McAfee Server Security Suite Advanced

물리적, 가상, 클라우드 배포를 위한 고급 서버 보안

주요 이점

- 중앙 콘솔에서 단일 창 관리를 통해, 클라우드 환경의 자산을 비롯한 모든 물리적 및 가상 서버를 탐색
- 블랙리스팅과 화이트리스팅을 결합하여 물리 및 가상 서버를 악성 프로그램으로부터 보호
  - 원치 않는 응용프로그램이 McAfee Application Control for Servers를 통해 실행되는 것을 막아 호스트의 보안을 보장함으로써 알려지지 않은 위협으로부터 보호해야 할 동적 화이트리스트를 제공
  - 분산된 위치 및 원격 위치 전반의 시스템 수준 변경 사항을 지속적으로 탐지하여 컴플라이언스 요건을 충족

데이터 센터는 지난 몇 년간 저장소, 서버, 네트워크 및 데이터 센터에서 제공하는 응용프로그램 전반에 걸쳐 큰 전환기를 맞고 있습니다. 데이터 센터의 다양한 특징 및 클라우드 컴퓨팅의 급격한 발전으로 인해 이러한 환경을 안전하게 보호할 수 있는 새로운 방법이 필요해졌습니다. 기업의 IT 및 보안 전문가들은 물리적, 가상 및 클라우드 환경을 위한 통합적이고 강력한 보안 상태를 조성하여 민첩성 및 경제성을 실현하도록 지원해야 하는 문제에 당면하고 있습니다. Intel® Security 제공 제품의 일부인 McAfee® Server Security Suite Advanced는 물리적, 가상 및 클라우드 배포를 위한 가장 포괄적인 서버 보호 및 관리를 제공하는 동시에, 화이트리스트 및 변경 제어 등의 추가적인 고급 서버 보안을 제공하여 컴플라이언스를 유지할 수 있도록 지원합니다.

모든 워크로드 탐색

물리적, 가상 및 클라우드 배포 전반에 걸쳐 적절한 보안 정책을 적용할 수 있도록 워크로드를 탐색하는 일은 쉽지 않은 경우가 많습니다. 보호되지 않은 엔드포인트를 감지하고 보안 컴플라이언스를 파악하도록 돕는 검색 보고서를 통해 관리를 용이하게 만듭니다. McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어를 위한 커넥터를 통해 McAfee Server Security Suite Advanced는 프라이빗 및 퍼블릭 클라우드를 포함한 모든 물리 및 가상 서버를 검색할 수 있습니다. 이 솔루션에는 McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack 및 Microsoft Azure가 포함되며, 이를 통해 구내형과 외부형의 모든 가상 시스템을 모니터링하고 강력한 보안 상태를 제공하는 세부적인 보안 정책을 적용할 수 있습니다. 대시보드는 운영 체제 메모리 보호, 하이퍼바이저 호스트-가상 시스템 관계, 각 가상 시스템의 위치 등을 포함한 보안 상태를 알려줍니다.

서버 보호

McAfee Server Security Suite Advanced는 물리, 가상화 또는 클라우드와 관계없이 서버를 위한 가장 포괄적인 보호를 제공합니다. 또한 변경 제어, 업계 최고의 블랙리스팅 및 화이트리스팅 보호 기술의 고유한 조합을 제공합니다.

intel Security

주요 이점(계속)

- McAfee MOVE AntiVirus를 통해 성능 영향을 최소화하여 최적화된 가상화 보안을 제공
- McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack 및 Microsoft Azure를 통해 프라이빗 및 퍼블릭 클라우드의 모든 가상 시스템에 대한 보안 상태를 완전히 파악

McAfee Server Security Suite Advanced에는 인증된 소프트웨어만 서버에서 실행하도록 허용하는 화이트리스트 솔루션인 McAfee Application Control for Servers가 추가됩니다. 중앙 집중식으로 관리되는 이 화이트리스트 솔루션은 관리가 필요한 노동 집약적인 목록 없이 인증되지 않은 응용프로그램을 차단하고 APT(Advanced Persistent Threat)를 저지하는 동적 신뢰 모델과 혁신적인 보안 기능을 사용합니다. 화이트리스트 기능은 시그니처 업데이트가 필요 없는 보호를 통해 호스트 성능에 미치는 영향을 줄여 줍니다.

핵심 서버 보호의 일부로서 이 제품군은 Microsoft Windows 및 Linux 서버를 위한 기존의 안티 맬웨어 솔루션을 제공하며, 여기에는 NSS Labs에서 제로 데이 취약성 공격 및 우회 공격 부문 1위 제품으로 선정한 McAfee VirusScan® Enterprise 소프트웨어도 포함됩니다. 또한 이 제품군에서는 기존의 안티 맬웨어 솔루션 외에, 가상 환경에 특화된 별도의 솔루션도 제공합니다. McAfee MOVE(Management for Optimized Virtual Environments) AntiVirus는 가상 환경을 위한 안티바이러스를 최적화하여 대규모 환경에 대해서도 성능 영향을 최소화하며 모든 주요 하이퍼바이저를 지원합니다. McAfee MOVE AntiVirus는 VMware 배포 환경을 위한 에이전트 없는 조정된 옵션 또는 KVM, Microsoft Hyper-V, VMware 및 Xen 기반 하이퍼바이저 환경을 위해 배포할 수 있는 다중 플랫폼 옵션으로 이용 가능합니다.

안티바이러스는 보안의 핵심이지만, 지능형 위협으로부터 보호하려면 추가적인 솔루션이 필요할 수 있습니다. McAfee Host Intrusion Prevention은 실수로 유입시키거나 허용할 가능성이 있는 복잡한 보안 위협으로부터 기업을 보호합니다.

클라우드로 확장

클라우드로 확장하게 되면 새로 프로비저닝된 워크로드에 적절한 보안 정책이 적용되었는지 확인하기가 점점 더 어려워집니다. McAfee는 프라이빗 및 퍼블릭 클라우드에서 실행 중인 가상 시스템과 중단된 가상 시스템을 모두 자동 검색함으로써 이러한 문제를 해결합니다. McAfee ePO 플랫폼에서 퍼블릭 클라우드 계정을 등록하기만 하면 적절한 보안 정책을 통해 가상 시스템을 자동으로 보호할 수 있습니다. 또한 McAfee 데이터 센터 보안 대시보드 프라이빗 및 퍼블릭 클라우드에서 보호 상태와 보안 사고에 대한 완전한 가시성을 제공합니다.

서버와 비즈니스 최적화

가상화 및 클라우드 컴퓨팅에 잠재된 막대한 기능은 충분한 보안이 뒷받침된 경우에만 완전하게 실현할 수 있습니다. McAfee는 조직의 발전에 따른 성장 옵션을 지원하는 서버 보안 솔루션을 제공합니다. 물리적 환경이든, 가상 환경이든 또는 클라우드 환경이든, McAfee는 서버의 보안을 유지하는 동시에 유연성을 유지할 수 있는 솔루션 제품군을 제공합니다. McAfee Server Security Suite Advanced는 조직 전반에 걸쳐 강력한 보안 상태를 설정하고 유지하는 고급 솔루션을 통해 물리적, 가상 및 클라우드 서버 보안을 제공합니다.

McAfee Server Security Suite Advanced의 이점에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오. **http://www.mcafee.com/kr/products/server-security-suite-advanced.aspx**.

기능	필요한 이유
응용프로그램 화이트리스팅	• 기존 엔드포인트 보안 제어를 넘어 호스트 성능에 미치는 영향을 대폭 축소 • 시그니처 업데이트 없이 제로 데이 및 APT에 대한 보호를 통해 빠른 보호 가능 • 동적 화이트리스팅으로 레거시 화이트리스팅 기술에 비해 적은 운영 간접 비용 필요
변경 제어	• 중요 시스템 파일, 디렉터리 및 구성에 대한 무단 변경을 차단함으로써 관리자가 보안 침해 문제 해결에 투자하는 시간을 절약 • 서버에서 모든 변경 시도를 실시간으로 추적하고 확인함으로써 시간, 소스 또는 승인된 업무 티켓을 기준으로 변경 정책을 적용 • 지속적인 제어로 임시 또는 무단 변경으로 인한 영향을 최소화
단일 콘솔 관리	• 프라이빗 및 퍼블릭 클라우드를 포함한 물리 및 가상 시스템을 위한 단일 관리 창으로 가시성을 크게 개선 • 운영 측면을 간소화하고 관리 직원의 시간 투자 축소 • 필요한 서버 설치 공간 감소를 통한 하드웨어 비용 절감
핵심 서버 보호	• NSS Labs[1]에서 제로 데이 취약성 공격 및 우회 공격에 대해 최고로 꼽은 물리적 서버를 위한 바이러스 보호 • Host Intrusion Prevention이 실수로 유입시키거나 허용할 가능성이 있는 복잡한 보안 위협으로부터 기업을 보호
가상화 보안	• 성능 및 리소스 사용에 대한 타협 없이 가상 인프라에 배포된 작업 부하의 보안을 최적화 • 데이터 센터 내 여러 하이퍼바이저를 보호함으로써 사용된 모든 하이퍼바이저 유형에 대한 공통의 보안 상태를 확보 • 뛰어난 성능 및 VM 밀도를 제공하기 위한 VMware에 최적화된 에이전트 없는 배포
프라이빗 및 퍼블릭 클라우드 내의 가상 시스템에 대한 완전한 가시성	• VMware vSphere, Amazon AWS, OpenStack 및 Microsoft Azure 환경에서 물리적 서버뿐 아니라 하이퍼바이저와 가상 시스템도 발견함으로써 보안이 필요한 대상에 대한 완전한 가시성 확보 • 언제 가상 시스템이 프로비저닝되는지, 어떤 것을 보안 정책을 통해 자동으로 보호함으로써 가상 시스템에 대한 적절한 보안 상태를 보장할 수 있는지 파악

1. NSS Labs, Inc. Protection & Evasion Test (NSS Labs, Inc. 보호 및 우회 테스트), 2013

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