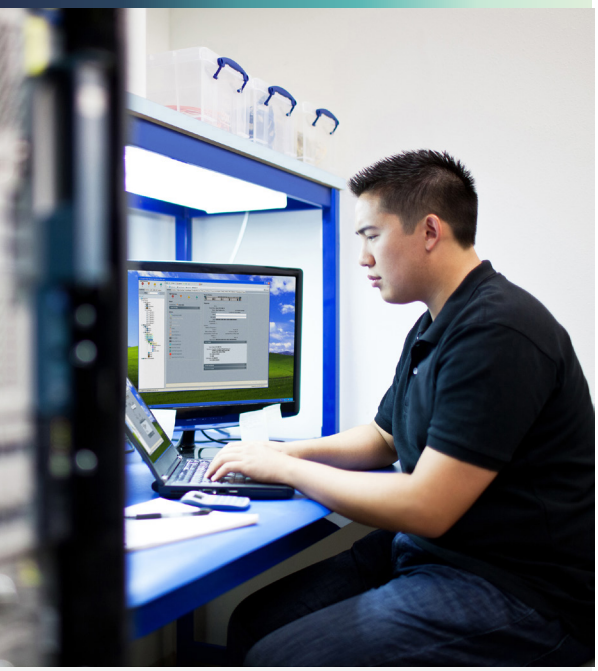
한눈에 보기



Advanced Malware Protection for Cisco Email Security

장점

- **보호:** 랜섬웨어나 Cryptoworm 같은 피싱 이메일 공격으로부터 보호합니다.
- **위협에 대한 이메일 분석:** 제로데이 공격과 파일 첨부 및 악성 URL에 숨겨진 공격 같은 위협에 대해 이메일을 분석합니다.
- **복합적 공격 차단:** 다른 AMP 구축과 통합함으로써 다중 위협 벡터에 걸쳐 복합적인 공격을 차단합니다.
- **은밀한 악성코드 발견:** 고급 샌드박싱 기능으로 은밀한 악성 코드를 찾아내고 어떻게 작동하는지 이해합니다.
- **탐지 시간 단축:** 회귀적 알림을 통해 탐지 시간을 단축합니다.
- **알 수 없는 파일 추적:** 지속적 파일 분석과 더불어 이메일 게이트웨이를 통과한 알 수 없는 파일을 추적합니다.

가장 은밀하게 침투하는 이메일 기반 공격 차단

오늘날의 조직은 급증하는 이메일 기반 공격에 직면해 있습니다. 스피어 피싱부터 표적성 공격에 이르기까지 사이버 공격은 네트워크에 침입하기 위해 이메일을 가장 주된 방법으로 사용하고 있습니다. 기존의 탐지 툴은 악성코드가 침입하면 잠재적 위협이 있는 활동에 대한 가시성을 제한적으로 제공하거나 전혀 제공하지 못합니다. IT 보안 팀은 이를 파악할 수 없어 신속한 조치가 불가능합니다. 그 결과 조직에 매일 보안 침해가 발생합니다.

따라서 공격의 전, 중, 후의 전 범위에 걸친 가시성을 제공할 수 있는 이메일 보안 솔루션을 구축하는 것이 중요합니다. AMP(Advanced Malware Protection) for Cisco® Email Security는 이메일 게이트웨이에서 지능형 악성코드의 전체 사이클을 처리하고, 기존 방어를 회피하는 가장 은밀한 이메일 공격을 차단해 줄 수 있는 유일한 시스템입니다.

AMP for Email Security를 선택해야 하는 이유

Cisco 이메일 보안 솔루션에 AMP를 추가함으로써 안티바이러스나 안티스팸 툴 같은 기존의 이메일 보안 기능과 더불어 지능형 위협 차단 기능을 추가하여 위협 보호 수준을 한 단계 높일 수 있습니다.

이러한 솔루션을 함께 사용하면 이메일 내용과 트랜잭션을 확인하고 실시간 위협 인텔리전스를 사용해 이를 분석할 수 있습니다. 그뿐만 아니라 회귀적 탐지 알림을 구축해 초기 방어선을 통과하여 향후에 악성으로 변화하는 코드를 추적할 수 있습니다.

공격 전, 중, 후에 대한 방어

Cisco Email Security 솔루션에 AMP 서브스크립션을 추가해 다음과 같은 이점을 누릴 수 있습니다.

공격 전: Cisco Talos의 실시간 위협 인텔리전스로 방어를 강화합니다. 이메일 내용과 트랜잭션을 확인하고 악성 콘텐츠는 자동으로 차단됩니다.

공격 중: AMP는 파일 평판을 이용해 게이트웨이를 통과하는 각 파일의 지문을 모두 캡처하여 파일 평판 판단을 위해 AMP의 클라우드 기반 인텔리전스 네트워크에 전송합니다. 최신 샌드박싱 기술을 사용하여 악성코드를 탐지할 수 있으며, 보안 관리자는 이를 통해 정확하고 상세하게 파일의 행동과 위협 레벨을 알아낼 수 있습니다.

공격 후: AMP는 지속적 파일 분석을 이용해 게이트웨이를 통과하고 향후 위협으로 간주된 악성 파일을 찾아낼 수 있습니다. AMP는 네트워크상에서 누가, 언제 감염되었는지를 보여주는 회귀적 알림을 전달합니다.

다음 단계

AMP for Email Security를 이용하여 지능형 사이버 공격으로부터 조직을 방어하는 방법에 대한 자세한 내용은 www.cisco.com/go/ampforemail를 참조하거나 Cisco 세일즈 담당자 또는 채널 파트너에게 문의하여 주십시오.

C45-730848-03 07/16