McAfee Embedded Control

여러분이 의존하는 장치를 위한 간단한 방어

오늘날의 확장된 공격 표면은 웨어러블 피트니스 장치에서부터 생성 및 배포를 제어하는 중요한 연결 센서에 이르기까지 새로운 엔드포인트에 의해 장악되고 있습니다. 연결된 장치 수가 증가하면 맬웨어 및 공격의 위험도 커집니다. McAfee® Embedded Control은 장치에 인증받은 액세스만 허용하고 인증받지 않은 실행 파일을 차단하여 시스템의 무결성을 보장합니다.

McAfee Embedded Control은 포함된 시스템에 상업용 운영 체제를 적용하여 발생하는 보안 위험 문제 해결에 초점을 둡니다. McAfee Embedded Control은 설치 공간이 작고 오버헤드가 낮은 응용프로그램 독립적 솔루션으로 '배포 후 잊기(deploy-and-forget)' 보안을 제공합니다. McAfee Embedded Control은 상업용 운영 체제에 내장된 시스템을 '블랙박스'로 변환하여 닫힌 독점 운영 체제처럼 보이도록 합니다. 또한 디스크에 있거나 메모리에 주입된 승인되지 않은 프로그램을 실행할 수 없도록 방지하고 인증된 기준선을 무단으로 변경할 수 없도록 합니다. 이 솔루션을 통해 제조업체는 추가 위험을 유발하지 않고 현장에서 시스템이 사용되는 방식을 제어하면서 상업용 운영 체제를 사용하는 혜택을 누릴 수 있습니다.

시스템 무결성 보장

실행 파일 제어

McAfee Embedded Control을 사용하면 McAfee 동적 화이트리스트에 포함된 프로그램만 실행할 수 있습니다. 다른 프로그램(exe, dll, 스크립트)은 승인되지 않은 것으로 간주됩니다. 이러한 프로그램의 실행은 방지되며 기본적으로 오류가 기록됩니다. 따라서 불법적으로 실행되어 자체적으로 설치되는 웜, 바이러스, 스파이웨어 및 기타 멀웨어를 방지할 수 있습니다.

메모리 제어

메모리 제어에서는 실행 중인 프로세스를 가로채려는 악의적인 시도로부터 해당 프로세스를 보호합니다. 실행 중인 프로세스에 주입된 인증되지 않은 코드는 트랩되고 중단된 후 로그됩니다. 이런 식으로 버퍼 오버플로, 힙 오버플로, 스택 실행 및 유사한 공격으로 시스템을 제어하려는 시도는 모두 유효하지 않게 되며 로그됩니다.[1]

주요 이점

- 포함된 장치에서 실행되는 대상을 제어하고 해당 장치의 메모리를 보호하여 보안 위험 최소화
- 액세스 제공, 제어 유지, 지원 비용 절감을 지원
- 선택적 시행
- 배포 후 잊기
- 장치 컴플라이언스 및 감사 준비를 지원
- 실시간 표시
- 포괄적인 감사
- 검색 가능한 변경 내용 보관
- 닫힌 루프 조정

McAfee GTI 통합: Air-Gap 환경에 대한 글로벌 위협을 처리하는 최적의 방법

McAfee® Global Threat Intelligence(McAfee GTI)는 전 세계에 있는 수백만 개의 센서를 사용하여 파일, 메시지 및 발신자의 평판을 실시간으로 추적하는 독자적인 McAfee 기술입니다. 이 기능은 클라우드 기반 정보를 사용하여 컴퓨팅 환경에 있는 모든 파일의 평판을 결정하고, '양호', '불량' 및 ' 알 수 없음'으로 분류합니다. McAfee GTI와 통합하면 악성 프로그램이 실수로 화이트리스팅되는 경우를 확실히 알 수 있습니다. GTI 평판은 고립된 McAfee® ePolicy Orchestrator® (McAfee ePO™) 소프트웨어 환경뿐만 아니라 인터넷 연결에서도 액세스할 수 있습니다.

변경 제어

McAfee Embedded Control은 변경을 실시간으로 탐지합니다. 이 기능은 변경 소스를 시각적으로 표시하고 변경 사항이 올바른 대상 시스템에 배포되었는지 확인합니다. 또한 변경 사항을 감사 추적하고 변경 작업이 인증된 수단을 통해서만 수행되도록 합니다.

McAfee Embedded Control을 통해 변경 작업을 수행할 수 있는 인증된 방법을 지정하면 변경 제어 프로세스를 적용할 수 있습니다. 변경을 적용할 수 있는 사람, 변경을 허용하는 데 필요한 인증서, 변경할 수 있는 내용(예: 특정 파일이나 디렉터리로 변경을 제한할 수 있음) 및 변경을 적용하는 시간(예: 한 주의 특정 시간에만 Microsoft Windows 업데이트를 열 수 있음)을 제어할 수 있습니다.

사전 변경에서는 대상 시스템에 적용되기 전에 각 변경 작업을 확인합니다. 이 모듈을 활성화하면 소프트웨어 시스템을 제어된 방식으로만 업데이트할 수 있습니다.

실시간 변경 추적 모듈에서는 코드, 구성 및 레지스트리를 포함하여 시스템 상태에 대한 모든 변경 내용을 기록합니다. 변경 이벤트를 발생될 때 실시간으로 기록되고 집계 및 보관을 위해 시스템 컨트롤러로 전송됩니다.

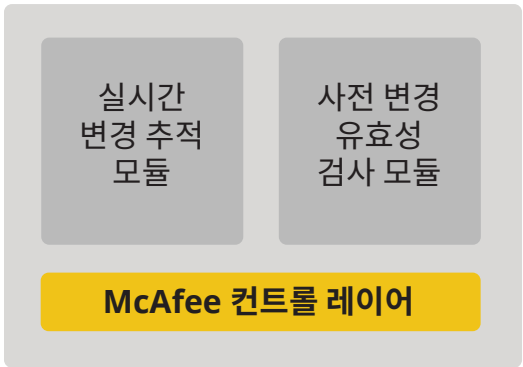

그림 1. McAfee 컨트롤 레이어.

시스템 컨트롤러 모듈이 시스템 컨트롤러와 에이전트 간 통신을 관리합니다. 또한 독립 레코드 시스템의 에이전트에서 변경 이벤트 정보를 집계하고 저장합니다.

그림 2. 보고, 검색 및 분석 모듈.

감사 및 정책 컴플라이언스

McAfee® Integrity Control에서는 컴플라이언트 요구 사항에 맞는 대시보드 및 보고서를 제공합니다. 이러한 대시보드 및 보고서는 사용자 및 관리자에게 웹 기반 UI를 제공하는 McAfee ePO 콘솔을 통해 생성됩니다.

McAfee Embedded Control는 통합된 닫힌 루프의 실시간 컴플라이언스 및 감사를 제공하며 인증된 활동 및 무단 시도에 대한 레코드의 물리적 조작 방지 시스템도 함께 제공합니다.

McAfee 임베디드 보안 정보

McAfee 임베디드 보안 솔루션을 통해 제조업체는 사이버 위협 및 공격으로부터 제품 및 장치를 보호할 수 있습니다. McAfee 솔루션은 응용프로그램 화이트리스트 작성, 안티바이러스 및 악성 프로그램 백신 보호, 장치 관리, 암호화, 위험 및 컴플라이언스 등 광범위한 기술을 제공하며 모두 업계 최고의 McAfee Global Threat Intelligence를 사용합니다. 또한 McAfee 솔루션은 제조업체의 장치 및 해당 아키텍처에 대한 특정 설계 요구 사항에 맞게 조정할 수 있습니다.

기능	설명	혜택
시스템 무결성 보장		
외부 위협 방어	인증된 코드만 실행되도록 합니다. 인증되지 않은 코드를 메모리에 주입할 수 없습니다. 인증된 코드는 조작할 수 없습니다.	▪ 비상 패치 적용 제거, 패치 적용 주기의 횟수 및 빈도 감소, 패치 적용 전에 더 많은 테스트 활성화, 패치 적용이 어려운 시스템에 대한 보안 위험 감소. ▪ 제로 데이의 보안 위험 감소, 웜, 바이러스, 및 트로이 목마와 같은 멀웨어를 통한 다형성 공격 감소, 그리고 버퍼 오버플로, 힙 오버플로 및 스택 오버플로와 같은 코드 주입 감소. ▪ 인증된 파일의 무결성을 유지 관리하여 생산 중인 시스템을 알려지고 확인된 상태로 유지. ▪ 계획되지 않은 패치 적용 및 복원으로 인한 가동 중단 시간을 제한하여 운영 비용을 절감하고 시스템 가용성 향상.
내부 위협 방어	로컬 관리자 잠금에서는 인증 키를 제공하지 않으면 보호된 시스템에서 실행할 권한이 있는 내용을 관리자도 변경할 수 없도록 하는 유연성을 제공합니다.	▪ 내부 위협으로부터 보호. ▪ 생산 중인 포함된 시스템에서 실행되는 내용을 잠그고 관리자도 변경할 수 없도록 함.
고급 변경 제어		
제조업체에 의한 인증된 업데이트 보호	현장의 포함된 시스템에 인증된 업데이트만 구현할 수 있도록 합니다.	▪ 대역 외 변경은 현장의 시스템에 배포할 수 없습니다. 가동 중단이 발생하거나 서비스 요청 전화를 걸기 전에 무단 시스템 변경을 방지합니다. ▪ 제조업체는 모든 변경 자체에 대한 제어를 유지하거나 신뢰할 수 있는 고객 에이전트에만 변경 제어 권한을 부여할 수 있습니다.
승인된 창 내에 수행된 변경 사항을 확인	변경이 인증된 변경 창 외부에 배포되지 않도록 합니다.	▪ 재정적으로 중요한 기간이나 업무가 많은 시간 동안의 무단 변경을 방지하여 업무가 중단되거나 컴플라이언스 위반이 발생하지 않도록 합니다.
인증된 업데이트 프로그램	인증된 업데이트 프로그램(사람 또는 프로세스)만 프로덕션 시스템에 변경을 구현할 수 있도록 합니다.	▪ 대역 외 변경은 프로덕션 시스템에 배포할 수 없습니다.
실시간, 닫힌 루프, 감사 및 컴플라이언스		
실시간 변경 추적	기업 전체에서 변경이 발생하는 즉시 변경을 추적합니다.	▪ 대역 외 변경은 프로덕션 시스템에 배포할 수 없습니다.
포괄적인 감사	모든 시스템 변경에 대한 전체 변경 정보 즉, 누가, 언제, 어디서, 무엇을, 어떻게 했는지에 대한 정보를 캡처합니다.	▪ 모든 시스템 변경 사항에 대한 정확하고 완전하며 확실한 기록을 유지합니다.
변경의 소스 식별	모든 변경을 소스 즉, 변경을 수행한 사람, 변경을 발생시킨 이벤트의 시퀀스, 변경에 영향을 준 프로세스/프로그램 등에 연결합니다.	▪ 승인된 변경의 유효성을 검사하고, 승인되지 않은 변경을 신속하게 식별하며, 변경 성공률을 향상시킵니다.

기능	설명	혜택
낮은 운영 오버헤드		
배포 후 잊기	몇 분 안에 설치할 수 있고 초기 구성이나 설정이나 지속적인 구성이 필요 없습니다.	▪ 제공된 상태로 작동합니다. 설치 후 바로 적용됩니다. 지속적인 유지 관리 오버헤드가 없으므로 저렴한 운영 비용의 보안 솔루션 구성으로 선택하는 경우가 많습니다.
규칙 없음, 시그너처 없음, 학습 기간 없음, 응용프로그램 독립적	규칙 또는 시그니처 데이터베이스를 사용하지 않으며, 학습 기간 없이 바로 모든 응용프로그램에서 사용할 수 있습니다.	▪ 서버 수명 주기 동안 관리자의 주의가 거의 필요하지 않습니다. ▪ 지속적인 운영 비용이 저렴하여 패치가 적용되거나 적용되지 않은 서버까지도 보호합니다. ▪ 효율성이 규칙이나 정책의 품질에 따라 달라지지 않습니다.
적은 설치 공간, 적은 런타임 오버헤드	20MB 미만의 디스크 공간을 사용합니다. 응용프로그램의 런타임 성능을 방해하지 않습니다.	▪ 시스템의 런타임 성능이나 저장소 요구 사항에 영향을 미치지 않고 업무상 중요한 프로덕션 시스템에 배포할 수 있습니다.
잘못된 긍정 또는 잘못된 부정 보장하지 않음	인증받지 않은 활동만 기록합니다.	▪ 결과의 정확성으로 인해 매일/주별로 로그를 분석하는 데 필요한 시간을 현저하게 줄일 수 있으므로 다른 호스트 침입 방지 솔루션에 비해 운영 비용을 절감할 수 있습니다. ▪ 관리자 효율성을 향상시키고 운영 비용을 절감합니다.

다음 단계

자세한 내용을 보려면 **www.mcafee.com/kr/partners/oem-alliances/index.aspx** 를 방문하거나 지역별 McAfee 담당자에게 문의하십시오.

1. Microsoft Windows 플랫폼에서만 사용할 수 있습니다.

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