McAfee MVISION Endpoint

Windows 데스크톱 및 서버를 위한 고급 엔드포인트 보안

모든 기능을 갖춘 EPP(엔드포인트 보안 플랫폼)보다 더욱 간편하고 저렴한 대안을 원하는 고객은 Microsoft Windows Defender와 같은 기본 보안을 수용합니다. Windows Defender는 기본적인 수준의 필수 보호를 제공하지만, 정교한 파일리스 위협 및 제로 데이 맬웨어 기반 위협에 대항할 완벽한 방어 태세를 갖추려면 기계 학습과 같은 첨단 대응 조치를 적용해야 합니다. 성공의 비결은 복잡하게 여러 콘솔을 도입하지 않고 Windows 데스크톱 및 서버 환경[1]에 이미 기본 제공되는 보안을 활용, 강화 및 관리하는 것입니다. McAfee® MVISION Insights[2]는 사전 엔드포인트 보안 분석을 제공하며 공격을 받기 전에 조치하여 보안 상황을 한층 개선합니다.

보안 또는 복잡성?

이러한 도구는 대개 별도로 관리되므로 보안 팀은 강력한 방어 기능을 얻는 대신 복잡함이 가중되는 딜레마에 직면하게 됩니다. 일반적으로 이는 재정 및 운영 비용을 절감하지 못하게 된다는 의미입니다.

더 나은 옵션: 고급 방어 및 통합 관리

McAfee® MVISION Endpoint를 사용하면 효과와 효율성을 모두 달성함으로써 양자택일의 딜레마에서 벗어날 수 있습니다. 파일, 파일리스, 행동 기반 기계 학습 분석을 바탕으로 사용하는 환경의 모든 엔드포인트에서 고급 위협 감지와 중앙 집중식 관리를 실현할 수 있습니다. Windows Defender 안티바이러스, Defender Exploit Guard, Windows 방화벽, McAfee 방어 및 Mac 또는 Linux 시스템의 정책을 중앙 콘솔에서 일관되게 관리하므로 워크플로가 복잡해지는 것을 방지할 수 있습니다. 공동 관리 및 통합된 정책을 통해 중복되는 진입 시간을 없앨 뿐만 아니라 엔드포인트 환경에 대한 가시성도 향상합니다.

방어와 보안을 극대화

MVISION Endpoint는 향상된 감지 및 정정 기능을 제공하여 기본 제어 기능을 강화하고 항상 최신 상태로 유지해 줍니다. 기계 학습, 자격 증명 도난 모니터링 및 롤백 교정을 통해 Windows 데스크톱 및 서버 OS(운영 체제)에 제공되는 기본 보안을 크게 강화하고 진화된 제로 데이 위협을 효과적으로 차단합니다. 이 접근 방식을 사용하면 기본 기술과 타사 기술의 장점만 조합하여 사용할 수 있으므로 둘 중 하나에만 투자해야 하는 곤란한 문제를 피할 수 있습니다. 우선순위가 높은 잠재적인 위협이 공격하기 전에 대응하기 위해 보안 상황을 업데이트하여 보호 역량을 강화합니다.

주요 이점

- **진화된 위협에 대비한 고급 방어:** 기계 학습, 자격 증명 도난 방어 및 롤백 교정을 통해 Windows 데스크톱 및 서버 기본 보안 기능을 보완합니다.
- **추가 복잡성이 없음:** 단일 정책 및 콘솔을 사용하여 McAfee 기술, Windows Defender 바이러스 백신 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.

McAfee에 문의

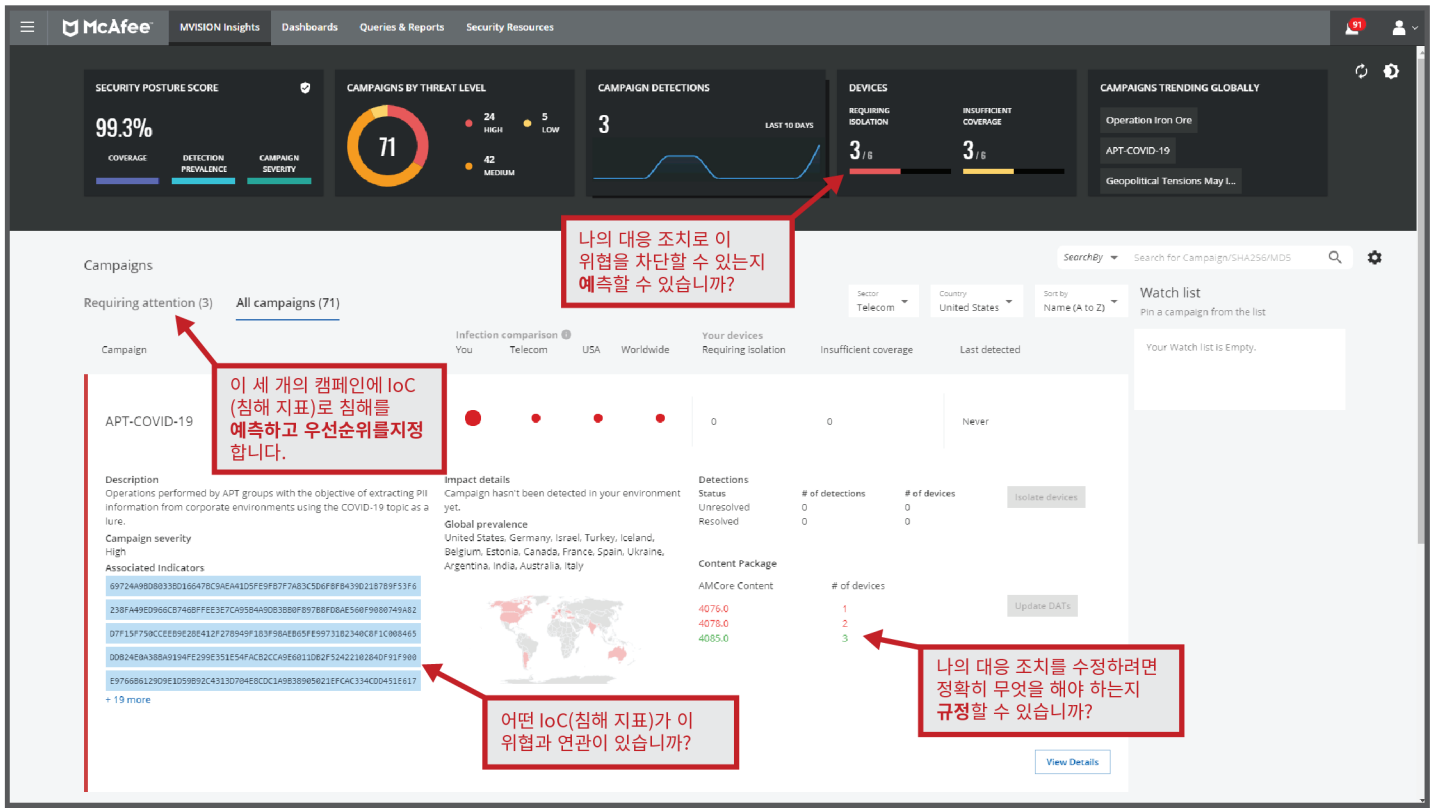

그림 1. MVISION Insights는 핵심적인 질문에 답변을 제공하는 통합 대시보드로 사전 사이버 보안을 제공합니다.

복구 시간

McAfee 기계 학습 기술은 경쟁 솔루션보다 오탐지 수가 적으며 시그니처 기반 방어보다 감지율이 훨씬 높습니다. 따라서 관리자가 악의적이지 않은 위협에 시간을 쓰는 대신 환경에 대한 실제 위협에 계속 집중할 수 있습니다.

MVISION Endpoint는 의심스러운 프로세스의 영향을 받은 파일을 모니터링하여 원래 버전으로 복원하고 침투했을 수 있는 다른 악의적인 파일이나 프로세스도 제거할 수 있습니다. 사용자는 교정 및 복구로 인한 가동 중지 시간을 처리하지 않고 생산성을 유지할 수 있습니다. 관리자는 손상된 엔드포인트를 이미지로 다시 설치하거나 복구하는 데 소요되는 시간을 줄이고 조직의 생산성을 높이는 데 시간을 더 많이 할애할 수 있습니다.

통합 방어로 Windows 10, Windows Server 2016 및 Windows Server 2019 시스템의 기본 보안을 활용, 강화 및 관리

신속하게 시작

- 조직에 문제가 되는 위협을 즉시 확인하고 대응합니다.
- 기본 제공 정책을 Windows Defender 바이러스 백신 에 적용하고 Defender Exploit Guard 관리를 가장 중요한 규칙으로 간소화하고 모범 사례 규칙 설정을 Windows 방화벽에 적용합니다.
- 기존 McAfee 관리를 사용하거나 SaaS 기반 콘솔을 사용하여 신속하게 배포합니다.
- Story Graph 기능을 사용하여 위협 및 위협에 대해 수행된 작업을 빠르게 시각화하고, 추후 공격에 대비하는 엔드포인트 추가 강화 방법을 결정하십시오.
- 클라이언트 크기가 작으므로 다운로드 크기가 작고 빠릅니다.

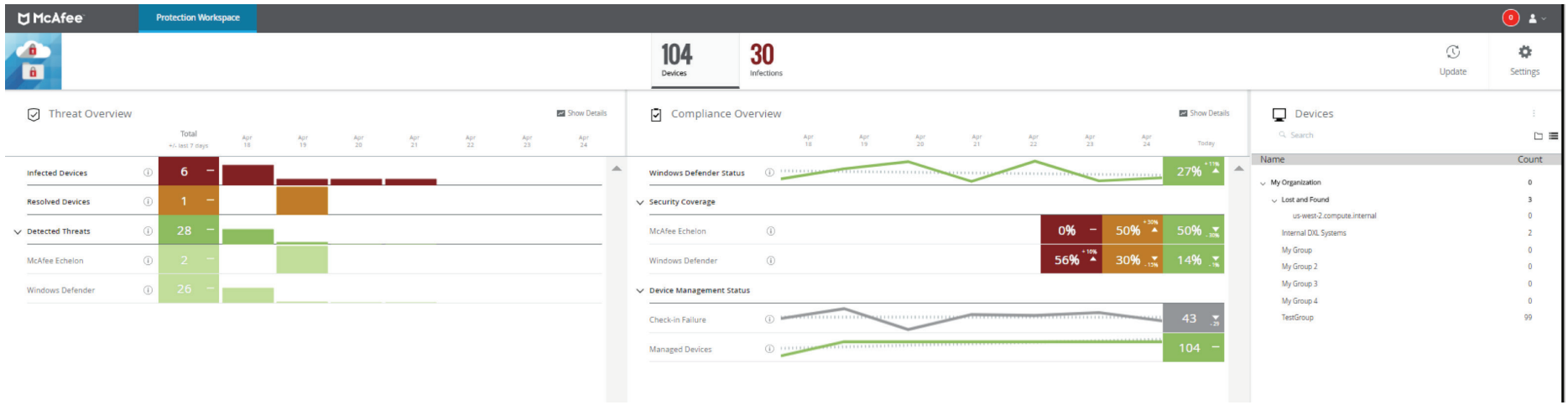

그림 2. 위협 보호 작업 공간을 사용하면 McAfee와 Microsoft 기술 전체에 대한 위협과 컴플라이언스를 볼 수 있습니다.

가시성 향상

MVISION Endpoint는 BitLocker에 대한 보고를 포함하여 사용자 환경에 대한 위협과 컴플라이언스를 파악할 수 있는 단일 패널을 사용하여 관리됩니다. 어떤 위협 이벤트가 어디서 어떻게 발생했는지 파악하기 위해 한 콘솔에서 다른 콘솔로 전환하는 대신 사용하기 쉬운 대시보드와 구성 가능한 경보를 통해 가장 중요한 데이터로 안내합니다.

Story Graph 기능은 조사를 간소화하고 관리자가 공격에 대비하여 엔드포인트를 강화할 수 있도록 돕는 추가 도구입니다. 이 기능은 위협 이벤트 탐지로 이어진 작업에 관한 추적 정보를 제공하고, 사용자의 해당 작업 검토 및 위협 원인 파악을 돕습니다.

관리 유연성

MVISION Endpoint에서는 다음을 선택할 수 있습니다.

- **순수한 SaaS 관리:** 멀티 테넌트, 전체적으로 확장 가능, McAfee에서 유지
  - **이점**: 언제 어디서나 관리 콘솔에 액세스할 수 있고, 자동으로 업데이트되고, 유지 관리하므로 TCO(총 소유 비용)를 낮출 수 있습니다.
- **가상 배포:** AWS(Amazon Web Services) 환경에 배포된 관리를 통해 1시간 이내에 완전히 가동 가능합니다.
  - **이점**: 가상화된 환경에서 기존 투자를 활용하여 배포 및 유지 관리 비용을 낮추고 사용자 지정된 제어 기능을 유지합니다.
- **로컬 배포:** 현장의 서버에 관리 소프트웨어를 로컬로 설치하여 배포합니다.
  - **이점**: 고객은 기존 배포를 사용하고 다양한 McAfee 기술을 중앙에서 관리할 수 있습니다.

성능을 위한 설계

MVISION Endpoint의 기능 대부분은 클라우드 기반 서비스를 통해 제공되므로 매우 가벼우며 아주 작은 공간만 사용합니다. 결과적으로 빠른 시작이 가능하며 클라이언트 파일 크기가 작으므로 가동 중단 시간이 짧아지고 대역폭에 미치는 영향이 경미합니다.

일단 설치하면 방어를 위해 업데이트할 필요가 없으며, 이후 업데이트가 자동으로 수행되므로 관리자가 업데이트 설치를 위한 조치를 수행할 필요가 없습니다.

항상 작동 상태로 두는 대신, 기본적으로 컴퓨팅 성능과 대역폭의 규모를 필요에 따라 균형 있게 조정하는 성능 설정을 사용해 엔드포인트 환경과 사용자에게 미치는 영향을 최소한으로 유지합니다.

전체 환경을 위한 통합 플랫폼

BYOD(Bring-Your-Own-Device), 모바일 및 IoT(사물 인터넷) 장치가 증가하면서 많은 조직에서는 서로 다른 운영 체제와 장치 유형을 보호해야 합니다. 이처럼 갈수록 증가하는 복잡성을 해결하기 위해 McAfee에서는 관리 간소화, Windows 보안 강화, 모바일 및 IoT 장치 보안에 대한 전략 비전을 McAfee 포트폴리오에 가져오는 혁신적인 MVISION 기술을 선보였습니다.

McAfee MVISION 기술은 보안 전문가가 McAfee, 타사 및 기본 OS(운영 체제)로 구성된 포괄적인 집합을 단일 지점에서 살펴보고 제어하는 기능을 통해 관리할 수 있는 클라우드 중심의 장치 보안 방법을 사용합니다.

McAfee Device Security 포트폴리오를 사용하면 데스크톱, 노트북, 태블릿, 모바일, 물리적/가상 서버, 클라우드 워크로드 및 IoT를 비롯한 전체 공격 영역에서 필요한 보호를 받을 수 있습니다.

McAfee MVISION Endpoint가 비즈니스에 제공하는 이점

- 모든 장치를 중앙 집중식으로 관리
- 고급화된 파일, 파일리스, 행동 기반 기계 학습 방어
- Mac, Linux, IoT 및 모바일 장치 보호
- 공격받기 전에 초기에 대응하도록 사이버 보안 절차 전환
- TCO를 줄이고 워크플로 간소화

McAfee를 선택해야 하는 이유

- 적은 수의 클릭으로 더 많은 작업을 더 빠르게 수행
- 업계에서 기본 제어 기능에 사전 조정된 고급 방어와 결합된 관리를 제공하는 유일한 공급업체
- 전체 장치 환경에 대한 가시성
- 다중 통합된 대규모 개방형 에코시스템
- 확실한 사전 엔드포인트 보안

자세한 내용

자세한 내용을 보려면 다음 웹 사이트를 방문하십시오. **www.mcafee.com/enterprise/ko-kr/products/mvision-endpoint.html**.

1. Microsoft Windows 10, Microsoft Windows Server 2016 및 Microsoft Windows Server 2019 시스템
2. 이 문서에는 제품, 서비스 및/또는 개발 프로세스에 대한 정보가 포함되어 있습니다. 여기에 설명된 이점은 시스템 구성에 따라 다르며 사용되는 하드웨어, 소프트웨어 및/또는 서비스 활성화를 필요로 할 수 있습니다. 여기에 제공된 모든 정보는 McAfee의 재량에 따라 예고 없이 변경될 수 있습니다. 최신 예측, 일정, 사양 및 로드맵을 받으려면 McAfee 담당자에게 문의하십시오.

설명된 비용 및 시간 절약 시나리오는 지정된 McAfee 제품의 구성과 배포를 최적화하면 향후 비용에 어떤 영향을 미치며, 비용과 시간을 어떻게 절약할 수 있는지를 보여주는 예입니다. 환경과 결과는 구성 및 배포에 따라 달라질 수 있습니다. McAfee에서는 시간 또는 비용 절약을 보장하지 않습니다.

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

McAfee 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2020 McAfee, LLC. 4496_0620
2020년 6월