McAfee Virtual Network Security Platform

클라우드 네트워크에 대한 완벽한 위협 탐지 및 침입 방지

McAfee® Virtual Network Security Platform(McAfee vNSP)은 개인 및 공용 클라우드의 고유한 요구 사항을 충족하도록 제작된 완벽한 네트워크 위협 및 IPS(침입 방지 시스템)입니다. 이 솔루션은 클라우드 아키텍처의 복잡한 위협을 정확하고 단순하면서도 빠르게 검색하고 차단함으로써 조직이 워크로드를 보호하고 컴플라이언스를 자신 있게 복원합니다. 고급 기술에는 시그니처를 사용하지 않는 탐지, 인라인 에뮬레이션 및 시그니처 기반 취약성 패치가 포함됩니다. 효율성 높은 워크플로우, 유연한 통합 옵션 및 간소화된 사용권으로 조직은 기존의 요구 사항과 향후 요구 사항을 충족하도록 보안을 쉽게 관리하고 조정할 수 있습니다.

완벽한 공용 클라우드 보안

공용 클라우드는 편리함과 비용 절감 효과는 물론, 인프라 비용을 운영 지출 모델로 전환할 수 있는 기회를 제공합니다. 그러나 공개적으로 액세스할 수 있는 소프트웨어의 취약성으로 인해 공격자가 클라우드에 침투하여 중요한 정보를 유출하거나, 동일한 서비스를 사용하여 고객 데이터를 실수로 다른 테넌트에 노출할 수 있는 새로운 수준의 위험이 있습니다. McAfee vNSP는 현재의 선두 공용 클라우드 서비스인 AWS(Amazon Web Services), Microsoft Azure, OCI(Oracle Cloud Infrastructure)를 지원하여 인터넷 게이트웨이 또는 서버 간(양방향 트래픽) 이동하는 데이터에 완벽한 위협 가시성 및 보호를 제공합니다.

가상 환경 보안

기업들은 물리적 서버에서 여러 VM(가상 머신)은 물론 가상화된 워크로드를 동시에 호스팅할 수 있는 가상화된 IT 인프라(예: 개인 및 공용 클라우드)를 빠르게 채택하고 있습니다. 그 결과로 생성된 VM 간 통신은 이러한 워크로드의 즉각적인 마이그레이션, 복제 및 백업과 함께 결합되어 개인 및 공용 클라우드는 물론 모든 SDDC(Software-defined Data Centers)에서의 횡적 트래픽이 크게 증가했습니다. 거기에 더해서, 네트워크 가상화를 통한 유연성으로 인해 이와 같이 급증하는 트래픽 흐름은 더 역동적이고 예측하기 어려워졌습니다. 이에 대처하려면 가상화된 보안 솔루션은 유연하고 확장 가능해야 합니다. 또한 더 중요한 것은 단기적인 특성을 지니는 이러한 VM 및 워크로드를 조정하는 SDN (소프트웨어 - 정의 네트워킹) 플랫폼과 원활히 작동해야 한다는 것입니다.

주요 이점

- 개인 및 공용 클라우드(AWS, Azure, OCI)에 완벽한 보호
- 진정한 양방향 트래픽 보호
- 제어 및 가시성을 위한 중앙 집중식 관리 콘솔
- 알려진 위협과 알려지지 않은 위협으로부터 보호하기 위한 고급 검사 기술
- 성능을 위한 고가용성, 재해 복구 및 부하 분산
- 개인 및 공용 클라우드 간 유용성을 위한 클라우드 사용권 공유
- 장치-클라우드 간 보안을 위해 McAfee 포트폴리오와 통합
- **AWS Marketplace**에서 사용 가능
- **Azure Marketplace**에서 사용 가능

McAfee에 문의

개인 클라우드의 민첩성

McAfee vNSP는 VMware NSX 및 OpenStack 기반 SDN 환경을 포함한 인기 개인 클라우드 플랫폼과 원활하게 통합됩니다. McAfee vNSP는 VMware NSX와 함께 작동하도록 인증된 유일한 전용 가상 IPS 솔루션입니다. 워크로드가 빠르게 생성, 마이그레이션 및 사용 중지되더라도 가상화된 환경에서는 VM의 마이크로 분류 및 횡적 트래픽의 심층 검사가 자동으로 이루어집니다.

고급 위협 방지

McAfee vNSP는 가상 네트워크 트래픽을 심층 검사하도록 설계된 차세대 검사 아키텍처를 기반으로 합니다. 이는 전체 프로토콜 분석, 위협 평판, 동작 분석 및 지능형 악성 프로그램 분석 등 각종 지능형 검사 기술의 조합을 사용하여 네트워크에서 확인된 공격과 확인되지 않은 제로 데이 공격을 모두 탐지하고 방어할 수 있습니다.

하나의 악성 프로그램 감지 기술로 모든 공격을 방어할 수 없기 때문에 McAfee vNSP는 원치 않는 악성 프로그램으로 인해 클라우드에 큰 손해가 발생하지 않도록 여러 가지 시그니처 및 무 시그니처 검색 엔진을 통합했습니다. 이 제품은 브라우저, JavaScript, Adobe 파일의 인라인 에뮬레이션, 봇네트, 악성 프로그램 콜백 탐지, 동작 기반 DDoS 탐지, 그리고 사이트 간 스크립팅, SQL 주입 등 진화한 공격으로부터의 보호와 같은 여러 검사 기술을 활용합니다.

McAfee vNSP는 또한 동작 분석을 위해 파일이 제출되는 McAfee Advanced Threat Defense와의 통합을 통해 은폐하기 쉬운 파일을 식별 및 차단할 수 있습니다. McAfee Advanced Threat Defense는 심도 있는 정적 코드 분석, 동적 분석(악성 프로그램 샌드박싱) 및 **기계 학습**을 결합하여 우회 공격 기술과 랜섬웨어를 사용하는 위협을 포함한 제로 데이 위협 탐지 기능을 향상시킵니다. McAfee는 또한 악성 프로그램을 감지하고 이로부터 보호하도록 Snort 시그니처에 대한 기본 지원을 제공합니다.

유연한 클라우드 사용권 공유

기업 조직은 종종 레거시 응용프로그램 지원 여부에 관계없이 단일 공급업체에 대한 종속성 또는 시스템 중복성을 줄이고 시스템 중복 및 비용 절감 효과를 실현하기 위해 여러 클라우드와 플랫폼에 IT 리소스 및 인프라를 분산합니다. 대부분의 공급업체에서는 개인 및 공용 클라우드는 물론 서로 다른 SDN 플랫폼에 대해 별도의 사용권을 구매하도록 요구하므로 가상화된 환경에 대한 보안 솔루션 사용권을 취득하려면 복잡하고 비용이 많이 들 수 있습니다.

McAfee는 클라우드 사용권 공유를 통해 사용권을 간소화하고 비용을 절감하여 조직이 모든 조합의 공용 및 개인 클라우드 플랫폼에서 McAfee vNSP 사용권 및 처리량을 공유하도록 합니다. 클라우드 사용권 공유를 통해 유연성이 제공되며 관리자는 복잡한 사용권과 시간이 많이 소요되는 구매 프로세스를 거치지 않고도 위치에 상관없이 가상 워크로드에 횡적 트래픽 보호 및 마이크로 분류를 빠르게 제공할 수 있으므로 보안이 강화됩니다.

자세히 알아보기

- **Amazon Web Services 가상 네트워크 보호**
- **Microsoft Azure 가상 네트워크 보호**

효율성 높은 워크플로우 및 분석

최신 위협은 대량의 경고를 생성하여 경고의 우선 순위를 지정하고 추적할 수 있는 보안 운영자의 능력을 빠르게 넘어설 수 있습니다. 응답이 너무 느리면 실제 위협은 탐지되지 않고 빠져나갈 수 있습니다. McAfee vNSP에는 여러 IPS 경보를 실행 가능한 단일 이벤트와 상호 연관시켜 관리자가 빠르게 관련 정보를 확인할 수 있는 고급 분석 및 실행 가능한 워크플로우가 포함됩니다. 또한 추가 McAfee 보안 솔루션과의 통합은 포괄적인 연결 네트워크 위협 탐지 및 완화 플랫폼을 생성합니다.

실시간 가시성 및 제어를 위한 중앙 집중식 관리

단일 McAfee Network Security Manager 어플라이언스는 실시간 가시성 및 제어를 위한 중앙 집중식의 웹 기반 관리 기능을 제공합니다. 최신식 콘솔을 사용하여 한 장의 유리창을 통해 실시간 데이터를 제어할 수 있습니다. 모든 가상 또는 물리 McAfee Network Security Platform 어플라이언스와 기존, 개인 및 공용 클라우드 환경의 McAfee Network Threat Behavior Analysis 어플라이언스를 간편하게 관리, 구성 및 모니터링할 수 있습니다. 직관적인 인터페이스 또한 넓게 배포된 핵심 클러스터를 쉽게 관리할 수 있도록 조정됩니다.

McAfee Network Security Manager는 VMware ESX 서버와 AWS 또는 Azure 환경의 가상 인스턴스로 배포할 수도 AWS 있습니다. McAfee vNSP는 AWS IAM(Identity and Access Management)을 지원하여 관리자가 특정 사용자 및 그룹에 할당된 권한을 기반으로 쉽고 안전하게 AWS 서비스 및 리소스에 대한 액세스를 관리할 수 있습니다.

고가용성, 재해 복구 및 부하 분산

McAfee vNSP는 여러 방법을 통해 중단되지 않는 제어, 보호 및 성능을 자동으로 제공합니다. McAfee Network Security Manager는 환경을 사전에 모니터링하여 고가용성을 제공합니다. 활성 컨트롤러를 사용할 수 없게 되면 McAfee Network Security Manager는 중단되지 않는 가시성 및 보안을 위해 대기 컨트롤러로 자동 페일오버됩니다. 또한 대기 중인 McAfee Network Security Manager는 AWS, Azure 및 OCI 환경에서 재해 복구를 위해 배포할 수 있습니다.

McAfee vNSP는 또한 IPS 센서에 고가용성을 제공합니다. 센서를 사용할 수 없게 되면 자동 확장 기능이 원활하고 중단되지 않는 보호를 위해 새 가상 IPS 센서를 자동으로 생성합니다. 또한 네트워크 트래픽이 증가하면 센서의 자동 부하 분산을 통해 성능이 최적화되고 필요한 처리량 성능을 충족하도록 추가 센서를 자동으로 배포할 수 있습니다.

통합 보안

정교한 공격은 제품 경계에 상관없이, 특히 보안 제품 사이의 인프라 간극을 빠르게 이용합니다. McAfee vNSP는 우수한 보안, 보호 및 높아진 투자 수익률에 대한 솔루션에서 데이터 및 워크플로우를 효율적으로 활용하도록 여러 보안 제품에서 원활하게 통합되는 유일한 IPS입니다. McAfee 보안 솔루션 통합의 예는 다음과 같습니다.

- **McAfee ePolicy Orchestrator®(McAfee ePO™) 소프트웨어:** 모든 IPS 이벤트와 경고에 대한 완전한 엔드포인트 가시성
- **McAfee Endpoint Intelligence Agent:** 네트워크 및 엔드포인트 관점을 결합하여 데이터 유출을 차단
- **McAfee Enterprise Security Manager:** 풍부한 데이터 공유 및 IPS 경고에 대한 IPS 검역을 지원
- **McAfee Threat Intelligence Exchange:** 다양한 유형의 기기 전반에서 공유된 학습
- **McAfee Global Threat Intelligence:** 세계에서 가장 크고 활동적인 평판 서비스
- **McAfee Network Threat Behavior Analysis:** 네트워크 전반의 가시성을 확장
- **McAfee Virtual Advanced Threat Defense:** 우회 위협을 감지하기 위한 심층 검사 제공
- **McAfee Cloud Threat Detection:** 기존 McAfee 보안 솔루션에 연결되어 진화한 악성 프로그램을 탐지하는 편리한 서비스
- **McAfee Management for Optimized Virtual Environments(McAfee MOVE):** 가상 환경을 위한 안티바이러스 솔루션
- **타사 취약성 스캐너:** 엔드포인트를 위한 위험 분석과 호스트

추가 기능

지능형 위협 방지

- McAfee Gateway Anti-Malware 에뮬레이션 엔진
- PDF JavaScript 에뮬레이션 엔진(경량 샌드박스)
- Adobe Flash 동작 분석 엔진
- 고급 우회 공격 방지

봇네트 및 악성 프로그램 콜백 보호

- 도메인 이름 서버(DNS)/도메인 생성 알고리즘(DGA) 빠르고 유연한 콜백 탐지
- DNS 싱크홀링
- 휴리스틱 봇 감지
- 다중 공격 상관 관계
- 명령 및 제어 데이터베이스

지능형 침입 방지

- IP 조각 모음 및 TCP 스트림 재조립
- McAfee의 사용자 정의 및 공개 소스 시그니처
- 호스트 격리 및 등급 제한
- 가상 환경 검사
- 서비스 거부(DoS) 및 분산 서비스 거부(DDoS) 방지
- STIX(Structured Threat Information eXpression)를 지원하는 화이트리스트/블랙리스트 개선 사항
- 임계값 및 휴리스틱 기반 감지
- 호스트 기반 연결 제한
- Snort 시그니처를 위한 기본 지원
- 자체 학습, 프로필 기반 감지

McAfee Global Threat Intelligence

- 파일 평판
- IP 평판
- 위치 기반 제한 액세스
- IP 주소 기반 액세스 제어

	센서 1형	센서 2형
플랫폼	VMware ESX 5.5/6.0/6.5	AWS Azure OCI 지원 VMware vSphere 6.5 및 NSX 6.3
가상 IPS 센서 모델	IPS-VM600	IPS-VM600-VSS
가상 IPS 유형 배포	독립형	분산형
VMware NSX 지원	없음	있음
AWS 지원	없음	있음
Azure 지원	아니요	있음
OCI 지원	아니요	있음
논리 CPU 수	4	AWS 4, Azure 5
메모리 요구 사항	7 GB	7 GB
저장 공간	8GB	8GB
가상 센서 사양		
최대 처리량	최대 1Gbps	최대 1Gbps
모니터링 포트 쌍 수	3	1(포트 쌍이 아닌 포트 모니터링)
센서당 가상 인터페이스(VIDS) 수	100	100
DoS 프로파일	300	300
관리 포트	있음	있음
응답 포트	아니요	없음
배포 모드	VM 간 검사, 물리적 컴퓨터와 VM 간 검사, 물리적 컴퓨터간 검사, SPAN/인라인 포트 검사	

McAfee Together is power.

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