

# McAfee MVISION ePO

## 단일 지점을 통해 어디서나 확인 및 제어

보안 관리는 복잡합니다. 도구와 데이터 간에 번거로운 이동이 필요합니다. 또한 사이버 보안 전문가는 보안 인프라를 관리하고 업데이트하는 데 많은 시간을 소모해서는 안 됩니다. 대신 감지 및 시행과 같은 중요한 보안 작업에 주력해야 합니다. 그러지 않으면 이처럼 중요한 작업을 수행하지 못하는 틈을 이용하여 적대 세력이 엄청난 손해를 유발할 수 있습니다. McAfee® MVISION ePolicy Orchestrator® (McAfee MVISION ePO™)를 사용하면 사내 보안 인프라를 유지 관리할 필요가 없으므로, 보안 전문가가 보안에 전념할 수 있습니다. 자격 증명을 사용하여 브라우저에서 간단하게 액세스하고 보안을 관리합니다.

사이버 보안 전문가 풀은 매우 희박하므로 현재 직원이 사이버 보안의 통합을 간소화하는 역할을 갖추어야 합니다. 그뿐만 아니라 모든 유형의 장치에서 신속하게 위협에 대응하여 손상을 최소화해야 합니다. 위협에 신속하게 대응하려면 조직의 보안 상황을 확실하게 파악하고 있어야 하며, 이는 위협 관리에 있어 가장 중요한 요소입니다. McAfee MVISION ePO는 당사의 입증된 고유 보안 관리 플랫폼인 McAfee ePO 소프트웨어의 글로벌 멀티 테넌트 엔터프라이즈 SaaS (Security-as-a-Service) 버전입니다.

McAfee MVISION ePO를 사용하면 시간이 많이 소요되는 사내 보안 관리 인프라를 유지 관리할 필요가 없어집니다. 따라서 오류 발생 가능성을 줄이고 보안 팀이 어디서나 더 효율적으로

보안을 관리하여 효과를 높일 수 있습니다. McAfee MVISION ePO에는 McAfee® MVISION Endpoint 기술을 활용하여 Microsoft Windows 운영 체제에 제공되는 기본 제어를 관리하는 기능도 포함되어 있습니다.

### 필수 보안 관리를 간편하게 수행

장치와 데이터를 모니터링 및 제어하는 기능은 모든 보안 접근 방식의 핵심이며 IT 보안 컴플라이언스의 기본입니다. [CIS](#) (Center for Internet Security) Controls and Benchmarks 및 [NIST \(National Institute of Standards Technology\) SP 800-53](#) 보안 및 개인 정보 제어와 같은 업계 표준에서는 사이버 보안 및 인프라의 모니터링 및 제어를 해야 강력한 보안의 요구사항으로 삼고 있습니다.

### 주요 이점

- 업계에서 인정받는 중앙 집중식 관리
- 사내 보안 플랫폼을 유지 관리하는 데 따르는 복잡성 제거
- Windows Defender와 같은 운영 체제의 기본 제어 기능과 McAfee 제품을 관리하는 포괄적인 플랫폼
- 효율적인 관리 업무를 위해 자동화된 워크플로
- 간소화된 사고 조사 및 교정
- 시장 점유율이 가장 높은 장치의 보안을 공통으로 관리
- 장치부터 클라우드에 이르는 수천 개의 장치로 보안 확장

McAfee에 문의



## 데이터시트

McAfee MVISION ePO 콘솔을 이용하면 중대한 가시성을 얻을 수 있으며 엔터프라이즈 전반에서 양호한 보안 태세를 갖출 수 있도록 어디서든 정책을 설정하고 자동으로 시행할 수 있습니다. 이제 엔터프라이즈 전체에서 정책을 관리하고 시행하기 위해 통합된 단일 패널을 통해, 여러 제품을 통합하는 데 따르는 복잡함을 줄일 수 있습니다.

위험을 더 효율적으로 관리하기 위해 보호 작업 공간에서는 위험의 우선순위를 지정하고 하나의 그래픽 보기에서 전체 디지털 영역의 보안 상태에 대한 요약を提供합니다. 관리자가 특정 이벤트를 드릴다운하여 더 많은 통찰력을 얻을 수 있습니다. 이 요약 보기를 사용하면 보고서를 작성하고, 데이터를 즉시 합리적으로 분석하는 데 필요한 시간을 줄이고,

산업 분석가에 따르면 많은 조직에서 McAfee 솔루션을 구매하고 계속 이용하는 이유가 McAfee ePO 소프트웨어 때문이라고 합니다.

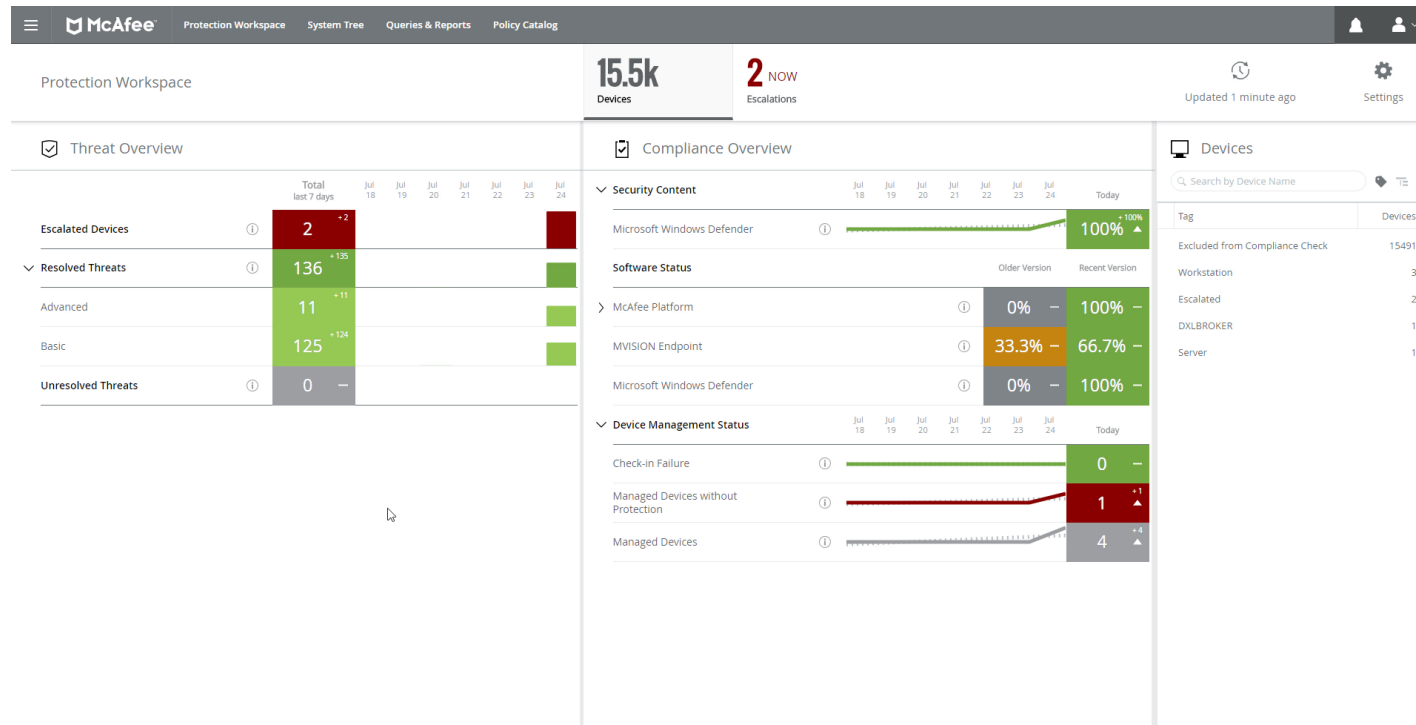


그림 1. McAfee ePO 보호 작업 공간.

## 데이터시트

수동 개입이 필요한 경우 발생할 수 있는 오류를 제거할 수 있습니다. 추가적으로, 보안 리소스 페이지에서 최신 위협 정보 및 리서치를 간편하게 찾을 수 있습니다. SaaS 오퍼링인 McAfee MVISION ePO를 사용하면 보안 인프라의 설정과 유지 관리를 할 필요가 없으므로 모든 장치의 모니터링과 제어에만 주력할 수 있습니다. 플랫폼 업데이트는 연속적으로 투명하게 수행됩니다. 장치 보안이 엔터프라이즈 전체에 자동으로 배포되므로, 각 장치의 보안을 직접 설치하거나 업데이트하는 작업이 없어지고 위협에 더 강력하게 대응할 수 있습니다. McAfee MVISION ePO는 보안을 관리하고, 컴플라이언스 프로세스를 간소화 및 자동화하고, 엔터프라이즈에 있는 모든 장치의 가시성을 높이려는 36,000곳 이상의 McAfee ePO 소프트웨어 고객을 통해 입증된 실적을 기반으로 구축되었습니다.

### 위협 분석 강화

McAfee MVISION ePO는 효율성과 효과를 높이기 위해 보안 관리를 통합하도록 설계되었습니다. McAfee MVISION ePO는 위협 관리와 사건 분석을 하나로 통합합니다. 따라서 장치에서 SIEM(보안 정보 및 이벤트 관리) 솔루션에 중요한 통찰력을 제공하므로, 분석가가 중요한 정보를 즉시 이용하여 위협에 더욱 확실하게 대응하고 정정할 수 있습니다.

### 광범위한 장치 보안: 기본 보안 도구 관리

McAfee MVISION ePO의 포괄적인 플랫폼은 기본 제어 기능이 포함된 장치를 비롯하여 다양한 장치를 관리합니다. McAfee에서는 Microsoft Windows 10에 이미 기본 제공된 보안을 강화하고 공동 관리하여 최적화된 보호를 제공합니다. 따라서 조직이 기본 Microsoft 시스템 기능을 이용할 수 있습니다. McAfee MVISION ePO는 Microsoft OS 기본

보안에 맞게 특별히 조정된 고급 기계 학습 기능을 결합하는 McAfee MVISION Endpoint를 관리합니다. 또한 추가 관리 콘솔을 설치하는 데 따르는 복잡성과 비용도 방지합니다. McAfee MVISION ePO는 Microsoft Windows 10 장치와 서로 다른 엔터프라이즈에 있는 모든 장치에서 공유하는 정책을 바탕으로 공통된 관리 환경을 제공하므로 단순함과 일관성을 유지할 수 있습니다.

### 자동화된 워크플로로 안정성 확보 및 시간 절약

2018년에 MSI가 McAfee의 의뢰로 진행한 연구에 따르면, 조직에서 반복 작업을 자동화하여 매일 약 25%의 시간을 절약할 수 있을 것을 기대합니다. McAfee MVISION ePO에서는 민첩하고 자동화된 관리 기능을 제공하므로 취약점, 보안 태세에 대한 변화, 알려진 위협을 모두 단일 콘솔에서 신속하게 식별, 관리 및 대처할 수 있습니다. 이 단일 보기에서 몇 가지 단계만 순차적으로 클릭하면 보안 정책을 간단하게 배포하고 시행할 수 있습니다.

관리자가 작업을 수행하면서 각 단계를 보고 다른 단계와 어떻게 연결되었는지를 확인하여 복잡성과 오류 발생 가능성을 없앴으므로 적절한 컨텍스트를 이용할 수 있게 합니다. 오류의 위험을 줄이고 품질 제어를 보장하기 위해 신규 또는 업데이트된 정책이나 작업을 배포하기 전에 승인 프로세스를 거치도록 하는 옵션이 있습니다.

컨텍스트 라우팅에서는 환경에 대한 보안 이벤트의 유형 및 중대성, 정책 및 도구를 바탕으로 경고 및 보안 대응을 지시합니다. McAfee MVISION ePO 플랫폼을 이용하면 보안 및 IT 운영 체제 사이에 자동화된 워크플로우를 생성하여 빠르게 문제를 개선할 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

---

### 일반적인 사용 사례

- 기본 제어 기능이 있는 장치를 비롯한 모든 장치에 정책을 배포하여 일관성을 유지하고 시간을 절약하십시오.
- 각 이해관계자의 요구 사항에 부합하도록 보안 컴플라이언스 보고서 일정을 지정하여 시간을 단축하고 중복 및 노동 집약적인 노력을 줄이십시오.
- 새로운 장치가 기업 네트워크에 추가되면 McAfee MVISION ePO 콘솔을 Microsoft Active Directory와 동기화하여 에이전트 또는 기계 학습 보안 솔루션을 배포함으로써 보안 태세를 유지하십시오.

### 신속한 완화 및 해결

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

### 자동 대응을 위한 일반 사용 사례

- 사전 결정된 임계치를 기준으로 이메일을 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
- 제약이 더 많은 정책으로 워크로드나 컨테이너(모든 장치)를 자동 격리
- 시스템에 태그가 지정되면 보호 작업 공간 대시보드에 에스컬레이션 상태가 자동으로 표시됩니다.

### 주요 기능

- 그래픽 보안 상황 대시보드
- 역할 기반 액세스 제어
- 이중 인증
- 사용자 정의 보고서 및 쿼리
- 가동 중지 시간 없는 업그레이드
- McAfee® Endpoint Security 및 McAfee® VirusScan® Enterprise용 마이그레이션 지원 도구

McAfee 기술의 특징과 이점은 시스템 구성에 따라 다르며 사용하는 하드웨어, 소프트웨어 또는 서비스 활성화를 필요로 할 수 있습니다. 완벽히 안전한 컴퓨터 시스템은 없습니다.

McAfee는 이 문서에 언급된 웹 사이트 또는 타사 벤치마크 데이터를 관리하거나 감사하지 않습니다. 언급된 웹 사이트를 방문하여 언급된 데이터가 정확한지 확인해야 합니다.

McAfee 및 McAfee 로고, ePolicy Orchestrator, McAfee ePO 및 VirusScan은 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2018 McAfee, LLC. 4186\_1118 2018년 11월



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