McAfee ePolicy Orchestrator

보안 전문가에게 영감을 주고 역량을 강화

보안 관리에는 도구와 데이터 사이를 번거롭게 오가는 과정이 필요합니다. 이러한 과정에서 도구 사이의 보이지 않는 틈이 악용되어 더 많은 손상을 입는 동안 더 많은 시간이 소요되어 적이 더 유리한 위치를 차지하게 됩니다. 사이버 보안 인력은 제한되어 있으며 복잡한 사이버 보안 환경을 간단하게 조직화할 수 있도록 권한이 부여되어야 합니다.

조직에서 손상을 최소화하려면 모든 유형의 장치에서 신속하게 위협에 대응해야 하며 관리 부서에는 보안 효율성의 증거가 필요합니다. 사내와 클라우드에서 사용 가능(두가지 모델SaaS 또는 IaaS 중에서 선택 가능)한 McAfee® ePolicy Orchestrator®(McAfee ePO™) 관리 플랫폼은 시간을 절약하고 잠재적인 인적 오류를 없애는데 도움을 주며 보안 관리 책임자들이 더 빠르고 더 효율적으로 대응할 수 있도록 도와줍니다.

기본 보안

필수 기능을 사용하여 시작해 보겠습니다. 모든 보안 아키텍처의 핵심은 장치 및 시스템의 상태를 모니터링하고 제어할 수 있는 기능입니다. Center for Internet Security (CIS) Controls™ and Benchmarks 및 National Institute of Standards Technology (NIST) SP 800-53 보안 및 개인정보 제어 등의 산업 표준에서는 보안 인프라를 필수적으로 모니터하고 제어해야 합니다. McAfee ePO 콘솔을 이용하면 중대한 가시성을 얻을 수 있으며 엔터프라이즈 전반에서 양호한 보안 상황을 갖출 수 있도록 정책을 설정하고 자동으로 시행할 수 있습니다. 단일 콘솔에서 전체 엔터프라이즈의 정책을 관리하고 시행하므로 여러 제품을 조직화해야 하는 복잡성이 없어집니다. 이 필수적인 보안 관리 기능은 IT 보안 컴플라이언스의 기본입니다.

주요 이점

- 클라우드나 사내에서 사용할 수 있으며, 우수한 간편성을 위해 통합된 고유한 단일 창을 사용하는 업계에서 인정받은 중앙 집중식 관리
- 관리 업무를 간소화하고 효율성을 높이는 자동화된 워크플로
- 더 빠르고 정확하게 대응하기 위해 McAfee와 150개 이상의 타사 솔루션을 통합하는 개방형의 포괄적인 플랫폼
- 시장에서 점유율이 가장 큰 장치의 보안을 공통으로 관리
- Windows Defender와 같은 운영 체제에 기본 제공되는 고유 제어 기능을 활용 및 향상
- 장치부터 클라우드까지 포함하여 범위를 수백 개에서 수천 개의 장치로 확장

McAfee에 문의

입증된 고급 보안 관리-간소화

36,000곳 이상의 비즈니스와 조직에서 보안을 관리하고 컴플라이언스 프로세스를 간소화 및 자동화하며 장치, 네트워크 및 보안 작업 전반에 대한 전체적인 가시성을 높이기 위해 신뢰할 수 있는 McAfee ePO 콘솔을 이용하고 있습니다. 대기업들은 확장성이 우수한 McAfee ePO 콘솔의 아키텍처를 활용하고 있으며 이는 대규모 기업이 통합된 단일 창에서 수십만의 노드를 관리할 수 있도록 지원합니다. 이 대시보드 보기를 사용하면 위험 작업의 우선순위를 지정할 수 있고, 전체 디지털 영역의 보안 상황을 요약하여 새 보호 작업 공간에 하나의 그래픽 보기로 제공합니다. 추가적으로, 보안 리소스 페이지에서 최신 위협 정보 및 리서치를 간편하게 찾을 수 있습니다.

관리자가 특정 이벤트를 드릴다운하여 추가적인 통찰력을 얻을 수 있습니다. 이 요약 보기를 사용하면 데이터를 작성하고 즉시 합리적으로 분석하는 데 필요한 시간을 줄이고 수동 개입이 필요한 경우에도 발생할 수 있는 오류가 제거됩니다. McAfee ePO 콘솔은 엔터프라이즈 보안 관리자에게 정책 유지 관리를 단순화하고, 당사의 업계 최고 메시징 패브릭인 Data Exchange Layer (DXL)를 활용해 타사 위협 인텔리전스를 가져오며 정책을 제품 어레이와 양방향으로 통합할 기회를 제공합니다. 이러한 운영 효율성은 프로세스 및 데이터 공유 오버헤드를 낮춰 더 신속하고 정확한 대응을 가능하게 합니다.

지원 센터는 McAfee 제품에 대한 정보에 쉽게 액세스할 수 있도록 해주며 고객 환경에서 ePO 서버 상태에 대한 개요를 제공합니다. 이는 사내 ePO 및 AWS의 ePO에서 사용 가능합니다. 사용자는 지원 및 제품 알림을 적극적으로 받을 수 있고, McAfee 콘텐츠 저장소 전체를 검색하고 ePO 콘솔에서 '모범 사례' 및 '방법' 리소스에 액세스할 수 있습니다. 또한 상태 현황을 쉽게 평가하고 상태 현황을 개선하기 위해 수행할 권장 단계를 받아서 ePO 인프라의 상태를 관리할 수 있습니다.

개방형 플랫폼 효율성을 통해 확산 해결

ESG 연구에 따르면 조직의 40%가 10~25가지의 도구를 사용하는 반면 30%는 26~50가지의 도구를 사용하여 수십억 가지의 새로운 위협과 장치를 관리하고 있습니다. 이 제품 사용의 다양성은 복잡성을 일으키며 설치부터 보고에 이르는 통합 관리 경험의 운영 수익을 배가시킵니다. 절반 이상의 조직에서 보안 도구를 통합하면 향상률이 20%가 넘을 것으로 예상합니다(2018년 MSI 연구). McAfee에서는 더욱 폭넓은 자산을 보호하고 위협 인텔리전스를 지원하고 오픈 소스 데이터를 관리하고 타사 제품을 통합하면서 확장된 범위를 통합할 수 있는 개방형 플랫폼 접근 방식의 보안 관리를 통해 이러한 요구 사항을 수용합니다. McAfee는 광범위한 보안 제품 전반의 컴플라이언스 및 관리를 위해 중앙 집중식 제어를 제공합니다. 분석가가 제품 전체를 신속하게 피벗하여 중요한 데이터를 찾고 필요한 정책 조치를 취할 수 있습니다. 또한 McAfee ePO 콘솔을 이용하면 차세대 기술에 투자하고 이를 단일 프레임워크 내의 기존 자산과 통합할 수 있습니다.

당사의 개방형 플랫폼에서는 다양한 통합 접근 방식(오픈 소스 DXL 메시징 패브릭을 통한 최소 작업, 비API, API 및 스크립팅)을 제공하므로, 막대한 사용자 지정 작업 또는 서비스 없이 필요에 맞는 최적의 접근 방식을 선택할 수 있습니다. McAfee® Security Innovation Alliance 프로그램을 통해 상호 운용할 수 있는 보안 제품 개발을 가속하고, 복잡한 고객 환경과 이러한 제품의 통합을 간소화하고, 실제로 통합되어 연결된 보안 에코시스템을 제공하여 기존 고객 보안 투자의 가치를 최대화하도록 지원합니다. McAfee Security Innovation Alliance 프로그램에는 150개가 넘는 파트너 통합이 있습니다.

산업 분석가에 따르면 고객이 McAfee를 채택하여 계속 이용하는 이유는 McAfee ePO 소프트웨어 때문이라고 합니다.

통합 플랫폼의 이점
통합 플랫폼을 갖춘 조직은 보호 성능이 향상되며 통합 플랫폼이 없는 상대에 비해 더욱 빠른 대응 시간을 달성할 수 있습니다.

통합 플랫폼을 사용하는 조직
- 78%가 지난해 5건 미만의 위반 사례를 경험했습니다.
- 80%가 8시간 이내에 위협을 발견했습니다.

통합 플랫폼을 사용하지 않는 조직
- 55%만이 지난해 5건 미만의 위반 사례를 경험했습니다.
- 54%만이 8시간 이내에 위협을 발견했습니다.

출처: 2016 Penn Schoen Berland

또한 Data Exchange Layer (DXL) 통신 패브릭은 여러 공급업체 제품을 비롯해 내부적으로 개발된 솔루션과 오픈 소스 전반의 보안 작업을 연결하고 최적화합니다. Cisco pxGrid와 DXL을 통합하면 50개의 추가 보안 기술을 통해 모든 데이터에 액세스할 수 있습니다. McAfee ePO는 강력한 개방형 플랫폼을 관리하는 주요 구성요소입니다.

장치 보안 확장: 기본 보안 도구 관리

포괄적인 McAfee ePO 플랫폼에서는 기본 제어 기능이 포함된 장치를 비롯하여 여러 장치를 관리합니다. McAfee에서는 Microsoft Windows 10에 이미 기본 제공된 보안을 강화하고 공동 관리하여 최적화된 보호를 제공하면서, 조직이 기본 Microsoft 시스템 기능을 이용할 수 있게 합니다. McAfee ePO 소프트웨어에서는 Microsoft 운영 체제(OS) 기본 보안을 위해 특별히 조정된 고급 기계 학습을 결합하면서 추가 관리 콘솔로 인한 복잡성과 비용을 방지하는 McAfee® MVISION Endpoint를 관리합니다. McAfee ePO 소프트웨어에서는 Microsoft Windows 10 장치와 서로 다른 엔터프라이즈에 있는 모든 장치에서 공유하는 정책을 바탕으로 공통된 관리 환경을 제공하므로 간단하고, 일관되게 작업을 수행할 수 있습니다.

자동화된 워크플로를 통한 일관성

McAfee ePO 소프트웨어에서는 유연하고 자동화된 관리 기능을 제공하므로 취약점, 보안 상황에 대한 변화, 알려진 위협을 단일 콘솔에서 신속하게 식별, 관리 및 대처할 수 있습니다. 2018년에 MSI가 McAfee의 의뢰로 진행한 연구에 따르면 조직에서 반복 작업을 자동화하여 매일 약 25%의 시간을 절약할 수 있을 것으로 기대합니다. McAfee ePO 소프트웨어를 사용하면 단일 보기에서 몇 가지 전개되는 논리적 단계를 클릭하여 보안 정책을 쉽게 배포하고 시행할 수 있습니다. 단일 창 보기에서는 작업을 진행함에 따라 적절한 컨텍스트를 제공하고 각 단계와 해당 단계가 다른 단계와 연관된 방식을 보여줍니다. 따라서 복잡성이 완화되고 오류 발생 가능성이 최소화됩니다. 사용자는 환경에 대한 보안 이벤트의 유형 및 중대성, 정책 및 도구를 바탕으로 McAfee ePO 콘솔이 어떻게 경고 및 보안 대응을 지시할 것인가를 정의할 수 있습니다. 개발 작업 및 보안 작업을 지원하기 위해 McAfee ePO 플랫폼을 이용하면 보안 및 IT 운영 체제 사이에 자동화된 워크플로우를 생성하여 빠르게 문제를 개선할 수 있습니다. McAfee ePO 콘솔을 이용해 더욱 엄격한 정책을 할당하는 등 IT 운영 체제별로 해결 조치를 트리거할 수 있습니다. 웹 API(애플리케이션 프로그래밍 인터페이스)를 활용하면 수동 업무가 줄어듭니다. 오류의 위험을 줄이고 품질 제어를 보장하기 위해 신규 또는 업데이트된 정책이나 작업을 배포하기 전에 승인 프로세스를 거치도록 하는 옵션이 있습니다.

시간 절약

최신 2018년 MSI 연구에 따르면 보안 도구를 통합하는 경우 고객은 최대 20%의 시간을 절약할 수 있다고 믿습니다.

통합의 가치

- 향상된 도구와 프로세스의 효율성: 61%
- 복잡성 및 수동 작업의 감소량(보안 전문가가 깊이 있게 고려해야 하는 작업에 주력할 수 있게 함): 61%
- 패턴과 컨텍스트로 데이터를 표시함으로써 향상된 가시성: 58%
- 빠른 대응을 위해 간소화된 워크플로 비율: 57%

출처: 2018년 MSI 연구

일반적인 사용 사례

- 각 이해관계자의 요구 사항에 부합하도록 보안 컴플라이언스 보고서 일정을 지정하여 시간을 단축하고 중복 및 노동 집약적인 노력을 줄입니다.
- 강력한 API(애플리케이션 프로그래밍 인터페이스) 세트를 활용하여 McAfee ePO 콘솔을 기존 비즈니스 프로세스와 기능에 쉽게 통합할 수 있으므로 더 많은 통찰력을 확보하고 워크플로를 가속화할 수 있습니다. 예를 들어, 티켓팅 시스템, 웹 응용프로그램 또는 셀프서비스 포털과 통합합니다.
- 새로운 시스템이 기업 네트워크에 추가되면 McAfee ePO 콘솔을 Microsoft Active Directory와 동기화하여 에이전트 및 기계 학습 보안 솔루션을 배포함으로써 보안 상황을 유지하십시오.

신속한 완화 및 해결

McAfee ePO 플랫폼에는 보안 작업 담당자가 위협을 완화하거나 컴플라이언스 복원을 위해 변경을 적용할 때 그들의 효율성을 높여줄 수 있는 고급 내장 기능이 있습니다. McAfee ePO 자동 대응은 발생하는 이벤트를 기반으로 하는 조치를 트리거할 수 있습니다. 조치는 단순한 알림이거나 승인된 개선책이 될 수 있습니다.

자동 대응을 위한 일반 사용 사례

- 사전 결정된 임계치를 기준으로 이메일이나 SMS를 통해 관리자에게 새로운 위협, 실패한 업데이트 또는 우선 순위가 높은 오류를 알림
- 호스트가 손상되었거나(명령 및 제어 활동 거부) 데이터 추출/송신 전송을 차단하는 경우 관리자가 정책을 재설정할 때까지 외부 통신을 방지하기 위한 정책과 같은 클라이언트 또는 위협 이벤트를 기반으로 하는 정책을 적용
- 위협이 감지되면 시스템에 태그를 지정하고 주문형 메모리 스캔 등의 개선을 위해 추가 작업을 실행함
- 서비스 데스크에서 티켓을 생성하거나 다른 비즈니스 프로세스에 통합하는 등의 외부 스크립트와 서버 명령을 실행하기 위해 등록된 실행 파일을 트리거
- 제약이 더 많은 정책으로 워크로드나 컨테이너(모든 장치)를 자동 격리

클라우드 기반 보안 관리

조직에서는 진화된 위협 솔루션의 배포를 간소화하고 가속화해야 합니다. 많은 조직에서 사내 인프라의 비용과 유지 관리를 제거하여 클라우드 기반 보안 관리의 효율성을 확인하고 있습니다. McAfee ePO 소프트웨어는 다음과 같은 두 개의 대체 배포 옵션을 통해 언제 어디서나 클라우드에서 구현할 수 있습니다. AWS (Amazon Web Services)의 McAfee ePO 소프트웨어 또는 McAfee MVISION ePO. 이 두 옵션 모두 1시간 이내에 가동하여 실행할 수 있습니다.

"McAfee ePO는 통합 보안 자동화 및 조정의 원조 기업 중 하나입니다. ...오늘날의 보안 전문가들은 기존 ePO의 힘이 필요하지만, 간소화된 경험으로 제공됨으로써 자신들의 작업을 효율적이고 효과적으로 만들어줄 것을 요구하고 있습니다... SaaS 제공 작업 공간으로서, MVISION은 대기업과 중견 기업이 전용할 수 있는 방식으로 분석, 정책 관리와 이벤트를 결합합니다."

—Frank Dickinson, Research Vice President, Security Products, IDC

- AWS의 McAfee ePO를 사용하면 조직에서 자동 확장 및 Amazon RDS와 같은 여러 기본 AWS 서비스를 활용할 수 있으므로, 개별 데이터베이스를 구매하고 관리할 필요가 없어집니다. 따라서 관리자가 인프라가 아니라 중요한 보안 작업에 주력할 수 있습니다. AWS의 McAfee ePO 소프트웨어에서는 McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, Data Exchange Layer 및 McAfee ePO 소프트웨어에 통합된 타사 솔루션을 관리합니다.
- McAfee® MVISION ePO는 SaaS (Software-as-a-Service) 오퍼링인 McAfee ePO의 이점을 기반으로 구축됩니다. 플랫폼 관리가 대폭 간소화되므로, 중요한 보안 작업에 주력할 수 있습니다. 연속 공급 모델을 통해 투명하게 플랫폼을 업데이트합니다. 에이전트가 배포되고 나면 장치 보안이 엔터프라이즈 전체에 자동으로 배포되므로, 각 장치의 보안을 직접 설치하거나 업데이트할 필요가 없어지고 위협에 더 강력하게 대응할 수 있습니다. 따라서 엔터프라이즈에서는 어디서든 단일 콘솔을 통해 McAfee MVISION Endpoint와 Data Exchange Layer를 관리할 수 있습니다. McAfee MVISION ePO를 사용하면 장치에서 SIEM (보안 정보 및 이벤트 관리) 솔루션에 중요한 통찰력을 제공하므로 분석가가 적절한 데이터를 즉시 이용하여 위협에 더욱 확실하게 대응하고 해결할 수 있습니다.

McAfee ePO에서 관리하는 McAfee 제품

McAfee 제품*
McAfee® Endpoint Protection (위협 방지,방화벽,웹 컨트롤)
McAfee MVISION Endpoint에서 첨단 위협 보호로 Windows Defender 보완
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention(McAfee DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**사내 McAfee ePO용*

유연한 배포

배포	주요 이점
사내 McAfee ePO	완벽한 데이터 및 기능 세트 제어
AWS의 McAfee ePO	사내 솔루션에 필요한 하드웨어 유지 관리의 필요성 제거
McAfee MVISION ePO ePO SaaS (Software-as-a-Service)*	인프라의 유지 관리와 업그레이드 필요성을 모두 제거하는 다중 테넌트 SaaS 오퍼링

**일부 ePO 기능은 McAfee MVISION ePO에서 사용할 수 없음*

"McAfee ePO 소프트웨어는 다른 솔루션에 비해 남다른 점이 있습니다. 엔드포인트 보호를 위한 원스톱 매장입니다. 단일 창에서 모든 McAfee 제품에 대해 확인해야 할 모든 것을 볼 수 있습니다. 사용이 용이한 대시보드와 내장 기능은 가시성, 보고, 배포, 업데이트, 유지 관리, 의사 결정을 비롯한 모든 것이 훨씬 더 쉬워지도록 지원합니다."

—Christopher Sacharok, Computer Sciences Corporation의 정보 보안 엔지니어

사용 사례: McAfee ePO 콘솔을 통해 중앙 집중식으로 보안을 관리하는 방법

제품 및 기술	사용 사례	이점
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO 소프트웨어는 고급 보호로 Microsoft Windows 10 기본 제어 기능을 강화하는 McAfee MVISION Endpoint를 관리합니다. Microsoft Windows와 McAfee Endpoint Security에 공통인 관리 플랫폼과 일관된 정책으로 진화된 위협을 쉽게 발견하고 관리할 수 있습니다.	Microsoft Windows용 기본 제어 기능의 보호를 강화하고 입증된 관리의 효율성을 향상합니다.
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security는 엔드포인트에서 알려진 악성 파일을 찾습니다. McAfee ePO 콘솔은 격리할 수 있도록 엔드포인트에 대해 더 엄격한 정책을 설정합니다. 이 작업은 하나의 일반 관리 인터페이스로 수행됩니다.	감염된 엔드포인트를 빠르게 격리
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager는 엔드포인트에서 중요한 데이터 반출을 감지하고 McAfee ePO 콘솔에서 태그를 지정합니다. McAfee ePO 콘솔은 데이터를 차단하고 컴플라이언스에 위배되는 사항을 사용자에게 조언할 수 있도록 데이터 손실 방지 정책을 적용합니다.	자동 데이터 손실 방지 정책 시행

통합 예시

제품 및 기술	통합 사용 사례	이점
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine(ISE) Cisco PxGrid	McAfee Endpoint Security는 의심스러운 호스트에 플래그를 지정합니다. McAfee ePO 콘솔은 추가적인 스캔을 트리거할 수 있습니다. PxGrid 및 DXL 교환(McAfee ePO 콘솔)을 통해 Cisco ISE에 전달됩니다. Cisco ISE는 수용 가능하다고 여겨질 때까지 호스트를 격리할 수 있습니다.	사전 예방적 보호가 증가됨
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO에서는 Nexpose와 자산 목록을 공유합니다. 이를 통해 사용자는 McAfee ePO 콘솔에서 위험 상황에 대해 이해할 수 있습니다. 취약점 데이터는 공급업체의 DXL 커뮤니티에서 공유됩니다.	▪ 복잡성 감소 ▪ 단일 대시보드에서 위험을 최소화할 수 있도록 포괄적이고 신뢰할 수 있는 상황을 마련하고 조치의 우선 순위를 설정함
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	이 통합으로 인해 네트워크 및 엔드포인트 사이에서의 양방향 및 실시간 인텔리전스 공유가 용이해졌습니다. 이벤트도 DXL 커뮤니티를 통해 공유됩니다. Check Point Anti-Bot 소프트웨어 블레이드에서는 명령 및 제어(C&C) 트래픽을 차단하고 공통 DXL 토픽을 통해 기타 통합된 타사 보안뿐만 아니라 McAfee ePO 소프트웨어에 알립니다. 이 인텔리전스를 통해 McAfee에서는 엔드포인트 장치에 적합한 해결 워크플로를 자동으로 시작합니다. Check Point와 McAfee에서는 또한 공격 시작 위치가 네트워크인지 아니면 엔드포인트인지에 상관없이 제로 데이 공격을 감지 및 방지하며 해당 공격을 알려진 공격으로 변환할 수 있습니다. 기업의 핵심 인텔리전스를 실시간으로 교환하므로 통합을 통해 각 제품에서 자동으로 위협을 감지, 차단 및 개선할 수 있습니다.	▪ 감지 시간 단축 ▪ 공격 차단 및 개선

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