McAfee Virtual Network Security Platform

클라우드 네트워크에 대한 완벽한 위협 탐지

McAfee® Virtual Network Security Platform은 개인 및 공용 클라우드의 고유한 요구 사항을 충족하도록 제작된 완벽한 네트워크 위협 및 IPS(침입 방지 시스템) 솔루션입니다. 이 제품은 클라우드 아키텍처에서 복잡한 위협을 정확하고 단순하게 발견 및 차단하므로 조직은 확신을 가지고 컴플라이언스를 복원하고 클라우드 보안을 구축할 수 있습니다. 고급 기술에는 무 시그니처 탐지, 인라인 에뮬레이션, 시그니처 기반 취약성 패치, 그리고 AWS(Amazon Web Services) 및 네트워크 가상화 지원이 포함됩니다. 조직은 효율적인 워크플로, 여러 통합 옵션 및 간소화된 사용권을 통해 가장 복잡한 클라우드 아키텍처에서도 쉽게 보안을 관리하고 확장할 수 있습니다.

고급 보안 기술로 완벽해진 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 Virtual Network Security Platform은 오늘날의 선도적인 공용 클라우드 서비스(AWS)를 지원하여 인터넷 게이트웨이를 통과하고 횡적(east-west) 트래픽으로 유입되는 데이터에 대한 완벽한 위협 가시성을 제공합니다. 이를 통해 완전한 횡적 트래픽 검사를 제공하는 침입 방지 시스템(IPS) 플랫폼으로 공용 클라우드 아키텍처에 대한 위협 가시성 및 보안 컴플라이언스를 복원할 수 있습니다.

가상 환경 보안

기업들은 물리적 서버에서 여러 VM(가상 머신)은 물론 전체 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 SDDC에서의 횡적 트래픽이

주요 이점

최고 수준의 지능형 위협 방지

- 무 시그니처 지능형 악성 프로그램 분석.
- 사이트 간 스크립팅과 SQL 주입에 대한 보호.
- 고급 봇네트 콜백과 악성 프로그램 보호.
- 동작 기반 분석 및 DDoS(분산 서비스 거부) 보호.
- McAfee Advanced Threat Defense와 통합.
- IPS 및 침입 방지 시스템(IDS) 배포.
- 향상 VMware ESX-McAfee Virtual Network Security Platform 솔루션에서 실행.

클라우드 지원 아키텍처

- 하나의 사용권으로 모든 조합의 공용 및 개인 클라우드에서 처리량을 공유할 수 있습니다.

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.

개인 클라우드의 민첩성 향상

가상화된 환경 보안 요구 사항을 충족하도록 제작된 McAfee Virtual Network Security Platform은 VMware NSX 및 OpenStack 기반 SDN 환경을 비롯하여 널리 사용되는 개인 클라우드 플랫폼과 원활히 통합됩니다. 실제로 McAfee Virtual Network Security Platform은 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.

최고 수준의 위협 방지

McAfee Virtual Network Security Platform은 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 제로 데이 공격을 모두 탐지하고 방어할 수 있습니다.

하나의 악성 프로그램 탐지 기술로 모든 공격을 방어할 수 없기 때문에 McAfee Virtual Network Security Platform은 원치 않는 악성 프로그램으로 인해 클라우드에 큰 손해가 발생하지 않도록 여러 가지 시그니처 및 무 시그니처 검색 엔진을 통합했습니다. 이 제품은 브라우저, JavaScript 및 Adobe 파일의 인라인 에뮬레이션, 봇네트 및 악성 프로그램 콜백 탐지, 동작 기반 DDoS 탐지, 그리고 사이트 간 스크립팅, SQL 주입 등 진화한 공격으로부터의 보호와 같은 다양한 검사 기술을 제공합니다. McAfee Virtual Network Security Platform은 또한 심층적인 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 학습을 결합하여 우회 공격 기술과 랜섬웨어를 사용하는 위협을 포함한 제로 데이 위협 탐지 기능을 향상시킵니다.

클라우드 사용권 공유를 통한 간소화

오늘날 대부분의 기업에서 IT 리소스 및 인프라는 레거시 응용프로그램 지원 여부에 관계없이 단일 공급업체에 대한 종속성 또는 시스템 중복성을 줄이거나 비용 절감 효과를 실현하기 위해 여러 클라우드와 플랫폼에 분산되어 있습니다. 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 사용권을 간소화하고 비용을 절감할 수 있습니다. 이는 고객이 모든 조합의 공용 및 개인 클라우드 플랫폼에서 McAfee Virtual Network Security Platform 처리량 및 사용권을 공유하도록 하는 새로운 개념입니다. 클라우드 사용권 공유를 사용하면 관리자는 시간이 많이 소요되는 구매 프로세스를 거치지

- 혁신적인 AWS 검사 접근법은 공용 클라우드에 완전한 횡적 트래픽 보호를 제공합니다.
- VMware NSX 및 OpenStack 기반 SDN 환경과의 오케스트레이션 지원으로 개인 클라우드 워크로드 간에 마이크로 분류 및 트래픽 검사를 자동화할 수 있습니다.
- VMware 통합으로 VM 인식 대시보드와 검역 시행 기능을 사용할 수 있습니다.
- 구내 및 클라우드 내의 물리 및 가상 센서를 위한 단일 중앙 집중식 관리 콘솔.

지능형 보안 관리

- 구내 및 클라우드 센서를 관리하는 단일 콘솔.
- 지능형 경보 상관 관계 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.
- AWS의 모든 VM의 보안 상태.

않고도 위치에 상관없이 가상 워크로드에 횡적 트래픽 보호 및 마이크로 분류를 빠르게 제공할 수 있으므로 보안이 강화됩니다.

워크플로 및 분석 효율화

아무리 정교한 위협도 쉽게 검색하여 차단할 수 있습니다. McAfee Virtual Network Security Platform에는 고급 분석 및 추가 보안 솔루션과의 통합 기능이 포함되어 있으므로 완전히 포괄적이고 서로 연결된 네트워크 위협 탐지 및 완화 플랫폼을 구축할 수 있습니다.

최신 위협은 대량의 경고를 생성하여 경고의 우선 순위를 지정하고 추적할 수 있는 보안 운영자의 능력을 빠르게 넘어설 수 있습니다. 점들이 제시간에 연결되지 않으면 실제 위협은 탐지되지 않고 빠져나갈 수 있습니다. McAfee Virtual Network Security Platform의 즉시 사용할 수 있는 고급 분석 및 실행 가능한 워크플로는 여러 IPS 경고를 실행 가능한 단일 이벤트로 연관지어 관리자가 빠르게 문제를 차단하고 실행 가능한 관련 정보를 얻도록 도와줍니다.

실시간 데이터의 실시간 제어로 중앙 집중식 관리

단일 McAfee Network Security Manager 어플라이언스는 중앙 집중식의 웹 기반 관리 기능 및 최상의 간편성을 제공합니다. 최첨단 콘솔 및 향상된 그래픽 사용자 인터페이스를 통해 실시간 데이터를 제어할 수 있습니다. 모든 가상 또는 물리 McAfee Network Security Platform 어플라이언스와 기존, 개인 및 공용 클라우드 리소스의 McAfee Network Threat Behavior Analysis 어플라이언스를 단일 콘솔에서 간편하게 관리, 구성 및 모니터링할 수 있습니다. 직관적인 웹 기반 관리 인터페이스를 통해 단일 장치뿐 아니라 광범위하게 분산된 업무 수행에 중요한 클러스터에 이르기까지 모든 배포를 처리할 수 있습니다. McAfee Network Security Manager는 VMware ESX 서버와 AWS의 가상 인스턴스로 배포할 수도 AWS 있습니다.

고가용성 및 재해 복구

McAfee Network Security Manager는 컨트롤러 사이를 중재하고 하나를 활성으로, 나머지를 대기 상태로 결정합니다. 활성 컨트롤러를 사용할 수 없는 경우에는 대기 컨트롤러가 활성 상태로 전환됩니다. 그런 경우, AWS 배포를 위해 컨트롤러 고가용성(HA)이 제공되어 하나의 컨트롤러가 항상 활성 상태를 유지하여 접근이 가능한 장애 조치 메커니즘을 제공합니다. 또한, 대기 중인 McAfee Network Security Manager는 AWS 환경을 위한 재해 복구 기능을 제공합니다.

McAfee Virtual Network Security Platform은 MDR(관리자 재해 복구), Ha(고가용성), 가상 IPS 센서 자동 확장 기능과 함께 고가용성을 제공합니다. 이를 통해 McAfee Virtual Network Security Platform은 중단 없이 원활하게 작동할 수 있습니다. MDR 솔루션은 기본 관리자를 사용할 수 없는 경우에 이를 대체하는 보조 관리자를 제공합니다. 컨트롤러 HA 쌍의 컨트롤러 중 하나는 언제나 활성 상태이며 접근 가능하여 네트워크가 가동 중단되는 것을 방지합니다. 가상 IPS 센서의 자동 확장 기능은 센서가 다운될 경우 새로운 가상 IPS 센서를 생성합니다. 네트워크 트래픽이 증가할 때마다 로드밸런싱 기능을 수행합니다.

통합 보안 아키텍처

정교한 공격은 제품 경계에 상관없이, 특히 보안 제품 사이의 인프라 간극을 이용합니다. McAfee Virtual Network Security Platform은 여러 보안 제품을 통합할 수 있는

유일한 IPS로, 데이터 및 워크플로를 활용하여 이러한 간극을 메우고 결과적으로 투자 수익을 높이고 총 소유비용을 절감할 수 있습니다. 추가적인 보안 제품 통합은 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**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments(McAfee MOVE)**
- **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.
- 지능형 우회 공격 방지.

봇네트 및 악성 프로그램 콜백 보호

- 도메인 이름 서버(DNS)/도메인 생성 알고리즘(DGA) 빠르고 유연한 콜백 탐지.
- DNS Sinkhole.
- 경험적 접근 봇 탐지.
- 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 DDoS 방지.
- 임계값 및 경험적 접근 기반 탐지.
- 호스트 기반 연결 제한.
- 자체 학습, 프로필 기반 탐지.

McAfee Global Threat Intelligence

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

	센서 1형	센서 2형	센서 3형
플랫폼	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
가상 HIP 센서 모델	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
가상 IPS 유형 배포	독립형	독립형	분산형
VMware NSX 지원	없음	없음	있음
AWS 지원	없음	없음	있음
논리 CPU 코어 수[2]	3	4	3
메모리 요구 사항[3]	4GB	6GB	5GB
가상 센서 사양			
최대 처리량[4]	최대 500Mbps	최대 1Gbps	최대 500Mbps
동시 연결 수	200,000	600,000	200,000
초당 설정된 연결 수	6,000	20,000	6,000
지원되는 UDP 흐름	39,168	254,208	39,168
모니터링 포트 쌍 수	2	3	1[5]
센서당 가상 인터페이스(VIDS)	32	100	32
DoS 프로파일	100	300	100
관리 포트	있음	있음	있음
응답 포트	있음	있음	없음
배포 모드	VM 간 검사, 물리적 컴퓨터와 VM 간 검사, 물리적 컴퓨터간 검사, SPAN 포트 검사		VMware NSX 인라인 검사

1. 삽입된 서비스로서 VMware NSX 환경 전용.
2. 릴리스에서 VM 리소스 요구 사항이 달라질 수 있습니다. 릴리스별 설명서를 참조하십시오.
3. 동일 자료.
4. 이상적인 테스트 조건에서 1518바이트 UDP 패킷으로 측정됩니다.
5. 인그레스 및 이그레스 가상 표현 검사는 커널 계층에서 VMware NSX에 밀접하게 연결되어 있습니다.

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