbps 이상의 속도로 확장되어 까다로운 네트워크 요구를 충족합니다. McAfee의 보안 관리를 통해 실시간 McAfee GTI(McAfee Global Threat Intelligence) 피드를 사용자, 장치 및 응용프로그램에 관한 다양한 컨텍스트 데이터와 결합함으로써 보안 작업을 간소화할 수 있으므로 네트워크에서 발생하는 공격에 대해 신속하고 정확하게 응답할 수 있습니다.

주요 이점

최고 수준의 지능형 위협 방지

- 시그니처를 사용하지 않는 지능형 악성 프로그램 분석
- 인라인 브라우저 및 JavaScript 에뮬레이션
- 고급 봇넷 및 악성 프로그램 콜백 탐지
- 브라우저 기반 분석 및 DDoS 보호
- McAfee Advanced Threat Defense와 통합

통합 보안 아키텍처

- McAfee TIE(Threat Intelligence Exchange)를 통한 실시간 위협 공유
- ePolicy Orchestrator®(McAfee ePO™)를 통한 엔드포인트 컨텍스트
- McAfee Endpoint Intelligence Agent를 통한 엔드포인트 프로세스 수정
- McAfee Enterprise Security Manager(SIEM)를 통한 데이터 공유 및 격리
- McAfee Vulnerability Manager를 통한 호스트 위험 분석
- McAfee GTI를 통한 예측 악성 프로그램 탐지

오늘날의 은폐형 위협으로부터 보호

네트워크는 기존의 탐지 방법을 회피할 수 있는 지능적인 은폐형 공격을 직면하고 있으므로 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 Platform은 지능형 위협 방지와 직관적인 보안 관리를 결합해 탐지 정확성을 개선하고 보안 운영을 간소화하는 통합 네트워크 보안 플랫폼입니다. 지능형 위협, 악성 프로그램 콜백, 제로 데이 위협 및 서비스 거부 공격에 대한 업계 최고의 보호 성능을 제공합니다. 처음부터 McAfee의 통합 보안 아키텍처와의 통합을 염두에 두고 개발된 McAfee Network Security Platform은 조직 간 보안 데이터를 활용하여 다른 보안 솔루션에서 놓치기 쉬운 보안 격차를 해소하는 데 도움이 됩니다.

최고 수준의 위협 방지

McAfee Network Security Platform은 라인 레이트 속도를 유지하면서 네트워크 트래픽을 심층적으로 검사할 수 있도록 설계된 차세대 검사 아키텍처에 기반을 두고 있습니다. 이는 전체 프로토콜 분석, 위협 평판, 동작 분석 및 지능형 악성 프로그램 분석 등 각종 지능형 검사 기술 조합을 사용하여 네트워크에서 확인된 공격과 제로 데이 공격을 모두 탐지한 후 방어할 수 있습니다.

포괄적 악성 프로그램 방어

하나의 악성 프로그램 탐지 기술로 모든 공격을 방어할 수 없기 때문에 McAfee Network Security Platform은 원치 않는 악성 프로그램으로 인해 네트워크에 큰 손해가 발생하지 않도록 여러 가지 시그니처 및 무 시그니처 검색 엔진을 통합했습니다. McAfee GTI의 파일 평판, JavaScript 검사를 통한 심층적인 파일 분석 및

주요 이점(계속)

성능 및 가용성

- 차세대 아키텍처
- 최대 40Gbps 처리량
- 비교할 수 없는 SSL 검사 성능
- 업계 최고의 안정성
- 능동-능동 및 능동-수동 가용성

지능형 보안 관리

- 지능형 경보 수정 및 우선 순위 분류
- 강력한 악성 프로그램 조사 대시보드
- 미리 구성된 조사 워크플로
- 확장 가능한 웹 기반 관리

가시성 및 제어

- 응용프로그램 식별
- 사용자 식별
- 장치 식별

지능형 안티맬웨어 엔진을 통합했기 때문에 사용자 지정 악성 프로그램 및 기타 은폐형 공격을 검색할 수 있습니다.

통합 보안 아키텍처

지금은 필요한 정보를 얻는 일이 어느 때보다 쉬워졌습니다. McAfee는 McAfee ePO 소프트웨어 및 McAfee Enterprise Security Manager의 실시간 통합을 제공하므로 관련된 모든 소스에 걸쳐 네트워크 이벤트의 상관관계를 실시간으로 확인할 수 있습니다. McAfee ePO 소프트웨어와 McAfee Enterprise Security Manager가 통합됨에 따라 McAfee Network Security Platform은 위협과 장치 및 사용자와의 관련성을 정확히 파악하고 어느 것이 조직에 가장 큰 위험이 되는지 식별할 수 있습니다. 조직은 장치 세부 정보, 사용자 정보, 엔드포인트 보안 상태, 취약성 평가를 비롯해 여러 가지 다양한 정보를 통합한 이 솔루션으로 위협 심각도와 비즈니스 위험 요인을 이해할 수 있습니다.

성능 및 확장성

보안과 고성능 두 부문의 이점을 모두 누리십시오. McAfee Network Security Platform은 싱글 패스(single-pass), 프로토콜 기반의 검사 아키텍처와 통신업체급 맞춤 하드웨어를 결합하여 하나의 장치에서 40Gbps 이상의 실제 환경 검사를 실시합니다. 이 고도로 효율적인 아키텍처는 보안 설정과 상관없이 성능을 유지하지만, 다른 침입 방지 시스템(IPS) 솔루션은 성능보다 보안을 중요시하는 정책으로 인해 처리량이 최대 50% 감소될 수 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 최초이자 유일한 IPS 솔루션입니다. McAfee는 위협 활동을 1,500 개 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 Platform은 응용프로그램 식별 이외에 사용자 및 장치 가시성을 제공합니다. 네트워크 이상 동작을 식별함으로써 활성 봇네트를 포함해 위험한 호스트와 사용자의 우선 순위를 지정합니다.

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 직관적인 점진적 정보 노출 워크플로를 통해 관리자는 경보 심각도와 관련성을 토대로 이벤트의 우선 순위를 자동으로 지정할 수 있습니다. 조직은 McAfee ePO 소프트웨어와 통합된 McAfee Network Security Platform을 사용하여 시스템 취약성, 네트워크 방어 및 엔드포인트 보안 수준을 기반으로 위험한 인프라에 대해 최신 평가를 수행할 수 있으며 기업 전체의 위험과 컴플라이언스를 통합적으로 볼 수 있습니다.



McAfee Network Security Platform을 통해 다음과 같은 이점을 누릴 수 있습니다

보안 허점 차단

- 악의적인 네트워크 활동 차단
- 은폐형 공격 방지
- 지능형 악성 프로그램 탐지

골치 아픈 관리 문제 감소

- 이벤트 우선 순위 자동 지정
- 조사 워크플로 간소화
- 불필요한 조정 제거

네트워크에 적용

- 1GigE, 10GigE, 40GigE 연결
- 40Gbps로 확장
- 능동-능동 및 능동-수동 가용성

추가 기능

지능형 위협 방지

- McAfee GAM(Gateway Anti Malware) 에디션 엔진
- PDF Javascript 에디션 엔진
- Adobe Flash 동작 분석 엔진
- 지능형 우회 공격 방지
- 모바일 위협 평판 및 클라우드 분석

봇넷 및 악성 프로그램 콜백 보호

- DNS/DGA Fast flux 콜백 감지
- DNS 싱크홀링
- 경험적 접근 봇 탐지
- 다중 공격 수정
- 명령 및 제어 데이터베이스

고급 침입 방지

- IP 조각 모음 및 TCP 스트림 재조립
- McAfee의 사용자 정의 및 공개 소스 시그니처
- 호스트 격리 및 등급 제한
- 가상 환경 검사

DoS 및 DDoS 방지

- 임계값 및 경험적 접근 기반 탐지
- 호스트 기반 연결 제한
- 자체 학습, 프로필 기반 탐지

McAfee GTI

- 파일 평판
- IP 평판
- 응용프로그램 및 프로토콜 평판
- 위치정보(Geo-locations)

고가용성

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

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, LDAP 및 TACACS)
- 자동 페일오버 및 페일백
- 중요한 구성 데이터의 재해 복구
- 중앙 집중식 계층적 정책 관리

McAfee Network Security Platform 사양

차세대 하드웨어



센서 하드웨어 구성 요소

NS9300

NS9200

NS9100

성능	NS9300	NS9200	NS9100
종합 성능	40Gbps	20Gbps	10Gbps
최대 처리량(UDP 1512바이트 패킷)	최대 70Gbps	최대 35Gbps	최대 30Gbps
최대 동시 연결	32,000,000	16,000,000	13,000,000
초당 연결	1,000,000	575,000	450,000
초당 HTTP 연결	750,000	375,000	260,000
SSL 암호 해독을 통한 처리량(10%의 SSL 트래픽 기준)	40Gbps	20Gbps	10Gbps
최대 SSL 플로우 수	3,200,000	1,600,000	1,200,000
가져온 SSL 키	1,024	1,024	1,024
통상적인 대기 시간	100µs 미만	100µs 미만	100µs 미만
가상 IPS 시스템 수	1,000	1,000	1,000
최대 DoS 프로파일	5,000	5,000	5,000
ACL 규칙	20,000	20,000	20,000
포트			
고정기가비트 이더넷 - 구리선 포트(내부 페일오븐)	16	8	8
고정 10 GigE/1 GigE(SFP+) 포트	—	—	—
고정 40기가비트 이더넷	—	2	2
네트워크 I/O 슬롯	4	2	2
네트워크 I/O 모듈(6가지 옵션)		4포트 10 GigE/1 GigE SR 광학 50 마이크론 페일오븐 4포트 10 GigE/1 GigE SR 광학 62.5 마이크론 페일오븐 4 포트(QSFP+) 40GigE, 2 포트(QSFP+) 40GigE, 8 포트(SFP+/SFP) 10GigE/1GigE 또는 6 포트(RJ45) 1GigE(내부 페일오븐)	
10기가비트 이더넷	최대 32	최대 16	최대 16
40기가비트 이더넷	최대 16	최대 10	최대 10
전용 응답 포트(RJ45)	1(10G/1G/100M)	1(10G/1G/100M)	1(10G/1G/100M)
전용 관리 포트(RJ45)	1(10G/1G/100M)	1(10G/1G/100M)	1(10G/1G/100M)
전용 저장 포트(RJ45)	1(10G/1G/100M)	1(10G/1G/100M)	1(10G/1G/100M)
물리적			
규격	2 x 2RU 랙 마운트 가능 17.24" (W) x 6.88" (H) x 28.76" (D)	2RU 랙 마운트 가능 17.24" (W) x 6.88" (H) x 28.76" (D)	2RU 랙 마운트 가능 17.24" (W) x 6.88" (H) x 28.76" (D)
무게	134lbs.	67lbs.	67lbs.
저장 장치	600GB(2 x RAID 1 구성의 이중 SSD 300GB)	RAID 1 구성의 이중 SSD 300GB	RAID 1 구성의 이중 SSD 300GB
최대 소비 전력	2,260W	1,130W	1,130W
DC 전원 사용 가능	선택 사항	선택 사항	선택 사항
예비 전원 공급 장치	포함됨	포함됨	선택 사항
전원	100-240VAC(50 / 60Hz)		
온도	0°~35°C(작동 시) -40°~70°C(비작동 시)		
상대 습도(비용결)	작동 시: 10%~90% 비작동 시: 5%~95%		
고도	0~10,000피트		
안전 인증	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB 라이선스 및 보고서는 모든 국가적 편차를 포함합니다.		
EMI 인증	FCC Part 15, 클래스 A(CFR 47)(미국) ICES-003 클래스 A(캐나다), EN55022 클래스 A(유럽), CISPR22 클래스 A(국제)		

Network Security Platform 사양 계속



센서 하드웨어 구성 요소	NS7300	NS7200	NS7100
성능			
종합 성능	5Gbps	3Gbps	1.5Gbps
최대 처리량(UDP 1512바이트 패킷)	최대 15Gbps	최대 10Gbps	최대 5Gbps
최대 동시 연결	10,000,000	5,000,000	3,000,000
초당 연결	225,000	200,000	135,000
초당 HTTP 연결	135,000	128,000	115,000
SSL 암호 해독을 통한 처리량(10%의 SSL 트래픽 기준)	5Gbps	3Gbps	1.5Gbps
최대 SSL 플로우 수	500,000	400,000	250,000
가져온 SSL 키	1,024	1,024	1,024
통상적인 대기 시간	100µs 미만	100µs 미만	100µs 미만
가상 IPS 시스템 수	1,000	1,000	1,000
최대 DoS 프로파일	5,000	5,000	5,000
ACL 규칙	5,000	3,000	3,000
포트			
고정기가비트 이더넷 - 구리선 포트(내부 페일오븐)	8	8	8
고정 10GigE/1GigE(SFP+) 포트(외부 수동 페일오븐 키트 지원)	2	2	2
고정 40기가비트 이더넷	—	—	—
네트워크 I/O 슬롯	2	2	2
네트워크 I/O 모듈(5가지 옵션)	4 포트 10GigE/1GigE SR 광학 50 마이크론 페일오븐, 4 포트 10GigE/1GigE SR 광학 62.5 마이크론 페일오븐, 4 포트 10GigE/1GigE LR 광학 페일오븐, 8 포트(SFP+/SFP) 10GigE/1GigE 또는 6 포트(RJ45) 1GigE 내부 페일오븐		
10기가비트 이더넷	최대 18	최대 18	최대 18
40기가비트 이더넷	—	—	—
전용 응답 포트(RJ45)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)
전용 관리 포트(RJ45)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)
전용 저장 포트(RJ45)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)	1 (1Gbps/100Mbps/10Mbps)
물리적			
규격	1RU 랙 마운트 가능 17.5" (W) x 1.69" (H) x 28.9" (D)	1RU 랙 마운트 가능 17.5" (W) x 1.69" (H) x 28.9" (D)	1RU 랙 마운트 가능 17.5" (W) x 1.69" (H) x 28.9" (D)
무게	31lbs.	31lbs.	29lbs.
저장 장치	반도체 160GB	반도체 160GB	반도체 160GB
최대 소비 전력	350W	350W	250W
DC 전원 사용 가능	선택 사항	선택 사항	선택 사항
예비 전원 공급 장치	선택 사항	선택 사항	선택 사항
전원	100-240VAC(50 / 60Hz)		
온도	0°~35°C(작동 시) -40°~70°C(비작동 시)		
상대 습도(비용결)	작동 시: 10%~90% 비작동 시: 5%~95%		
고도	0~10,000피트		
안전 인증	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB 라이선스 및 보고서는 모든 국가적 편차를 포함합니다.		
EMI 인증	FCC Part 15, 클래스 A(CFR 47)(미국) ICES-003 클래스 A(캐나다), EN55022 클래스 A(유럽), CISPR22 클래스 A(국제)		

Network Security Platform 사양 계속



센서 하드웨어 구성 요소	NS5200	NS5100
성능		
종합 성능	1Gbps	600Mbps
최대 처리량(UDP 1512바이트 패킷)	최대 3Gbps	최대 1.5Gbps
최대 동시 연결	1,350,000	750,000
초당 연결	45,000	40,000
초당 HTTP 연결	30,000	25,000
SSL 암호 해독을 통한 처리량(10%의 SSL 트래픽 기준)	1Gbps	600Mbps
최대 SSL 플로우 수	75,000	40,000
가져온 SSL 키	1,024	1,024
통상적인 대기 시간	100µs 미만	100µs 미만
가상 IPS 시스템 수	1,000	100
최대 DoS 프로파일	5,000	300
ACL 규칙	2,000	2,000
포트		
고정기가비트 이더넷 - 구리선 포트(내부 폐일오픈)	8	8
고정 1GigE(SFP) 포트	12	12
고정 10GigE/1GigE(SFP+) 포트(외부 수동 폐일오픈 키트 지원)	2	2
고정 40기가비트 이더넷	—	—
네트워크 I/O 슬롯	—	—
네트워크 I/O 모듈	—	—
10기가비트 이더넷	—	—
40기가비트 이더넷	—	—
전용 응답 포트(RJ45)	1(1G/100M)	1(1G/100M)
전용 관리 포트(RJ45)	1(1G/100M)	1(1G/100M)
전용 저장 포트(RJ45)	1(1G/100M)	1(1G/100M)
물리적		
규격	1RU 랙 마운트 가능 17.25" (W) x 1.75" (H) x 24.625" (D)	1RU 랙 마운트 가능 17.25" (W) x 1.75" (H) x 24.625" (D)
무게	22lbs.	22lbs.
저장 장치	반도체 80GB	반도체 80GB
최대 소비 전력	225W	225W
DC 전원 사용 가능	선택 사항	선택 사항
예비 전원 공급 장치	선택 사항	선택 사항
전원	100-240VAC(50 / 60Hz)	
온도	0°~35°C(작동 시) -40°~70°C(비작동 시)	
상대 습도(비응결)	작동 시: 10%~90% 비작동 시: 5%~95%	
고도	0~10,000피트	
안전 인증	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB 라이선스 및 보고서는 모든 국가적 편차를 포함합니다.	
EMI 인증	FCC Part 15, 클래스 A(CFR 47)(미국) ICES-003 클래스 A(캐나다), EN55022 클래스 A(유럽), CISPR22 클래스 A(국제)	

Network Security Platform 사양 계속



센서 하드웨어 구성 요소	NS3200	NS3100
성능		
종합 성능	200Mbps	100Mbps
최대 처리량(UDP 1512바이트 패킷)	최대 1Gbps	최대 600Mbps
최대 동시 연결	80,000	40,000
초당 연결	20,000	15,000
초당 HTTP 연결	15,000	12,000
SSL 암호 해독을 통한 처리량(10%의 SSL 트래픽 기준)	—	—
최대 SSL 플로우 수	—	—
가져온 SSL 키	—	—
통상적인 대기 시간	100µs 미만	100µs 미만
가상 IPS 시스템 수	32	16
최대 DoS 프로파일	128	128
ACL 규칙	1,000	1,000
포트		
고정 기가비트 이더넷 - 구리선 포트(내부 폐일오픈)	8	8
고정 1GigE(SFP) 포트	—	—
고정 10GigE/1GigE(SFP+) 포트(외부 수동 폐일오픈 키트 지원)	—	—
고정 40기가비트 이더넷	—	—
네트워크 I/O 슬롯	—	—
네트워크 I/O 모듈	—	—
10기가비트 이더넷	—	—
40기가비트 이더넷	—	—
전용 응답 포트(RJ45)	1(1G/100M)	1(1G/100M)
전용 관리 포트(RJ45)	1(1G/100M)	1(1G/100M)
전용 저장 포트(RJ45)	1(1G/100M)	1(1G/100M)
물리적		
규격	1RU 랙 마운트 가능 17.375" (W) x 1.75" (H) x 11.0" (D)	1RU 랙 마운트 가능 17.375" (W) x 1.75" (H) x 11.0" (D)
무게	8.1lbs.	8.1lbs.
저장 장치	반도체 30GB	반도체 30GB
최대 소비 전력	100W	100W
DC 전원 사용 가능	—	—
예비 전원 공급 장치	—	—
전원	100-240VAC(50 / 60Hz)	
온도	0°~35°C(작동 시) -40°~70°C(비작동 시)	
상대 습도(비용결)	작동 시: 10%~90% 비작동 시: 5%~95%	
고도	0~10,000피트	
안전 인증	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB 라이선스 및 보고서는 모든 국가적 편차를 포함합니다.	
EMI 인증	FCC Part 15, 클래스 A(CFR 47)(미국) ICES-003 클래스 A(캐나다), EN55022 클래스 A(유럽), CISPR22 클래스 A(국제)	

