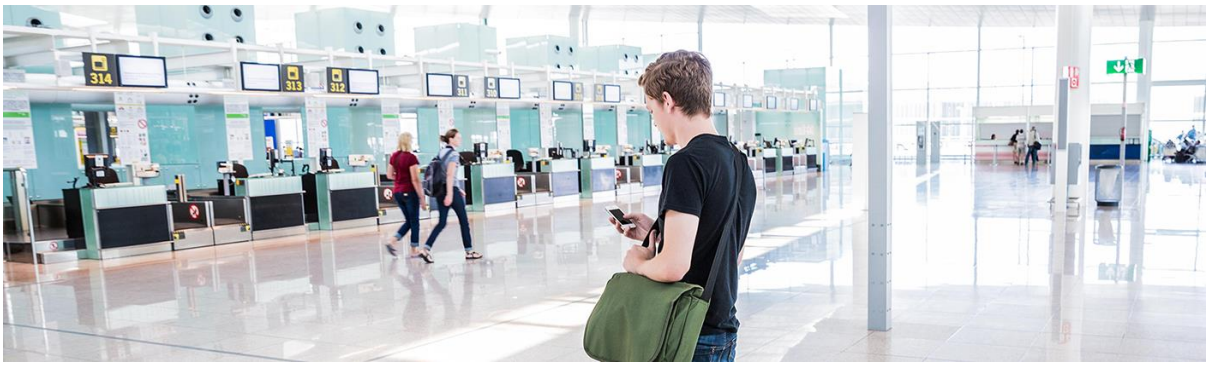
# Advanced Malware Protection을 통해 Office 365를 개선하는 Cisco Email Security



Microsoft Office 365에서 제공하는 혜택을 활용하면서 "적당한" 이메일 보안 기능에 만족하지 마십시오. Cisco는 오늘날의 피싱 및 고급 악성코드 위협을 방지하는 업계 최고의 이메일 보안을 제공합니다.

### 혜택

- 최고의 효율성(차단율 99%, 이메일 1백만 건당 오탐 수 1건 미만)을 자랑하는 업계 최고의 이메일 기반 위협(피싱/표적 공격 포함) 방지 기능
- 데이터 유출 방지 및 매우 안전한 메시징을 위한 최고의 컨트롤
- 전용 클라이언트 인프라(다른 고객으로 인한 중단 위험 감소)
- Cisco의 전용 모니터링 및 지원

오늘날에는 이메일을 통한 사이버 공격이 매우 흔히 발생하고 있습니다. 매주 사이버 공격으로 인해 널리 알려진 브랜드의 보안이 침해되고 있습니다. 이러한 공격의 수가 증가함에 따라 공격을 방지하지 못하는 조직의 비용도 증가하고 있습니다. Ponemon Institute의 설명에 따르면 보안 침해와 관련된 평균 비용은 590만 달러에 달하며 매년 50만 달러씩 증가한다고 합니다.

Cisco® Cloud Email Security를 사용하면 중요한 비즈니스 이메일을 스팸, 악성코드 및 기타 위협으로부터 안전하게 보호할 수 있습니다. 이 클라우드 기반 솔루션을 통해 온사이트 데이터 센터 사용 공간과 비용을 줄일 수 있습니다. 이 솔루션은 10년 이상 Gartner의 Email Security Gateway Magic Quadrant에서 높은 순위를 차지해 왔으며 Fortune 1000대 기업의 40%, 10대 ISP 중 8곳에서 이메일 인프라를 보호하는 포괄적인 플랫폼을 기반으로 합니다.

## 진화하는 위협 환경

사이버 범죄는 최근 소규모 표적 공격으로 변화하고 있습니다. 이메일은 여전히 주요 공격 벡터이며 이메일 공격의 빈도 및 공격 대상에 미치는 경제적 피해가 증가하고 있습니다. Cisco Talos의 연구 결과에 따르면 고도의 맞춤형 표적 공격으로 인한 비즈니스 활동이 작년에만 3배나 증가했다고 합니다. 이러한 공격은 기업에 금전적 손실과 자격 증명 도용 이상의 영향을 줍니다. 그리고 이러한 공격 피해를 당한 조직은 감염된 호스트를 치료하고 실추된 평판을 회복하는 데 적잖은 비용을 부담해야 합니다.

Cisco Talos의 연구 결과에 따르면 스팸 양은 2014년 1월부터 2014년 11월까지 250% 증가했습니다. 여기에는 제로 데이 악성코드, 스피어피싱 및 스노우슈(Snowshoe) 스팸이 포함됩니다. 스노우슈(Snowshoe) 스팸은 보안 탐지를 피하기 위해 대량의 IP 주소에서 소량의 스팸을 발송하는 새롭게 등장한 위협입니다. 이러한 모든 방법은 효율성이 매우 높은 것으로 확인되었으며 스팸 필터를 통과하는 경우가 많습니다.

**결과:** 클라우드를 사용하는 경우에도 기업과 고객의 데이터를 도용하려는 매우 정교한 악성코드를 통한 이메일 공격을 끊임없이 받고 있습니다.

## Cloud Email Security가 제공하는 기능

Cisco는 2015년의 Gartner Magic Quadrant® for Email Gateways에서 1위 업체로 선정되었습니다. Cisco Email Security 솔루션은 다음과 같은 기능을 제공합니다.

- 업계 최대의 고급 위협 인텔리전스 서비스인 Cisco Talos의 동적 업데이트
- 이중화를 위한 미국과 유럽의 여러 데이터 센터
- 자금 지원 SLA(Service-Level Agreement)
- 역할 기반 관리
- 공동 관리
- 99.999% 업타임
- 오탐률 1백만 분의 1 미만

주요 기능은 다음과 같습니다.

- TLS(Transport Layer Security)
- RSA Data Loss Prevention
- S/MIME(Secure/Multipurpose Internet Mail Extension) 암호화
- 통합 메시지 수준 암호화(서드파티 제품 불필요)
- 다른 고객과 함께 차단 목록에 포함되는 현상 방지를 위한 전용 IP 주소
- 그레이메일 관리
- 웹 상호작용 추적

Cisco의 레이어형 보안에는 다음과 같은 기능이 포함됩니다.

- Cisco AMP Threat Grid를 통한 파일 평판, 분석(샌드박싱) 및 회귀 기능
- URL 분류 및 평판 필터
- 업계 최고의 안티 스팸 필터
- 수상 경력에 빛나는 Sophos 및 McAfee의 안티바이러스 보호
- 인바운드 및 아웃바운드 콘텐츠 필터링
- Outbreak 필터를 통한 안티피싱 및 제로 데이 보호

## Cisco만의 업계 서비스

Cloud Email Security는 다음과 같은 여러 가지 차별화된 기능을 제공합니다.

- **전용 클라우드 인프라:** 각 고객은 여러 Cisco 데이터 센터에서 호스팅되는 전용 이메일 보안 인스턴스를 이용할 수 있습니다.
- **클라우드 용량 보장:** 스팸 양의 증가와 상관없이 사용자를 보호하고 최고의 성능을 유지할 수 있습니다. 추가 용량은 간단한 사용자별, 연간 가격 모델에 포함됩니다.
- **클라우드 가용성 보장:** Cloud Email Security는 99.999% 업타임을 보증하므로 다수의 데이터 센터를 통해 보안을 유지할 수 있습니다. Cisco는 전 세계에 여러 클라우드 데이터 센터를 운영하고 있습니다.

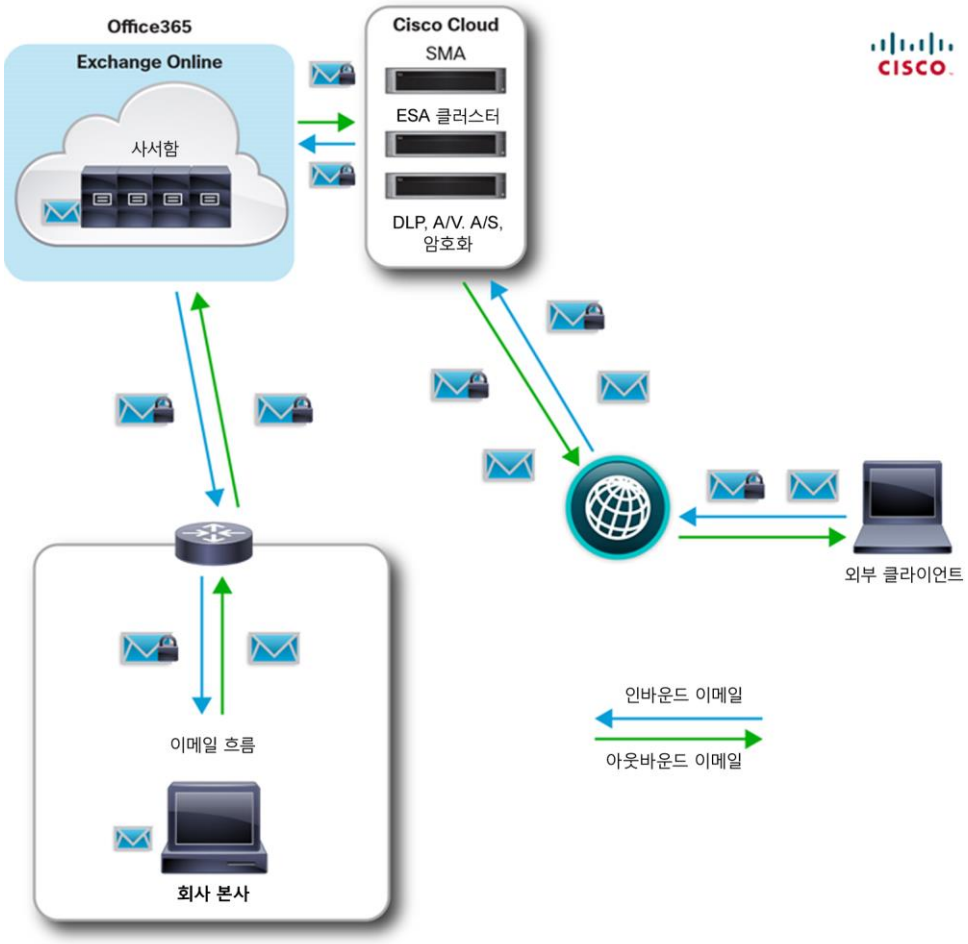
## 구축 옵션

- **Cisco Cloud Email Security:** 이 클라우드 기반 SaaS(Software as a Service) 제품은 매우 안전한 Cisco 데이터 센터 내에 위치하므로 온사이트 하드웨어가 필요하지 않습니다. 민감한 데이터를 온프레미스(구내 장비)에 유지해야 하며 특히 성능 저하 위험을 우려하는 조직을 위해 Cisco에서는 추가 솔루션을 제공합니다.
- **Cisco Hybrid Email Security:** 이 서비스에서는 이메일 보안의 온프레미스(구내 장비) 및 클라우드 구축을 위한 기능을 번들로 제공합니다. 또한 조직의 사이트와 Cisco의 클라우드 기반 SaaS 제품 간에 제어를 분할합니다. 하이브리드 서비스도 Cloud Email Security와 마찬가지로 Cisco 데이터 센터에서 전용 이메일 보안 인스턴스를 제공하지만 온프레미스(구내 장비) 인프라와 클라우드 인프라에 계속 액세스할 수 있으며 인프라를 확인할 수 있습니다. 온프레미스(구내 장비) 어플라이언스에서는 암호화, DLP(데이터 유출 방지) 및 온사이트 LADP(Lightweight Directory Access Protocol) 통합을 통해 고급 아웃바운드 제어 기능을 추가로 제공합니다.
- **Cisco Managed Email Security:** 이 사용자 정의 이메일 서비스에서는 스팸 및 바이러스를 차단하여 이메일 인프라를 보호하면서 IT 조직의 부담을 줄여줍니다. 이 서비스에서는 고성능 어플라이언스와 전문가 모니터링 및 관리를 결합하여 복잡한 이메일 인프라를 포괄적으로 보호합니다. 지속적으로 확대되는 이메일 인프라를 유연하게 관리하도록 설계된 Managed Email Security에서는 체계적으로 정의된 단계(평가, 시스템 디자인, 시스템 구현, 서비스 활성화, 제품 구현)에 따라 구조화된 구현 모델을 제공합니다.

## 솔루션 작동 방식

Cisco Cloud Email Security는 365 클라우드에 있는 사서함 중 일부만 포함하든 모든 사서함을 포함하든 설정 방식에 관계없이 Microsoft Office 365와 투명하게 통합됩니다(그림 1). MX(mail exchange) 레코드가 Cloud Email Security 플랫폼을 가리키도록 지정하기만 하면 수신 메시지에서 피싱, 스팸, 바이러스 및 고급 악성코드 공격이 정리됩니다. Cloud Email Security 플랫폼을 통해 아웃바운드 메일을 배달하도록 Office 365에서 스마트 호스트 설정을 구성하면 간편하게 사용 및 구성할 수 있는 Cisco의 DLP 및 암호화 기능이 아웃바운드 메일 흐름을 제어하여 민감한 데이터의 유출을 방지합니다. Cisco는 조직의 클라우드에서 전용 Email Security Appliance를 관리합니다. 고객은 테넌트가 모두 같은 방식으로 구성되는 멀티테넌트 환경에서 작업을 하는 대신 이러한 어플라이언스에 직접 액세스하여 컨피그레이션 및 보고를 수행할 수 있습니다.

**그림 1.** Office 365와 통합된 Cloud Email Security




**메모:** Cisco Cloud Email Security 구성 요소에는 Content Security Management Appliance, Email Security Appliance 클러스터, 데이터 유출 방지, 안티바이러스/안티 스팸 툴 및 암호화 기능이 포함됩니다.

## 활용 사례 시나리오

| 시나리오 | Cisco Cloud Email Security 솔루션 |
|---|---|
| **위험 감소, 기존 보안 시스템과의 통합, 고급 악성코드 방지를 위한 회귀 보고** | 온프레미스(구내 장비) 및 클라우드에서 사용 가능한 세계 최고 수준의 Cisco 기술을 시연하기 위해 Office 365에서 다운스트림에 Cisco Email Security Appliance를 배치해 1년(2013~14년)에 걸쳐 테스트를 진행했습니다. Cisco Email Security Appliance에는 안티 스팸 및 안티바이러스 기능용 라이센스만 적용되었으며 고급 악성코드 차단 및 Outbreak 필터는 비활성화되었습니다. 이 테스트에 대해 고객이 공유한 결과는 다음과 같습니다.<br>Office 365에서 전달된 메시지의 52%가 차단되었습니다. 6500만 개의 메시지 중 9백만~1천만 개는 마케팅 메시지였습니다. 150만~250만 개의 메시지가 피싱 공격이었습니다. 테스트의 일환으로 Security Appliance에서 제공되는 멀티레이어 필터링을 우회했습니다. 이 기간 동안 매월 70만 건 이상의 위협이 조직에 침투했습니다. |
| **파일 분석, 피싱 캠페인** | Cisco Advanced Malware Protection은 감염된 첨부 파일을 사용하는 소규모 제로 데이 표적 공격으로부터 고객을 보호합니다. 이 솔루션은 Sourcefire AMP 파일 평판 클라우드를 사용해 첨부 파일을 검사하여 알려진 정상 파일인지 아니면 알려진 불량 파일인지를 확인합니다. 알려지지 않은 파일은 검사를 위해 클라우드에 업로드할 수 있습니다. 이 솔루션만의 독특한 특징은 파일 판정 변경 사항을 관리자에게 알리는 기능입니다. 이 기능을 통해 샌드박싱을 우회하기 위해 난독 처리 기술 및 기타 수법을 사용한 파일에 대해 관리자에게 알림을 보낼 수 있습니다.<br>Outbreak 필터는 이메일에서 피싱, "해외 도난 사고" 메시지, 송금 사기, 419 스캠 등 서로 다른 약 20가지의 위협 범주를 스캔합니다. URL이 포함된 위협 이메일의 경우 사용자가 클릭하면 클라우드에서 추가로 스크럽이 수행되도록 URL이 재작성됩니다. |

| 시나리오 | Cisco Cloud Email Security 솔루션 |
| --- | --- |
| **아웃바운드 암호화<br>데이터 유출 방지** | 기업 내에서 Email Security Appliance를 사용할 수 있는 경우에는 Cisco Registered Envelope Service를 통해 온프레미스(구내 장비) DLP 및 온프레미스(구내 장비) Business-Class Email 암호화를 사용할 수 있습니다.<br>하이브리드 호스팅 모델에서는 아웃바운드 메시지가 고객 기업 외부로 전송되기 전에 해당 메시지에 Registered Envelope Service 암호화를 효율적으로 구현할 수 있습니다. 암호화는 발신자가 트리거할 수도 있고 어플라이언스의 기본 엔진에서 DLP 정책에 의해 트리거될 수도 있습니다. 고객은 어플라이언스 인터페이스에서 제공되는 120가지 DLP 정책 중에서 선택하거나 마찬가지로 온프레미스(구내 장비)에 있는 RSA Enterprise Manager를 사용하여 이러한 정책을 관리할 수 있습니다. 발신자는 Registered Envelope Service로 암호화된 메시지를 다운로드한 다음 개별 수신자에 대해 해당 메시지 액세스를 잠글 수 있습니다. 온프레미스(구내 장비) 키 저장소가 필요한 고객을 위해 Cisco는 Zix Corporation과 제휴하여 로컬 키 서버를 제공합니다. 이러한 로컬 서비스를 선택하는 경우 이메일 보안을 정밀하게 제어하고 확인하는 기능과, 트래픽/위협/DLP에 대해 구체적인 작업을 실행할 수 있는 보고 기능이 제공됩니다. 이러한 옵션은 호스팅된 보안을 적용하고자 하는 금융 또는 의료 업종에 매우 적합합니다. |

## Cisco 서비스 활용

| | |
| --- | --- |
| **Cisco Remote Managed Services** | Cisco 전문가가 보다 신속한 구축을 위해 고급 활성화 서비스를 제공합니다. |
| **Cisco Branded Services** | Cisco Security Planning and Design Service: 강력한 보안 솔루션을 신속하고 비용 효율적으로 구축할 수 있도록 지원합니다. Cisco Email Security Configuration and Installation Remote Service: 솔루션을 설치, 구성 및 테스트하여 보안 위험을 완화합니다. Cisco Security Optimization Service: 설계, 성능 조정, 시스템 변경 지원 등을 통해 새로운 보안 위협에 대응할 수 있도록 진화하는 보안 시스템을 지원합니다. |
| **협업 및 파트너 서비스** | Cisco Collaborative Professional Services Network Device Security Assessment Service: 보안상의 허점을 찾아내 더 강력한 네트워크 환경을 유지할 수 있도록 지원합니다. Cisco Smart Care Service: 네트워크 성능에 대한 매우 안전한 가시성에 기반한 인텔리전스를 사용하여 사전 예방적으로 모니터링함으로써 비즈니스를 최상의 상태로 실행할 수 있습니다. 또한 Cisco 파트너는 계획, 설계, 구현 및 최적화 라이프사이클 전체에서 다양한 추가 서비스를 제공합니다. |
| **Cisco 파이낸싱** | Cisco Capital®에서는 비즈니스 요구 사항에 부합하는 맞춤형 금융 지원 솔루션을 제공합니다. 조속히 Cisco 기술을 활용하여 더욱 신속하게 비즈니스 혜택을 누리십시오. |
| **Cisco SMARTnet™ Support Services** | 기술투자의 가치를 극대화하려면 SMARTnet® Service를 구매하여 Email Security Appliance와 함께 사용하십시오. 이 서비스는 고객이 언제든 직접 Cisco 전문가에게 문의하거나 셀프 헬프 지원 툴, 빠른 하드웨어 교체를 이용하여 네트워크 문제를 신속하게 해결할 수 있도록 지원합니다. |

## Cisco Capital

### 목표 달성을 지원하는 파이낸싱

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 알아보십시오.

"Cloud Email Security 설치를 진행하기 위해 함께 작업을 했던 Ironport 팀은 항상 작업을 매우 효율적으로 수행했으며, 이로 인해 모든 서비스에서 추가적인 혜택을 제공할 수 있었습니다."

**– Petter Österlund(Commsec.se 수석 네트워크 엔지니어)**

## Office 365에 Cisco Email Security를 통합해야 하는 이유

모든 기업은 오늘날 가장 흔히 활용되는 위협 벡터인 기업 이메일을 안전하게 보호해야 합니다. Cisco Cloud Email Security는 고급 위협 인텔리전스를 통해 인바운드 보호 및 아웃바운드 위협을 제어할 수 있는 동급 최고의 기능을 제공합니다. 업계 최고 품질을 자랑하는 Cisco의 솔루션으로 정교한 공격으로부터 기업을 보호하십시오.

## 다음 단계

Office 365용 Cisco Cloud Email Security에 대한 자세한 내용을 확인하려면 Cisco Cloud Email Security 제품 페이지를 참고하십시오. 무료 Cisco Email Security를 시험 사용해 볼 수도 있습니다.


**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, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.





Printed in USA C22-735430-00 07/15