McAfee Cloud Threat Detection

McAfee® 보호 기술을 쉽게 개선하여 지능형 악성 프로그램을 진단하여 우회 위협 노출

기계 학습을 비롯한 McAfee의 다양한 최신 분석으로 악성 프로그램을 식별하고 진단을 조치로 전환할 수 있어 보호 기능을 업데이트하여 미래의 유사한 공격을 차단할 수 있습니다.

주요 이점:

- 비즈니스에 손상을 입히는 알 수 없는 위협에 대한 위험을 완화합니다.
- 빅데이터 및 시스템 학습의 강점을 활용합니다.
- 보안 투자를 최적화합니다.
- 진화한 위협 분석 배포를 간소화합니다.

교묘한 악성 프로그램이 기존의 방어 기술을 우회함에 따라 조직은 어려운 싸움에 직면해 있습니다. 고급 탐지 솔루션이 도움이 될 수 있지만, 보안 인력과 리소스가 한정되어 있는 경우 이 방법은 비용이 많이 소요되고 복잡해 보일 수 있습니다. 대부분의 솔루션은 보호 인프라와 통합되지 않으므로 응답기가 성급하게 조치를 수행하면서 취약성 노출이 증가할 수 있습니다.

그렇다면 무엇이 필요할까요? 극히 간단한 배포와 사용이 가능한 비용 효과적인 고급 탐지 기술인 McAfee® Cloud Threat Detection. 이 편리한 신규 서비스는 기존 McAfee 솔루션에 연결되어 지능형 악성 프로그램을 진단하고 우회 위협을 노출합니다. 이 클라우드 솔루션을 사용하면 막대한 컴퓨팅 마력을 쉽게 활용하여 일련의 최신 분석 기술을 작동할 수 있습니다. 탐지 기능을 개선하고 기존 보안 투자를 최적화할 수 있습니다.

보호 기술과 통합된 탐지

McAfee 솔루션은 에뮬레이션 및 평판과 같은 고급 도구를 사용하여 알려진 악성 프로그램 및 악성 프로그램일 가능성이 높은 프로그램을 차단하는 1차 방어선을 제공합니다. 그러나 파일이 악성 파일인지 확실하지 않은 경우에는 철저한 분석을 위해 클라우드로 보낼 수 있습니다.

시스템과 새로운 우회 악성 프로그램 비교

McAfee Cloud Threat Detection을 사용하는 경우 정적 분석 엔진이 파일 상세 정보를 추출하는 작업을 진행합니다. 포괄적인 파일 형식 적용 범위는 의심이 가는 파일에 대한 필수 컨텍스트를 제공하여 악성 파일과 치료된 파일 모두를 효과적으로 식별합니다. 또한, 파일이 샌드박스 환경에서도 실행되므로 동작 분석이 수행됩니다. 악성 프로그램의 동작은 모두 기록되어 악의적인 의도가 있는지 검토 및 평가됩니다. 특정 파일이 임의 폴더를 생성하고 새 파일을 해당 폴더에 쓴 후 원본 파일을 삭제했습니까? Google, Amazon 또는 Facebook 같은 알려진 사이트로 이동하는 트래픽 중에 알 수 없는 URL 또는 의심스러운 URL로 목적지가 위장되었습니까? 이는 McAfee Cloud Threat Detection 서비스가 알 수 없는 파일을 분류하는 데 사용할 수 있는 동작의 몇 가지 예시에 불과합니다. 이러한 프로세스에서는 메타데이터, URL, 파일 이름, 폴더 위치 등도 밝혀냅니다. 이러한 정보는 고객이 조사하여 다른 시스템이 손상되었는지 파악할 수 있도록 고객에게 다시 보고됩니다.

감독형 기계 학습

McAfee Labs에 의해 관리되고 조정되는 각 분석 주기 단계에서는 빅 브레인, 빅데이터 및 기계 학습의 강점을 활용합니다. 25여 년에 걸쳐 축적된 데이터와 20억 개 이상의 파일을 바탕으로 확보한 통찰력을 사용하여 클라우드의 빅데이터 시스템에서 광범위한 분류 모델을 개발하고 교육했습니다. 활발한 연구 및 검사 결과에 대한 꾸준한 해석은, 악성 프로그램 기술 및 동작이 바뀌고 연구가 발전함에 따라 이러한 모델이 진화할 수 있도록 지속적인 기계 학습을 보강합니다.

정확도에 집중

McAfee는 경험을 통해 잘못된 부정 또는 잘못된 긍정은 비용 부담을 주고 손상을 입힐 수 있음을 깨달았습니다. 따라서 McAfee가 사용하는 시스템의 경우 시기적절하면서 안정적인 진단이 이루어질 수 있도록 중요한 시스템 파일 및 서명 인증서에 대한 검사 및 평가가 포함됩니다. 고급 분석에서 새로운 위협을 탐지하긴 하지만, McAfee는 악성 프로그램 아티팩트 및 동작과 상황별 특성을 상호 참조하고 연결하여 잘못된 긍정을 최소화합니다. 이는 클라우드 분석 및 광범위한 안티맬웨어 리소스 조합이 가진 두드러진 이점 중 하나입니다.

탐지 작동 방식

각각의 판정에 대해 McAfee Cloud Threat Detection은 유사한 공격을 차단할 수 있도록 시스템 격리 또는 보호를 적용하는 등의 정책을 실시하는 원래 시스템에 알립니다. 추가 조사와 함께 공격 후 수정 및 복구에 필요한 통찰력을 확보할 수 있도록 자세한 IoC(손상 징후) 및 보고서가 제공됩니다. 진단에 따라 McAfee GTI(Global Threat Intelligence)의 평판이 업데이트되어 McAfee GTI 지원 솔루션을 사용하는 모든 조직을 더 빠르게 보호할 수 있습니다. 수동 제출은 조사를 지원하며 분석가가 일회성 분석을 위해 파일을 손쉽게 업로드할 수 있도록 지원합니다.

신속한 조치가 가능하고 경제적이며 중소기업에 친화적인 솔루션

클라우드 기반 서비스로서 통합 McAfee 제품에서 암호화된 공유 키를 입력하기만 하면 되므로 신속한 프로비저닝이 가능합니다. 분산 시스템이 있는 경우 트래픽을 데이터 센터로 역전송할 필요가 없으며 클라우드로 보내기만 하면 됩니다. McAfee 전문가가 지속적인 유지 관리를 관리하고 업데이트 및 업그레이드를 투명하게 구현합니다. 초기 자본 지출 대신 모든 통합 McAfee 솔루션에 적용되는 볼륨 기반의 구독 가격 책정은 비용 기반의 진입 장벽을 없앱니다.

www.mcafee.com/kr/products/cloud-threat-detection.aspx에서 자세히 알아보십시오.

통합 솔루션

- McAfee® ePolicy Orchestrator® Cloud
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Endpoint Protection
- McAfee Web Gateway 및 Web Gateway Cloud Service

McAfee Together is power.

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