Cisco Email Security + AMP Threat Grid

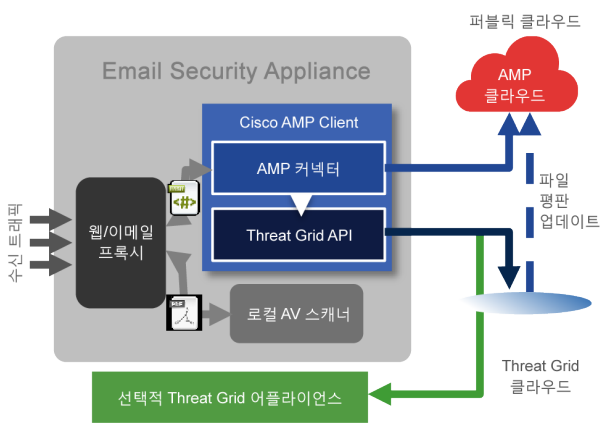
Cisco Email Security 9.5

제품 설명

2015 Cisco 연례 보안 보고서에 따르면 이메일은 사이버 공격의 가장 큰 위협 벡터입니다. 중요한 비즈니스 이메일을 스팸, 악성코드, 기타 위협으로부터 안전하게 보호합니다. 업계 최고의 Cisco 솔루션은 이메일 기반 위협을 차단하고 공격 전, 공격 중, 공격 후의 모든 단계에 걸쳐 지속적인 보호를 제공하므로 더 빨리 더 완벽하게 이메일을 보호할 수 있습니다.

활용 사례

- 공격 이전에 Cisco Email Security는 Cisco Talos Security Intelligence and Research Group의 전문지식을 활용합니다. Talos 위협 인텔리전스는 알려진 위협과 새로운 위협을 탐지, 분석하고 차단할 수 있습니다.
- 공격 중에 Cisco Email Security는 업계 최초로 검증된 제로아워(zero-hour) 안티바이러스 솔루션을 제공합니다. 이 솔루션은 중요한 아웃바운드 이메일을 제어하고 암호화할 수 있는 동급 최고의 기능을 제공합니다. 그와 동시에, 단일한 어플라이언스에 구축된 계층형 방어로 들어오는 공격을 신속하게 차단합니다.
- 공격 후에 Cisco AMP(Advanced Malware Protection)와 함께 Cisco Email Security는 이메일 게이트웨이를 통과한 후에도 위협을 지속적으로 분석할 수 있도록 파일 평판 점수 및 차단, 정적 및 동적 파일 분석, 파일 회귀 분석 등의 기능을 제공합니다. 사용자는 더 많은 공격을 차단하고, 의심스러운 파일을 추적하며, 문제 발생의 범위를 완화하고, 신속하게 치료할 수 있습니다. 추가된 Cisco AMP Threat Grid 어플라이언스는 클라우드에 악성코드 샘플을 제출할 때 규정준수 또는 정책 제한사항을 적용해야 하는 조직에 온프레미스 어플라이언스를 통한 악성코드 분석 기능을 제공합니다.



AMP Threat Grid 포털 서브스크립션

제품 설명

AMP Threat Grid는 폐쇄된 커뮤니티에서 악성코드 샘플을 안전하게 크라우드 소싱하여 악성코드 공격, 캠페인 및 분산에 대한 정보를 전체적으로 보여주는 최초의 통합 악성코드 분석 및 위협 인텔리전스 솔루션입니다. 고객은 샘플의 특성을 수백만 개의 다른 샘플과 연결하여 잠재적 악성 파일을 신속하게 파악함으로써 주요 행동 지표에 대한 통찰력을 제공하여 광범위한 위협을 효율적으로 방어할 수 있습니다.

활용 사례

- AMP Threat Grid는 단일 솔루션에서 지능형 악성코드 분석을 심층적인 위협 분석 콘텐츠와 결합하여 후배 보안 분석가와 리버스 엔지니어가 조직을 사전대응적으로 방어할 수 있도록 역량을 강화하는 악성코드 분석 및 위협 인텔리전스에 대한 통합된 접근 방식을 제공합니다.
- AMP Threat Grid 포털에서는 효율적이고 효과적으로 대응해야 하는 리버스 엔지니어 및 사고 대응자에게 심층적인 악성코드 분석 및 데이터 전환 기능을 제공합니다.
- AMP Threat Grid를 사용하는 고객은 강력한 API에 액세스하여 기존 보안 기술(방화벽, 프록시, 게이트웨이 등)의 샘플 제출을 통합 및 자동화함으로써 기존 IT 보안 인프라의 기능을 강화할 수 있습니다.
- AMP Threat Grid에서는 하이파이(Hi-Fi) 분석 콘텐츠를 통해 후배 보안 운영 분석가가 사고에 신속하게 대응하도록 지원하고 향후 위협에 대해 사전에 대해 알려주는 직관적인 웹 포털을 제공합니다. 또한 이 포털에서는 세부적인 위협 점수 분석, 분석에 대한 비디오 재생, 글로브박스(Glovebox)를 통한 악성코드와 사용자 상호작용 기능을 제공합니다.
- 악성코드 분석 콘텐츠의 폐쇄형 소스 저장소를 통해 AMP Threat Grid는 고객의 고유한 보안 요건에 맞게 사전 패키지화되거나 사용자 지정된 자동화된 위협 정보 피드를 제공합니다.

Cisco Email Security + AMP Threat Grid

기능	AMP Threat Grid를 통한 이메일 보안	AMP Threat Grid 서브스크립션
SPAM 차단	✔	
그레이메일 탐지	✔	
발신자 기본 평판 필터	✔	
URL 위협 차단	✔	
안티바이러스	✔	
피싱 보호	✔	
이메일 암호화	✔	
웹 상호작용 추적	✔	
보안 침해 필터	✔	
데이터 유출 방지	✔	
이름 및 SHA256의 단순 검색	✔	✔
클라우드 또는 온프레미스 구축	✔	✔
네트워크, 프로세스, 아티팩트 및 파일 활동 보고서	✔	✔
행동 지표	✔	✔
위협 점수		✔
PCAP, JSON 다운로드		✔
샘플, 관련 아티팩트, 비디오 다운로드		✔
위협 정보 컨텍스트 및 상관 관계(하이퍼링크로 보고서 상호 전환)		✔
글로브박스(Glovebox)의 악성코드 샘플과 상호 작용		✔
레지스트리 활동 보고서/레지스트리 콘텐츠 JSON 다운로드		✔
프로세스 그래프 및 프로세스 타임라인 JSON		✔
고급 검색(샘플, 아티팩트, IP, 레지스트리, sURL 등)		✔
샘플 업로드 자동화를 위한 API 통합		✔
위협 정보를 SIEM, 시각화 툴 등으로 API 통합		✔
위협 정보 피드		✔

Cisco® AMP Threat Grid는 전사적 범위에서 여러 보안 기능을 강화합니다.

자세히 보기

AMP Threat Grid에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.
http://www.cisco.com/go/amptg