Cisco Advanced Malware Protection for Meraki MX

이점

- **위협에 대한 가시성 확보:** 네트워크 내부 및 다수의 브랜치 환경 전반에서 지원
- **보안 관리 간소화:** 클라우드 기반 네트워크 보안 플랫폼 활용
- **보안 침해를 신속하게 탐지, 분석, 치료:** 심층적 위협 가시성 활용
- **네트워크 방어 강화:** 글로벌 위협 인텔리전스 활용
- **복잡성 감소:** 단일 웹 기반 대시보드를 통해 클라우드에서 보안 서비스를 관리
- **비용 및 시간 절감:** 구축 및 관리가 쉽고 경제적인 서브스크립션 서비스

지능형 위협 차단 기능을 갖춘 간소화된 클라우드 기반 보안 관리

제로데이 공격, APT(Advanced Persistent Threat), 악성코드는 확고한 동기를 가진 사이버 범죄자들이 얼마나 끊임없이 새로운 공격을 모색하는지 보여주는 몇 가지 예시에 불과합니다. 그리고 공격자는 조직에 침입하기 위한 새로운 방법을 찾아내고 있으므로, 보안 전문가는 이러한 사이버 공격에 맞서 싸우는 데 고군분투하고 있습니다. 효과적인 보안 솔루션을 조정하는 데 필요한 가시성, 툴, 전문 지식이 부족하기 때문입니다. 공격자는 이러한 보안 허점을 이용하여 탐지를 우회하고 악의적인 활동을 숨깁니다. 공격이 점점 더 지능화되고 있으므로 조직에서는 보안 솔루션을 사용하여 스스로를 보호해야 합니다.

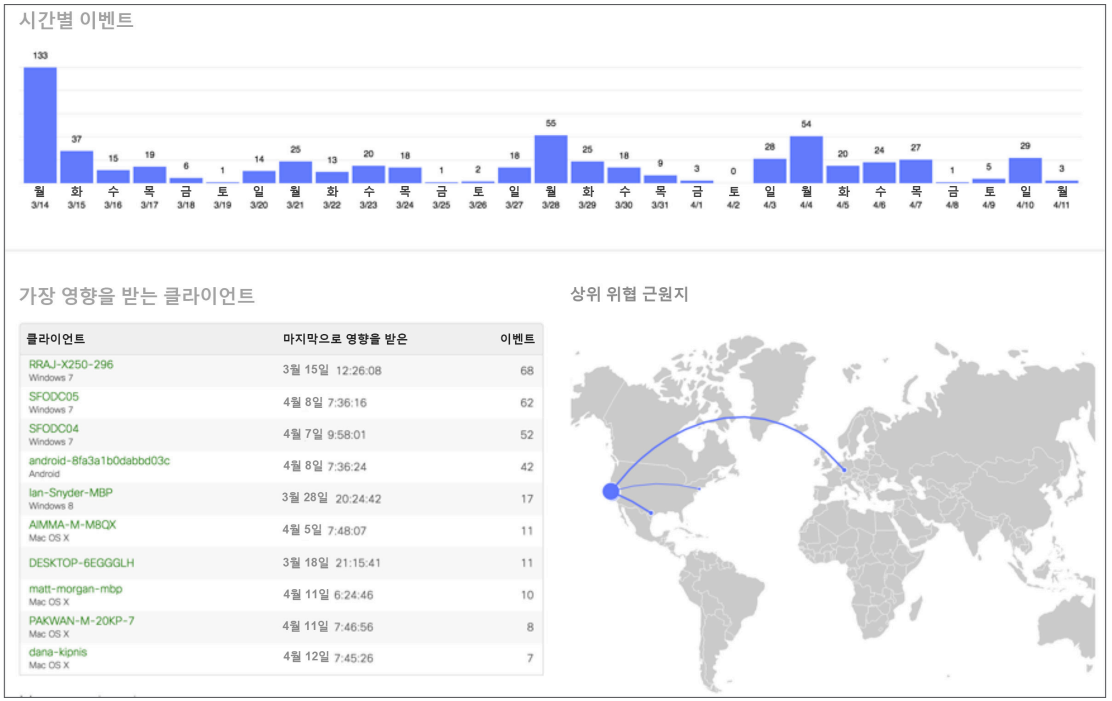
조직에서는 전체 네트워크에 걸쳐 뛰어난 가시성, 지속적인 제어, 지능형 위협 차단 기능이 그 어느 때보다도 필요합니다. Cisco® AMP(Advanced Malware Protection) for Meraki MX는 바로 이러한 수준의 보안을 제공합니다.

AMP + Meraki MX: 포괄적인 보안

Cisco AMP를 Meraki MX UTM(Unified Threat Management) 기반의 Threat Grid와 함께 사용할 경우 지능형 위협 차단 기능을 갖춘 클라우드 기반 관리 플랫폼을 제공합니다. 조직에서는 이 솔루션의 지능형 위협 차단 기능을 사용하여 기존의 탐지 툴이 가진 기능을 뛰어넘어 모든 브랜치 위치 및 원격 사무소 전반의 악성코드 위협에 대한 가시성을 확보할 수 있으므로, 보안 침해를 신속하게 탐지, 억제, 치료하는 것이 가능합니다.

기능

- **향상된 위협 차단 기능:** AMP는 네트워크 경계에서 업계 최고의 위협 차단 기능을 제공하여 보안 침해가 발생하기 전에 공격을 차단할 수 있도록 지원합니다.
- **지속적인 파일 모니터링:** AMP는 파일 활동을 지속적으로 모니터링, 분석 및 기록하여 1차 방어선을 우회한 악성코드를 빠르게 탐지함으로써 보안 침해 범위를 파악하고 신속히 대응할 수 있도록 합니다.
- **회귀적 알림:** AMP는 네트워크에 들어오는 악성 파일을 관리자에게 회귀적으로 알리며, 네트워크 진입 시 해당 파일의 악성 여부가 알려지지 않은 경우에도 마찬가지입니다.
- **지능형 악성코드 분석:** 고도로 안전한 환경에서 대규모의 행동 분석 지표 세트를 바탕으로 악성코드를 실행하고 분석하여 이전에 알려지지 않았던 제로데이 위협을 찾아낼 수 있습니다.
- **중앙 집중식 보안 관리:** 이 솔루션은 단일한 중앙 위치에서 보안, 네트워크, 애플리케이션 제어를 관리할 수 있는 기능을 갖춘 올인원(all-in-one) 클라우드 매니지드 네트워크 보안 플랫폼을 제공합니다.
- **Talos 위협 연구:** AMP는 글로벌 Talos 데이터베이스를 기반으로 네트워크에 들어오는 모든 파일을 확인하여 해당 파일의 악성 여부를 판별합니다.



분산된 환경의 대기업 및 중소기업에 적합한 AMP for Meraki에서는 다음 기능을 제공합니다.

위협에 대한 심층적인 가시성

오늘날 사이버 공격은 은밀하게 이루어집니다. 이러한 공격을 차단하려면 여러 사이트 전반에 걸쳐 지속적으로 네트워크의 위협 환경에 대한 가시성을 제공하는 솔루션이 필요합니다. AMP for Meraki MX는 기존의 탐지 기능을 뛰어넘어 전체 네트워크에 걸쳐 파일 및 트래픽 활동을 지속적으로 캡처하고 분석합니다. 이 경우 네트워크 전체에서 일어나는 상황에 대한 가시성을 높일 수 있습니다.

탐지 소요 시간 단축

위협은 얼마든지 침투할 수 있으며 실제로 발생하는 일입니다. 이러한 일이 발생할 경우, 이를 신속하게 탐지하고 조치를 취해야 합니다.

보안 팀은 AMP for Meraki를 통해 회귀적 악성코드 알림을 활용할 수 있습니다. 이러한 알림은 악성인 것으로 확인된 파일이 네트워크 경계를 이미 통과한 경우 고객에게 이를 알려 탐지 소요 시간을 단축합니다.

지능형 샌드박싱 기능

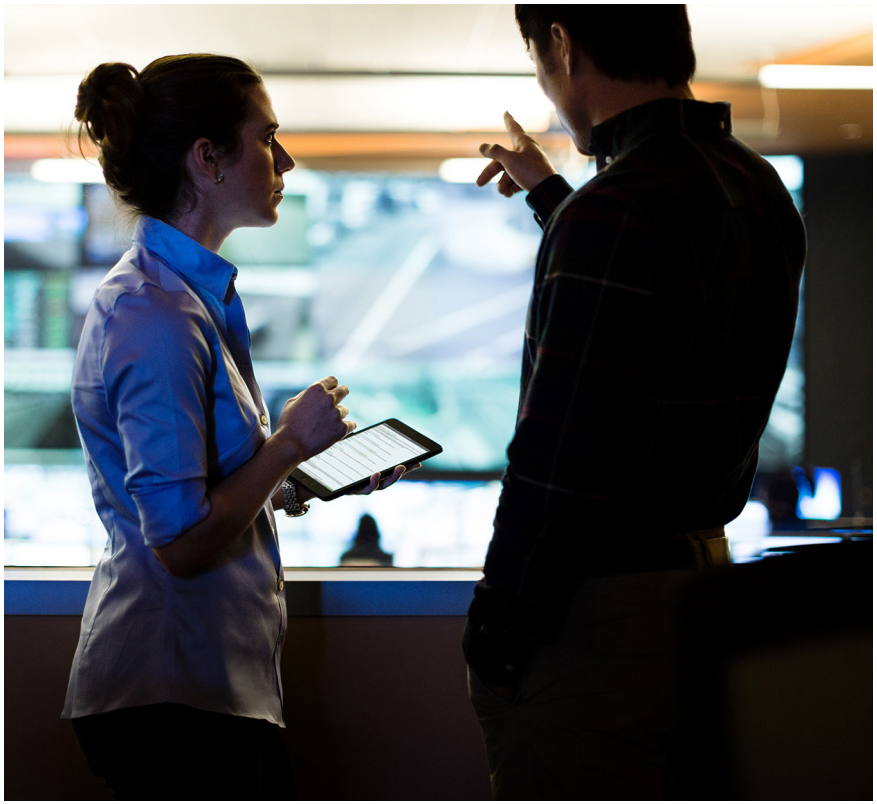
Meraki MX 기반의 Threat Grid에서는 지능형 샌드박싱 기술을 통해 가장 정교한 악성코드에 대해서도 심층적 가시성을 제공합니다. 보안 관리자는 알 수 없는 파일을 클라우드 또는 온프레미스 샌드박스에 전송할 수 있으므로, 해당 악성코드를 가상 환경에서 안전하게 실행하고 악성 콘텐츠인지 여부를 검사할 수 있습니다. 이를 통해 보안 팀은 악성코드가 어떤 일을 하고 있는지, 영향을 미치는 프로세스는 무엇인지, 어떤 사항을 변경하고 있는지 파악할 수 있습니다. 이러한 기능을 사용하여 그 어느 때보다 더욱 정확한 상황 기반 분석이 가능합니다.

간소화된 보안 관리

Meraki MX UTM은 단일한 중앙 위치에서 보안, 네트워킹, 애플리케이션 제어를 관리할 수 있는 기능을 갖춘 올인원(all-in-one) 클라우드 매니지드 네트워크 보안 플랫폼을 제공합니다. 조직에서는 Meraki의 운영 효율성 및 간소화된 관리의 이점을 누리는 동시에, AMP에서 제공하는 동급 최고의 위협 차단 및 악성코드 분석 기능을 사용할 수 있습니다.

다음 단계

Meraki MX 기반의 Cisco AMP를 통해 지능형 사이버 공격으로부터 조직을 방어하는 방법에 대한 자세한 내용은 Cisco 세일즈 담당자 또는 채널 파트너에게 문의하여 주십시오.
자세한 내용은 https://meraki.cisco.com/amp를 참조하십시오.



C45-737164-00 05/16