한눈에 보기

Cisco Email Security 솔루션

오늘날의 이메일 기반 위협에 대응하려면 기존의 공격과 진화하는 공격으로부터 조직을 보호할 수 있는 전용 리소스, 기술 및 전문 지식이 필요합니다. Cisco® Email Security는 이러한 지능형 위협에 한 발 앞서 대응함으로써 받은 편지함을 매우 안전하게 보호합니다. 이 올인원(all-in-one) 솔루션은 스팸, 지능형 악성코드, 피싱 및 데이터 유출을 방어합니다.

자세한 내용은 Cisco Account Manager에게 문의하거나 www.cisco.com/go/emailsecurity에서 문의하십시오.

표적 공격 방지

아키텍처	Cisco 솔루션
차세대 탐지	**지원됨:** 이메일 보안을 위한 차세대 탐지 기능에서는 내부 및 외부 이메일에 포함된 위협 소스와 기타 소스의 텔레메트리를 활용합니다. Cisco에서는 이메일 보안, 웹 보안, IPS, 방화벽, 파일 기록 및 지능형 악성코드에 대한 강력한 글로벌 입지를 구축하고 있습니다. 이러한 제품의 텔레메트리를 결합하여 모든 Cisco Security 제품에 사용되는 풍부한 보안 정보를 제공합니다. Talos 팀은 Cisco에서 위협 인텔리전스를 제공합니다. Talos
URL 재작성	**지원됨:** Cisco ESA를 사용하면 메시지의 모든 URL을 재작성하거나 위협 인텔리전스를 사용하여 URL의 위험을 확인하고 선택적으로 재작성할 수 있습니다. 선택적 재작성은 메시지를 변칙 이메일 흐름에 연결하는 대신 메시지 상황과 URL 평판을 기반으로 합니다. 모든 URL을 재작성하면 메시지가 차단되고 비효율성으로 인해 최종 사용자가 불만을 갖고 이탈하게 되므로 선택적 재작성은 매우 탁월한 방법입니다. URL 평판 정보, 범주화 및 샌드박싱에서는 Cisco Cloud Web Security를 사용합니다. Cisco의 클라우드 웹 프록시 기술은 Cisco의 소유이며 업계 최고의 기술로 인정 받고 있습니다. Cloud Web Security
재작성된 URL은 기존 보안 투자를 지원	**지원됨:** 재작성된 URL을 클릭하면 맞춤형 알림 페이지를 사용하여 악의적인 것으로 탐지된 콘텐츠를 차단합니다. 허용되는 콘텐츠로 간주되는 경우 알림을 확인하라는 메시지가 표시되고 연결이 재설정되어 웹 트래픽에서 기본 또는 로컬 Web Security 어플라이언스 또는 서비스를 사용하게 됩니다. Defending Against Targeted Attacks
전송하기 전에 URL 분석	**지원됨:** URL을 전체 이메일 본문의 중요 부분으로 분석합니다. 이 분석에는 웹 평판, 카테고리 등과 같은 기준이 포함됩니다. 그런 다음 익명 이메일 트래픽 흐름과 관련해 잘못된 URL인지 정상 URL인지를 판정합니다.
클릭한 URL에 대한 고정 분석	**지원됨:** 웹 상호작용 추적에서는 사용자 활동을 중심으로 다른 중요 공격 정보를 제공하는 데 주력합니다. Cisco의 웹 상호작용 추적 기능은 "잘못된" URL뿐만 아니라 재작성(웹 범주화 및 평판 기반 재작성 포함)된 모든 URL을 클릭하는 사용자를 보호합니다. 또한 웹 상호작용 추적은 대화 상자에 직접 통합되며 모든 보고 온박스(On-box)를 통한 보안 침해 필터에 따라 재작성된 URL과 정책에 따라 재작성된 URL을 모두 추적할 수 있습니다. Defending Against Targeted Attacks
동적 분석(샌드박싱)	**지원됨:** Cisco Email Security에서는 URL 및 첨부 파일의 샌드박싱뿐만 아니라 동일한 상자에 심층 악성코드 분석도 함께 제공할 수 있습니다. 특정 경쟁사에서는 바이러스로 알려진 첨부 파일을 포착하기 위해 안티바이러스 기술을 사용합니다. 하지만 다시 쓸 URL을 선택하는 것과 마찬가지로 악성코드 분석을 적용할 첨부 파일을 선택하는 것은 변칙 이메일 트래픽 흐름에 연결된 메시지에 따라 다릅니다. 악성코드 분석 프로세스는 첨부 파일의 기록과 관련이 없습니다. What is AMP Malware Protection AMP on ESA Cisco Cloud Web Security 데이터 시트(URL 샌드박싱)

예측 방어	**지원됨:** 예측 방어를 적용하려면 서드파티 서비스의 피드를 포함하여 위협 정보를 구성해야 합니다. Cisco에서는 Talos에서 수집한 데이터를 사용하여 제로 아워(zero-hour) 공격에 대한 심층적 위협 인텔리전스 소스를 제공합니다. Cisco에서는 전체 데이터에 대한 심층적 행동 분석을 사용하여 공격 전 범위에 걸쳐 상관관계가 있는 데이터를 제공할 수 있습니다.
Talos Security Intelligence and Research Group	**지원됨:** Cisco에서는 전체 데이터에 대한 심층적 행동 분석을 사용하여 제로 아워(zero-hour) 공격을 방어할 수 있습니다. Talos
포렌식	**Cisco 솔루션**
공격에 대한 대시보드 가시성	**지원됨:** Cisco Email Security에서는 보고 및 세부 메시지 추적을 기반으로 공격에 대한 가시성이 제공됩니다. Cisco Outbreak Filters, Advanced Malware Protection 파일 분석, 잘못된 URL, 회귀적 보안 보고서 등의 데이터를 비롯하여 보안과 관련한 구체적인 정보가 필요한 고객은 이러한 모든 데이터를 "My Reports(내 보고서)"에 보관할 수 있습니다. Advanced Malware Protection 사용 설명서(28-5페이지) AMP 대시보드(그림 3)
악성코드 상세 분석 정보	**지원됨:** Cisco ESA에서는 온박스(On-Box) 및 TALOS 사이트를 통해 악성코드 상세 분석을 제공합니다. 온박스(On-Box) 악성코드 분석 페이지에는 클라이언트 또는 SHA256 핑거프린트에 의해 제출되는 샌드박싱된 파일의 결과에 대한 세부사항이 제공됩니다. 또한 자세한 정보를 확인할 수 있도록 ThreatGrid 샌드박스 정보에 ESA의 링크를 제공합니다. 제로 데이 분석의 경우 Talos가 제어하는 Sourcefire VRT 웹 사이트에서 특정 파일에 대한 세부사항을 확인할 수 있습니다. AMP 지원 제품 및 Cisco FireSIGHT Management Center에서 심층적 포렌식 분석을 사용하여 이메일을 비롯한 엔터프라이즈 내의 모든 매체를 통한 공격에 대해 포렌식 세부사항을 제공할 수 있습니다. FireSIGHT Management Center AMP 대시보드(그림 3)
포렌식 세부사항 내보내기	**지원됨:** Cisco Email Security에서는 회귀적 파일 변경을 비롯하여 이메일 보안을 우회하는 악성코드에 대한 커스텀 보고서를 통해 포렌식 공격 정보를 내보낼 수 있습니다. 분석에 대한 정보를 PDF로 내보내고 JSON 형식으로 검색하여 다양한 플랫폼에서 사용할 수 있습니다. 판정 및 속성 정보가 로그에 표시되며, 추가적인 상관관계 및 분석을 위해 syslog를 통해 SIEM에 로그를 보낼 수 있습니다. 보고서가 이메일 관리자에게 정기 이메일로 전송되도록 예약할 수 있습니다. ESA의 AMP
온박스(On-Box) URL 상호작용 추적	**지원됨:** Cisco의 웹 상호작용 추적은 완전히 통합된 솔루션으로, IT 관리자가 ESA에서 재작성한 URL을 클릭한 최종 사용자를 추적할 수 있도록 해줍니다. 보고서에는 다음 내용이 표시됩니다. • 악성 URL 을 클릭한 상위 사용자 • 엔드 유저가 클릭한 상위 악성 URL • 날짜/시간, 재작성 이유, URL 에서 수행한 작업 관리자는 특정 URL이 포함된 모든 메시지를 역추적할 수도 있습니다.
최종 사용자 경험	Cisco 솔루션
지연 없이 전달되는 이메일	**지원됨:** 이 항목은 관리자가 구성할 수 있으며 사용자 정의할 수 있습니다. 기본적으로 첨부 파일은 격리되거나 보관되지 않지만 원하는 경우 그렇게 할 수 있습니다. Cisco에서 AMP를 ESA 및 WSA 어플라이언스에 추가
의심스러운 URL 처리	**지원됨:** URL은 정상적인 것처럼 보이지만 내용이 의심스러운 메시지에 전달되는 경우 Cisco Email Security에서는 수신자에게 웹 사이트로 계속 진행하기 전에 한 번 더 생각해 볼 수 있는 옵션을 제공합니다. 이 옵션 없이 리디렉션하면 위협에 취약할 수 있습니다. Cloud Web Security

피싱에 대한 방어	Cisco 솔루션
피싱 메시지에 대한 세분화되고 구성 가능한 정책	**지원됨:** Cisco의 세부 피싱 정책에서는 URL을 공격적으로 필터링하는 별도의 메일 정책, 공격적 안티 스팸 정책 또는 둘 모두를 작성합니다. 또한 해당 정책의 보안 침해 필터에서 메시지 수정을 지원합니다. 사용 설명서(14-1페이지)
피싱 메시지에 대한 개별적 격리	**지원됨:** 보안 침해 격리 기능은 피싱 메시지를 동적으로 격리합니다. 피싱 샘플을 보관하기 위해 정적으로 격리해야 하는 경우 재주입을 사용할 수 있습니다. FAQ: 보안 침해 필터
피싱 메시지에 대한 실시간 알림 및 경고	**지원됨:** 피싱 공격이 광범위하게 확산되므로 관리자 또는 수신자에게 경고하는 것이 부담스러울 수 있습니다. 이메일 보안 관리자는 피싱 공격에 대한 보고서를 정기적으로 전달하도록 예약할 수 있습니다.
피싱 메시지에 대한 보고서 자동 전달	**지원됨:** 피싱 공격이 광범위하게 확산되므로 관리자 또는 수신자에게 경고하는 것이 부담스러울 수 있습니다. 이메일 보안 관리자는 피싱 공격에 대한 보고서를 정기적으로 전달하도록 예약할 수 있습니다.
그레이메일 안전 수신 거부	**지원됨:** 안전한 수신 거부 솔루션은 다음을 제공합니다. · 수신 거부 링크로 가장하는 악의적인 위협으로부터 보호 · 모든 서브스크립션 관리를 위한 일관적 인터페이스 · 이메일 관리자 및 최종 사용자에게 이메일에 대한 향상된 가시성 제공
기본 URL 평판 및 범주화	**지원됨:** Cisco ESA는 인바운드 메시지와 아웃바운드 메시지에 대한 기본 URL 평판 및 범주화를 제공하는 유일한 이메일 보안 게이트웨이입니다. 이 기능은 효율성을 높이고 관리자가 환경 보안을 개선하는 데 사용할 수 있는 세분화된 규칙 집합을 제공합니다.
기존 위협(스팸, 바이러스, DOS)에 대한 방어	**Cisco 솔루션**
스팸, 바이러스, 벌크 및 감사에 대한 별도의 정책	**지원됨:** Cisco에서는 스팸, 마케팅/벌크/소셜 메시징, 바이러스, 파일 평판/분석, 콘텐츠 필터링, 제로 데이 및 피싱 메시지에 대한 세분화된 정책을 제공합니다.
스팸, 바이러스, 벌크 및 감사에 대한 개별적 격리	**지원됨:** ESA에서는 활용 사례에 따라 동적, 관리적, 사용자 액세스 가능한 방식으로 격리합니다. 스팸, 바이러스, 제로 데이 및 피싱은 미리 정의된 방식으로 격리되며, 기타 필요한 경우 관리자가 격리할 수 있습니다.
스팸 효율성 및 오탐지 SLA	**지원됨:** 독립 Opus One 보고서에 따르면 상위 8개 안티 스팸 벤더를 기준으로 한 테스트에서 Cisco의 오탐지 SLA(Service-Level Agreement)는 업계 최고임을 인정받았습니다. Opus One Report
100% 안티바이러스 SLA, 엔진 선택 가능	**지원됨:** Cisco의 SLA 및 EULA(End User License Agreement) 참조
평판 기반 스팸 탐지	**지원됨:** 경쟁업체에서는 이메일 도메인에 평판을 객관적으로 할당하지 못하는 경우도 있습니다. 아래 "셀프 교정"을 참조하십시오.
평판 셀프 교정	**지원됨:** Cisco Email Security에서는 고객이 평판 점수를 자체적으로 교정할 수 없습니다. Cisco에서는 고객이 낮은 점수를 받은 이유와 점수를 변경하기 위해 취할 수 있는 조치에 대해 조언합니다. 내 평판 수정
글로벌 안전 목록 및 차단 목록	**지원됨:** Cisco Email Security에서는 글로벌 안전 목록과 차단 목록을 제공합니다. 관리자는 개별 사용자 계정을 편집할 수 있습니다. 안전 목록/차단 목록

이메일 연결 제한 및 종료	**지원됨:** Cisco Email Security에서는 다양한 조건에서 연결 제한 및 종료를 트리거할 수 있습니다. 대량 메일 흐름 제어
정확한 콘텐츠 분석을 위한 기계 학습 기술	**지원됨:** Cisco에서는 10년 동안 CASE 및 보안 침해 필터 엔진을 통한 기계 학습을 개척했습니다. 또한 효율적인 자동 학습 및 규칙 생성 엔진을 통해 효율성을 지속적으로 개선하고 있습니다. 보안 침해 필터
제로 아워 안티바이러스 탐지	**지원됨:** Cisco에서는 모든 다른 보안 회사에 비해 제로 아워 안티바이러스 탐지를 13시간 빨리 파악할 수 있습니다. 보안 침해 필터
기타 위협(인바운드 및 아웃바운드)에 대한 방어	**Cisco 솔루션**
아웃바운드 스팸 탐지	**부분 지원 이상 - 전체 지원됨:** Cisco에서는 엄격한 콘텐츠 인식 검사가 필요한 경우에 대비하여 인바운드 및 아웃바운드 메일에 대한 다양한 안티스팸 엔진을 제공합니다.
정책 기반 암호화	**지원됨:** Cisco Email Security에서는 정책 기반 암호화를 제공합니다.
Office 2007, 2010, 2013 및 PDF 첨부 파일에 대한 콘텐츠 필터링	**지원됨:** ESA의 AMP
SSN 및 CC에 대해 사전 구성된 규정준수 정책	**지원됨:** Cisco Email Security에서는 SSN 및 CC 콘텐츠 필터에 대해 사전 구성된 규정준수 정책을 제공하고, 어플라이언스로 구현되는 RSA DLP 엔진에 훨씬 더 포괄적인 정책을 제공합니다. 경쟁업체 솔루션에서는 ICAP 파일을 사용하여 정책을 관리하기 위해 별도의 어플라이언스가 필요할 수 있습니다.
HIPAA, GLBA 및 PCI에 대해 사전 구성된 규정준수 정책	**지원됨:** Cisco Email Security에서는 HIPAA, GLBA, PCI, HITECH, 미국 및 국제 식별 번호, 전국 규정준수 법 등을 위한 사전 구성된 규정준수 정책을 제공합니다. RSA Enterprise Manager Integration을 지원하는 포괄적인 DLP 솔루션은 데이터 인 모션(웹, 이메일) 및 저장 상태인 데이터(파일 공유)를 처리할 수 있습니다. RSA Enterprise Manager Integration
스마트 식별자 - 구조적 데이터에 대한 알고리즘 검사	**지원됨:** Cisco에서는 콘텐츠 필터 내의 기본 제품에 스마트 식별자를 제공합니다. RSA 이메일 DLP 엔진에 내장된 분류자 및 엔터티에도 스마트 식별자가 있습니다. 사용 설명서(9-21페이지)
매니지드 사전 - 미리 정의되고 업데이트된 라이브러리	**지원됨:** 매니지드 사전은 Cisco의 온보드 DLP 엔진의 일부입니다. DLP 사례 연구
고급 근접성 및 상관관계 분석	**부분 지원 이상 - 전체 지원됨:** Cisco Email Security의 온보드 RSA DLP 엔진에서는 DLP 위반을 결정하는 과정에서 근접성 및 상관관계 분석을 사용합니다. DLP 및 암호화 사례 연구
디지털 자산 보호를 위한 문서 핑거프린팅	**지원됨:** Cisco의 RSA Enterprise Manager Integration에는 핑거프린팅이 포함됩니다.

메시징 암호화	Cisco 솔루션
모바일 디바이스에 대한 간소화되고 암호화된 메시지 전달	**지원됨:** 경쟁업체 모바일 플러그인은 추가 라이센스가 필요할 수 있습니다. Cisco Email Security 플러그인은 무료입니다. 어플라이언스의 암호화 라이센스에 따라 암호화된 메일을 보내거나 온보드 앱 암호화/암호 해독 기능을 사용합니다. 라이센싱 없이 스팸 및 피싱 샘플을 제출합니다. 이메일 보안 플러그인 VoD Basic Envelope Encryption using Cisco Registered Envelope Service
클라이언트가 없는 모바일 솔루션	**지원됨:** Cisco에서는 클라이언트가 없는 모바일 암호 해독 솔루션을 제공합니다.
기본 모바일 앱 권장	**지원됨:** 기본 암호화 앱이 클라이언트가 없는 모바일 솔루션보다 더 안전하다는 것은 일반적으로 업계의 정설입니다.
JavaScript로 암호화된 메시지 전달(일반적으로 차단됨)	**지원됨:** JavaScript는 일반적으로 차단되지 않습니다. 일부 웹메일 제공자는 JavaScript 공격을 적절하게 필터링하는 데 문제가 있으므로 이메일에서 모든 JavaScript를 필터링합니다. 이러한 웹메일 제공자들이 Cisco와 제휴하여 고객을 위한 Cisco의 암호화된 메시지 기술을 차단하지 않게 되었습니다.
메시지별 암호화 키	**지원됨:** Cisco의 탁월한 "수신자별" 암호화 키를 사용하면 발신자가 각 수신자의 액세스를 세부적으로 제어할 수 있습니다. 특정 경쟁업체에서는 발신자가 메시지 수신자 목록의 세부사항에 액세스할 수 없습니다. BCE(Business Class Email)
수신자별 메시지 철회, 관리자 레벨	**지원됨:** Cisco Email Security 관리자는 마지막 레코드에 설명된 각 발신자 계정을 동일한 수준으로 제어할 수 있습니다. 발신자와 관리자 모두에 대해 Registered Envelope Service 포털 로그인에는 보안 메시지를 열어 본 수신자와 키 철회 제어가 표시됩니다. BCE(Business Class Email)
브랜딩 사용자 정의	**지원됨:** 고객 등록 브랜딩이 향후 개발을 위한 Cisco 로드맵에 포함되어 있습니다.
관리 및 보고	**Cisco 솔루션**
중앙 집중식 보고 및 격리	**부분 지원 이상 - 전체 지원됨:** Cisco Email Security에서는 Content Security Management Appliance에서 중앙 집중식 정책, 바이러스 및 스팸 격리를 제공합니다. 어플라이언스를 쉽게 통합하여 추적 및 보고 데이터를 격리와 함께 통합하는 데 사용할 수 있습니다. 성장하는 조직에서는 로컬 Email Security Appliance에서 중앙의 Content Security Management Appliance로 정책, 바이러스 및 스팸 격리를 동적으로 마이그레이션할 수 있습니다. Content Security Management Appliance
통합되고 집계된 기록	**지원됨:** Cisco의 로그를 고객의 기존 엔터프라이즈 기록 시스템으로 내보낼 수 있습니다.
이메일 방화벽 규칙 사용자 정의	**지원됨:** Cisco에서는 경쟁업체에서 "이메일 방화벽"이라는 이 플랫폼 레이아웃에 나열하는 모든 기능을 제공합니다.
제로 아워 메시지 추적, 피싱 메시지 찾기 기능 포함	**지원됨:** 보안 침해 공격 정보는 Cisco Email Security Appliance 및 Content Security Management Appliance의 보고 및 메시지 추적에서 모두 사용할 수 있습니다.
제로 아워 보고, 피싱 메시지 요약 포함	**지원됨:** Cisco Email Security의 보안 침해 필터 페이지에는 이전 연도의 제로 아워 공격 기록, 보안 침해 이름, 공격을 전달하는 메시지에 대한 최종 처리, 발신자 및 수신자에 대한 세부사항을 제공하는 메시지 추적 링크 등이 나열됩니다.
보고서의 자동 게시, 예약 및 이메일 전달	**지원됨:** Cisco Email Security에서는 Email Security Appliance에서 로컬로 또는 Content Security Management Appliance에서 중앙 집중식으로 보고서를 자동으로 게시, 예약 및 이메일로 전달합니다.
그레이메일 탐지 및 보고	**지원됨:** 그레이메일은 마케팅, 소셜 네트워킹, 벌크 메시지로 구성됩니다. 그레이메일 탐지 기능은 조직에 유입되는 그레이메일을 정확하게 분류하고 모니터링하는 데 유용합니다. 이를 토대로 관리자는 각 카테고리의 그레이메일에 대한 적절한 조치를 취할 수 있습니다.
메시징 보안 및 DLP를 위한 단일 관리 콘솔	**지원됨:** Cisco Email Security에서는 메시징 보안 및 DLP를 위한 단일 관리 콘솔 또는 RSA Enterprise Manager와 통합된 경우 개별 DLP 콘솔을 제공합니다.

최종 사용자 제어	Cisco 솔루션
아웃바운드 스팸 및 DLP 위반에 대한 자체 교정	**지원됨:** Cisco Email Security에서는 아웃바운드 스팸에 대한 자체 교정 기능을 제공하지 않습니다. 고객이 실수로 자신을 차단 목록에 등록할 수 있습니다. Enterprise Manager Integration에서 DLP 위반에 대한 자체 교정을 사용할 수 있습니다.
수신자별 메시지 철회, 사용자 레벨	**지원됨:** Cisco Email Security에서는 최종 사용자 안전 목록과 차단 목록을 제공합니다. 관리자는 개별 사용자 계정을 편집할 수 있습니다.
스팸 메시지에 대한 간소화된 보고 및 감사	**지원됨:** Cisco Email Security에서는 전체 메일 볼륨에 대한 스팸의 비율을 수신자 레벨 세부사항과 함께 제공합니다.
구축 옵션	**Cisco 솔루션**
퍼블릭 클라우드(SaaS)	**지원됨:** Cisco Email Security에서는 CES(Cloud Email Security) 솔루션에 SaaS(Software as a Service)를 제공합니다. 클라우드 이메일 보안
가상 어플라이언스	**지원됨:** ESAV(Email Security Virtual Appliance)는 물리적 어플라이언스와 동일한 모든 기능을 제공할 뿐만 아니라, 가상 구축 모델의 편리성과 비용 절감 효과를 추가로 구현합니다. 이는 즉각적인 셀프 서비스 프로비저닝을 제공합니다. Cisco Email Security Virtual Appliance 라이센스를 사용하면 인터넷 연결 없이도 네트워크에 이메일 보안 게이트웨이를 구축할 수 있습니다. 이 라이센스는 내장된 소프트웨어 라이센스를 구매한 것입니다. 로컬에 저장된 새로운 가상 이미지 파일에 언제든지 라이센스를 적용할 수 있습니다. 필요한 경우 초기 상태 가상 이미지 파일을 복제할 수 있으므로 여러 이메일 보안 게이트웨이를 즉시 구축할 수 있습니다. Cisco Email Security Virtual Appliance에서는 Vsphere 5.0, 5.1, 5.5 및 KVM 하이퍼바이저를 지원합니다.