McAfee Security Suite for Virtual Desktop Infrastructure

성능에 미치는 영향을 최소화하여 필요한 보안 구축

현재 가상 데스크톱의 채택이 이루어지고 있지만 성능 문제를 일으키거나 원하는 서버 밀도에 영향을 주지 않고 비즈니스를 보호하려면 솔루션 내부에 강력한 데스크톱 보안을 설계해야 합니다. 기존 안티바이러스는 가상화 인프라 내에서 제대로 동작하지 않습니다. 해답은 무엇일까요? McAfee® Security Suite for Virtual Desktop Infrastructure(VDI)는 가상 데스크톱에 최적화된 포괄적인 보안을 제공합니다.

McAfee Security Suite for VDI는 가상화에 최적화된 악성 프로그램 방지, 제로 데이 위협 보호를 위한 화이트리스팅, 데스크톱 침입 방지 및 데이터 보호를 제공합니다. 또한 사용자에게 악의적인 웹 사이트에 대해 경고하거나 그러한 사이트를 차단할 수 있습니다.

최적화된 스캐닝 아키텍처

가상 데스크톱은 동적이므로 신중하게 취급해야 합니다. 이미지는 오프라인 상태에서 반드시 악성 프로그램이 없거나 사용자가 세션을 시작할 때 지연 없이 검색되어야 합니다. 시작되는 서비스가 악성 프로그램 백신 하나가 아니고 사용자가 그룹으로 작업하는 경우가 많기 때문에 모든 리소스를 소모하고 사용자가 세션을 확보할 수 없게 만드는 최대 수요인 "안티바이러스 스톰"이 발생하게 됩니다.

스캐닝 병목 현상과 지연을 방지하기 위해 McAfee MOVE(Management for Optimized Virtual Environments) AntiVirus는 스캐닝, 구성, .DAT 업데이트 작업을 개별 게스트 이미지에서 강화된 가상 어플라이언스/오프로드 스캔 서버로 오프로드합니다. 우리는 검색 파일의 글로벌 캐시를 구축하고 유지하여 파일이 일단 검색되고 깨끗한 것으로 확인되면 이후에 해당 파일을 액세스하는 VM(가상 시스템)은 검색을 기다릴 필요가 없도록 합니다. 각 VM에 대한 메모리 리소스 할당이 감소하며 더욱 효과적인 활용을 위해 리소스 풀로 돌아갈 수 있습니다. 지능적으로 주문형 검색을 예약하면 검색이 하이퍼바이저 성능을 방해하지 않도록 보장합니다.

세부적인 정책 관리

McAfee® ePolicy Orchestrator®(McAfee ePO™) 콘솔은 McAfee MOVE AntiVirus에 대한 정책 및 제어를 구성할 수 있는 기능을 제공합니다. 가상 데스크톱의 데이터를 통합 대시보드와 리포트 내 다른 시스템의 데이터와 롤업할 수 있습니다. 관리자는 Cloud Workload Discovery를 통해 VM, 리소스 풀, 클러스터 또는 데이터 센터별로 고유한 정책을 구성함으로써 데이터 센터의 구성에 맞게 보안 요구 사항을 조정할 수 있습니다.

주요 이점

- McAfee ePO 소프트웨어와 Cloud Workload Discovery를 통해 검색 및 가시성을 제공
- 블랙리스트 기술과 화이트리스트 기술의 고유한 조합을 통해 악성 프로그램으로부터 가상 데스크톱을 보호
- 성능 영향을 최소화하는 최적화된 가상화
- 메모리 보호 및 웹 애플리케이션 보호를 통해 침입 방지 및 웹 보호를 추가
- McAfee ePO 소프트웨어를 활용하여 여러 엔드포인트에 걸쳐 한눈에 볼 수 있는 가시성, 제어 및 보고 제공
- 유연하고 에이전트가 없는 다중 플랫폼 배포 지원
- 수요에 따라 확장할 수 있도록 탄력적인 오프라인 스캐너 프로비저닝 지원(다중 플랫폼)
- 로컬 평판 인텔리전스와 통합되어 보다 빠르게 위협에 대응(다중 플랫폼)

VMware에 적합한 에이전트 없는 배포

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 VMware SVM과 VMware NSX 또는 VMware vCNS 구성 요소를 설치 및 구성하면, 각 클라이언트 VM에 당사 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.

vCNS와의 McAfee MOVE AntiVirus 통합을 통해 VMware vCenter 내에서 SVM 상태를 모니터링하고 SVM 연결이 끊기는 경우 경고를 받을 수 있습니다. VM이 감염된 경우 McAfee ePO 소프트웨어는 영향을 받은 특정 VM에 대한 상세 정보를 담은 이벤트 데이터를 수신합니다. NSX와의 긴밀한 통합으로 McAfee ePO 소프트웨어에서 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.

모든 하이퍼바이저에 적합한 다중 플랫폼

다중 플랫폼 설치에서 경량 엔드포인트 구성 요소인 McAfee MOVE AntiVirus 에이전트가 McAfee MOVE Offload Scan Server와 통신함으로써 각 가상 데스크톱을 대신하여 안티바이러스 처리를 중개합니다. McAfee ePO 소프트웨어 에이전트는 정책 및 검색을 관리합니다. 또한 클린 마스터로 사용할 골드 이미지를 지정하고 검색할 수 있는 기능도 제공됩니다. 따라서 관리자가 클린 이미지로 글로벌 캐시를 미리 입력함으로써 더욱 빠른 가상 데스크톱 부팅 시간을 실현할 수 있습니다.

사용자가 파일을 액세스할 때 McAfee MOVE Offload Scan Server는 온액세스 검색을 수행하여 응답을 다시 VM으로 전달합니다. 사용자는 팝업 경고를 통해 알림을 받고 파일은 격리되어 처분을 기다립니다. 각 가상 데스크톱은 McAfee ePO 콘솔에서 설정한 고유한 개별 정책에 따라 구성하거나 여러 가상 데스크톱을 그룹으로 관리할 수 있습니다.

다중 플랫폼 배포에서 워크로드의 변화에 따라, SVM을 자동으로 리소스 풀에서 추가하거나 제거하여 기능을 확대/축소할 수 있으므로 탁월한 확장성을 달성하고 효율적인 리소스 활용이 가능합니다. 이벤트 통보는 관리자가 SVM 사용 경향을 파악하여 리소스 관리를 최적화하는 데 도움이 됩니다.

McAfee Security Suite for VDI 구성

- McAfee MOVE AntiVirus
  - 다중 플랫폼 배포
  - 에이전트 없는 배포
- 개인 클라우드를 위한 Cloud Workload Discovery(VMware 및 OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise 기술
- McAfee ePolicy Orchestrator

다중 플랫폼 배포의 McAfee MOVE AntiVirus는 계속 증가하는 고유 악성 프로그램 샘플을 즉시 식별하여 대처할 수 있도록 McAfee Global Threat Intelligence의 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 샌드박스 안에서 동적으로 분석하고 새롭게 탐지된 악성 프로그램으로부터 모든 가상 데스크톱을 자동으로 면역화합니다.

기능	필요한 이유
가상화 보안	▪ 성능 타협 및 리소스 사용 없이 가상 데스크톱 인프라에 배포된 작업 부하의 보안을 향상 ▪ VMware에 최적화된 에이전트 없는 배포를 통해 뛰어난 성능과 VM 밀도를 제공합니다. 가상 데스크톱마다 당사 에이전트를 설치/업데이트할 필요가 없어 복잡성은 줄고 사용성은 대폭 향상됩니다 ▪ 모든 하이퍼바이저에 적합한 다중 플랫폼 배포가 수요에 따라 확장할 수 있도록 탄력적인 오프라인 스캐너 프로비저닝을 지원하며 로컬 평판 인텔리전스와 통합되어 보다 빠르게 위협에 대응할 수 있습니다
핵심 엔드포인트 보호	▪ McAfee 안티바이러스 보호는 다른 제품에 비해 검색 속도가 더 빠르고 메모리와 CPU를 더 적게 사용하며 보호 기능이 더 뛰어납니다 ▪ 호스트 침입 방지가 실수로 유입시키거나 허용할 가능성이 있는 복잡한 보안 위협으로부터 기업을 보호 ▪ McAfee SiteAdvisor® Enterprise가 악성 웹 사이트와의 상호 작용을 차단하고 사용자 지정 가능한 정책을 허용하여 유해한 웹 사이트 액세스를 제한함으로써 정책 준수를 보장
응용프로그램 화이트리스팅	▪ 기존 엔드포인트 보안 제어를 넘어 호스트 성능에 미치는 영향을 대폭 축소 ▪ 시그니처 업데이트 없이 제로 데이 및 APT(advanced persistent threat)에 대한 보호를 통해 보호 시간 단축 ▪ 동적 화이트리스팅으로 레거시 화이트리스팅 기술에 비해 적은 운영 간접 비용 필요
Cloud Workload Discovery	▪ 취약한 보안 제어를 식별할 수 있도록 개인 클라우드 워크로드 및 기본 플랫폼에 대한 완벽한 가시성 제공

기능	필요한 이유
파일 및 이동식 미디어 보호(암호화)	▪ 파일 및 이동식 미디어 보호를 통해 훨씬 쉽고 위험이 적은 암호화 ▪ Intel® AES-NI 기술의 최적화된 구현을 통해 암호화된 호스트에서 네이티브에 가까운 성능 발휘 ▪ 정책 적용, 자동, 투명 파일/폴더 암호화 및 이동식 미디어 암호화(USB 드라이브, CD, DVD) 제공 ▪ 사용자가 USB 미디어를 사용하여 안전하게 정보를 전송할 수 있음 ▪ 네트워크 공유에서 데이터에 대한 안전한 액세스 가능
McAfee ePO 소프트웨어를 통한 중앙 집중식 관리	▪ 보안 제어를 향상하기 위해 모든 플랫폼에서 정책 관리, 배포, 가시성 및 보안 관리를 비롯하여 물리적, 가상 및 클라우드 배포를 중앙에서 관리 ▪ 운영 프로세스를 간소화하고 관리 직원의 시간 투자 축소 ▪ 서버 설치 공간 감소를 통한 하드웨어 비용 절감

자세한 내용

McAfee 솔루션은 성능에 미치는 영향을 최소화하면서 귀사에 필요한 보안을 제공합니다. **www.mcafee.com/kr/products/data-center-security-suite-for-vdi.aspx**를 방문하십시오.

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