McAfee Endpoint Threat Defense and Response 제품군

제로 데이 악성 프로그램을 탐지하고 최초 감염자를 보호하며 지능형 공격에 대처

사이버 위협이 점점 정교해짐에 따라 엔드포인트에 대한 차세대 보호 기능이 필요합니다. 위협이 진화하고 알 수 없는 취약성에 대한 위험이 증대됨에 따라 조직은 가시성이 제한되고 복잡성이 증가하는, 중첩되고 단절된 보안 솔루션을 짜맞춰야 할 수 있습니다. Intel Security는 McAfee® Endpoint Threat Defense 및 McAfee Endpoint Threat Defense and Response를 통해 이러한 문제를 해결합니다. 두 솔루션 모두 정적 및 동작 분석과 종합 인텔리전스를 활용하여 새로운 위협을 방어, 탐지, 수정하고 그에 대처하도록 조정합니다. 통합된 보안 구성요소는 가시성 및 위협 인텔리전스를 공유하고 워크플로를 간소화할 수 있는 개방형 통합 접근법을 통해 단일 시스템으로 작동합니다. 연결된 보안 및 실행 가능한 위협 포렌식은 빠르고 확실하게 위협을 진단하고 잠재적인 공격자를 미리 차단할 수 있는 보안 인프라를 제공합니다.

주요 이점

- 제로 데이 악성 프로그램, 그레이웨어 및 랜섬웨어를 탐지, 보호 및 수정하는 동시에 그에 대한 방어 기술을 사전에 조정합니다.
- 동적 평판, 동작 분석 및 기계 학습을 사용하여 보다 효과적으로 보호합니다.
- 사용자 및 신뢰할 수 있는 기업 응용프로그램에 대한 영향을 최소화하여 향상된 보호를 구현합니다.
- 보안 에코시스템 전체에서 공유되는 위협 인텔리전스를 통해 더 많은 위협에 빠르게 대처하고 교정합니다.
- McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어를 통해 통합 워크플로 및 관리용 단일 콘솔을 사용하여 인시던트 조사 및 교정을 간소화합니다.

제로 데이 악성 프로그램, 그레이웨어 및 랜섬웨어 차단

향상된 평판 및 동적 분석을 활용하여 잠재적인 취약성 공격을 탐지하는 정적 및 동적 위협 분석을 통해 새로운 위협을 미리 차단합니다. McAfee Threat Intelligence Exchange를 통해 **종합 인텔리전스를 적용하여 위협을 즉시 차단 및 억제하고 미래의 공격을 방지하도록 위협 평판을 바로 업데이트합니다.**

McAfee Endpoint Threat Defense 및 McAfee Endpoint Threat Defense and Response는 **클라우드 검색(미국에서 호스팅되는 데이터 센터)을 통해 노출된 악의적인 행동과 광범위한** Real Protect **위협 모델 간의 유사성을 식별하여 제로 데이 악성 프로그램을 차단합니다. 이 동작 분류 기술은 다른 보안 소프트웨어의 방어를 우회할 수 있는 실시간 위협을 근절시키는 데 사용됩니다. 이 기술은 제로 데이 탐색 및 실시간 교정을 지원하는** McAfee ePolicy Orchestrator **소프트웨어를 통해 실행 가능한 위협 인텔리전스를 제공합니다. 동작 분류는 동적 기계 학습을 통해 자동으로 개선되므로 보호 및 효율성을 극대화하는 동시에 보안 노출을 제한합니다.**

intel Security

이벤트 수 감소 및 보다 빠른 위협 해결

보안 이벤트 수를 줄이고, 더 많은 위협을 자동으로 진단하며, 인텔리전스를 공유하고, 사전 예방적 경보를 활용하여 자동 응답을 정의하는 방식으로 가장 중요한 요소에 초점을 맞춥니다. 이벤트를 더 빠르게 확인하고 보안 용량을 확대하는 동시에 전사적으로 보호를 강화할 수 있는 간소화된 워크플로를 통해 위협을 조사하고 해결하는 데 필요한 노력을 줄일 수 있습니다.

연결된 구성요소는 McAfee Data Exchange Layer를 통해 유용한 보안 정보를 자동으로 공유합니다. McAfee Threat Intelligence Exchange를 사용하면 McAfee Global Threat Intelligence 및 다른 타사 소스를 비롯한 전체 에코시스템에서 포괄적인 위협 인텔리전스를 종합하고 위협 정보를 즉시 공유하여 보호 기능을 자동으로 조정할 수 있습니다.

최초 감염자 보호

제로 데이 악성 프로그램을 탐지하고 엔드포인트 시스템을 악의적으로 변경하지 못하게 차단합니다. 동적 응용프로그램 억제는 그레이웨어의 동작을 감시하고, 취약성 공격이 시작되기 전에 이를 효과적으로 차단할 수 있도록 악의적인 변경을 방지합니다. 네트워크 안과 밖에서 엔드포인트의 보안을 유지하고, 사용자에게 보이지 않는 보호 기능을 통해 악의적인 행동을 억제합니다.

확장 및 조정이 가능하도록 보안 프로세스 운영

정책 실시, 인시던트 조사 및 교정은 모든 시스템에 대해 가시성을 제공하는 단일 창 방식의 관리 콘솔인 McAfee ePO 소프트웨어를 통해 간소화되므로 엔드포인트의 보안 상황을 언제든지 평가할 수 있으며 실시간 보호가 가능합니다. 단일 엔드포인트 또는 전체 인프라에서 통합 워크플로 및 단일 클릭 교정을 통해 모니터링, 검색 및 대응 노력을 줄일 수 있습니다. McAfee Endpoint Threat Defense 및 McAfee Endpoint Threat Defense and Response를 사용하면 자동화된 기계 학습을 활용하여 동작 분류 모델을 업데이트하고 모든 보안 구성요소에서 위협 인텔리전스를 즉시 공유할 수 있으므로 새로운 위협에 대해 단일의 통합된 시스템으로 작동할 수 있습니다. 미래의 공격을 방지하고 사전 구성된 대응을 활용하여 잠재적인 위협을 억제할 수 있으므로 다른 보안 관리 우선순위에 집중하도록 직원의 업무를 줄일 수 있습니다.

진화한 공격 파악, 우선순위 지정 및 교정

McAfee Endpoint Threat Defense and Response는 공격의 출처, 범위 및 영향을 판단하는 데 도움이 됩니다. 이는 McAfee Active Response 기술을 사용하여 인프라의 엔드포인트 전체에서 실시간 가시성과 이전의 가시성을 모두 제공합니다. 공격 지표는 보다 신속하게 대응할 수 있도록 강력한 컨텍스트로 식별되어 우선 순위가 지정됩니다.

현재 전파되고 있거나, 대기 중이거나, 탐지를 회피하기 위해 진행 경로를 지워버린 위협을 사전에 빠르고 정확하게 발견하여 대처합니다. 지식 기반의 가시성과 제어력은 위협이 기반을 마련하고자 하는 위치를 파악할 수 있으며, 응답기가 즉시 위협을 억제 및 교정하여 노출을 몇 달에서 분 단위 또는 심지어 밀리초 단위로 줄일 수 있게 해줍니다.

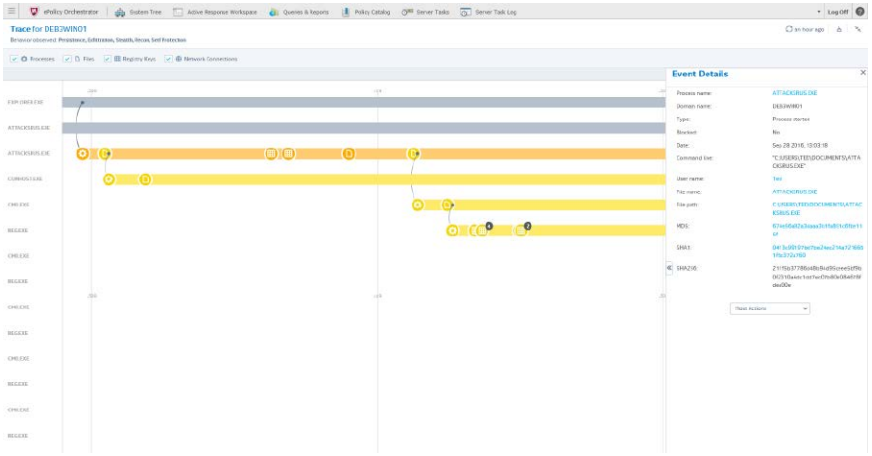

그림 1. 위협 작업 공간은 의심스러운 인시던트의 출처와 동작을 추적하여 인시던트 대응 시간을 단축합니다.

McAfee Endpoint Threat Defense and Response 제품군 기능

구성 요소	이점	고객 혜택	차별화	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
동적 응용프로그램 억제[1]	그레이웨어가 네트워크 안과 밖에서 엔드포인트를 악의적으로 변경하지 못하게 차단하여 최초 감염자를 보호합니다.	• 최초 감염자에게 영향을 주지 않으면서 잠재적인 위협 분석을 지원합니다. • 사용자나 신뢰할 수 있는 응용프로그램에 영향을 주지 않고 향상된 보호를 구현합니다. • 수동 개입을 최소화하여 위협 발생부터 억제까지의 시간을 단축합니다. • 최초 감염자를 보호하는 동시에 엔드포인트 생산성을 유지하고 네트워크가 감염되지 않도록 격리합니다.	• Intel Security 인프라의 통합된 부분으로 최적의 보호와 효율성을 제공합니다. • 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 제로 데이 악성 프로그램이 실행되기 전에 차단하고 이전 탐지를 회피한 실시간 위협을 중단시킵니다.	• 랜섬웨어 같이 탐지하기 어려운 개체를 비롯하여 더 많은 제로 데이 악성 프로그램을 쉽게 차단합니다. • 위협을 자동으로 파악, 분석 및 교정하므로 수동으로 개입할 필요가 없습니다. • 자동화된 분류 및 연결된 보안 인프라를 사용하여 방어 기능을 조정합니다.	• 정적 및 동적 동작 분석은 1단계 접근법보다 더 강화된 보호를 제공합니다. • 동적 동작 분석을 통해서만 발견할 수 있는 악성 프로그램을 탐지합니다. • 긴밀한 통합으로 실시간 평판 업데이트를 공유하고 모든 보안 구성요소에 대한 보안 효율성을 개선합니다.	√	√

구성 요소	이점	고객 혜택	차별화	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	보안 구성요소를 연결하여 상황별 통찰력을 공유하고 적응형 위협 방지를 위해 전사적인 가시성 및 제어력을 제공합니다.	• 보안 시스템 전체에서 최초 감염자 위협을 식별하고 이를 즉시 공유하여 이후의 감염을 방지할 수 있습니다. • 총 소유 비용을 절감하고 엔드포인트 보안을 효율적으로 운영할 수 있습니다. • 독립 보안 기술을 단일의 조화된 시스템으로 전환하여 폐쇄형 루프 보호를 제공하도록 보안 구성요소를 연결합니다.	• McAfee Global Threat Intelligence 피드, 타사 및 로컬 인텔리전스를 종합합니다. • 로컬 또는 타사 인텔리전스를 사용하여 신뢰할 수 있는 항목과 신뢰할 수 없는 항목을 정의합니다. • 엔드포인트, 웹, 네트워크 및 클라우드 제품 전체에서 위협 평판 정보를 즉시 연결합니다. • 세부 정보가 있는 실행 가능한 위협 인텔리전스 보고서를 추출하여 방어 기능을 조정합니다.	√	√
McAfee Data Exchange Layer	Intel Security 제품 및 다른 타사 제품과 통합하여 효율적으로 통신할 수 있도록 보안을 연결합니다.	• 위험을 줄이고 대응 시간을 단축합니다. • 오버헤드 및 운영 직원 비용을 절감할 수 있습니다. • 프로세스를 최적화하고 실용적인 권장 사항을 제시합니다.	• 모든 보안 제품에서 위협 정보를 공유합니다. • 감염을 방지하고 보호 기능을 업데이트하도록 최초 감염자 위협 통찰력을 다른 모든 엔드포인트와 즉시 공유합니다.	√	√
McAfee ePO 관리 플랫폼	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. • 전체 시스템에서 단일 창 가시성을 확보하여 언제든지 실시간으로 보안 상황 및 보호를 평가할 수 있습니다. • 사용자 지정된 정책을 실시하여 Intel Security 보호 기술을 빠르게 배포하고 관리합니다. • 자동화된 동적 쿼리, 대시보드 및 응답을 통해 인사이트에서부터 대응까지의 시간을 단축합니다.	• 단일 콘솔을 통한 세밀한 제어, 비용 절감 및 신속한 운영 보안 관리가 가능합니다. • 끌어서 놓기 대시보드로 전체 에코시스템에서 실시간 가시성을 향상시킵니다. • 개방형 플랫폼 SDK (소프트웨어 개발 키트)로 미래의 혁신적인 보안 기능을 신속히 채택할 수 있습니다.	√	√
McAfee Active Response	사전 예방적 위협 가시성을 제공하고, 일정을 관리하며, 실시간 발견 및 기록을 발견하고, 탐지할 수 있으며 즉각적인 조치가 가능하고 보호 기술을 조정합니다.	• 실시간 및 기록 위협 데이터를 빠르게 검색하여 공격의 전체 범위를 파악하고 신속히 조사하여 대응 시간을 줄입니다. • 위협 대응을 자동화하여 실시간 보안 보호를 제공하므로 수동으로 개입할 필요가 없습니다. • 중요한 위협에 우선순위를 지정합니다. • 지속적인 모니터링 및 사용자 지정 가능한 수집기를 사용하여 심층적으로 검색하여 실행 중이거나 휴면 상태에 있는 것은 물론 삭제되었을 수도 있는 공격 지표까지 찾아냅니다.	• 보호 기술로 탐지되지 않았던 환경에서 알 수 없는 취약성 공격 시도 및 위험한 동작에 대한 즉각적인 가시성을 확보합니다. • 모든 엔드포인트에서 통합 실시간 검색을 통해 각 엔드포인트의 이벤트 일정을 조사하여 위협을 발견합니다. • 보호, 수정 및 조정을 위한 단일 클릭 동작이 지원되므로 여러 도구 및 단계를 단일 작업으로 줄일 수 있습니다.		√

사양

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
지원되는 플랫폼: • Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary • Mac OS X 버전 10.5 이상 • Linux: 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	**지원되는 플랫폼:** • Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary • RedHat 6.5 • CentOS 6.5 • Windows Server 2008, 2012, 2016

1. McAfee Endpoint Threat Defense and Response는 미국에 위치한 호스팅된 데이터 센터를 포함하여 고객 인증을 확인하고 파일 평판을 확인하며 의심스러운 파일 탐지 및 발견과 관련된 데이터를 저장하는 데 사용됩니다. 필수는 아니지만, 동적 응용프로그램 억제는 클라우드 연결을 통해 최적의 성능을 발휘합니다. 전체 McAfee Active Response, 동적 응용프로그램 억제 및 Real Protect 제품 기능을 사용하려면 클라우드 액세스, 활성 지원이 필요하며 클라우드 서비스 약관의 적용을 받습니다.

자세한 내용

www.mcafee.com/kr/products/endpoint-threat-defense.aspx에서 McAfee Endpoint Threat Defense의 이점에 대해 자세히 알아보십시오.

www.mcafee.com/kr/products/endpoint-threat-defense-response.aspx에서 McAfee Endpoint Threat Defense and Response의 이점에 대해 자세히 알아보십시오.

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