McAfee ePolicy Orchestrator

보안 인사이트를 중앙에서 확보, 가시화, 공유하여 이를 바탕으로 조치를 취할 수 있습니다.

보안 관리에는 도구와 데이터 사이를 번거롭게 오가는 과정이 필요합니다. 이러한 과정에서 도구 사이의 보이지 않는 틈이 악용되고 손상을 입는 동안 더 많은 시간이 소요되어 적이 더 유리한 위치를 차지하게 됩니다. 또한 사이버 보안 인력은 제한되어 있으며 사이버 보안 복잡성을 관리할 수 있도록 권한이 부여되어야 합니다. McAfee® ePolicy Orchestrator®(McAfee ePO™) 관리 플랫폼은 시간이 오래 소요되는 잠재적 인적 오류 개선 노력을 없애고 더욱 향상된 효율성으로 보안을 관리할 책임이 있는 사람들의 의욕을 고취시킵니다.

기본 보안

기본에서 시작합시다. 모든 보안 아키텍처의 핵심은 엔드포인트 및 시스템의 상태를 모니터링하고 제어할 수 있는 기능입니다. **CIS**(Center for Internet Security) 제어 및 **NIST**(National Institute of Standards Technology) **SP 800-53** 보안 및 개인정보 제어 등의 산업 표준은 이를 필수 사항으로 요구합니다. McAfee ePO 콘솔을 이용하면 중대한 가시성을 얻을 수 있으며 엔터프라이즈 전반에서 양호한 보안 태세를 갖출 수 있도록 정책을 설정하고 자동으로 시행할 수 있습니다. 전체 엔터프라이즈를 위한 보안 제품 전반의 정책 관리 및 시행이 단일 콘솔에서 이루어지므로 여러 제품을 관리하는 데 따르는 복잡성이 제거됩니다. 이 필수적인 보안은 IT 보안 컴플라이언스의 기본입니다.

입증된 고급 보안 관리

3만 곳 이상의 비즈니스와 조직에서 보안을 관리하고 컴플라이언스 프로세스를 간소화 및 자동화하며 엔드포인트, 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 단일 콘솔에서 수십만의 노드를 관리할 수 있도록 지원합니다. McAfee ePO 콘솔은 엔터프라이즈 보안 관리자에게 정책 유지 관리를 단순화하고 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 정밀한 응답을 가능하게 합니다.

McAfee에 문의

무질서를 이기는 효율성

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 야기하며 설치부터 보고에 이르는 통합 관리 경험의 운영 수익을 배가시킵니다. McAfee는 더욱 폭넓은 자산을 보호하고 위협 인텔리전스를 지원하고 오픈소스 데이터를 관리하고 타사 제품을 통합하면서 확장된 범위를 통합할 수 있는, "함께하는 것이 힘"(Together is power)이라는 보안 관리에 대한 접근 방식으로 이러한 요구 사항을 수용합니다. McAfee는 광범위한 보안 제품 전반의 컴플라이언스 및 관리를 위해 중앙 집중식 명령과 제어를 제공합니다. 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.

McAfee ePO로 관리되는 제품 샘플 목록

McAfee 제품	타사 제품
McAfee Endpoint Protection(위협 방지,방화벽,웹 컨트롤)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments(McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention(McAfee DLP)	DXL
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	

사용 사례 예: McAfee ePO 콘솔이 보안 제품의 중앙 집중식 관리를 생성하는 방법

제품 및 기술	샘플 중앙 집중식 관리 사용 사례	이점
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 단일한 일반 관리 인터페이스에서 수행됩니다.	불량한 엔드포인트의 빠른 격리
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	McAfee Enterprise Security Manager는 엔드포인트에서 중요한 데이터 반출을 감지하고 McAfee ePO 콘솔에서 태그를 지정할 수 있습니다. 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. 이것은 PxGrid 및 DXL 교환(McAfee ePO 콘솔)을 통해 Cisco ISE에 전달됩니다. Cisco ISE는 수용 가능하다고 여겨질 때까지 호스트를 격리시킬 수 있습니다.	사전 예방적 보호가 증가됨
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	McAfee ePO에서 제공하는 업계 최고의 권한 관리 솔루션인 Avecto Defendpoint를 배포 및 관리합니다. Avecto Defendpoint 구성 변경은 McAfee Threat Intelligence Exchange 애플리케이션 평판 데이터에 의해 알려집니다.	복잡성 감소 추가 인프라 없음, TCO 낮춤 위협 인텔리전스를 기반으로 변경되는 액세스 권한
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO는 Nexpose에 자산 목록을 공유합니다. 이를 통해 사용자는 McAfee ePO 콘솔에서 위험 태세에 대한 이해를 확보할 수 있습니다. 취약점 데이터는 공급업체의 DXL 커뮤니티에서 공유됩니다.	복잡성 감소 단일 대시보드에서 위험을 최소화할 수 있도록 포괄적이고 신뢰할 수 있는 태세를 갖추고 조치의 우선 순위를 설정합니다.
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. 이벤트는 DXL 커뮤니티를 통해 공유됩니다.	감지 시간 단축 공격 차단 및 개선

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

	통합된 조직	통합되지 않은 조직
지난해 5건 미만의 위반 사례를 경험	78%	55%
8시간 이내에 위협을 발견	80%	54%

2016 Penn Schoen Berland

프로세스를 간소화하는 확장 가능한 워크플로우

McAfee ePO 데이터베이스는 유연하고 자동화된 관리 기능을 제공하므로 취약점, 보안 태세에 대한 변화, 알려진 위협을 단일 콘솔에서 신속하게 식별, 관리 및 대처할 수 있습니다. 사용자는 환경에 대한 보안 이벤트의 유형 및 중대성, 정책 및 도구를 바탕으로 McAfee ePO 콘솔이 어떻게 경고 및 보안 응답을 전달할 것인가를 정의합니다. 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 애플리케이션 프로그래밍 인터페이스(API)를 활용하면 수동 노력이 줄어듭니다.

일반적인 사용 사례

- 각 이해관계자의 요구 사항에 부합하도록 보안 컴플라이언스 보고서 일정을 지정하여 시간을 단축하고 중복 및 노동 집약적인 노력을 줄이십시오.
- 더 향상된 인사이트를 확보하고 워크플로우(예: 발권 시스템, 웹 애플리케이션 또는 셀프 서비스 포털과의 통합)를 가속화할 수 있도록 견고한 API 세트를 활용해 McAfee ePO 콘솔을 기존 비즈니스 프로세스 및 부서에 간편하게 통합하십시오.
- 새로운 기계가 기업 네트워크에 추가되면 McAfee ePO 콘솔을 Active Directory와 동기화하여 에이전트 및 보안 솔루션을 배포함으로써 보안 태세를 유지하십시오.

"현재 시장에서 가장 강력한 엔드포인트 관리 플랫폼인 McAfee ePolicy Orchestrator는 기업의 모든 보안 제품을 위한 기본 관리 도구이며 엔터프라이즈 구매자가 원하는 강력한 성능과 유연성을 제공합니다. 보안 기능은 폭넓으며 공통 정책 엔진과 인텔리전스 스트림을 통해 긴밀하게 통합됩니다."

—Forrester Wave: Endpoint Security Suites(엔드포인트 보안 제품군) 2016

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 응답은 발생하는 이벤트를 기반으로 하는 조치를 트리거할 수 있습니다. 조치는 단순한 알림이거나 승인된 개선책이 될 수 있습니다.

자동 응답을 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 가능) 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
- 더욱 엄격한 정책으로 엔드포인트를 자동으로 격리

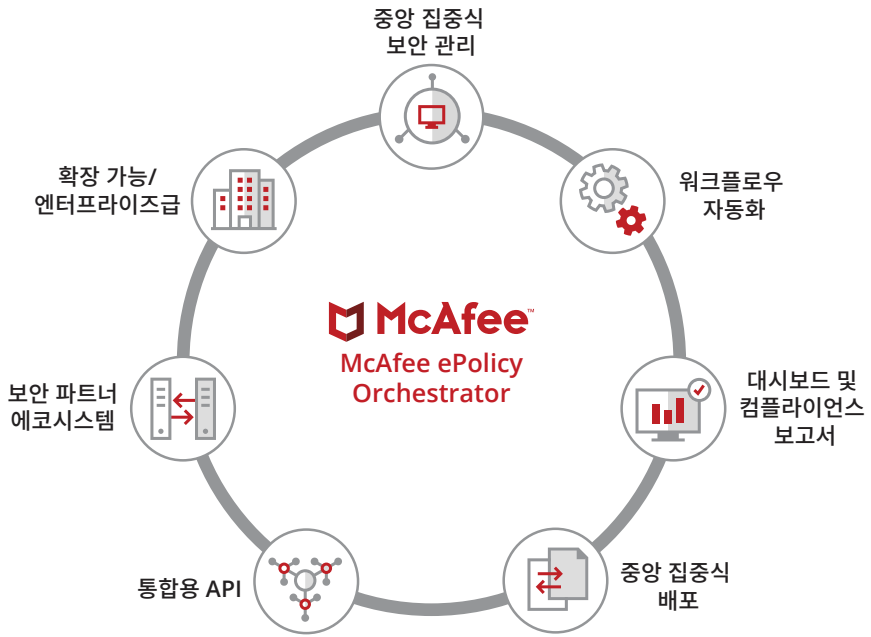

그림 1. McAfee ePO 콘솔을 이용한 중앙 집중식 보안 관리

McAfee ePO 콘솔을 이용해 조직 전반을 보호

중앙에서 보안 관리

- 엔터프라이즈 전반의 최대 수십만에 이르는 노드에 대한 가시성 확보와 중앙 집중식 관리를 위한 차별화된 단일 콘솔
- McAfee 및 타사 솔루션을 통한 폭넓은 시스템 보안 관리를 위한 개방형 프레임워크
- 운영상의 마찰을 줄이기 위해 기존 IT 인프라에 통합되며 이를 활용하는 확장형 플랫폼

확신을 갖고 응답 시간 가속화

- 내부 및 외부 보안 문제를 예방적으로 처리하기 위한 포괄적 보기 및 인사이트
- 엔드포인트가 최신 위협으로부터 보호되도록 보장할 수 있게 보안 업데이트 및 정의를 신속하게 중앙 집중식으로 배포
- 실행 가능한 대시보드 및 고급 쿼리 및 보고 기능을 통해 응답 시간을 가속화

복잡성 최소화 및 프로세스 합리화

- 안내식 구성, 자동화된 정책 관리 작업 스트림, 사전 정의된 대시보드로 신속하게 시작 및 실행할 수 있는 기능
- 태그 기반 정책 과제가 사전 정의된 보안 프로파일을 비즈니스 역할 또는 위험 상태에 따라 개별 시스템 또는 시스템 그룹에 정확히 적용하도록 할당
- 작업 카탈로그 및 자동화된 관리 기능으로 관리 프로세스 합리화 및 오버헤드 최소화
- 여러 엔드포인트 제품을 관리할 수 있는 단일 에이전트는 엔드포인트 충돌 위험성을 낮춤

기업 배포에 적합한 확장성

- 엔터프라이즈급 아키텍처를 통해 하나의 서버에서 수십만 대의 장치를 관리할 수 있도록 지원
- 복잡한 이질적 IT 환경에서 지원 및 입증됨
- 보안 태세 및 컴플라이언스에 대한 포괄적인 보기를 취합하는 엔터프라이즈 보고

"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

McAfee Together is power.

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