한눈에 보기

이점

- **지능형 위협 탐지:** AMP for Web Security는 공격 전, 중, 후에 걸친 전 범위에서 모든 웹 관련 위협을 종합적으로 차단합니다.
- **지속적 분석 및 회귀적 보안:** 파일이 웹 게이트웨이를 지난 후에도 AMP는 이 파일의 초기 성향과 관계없이 행동을 지속적으로 감시하고 분석하고 기록합니다. 악의적 행동이 사후에 관찰되면 AMP는 악성코드를 격리하고 치료할 수 있도록 회귀 알림을 보냅니다.
- **강화된 네트워크 방어:** AMP for Web Security는 빅 데이터와 뛰어난 보안 인텔리전스를 바탕으로 구축되었습니다. Cisco Talos 그룹이 매일 수백만 개의 악성코드 샘플과 테라바이트 단위의 데이터를 분석하여 그 결과로 얻어진 정보를 AMP로 보냅니다. AMP는 이 풍부한 상황 정보를 기준으로 파일, 텔레메트리 데이터 및 파일 행동의 상관관계를 분석하여 알려진 위협과 새롭게 등장하는 위협을 사전에 차단합니다.

Cisco Advanced Malware Protection for Web Security

정교한 위협에 대응하는 정교한 웹 보안

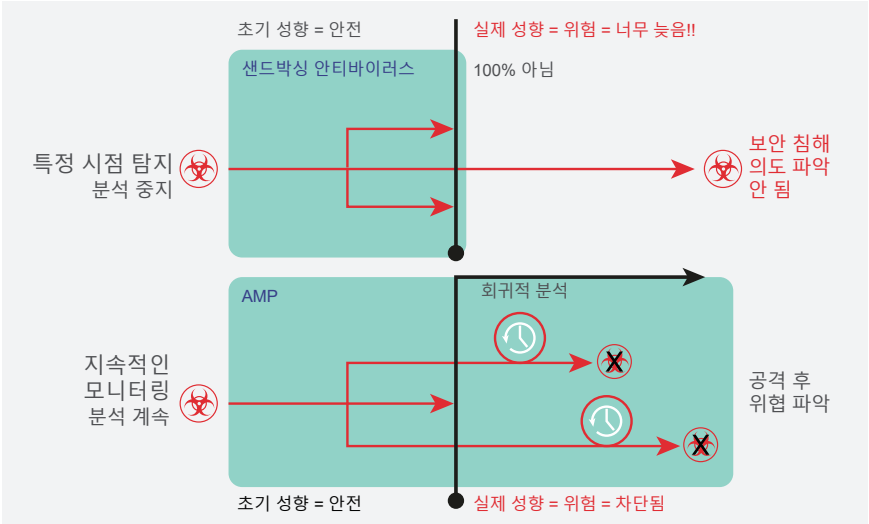
오늘날 효과적으로 웹 보안을 유지하려면 단순히 악성 웹사이트를 차단하는 것만으로는 부족합니다. 합법적인 웹사이트를 통해서도 바이러스나 악성코드가 다운로드될 수 있습니다. 모바일 액세스, 소셜 미디어, 인터랙티브 애플리케이션과 관련하여 새로운 취약점이 발견되었습니다. 웹 위협이 지속적으로 증가함에 따라 위협 탐지, URL 필터링 및 애플리케이션 제어에 있어 더욱 혁신적인 솔루션이 필요하게 되었습니다.

보안 팀이 가장 은밀한 위협도 잡아낼 수 있도록 지속적인 모니터링과 분석을 제공하는 웹 보안 솔루션이 필요합니다. CTA(Cognitive Threat Analysis) for WSA가 탑재된 Cisco® AMP(Advanced Malware Protection)가 해답이 될 것입니다.

AMP가 중요한 이유

기존 웹 보안 수단은 오늘날의 지능형 위협을 충분히 막아내지 못합니다. Cisco의 웹 보안 솔루션에 AMP를 추가함으로써 기존의 웹 보안 기능에 더불어 지능형 공격을 차단하는 지능형 위협 차단 기능을 제공합니다.

그림 1. AMP를 사용한 회귀적 분석



AMP는 악성코드 탐지, 차단, 지속적 분석, 회귀 알림(그림 1)을 Cisco Web Security Appliance 라이선스에 추가합니다 제공되는 기능은 다음과 같습니다.

- **유연성 및 다양한 옵션:** 기존 Cisco 보안 게이트웨이와 AMP의 통합이 지원되므로 사용자 환경에 가장 이상적인 AMP를 구축할 수 있습니다.

- **진화된 샌드박싱:** 네트워크에 침입을 시도한 파일의 행동, 평판, 위협 수준에 대해 풍부한 데이터를 기반으로 하는 상세한 분석을 제공합니다. 사용자 환경에 가시성과 제어 기능을 제공합니다.
- **네트워크 내에서 작동하는 위협 검색 시간 단축:** 웹 프록시를 보안 센서로 변환하여 자동으로 의심스러운 웹 트래픽을 검사합니다.

다음 단계

Cisco AMP for Web Security에 대한 자세한 내용은 http://www.cisco.com/go/ampforweb 를 참조하십시오.

Cisco 세일즈 담당자, 채널 파트너, 시스템 엔지니어와 함께 여러분 회사에 얼마나 효과적으로 Cisco 제품을 적용할 수 있는지 평가해 보십시오.

- **파일 평판:** AMP는 Cisco Web Security 게이트웨이를 통과하는 각 파일의 지문을 캡처하여 평판을 판정할 수 있도록 Cisco의 클라우드 기반 인텔리전스 네트워크에 전송합니다. 판정 결과에 따라 악의적인 파일을 자동으로 차단하고 관리자가 정의한 정책을 적용할 수 있습니다.
- **파일 분석:** AMP Threat Grid 기술을 바탕으로 웹 게이트웨이를 통과하는 알 수 없는 파일의 정적 및 동적 분석(샌드박싱)이 가능합니다. Threat Grid는 파일 행동과 위협 수준에 대한 상세한 정보를 얻기 위해 글로벌 위협 인텔리전스와 함께 700개 이상의 행동 지표를 사용해 고도의 보안 환경에서 샘플을 분석합니다.
- **파일 회귀 분석:** AMP는 경계 방어를 회피한 악성 파일 문제를 해결합니다. 또한 파일의 초기 성향과 관계없이 보안 게이트웨이를 통과 하는 파일을 지속적으로 분석 합니다. 파일이 위협으로 식별되면 AMP는 회귀적 알림을 보내고, 네트워크의 누가, 언제 감염되었는지 보여줍니다. 따라서 보안 팀은 공격이 확산되기 전에 빠르게 파악하여 해결할 수 있습니다.

Cognitive Threat Analytics로 AMP를 보완하여 가시성 증가

Cisco 클라우드 기반 Cognitive Threat Analytics 솔루션은 Web Security Appliance의 AMP 애드온 라이선스로 이용할 수 있습니다. Cognitive Threat Analytics를 통해 이미 진행 중이거나 해당 환경에 침입하고자 시도 중인 정교하고 은밀한 공격을 탐지하고 대응할 수 있습니다.

AMP for Web Security와 Cognitive Threat Analytics를 통합하면 다음을 수행할 수 있습니다.

- 의심스럽거나 악성인 웹 기반 트래픽을 자동으로 식별하고 조사합니다.
- 추가 하드웨어나 소프트웨어가 없어도 기존 웹 보안 솔루션에서 생성된 정보를 분석합니다.
- 조직을 공격하는 데 사용할 수 있는 암호화된 표준 익명 채널을 비롯하여 웹 기반 통신을 사용하고 보안 제어를 우회하는 악의적인 활동을 집중적으로 감시합니다.
- 정상적인 활동의 기준을 정하고 네트워크 내에서 발생하는 비정상적인 트래픽을 식별합니다.
- 디바이스 행동 및 웹 트래픽을 분석하여 커맨드 앤 컨트롤 커뮤니케이션과 데이터 유출을 찾아냅니다.

Cisco CTA(Cognitive Threat Analytics)에 대한 자세한 내용은 www.cisco.com/go/cognitive 를 참조하십시오.

C45-730851-03 10/16