한눈에 보기

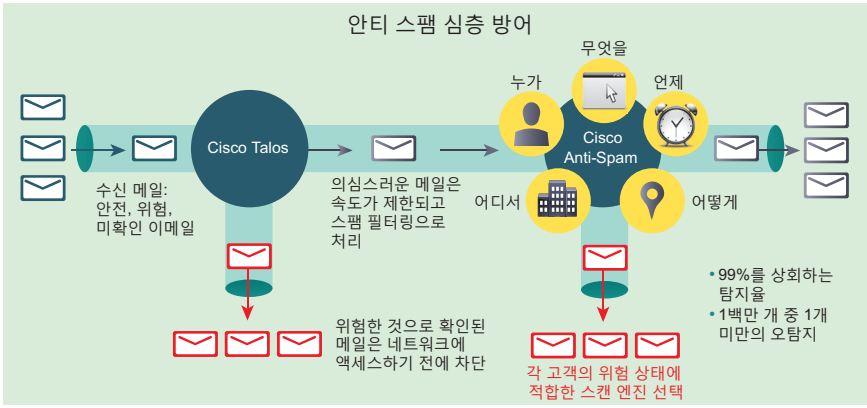
장점

- **더 신속하고 포괄적인 이메일 보호:** 일반적으로 경쟁업체보다 몇 시간 또는 며칠 앞서 조치 가능
- **최대 규모의 위협 인텔리전스 네트워크 중 하나에 액세스:** 실시간 종합 보안 분석에 기반한 Cisco Talos 사용
- **아웃바운드 메시지 보호:** 온디바이스(on-device) 데이터 유출 방지 (DLP), 이메일 암호화, RSA의 Enterprise DLP 솔루션과의 선택적인 통합 활용
- **총 소유 비용 절감:** 작은 설치 공간, 간편한 구현, 장기적인 절감 효과가 있는 자동화된 관리
- **최대 구축 유연성 확보:** 온프레미스, 클라우드, 하이브리드 구축으로 유연성 확보 계약 기간 동안 언제든지 구축 조합 변경 가능

Cisco Email Security Appliance

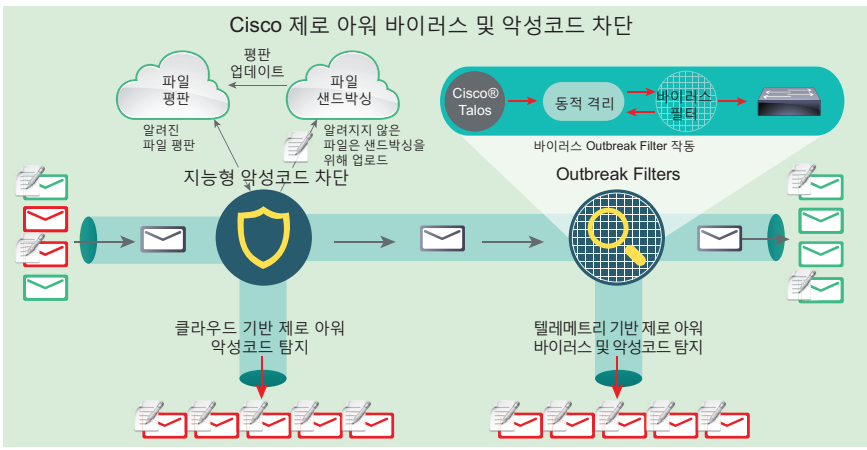
이메일 기반 공격으로부터 비즈니스 보호

이메일은 중요한 비즈니스 통신 툴이지만 해결하기 어려운 위협에 노출될 수 있습니다. Radical Group의 "Email Statistics Report, 2012-2016"에 따르면, 보안 침해의 평균 비용은 450만 달러에 달합니다. 그리고 이메일 게이트웨이는 보안 침해의 가장 큰 위협 벡터입니다. 정교한 표적 공격은 개인 정보 및 소셜 엔지니어링 전술을 사용하여 사용자를 속이고 악성코드를 퍼뜨리는 악의적인 사이트로 연결합니다.



오늘날의 이메일 기반 위협에 대응하려면 기존의 공격과 진화하는 공격으로부터 시스템을 안전하게 보호할 수 있는 전용 리소스, 기술 및 전문 지식이 필요합니다. Cisco® ESA(Email Security Appliance)는 이러한 지능형 위협에 한 발 앞서 대응함으로써 받은 편지함을 매우 안전하게 보호합니다.

이 올인원(all-in-one) 어플라이언스는 스팸, 지능형 악성코드, 피싱 및 데이터 유출을 방어합니다. 간단한 애드온 라이선스로 사용할 수 있는 Cisco의 AMP(Advanced Malware Protection) 기능은 위협을 차단하고, 공격 범위를 차단하며, 공격 후 신속하게 치료하여 공격 전, 중, 후 전 단계에서 지속적인 보호를 제공합니다. 그리고 AMP 시스템은 Threat Grid 어플라이언스와 함께 AMP 프라이빗 클라우드 라이선스를 이용하여 완벽한 온프레미스 구축이 가능합니다. 이는 AMP 퍼블릭 클라우드 사용을 허용하지 않는 엄격한 정책 요구 사항을 가진 고객에게 대단히 중요합니다.



"Cisco 덕분에 총 소유 비용을 크게 줄이고 바이러스와 스팸을 퇴치하는 새로운 기능도 갖추게 되었습니다."

Kenichi Tabata
Komatsu Ltd., Japan

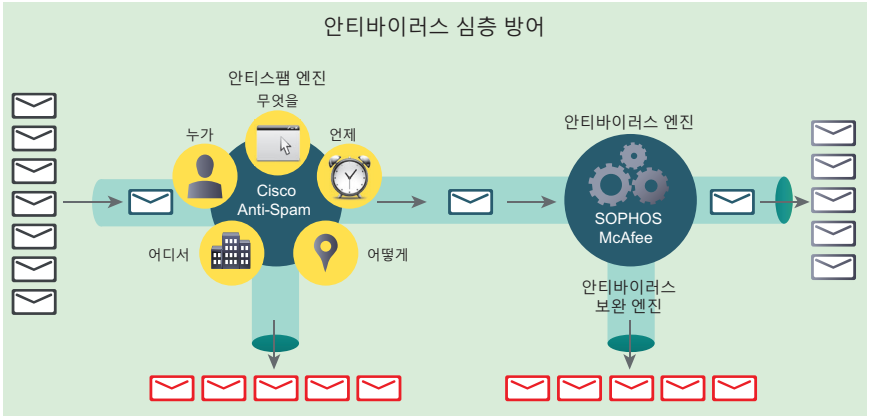
다음 단계

자세히 보기

Cisco ESA에 대한 자세한 정보는 http://www.cisco.com/go/esa를 참조하십시오. Cisco 세일즈 담당자, 채널 파트너 또는 시스템 엔지니어와 함께 여러분 회사에 얼마나 효과적으로 Cisco 제품을 적용할 수 있는지 평가해 보십시오.

멀티 레이어 방어를 구축하여 여러 위협 차단

Cisco ESA에 통합된 Cisco Talos 서비스는 글로벌 트래픽 활동 상황에 대한 24시간 가시성을 제공합니다. 이 인텔리전스를 통해 이상 징후를 분석하고, 새로운 위협을 발견하며, 트래픽 트렌드를 모니터링할 수 있습니다. 또한 자동 정책 업데이트가 3분에서 5분 간격으로 네트워크 디바이스에 적용됩니다.



스팸이 편지함에 도달하는 것도 쉽게 막을 수 있습니다. 발신자의 평판 및 유효성을 기준으로 필터링하는 외부 레이어와 메시지를 심층적으로 분석하여 필터링하는 내부 레이어가 결합된 멀티레이어 방어 기능이 제공됩니다.

위조 이메일 탐지를 이용하여 스푸핑 공격을 차단할 수 있습니다. 이러한 표적성 공격은 고가치 표적으로 알려진 경영진에게 초점을 맞춥니다. 이 기능은 모든 공격 시도와 관련 행동에 대한 자세한 로그 기록을 제공합니다.

ESA는 다음과 같은 기능도 제공합니다.

- 피싱 및 혼합 위협 차단
- 그레이메일 식별 및 "안전한 수신 거부" 옵션 태그 지정
- 키를 온프레미스나 클라우드에 저장하는 등 신뢰할 수 있는 보안 암호화를 통해 매우 안전한 메시징을 위한 요구 조건 충족
- 업계 및 정부의 데이터 유출 방지 규정준수
- 지능형 위협 및 표적 공격 방어
- 악성 URL을 클릭한 사용자 추적
- 세부적인 이메일 정책 설정 및 시행

물리적 어플라이언스, 가상, 클라우드 기반 구축 또는 하이브리드 구축 중에서 선택하여 비즈니스 요구사항을 충족하는 솔루션을 찾을 수 있습니다.

C45-728633-04 06/16