McAfee Advanced Threat Defense

위협적인 대상 공격 탐지

Intel Security® 제품의 일부인 McAfee® Advanced Threat Defense를 사용하면 위협적인 대상 공격을 탐지하고 위협 정보를 즉각적인 조치 및 보호로 전환할 수 있습니다. 기존 샌드박스와 달리 이 솔루션에는 탐지 기능을 확대하고 우회 위협을 노출하는 조사 기능이 추가되어 있습니다. 환경 전반에서 위협 정보를 즉각적으로 공유할 수 있도록 네트워크부터 엔드포인트까지 Intel Security 솔루션 간의 통합을 강화하여 보호 및 조사 성능이 향상되었습니다. 유연한 배포 옵션은 모든 네트워크를 지원합니다.

McAfee Advanced Threat Defense의 핵심 차별화 요소

Intel Security 솔루션 통합 강화

- 조직 전반에서 발생부터 억제 및 차단 시점까지의 격차를 해소합니다.
- 워크플로를 간소화하여 대응 및 교정 시간을 단축합니다.

강력한 분석 기능

- 강력한 언패킹 기능을 사용하여 보다 뛰어나고 완전한 분석을 가능하게 합니다.
- 심층적인 코드 분석과 동적 분석을 결합하여 뛰어난 분석 데이터를 통해 보다 정확한 탐지가 가능해집니다.

유연한 중앙 집중식 배포

- 여러 프로토콜을 지원하는 중앙 집중식 배포로 비용을 절감합니다.
- 유연한 배포 옵션은 모든 네트워크를 지원합니다.

McAfee 기술은 네트워크 주변부에서 엔드포인트까지 전체 영역의 진화한 악성 프로그램 분석 기능을 기존 기능과 연계하고 위협 인텔리전스를 전체 IT 환경과 공유하여 탐지 방법을 혁신했습니다. McAfee 솔루션은 관리, 네트워크 및 엔드포인트 시스템 간에 위협 인텔리전스를 공유하여 명령 및 컨트롤 통신을 즉시 종료하고, 손상된 시스템을 격리하고, 동일하거나 유사한 위협의 추가 인스턴스를 차단하고, 손상이 발생할 수 있는 위치를 평가하고, 적절한 조치를 취합니다.

McAfee Advanced Threat Defense: 진화한 위협 탐지

McAfee Advanced Threat Defense는 혁신적인 계층화된 접근 방법을 사용하여 오늘날의 은폐형 제로 데이 악성 프로그램을 탐지합니다. 이 프로그램은 로우터치 안티바이러스 시그니처, 평판 및 실시간 에뮬레이션 방어 기능을 심층적인 코드 및 동적 분석(샌드박스)과 결합하여 실제 동작을 분석합니다. 이를 통해 시중에 나와 있는 가장 강력한 진화한 악성 프로그램 보안 보호 기능이 되었으며 보호 및 성능의 두 요건을 고려하면서 효과적으로 균형을 유지합니다.

알려진 악성 프로그램을 탐지하여 서명, 실시간 에뮬레이션 성능 이점 등과 같은 분석 방법의 강도는 낮추면서 샌드박스에 심층적인 코드 분석을 추가하여 위장한 우회 위협에 대한 보호 수준을 강화합니다. 코드 재사용을 이용하는 알려진 악성 프로그램 패밀리와 함께 유사성 평가를 비롯한 자세한 악성 프로그램 분류 정보를 제공합니다. 지연되거나 조건부 실행 경로 등과 같이 종종 동적 환경에서 실행되지 않는 샌드박스 우회 기술을 언패킹 및 심층적인 정적 코드 분석을 통해 탐지할 수 있습니다.

악성 프로그램 작성자는 패킹을 사용하여 코드의 구성을 바꾸거나 숨겨 탐지를 피합니다. 대부분의 제품은 분석을 위해 전체 원본(소스) 실행 코드를 제대로 언패킹할 수 없습니다. McAfee Advanced Threat Defense에는 불명확성을 해소하여 원래의 실행 코드를 드러내는 확장된 언패킹 기능을 포함합니다. 따라서 심층적인 정적 코드 분석은 높은 수준의 파일 특성에 이상이 있는지 확인하여 모든 특성 및 명령 세트의 예상 동작을 파악할 수 있습니다.

심층적인 정적 코드와 동적 분석이 함께 진행되어 의심스런 악성 프로그램을 완벽하고 세부적으로 평가합니다. 뛰어난 분석 결과에서는 상황을 전반적으로 파악하고 조치 우선순위를 정하는 데 도움이 되는 요약 보고서뿐 아니라, 악성 프로그램에 대한 분석가 등급 데이터가 포함된 상세한 보고서를 생성합니다.

intel Security

통합 솔루션

- McAfee Active Response
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Server Security
- McAfee Web Gateway

향상된 보호

진화한 악성 프로그램을 찾아내는 일은 중요합니다. 하지만 솔루션의 기능이 보고서 또는 경고를 제공하는 데 한정될 경우 관리자는 많은 작업을 수행해야 하고 네트워크는 보호되지 않습니다.

네트워크 주변부에서 엔드포인트까지 전체 영역에서 McAfee Advanced Threat Defense와 보안 장치 간에 견고한 통합이 이루어지면 McAfee Advanced Threat Defense가 파일을 악성 파일로 결정하는 즉시 통합 보안 장치에서 즉각적인 조치가 수행될 수 있습니다. 탐지 및 보호 동작이 서로 견고하게 자동으로 통합되는 것도 중요합니다.

McAfee Advanced Threat Defense를 두 가지 방법 즉, 선택한 보안 솔루션과 직접 통합하거나 McAfee Threat Intelligence Exchange를 통해 통합할 수 있습니다.

직접 통합하면 McAfee Advanced Threat Defense가 파일을 악성 파일로 결정하는 즉시 Intel Security 솔루션에서 조치를 취할 수 있습니다. 위협 인텔리전스를 기존 정책 시행 프로세스에 즉시 통합하고 동일하거나 유사한 파일의 추가 인스턴스를 네트워크에 침입하지 못하도록 차단합니다.

McAfee Advanced Threat Defense에서 악성 파일로 결정한 파일은 전체 분석을 내장된 기능으로 수행한 경우처럼 통합 제품의 로고와 대시보드에 표시되므로, 워크플로가 간소화되고 관리자가 단일 인터페이스를 통해 경로를 효율적으로 관리할 수 있습니다.

McAfee Threat Intelligence Exchange를 통합하여 McAfee Advanced Threat Defense의 방어 기능이 강화되고(McAfee Endpoint Protection 포함) 을 비롯한 방어 기능이 강화되고 광범위한 통합 보안 솔루션에서 분석 결과와 손상 표시기에 액세스할 수 있습니다. McAfee Advanced Threat Defense에서 파일을 악성 파일로 결정하면 McAfee Threat Intelligence Exchange는 평판 업데이트를 통해 위협 정보를 조직 내에 통합된 모든 대응 조치에 즉시 게시합니다.

McAfee Threat Intelligence Exchange 지원 엔드포인트에서는 최초 감염 악성 프로그램의 설치를 차단하고 파일이 이후에 나타날 경우에 대비하여 사전 예방적으로 보호할 수 있습니다. McAfee Threat Intelligence Exchange 지원 게이트웨이는 파일이 조직에 침입하는 것을 차단할 수 있습니다. 또한 McAfee Threat Intelligence Exchange 지원 엔드포인트는 네트워크에 연결되어 있지 않은 상태에서도 악성 파일 업데이트를 계속 수신하므로 대역 외 페이로드 제공의 사각지대를 제거할 수 있습니다.

손상된 시스템을 찾아서 수정

조직에서 공격을 교정하기 위해서는 더 나은 결정을 내리고 적절히 대응할 수 있도록 우선 순위가 지정되고 실행 가능한 포괄적인 정보를 갖추어야 합니다. McAfee 솔루션은 함께 작동하여 조직에서 필요한 정보를 정확히 제공합니다.

McAfee Enterprise Security Manager는 McAfee Advanced Threat Defense 및 기타 보안 시스템에서 제공하는 세부 파일 평판 및 실행 이벤트를 사용하고 상호 연계하여 진화한 보안 정보, 위험 우선 순위 지정 및 실시간 상황 인식을 위한 고급 경보 및 기록 보기를 제공합니다. McAfee Advanced Threat Defense의 데이터 손상 표시기를 통해 McAfee Enterprise Security Manager는 최대 6개월 전부터 유지하고 있는 네트워크 또는 시스템 데이터에서 아티팩트의 징후를 발견하게 됩니다. 새로 식별된 악성 프로그램 소스와 이전에 통신했던 시스템을 밝혀낼 수 있습니다. McAfee Enterprise Security Manager는 즉각적인 시정 조치(대화형 또는 자동)가 수행되도록 정확한 위험 정보를 제공합니다. McAfee Endpoint Protection, McAfee Threat Intelligence Exchange 및 McAfee Active Response와의 긴밀한 통합 덕분에 새로운 구성 실행, 새로운 정책 구현, 파일 제거, 위험을 사전 예방적으로 완화할 수 있는 소프트웨어 업데이트 배포 등과 같은 작업 및 가시성을 통해 보안 작업의 응답성과 효율성을 최적화할 수 있습니다. 네트워크를 통해 감염된 엔드포인트가 McAfee Active Response에서 자동으로 식별되고 McAfee Advanced Threat Defense 보고서에 나열되면 정보에 기반한 조치를 쉽게 수행할 수 있습니다.

배포

유연성이 높은 진화한 위협 분석 배포 옵션은 모든 네트워크를 지원합니다. Advanced Threat Defense는 사내 어플라이언스 또는 가상 폼 팩터로 사용할 수 있습니다. 모든 폼 팩터는 여러 Intel Security 솔루션 간에 공유 리소스로 작동하며 비용 효과적으로 확장되고 비용을 절감할 수 있습니다.

또한 보안 운영 센터 및 악성 프로그램 분석가는 Advanced Threat Defense를 사용하여 조사할 수 있습니다.

McAfee Advanced Threat Defense는 다음을 비롯하여 다양한 고급 기능을 제공합니다.

- 사용자 지정 이미지 지원: 특정 호스트 프로파일 조건에서 위협을 확인합니다.
- 사용자 대화식 모드: 분석가가 악성 프로그램 샘플과 직접 상호 작용할 수 있습니다.
- 포괄적인 언패킹 기능: 조사 시간을 며칠에서 몇 분으로 단축할 수 있습니다.
- 전체 로직 경로: 일반적인 샌드박스 환경에서 유휴 상태로 남아 있는 추가적인 로직 경로를 강제 실행하여 보다 심층적인 샘플 분석을 수행할 수 있습니다.
- 여러 가상 환경에 샘플 제출: 파일 실행을 위해 필요한 환경 변수를 결정하여 조사 시간을 단축합니다.
- 디스어셈블리 출력과 메모리 덤프부터 그래픽 기능 호출 다이어그램과 임베디드 또는 삭제된 파일, 사용자 API 로그 및 PCAP 정보에 이르는 세부 보고서: 분석가의 조사에 필요한 중요한 정보를 제공합니다.

McAfee Advanced Threat Defense에 대한 자세한 내용을 원하거나 이 솔루션을 평가하려면 해당 지역의 담당자에게 문의하거나 **http://www.mcafee.com/kr/products/advanced-threat-defense.aspx**를 참조하십시오.

McAfee Advanced Threat Defense 사양		
물리적 폼 팩터	ATD-3000 1U·랙 마운트	ATD-6000 2U·랙 마운트
가상 폼 팩터	v1008, v1016, v3032, v6064 ESXi 6.0	v1008, v1016, v3032, v6064 ESXi 6.0
탐지		
지원되는 파일 샘플 유형	PE 파일, Adobe 파일, Microsoft Office 제품군 파일, 이미지 파일, 아카이브, Java, Android 응용프로그램 패키지, URL	
분석 방법	McAfee Anti-Malware Engine, GTI 평판: 파일/URL/IP, Gateway Anti-Malware(에뮬레이션 및 동작 분석), 동적 분석(샌드박스), 심층적인 코드 분석, 사용자 지정 YARA 규칙	
지원되는 OS	Windows 10(64비트), Windows 8.1(64비트), Windows 8(32비트/64비트), Windows 7(32비트/64비트), Windows XP(32비트/64비트), Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Windows 운영 체제 지원은 모든 언어로 제공됩니다.	
출력 형식	STIX, OpenIOC, XML, JSON, HTML, PDF, 텍스트	
제출 방법	통합 제품군, 직접/수동, API	

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