



McAfee Endpoint Protection—Advanced Suite

제로 데이 공격 방지 및 컴플라이언스 규제정책 지원

주요 사항

- 시스템, 데이터, 이메일 및 웹 위협과 컴플라이언스 위반 위협으로부터 Microsoft Windows, Mac, Linux 장치 보호.
- 단일 공급업체의 통합 솔루션을 통해 엔드포인트 및 데이터 보안 노력을 통합하여 적은 비용으로 더욱 강력한 보호를 제공할 수 있습니다.
- 단순하고 효율적인 중앙 집중식 관리 및 확장 가능한 엔드포인트 보안 프레임워크를 통해 향상된 보호 성능을 즉시 제공합니다.

모바일 근무 인력과 강화된 규제로 보안에 큰 부담이 생기게 됩니다. McAfee® Endpoint Protection — Advanced Suite(Intel® Security 제품 라인에 속함)는 지능적인 악성 프로그램과 제로 데이 위협을 차단하는 통합된 사전 예방적 보안 기술을 사용하여 네트워크 밖으로 이동할 때 엔드포인트를 보호하고 엔드포인트가 다시 네트워크 안으로 돌아올 때 네트워크를 보호합니다. 통합 침입 방지를 통해 지능형 위협으로부터 데스크톱과 랩톱을 보호합니다. 중앙 집중식 정책 기반 관리, 액세스 제어, 다중 플랫폼 지원 및 감사 기능을 통해 모든 엔드포인트 자산이 지속적으로 안전하게 보호되고 컴플라이언스를 준수합니다.

공격자가 더 정교해짐에 따라 보안 관련자가 지능형 위협에 대한 탐지 및 방어에 필요한 도구 및 가시성을 확보하는 데 어려움을 겪고 있습니다. 오늘날 범죄자가 사용하는 교묘한 기술의 위협에서 안전한 엔드포인트는 없지만, 휴대용 시스템은 추가적인 위협에 노출되어 있습니다. 랩톱은 웹 및 이메일 게이트웨이, 네트워크 방화벽 및 네트워크 침입 방지 시스템과 같은 기존의 보호 계층 없이 호텔, 커피숍 및 홈 오피스 등에서 제약 없이 사용되고 있습니다. Wi-Fi 네트워크에서는 누구든지 뉴스를 비롯한 여러 가지 정보를 듣고 가져갈 수 있습니다.

회사 네트워크와 연결되어 있지 않다는 이유만으로 PC는 패치 및 기타 업데이트를 놓치게 되어 제로 데이 위협에 더욱 취약하게 될 수 있습니다. 또한 이러한 패치 및 기타 업데이트를 의무화하는 규제가 늘어나고 있습니다. 엄격한 산업 규정뿐 아니라 관리 체제 제어 측면에서도 현장 또는 이동 중에 중요한 데이터 배포를 관리하고 웹 환경에서 이를 적절히 사용해야 합니다.

McAfee Endpoint Protection — Advanced Suite를 사용하면 광범위한 보호, 컴플라이언스 제어 및 통합 관리를 담당할 수 있습니다. 바이러스, 해커, 스팸 발송자, 데이터 도용자 또는 도청자 중 어떤 것이라도 차단하려는 경우 이 원활한 솔루션으로 최적의 기능과 비용 절감 효과를 얻을 수 있습니다.

지능적이고, 협력적인 방어

위협 보호, 탐지 및 교정을 위한 전략은 물론 표적 공격에 대한 신속한 탐지 및 조치를 위해 보안 구성요소 간 협력을 강화하는 보안 프레임워크가 조직에 필요합니다. McAfee Endpoint Security 10 (제품군에 포함)은 여러 엔드포인트 방어 기술과 실시간으로 통신하여 새로운 지능형 위협에 대한 분석 및 협력을 수행하고 시스템 또는 사용자에 영향을 주기 전에 이러한 위협을 신속하게 차단하고 중지합니다. 이 프레임워크는 중복된 기술을 제거하고 다른 Intel Security 솔루션과의 연결을 통해 더 간단한 관리 및 더 강력한 방어를 지원합니다. 또한 McAfee GTI(Global Threat Intelligence)는 시장에서 제공되는 가장 큰

Intel Security를 선택하는 이유

- McAfee는 관리자용 위해 실제 중앙 집중식 환경을 제공합니다.
- 통합된 엔드포인트 및 보안 프레임워크를 통해 중복된 요소를 제거하고, 다른 솔루션과 연결하며, 구축 기반으로 확장 가능한 아키텍처를 제공할 수 있습니다.
- McAfee Global Threat Intelligence는 시장에서 가장 강력한 규모의 위협 인텔리전스를 제공합니다. McAfee는 누구보다 더 많이 발견하고 보호합니다.

규모의 관찰 및 분석을 통해 강력한 통찰력을 제공합니다.

고급 이메일 바이러스 및 스팸 방지

McAfee 솔루션은 인바운드 및 아웃바운드 이메일을 검색하여 스팸, 부적절한 콘텐츠 및 유해한 바이러스를 차단합니다. 의심스러운 이메일을 격리하여 나날이 지능화되는 이메일 위협이 네트워크와 사용자에게 영향을 미치지 못하게 합니다. 또한 이메일 서버에 대한 안티바이러스 계층이 악성 프로그램이 사용자의 받은 편지함에 도달하지 못하도록 방지합니다.

제로 데이 및 취약성 보호

이제 더 이상 비상 패치를 적용할 필요가 없습니다. 취약성 공격 및 침입 방지 기술은 맬웨어로부터 데스크톱 및 랩톱을 감시하고, 악성 코드가 응용 프로그램을 해킹하고 더 높은 권한으로 실행하려는 것을 차단하고, 랩톱과 데스크톱을 공격으로부터 보호하는 자중으로 업데이트된 서명을 제공합니다. 일정에 따라 패치를 구현하고 테스트하는 것이 안전합니다. 버퍼 오버플로 공격을 방지하는 McAfee 특허 동작 보호를 함께 사용하면 업계 최고의 시스템 취약성 보호 기능을 누릴 수 있습니다.

통합 방화벽

McAfee GTI를 사용하여 봇네트, 분산 서비스 거부 (DDoS) 공격, 지능형 지속가능 위협 및 위험한 웹 연결로부터 데스크톱 및 랩톱을 보호하는 통합 방화벽을 통해 원하지 않는 인바운드 트래픽을 차단하고, 아웃바운드 트래픽을 제어합니다. 또한 전체 방화벽 정책이 완전히 시행될 때까지 시작 중 아웃바운드 트래픽만 허용함으로써 시스템을 보호합니다.

효율적인 정책 감사 및 컴플라이언스

에이전트 기반 정책 감사는 엔드포인트 및 문서를 검색하여 모든 정책이 최신 상태인지 확인합니다. 조직은 모범 사례 정책(ISO 27001 및 CoBIT)과 주요 산업 규정에 대한 컴플라이언스 상태를 측정할 수 있습니다.

포괄적인 장치 제어

USB 드라이브, Apple iPod, Bluetooth 장치, 기록 가능 CD 및 DVD를 통해 중요한 데이터가 회사 외부로 유출되는 것을 방지합니다. 도구를 사용하여 사용자 및 기밀 데이터가 이동하는 위치에 상관없이 사용자가 회사 네트워크에 연결되어 있지 않은 경우에도 모든 데스크톱 및

랩톱에서 전송되는 데이터를 모니터링 및 제어할 수 있습니다.

사전 웹 보안

사용자가 악의적인 웹 사이트를 방문하기 전에 미리 경고함으로써 웹 서핑으로 인한 위험을 줄이고 컴플라이언스가 보장되도록 지원합니다. 호스트 기반 웹 필터링을 사용하면 웹 사이트 액세스를 허가하고 차단하여 사용자가 언제 어디서 웹 서핑을 하든지 간에 사용자를 보호하고 정책을 준수할 수 있도록 합니다. 마지막으로, 개인 URL이 차단될 수도 있으며 최신 버전의 여러 웹 브라우저가 지원됩니다.

운영 비용을 절감하는 관리

McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어는 효율성을 높이고 보안 및 컴플라이언스 상태를 포괄적으로 파악하기 위해 보안을 관리하고 보호를 실행하며 보안 운영 비용을 절감하는 중앙 집중식 단일 플랫폼을 제공합니다.

엔드포인트, 네트워크 및 데이터 보안 측면의 위협, 공격 및 이벤트와 컴플라이언스 감사를 연관 지어 보안 작업 및 컴플라이언스 보고서의 관련성 및 효율성을 높입니다. 이 모든 보안 영역을 포괄하는 단일 통합형 관리 플랫폼을 공급하는 업체는 McAfee뿐입니다. McAfee ePO 소프트웨어는 보안 관리 과정을 간소화합니다.

빠르고 간편한 배포

지연 없이 보호 수준을 높일 수 있습니다. EASI 설치 프로그램은 4번 클릭으로 강력한 보호를 실행할 수 있습니다. McAfee ePO 소프트웨어와의 통합을 통해 단일 환경에서 보안 기능을 배포하고 관리하는 것이 가능합니다.

간편한 마이그레이션

최신 버전의 McAfee ePO 소프트웨어가 설치된 환경에서 McAfee® VirusScan® Enterprise 및 McAfee agent는 자동 마이그레이션 도구를 이용하여 기존 정책을 20분 안에 McAfee Endpoint Security 10으로 마이그레이션할 수 있습니다.*

자세한 내용

자세한 내용은 www.mcafee.com/kr/products/endpoint-protection/index.aspx를 참조하거나 (02)3458-9800으로 전화하십시오. 연중무휴입니다.

기능	필요한 이유
단일 통합형 관리	McAfee ePO 소프트웨어를 사용하면 보안 상태와 이벤트를 즉시 확인할 수 있으며 경영진과 직접 소통하여 모든 보안 및 컴플라이언스 도구를 통합적으로 제어할 수 있습니다.
다중 플랫폼	모바일 인력과 기술 인력에게 필요한 Mac, Linux, Microsoft Windows 등의 전체 엔드포인트를 보호합니다.
장치 제어	회사 통제를 벗어나지 않도록 하기 위해 이동식 저장 장치 및 미디어에 복사하는 데이터를 모니터링하고 제한할 수 있습니다.
데스크톱 및 랩톱을 위한 IPS 및 통합 방화벽	새로운 취약성에 대한 제로 데이 보호를 제공함으로써, 긴급 패치가 필요한 상황을 줄이고 네트워크에 액세스할 수 있는 데스크톱 응용프로그램을 제어하며 네트워크에서 발생하는 공격을 차단합니다.
악성 프로그램 차단	바이러스, 트로이 목마, 웜, 애드웨어 및 스파이웨어를 비롯하여 기밀 데이터를 도용하고 사용자 생산성을 떨어뜨리는 다른 잠재적으로 원하지 않은 프로그램을 차단합니다.
안티스팸	악성 프로그램 및 피싱을 배포하는 사이트를 사용자가 의심 없이 방문하도록 유도하는 스팸을 제거해 줍니다.
URL 필터링 및 안전 검색을 통한 웹 컨트롤	규정 준수를 보장하고, 악의적인 웹 사이트를 방문하기 전 사용자에게 경고를 표시하고, 기업 네트워크 내부 및 외부의 사용자를 보호할 수 있습니다.
이메일 서버 보안	전자 메일 서버를 보호하고 사용자 받은 편지함에 악성 프로그램이 도착하기 전에 차단합니다.
정책 감사	HIPAA 및 PCI 등에 대한 완벽하게 통합된 컴플라이언스 보고를 제공합니다.



* 마이그레이션에 걸리는 시간은 기존 정책 및 환경에 따라 달라질 수 있습니다.