McAfee Complete Endpoint Threat Protection

정교한 공격에 대한 지능적인 위협 방지

조직에서 직면하는 위협에 대해서는 전반적인 위협 방어 수명 주기에 걸쳐 조치를 취하고 지배권을 가질 수 있도록 해주는 높은 가시성과 도구가 요구됩니다. 따라서 보안 전문가는 정밀하게 작동하고 진화한 위협에 대한 탁월한 통찰력을 제공하는 기능을 갖춰야 합니다. McAfee® Complete Endpoint Threat Protection은 제로 데이 위협 및 정교한 공격을 조사, 억제하고 그에 대한 조치를 수행하는 고급 방어 기능을 제공합니다. 핵심 엔드포인트 보호는 통합 기계 학습 및 동적 억제와 함께 작동하여 제로 데이 위협을 거의 실시간으로 탐지함으로써 시스템을 감염시키기 전에 미리 위협을 분류하여 중단시킵니다. 실행 가능한 포렌식 데이터 및 보고서는 사용자에게 계속 정보를 제공하며 아웃브레이크에 대한 대응에서 방어 조사 및 강화로 전환하도록 도와줍니다. 또한, 이 솔루션은 확장 가능한 프레임워크를 사용하여 구축되었으므로 사용자 요구와 위협 환경의 변화에 따라 현재는 물론 미래에도 간단하게 다른 지능형 위협 방어 기능을 추가할 수 있습니다.

주요 이점

- 기계 학습 및 DAC를 통해 제로 데이 위협, 랜섬웨어 및 그레이웨어에 대비할 수 있도록 돕습니다.
- 자동화된 조치 및 분석을 사용하여 교정 시간을 단축하고 생산성을 보호합니다.
- 중앙 집중식 관리로 사용자 환경, 배포 및 지속적인 관리를 간소화합니다.

자동화된, 지능형 위협 방어

지능형 위협은 공격을 시작하기 전에 멈출 수 있어야 합니다. 이것이 바로 McAfee Complete Endpoint Threat Protection에 DAC(동적 응용프로그램 억제) 및 Real Protect[1] 기술이 포함된 이유입니다. DAC는 악의적인 행동이 탐지되면 시스템을 감염시키거나 사용자에게 영향을 미치지 않도록 그레이웨어 및 의심스러운 제로 데이 위협을 자동으로 억제합니다. Real Protect는 기계 학습을 통해 위협을 조사하고 분류하여 얻게 되는 통찰력을 저장하여 향후에 자동으로 취할 수 있는 조치에 사용합니다.

복잡성을 줄이도록 구축된 설계

복잡성은 효율성의 적입니다. 이제 사용자는 서로 다른 인터페이스 및 관리 콘솔을 사용하여 여러 포인트 솔루션을 관리하느라 시간을 허비할 필요가 없습니다. McAfee Complete Endpoint Threat Protection은 단일 콘솔을 사용하여 관리됩니다. McAfee® ePolicy Orchestrator® (McAfee ePO™) 소프트웨어. 단일 창을 통해 빠르게 확대하고 배포 시간을 단축하며 지속적인 관리 부담을 완화할 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.

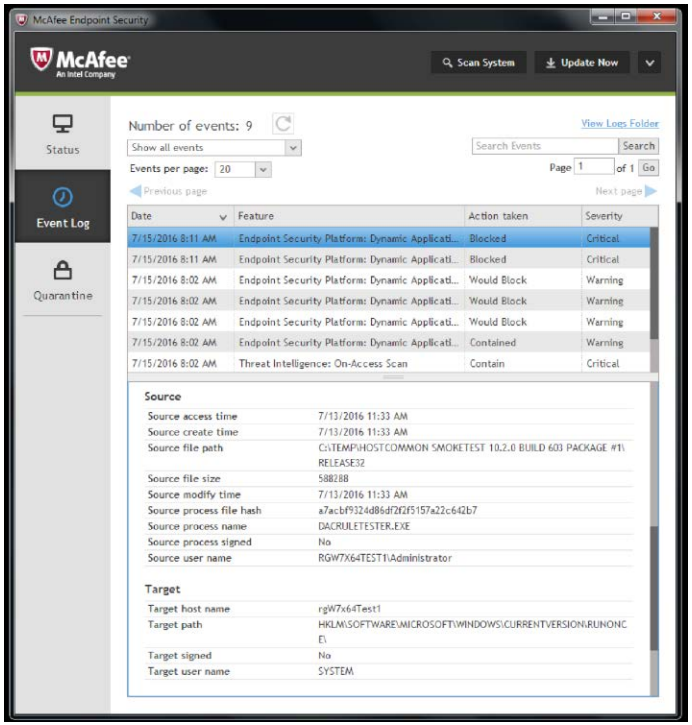

그림 1. DAC는 심각도에 따라 위협을 차단하고 억제합니다.

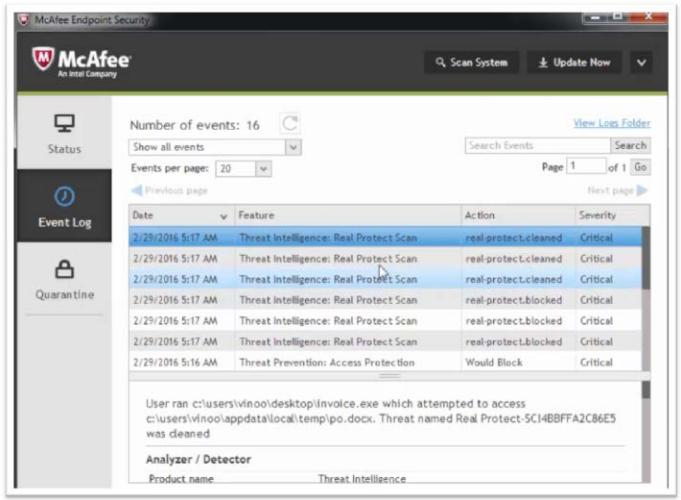

그림 2. Real Protect에서는 기계 학습을 사용하여 시그니처 기반 검색에서 종종 놓치는 제로 데이 악성 프로그램을 거의 실시간으로 탐지합니다.

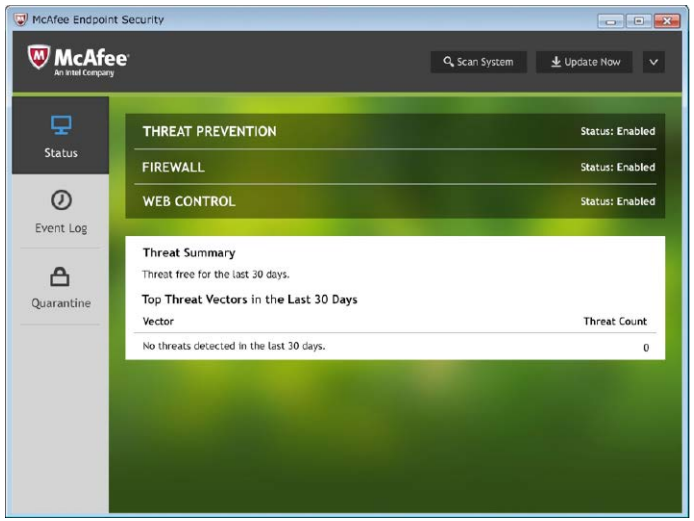

그림 3. 직관적인 사용자 인터페이스로 관리자 및 사용자 작업을 간소화할 수 있습니다.

현재와 미래를 위해 구축된 유연한 프레임워크

McAfee Complete Endpoint Threat Protection은 여러 보호 기술을 포괄하여 연결되고 협력적인 프레임워크와 실시간에 가까운 보호를 제공합니다. 이 솔루션을 사용하면 위협을 보다 효과적으로 분석할 수 있을 뿐 아니라, 다른 방어 기능과 공유하기 위해 수집된 위협 포렌식 데이터를 보다 지능적으로 사용할 수 있습니다 핵심 엔드포인트 보호 방어에서는 공통 통신 계층을 사용하여 위협이 처음 발견된 순간부터 탁월한 통찰력을 확보하고 진단을 내릴 수 있도록 지능형 위협 방어에 대한 정보 및 컨설팅을 제공할 수 있습니다.

이러한 접근법 덕분에 유연한 배포가 가능하므로 구매한 제품과 함께 제공된 모든 기능을 바로 설치할 수 있습니다. 그런 다음 당장 어떤 기능을 구성하고 활성화할지 결정하고, 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 확대할 수 있습니다.

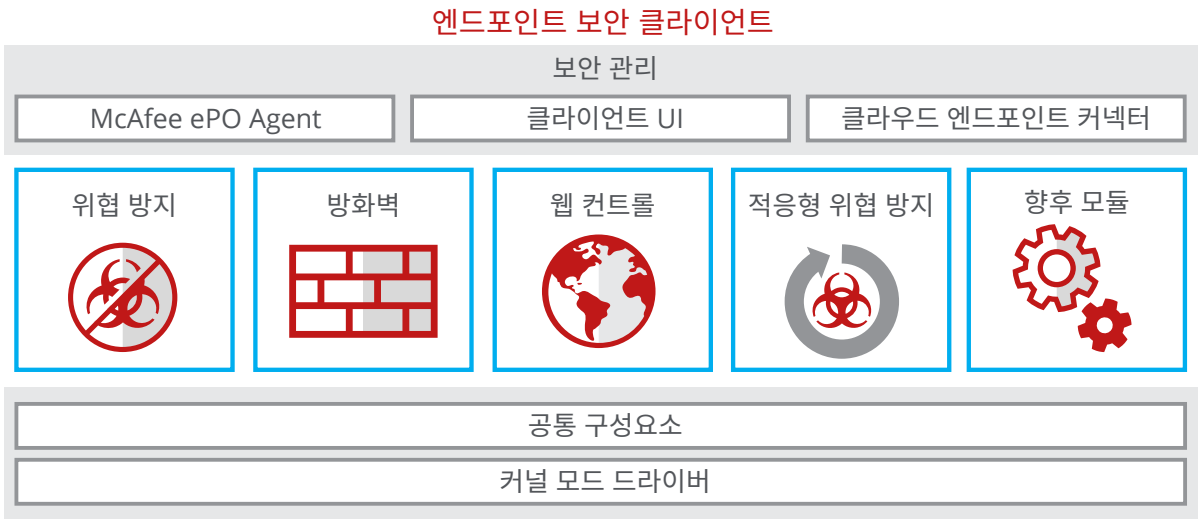

그림 4. McAfee 엔드포인트 보안 클라이언트 프레임워크.

지원되는 플랫폼

- Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OSX 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
동적 응용프로그램 억제	그레이웨어가 엔드포인트를 악의적으로 변경하지 못하게 차단하여 최초 감염자를 보호합니다.	▪ 최종 사용자나 신뢰할 수 있는 응용프로그램에 영향을 주지 않고 향상된 보호를 구현합니다. ▪ 수동 개입을 최소화하여 위협 발생부터 억제까지의 시간을 단축합니다. ▪ 최초 감염자를 보호하고 네트워크가 감염되지 않도록 격리합니다.	▪ 인터넷 연결 여부에 상관없이 작동하며 외부 입력 또는 분석이 필요하지 않습니다. ▪ 사용자에게 투명합니다. ▪ 감시 모드는 환경 내 잠재적인 취약성 공격 동작에 대한 즉각적인 위협 가시성을 제공합니다.
Real Protect	기계 학습 동작 분류를 적용하여 공격을 실행하기 전에 제로 데이 위협을 차단하고 이전 탐지를 회피한 위협이 실제로 실행되지 못하게 중단시킵니다.	▪ 랜섬웨어같이 탐지하기 어려운 개체를 비롯하여 더 많은 제로 데이 악성 프로그램을 쉽게 무효화합니다. ▪ 위협을 자동으로 파악, 분석 및 교정하므로 수동으로 개입할 필요가 없습니다. ▪ 자동화된 분류 및 연결된 보안 인프라를 사용하여 방어 기능을 조정합니다.	▪ 동적 동작 분석을 통해서만 발견할 수 있는 악성 프로그램을 탐지합니다. 긴밀한 통합으로 실시간 평판 업데이트를 공유하고 모든 보안 구성요소에 대한 보안 효율성을 개선합니다.
위협 방지	여러 보호 계층을 사용하여 악성 프로그램을 신속하게 검색, 중단 및 수정하는 포괄적인 보호를 제공합니다.	▪ 경험적 접근과 동작 및 온액세스 검색 기술을 활용하여 알려진 악성 프로그램과 알 수 없는 악성 프로그램을 차단합니다. ▪ Windows, Mac 및 Linux 시스템 전체에서 데스크톱 및 서버에 대한 보호 기능을 사용하여 정책 및 배포를 간소화합니다. ▪ 신뢰할 수 있는 프로세스에 대한 검색을 방지하고 의심스러워 보이는 프로세스에 우선순위를 지정하여 성능을 향상합니다.	보다 효과적인 분석과 위협 방지를 위해 웹 및 방화벽 방어와 함께 사용할 수 있는 다계층 안티맬웨어입니다.
통합 방화벽	봇네트, DDoS(분산 서비스 거부) 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.

구성 요소	이점	고객 혜택	차별화
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. ▪ 웹 사이트 액세스를 인증하거나 차단하여 위협을 방지하고 생산성을 보호합니다. ▪ 위험한 다운로드를 실제로 다운로드하기에 앞서 차단하는 방식으로 안전하게 보호합니다.	Windows, Mac 및 여러 브라우저에서 보호합니다.
Data Exchange Layer	McAfee 제품 및 다른 타사 제품과 통합하여 효율적으로 통신할 수 있도록 보안을 연결합니다.	▪ 통합을 통해 위험을 줄이고 대응 시간을 단축합니다. ▪ 간접 비용 및 운영 직원 비용을 절감할 수 있습니다. ▪ 프로세스를 최적화하고 실용적인 권장 사항을 제시합니다.	보안 방어 제품 간에 가장 중요한 위협 정보를 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. ▪ 직관적인 대시보드 및 보고서를 통해 인사이트에서 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.

자세히 알아보기

McAfee Complete Endpoint Threat Protection의 이점에 대해 자세히 알아보려면 다음 사이트를 방문하십시오. **www.mcafee.com/kr/products/complete-endpointthreat-protection.aspx**.

1. 이 솔루션은 미국에 위치한 호스트된 데이터 센터를 포함하여 파일 평판을 확인하고 의심스러운 파일 탐지와 관련된 데이터를 저장하는 데 사용됩니다. 필수는 아니지만, DAC는 클라우드 연결을 통해 최적의 성능을 발휘합니다. 전체 DAC 및 Real Protect 제품 기능을 사용하려면 클라우드 액세스, 활성 지원이 필요하며 클라우드 서비스 약관의 적용을 받습니다.

McAfee Together is power.

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