McAfee Endpoint Security

사전 예방적 위협 관리 및 검증된 보안 제어에 맞춤화된 보안

엔드포인트 보안: 여러분의 우선 순위는 무엇입니까?

오늘날 기업에서는 하나 또는 여러 팀이 보안을 담당할 수 있습니다. 엔터프라이즈 조직의 경우 보안은 IT 관리팀 및 보안 운영팀과 같이 여러 팀에서 공유하는 기능입니다. 자신이 비즈니스에서 맡는 역할을 가장 잘 설명하는 방법이 무엇이든, 엔드포인트 보호 플랫폼과 관련해서는 다른 기능 및 결과에 더 관심을 기울이게 될 것입니다.

의존하는 엔드포인트 솔루션은 본인에게 가장 중요한 우선 순위와 맞아야 합니다. 사용자가 담당하는 역할이 무엇이든 McAfee® Endpoint Security는 위협 방지 및 추적에서 보안 제어 조정에 이르기까지 사용자의 특정한 중요 요구 사항을 충족합니다. McAfee® MVISION Insights 기능을 사용하면 공격이 발생하기 전에 특정 위협 우선순위가 적용됩니다. 이 솔루션을 통해 사용자를 위한 시스템 가동 시간을 보장하고, 더 많은 자동화 기회를 찾고, 복잡한 워크플로를 단순화할 수 있습니다.

가동 시간 및 가시성 보장

McAfee Endpoint Security를 사용하면 고객이 사전 방어 및 해결 도구로 위협 방어 라이프사이클의 대응 및 관리가 가능합니다. 자동 롤백 교정은 시스템을 정상 상태로 되돌려 사용자 및 관리자가 생산성을 유지하고 시스템 교정, 복구 수행 또는 감염된 시스템의 이미지 재생성에 소요될 시간을 절약해 줍니다. 글로벌 위협 인텔리전스 및 실시간 로컬 이벤트 인텔리전스를 엔드포인트 및 McAfee® MVISION EDR 간에 공유하여 위협 이벤트 상세 정보를 수집하고, 탐지하고, 탐지 회피를 시도하는 위협을 방지하고, 추가 조사를 위해 MITRE ATT&CK 프레임워크로 위협을 맵핑합니다. 관리는 현지, SaaS 또는 가상 환경 배포 중에서 선택할 수 있는 중앙 집중식 관리 콘솔을 통해 단순하게 유지됩니다. MVISION Insights는 공격 성향이 강한 잠재적인 우선순위가 높은 위협에 대해 고유한 가시성 및 제어를 제공할 뿐만 아니라 조직의 보안 상황이 위협에 대한 보호를 제공하는지도 판단합니다. 이를 통해 치명적인 위협에 대응하는 보호 수준을 적용하고 공격자가 공격하기 전에 차단합니다.

주요 이점

- **진화된 위협에 대비한 고급 방어:** 기계 학습, 자격 증명 도난 방어 및 롤백 교정을 통해 Windows 데스크톱 및 서버 시스템의 기본 보안 기능 보완
- **추가 복잡성이 없음:** 단일 정책 및 콘솔을 사용하여 McAfee 기술, Windows Defender 안티바이러스 정책, Defender Exploit Guard 및 Windows 방화벽 설정을 관리합니다.
- **MVISION Insights:** 지금 이용할 수 있는 최고의 실행 가능한 보안 인텔리전스 솔루션으로 사용자의 섹터나 지역을 목표로 하여 우선순위로 지정된 잠재적인 활성 캠페인에 즉시 대응하십시오. MVISION Insights는 캠페인에 대해 보호가 부족한 엔드포인트를 예측하며 탐지를 향상할 방법에 대한 규범적인 지침을 제공합니다. MVISION Insights는 동시에 행동을 규정하고, 우선순위를 지정하며, 예측할 수 있는 유일한 엔드포인트 솔루션입니다.

McAfee에 문의

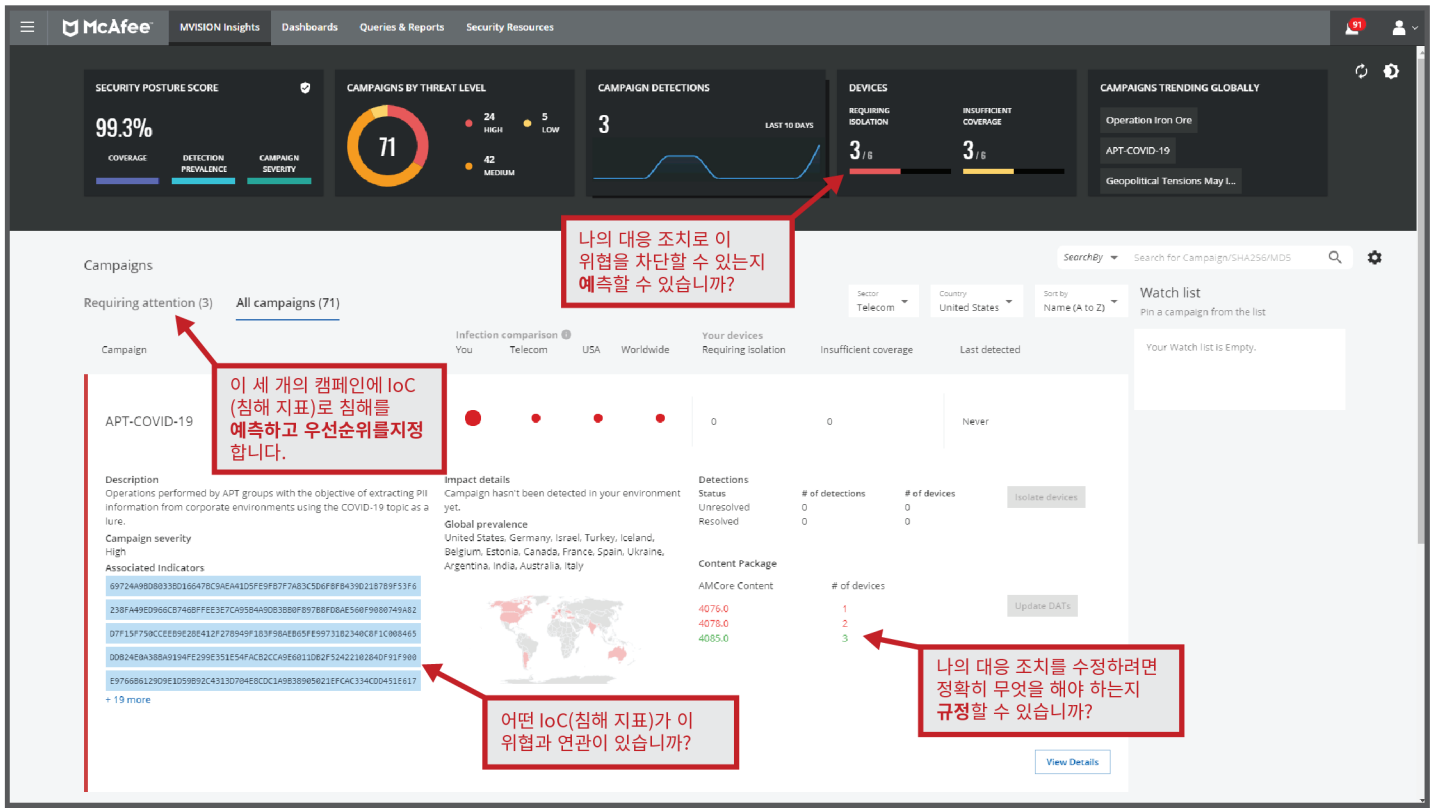

그림 1. MVISION Insights 대시보드. (MVISION Insights가 효율적으로 작동하려면 McAfee Endpoint Security 원격 측정(옵트인)이 필요합니다.)

MVISION Insights를 사용하면 조직은 산업 및 지역을 기반으로 공격 가능성에 따라 우선순위가 지정된 잠재적 위협에 대해 경보 및 알림을 받습니다. 또한 MVISION Insights는 보안 상태와 위협에 대응한 보호 가능 여부에 대해 로컬 평가를 제공합니다. 위협에 취약한 엔드포인트를 식별하고 업데이트할 항목에 관한 규범 지침도 제공합니다. 따라서 공격 가능성이 있는 적들보다 앞서 있기 위해 더욱 사전 예방적인 조치를 취할 수 있습니다.

McAfee Endpoint Security는 단일 소프트웨어 에이전트를 사용하여 여러 관여 계층에서 위협 통찰력을 수집하여 여러 포인트 제품으로 인한 중복을 제거합니다. 그 결과, 보안에 대한 통합 접근 방식으로 수동으로 위협 상관관계를 파악할 필요가 없습니다. 추가 조사가 필요한 위협 세부 정보는 사고 대응자에게 자동으로 전달됩니다. 위협 이벤트 데이터는 Story Graph를 통해 단순하고 한눈에 알아볼 수 있는 형식으로 제공되므로 위협 세부 정보를 시각화하고 관리자가 악의적 행위자의 출처를 쉽게 파악하고 조사할 수 있습니다.

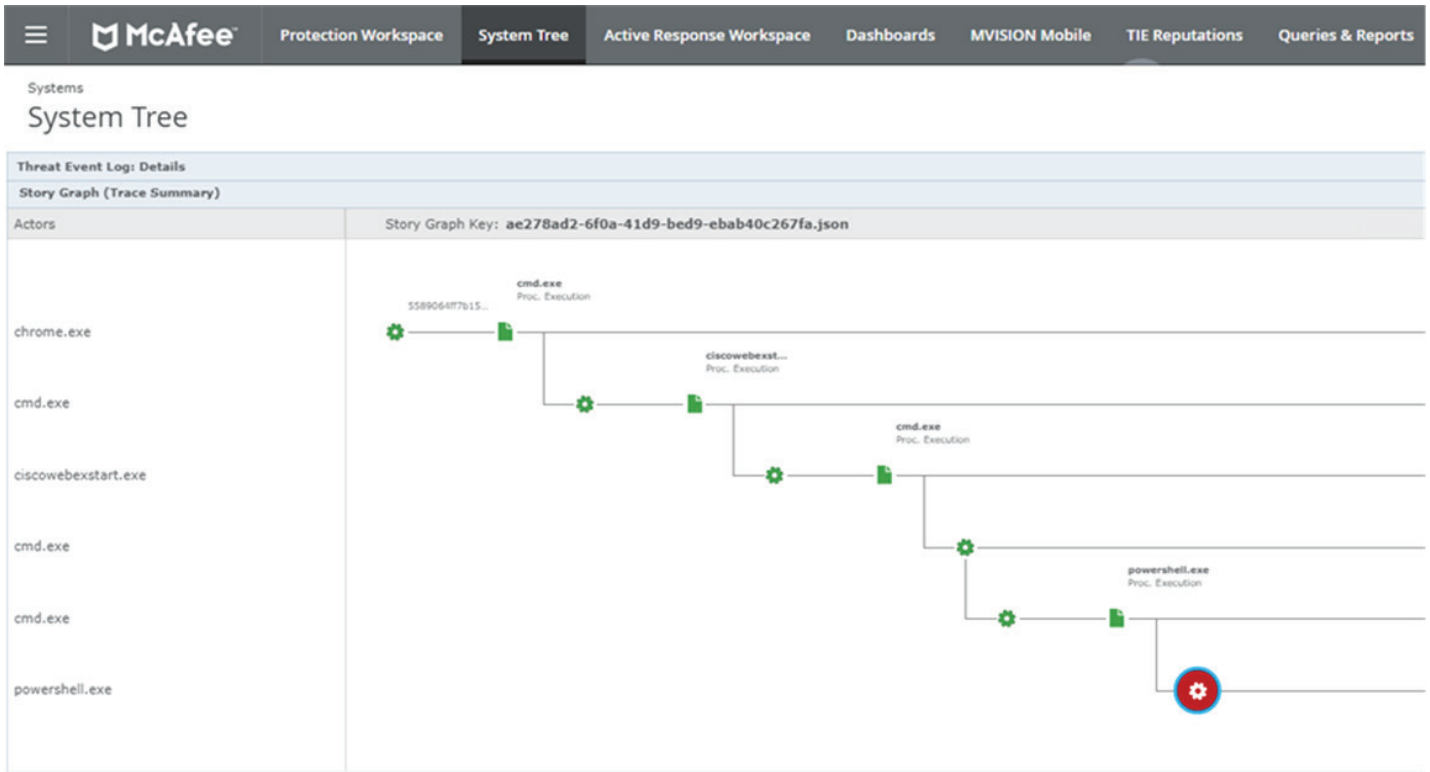

그림 2. Story Graph.

진화한 통합 위협 방어로 자동화 및 대응 시간 단축

동적 응용프로그램 억제(Dynamic Application Containment, DAC)와 같은 추가적인 고급 위협 방어는 통합 McAfee Endpoint Security 프레임워크의 일부로 사용 가능하며 조직이 진화된 최신 위협을 방어할 수 있도록 돕습니다.[1] 예를 들어, DAC는 그레이웨어 및 기타 새로운 악성 프로그램을 분석하고 조처하여 감염을 방지합니다.

진화한 위협에 대한 또 다른 기술에는 기계 학습 동작 분류를 사용하여 제로 데이 악성 프로그램을 찾아내고 감지를 개선할 수 있는 Real Protect가 있습니다. 클라우드에서 무시그니처 분류가 수행되며 실시간에 준하는 탐지를 제공하면서 클라이언트 공간을 조금만 차지합니다. 실행 가능한 통찰력이 제공되며 이를 사용해 공격 지표(IoA)와 침해 지표(IoC)를 생성할 수 있습니다. 특히 측면 이동 탐지, 최초 감염자 검색,

위협 행위자 속성 파악, 포렌식 조사 및 교정에 유용합니다. 또한 Real Protect는 자동으로 동작 분류를 진화시켜 동작을 확인하고 규칙에 추가하는 방법으로 향후 분석 속도를 높이고 정적 및 런타임 기능 모두를 사용해 미래의 유사한 공격을 식별합니다.

마지막으로, 감염을 즉시 방지하고 IT 보안 관리자가 소요하는 시간을 줄이기 위해 클라이언트는 마지막으로 알려진 정상 상태로 확인된 엔드포인트를 복구합니다.

지능적인 엔드포인트 보호는 공격자가 현재 무엇을 하고 있는지 알려줍니다.

더 나은 인텔리전스는 더 나은 결과를 가져옵니다. McAfee Endpoint Security는 관찰한 바를 프레임워크에 연결된 여러 엔드포인트 방어 기술과 실시간으로 공유하고 협업을 통해 의심스러운 동작을 더 빠르게 파악하고, 방어에서 더욱 긴밀하게 협조하고, 표적 공격 및 제로 데이 위협을 더욱 확실하게 막아냅니다. 파일 해시, 소스 URL, AMSI 및 PowerShell 이벤트와 같은 통찰력을 추적하고 다른 방어 기술뿐만 아니라 클라이언트 및 관리 인터페이스와도 공유하여 사용자가 공격을 이해하도록 돕고 관리자에게 실행 가능한 위협 포렌식을 제공합니다.

추가적으로 McAfee® Threat Intelligence Exchange 기술은 게이트웨이, 샌드박스 및 SIEM(보안 정보 및 이벤트 관리) 솔루션을 포함한 다른 McAfee 솔루션과 협업하기 위해 적응형 보안을 강화합니다. 로컬, 커뮤니티 및 글로벌 보안 인텔리전스를 수집하고 배포하면 공격 및 발견과 억제 사이의 시간 격차가 몇 주, 몇 개월에서 밀리초 단위로 줄어듭니다.

McAfee Endpoint Security 프레임워크를 McAfee® Global Threat Intelligence(McAfee® GTI)와 결합하면 클라우드를 활용해 파일, 웹, 메시지, 네트워크 등 모든 벡터에서 새롭게 등장한 모든 위협에 관한 정보를 실시간으로 모니터링하고 조치를 취합니다. 기존 엔드포인트 공간 및 관리 시스템은 현지화된 글로벌 위협 인텔리전스를 통해 강화되어 알려지지 않은 표적 악성 프로그램의 침입을 즉시 막습니다. 의심스러운 응용프로그램 및 프로세스에 대한 자동 조치는 새롭게 등장한 공격 형태에 대한 대응을 신속하게 에스컬레이션하는 한편, 다른 방어 및 글로벌 커뮤니티에 정보를 공유합니다.

DAC 및 Real Protect를 사용하는 고객은 더 진화한 위협과 해당 위협의 동작에 대한 통찰력을 얻습니다. 예를 들어, DAC는 포함된 응용프로그램 그리고 레지스트리 또는 메모리와 같이 응용프로그램이 가져오려고 시도하는 액세스 유형에 대한 정보를 제공합니다.

엔드포인트 프로세스 위협 통찰력을 수집하고 사고 대응자를 지원하여 악성 프로그램을 추적하는 데 관심 있는 조직을 위해, Real Protect는 악의적이라고 간주된 동작에 대한 통찰력을 제공하고 위협을 분류합니다. 이러한 통찰력은 파일 기반 악성 프로그램이 압축, 암호화 또는 합법적 응용프로그램 오용과 같은 기술을 통해 탐지를 회피하기 위한 시도를 파헤치는 데 특히 도움이 될 수 있습니다.

강력하고 효과적인 성능으로 제시간에 대응하도록 지원

느린 검색으로 사용자를 방해하거나 설치 시 오랜 시간이 걸리거나 관리하기가 복잡한 지능적 방어는 쓸모가 없을 것입니다. McAfee Endpoint Security는 일반적인 서비스 계층과 사용자의 시스템에 필요한 리소스와 전력을 줄이는 데 도움을 주는 새로운 안티맬웨어 코어 엔진을 이용하여 사용자의 생산성을 보호합니다. 엔드포인트 검색은 장치가 유휴 상태인 경우에만 수행되며 재시작 또는 종료 후에 원활하게 재개되기 때문에 사용자 생산성에 영향을 주지 않습니다.

적응형 검색 프로세스는 의심스럽거나 알 수 없는 소스로부터 오는 리소스에만 집중하도록 신뢰하는 프로세스와 소스를 학습하므로 CPU 부담을 줄이는 데도 도움이 됩니다. McAfee Endpoint Security는 McAfee GTI를 사용하는 통합 방화벽을 갖춰 봇네트, 분산 서비스 거부(DDoS) 공격, 지능형 지속가능 위협 및 위험한 웹 연결로부터 엔드포인트를 보호합니다.

복잡성 감소와 향상된 지속 가능성으로 압력을 완화합니다.

중복되는 기능과 별도의 관리 콘솔이 있는 보안 제품들이 빠른 속도로 늘어나면서 많은 사람이 잠재적 공격을 분명히 파악하는 데 어려움을 겪고 있습니다. McAfee Endpoint Security는 현재 및 미래의 엔드포인트 솔루션을 중앙 집중화하는 데 기반이 되는 개방적이고 확장 가능한 프레임워크 덕분에 강력하고, 장기적인 보호를 제공합니다. 이 프레임워크는 기존 보안 투자와 기술 간 협력을 위해 Data Exchange Layer를 활용합니다. 통합 아키텍처는 다른 McAfee 제품과 원활하게 통합되며 보안 허점, 기술 사일로와 중복을 더욱 줄이는 동시에 운영 비용 및 관리 복잡성을 줄여 생산성을 높입니다.

McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어는 엔드포인트를 모니터링, 배포 및 관리하기 위한 단일 창을 제공하여 복잡성을 더욱 줄입니다. 이해할 수 있는 언어로 된 사용자 지정 가능한 보기와 실행 가능한 워크플로는 시스템 검역, 악의적인 프로세스 중단 또는 데이터 추출을 차단함으로써 보안 상태를 빠르게 평가하고, 감염 위치를 찾고, 위협의 영향을 완화할 수 있는 도구를 제공합니다. 또한 모든 엔드포인트, 다른 McAfee 기능 및 130개 이상의 타사 보안 솔루션을 관리할 수 있는 단일 위치를 제공합니다.

기능	필요한 이유
사전 위협 탐지 및 대응(MVISION Insights)	▪ 사용자의 산업 및 지역을 기반으로 잠재 위협을 예측적 및 선제적으로 탐지합니다. ▪ 잠재적 위협에 대응한 보안 상태 및 개선 방법에 대한 수정 지침을 로컬에서 평가합니다. ▪ 공격 발생 전에 보호를 설정하여 적들보다 한발 앞서 나갑니다.
Real Protect	▪ 기계 학습 동작 분류가 제로 데이 위협을 거의 실시간으로 감지하고 실행 가능한 위협 인텔리전스를 지원합니다. ▪ 동작 분류를 자동으로 진화시키고 규칙을 추가하여 미래의 공격을 파악합니다.
표적 공격에서 엔드포인트 보호	▪ 엔드포인트 보호는 공격 발생에서 억제까지의 시간 격차를 일 단위에서 밀리초로 단축합니다. ▪ McAfee Threat Intelligence Exchange는 여러 소스로부터 인텔리전스를 수집하여 월등히 진화한 새로운 공격에 대한 정보를 보안 구성 요소 간에 즉시 공유할 수 있도록 지원합니다. ▪ AMSI와 PowerShell 이벤트 로깅은 파일이 없는 스크립트 기반 공격을 발견하고 방어합니다.
지능적인 적응형 검색	▪ 신뢰할 수 있는 프로세스에 대한 검색을 우회하고 의심스러워 보이는 프로세스 및 응용프로그램에 우선순위를 지정하므로 성능 및 생산성이 향상됩니다. ▪ 적응형 동작 검색은 활동을 모니터링 및 조사하고 의심스러운 것이 확실한 활동은 에스컬레이션합니다.
롤백 교정	▪ 롤백 교정은 악성 프로그램에 의한 변경 사항을 자동으로 복구하고 시스템을 마지막으로 알려진 정상 상태로 되돌려 사용자의 생산성을 유지합니다.
사전 웹 보안	▪ 사전 웹 보안은 웹 보호 및 엔드포인트 필터링으로 안전한 탐색을 보장합니다.
동적 응용프로그램 억제	▪ DAC는 랜섬웨어 및 그레이웨어를 차단하고 '최초 공격 대상'을 보호합니다. [2]
악의적인 네트워크 공격 차단	▪ 통합 방화벽은 McAfee GTI 기반의 평판 점수를 이용하여 봇네트, DDoS, 지능형 지속가능 위협 및 의심스러운 웹 연결로부터 엔드포인트를 보호합니다. ▪ 방화벽 보호는 시스템 시작 중 아웃바운드 트래픽만 허용하여 회사 네트워크에 포함되지 않은 엔드포인트를 보호합니다.
Story Graph	▪ 관리자가 위협을 이해하고 더욱 빠르게 대응할 수 있도록 감염이 있는 곳을 빠르게 확인하고 발생 원인을 파악하며 노출 기간을 파악할 수 있습니다.
다양한 배포 선택으로 중앙 집중식 관리(McAfee ePO 플랫폼)	▪ 진정으로 집중화된 관리는 더욱 향상된 가시성을 제공하고, 작동을 단순화하고, IT 생산성을 향상하고, 보안을 통합하고, 비용을 낮춰줍니다.
개방적이고 확장 가능한 엔드포인트 보안 프레임워크	▪ 통합 아키텍처를 사용하면 엔드포인트 방어에서 협업 및 소통이 가능하므로 방어력이 더욱 강화됩니다. ▪ 따라서 중복을 제거하고 프로세스를 최적화하여 운영비를 절감합니다. ▪ 기타 McAfee 제품 및 타사 제품과 원활하게 통합하여 보안 허점을 줄입니다.

표 1. 주요 기능과 이러한 기능이 필요한 이유.

사이버 위협에 대한 우위 확보

McAfee Endpoint Security는 오늘날의 보안 실무자가 공격자의 장점을 극복하는 데 필요한 인텔리전스, 협력적 방어, 복잡한 환경을 단순화하는 프레임워크 등을 제공합니다. 타사 테스트에서 증명된 강력하고 효과적인 성능과 위협 탐지 효율성으로 조직은 사용자를 보호하고, 생산성을 증대하고, 안심할 수 있습니다.

엔드포인트 보안 분야의 마켓 리더인 McAfee는 강력한 보호를 보안팀이 더 적은 리소스로도 더 빠르게 위협을 해결할 수 있도록 지원하는 효율적인 관리와 결합하여 심층 및 사전 방어를 구성하는 광범위한 솔루션을 제공합니다.

간편한 마이그레이션

최신 버전의 McAfee ePO 소프트웨어가 설치된 환경에서 McAfee VirusScan® Enterprise 및 McAfee® Agent는 자동 마이그레이션 도구를 활용하여 기존 정책을 약 20분 이내에 McAfee Endpoint Security로 마이그레이션할 수 있습니다.[3]

또한 McAfee Endpoint Security를 사용하면 다음과 같은 이점이 있습니다.

- 사용자 검색의 영향이 없으므로 사용자 생산성이 향상됩니다.
- Story Graph에 맵핑된 강력한 포렌식 데이터로 통찰력을 쉽게 확보하고 조사를 간소화하여 정책을 강화할 수 있습니다.
- 롤백 교정은 자동으로 악성 프로그램으로 인한 변경 사항을 복구하고 시스템을 정상적으로 유지합니다.
- MVISION Insights를 통해 우선순위가 지정된 잠재적 위협에 대한 사전 통찰력 및 위협 대응의 조정에 대한 규범 지침을 제공합니다.
- 관리할 에이전트가 적고 검색 회피를 사용하므로 수동 입력이 줄어듭니다.
- 협업 방어를 제공하여 진화한 위협을 방어합니다.
- 다른 진화한 위협과 EDR(엔드포인트 탐지 및 대응) 솔루션에 연결할 수 있는 차세대 프레임워크입니다.

자세히 알아보기

McAfee Endpoint Security에 대해 더 자세히 알아보려면 여기를 방문하십시오.

McAfee Endpoint Security가 McAfee 제품 포트폴리오를 보완하는 방법에 대해 알아보려면 다음을 방문하십시오.

- MVISION Endpoint
- MVISION 제품군
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. 대부분의 McAfee 엔드포인트 제품군과 사용 가능합니다. 자세한 내용은 영업 담당자에게 문의하십시오.
2. 동일 자료.
3. 마이그레이션 시간은 기존 정책 및 환경에 따라 달라질 수 있습니다.

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