McAfee Threat Intelligence Exchange

표적 공격에 대처하기 위한 위협 지능 공유

McAfee® Threat Intelligence Exchange는 엔드포인트, 게이트웨이, 네트워크, 및 데이터 센터 보안 솔루션의 지능을 실시간으로 운영화하여 적응형 위협 감지 및 대응을 가능하게 해줍니다. 가져온 글로벌 위협 지능을 지역에서 수집된 지능과 결합하고 즉시 공유함으로써 공유 지능을 서로 교환하고 이를 토대로 하여 여러 개의 보안 솔루션이 단일 방식으로 작동할 수 있습니다. McAfee Threat Intelligence Exchange는 문제 발생부터 방지까지의 간격을 일, 주 및 월 단위에서 밀리초까지 줄여줍니다.

주요 이점

- 위협 보호 기능은 문제 발생부터 진화한 타겟화된 공격 방지까지의 간격을 일, 주 및 월 단위에서 밀리초까지 줄여줍니다.
- 협력 가능한 위협 지능은 로컬 위협 지능 수집과 결합된 글로벌 지능 데이터 소스를 기반으로 구축됩니다.
- 조직에서 발견된 고급 표적 공격이 존재하는지 여부를 즉시 확인할 수 있습니다.
- 관련 보안 지능이 엔드포인트, 게이트웨이, 네트워크 및 데이터 센터 보안 솔루션 간에 실시간으로 공유됩니다.

협력 가능한 위협 지능 에코시스템 구축

McAfee Threat Intelligence Exchange는 McAfee Data Exchange Layer를 통해 정보를 공유하고 통합 방식의 보안을 제공합니다. 여러 개의 위협 정보 소스로부터 입력된 정보를 결합하여 타사 솔루션을 포함한 사용자의 보안 솔루션에서 즉시 공유할 수 있습니다.

보안 구성 요소가 하나로 작동하면 위협 감지 및 보호를 돕기 위한 관련 지능을 엔드포인트, 게이트웨이, 데이터 센터, 클라우드 및 기타 사용자 환경에 있는 보안 제어 지점에서 즉시 공유할 수 있습니다. McAfee Data Exchange Layer를 통해 구현되는 통합 간편성으로 구현 및 운영 비용이 크게 절감되며, 뛰어난 보안, 운영 효율성 및 효과가 제공됩니다.

개방형 프레임워크로 설계된 McAfee Data Exchange Layer는 타사 보안 제품을 비롯해서 모든 보안 솔루션이 McAfee Threat Intelligence Exchange 에코시스템에 동적으로 참여할 수 있게 해줍니다. 서로 완벽한 통신이 가능한 보안 구성 요소를 사용해서 총소유비용을 줄이고, 기존 보안 제품 및 솔루션 투자 가치를 보다 효과적으로 활용할 수 있습니다.

협력이 가능한 적응형 위협 방지 기술은 진정한 보안 조정을 위해 분산된 시스템을 하나로 연결하는 기업 IT 보안을 위한 새로운 접근 방식입니다. 보안 팀은 조직 및 예산에 따른 한계를 초월해서 보안 위협 정보 공유를 자동화하고, 네트워크의 모든 지점에 예방 정책 및 보호 체계를 미리 적용할 수 있는 능력이 필요합니다.

보안 관리자는 보안 인프라를 공동 작업 시스템으로 변환함으로써 위협을 탐지, 공유하고, 위협에 대한 내성을 기를 수 있습니다. McAfee Threat Intelligence Exchange는 복원력을 크게 높여주며 보다 주도적으로 새로운 위협 및 표적 공격에 대처할 수 있도록 합니다.

위협에 적응 및 내성 증가

네트워크의 모든 위치에서 감지되는 공유 정보를 통해 표적 공격에 보다 효과적으로 대처할 수

intel Security

주요 이점(계속)

- 총체적 위협 지능과 결합된 엔드포인트 컨텍스트(파일, 프로세스 및 환경 속성)를 기준으로 처음 발견된 파일에 대해 보다 효과적인 결정을 내릴 수 있습니다.
- McAfee Data Exchange Layer를 통해 통합이 간소화되었습니다. Intel Security 및 비Intel Security 보안 솔루션을 하나로 연결해서 위협 지능을 실시간으로 운영화함으로써 구현 및 운영 비용이 줄어듭니다.

있습니다. 이러한 위협은 본래부터 많은 주목을 받아온 공격이므로 조직은 경향을 알아내고 직면한 고유한 공격을 포착하기 위한 로컬 감시 시스템이 필요합니다. 인카운터에서 수집된 상황별 지역 데이터를 글로벌 위협 지능과 결합하여 처음 발견된 파일에 대해 보다 적절한 결정을 내릴 수 있으므로, 더 빠른 시간 내에 보호 및 탐지 효과를 얻을 수 있습니다.

네트워크 어디에서든 알려지지 않은 파일이 발견될 경우, McAfee Threat Intelligence Exchange에서 로컬로 평가됩니다. 확신 수준에 따라 보호 조치는 실시간으로 전체 시스템까지 전파됩니다. 이러한 로컬 위협 지능은 이후 사례를 위해 저장되므로, 다른 장치 또는 서버에서 같은 문제가 발견되더라도, 더 이상 알려지지 않은 문제가 아니며, 즉시 감지됩니다.

예를 들어, 게이트웨이에서 발견된 악성 파일에 대한 정보는 McAfee Data Exchange Layer를 통해 McAfee Threat Intelligence Exchange에 전송되며 사용자의 엔드포인트 및 데이터 센터에 밀리초 내에 도착합니다. 따라서 이러한 위협에 사전에 대처하기 위해 필요한 정보가 즉시 준비됩니다. 엔드포인트에서 손상을 주려는 시도가 차단되고 악성 프로그램으로 드러나면 이 정보가 즉시 게이트웨이 및 기타 보안 구성 요소로 전달 및 공유되어 위협을 사전에 차단합니다.

실시간 위협 지능 운영화

이제는 McAfee Global Threat Intelligence(McAfee GTI), 타사 위협 지능 및 공유 위협 지표(IoC)(예: STIX(Structured Threat Information eXpression) 파일)와 같은 글로벌 소스로부터 가져온 위협 지능을 결합할 수 있습니다. McAfee Global Threat Intelligence는 엔드포인트, 데이터 센터, 게이트웨이, 사용자 네트워크 및 McAfee Advanced Threat Defense 샌드박스 솔루션으로부터 실시간 로컬 및 이전 데이터를 수집합니다. 이렇게 결합된 글로벌 및 로컬 위협 데이터는 운영화 방식을 거쳐서 실시간으로 사용자의 전체 보안 에코시스템에 공유됩니다.

McAfee Threat Intelligence Exchange를 통해 관리자는 McAfee GTI, 타사 데이터 및 가져온 STIX 파일과 같은 글로벌 소스로부터 포괄적인 위협 지능을 쉽게 조정할 수 있습니다. 이러한 지능은 엔드포인트, 게이트웨이, 샌드박스 솔루션 및 기타 보안 구성 요소로부터 제공되는 실시간 및 이전 이벤트 데이터로부터 얻은 로컬 위협 지능과 함께 결합됩니다. 보안 관리자는 포괄적인 지능 정보를 취합, 재정의, 확대 및 조정하여 조직에 지정되고 사용되는 파일 또는 인증서에 대한 블랙리스트와 화이트리스트를 포함해서 해당 환경 및 조직에 맞게 보호 방식을 맞춤화할 수 있습니다.

이러한 로컬 우선 및 조정된 위협 정보를 통해 어떠한 미래 위협에 대해서도 즉각적으로 대처할 수 있습니다. 핵심 개체에 대한 설명형 메타데이터가 유지 관리되고 통합 지능에 반영됩니다. 관리자와 SIEM(보안 정보 및 이벤트 관리) 제품은 수집된 통찰력을 취합하여 악의적인 과거 활동을 토대로 손상될 가능성이 높은 시스템을 즉석에서 식별할 수 있습니다.

최첨단 엔드포인트 보호

McAfee Threat Intelligence Exchange는 McAfee Threat Intelligence Exchange VirusScan® Enterprise 모듈을 통해 혁신적인 엔드포인트 방지 기능을 제공합니다. 이 모듈은 구성 가능한 규칙을 사용하여 정확한 파일 실행 결정을 내리고, 로컬 엔드포인트 컨텍스트(파일, 프로세스 및 환경 특성)에서 얻은 지능과 현재 사용 가능한 통합 위협 지능(예: 조직적 확산, 사용 기간, 평판 등)을 함께 활용합니다.

엔드포인트에서 조직의 위험 허용치 수준에 따라 McAfee Threat Intelligence Exchange VirusScan Enterprise 모듈을 사용자 지정할 경우 관리자는 특정 요구에 맞게 실행 조건을 유연하게 설정할 수 있습니다. 이 방법은 알려져 있으며 허용되는 평판을 가진 파일이 아니면 액세스할 수 없도록 하는 규칙을 설정하여 알려지지 않은 파일 또는 '그레이' 파일에 대해 제로 허용치 정책을 고수하는 것만큼 엄격할 수 있습니다.

언제 어디에서나 엔드포인트 관리 가능

McAfee Threat Intelligence Exchange는 전역적으로 작용하는 적응형 위협 방지 및 보안 관리 기능을 제공합니다. 이 제품은 위치에 관계없이 엔드포인트에 연결되며, 위협 정책, 탐지 및 보안 업데이트의 관리와 원격 조사 기능을 제공합니다. 보안 구성요소들은 물리적 범주에 관계없이 하나의 요소처럼 작동합니다. 위치에 관계없이 엔드포인트, 게이트웨이 및 다른 보안 제품들 간에 관련 보안 데이터를 즉시 공유하여 적응형 위협 방지를 지원합니다.

진화한 표적 공격은 현실적인 과제

조직에서 탐지를 어렵게 하고 고가치 데이터를 추출하는 프로그램을 심어놓도록 설계된 진화한 타겟화된 공격은 조직에 계속적으로 해를 입힙니다. *Verizon 2015 Data Breach and Investigations Report(Verizon 2015 데이터 유출 조사 보고서)* 에서 최근 발표된 데이터에 따르면 악성 프로그램 샘플 중 70%~90%가 단일 조직에서만 고유하게 발생하여, 고유 위협 지표가 오늘날 가장 큰 문제임을 보여줍니다.[1]

자세한 내용은 **mcafee.com/TIE**를 참조하십시오.

다른 보안 관리 솔루션으로는 엔드포인트에 정책 변경 사항, 내용 및 프로그램 업데이트를 즉시 전달할 수 없습니다. 그렇지만 McAfee Threat Intelligence Exchange를 사용하면 조직이 증가하는 위협에 노출될 경우 창이 열린 상태로 유지됩니다. McAfee Data Exchange Layer를 활용해서 McAfee Threat Intelligence Exchange는 네트워크 장애물이 있더라도 지속적인 연결을 유지할 수 있습니다. 따라서 이러한 위험이 발생하는 즉시 방어할 수 있으며 무방비 상태로 남아 있는 엔드포인트가 없습니다.

공동 작업의 혜택

클릭 한 번으로 평판 쿼리

조직 내 모든 보안 구성 요소(게이트웨이, 엔드포인트 또는 네트워크)에서 알 수 없는 파일이 발견될 경우, 복합 위협 지능 및 속성을 기준으로 평판을 쉽게 확인할 수 있습니다.

향상된 위협 분석

파일에 대해 더 많은 정보가 필요한 경우 McAfee Threat Intelligence Exchange에서 McAfee Advanced Threat Defense로 자동으로 전송해서 즉시 잠재적인 신규 위협에 대한 추가 정보를 확인할 수 있습니다. 이 두 프로그램은 정적 및 동적 코드 분석의 위협 분석을 이용하여 문제의 파일에 대한 평판을 확인합니다. 이러한 모든 기능은 전체 보안 에코시스템 보호를 위해 McAfee Data Exchange Layer를 통해 자동화 및 문서화되며 종합적으로 공유됩니다.

보안 이벤트 관리

McAfee Enterprise Security Manager는 McAfee Threat Intelligence Exchange로 확인된 IoC를 조사할 때 보다 심도 있는 조사가 가능하게 해줍니다. 이전 보안 정보에 액세스할 수 있고 자동화된 감시 목록을 생성할 수 있으므로 조직의 보안 효율성이 증가됩니다.

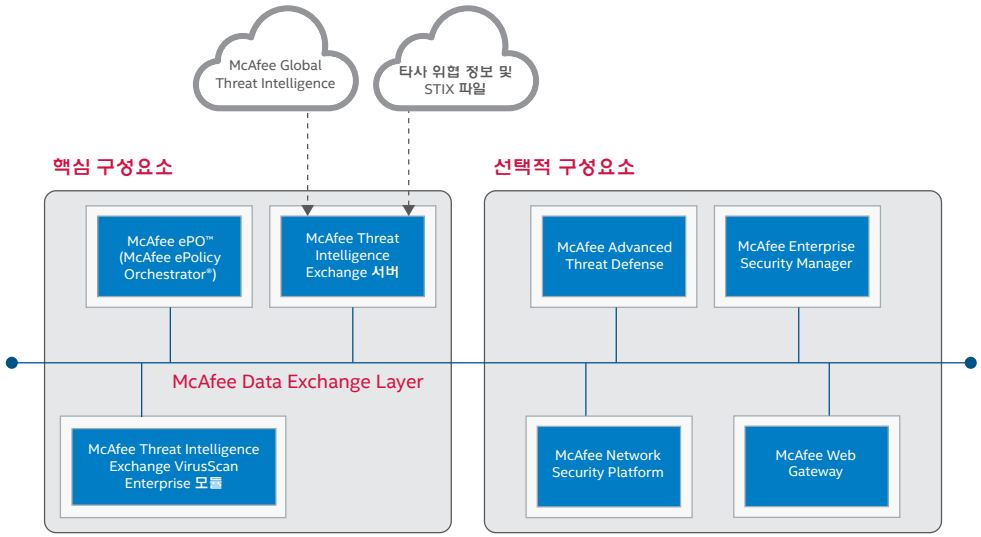

그림 1. McAfee Data Exchange Layer를 통한 통합 간소화로 구현 및 운영 비용을 줄이고 Security Connected 플랫폼의 발전을 능가하는 뛰어난 운영 효율성을 제공합니다.

1. http://www.verizonenterprise.com/DBIR/2015/

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

62276ds_threat-intelligence-exchange_0216