

Cisco Hybrid Email Security

이 유연한 서비스 제품은 인바운드 및 아웃바운드 이메일 관리의 고유한 보안 요구를 충족하도록 설계되었습니다.

Cisco® Hybrid Email Security는 온프레미스와 클라우드 모두에서 이메일 보안 인프라를 쉽게 구축할 수 있는 특별한 서비스 솔루션입니다. Fortune 1000대 기업의 40%를 인바운드 및 아웃바운드 이메일 위협으로부터 보호하는 업계 최고의 기술을 기반으로 하는 Cisco Hybrid Email Security 서비스는 고객이 기밀 정보에 대한 제어력을 유지하고 클라우드 서비스 도입을 간소화하면서 온사이트 데이터 설치 면적을 줄여 줍니다. Cisco Cloud Email Security와 마찬가지로 이 하이브리드 서비스에서는 온프레미스 인프라와 클라우드 인프라 모두에 액세스하여 가시성을 확보할 수 있습니다. 또한 매우 유연한 이메일 관리를 위해 포괄적인 보고 및 메시지 추적 기능을 제공합니다. 이 서비스에는 온프레미스 Cisco Email Security Appliance(물리 및 가상) 및 Cisco Cloud Email Security 서비스를 실행하는 데 필요한 라이선스가 포함되어 있습니다. 물리적 어플라이언스를 구축하려는 경우 하드웨어만 추가적으로 구매하면 됩니다.

Cisco Cloud Security의 차이점

Cisco Cloud Security 서비스 제품군은 Cisco Talos 기술을 사용하여 인바운드 보호를 제공하고, RSA DLP(Data Loss Prevention) 및 Cisco Registered Envelope Service를 사용하여 아웃바운드 보호를 제공합니다.

특징

오늘날의 이메일 보안 위협은 다양한 바이러스, 스팸, 오탐, DDoS(Distributed Denial of Service) 공격, 스파이웨어, 피싱(사기), 지능형 악성코드로 구성되어 있습니다. Cisco에서는 다양한 방법으로 가장 포괄적인 이메일 보안을 제공하며, 예방적 조치와 사후 대응적 조치를 통합하여 방어 역량을 강화합니다.

입증된 스팸 보호

Cisco 기술은 멀티레이어 검사 아키텍처를 사용하여 모든 유형의 원치 않는 이메일 메시지를 차단합니다. Cisco Hybrid Email Security는 99%가 넘는 업계 최고의 스팸 차단율을 제공하며 오탐률이 100만 분의 1도 안 됩니다.

Cisco Reputation Filters는 Cisco SenderBase® Network의 데이터를 사용하여 실시간 이메일 트래픽 위협 평가를 수행하고 의심스러운 이메일 발신자를 식별하기 위한 외부 방어 레이어를 제공합니다.

Cisco Anti-Spam에서는 고유한 Cisco CASE(Context Adaptive Scanning Engine)를 기반으로 위협 탐지에 대한 업계에서 가장 혁신적인 접근 방식을 사용하여 다음을 결정합니다.

- 메시지에 포함된 콘텐츠
- 메시지의 구성 방식
- 메시지 발신자
- 메시지의 실행 촉구 문구가 안내하는 위치

강력한 바이러스 방어

Cisco의 고성능 바이러스 검사 솔루션은 바이러스 필터링에 대한 멀티레이어 접근 방식을 제공합니다.

Cisco Virus Outbreak Filter는 새로운 바이러스 침투를 막는 데 중요한 1차 방어선의 역할을 합니다. 이러한 필터는 기존 바이러스 서명이 사용 가능해지기 전에 바이러스를 탐지하여 차단합니다.

McAfee 및 Sophos 안티바이러스 기술을 완벽하게 통합하여 기존 바이러스 탐지 기능을 제공할 뿐만 아니라 아무리 복잡한 바이러스 공격도 차단할 수 있습니다.

Cisco Advanced Malware Protection은 클라우드에서 파일 평판 서비스와 파일 실행 샌드박싱을 제공하여 기존 안티바이러스 스캐너를 통해 탐지되지 않고 통과되는 지능형 악성코드를 차단하는 애드온으로 사용 가능합니다.

민감 정보에 대한 정교한 아웃바운드 제어

아웃바운드 제어도 인바운드 보안에 못지않게 중요합니다. 아웃바운드 제어에서는 추가 메시지 보호 및 정책을 적용하여 민감한 정보를 보호할 수 있습니다.

RSA Email DLP에서는 완벽하게 통합되고 포괄적이고 정확하며 구축하기 쉬운 솔루션을 통해 민감한 데이터를 보호합니다. 이 기능은 미국의 HIPAA(Health Insurance Portability and Accountability Act), 영국의 Data Protection Act를 비롯한 정부 규정과 PCI DSS(Payment Card Industry Data Security Standard)와 같은 산업 규정을 포함하여 100개 이상의 미리 정의된 정책을 적용합니다. 이러한 정책은 정교한 콘텐츠 분석을 사용하며 오탐을 제거하고 차단율을 높이도록 특별히 조정됩니다. 또한 관리자는 회사별 지적 재산권 또는 민감한 데이터를 식별하기 위한 커스텀 정책을 쉽게 작성할 수 있습니다.

단일 사용자 인터페이스에서 관리자는 안티 스팸, 안티바이러스, 콘텐츠 필터링, 암호화 및 이메일 DLP 작업을 사용자 단위로 구성할 수 있습니다. 관리자는 실시간 및 예약 보고서에 액세스하여 정책, 심각도, 발신자를 기준으로 위반 사례를 검토할 수 있습니다.

안전한 통신을 위한 암호화

Cisco Registered Envelope Service에서는 보안을 제공하고 가시성과 제어 기능을 개선합니다. 또한 파트너, 고객 및 규정 준수 요구 사항을 준수하도록 인증된 기밀 데이터를 보호합니다. 이 서비스에서는 게이트웨이에서 수신자 인박스로의 통신을 간단하고 매우 안전하게 제공합니다. 동시에 TLS(Transport Layer Security) 및 S/MIME(Secure/Multipurpose Internet Mail Extensions) 기술을 통해 파트너 이메일 게이트웨이 간의 보안을 보장할 수 있습니다.

발신자는 Cisco Registered Envelope Service의 **Guaranteed Read receipts(읽음 확인 메일 요청)** 기능을 사용하여 메시지가 전달된 시간과 각 수신자가 확인한 시간을 정확하게 알 수 있습니다.

Message expiration and locking(메시지 만료 및 잠금) 기능은 메시지가 수신자의 인박스에 전달되었더라도 수신자가 메시지를 보지 못하도록 차단합니다.

공동 관리를 위한 포괄적인 관리 및 쉬운 액세스

포괄적인 지원 포털에서는 고객이 사용자 정의 홈 페이지를 작성하고 다음을 비롯한 고유한 보안 관련 사항에 빠르게 액세스할 수 있습니다.

- 이벤트 및 티켓 기록
- 지리적 데이터
- 보안 그래픽
- 트렌드
- 네트워크 상태
- 성능

Consolidated and robust reporting(통합 및 강력한 보고) 옵션은 지리적으로 분산된 인프라 구축에서 트래픽 데이터를 분석하여 완벽하게 통합된 보안 보고를 제공합니다.

Message tracking(메시지 추적) 기능은 고객에게 메시지 처리를 추적하기 위한 실시간 가시성을 제공합니다. 관리자는 로그 파일을 검색할 필요 없이 유연한 추적 인터페이스를 사용하여 메시지를 찾을 수 있습니다. 클라우드 구축과 온프레미스 구축을 모두 추적합니다.

SLA(Service-Level Agreement)

Cisco Hybrid Email Security에서는 업계 최고 수준의 보증이 지원되는 고성능 이메일 보안을 제공합니다. 솔루션이 다음과 같은 SLA를 충족하지 않을 경우 고객에게 환불됩니다.

- 99.999% 업타임
- 99%의 스팸 차단율
- 100만 분의 1 이하의 오탐률
- 알려진 바이러스 100% 차단 보장

탁월한 데이터 보호: Cisco Hybrid Email Security에서는 물리적 분리를 통해 데이터를 보호하고 비공개 상태로 유지하여 데이터 손상을 방지합니다. Cisco 데이터 센터는 여러 레벨로 완벽하게 이중화되어 이메일 인프라를 가용성이 높은 상태로 유지합니다.

용량 보장: Cisco Hybrid Email Security에서는 사용자를 보호하면서 최고 성능을 유지할 수 있는 서비스 용량을 제공합니다. 스팸 볼륨이 증가하면 조직에서는 일반적으로 보호 상태를 유지하기 위해 새로운 하드웨어를 구입해야 합니다. Cisco에서는 증가하는 스팸 볼륨과 새로운 하드웨어 비용에 대한 최종 예산 편성과 관련된 걱정을 덜어 줍니다. 추가 용량은 단일 사용자 기준, 년 기준 가격 모델에 항상 포함됩니다.

공동 관리 지원: 고객이 Cisco와 관리 책임을 공유할 수 있습니다. 이 단일 인터페이스가 제공하는 이점은 다음과 같습니다.

- Cisco 기술 자료에 대한 액세스
- 문제 해결에 대한 직접 지원
- 실시간 상태 정보
- 추적 데이터에 항상 액세스 가능
- 리소스 및 교육 비용 절감
- 효율성 향상

Cisco Talos 제공: Cisco Talos는 위협을 식별, 분석, 방어하는 보안 에코시스템입니다. 다음과 같은 3 가지 구성 요소로 이루어져 있습니다.

- Cisco SensorBase: 세계 최대의 위협 모니터링 네트워크 및 취약성 데이터베이스
- Cisco Threat Operations Center: 보안 분석가와 실행 가능한 정보를 추출하는 자동 시스템으로 이루어진 글로벌 팀
- 동적 업데이트: 모범 사례 권장 사항과 함께 Cisco 보안 디바이스에 자동으로 전달되는 실시간 업데이트

요약

Cisco Hybrid Email Security는 고유한 폼 팩터에서 최고의 이메일 보안을 제공하는 "온프레미스와 클라우드 모두에서 최고"의 서비스입니다. 또한 비용을 예측 가능한 상태로 유지하여 예산 계획을 간소화함으로써 탁월한 유연성과 선택 옵션을 제공합니다. 고객이 이메일 보안 전문가의 가장 높은 수준의 보호를 받아 공동 관리 지원 모델을 평가하며, 온프레미스에서 기밀 정보가 안전하게 유지되므로 안심할 수 있습니다.

다음 단계

Cisco Cloud Email Security의 장점을 이해하는 가장 좋은 방법은 구매 전 시험 사용(Try Before You Buy) 평가 프로그램에 참여하는 것입니다. 자세한 내용은 www.cisco.com/go/cloudemail을 참조하십시오.



미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 www.cisco.com/go/offices에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

Printed in USA

C78-734189-00 03/15