데이터시트

McAfee Public Cloud Server Security Suite

AWS 및 Azure 클라우드 워크로드를 위한 포괄적인 보안

주요 이점

- AWS 및 Azure 워크로드를 위한 설계
- 즉각적인 검색
- 보안 평가 및 위협 교정
- 확장 가능한 보안
- 포괄적인 보호 기능
- McAfee® ePolicy Orchestrator®(McAfee ePO™) 관리 콘솔 활용
- 배포 옵션으로 Chef, Puppet 및 OpsWorks 포함
- 컴플라이언스 입증
- 다른 Intel Security 솔루션과 통합

기업에서 퍼블릭 클라우드 서버 인스턴스를 포함하거나 퍼블릭 클라우드 서버 인스턴스 중심으로 데이터 센터 전략을 변화하고 있으므로, 보호를 위한 공유 책임 모델[1]을 중요하게 고려하는 것이 좋습니다. Amazon Web Services (AWS), Microsoft Azure 등과 같은 퍼블릭 클라우드 공급자가 경계를 보호하고, 사용자는 콘텐츠를 보호해야 합니다. 하지만 기업에서 클라우드 전략에 따라 비용을 절감하면서 제로 데이 및 APT (Advanced Persistent Threat)로부터 클라우드 워크로드를 보호하려면 어떻게 해야 합니까? 클라우드를 채택하는 기업의 주요 과제:

- 제로 데이 및 APT 위협에 대처하기가 점점 어려워지고 있습니다.
- 가시성과 중앙 관리 부족으로 여러 클라우드 인프라를 관리하기가 매우 부담스럽습니다.
- 클라우드 워크로드 보안에서 성능 저하가 우려됩니다.

McAfee® Public Cloud Server Security Suite는 AWS 및 Azure 워크로드와 위협에 대한 즉각적인 검색과 제어를 제공하여 성능 영향을 최소화하면서도 완전하고 일관적이며 지속적인 보호를 실현합니다. 여러 클라우드 데이터 센터, 클라우드 계정, 가상 시스템, 새로운 위협을 검색할 수 있습니다.

McAfee Public Cloud Server Security Suite에서 제공하는 포괄적인 보안에는 기본적인 안티바이러스 및 침입 방지와 제로 데이 위협 차단을 위한 세부적인 화이트리스팅, 규제 준수 요구 사항 충족을 위한 변경 제어, 데이터 보호를 위한 암호화 관리가 포함됩니다. 단일 관리 콘솔로 여러 개의 클라우드를 관리하고 정책을 적용하기가 쉽습니다. Chef, Puppet 및 OpsWorks DevOps 도구를 통한 유연한 배포 옵션으로 영향을 최소화하고 원활한 경험을 제공합니다.

그림 1. 여러 클라우드 인프라와 여러 Intel Security 기술에 대한 단일 관리 콘솔을 사용합니다.

intel Security

지원되는 플랫폼

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux(Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

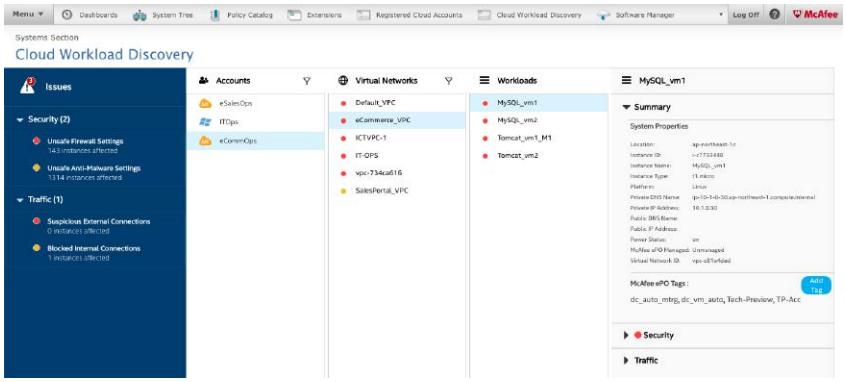

그림 2. 여러 클라우드 인프라 및 새로운 위험을 발견하고 모니터링

클라우드 인프라 및 위협 검색

클라우드 인프라와 위협을 효율적으로 관리하려면 그에 대한 향상된 가시성이 필요합니다.

- AWS와 Azure 클라우드 인프라에 대한 모든 가상 네트워크 또는 개인 클라우드(VPC), 템플릿, 워크로드를 몇 분 만에 검색합니다. 클라우드 인프라 계정에 대한 상세한 정보를 확보하고 어떤 사용자가 인프라의 어떤 부분에 액세스할 수 있는지 파악하며, 템플릿과 VPC에 워크로드가 어떻게 할당되는지 이해하고 클라우드 인프라에 연결된 시스템 트리에 대한 스냅샷을 얻는 것이 충분한 클라우드 인프라 보호를 위한 첫 걸음입니다.
- 여러 클라우드의 보안 상태를 한 곳에서 파악하십시오. 향상된 보안 관리를 위한 공격 소스를 포함하여 엔드 투 엔드 위협 정보를 활용하십시오.
- 모든 워크로드에 대한 트래픽을 보고 워크로드 사이의 정보 흐름과 조직 외부에서 정보 액세스를 관리하십시오.

클라우드를 모니터링하고 보안 경고 시 빠른 조치

빠른 조치가 점점 더 중요해지고 있으므로 이 솔루션을 이용하면 더 심층적인 수준에서 보안 문제를 평가하고 즉각적인 조치를 취할 수 있습니다.

- 즉시 주의가 필요한 문제를 식별하고 색이 구분된 위협을 사용하여 적절한 조치를 취하십시오.
- 맞춤 태그를 만들고 고유한 요구 사항에 따라 워크로드에 할당하십시오.
- 보안 문제를 억제할 조치를 취하고 향후 보안 사고로부터 인프라를 보호할 수 있도록 정책을 채택하거나 위협 평판 데이터를 정의하십시오.
- 개별 워크로드 또는 워크로드 그룹에 대한 맞춤 정책으로 클라우드 방화벽을 관리하십시오. 하나 또는 여러 인스턴스에 대한 트래픽 제어를 위해 AWS 보안 그룹에 대한 정책을 관리하십시오.
- VPC에서 발생하는 의심스러운 트래픽을 확인하고 교정 단계를 수행하여 중요한 정보의 도용을 차단하십시오.

포괄적인 위협 방지

McAfee Public Cloud Server Security Suite는 단일 에이전트를 활용하고 이 에이전트는 여러 클라우드 플랫폼에서 단일 관리 콘솔을 사용하여 관리할 수 있는 여러 계층의 보안을 제공합니다. 이 솔루션은 DevOps용 도구로 배포할 수 있으므로 최상의 경험을 제공합니다.

자세히 알아보기

제품 페이지 방문: **http://www.mcafee.com/kr/products/public-cloud-server-security-suite.aspx**.

AWS Marketplace에서도 구매할 수 있습니다.

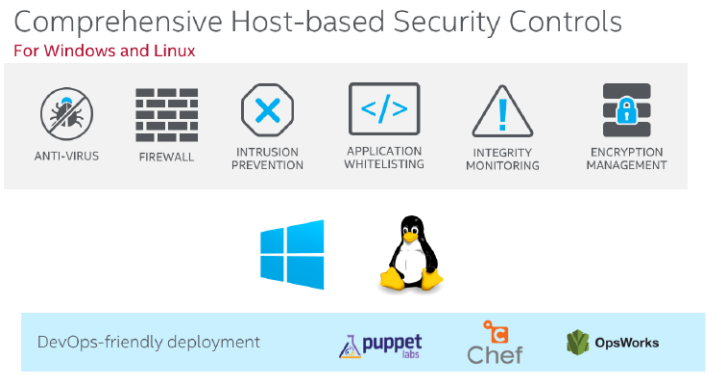

그림 3. 공용 클라우드 워크로드를 위한 포괄적인 보안

기능	이점
Chef, Puppet 및 AWS OpsWorks 배포 옵션	• DevOps 배포 도구를 사용하면 배포가 편리하고 미리 보안을 고려할 수 있습니다. • 보안을 작업의 일부로서 구성할 수 있습니다.
클라우드 워크로드 검색	• 클라우드 인프라에 대한 즉각적인 가시성으로 가상 데이터 센터, 클라우드 워크로드, 클라우드 방화벽을 검색합니다. • 자동 보안 상태 평가와 빠른 위험 알림이 제공됩니다. • 위협의 중요도에 따라 우선 순위가 지정된 경고를 제공하고 빠른 대응을 위한 단계를 안내하여 신속한 교정이 가능합니다.
여러 클라우드 인프라 솔루션을 위한 단일 관리 콘솔(McAfee ePO 소프트웨어)	• 하이브리드 환경 설정에 매우 도움이 됩니다. • 물리, 가상, 클라우드 워크로드 및 정책을 하나의 창으로 관리할 수 있습니다. • Intel Security와 파트너의 클라우드 및 사내 보안 기술 통합 • 보안 프로세스 및 빠른 해결 단계 통합으로 총 소유 비용 감소
악성 프로그램 차단	• 악성 프로그램 방어 기능을 극대화합니다. 시스템과 파일을 바이러스, 스파이웨어, 웜, 트로이 목마 및 기타 보안 위험으로부터 보호합니다. 악성 프로그램을 감지하여 삭제하고, 사용자가 격리된 항목을 관리하기 위한 정책을 쉽게 구성할 수 있도록 지원합니다.
호스트 방화벽	• 무단 액세스와 공격으로부터 워크로드를 보호합니다.
호스트 침입 방지	• 특허 받은 기술을 사용하여 원하지 않거나 유해한 네트워크 트래픽을 차단하거나 제로 데이 공격과 알려진 공격을 미리 차단합니다. • 지정된 포트, 파일, 공유, 레지스트리 키와 레지스트리 값에 대한 액세스를 제한함으로써 워크로드에 원하지 않는 변경이 발생하지 않도록 합니다. • 메모리 보호는 버퍼에 데이터를 쓸 때 비정상적인 프로그램이나 위협이 버퍼의 경계를 넘어서 인접 메모리에 덮어쓰지 않도록 방지합니다. 악용된 버퍼 오버플로는 컴퓨터에서 임의의 코드를 실행할 수 있습니다.
응용프로그램 화이트리스팅	• 시그니처를 업데이트하지 않고 제로 데이 및 지능형 지속가능 위협으로부터 보호합니다. • 신뢰할 수 있는 채널을 통해 새로 추가된 소프트웨어를 자동으로 허용하는 동적 화이트리스팅을 사용하여 보안을 강화하고 소유 비용을 줄일 수 있습니다. • 안전한 응용프로그램 화이트리스팅 및 고급 메모리 보호를 통해 패치 주기 단축
파일 무결성 모니터링	• 분산된 원격 위치에서의 시스템 수준 변경을 지속적으로 감지합니다. • 중요한 시스템 파일, 디렉터리 및 구성에 대한 인증 받지 않은 변경을 방지합니다. • 워크로드에서 모든 변경 시도를 실시간으로 추적하고 확인함으로써 시간, 소스 또는 승인된 업무 티켓을 기준으로 변경 정책을 적용
암호화 관리	• AWS EBS 볼륨에 저장된 데이터를 AWS AES (Advanced Encryption Standard)로 암호화합니다. • 기존 데이터가 포함된 볼륨을 쉽게 암호화할 수 있습니다. • 암호화를 위해 Amazon의 KMS (Key Management Service)와 통합됩니다.

1. http://www.mcafee.com/us/resources/white-papers/wp-cloud-security-primer-techtarget.pdf

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com