

McAfee Complete Endpoint Protection— Business

손쉬운 중앙 집중식 관리를 제공하는 연결된 지능적 방어

McAfee® Complete Endpoint Protection - Business를 사용하여 엔드포인트 장치를 방어합니다. McAfee Complete Endpoint Protection은 고급 위협으로부터 방어하기 위한 협력적인 위협 및 포괄적인 위협 인텔리전스, 데이터 보호를 위한 암호화, 데스크톱 및 랩톱에서 제로 데이 취약성 공격을 중단하기 위한 동적 응용프로그램 억제 및 시스템 학습을 사용하는 경제적인 일체형 솔루션입니다. 이메일, 웹 및 협력적 엔드포인트 방어를 통해 피싱 및 다단계 공격도 차단합니다. 끝으로, 중앙 집중식 웹 기반 관리 기능은 IT 직원의 일상적인 업무 부담을 줄여주고 위협이 발생했을 때 신속하게 대응할 수 있도록 지원합니다.

McAfee Complete Endpoint Protection - Business 제품군은 성장 중인 기업이 올바른 보안을 구현할 수 있도록 터키 방식 설치부터 신속한 대응까지 지원합니다. 하나의 통합 솔루션을 통해 PC, Mac, Linux 시스템 등을 보호할 수 있습니다. 이 제품은 복잡성과 비용 부담을 줄이면서 루트킷, 표적 웹 및 이메일 공격, 지속가능 위협으로부터 보호합니다. 엔드포인트 보안 시장의 선두 기업인 McAfee에서만 제공하는, 고도의 강력하고 효율적인 보호와 간편한 관리 기능을 만나보십시오.

고급 위협 보호

감염된 한 대의 시스템 때문에 비즈니스가 중단될 수 있으며, 안티바이러스만으로는 오늘날의 지능적인 위협을 막아내기에 역부족입니다. McAfee Complete Endpoint Protection - Business는 각종 위협으로부터 보호하는 최고의 솔루션입니다. McAfee의 협력적인 엔드포인트 프레임워크를 통해 방어가 함께 작동함으로써 새로운 위협에 대한 조치를 취하고, 포렌직 데이터를 실시간으로 공유할 수 있습니다.

McAfee는 지능형 위협에 협력하여 대응하는 지능적인 방어, 데스크톱 및 랩톱을 위한 동적 응용프로그램 억제 및 시스템 학습, 장치 제어, 암호화 등 다양한 보호 계층을 통해 악성 프로그램을 빠르게 차단, 탐지 및 교정합니다.

McAfee는 여러 보호 계층을 제공합니다. 고급 암호화를 통해 기밀 정보를 자동으로 보호하고, PC, Mac, 랩톱, 가상 시스템, 이동식 미디어 및 클라우드 스토리지(예: Box, DropBox, Google Drive 및 Microsoft OneDrive)에서 인증 받지 않은 액세스를 차단할 수 있습니다. McAfee® ePolicy Orchestrator® (McAfee ePO™)의 웹 기반 중앙 관리 플랫폼을 사용하여 시스템 성능 저하 없이 중요 자산을 보호할 뿐 아니라 손쉽게 정책을 관리하고 적용할 수 있습니다.

파일, 웹, 메시지, 네트워크 등 모든 공격 벡터에서 새롭게 등장한 모든 위협에 관한 정보를 실시간으로 전달하는 클라우드 기반 McAfee Global Threat Intelligence를 통해 더 광범위한 정보와 지식을 얻고 이를 바탕으로 더 확실하게 기업 환경을

주요 이점

- 지능적이고, 협력적인 엔드포인트 방어, 데스크톱 및 랩톱을 위한 침입 방지 및 방화벽, 장치 제어, 암호화 등 다양한 기능이 포함된 최고 등급의 포괄적 계층형 보호를 제공합니다.
- 사전 실행 억제는 랜섬웨어와 고급 위협이 시스템을 감염시키기 전에 이들을 격리시킵니다. 컴퓨터 학습과 결합된 동작 분류를 통해 제로 데이 악성 프로그램을 찾아내고 감지를 개선할 수 있습니다.
- 모든 엔드포인트 간 관리 통합: PC, Mac 및 Linux 시스템.
- 이해할 수 있는 언어로 수행 가능한 위협 포렌직을 확보하여 지능형 위협을 효율적으로 이해하고 빠르게 대처할 수 있습니다.
- 안전하게 파일을 공유하는 동안 모든 장치, 이동식 미디어 및 클라우드 스토리지에 저장된 기밀 데이터를 보호합니다.

데이터시트

보호할 수 있습니다. 120개 이상의 국가에 1억 개 이상의 글로벌 위협 센서가 배치되어 있고, 하루 쿼리량이 450억 건에 달하고, 하루에 150만 개 이상의 파일 및 100만 개가 넘는 URL이 분석되는 McAfee는 업계에서 가장 강력한 글로벌 위협 인텔리전스를 제공합니다.

간편한 배포, 중앙 집중식 관리

모든 사무실에 보안 전문가가 있는 건 아니므로 McAfee는 간편한 기능을 제공합니다. 단 4번의 클릭으로 보안 프로그램을 설치하고 실행 준비를 완료할 수 있습니다. McAfee ePO 소프트웨어를 사용하면 손쉽게 관리할 수 있습니다. 하나의 창에서 모든 장치의 보안 상황을 모니터링하고 정책을 관리하는 것이 가능합니다.

강력하고 효과적인 성능

확장 가능한 엔드포인트 프레임워크를 사용하면 중복 요소를 찾아서 제거하고 IT 운영 효율을 개선할 수 있습니다. 성능은 물론 유휴 시간 검색 및 셀프 학습 기능과 파일 및 프로세스의 동작을 기반으로 하는 적응형 검색까지 포함하도록 검색 기능이 최적화되어, 보다 공격적인 검색 성능이 필요할 때 즉시 필요한 성능을 활용할 수 있습니다.

전체 위협 수명 주기에 대한 제어

McAfee Complete Endpoint Protection - Business는 보안과 민첩성을 유지하도록 지원합니다. 협력적인 보안 프레임워크를 제공하여 엔드포인트 보안 환경의 복잡성을 없애고, 귀사 및 귀사 사용자의 생산성을 보호하고, 탐지 및 교정 대응 속도를 높일 수 있는 지능형 위협에 대한 가시성을 확보합니다. 글로벌 클라우드 기반 위협 인텔리전스를 통해 효과적이고 신속한 대응 및 관리자를 위한 실행 가능한 포렌직 기술로 새로운 지능형 위협에 즉시 대처할 수 있습니다. 끝으로, 중앙 집중식 웹 기반 관리를 통해 타사 및 McAfee 제품을 단일 콘솔과 통합하여 여러 솔루션 관리에 따른 IT 팀의 부담을 덜어주며, 위협 방어 수명 주기를 더욱 쉽게 파악 및 대응하며 관리할 수 있습니다.

McAfee: 업계의 선두 주자

- 선두 주자 Forrester Wave: Endpoint Security Suites, 2016년 4분기.¹
- NSS Labs에서 McAfee Endpoint Security를 권장합니다.²

McAfee Complete Endpoint Protection - Business의 주요 사항

악성 프로그램 차단(PC, Mac, Linux, 가상 시스템)

McAfee Endpoint Security

여러 엔드포인트 방어 기술과 실시간으로 통신하여 새로운 지능형 위협에 대한 분석 및 협력을 수행하고 시스템 또는 사용자에게 영향을 주기 전에 이러한 위협을 신속하게 차단하고 중지합니다.

동적 응용프로그램 억제

안전하게 동작을 시험하고, 클라우드에 연결하지 않고도 그레이웨어, 랜섬웨어, 환자 제로 위협 등과 같은 위협을 억제합니다.

Real Protect

- 사전 실행 기능 추출과 사후 실행 동작 및 메모리 분석을 결합하여 위협을 진단하는 실시간 동작 분석 및 시스템 학습을 통해 지능형 및 제로 데이 위협을 감지하고 차단합니다.
 - 모래상자 인식 악성 프로그램에서 "오류발생" 동작을 실행하고, 실시간으로 분석한 다음, 악성 프로그램이 시스템을 감염시키기 전에 동적 응용프로그램 억제가 악성 활동을 자동으로 차단하도록 하여 보호합니다.
-

Application Control

원치 않는 응용프로그램과 악성 프로그램의 설치 및 실행을 방지하며, 이때 시스템 성능, 사용자 또는 관리자에게 미치는 영향을 최소화합니다.

데스크톱을 위한 침입 방지 및 방화벽

- 알려지지 않은 제로 데이 위협과 새로운 취약성으로부터 보호합니다.
 - 시급하게 패치를 설치해야 하는 부담을 줄입니다.
-

Global Threat Intelligence

- 전 세계 수백만 개의 센서로부터 실시간으로 수집하는 정보를 바탕으로 모든 공격 벡터에서 새로운 위협을 막아냅니다.
 - 취약성 공격, 메모리 공격 및 더 높은 권한으로 실행을 시도하는 위협을 방지하기 위해 사용자 지정 제어를 생성할 수 있습니다.
-

웹 및 메시징 보안

URL 필터링 및 안전 검색을 통한 McAfee 웹 컨트롤

- 사용자가 악성 웹 사이트에 방문하기 전에 경고하여 위험을 줄이고 컴플라이언스를 보장합니다.
 - 웹 사이트 액세스에 대한 인증 또는 차단을 통해 웹 검색 정책을 강화합니다.
-

이메일 악성 프로그램 차단 및 안티스팸

- 이메일 서버를 보호하고 사용자의 받은 편지함에 악성 프로그램이 도착하기 전에 차단합니다.
 - McAfee Security for Email Servers를 사용하여 Microsoft Exchange 및 Lotus Domino 서버에서 악성 프로그램을 탐지, 제거하고 차단합니다.
-

McAfee Complete Endpoint Protection - Business의 주요 사항 (계속)

데이터 보호

장치 제어

이동식 미디어의 사용을 제한하여 중요한 데이터의 손실을 방지합니다.

전체 디스크, 파일, 폴더, 이동식 미디어 및 클라우드 스토리지 암호화

모든 PC, Mac, 랩톱, 네트워크 서버, 이동식 미디어 및 클라우드 스토리지 서비스에 저장된 기밀 데이터를 보호.

관리

McAfee ePO 소프트웨어

- 중앙의 단일 콘솔에서 정책과 컴플라이언스를 관리하고 보고합니다.
- 교차 플랫폼 정책을 사용하여 혼합된 OS 환경의 관리를 단순화합니다.

지능형 위협 방어 의 작동 방식

기술	역할	수행 방법
McAfee Endpoint Security 10	겉보기에 단절된 것으로 보이는 이벤트들을 표적 공격에 포함된 관련 이벤트로 탐지해낼 수 있도록 여러 위협 방어 사이에 통신을 사용합니다.	<ul style="list-style-type: none">• 위협 방어가 새로운 위협에 대한 정보를 서로 공유 및 학습하고, 알립니다.• 지능적인 적응형 검색은 여러 소스에서 얻은 관찰 결과를 활용하여 새로운 형태의 공격을 실시간으로 탐지하고 서로 정보를 제공합니다.• 로컬 및 글로벌 위협 인텔리전스를 통해 방어 정보를 제공합니다.• 의심스러운 응용프로그램 및 프로세스에 대해 자동 조치를 수행하고, 다른 방어 및 글로벌 커뮤니티에 정보를 공유하는 한편 신속하게 문제를 에스컬레이션합니다.
McAfee Threat Intelligence Exchange*	글로벌 데이터 소스 및 타사에서 가져온 확장 위협 인텔리전스를 제공하고 실시간 및 이전 이벤트로부터 로컬 위협 인텔리전스를 가져옵니다.	<ul style="list-style-type: none">• 보안 구성요소는 엔드포인트, 게이트웨이 및 기타 보안 구성요소를 통해 발견된 글로벌 네트워크의 조직 대상 위협에 대해 추가적인 통찰력을 얻을 수 있습니다.• 악성 프로그램 발견 시 수집되는 위협 세부 정보는 밀리초 단위로 Data Exchange Layer를 통해 전파되어 모든 엔드포인트에 도달하고 정보를 제공하여 위협에 적극적으로 대응합니다.• 게시자 인증서 목록, 파일 해시 및 조직 기본 설정에 맞는 위협 허용 결정과 같은 위협 인텔리전스에 대해 맞춤화할 수 있습니다.

지능형 위협 방어의 작동 방식 (계속)

기술	역할	수행 방법
McAfee Active Response*	자세한 라이브, 대화형 및 지속적인 조사 통찰력 및 분석으로 사고 대응 기능을 확장합니다.	<ul style="list-style-type: none"> 휴면 상태인 공격 구성요소 뿐만 아니라 IoA(공격 지표)일 수 있는 컨텍스트 및 시스템 상태 변화를 자동으로 캡처 및 모니터링하고 인텔리전스를 분석, 운영 및 포렌식 팀에 전송합니다. 공격 방식 변화에 대한 조정, 자동 데이터 수집, 경보 및 관심 객체에 대해 대응할 수 있으며 맞춤형 워크플로를 제공합니다. 공격 이벤트 탐지 시 지속적인 영구 수집기가 트리거되어 관리자 및 시스템에 공격 활동을 알립니다.
McAfee Application Control	기업 데스크톱 및 고정 기능 장치에서 인증 받지 않은 실행 파일을 차단합니다.	<ul style="list-style-type: none"> 시그니처 업데이트나 노동 집약적인 목록 관리를 하지 않고도 지속적인 고급 위협을 차단하는 신뢰 모델과 혁신적인 보안 기능을 사용합니다. McAfee Global Threat Intelligence와의 통합 지원을 통해 사용자가 일관된 방식으로 '확인된 정상' 응용프로그램 및 코드를 사용하고 '확인된 비정상' 및 '확인되지 않은 비정상' 대상을 차단할 수 있습니다. McAfee Threat Intelligence Exchange와 함께 배포할 경우, 지역화된 위협 인텔리전스를 통한 화이트리스트를 개선하여 알려지지 않은 표적 악성 프로그램에 즉시 대처할 수 있습니다. McAfee Threat Intelligence Exchange는 McAfee Advanced Threat Defense와 함께 협력하여 알려지지 않은 응용프로그램의 동작을 샌드박스에서 동적으로 분석하고 새로 탐지된 악성 프로그램으로부터 모든 엔드포인트를 자동으로 방어합니다.

* McAfee Threat Intelligence Exchange, McAfee Active Response 및 McAfee Advanced Threat Defense는 McAfee Complete Endpoint Protection 고객을 위해 별도로 판매되는 선택적인 기능입니다.

더 알아보기

자세한 내용을 보려면 다음 웹 사이트를 방문하십시오.

www.mcafee.com/kr/products/complete-endpoint-protection-business.aspx

1. The Endpoint Security Advantage, Forrester Wave™ 제공: Endpoint Security Suites, 2016년 4분기 www.mcafee.com/kr/resources/reports/rp-endpoint-security-advantage-forrester.pdf
2. NSS Labs 2017 AEP(첨단 엔드포인트 보호) 그룹 테스트, www.mcafee.com/kr/resources/reviews/nss-labs-aep-endpoint-security.pdf



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

McAfee 및 McAfee 로고, ePolicy Orchestrator 및 McAfee ePO 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2017 McAfee, LLC. 2814_0417 2017년 4월