McAfee Endpoint Threat Protection

비즈니스와 함께 성장하는 필수적이고 효과적인 보호

위협 환경이 계속 진화할 것이라는 데에는 의심의 여지가 없습니다. 강력한 방어선을 구축하기 위한 시작점이 엔드포인트라는 것은 알려진 사실입니다. 그러나 시간 경과에 따라 새로운 기술을 추가할 수 있는 기능이 없다면 오늘날 기업에 필요한 보호를 받기가 어려울 수 있습니다. 그러한 신기술은 궁극적으로 복잡하고 단절된 보안 작업을 생성하게 됩니다. McAfee® Endpoint Threat Protection은 오늘날 기업에 필요한 기본적인 보호 기능을 제공하며 미래의 지능형 위협 방어 요건에 대비할 수 있게 해줍니다. 이 솔루션은 실시간으로 함께 실행되어 위협을 분석하고 그에 대한 협력을 강화하는 통합 위협 방지, 방화벽, 웹, 이메일 및 장치 제어 방어 기능을 제공합니다. 이를 통해 시스템이나 사용자에게 영향을 미치기 전에 빠르게 위협을 차단 및 교정할 수 있습니다.

주요 이점

- 협력적인 보호 기술 계층으로 보안 상황을 강화합니다.
- 변화하는 요구사항에 따라 보호를 용이하게 확대할 수 있는 유연성을 확보합니다.
- 시스템 리소스에 대한 영향을 최소화한 중앙 집중식 관리, 영향이 없는 사용자 검색으로 생산성을 증대합니다.

협력적인 엔드포인트 프레임워크

통합을 염두에 두고 설계된 McAfee Endpoint Threat Protection 방어 기능은 실시간으로 인식되는 위협을 협력을 통해 공유하여 식별을 조율하고 의심스러운 파일, 웹 사이트 및 잠재적으로 원하지 않는 프로그램의 실행을 차단함으로써 높은 수준의 보호를 제공합니다.

사용 사례
웹에서 악성 파일 다운로드

파일 해시가 웹 컨트롤에서 위협 예방으로 전송되어 ODS를 트리거합니다.

악성 파일이 시스템에 액세스하기 전에 미리 탐지되어 차단됩니다.

포렌식 데이터(소스 URL, 파일 해시 및 기타 정보)가 캡처됩니다.

이벤트 데이터가 다른 모듈 및 McAfee® ePolicy Orchestrator® (McAfee ePO™) 소프트웨어와 공유되어 클라이언트 사용자 인터페이스에 표시됩니다.

그림 1. McAfee Endpoint Threat Protection 방어 기능이 함께 작동하는 방식.

현재와 미래를 위해 통합된 솔루션

McAfee Endpoint Threat Protection을 사용하면 단절된 포인트 제품 배포를, 여러 보호 기술 전반에서 연결되고 협력적인 프레임워크 및 실시간에 가까운 보호로 바꿀 수 있습니다. 이 솔루션을 사용하면 위협을 보다 효과적으로 분석할 수 있을 뿐만 아니라 다른 방어 기능과 공유하기 위해 수집된 위협 포렌식 데이터를 보다 지능적으로 사용할 수 있으며 다른 엔드포인트에 있거나 다른 진입점에서 발견된 위협을 보다 빠르게 식별하여 차단할 수도 있습니다.

이러한 접근법 덕분에 유연한 배포가 가능합니다. 구매한 제품과 함께 제공된 모든 기능을 당장 설치한 다음 어떤 기능을 구성하고 활성화할지 결정할 수 있습니다. 나중에 정책 변경을 통해 사용하고자 하는 기능을 쉽게 활성화할 수 있습니다.

마지막으로 McAfee 프레임워크를 사용하면 추가 기술을 포함하도록 설계된 아키텍처 덕분에 변화하는 요구사항에 따라 보호를 용이하게 확대할 수 있습니다. 이를 통해 보다 정교한 위협에 대한 방어를 위해 언제든지 다른 진화한 보호 기능을 도입할 수 있습니다.

경제적이며 성능에 영향을 주지 않는 솔루션

McAfee Endpoint Threat Protection은 복잡성을 야기하거나 성능에 영향을 주지 않으면서 핵심 보호 기술에 확장 가능한 프레임워크를 제공하므로 기업과 사용자 모두의 생산성을 높일 수 있습니다. 예를 들어 사용자 환경 전반에 걸쳐 보안 정책을 배포, 모니터링 및 관리할 수 있는 단일 창을 제공하는 McAfee ePolicy Orchestrator 소프트웨어를 통한 중앙 집중식 관리로 인해 작업을 보다 효율적으로 실행할 수 있습니다. 사용 중인 환경에 운영 체제가 여러 개 있는 고객은 Microsoft Windows, Apple Macintosh 및 Linux 시스템에 대한 교차 플랫폼 정책을 사용하여 생산성을 높일 수 있습니다. 그리고 McAfee Endpoint Threat Protection 구성요소에는 공용 언어(McAfee Data Exchange Layer)가 사용되기 때문에 기술과 위협에 대한 신속한 대응 간의 프로세스를 최적화하여 노출 시간을 단축하는 방식으로 위험을 완화할 수 있습니다.

또한, 사용자는 시스템에 대한 영향을 최소화하도록 최적화된, 영향이 없는 사용자 검색, 메모리 및 CPU 사용으로 생산성을 높일 수 있습니다. 직관적인 사용자 인터페이스가 기본적으로 제공되므로 기업과 사용자 모두 수행된 조치 및 그 이유에 대한 통찰력을 쉽고 빠르게 확보할 수 있습니다.

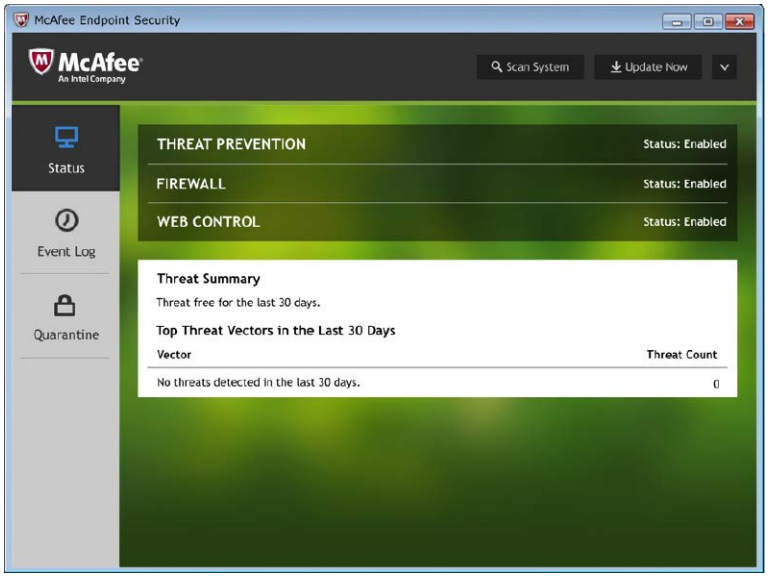

그림 2. 직관적인 사용자 인터페이스로 관리자 및 사용자 작업을 간소화할 수 있습니다.

지원되는 플랫폼

- Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X 버전 10.5 이상
- Linux 32비트 및 64비트 플랫폼: RHEL, SUSE, CentOS, OEL, Amazon Linux 및 Ubuntu 최신 버전

서버:

- Windows Server(2003 SP2 이상, 2008 SP2 이상, 2012), Windows Server 2016
- Windows Embedded(Standard 2009, Point of Service 1.1 SP3 이상)
- Citrix Xen Guest
- Citrix XenApp 5.0 이상

구성 요소	이점	고객 혜택	차별화
위협 방지	여러 보호 계층을 사용하여 악성 프로그램을 신속하게 검색, 중단 및 수정하는 포괄적인 보호를 제공합니다.	• 경험적 접근과 온액세스 검색 기술을 활용하여 알려진 악성 프로그램과 알 수 없는 악성 프로그램을 차단합니다. • Windows, Mac 및 Linux 플랫폼에서 보호를 적용하여 정책 및 배포를 간소화합니다. • 신뢰할 수 있는 프로세스에 대한 검색을 방지하고 의심스러워 보이는 프로세스에 우선순위를 지정하여 성능을 향상시킵니다.	보다 효과적인 분석을 위해 웹 및 방화벽 방어와 협력하여 정보를 알려주는 다계층 안티맬웨어로서, 지능적으로 규칙을 적용하여 잠재적인 위협을 차단합니다.
통합 방화벽	봇넷, 분산 서비스 거부(DDoS) 공격, 신뢰할 수 없는 실행 파일, 지능형 지속가능 위협 및 위험한 웹 연결로부터 엔드포인트를 보호합니다.	• 정책을 실시하여 사용자를 보호하고 생산성에 영향을 미치지 않도록 합니다. • 원하지 않는 인바운드 연결을 차단하고 아웃바운드 요청을 제어하여 대역폭을 보호합니다. • 신뢰할 수 있는 네트워크 및 실행 파일, 그리고 위험한 파일이나 연결에 대해 사용자에게 알려주어 사용자가 준비를 갖추도록 합니다.	응용프로그램 및 위치 정책으로 특히 회사 네트워크에 포함되지 않은 랩톱 및 데스크톱을 보호합니다.
웹 컨트롤	엔드포인트에 대한 웹 보호 및 필터링을 사용하여 안전한 웹 검색을 보장합니다.	• 사용자가 악성 사이트에 방문하기 전에 미리 경고를 표시하여 위험을 완화하고 컴플라이언스를 보장합니다. • 위험하거나 부적절한 웹 사이트를 인증하거나 차단하여 위협을 방지하고 생산성을 보호합니다. • 위험한 다운로드를 실제로 다운로드하기에 앞서 차단하는 방식으로 안전하게 보호합니다.	Windows, Mac, Linux 및 여러 브라우저에서 McAfee Global Threat Intelligence에 의한 알림을 통해 보호 기능을 제공합니다.
McAfee Data Exchange Layer	Intel Security 제품 및 다른 타사 제품과 통합하여 효율적으로 통신할 수 있도록 보안을 연결합니다.	• 통합으로 위험을 줄이고 대응 시간을 단축합니다. • 오버헤드 및 운영 직원 비용을 절감할 수 있습니다. • 프로세스를 최적화하고 실용적인 권장 사항을 제시합니다.	• 보안 제품 간에 가장 중요한 위협 정보를 공유합니다. • 감염을 방지하고 보호 기능을 업데이트하도록 최초 감염자 위협 통찰력을 다른 모든 엔드포인트와 즉시 공유합니다.
McAfee ePO 관리	고도로 확장 가능하고 유연하며 자동화된 보안 정책 관리가 가능한 단일 창으로 보안 문제를 식별하고 그에 대응할 수 있습니다.	• 보안 워크플로를 통합하고 간소화하여 검증된 효율성을 제공합니다. • 탁월한 가시성 및 유연성이 제공되어 확신을 가지고 조치를 취할 수 있습니다. • 사용자 지정 가능한 정책 실시로 단일 에이전트를 빠르게 배포하고 관리합니다. • 자동화된 동적 쿼리, 대시보드 및 응답을 통해 인사이트에서부터 대응까지의 시간을 단축합니다.	• 단일 콘솔로 제어력을 강화하고, 비용을 절감하며, 보다 빠르게 운영 보안을 관리할 수 있습니다. • 업계 전체에서 탁월성을 널리 인정받은 검증된 인터페이스입니다. • 광범위한 보안 에코시스템 전체에서 끌어서 놓기 대시보드를 사용할 수 있습니다. • 개방형 플랫폼은 혁신적인 보안 기능을 신속히 채택할 수 있도록 합니다.

www.mcafee.com/kr/products/endpoint-threat-protection.aspx에서 McAfee Endpoint Threat Protection**의 이점에 대해 자세히 알아보십시오.**

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