McAfee Application Control

엔드포인트, 서버 및 고정 장치를 제어하기 위해 인증되지 않은 응용프로그램의 위험을 줄임

원격 공격 또는 사회 공학을 통한 APT(지능형 지속가능 위협)로 인해 비즈니스 보호가 점점 더 어려워지고 있습니다. McAfee® Application Control은 사이버 범죄자보다 한 수 앞서 나가고 비즈니스 보안과 생산성을 유지하도록 도와줍니다. 동적 신뢰 모델 및 로컬 및 글로벌 평판 정보, 실시간 동작 분석 및 자동 엔드포인트 면역과 같은 혁신적인 보안 기능을 사용하는 이 Intel® Security 솔루션은 노동 집약적인 목록 관리 또는 시그니처 업데이트 없이도 APT를 즉시 무력화시킬 수 있습니다. 제로 데이 위협을 전혀 허용하고 싶지 않다면 McAfee Application Control을 더욱 면밀히 살펴보시기 바랍니다.

주요 이점

- 시그니처를 업데이트하지 않고 제로 데이 및 APT 로부터 보호
- McAfee Global Threat Intelligence 및 McAfee Threat Intelligence Exchange를 사용하여 파일 및 응용프로그램의 글로벌 및 로컬 평판을 제공할 수 있습니다.
- 신뢰할 수 있는 채널을 통해 새로 추가된 소프트웨어를 자동으로 허용하는 동적 화이트리스팅을 사용하여 보안을 강화하고 소유 비용을 줄일 수 있습니다.
- McAfee 보안 솔루션 관리를 위한 중앙 집중식 플랫폼인 McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어를 통해 응용프로그램 액세스를 효율적으로 제어할 수 있습니다.
- 안전한 화이트리스트 및 고급 메모리 보호를 통해 패치 주기 단축
- 신뢰할 수 있는 업데이트를 사용하여 최신 패치로 시스템을 최신 상태로 유지할 수 있습니다.

지능적인 화이트리스팅

McAfee Application Control은 승인되지 않은 응용프로그램 실행을 차단하여 제로 데이 및 APT 공격을 방지합니다. 인벤토리 기능을 사용하여 모든 응용프로그램 관련 파일을 쉽게 찾고 관리할 수 있습니다. 기업 내 모든 바이너리(EXEs, DLLs, drivers, and scripts)를 응용 프로그램 및 공급업체별로 그룹화하고 이를 직관적인 계측적 형식으로 표시하고, 잘 알려진, 알 수 없는, 알려진 불량 응용프로그램으로 지능적으로 분류합니다. 화이트리스팅을 사용하면 알려진 정상적인 화이트리스트 응용프로그램만 실행하도록 허용하여 알 수 없는 악성 프로그램의 공격을 방지할 수 있습니다.

올바른 보안 자세 구현

소셜 및 클라우드 기반 비즈니스 환경에서 애플케이션 사용에 대한 사용자의 보다 많은 유연성 요구가 늘어남에 따라 McAfee Application Control은 위협 방지를 위한 화이트리스팅 전략을 극대화할 수 있는 세 가지 옵션을 다음과 같이 조직에 제공합니다.

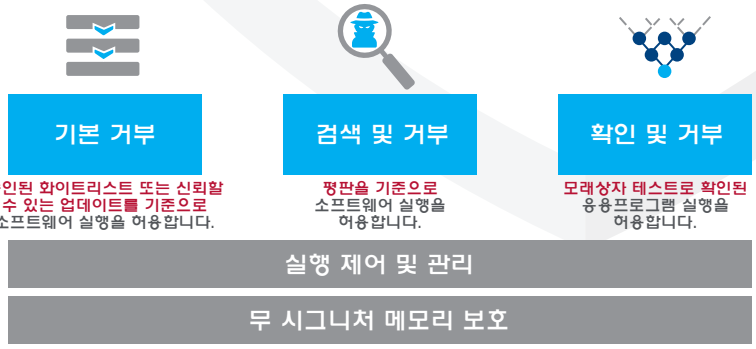

그림 1. 화이트리스트 전략을 극대화하기 위한 세 가지 방법.

주요 이점(계속)

- 연결되거나 연결이 끊긴 서버, 가상 시스템, 엔드포인트 및 POS(point-of-sale) 터미널과 같은 고정된 장치, Microsoft Windows XP와 같은 레거시 시스템에 대한 제어를 강화할 수 있습니다.
- 응용프로그램 등급 또는 비즈니스 연속성 향상을 위한 자체 승인을 기반으로 새로운 응용프로그램을 허용합니다.
- 간접 비용이 낮은 솔루션을 통해 사용자 생산성 및 서버 성능 유지
- 레거시 시스템 및 현재의 기술 투자를 쉽게 보호합니다.

지원되는 플랫폼

Microsoft Windows(32비트 및 64비트)

- 내장: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, 8, 8.1 Industry, 10
- 서버: Windows Server 2008, 2008 R2, 2012, 2012 R2
- 데스크톱: Windows NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

강력한 기본 제공 제안

인벤토리 검색 및 미리 정의된 보고서를 사용하여 사용자 환경에 존재하는 취약성, 컴플라이언스 및 보안 문제를 신속하게 찾아내고 해결할 수 있습니다. 최근에 추가된 응용프로그램, 인증되지 않은 바이너리, 평판을 알 수 없는 파일, 오래된 버전의 소프트웨어를 실행하는 시스템 등 유용한 정보를 검색하여 취약성을 신속하게 파악하고 소프트웨어 사용권의 컴플라이언스를 검증할 수 있습니다.

완벽하고 신속한 대응

화이트리스팅이 McAfee GTI(McAfee Global Threat Intelligence)의 글로벌 위협 인텔리전스를 통해 강화되었습니다. McAfee GTI는 전 세계에 있는 수백만 개의 센서를 사용하여 파일, 메시지 및 발신자의 평판을 실시간으로 추적하는 독자적인 Intel Security 기술입니다. McAfee Application Control은 이러한 정보를 사용하여 컴퓨팅 환경에 있는 파일의 평판을 결정하고, 양호, 불량 및 알 수 없음으로 분류합니다.

개별적으로 판매되는 선택 모듈인 McAfee Threat Intelligence Exchange와 함께 배포될 경우, McAfee Application Control은 즉각적인 위협 대처를 위해 로컬 평판 정보를 기반으로 화이트리스트를 업데이트합니다. McAfee Application Control은 McAfee Advanced Threat Defense와 함께 Threat Intelligence Exchange를 사용하여 알려지지 않은 응용프로그램의 동작을 모래상자 안에서 동적으로 분석하고 새롭게 감지된 악성 프로그램으로부터 모든 엔드포인트를 자동으로 면역화합니다.

비즈니스 연속성에 대한 영향 제거

비즈니스 연속성에 방해가 되지 않도록 새로운 응용프로그램은 응용프로그램 평판을 기준으로 자동으로 허용됩니다. 알려지지 않은 응용프로그램의 경우, 제안 인터페이스가 엔드포인트에서의 실행 패턴을 기준으로 새로운 업데이트 정책을 추천합니다. 이렇게 하면 차단된 응용프로그램에서 생성되는 예외를 효과적으로 관리할 수 있습니다. 차단된 응용프로그램의 예외 및 세부 사항을 조사한 후에는 단순히 파일을 승인 및 화이트리스트로 지정하거나 이를 무시하여 응용프로그램을 차단할 수 있습니다.

문제 해결에 사용자 참여 유도

알려지지 않은 응용프로그램에 대해 McAfee Application Control은 사용자가 새로운 응용프로그램을 설치할 수 있는 여러 가지 방법을 제공합니다.

사용자 통보 - 사용자에게 인증되지 않은 응용프로그램에 대한 액세스가 필요한 이유를 설명하는 정보 전달용 팝업 메시지가 표시됩니다. 이러한 메시지는 이메일 또는 헬프데스크를 통해 승인을 요청하도록 사용자에게 알립니다.

사용자 자체 승인 - 이 권한이 있는 사용자는 IT 승인을 기다릴 필요 없이 새로운 소프트웨어를 설치할 수 있습니다. IT는 이러한 자체 승인을 검사하고 전사적 정책을 만들어 모든 시스템에 앱을 금지하거나 허용하도록 합니다.

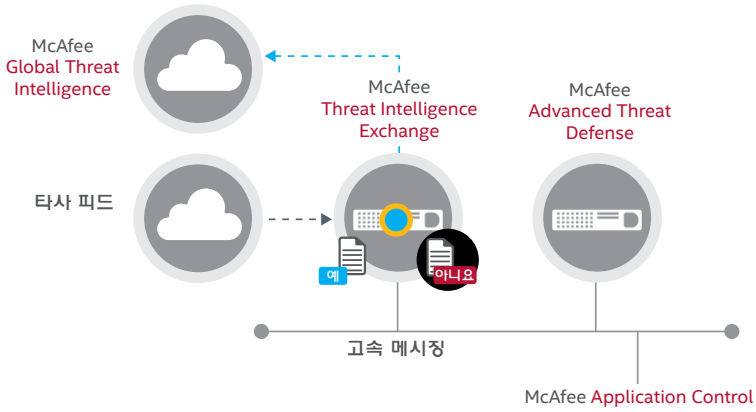

그림 2. McAfee GTI는 파일 및 발신자의 평판을 지속적으로 모니터합니다. McAfee Threat Intelligence Exchange와 함께 배포된 McAfee Application Control은 로컬 평판 정보를 기준으로 화이트리스트를 자동으로 업데이트하고 파일에 대한 추가 정보가 필요한 경우 McAfee Advanced Threat Defense와 함께 협력할 수 있습니다.

시스템을 최신 상태로 유지

시스템은 최신 패치를 통해 항상 최신 상태로 유지하는 것이 중요합니다. 동적 신뢰 모델은 비즈니스 연속성에 영향을 주지 않으면서 시스템을 자동으로 업데이트할 수 있게 해줍니다. 신뢰할 수 있는 사용자, 인증서, 프로세스 및 디렉터리를 사용하여 시스템을 최신 상태로 유지하십시오. 또한 McAfee Application Control은 Windows 32 및 64비트 시스템에서 메모리 버퍼 오버플로 공격이 화이트리스트 응용프로그램의 취약성을 공격하지 못하도록 방지합니다.

McAfee ePolicy Orchestrator 소프트웨어: 단일 관리 창

McAfee ePO 소프트웨어는 관리 기능을 통합하고 중앙 집중화하므로 사각지대 없이 기업 보안에 대한 전체적인 파악이 가능합니다. 수상 경력으로 입증된 이 플랫폼은 McAfee Application Control을 McAfee Host Intrusion Prevention 및 블랙리스팅을 위한 안티맬웨어를 포함한 기타 McAfee 보안 제품과 통합합니다. Microsoft System Center에서 McAfee Application Control을 한 번에 설치하고 업데이트할 수 있습니다.

관찰 모드에서 보기 및 파악

관찰 모드를 통해 화이트리스트 잠금을 시행하지 않고 동적 데스크톱 환경에 대한 정책을 검색할 수 있습니다. 따라서 응용프로그램을 중단하지 않고 이전 또는 초기 생산 환경에서 McAfee Application Control을 점진적으로 배포할 수 있습니다. 관리자는 McAfee Application Control을 통해 관찰 및 자체 승인 요청을 위한 정책 정의에 단일 정책 검색 페이지를 사용할 수 있습니다.

레거시 시스템 및 최근 기술 투자 보호

Microsoft Windows NT, 2000 및 XP와 같이 오래된 운영 체제를 보호해야 합니까? Microsoft 및 다른 보안 공급업체에서는 이러한 레거시 시스템을 지원하지 않지만 McAfee Application Control은 지원합니다. 또한 McAfee Application Control은 Microsoft Windows 10과 같은 최신 운영 체제를 지원합니다.

다음 단계

자세한 내용은 **http://www.mcafee.com/kr/products/application-control.aspx**를 참조하거나 (02)3458-9800으로 전화하십시오 (연중무휴 24시간).

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com