

McAfee Management for Optimized Virtual Environments AntiVirus

성능 저하 없는 개인 클라우드에 대한 보안

기존 안티바이러스는 가상화 인프라에 적합하지 않습니다. McAfee® MOVE AntiVirus (Management for Optimized Virtual Environments AntiVirus)는 최적화된 고급 악성 프로그램 백신을 가상화된 데스크톱과 서버로 가져옵니다. 여러 하이퍼바이저에 구현할 수도 있고, VMware NSX 또는 VMware vCNS용으로 에이전트가 없는 조정된 옵션을 선택할 수도 있습니다. 어느 쪽이든 가상 시스템(VM) 성능에 미치는 영향은 최소화하면서 즉각적인 위협 탐지 및 억제를 위한 최고 등급의 보안 기능을 확보할 수 있습니다. McAfee MOVE AntiVirus는 가상화된 배포를 위해 안티말웨어 보호를 최적화하여 최신 보안 스캔이 정책에 따라 실행되도록 보장하면서 하이퍼바이저 리소스를 확보할 수 있도록 돕습니다.

최적화된 검색 컨트롤

게스트 데스크톱과 가상 서버는 동적이므로 신중하게 취급해야 합니다. 사용자가 세션을 시작할 때 이미지에 악성 코드가 없어야 합니다. 이는 어려운 과제가 될 수 있는데, 사용자가 그룹으로 작업하는 경우가 많기 때문에 리소스를 소모하고 사용자가 세션을 확보할 수 없도록 수요가 최대가 되는 '안티바이러스 스캔'을 유발하기 때문입니다.

검색 병목 현상과 지연을 방지하기 위해 McAfee MOVE AntiVirus는 검색, 구성, .DAT 업데이트 작업을 개별 게스트 이미지에서 오프로드 스캔 서버로 오프로드합니다. McAfee는 검색 파일의 글로벌 캐시를 구축하고 유지하여 파일이 일단 검색되고 깨끗한 것으로 확인되면 이후에 해당 파일을

액세스하는 VM이 검색을 기다릴 필요가 없도록 합니다. 각 VM에 대한 메모리 리소스 할당이 감소하며 리소스 풀로 반환할 수 있어 더욱 효과적으로 활용할 수 있습니다.

McAfee MOVE AntiVirus는 온액세스 검색과 주문형 검색에 별도의 정책을 적용할 수 있어 보안 실행을 세부 조정할 수 있도록 합니다. 예를 들어 관리자는 성능 저하를 방지하기 위해 실시간 온액세스 검색에 합당한 수준의 리스크를 감수하고 나중에 영향이 감소할 때 보다 엄격한 정책이 실행되는 주문형 검색을 사용할 수 있습니다.

모든 클라우드에 대한 완벽한 엔드 투 엔드 가시성

가시성이 부족할 경우 가상화된 환경에 적합한 보안 정책을 구현하기가 어렵습니다. VMware 및 OpenStack을 포괄하는

주요 이점

- 악성 프로그램 검색 오프로드: 메모리와 처리 성능에 미치는 영향이 적은 즉각적인 보호
- 안티바이러스 스캔 방지: 온액세스 및 주문형 검색 옵션 지원
- 유연한 배포 활성화: 다중 플랫폼(모든 주요 하이퍼바이저, Windows VM) 또는 에이전트 없는 배포(VMware, Windows 및 Linux VM)
- 향상된 리소스 최적화: 이벤트 통보를 통한 탄력적인 오프라인 스캐너 프로비저닝(다중 플랫폼)
- 제로 데이 및 알려지지 않은 위협을 몇 초 만에 차단: 모래상자에서 동작 분석과 결합된 로컬 평판 인텔리전스(다중 플랫폼, 별도로 판매되는 추가 모듈)
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 콘솔 활용: 물리, 가상 및 클라우드 배포에 대한 엔드 투 엔드 가시성 및 제어 기능

데이터시트

McAfee Cloud Workload Security(McAfee CWS)는 온-프레미스, 개인용 및 공용 클라우드 환경에서 가상 데이터 센터에 대한 완벽한 가시성을 제공하며 서버, 하이퍼바이저 및 VM와 같은 주요 속성을 McAfee ePO 콘솔에 제공합니다. 관리자가 모든 VM의 보안 상태에 대한 가시성을 확보하여 거의 실시간으로 하이퍼바이저와 VM간의 관계를 모니터링할 수 있다면 가상 데이터 센터를 보호하기가 훨씬 쉬워집니다. 사용자 지정 가능한 대시보드를 통해 자산에 대한 검색 상태, 총괄 개요, 보안 데이터 내역을 볼 수 있습니다.

McAfee CWS Essentials 및 McAfee CWS Advanced는 AWS (Amazon Web Services) 및 Microsoft Azure 공용 클라우드와 물리적 서버 전체에 대한 가시성과 제어 기능을 확대합니다.

세부적인 정책 관리

친숙한 McAfee ePO 콘솔을 통해 McAfee MOVE AntiVirus에 대한 정책을 구성하고 제어할 수 있습니다. 가상 데이터를 물리적 시스템 및 공용 클라우드의 데이터와 통합하여 통합 대시보드 및 보고서를 제공할 수 있습니다. 관리자는 McAfee Cloud Workload Security를 통해 VM, 클러스터 또는 데이터 센터별로 고유한 정책을 구성함으로써 데이터 센터의 구성에 맞게 보안 환경을 조정할 수 있습니다.

추가 McAfee MOVE AntiVirus 기능

관리 용이성 및 가시성:

- VM 또는 VM 그룹에 대한 주문형 검색을 즉시 예약.
- 주문형 목표 검색으로 검색 정밀도를 높입니다.
- VMware NSX Service Composer와의 통합을 통해 각 하이퍼바이저에서 오프로드 스캐너를 자동으로 배포합니다.
- 대시보드, 보고서 및 이메일 경보를 통해 문제를 파악할 수 있습니다.

배포와 구성 간소화:

- 여러 하이퍼바이저에 오프로드 스캐너를 배포하고 구성합니다(에이전트 없음).
- McAfee ePO 콘솔을 사용하여 격리된 파일을 복원합니다(다중 플랫폼).
- 안티바이러스 성능 조정을 위해 세부적으로 진단합니다.
- 원활하고 에이전트가 없는 다중 플랫폼 정책 관리가 가능합니다.

VMware를 위한 에이전트 없는 옵션

McAfee MOVE AntiVirus는 효율성 개선을 위해 VMware NSX 또는 VMware vCNS를 사용합니다. 에이전트 없는 배포에서 이러한 솔루션은 고속 연결로 하이퍼바이저를 사용하여 McAfee MOVE AntiVirus 보안 가상 시스템(SVM)이 게스트 이미지 외부에서 VM을 검색할 수 있게 합니다. 검색하는 동안 SVM은 VMware NSX 또는 VMware vCNS를 다이렉트하여 양호한 파일을 캐시에 저장하고, 악성 파일을 삭제하거나 액세스를 거부하거나 격리합니다.

게스트 VM에 VMware NSX 또는 VMware vCNS 엔드포인트 드라이버를 설치하고 VMware ESX 서버에 SVM과 VMware NSX 또는 VMware vCNS 구성 요소를 설치 및 구성하면, 각 클라이언트 VM에 McAfee 소프트웨어를 설치하지 않아도 모든 이미지가 자동으로 보호됩니다. McAfee의 vMotion 인식 구현은 VM을 하나의 호스트에서 다른 호스트로 이동할 수 있으며 대상 호스트의 SVM을 통해 검색이나 사용자 환경에 대한 영향 없이 가상 시스템을 원활히 보호될 수 있음을 의미합니다.

McAfee 제품과 VMware vCNS의 통합을 통해 VMware vCenter 내에서 SVM 상태를 모니터링하고 SVM 연결이 끊기는 경우 경보를 받을 수 있습니다. VM이 감염된 경우

McAfee MOVE AntiVirus 구성

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
 - 다중 플랫폼 배포
 - 에이전트 없는 배포
- 개인 클라우드를 위한 Cloud Workload Security (VMware 및 OpenStack)
- McAfee ePO 소프트웨어

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
 - 다중 플랫폼 배포
 - 에이전트 없는 배포
- 개인 클라우드를 위한 Cloud Workload Security (VMware 및 OpenStack 지원)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- 메모리 보호 및 웹 응용프로그램 보호
- McAfee ePO 소프트웨어

데이터시트

McAfee ePO 콘솔은 영향을 받는 특정 VM에 대한 상세 정보를 담은 이벤트 데이터를 수신합니다. VMware NSX와의 긴밀한 통합으로 McAfee ePO 콘솔에서 생성된 정책과 VMware NSX에 할당된 규칙을 동기화할 수 있습니다. 안티맬웨어 보호 기능이 없는 취약한 시스템 또는 악성 프로그램이 있는 시스템에 대한 태그 지정으로 VMware NSX 방화벽을 통해 VM을 즉시 격리하도록 지원합니다.

VMware vCNS 및 VMware NSX와 동시에 에이전트 없는 McAfee MOVE AntiVirus 배포가 지원되므로 VMware vCNS 고객은 VMware NSX로 쉽고 매끄럽게 전환할 수 있습니다.

모든 주요 하이퍼바이저에 적합한 다중 플랫폼

vSphere, Hyper-V, KVM 및 XenServer를 포함한 다중 플랫폼 설치에서는 경량 엔드포인트 구성 요소인 McAfee MOVE AntiVirus 에이전트가 SVM와 통신함으로써 각 VM을 대신하여 안티바이러스 처리를 중개합니다. McAfee MOVE AntiVirus 에이전트는 로컬 캐시를 유지하고 정책 및 검색 기능을 관리합니다. 클린 마스터로 사용할 골드 이미지를 지정하고 검색할 수 있습니다. 클린 이미지로 글로벌 캐시를 미리 채우면 빠른 VM 부팅이 가능합니다.

파일을 액세스할 때 McAfee MOVE Offload Scan Server는 온액세스 검색을 수행하여 응답을 다시 VM으로 전달합니다.

사용자는 팝업 경보를 통해 문제에 대한 알림을 받고 악성 파일을 삭제하거나 액세스를 거부하거나 격리하는 등의 조치를 취할 수 있습니다.

다중 플랫폼 배포에서 검색 수요의 변동에 따라 SVM을 자동으로 리소스 풀에 추가하거나 리소스 풀에서 제거하여 기능을 확대/축소할 수 있으므로 탁월한 확장성이 제공되며 효율적인 리소스 활용이 가능합니다. 이벤트 통보는 관리자가 SVM 사용 경향을 파악하여 리소스 관리를 최적화하는 데 도움이 됩니다.

다중 플랫폼 배포의 McAfee MOVE AntiVirus는 계속 증가하는 고유 악성 프로그램 샘플을 즉시 식별하고 그에 대처할 수 있도록 McAfee Global Threat Intelligence (McAfee GTI)의 글로벌 평판 인텔리전스를 McAfee Threat Intelligence Exchange (별도로 판매되는 추가 모듈)의 로컬 데이터로 강화합니다. McAfee MOVE AntiVirus는 McAfee Advanced Threat Defense와 함께 McAfee Threat Intelligence Exchange를 사용하여 알려지지 않은 응용프로그램의 동작을 모래상자 안에서 동적으로 분석하고 새롭게 감지된 악성 프로그램으로부터 모든 엔드포인트를 자동으로 면역화합니다. McAfee Threat Intelligence Exchange를 통한 McAfee MOVE AntiVirus와 McAfee Network Security Platform의 통합으로 일원화된 경계 및 가상 시스템 보호를 위한 계층화된 보안 접근법이 제공됩니다.

에이전트가 없는 다중 플랫폼을 위한 통합된 정책 관리

대부분의 조직은 에이전트 없는 배포와 다중 플랫폼 배포 모두를 지원할 수 있는 McAfee MOVE AntiVirus의 기능을 활용하고자 할 수 있습니다. McAfee MOVE AntiVirus는

보안 관리자에게 McAfee ePO 콘솔에서 하나의 확장 지점을 사용하여 일관된 보안 정책을 정의 및 관리하는 기능을 제공합니다. 따라서 이와 같이 다양한 방법을 쉽고 원활하게 관리할 수 있습니다.

자세한 내용

McAfee 솔루션은 귀사에 필요한 보안과 유연성을 제공합니다.

자세한 내용은 www.mcafee.com/kr/products/move-anti-virus.aspx를 참조하십시오.

아키텍처	다중 플랫폼 배포	에이전트 없는 배포
하이퍼바이저/플랫폼 지원	VMware, Citrix, Hyper-V 및 KVM을 포함한 모든 주요 하이퍼바이저	VMware
스캐닝 플랫폼	Windows 2008, Windows 2012 R2, Windows Server 2016, Windows 10 R4 및 RS5	Linux Ubuntu 16.04
배포 확장성	단일 SVM으로 여러 하이퍼바이저의 VM을 보호할 수 있습니다. SVM은 탄력적으로 프로비저닝할 수 있습니다.	ESX 호스트당 하나의 SVM
VM과 통신	네트워크를 통한 통신	하이퍼바이저를 통한 통신
가상 시스템 보호	Windows	Windows 및 Linux



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

McAfee 및 McAfee 로고, ePolicy Orchestrator, McAfee ePO 및 SiteAdvisor는 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2018 McAfee, LLC. 4152_1018 2018년 10월