Cisco Email Security Appliance

매일 1,000억 개 이상의 기업 이메일 메시지가 교환되고 있습니다. 이메일 사용이 증가하면서 보안의 우선순위는 더욱 높아지고 있습니다. Cisco® 솔루션은 동적으로 빠르게 변화하면서 조직에 영향을 미치는 위협을 차단하는 고가용성 이메일 보호 기능을 제공합니다.

기능 및 혜택

물리적, 가상, 클라우드 또는 하이브리드인지에 상관없이 Cisco 이메일 보안 솔루션은 다음과 같은 기능을 제공하는 업계 최고의 솔루션으로 인정받고 있습니다.

- **신속하고 포괄적인 보호** - 일반적으로 경쟁업체보다 몇 시간 또는 며칠 앞서 조치 가능
- **최대 규모의 위협 인텔리전스 네트워크 중 하나** - Cisco Talos의 광범위한 종합 보안 분석에 기반
- **아웃바운드 메시지 보호** - 디바이스에서 DLP(데이터 유출 방지) 및 이메일 암호화 활용
- **총 소유 비용 절감** - 작은 설치 공간, 간편한 구현, 장기적인 절감 효과가 있는 자동화된 관리

제품 개요

오늘날, 스팸과 악성코드는 인바운드 위협과 아웃바운드 위험을 수반하는 복합적인 이메일 보안 문제의 일부입니다. 올인원(all-in-one) 솔루션인 Cisco Email Security Appliance는 적은 유지 보수 요건, 낮은 레이턴시, 낮은 운영 비용으로 간단하고 신속하게 구축할 수 있습니다. Cisco 제품에서는 설정 후 자동 실행되는 기술을 지원하므로 자동 정책 설정을 활용하여 직원들의 업무 부담을 덜 수 있습니다. 이후 Cisco의 클라우드 기반 위협 인텔리전스 솔루션에보안 업데이트가 자동으로 전달됩니다. 3분에서 5분 간격으로 위협 인텔리전스 데이터가 업데이트되어 다른 벤더보다 몇 시간 또는 며칠 앞서 최신 위협 방어 대응 조치를 취합니다. 이 어플라이언스는 유연한 구축 옵션을 제공하고 기존 보안 인프라와 원활히 통합되므로 기업의 비즈니스 요구 사항을 완벽하게 충족할 수 있습니다.

가상 어플라이언스

Cisco Email Security Virtual Appliance는 이메일 보안 구축 비용을 크게 절감해 줍니다. 특히 매우 분산된 네트워크의 경우 그 효과가 큽니다. 이 어플라이언스를 사용하면 네트워크 관리자가 기존 네트워크 인프라를 사용하여 필요한 경우 언제 어디서나 인스턴스를 생성할 수 있습니다. 물리적 어플라이언스의 소프트웨어 버전으로, VMware ESXi 하이퍼바이저와 Cisco UCS®(Cisco Unified Computing System™) 서버를 기반으로 실행됩니다. Cisco Email Security 소프트웨어 번들 중 하나를 구매하면 가상 어플라이언스에 대한 무제한 라이선스를 받게 됩니다.

이 가상 어플라이언스를 사용하면 간소화된 용량 계획을 통해 트래픽 증가에 즉시 대응할 수 있습니다. 어플라이언스를 구매하고 배송할 필요가 없습니다. 따라서 데이터 센터가 복잡해진다거나 인력을 충원하지 않아도 새로운 비즈니스 기회를 지원할 수 있습니다.

주요 기능

물리적, 가상, 클라우드, 하이브리드 솔루션을 사용하여 미션 크리티컬 이메일 시스템을 보호할 수 있습니다. 표 1에는 Cisco 이메일 보안 솔루션의 주요 기능이 요약되어 있습니다.

위조 이메일 탐지는 고가치 표적으로 알려진 상위 경영진에게 초점을 맞춘 스푸핑 공격을 차단합니다. 위조 이메일 탐지는 전용 콘텐츠 필터를 사용해 이러한 맞춤형 공격을 차단할 수 있습니다.

이 기능은 모든 공격 시도와 관련 행동에 대한 자세한 로그 기록을 제공합니다.

표 1. 주요 기능

기능	설명
글로벌 위협 인텔리전스	전 세계 최대 규모의 위협 탐지 네트워크 중 하나인 Cisco Email Security에서 제공하는 빠르고 완벽한 이메일 보호 기능을 사용해보십시오. Cisco에서는 다음과 같은 광범위한 가시성과 큰 설치 범위를 제공합니다. • 하루 100테라바이트(TB)의 보안 인텔리전스 • 방화벽, Cisco IPS 센서, 웹 및 이메일 어플라이언스를 포함하는 160만 대의 보안 디바이스 구축 • 1억 5000만 개의 엔드포인트 • 매일 130억 건의 웹 요청 전 세계 기업 이메일 트래픽의 35% Cisco Talos는 글로벌 트래픽 활동에 대한 24시간 가시성을 제공합니다. 이상 징후를 분석하고, 새로운 위협을 발견하며, 트래픽 트렌드를 모니터링합니다. Talos는 보안 어플라이언스에 업데이트를 제공하는 규칙을 지속적으로 생성하여 제로 아워 공격을 차단합니다. 이러한 업데이트는 3분에서 5분 간격으로 수행되어 업계 최고의 위협 방어 기능을 제공합니다.
스팸 차단	스팸은 정교한 솔루션이 필요한 복잡한 문제입니다. 하지만 Cisco는 이를 간단하게 해결합니다. 스팸이 받은 편지함에 전송되지 않도록 하기 위해 발신자 평판을 기준으로 필터링하는 외부 레이어와 메시지를 심층적으로 분석하여 필터링하는 내부 레이어를 결합하여 멀티레이어 방어 기능이 제공됩니다. 평판 필터링을 통해 80% 이상의 스팸이 회사의 네트워크에 도달하기도 전에 차단됩니다. 최근의 기능 향상에는 상황 분석, 향상된 자동화, 자동 분류가 포함되어 스노우슈(snowshoe) 캠페인을 차단할 수 있는 강력한 방어 기능을 제공합니다.
그레이메일 탐지 및 안전한 수신 거부	그레이메일은 마케팅, 소셜 네트워킹, 벌크 메시지로 구성됩니다. 그레이메일 탐지 기능은 조직에 유입되는 그레이메일을 정확하게 분류하고 모니터링하는 데 유용합니다. 이를 토대로 관리자는 각 범주에 대한 적절한 조치를 취할 수 있습니다. 그레이메일에는 엔드 유저가 이러한 이메일을 받지 않도록 옵트아웃하겠다는 사실을 발신자에게 알리는 수신 거부 링크가 포함되어 있는 경우가 많습니다. 수신 거부 메커니즘을 모방하는 수법은 잘 알려진 피싱 기법이므로, 사용자는 이러한 수신 거부 링크를 클릭하는 것을 경계해야 합니다. 안전한 수신 거부 솔루션은 다음을 제공합니다. • 수신 거부 링크로 가장하는 악의적인 위협으로부터 보호 • 모든 서브스크립션 관리를 위한 일관적 인터페이스 • 이메일 관리자 및 엔드 유저에게 이메일에 대한 향상된 가시성 제공
Advanced Malware Protection	이제 Cisco Email Security Appliance에 Cisco Advanced Malware Protection이 포함됩니다. 이메일 게이트웨이를 통과한 후에도 위협을 지속적으로 분석할 수 있도록 파일 평판 점수 및 차단, 정적 및 동적 파일 분석(샌드박싱), 파일 회귀 분석 등의 기능을 제공합니다. 사용자는 더 많은 공격을 차단하고, 의심스러운 파일을 추적하며, 문제 발생의 범위를 완화하고, 신속하게 치료할 수 있습니다. Advanced Malware Protection은 모든 Email Security Appliance 고객이 추가 라이선스 기능으로 사용할 수 있습니다. Cisco AMP Threat Grid는 클라우드에 악성코드 샘플을 제출할 때 규정 준수 또는 정책 제한사항을 적용해야 하는 조직에 대해 온프레미스 어플라이언스를 통한 악성코드 차단 기능을 제공합니다. AMP 시스템은 이제 AMP 프라이빗 클라우드 라이선스를 사용하여 온프레미스에 완벽하게 구축될 수 있습니다. 이것은 AMP

기능	설명
	퍼블릭 클라우드의 사용을 허용하지 않는 엄격한 정책 요구 사항을 지닌 고객에게 중요하며 이러한 고객들은 계속해서 AMP 퍼블릭 클라우드 업데이트의 이점을 활용하고 있습니다. Office 365용 자동 악성코드 치료와 AMP를 함께 사용하면 회귀적 보안을 통해 보안 침입을 더 빠르고 쉽게 해결할 수 있습니다. 고객은 감염된 이메일에 자동 조치를 취하도록 이메일 보안 솔루션을 설정하기만 하면 됩니다.
Outbreak Filter	Outbreak Filter는 새로운 위협 및 복합적인 공격을 차단합니다. 이러한 필터는 파일 유형, 파일 이름, 파일 크기, 메시지의 URL을 포함하여 6가지 파라미터의 조합에 대한 규칙을 모두 작성할 수 있습니다. Talos가 보안 침해에 대해 더 많은 정보를 입수하면 그에 따라 규칙을 수정하고 격리된 메시지를 해제할 수 있습니다. Outbreak Filter는 의심스러운 메시지에 링크된 URL을 다시 작성할 수도 있습니다. 새 URL을 클릭하면 수신자는 Cisco Web Security 프록시를 통해 리디렉션됩니다. 그런 다음 웹사이트 콘텐츠를 철저히 검사하며, Outbreak Filter는 차단 화면을 표시하여 사용자에게 사이트에 악성코드가 포함되어 있는지 알립니다.
웹 상호작용 추적	IT 관리자는 완전히 통합된 솔루션을 사용하여 Email Security Appliance에서 재작성한 URL을 클릭한 엔드 유저를 추적할 수 있습니다. 보고서에는 다음 내용이 표시됩니다. • 악성 URL을 클릭한 상위 사용자 • 엔드 유저가 클릭한 상위 악성 URL • 날짜/시간, 재작성 이유, URL에서 수행한 작업 관리자는 특정 URL이 포함된 모든 메시지를 역추적할 수도 있습니다.
아웃바운드 메시지 제어	Email Security Appliance는 DLP, 이메일 암호화를 통해 아웃바운드 메시지를 제어합니다. 이러한 제어를 통해 가장 중요한 메시지가 업계 표준을 준수하고 전송 중에 보호되도록 보장할 수 있습니다. 또한 아웃바운드 안티 스팸 및 안티 바이러스 스캔을 아웃바운드 속도 제한과 함께 사용하여 감염된 시스템 또는 계정으로 인해 자신의 회사가 이메일 블랙리스트에 오르는 것을 방지할 수 있습니다. 새로운 기능: 이제 Email Security Appliance는 TLS(Transport Layer Security)뿐만 아니라 S/MIME(Secure/Multipurpose Internet Mail Extensions) 암호화 및 서명을 지원합니다.
위조 이메일 탐지	위조 이메일 탐지는 고가치 표적으로 알려진 경영진에게 초점을 맞춘 스푸핑 공격을 차단합니다. 위조 이메일 탐지는 전용 콘텐츠 필터를 사용해 이러한 맞춤형 공격을 차단할 수 있습니다. 이 기능은 모든 공격 시도와 관련 행동에 대한 자세한 로그 기록을 제공합니다.
탁월한 성능	보안 어플라이언스는 새로운 인바운드 이메일 바이러스를 신속하게 차단합니다. 도메인 딜리버리 대기열에서는 전달할 수 없는 이메일로 인해 다른 도메인에 보낼 중요한 딜리버리를 백업해야 하는 상황이 발생하지 않도록 합니다. 이 솔루션은 99.9% 이상에 달하는 업계 최고의 스팸 포착률을 제공하며 오탐 확률이 100만 분의 1도 안 됩니다.
DLP	네트워크에서 기밀 데이터가 유출되는 것을 방지하기 위해 정부, 민간 부문 및 회사 관련 규정을 포함하는 100개 이상의 전문가 정책으로 구성된 광범위한 정책 라이브러리에서 선택합니다. 원하는 경우 사전 정의된 정책의 일부를 사용하여 고유한 맞춤형 정책을 생성할 수 있습니다. Cisco Email Security DLP 엔진은 단어, 구, 사전, 정규식 등의 선택적인 고유한 데이터 포인트와 함께 미리 조정된 데이터 구조를 사용하여 오탐을 최소화하면서 정확한 정책을 신속하게 생성합니다. DLP 엔진은 심각도에 따라 위반 점수를 매기므로 요구사항에 맞게 서로 다른 수준의 치료를 적용할 수 있습니다. 치료 방법으로는 암호화, 면책조항 및 바닥글(footer) 추가, 숨은 참조(BCC) 추가, 알림 공지, 격리 등 다양한 방법이 있습니다.
낮은 비용	작은 설치 공간, 간편한 설정 및 자동화된 업데이트 관리를 통해 이메일 보안 솔루션의 수명 기간 동안 비용이 절감됩니다. Cisco의 솔루션은 사용 가능한 최저 수준의 TCO를 실현합니다.
유연한 구축	모든 Cisco 이메일 보안 솔루션은 구현에 대한 간단한 접근 방식을 공유합니다. 시스템 설정 마법사는 복잡한 환경도 처리할 수 있으며, 단 몇 분 만에 운영을 시작하고 보호 기능을 구현하여 신속하고 더욱 안전한 환경을 구축합니다. 라이선스는 디바이스가 아니라 사용자를 기반으로 하므로 디바이스 대신에 사용자당 라이선스를 적용하여 추가 비용 없이 인바운드 및 아웃바운드 이메일 게이트웨이 보호 기능을 제공할 수 있습니다. 이 기능을 통해 안티 스팸 및 안티 바이러스 엔진을 사용하여 아웃바운드 메시지를 스캔함으로써 비즈니스 요구사항을 완벽하게 지원할 수 있습니다. 가상 어플라이언스는 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 라이선스를 사용하면 인터넷 연결 없이도 네트워크에 이메일 보안 게이트웨이를 구축할 수 있습니다. 이 라이선스는 내장된 소프트웨어 라이선스를 구매한 것입니다. 로컬에 저장된 새로운 가상 이미지 파일에 언제든지 라이선스를 적용할 수 있습니다. 필요한 경우 초기 상태 가상 이미지 파일을 복제할 수 있으므로 여러 이메일 보안 게이트웨이를 즉시 구축할 수 있습니다. 동일한 구축에서 하드웨어 및 가상 이메일 보안 솔루션을 실행할 수 있습니다. 따라서 소규모 지사 또는 원격 위치에서 해당 위치에 하드웨어를 설치하고 지원할 필요 없이 본사에서와 동일한 보호 기능을 구현할 수 있습니다. 다음을 활용하여 맞춤형 구축을 쉽게 관리할 수 있습니다. Cisco Content Security Management Appliance 또는 Cisco Content Security Management Virtual Appliance
비즈니스에 적합한 솔루션	Cisco Cloud Email Security는 소프트웨어, 컴퓨팅 성능, 지원을 포함하는 포괄적이고 신뢰할 수 있는 서비스입니다. 공동 관리되는 사용자 인터페이스는 Cisco 물리적 및 가상 이메일 보안 어플라이언스의 사용자 인터페이스와 동일합니다. 따라서 관리 오버헤드가 거의 발생하지 않으며 모니터링 및 관리해야 하는 온 온사이트 하드웨어 없이 탁월한 보호 기능을 구현할 수 있습니다. Microsoft Office 365 고객은 Cloud Email Security for Office 365를 통해 동일하게 강력한 업계 최고의 보호를 받을 수 있습니다. 이 솔루션은 구축하기 쉬우며 최고 수준의 서비스 가용성 및 데이터 보호를 지원하는 복원력이 뛰어난 멀티 데이터 센터를 통해 안정성을 보장받을 수 있습니다. 하이브리드 솔루션은 민감한 메시지에 대한 지능형 아웃바운드 제어 기능을 온사이트에서 제공하는 동시에 클라우드의 편리한 비용 효율성을 활용할 수 있도록 지원합니다. 온프레미스 사용자와 클라우드 사용자 수는 계약 기간 내 총사용자 수가 변하지 않는다는 전제하에 언제든지 변경할 수도 있습니다. 이는 조직의 요구사항 변화에 따른 구축 유연성을 제공합니다. 온프레미스 하드웨어 및 가상 어플라이언스가 플러그인 준비가 된 상태로 제공됩니다. 해당 환경에 가장 적합한 모델을 선택하여 게이트웨이에서 인바운드 및 아웃바운드 메시지를 보호할 수 있습니다.

제품 사양

표 2에는 Email Security Appliance의 성능 사양이 나와 있고, 표 3에는 어플라이언스의 하드웨어 사양이 나와 있으며, 표 4에는 가상 어플라이언스의 사양이 나와 있고, 표 5에는 Security Management Appliance의 사양이 나와 있습니다.

표 2. Email Security Appliance 성능 사양

구축	모델	디스크 공간	RAID 미러링	메모리	CPU
대기업	ESA C690	2.4 TB (600 x 4)	예(RAID 10)	32 GB DDR4	2 x 2.4 GHz, 6코어
대기업	ESA C690X	4.8 TB (600 x 8)	예(RAID 10)	32 GB DDR4	2 x 2.4 GHz, 6코어
대기업	ESA C680	1.8 TB (300 x 6)	예(RAID 10)	32 GB DDR3	2 x 2.0 GHz, 6코어
중견기업	ESA C390	1.2 TB (600 x 2)	예(RAID 10)	16 GB DDR4	1 x 2.4 GHz, 6코어
중견기업	ESA C380	1.2 TB (600 x 2)	예(RAID 10)	16 GB DDR3	1 x 2.0 GHz, 6코어
중소기업 또는 지사	ESA C190	1.2 TB (600 x 2)	예(RAID 10)	8 GB DDR4	1 x 1.9 GHz, 6코어
중소기업 또는 지사	ESA C170	500 GB (250 x 2)	예(RAID 10)	4 GB DDR3	1 x 2.8 GHz, 2코어

참고: 정확한 규모 결정을 위해 Cisco 콘텐츠 보안 전문가와 함께 최대 이메일 전달 속도와 평균 메시지 크기를 체크하여 선택한 항목을 확인해 주십시오.

표 3. Email Security Appliance 하드웨어 사양

모델	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
Rack Units (RU)	2RU	2RU	2RU	1RU	2RU	1RU	1RU
크기(H x W x D)	3.4 x 19 x 29인치 (8.6 x 48.3 x 73.7cm)	3.4 x 19 x 29인치 (8.6 x 48.3 x 73.7cm)	3.5 x 19 x 29 인치 (8.9 x 48.3 x 73.7cm)	1.7 x 19 x 31인치 (4.3 x 48.3 x 78.7cm)	3.5 x 19 x 29 인치 (8.9 x 48.3 x 73.7cm)	1.7 x 19 x 31인치 (4.3 x 48.3 x 78.7cm)	1.67 x 16.9 x 15.5인치 (4.24 x 42.9 x 39.4cm)
DC 전원 옵션	예(930W)	예(930W)	예(930W)	아니요	예(930W)	아니요	아니요
원격 전원 제어	예	예	예	예	예	예	아니요
Redundant power supply	예	예	예	예	예	예(액세서리 옵션)	아니요
핫 스왑 가능한 하드 디스크	예	예	예	예	예	예	예
전력 소비량	2216.5BTU/시간	2216.5BTU/시간	2216.5BTU/시간	2626BTU/시간	2216.5BTU/시	2626BTU/시간	1364BTU/시간
전력 공급 장치	650W	650W	650W	770W	650W	770W	400W
이더넷 인터페이스	6-포트 1GBASE-T 구리 네트워크 인터페이스(NIC), RJ-45	6-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45	4-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45	6-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45	4-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45	2-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45	2-포트 1GBASE-T 구리 네트워크 인터페이스 (NIC), RJ-45
속도(Mbps)	10/100/1000, 자동 협상	10/100/1000, 자동 협상	10/100/1000, 자동 협상	10/100/1000, 자동 협상	10/100/1000, 자동 협상	10/100/1000, 자동 협상	10/100/1000, 자동 협상
파이버 옵션	예(개별 SKU) 2-포트 1GBASE-SX 파이버: ESA-C690-1G 2-포트 10GBASE-SR 파이버: ESA-C690-10G	예(개별 SKU) 2-포트 1GBASE-SX 파이버: ESA-C690-1G 2-포트 10GBASE - SR 파이버: ESA-C690-10G	예(개별 SKU) 2-포트 1GBASE-SX 파이버: ESA-C680-1G 2-포트 10GBASE - SR 파이버: ESA-C680-10G	아니요	아니요	No아니요	아니요

모델	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
HD 크기	4개의 600GB 하드 디스크 드라이브(2.5" 10K SAS 4Kn)가 SAS 드라이브에 대해 핫스왑 가능한 액세스를 제공하는 전면 패널 드라이브 베이에 설치됨	8개의 600GB 하드 디스크 드라이브(2.5" 10K SAS 4Kn)가 SAS 드라이브에 대해 핫스왑 가능한 액세스를 제공하는 전면 패널 드라이브 베이에 설치됨	Cisco C680 Email Security 어플라이언스에는 6개의 300G HDD가 있음	2개의 600GB 하드 디스크 드라이브(2.5″ 10K SAS 4Kn)가 SAS 드라이브에 대해 핫스왑 가능한 액세스를 제공하는 전면 패널 드라이브 베이에 설치됨	Cisco C380 Email Security 어플라이언스에는 2개의 600G HDD가 있음	2개의 600GB 하드 디스크 드라이브(2.5″ 10K SAS 4Kn)가 SAS 드라이브에 대해 핫스왑 가능한 액세스를 제공하는 전면 패널 드라이브 베이에 설치됨	250 GB, RAID 1
CPU	2개의 E5-2620 v3 프로세서	2개의 E5-2620 v3 프로세서	2개의 Intel Xeon E5-2620 Series 프로세서(2.0G, 6C)	1개의 E5-2620 v3 프로세서	1개의 Intel Xeon ES-2620 Series 프로세서(2.0G, 6C)	1개의 E5-2609 v3 프로세서	1x2(듀얼 코어 1개)
RAM	4개의 8GB DDR4-2133 DIMM1	4개의 8GB DDR4-2133 DIMM1	8개의 4GB DDR3-1600-MHz RDIMM DRAM	2개의 8GB DDR4-2133 DIMM1	4개의 4GB DDR3-1600-MHz RDIMM DRAM	1개의 8GB DDR4-2133 DIMM1	4 GB

표 4. Email Security Virtual Appliance 사양

이메일 사용자				
	Model	**Disk**	**Memory**	**Cores**
평가 전용	ESAV C000v	200 GB (10K RPM SAS)	4 GB	1 (2.7 GHz)
소규모 기업 직원 수 최대 1000명	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
중견기업(직원 수 최대 5,000명)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2.7 GHz)
대기업 및 서비스 제공업체	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2.7 GHz)
Servers				
Cisco UCS	VMware ESXi 5.0, 5.1 및 5.5 하이퍼바이저			

표 5. Secure Management Appliance M-Series 플랫폼 사양

모델	SMA M690/690X/680	SMA M390/380	SMA M190/M170
사용자 수	10,000명 이상	최대 10,000명	최대 1,000명

구축 위치

다음과 같이 Cisco 이메일 보안 솔루션을 구축할 수 있습니다.

- **온프레미스:** Email Security Appliance는 일반적으로 방화벽 밖의 네트워크 에지(소위 비무장지대)에 구축되는 게이트웨이입니다. 수신 SMTP(Simple Mail Transfer Protocol) 트래픽은 메일 교환 레코드에 의해 설정된 사양에 따라 어플라이언스의 데이터 인터페이스로 전달됩니다. 어플라이언스는 해당 트래픽을 필터링하여 네트워크 메일 서버에 다시 전달합니다. 또한, 메일 서버는 발신 메일을 데이터 인터페이스에 전달하여 발신 정책에 따라 필터링한 후 외부 대상에 전달합니다.
- **가상:** 소규모 지사에서 Cisco UCS를 실행하면 가상 어플라이언스를 Cisco Web Security Virtual Appliance와 같은 다른 Cisco 제품과 함께 호스팅할 수 있습니다. 이러한 제품을 함께 사용하면 이에 상응하는 하드웨어 제품과 동일한 수준의 보호 기능이 구현될 뿐만 아니라 공간 및 전원 리소스 관련 비용이 절감됩니다. Secure

Management Appliance 또는 Virtual Appliance를 사용하여 이러한 맞춤형 구축을 중앙 집중식으로 관리할 수 있습니다.

클라우드 보안을 위한 옵션

Cisco Cloud Email Security는 이메일 보안을 위한 유연한 구축 모델을 제공합니다. 이 제품을 사용하면 온사이트 이메일 보안 인프라 없이 공동 관리를 통해 비용을 절감할 수 있습니다.

Cisco Hybrid Email Security는 Cloud Email Security의 이점뿐만 아니라 메시지 암호화에 대한 고급 아웃바운드 제어 및 온사이트 DLP를 제공합니다. 이 하이브리드 솔루션을 사용하면 원하는 속도로 클라우드 솔루션으로 전환할 수 있습니다.

Cisco Email Security: 물리적 및 가상 어플라이언스 라이선스

가상 어플라이언스의 라이선스는 Cisco Email Security Inbound, Email Security Outbound, Email Security Premium 번들 등 모든 이메일 보안 소프트웨어 번들에 포함됩니다. 이 라이선스는 번들에 포함된 나머지 소프트웨어 서비스와 기간이 동일하며, 구매한 사용자 수를 준수하는 한 필요한 수의 가상 인스턴스에 대해 사용할 수 있습니다. Email Security Appliance 라이선스는 모든 이메일 보안 소프트웨어 번들에 포함됩니다. 지원해야 하는 사서함 수에 적합한 라이선스를 구매한 후 적합한 온프레미스 어플라이언스를 구매하십시오. 가상 어플라이언스의 경우 소프트웨어 라이선스를 주문하여 사용 자격을 얻으십시오.

기간 기반 서브스크립션 라이선스

라이선스는 1년, 3년 또는 5년의 기간 기반 서브스크립션입니다.

라이선스는 1년, 3년 또는 5년의 기간 기반 서브스크립션입니다.

Cisco Email Security 포트폴리오에는 사서함 수에 기반한 계층형 가격이 적용됩니다. 세일즈 및 파트너 담당자가 올바른 고객 구축을 결정할 수 있도록 도와드립니다.

Email Security 소프트웨어 라이선스

3가지 Email Security 소프트웨어 라이선스 번들 제공: Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium. AMP(Advanced Malware Protection)는 별도 구매가 가능합니다. 각 소프트웨어 제품의 주요 구성 요소는 표 6에 나와 있습니다.

표 6. 소프트웨어 구성 요소

번들	설명
Cisco Email Security Inbound Essentials	Cisco Email Security Inbound Essentials 번들은 그레이메일 탐지 기능이 포함된 안티 스팸, Sophos 안티바이러스 솔루션, Outbreak Filter, 위조 이메일 탐지, 클러스터링을 비롯한 이메일 기반 위협 차단 기능을 제공합니다.
Cisco Email Security Outbound Essentials	Cisco Email Security Outbound Essentials 번들은 DLP 컴플라이언스, 이메일 암호화, 클러스터링을 통해 데이터 유출을 방지합니다.
Cisco Email Security Premium	Cisco Email Security Premium 번들에는 위에서 설명한 2가지 Cisco Email Security Essentials 라이선스에 포함된 인바운드 및 아웃바운드 보호 기능이 결합되어 있어 이메일 기반 위협에 대한 보호 및 중요 데이터 유출 방지 기능을 제공합니다.
독립형 서비스	**설명**
Cisco Advanced Malware Protection	Cisco AMP(Advanced Malware Protection)는 Cisco Email Security 소프트웨어 번들과 함께 개별적으로 선택하여 구매할 수 있습니다. AMP는 악성코드 탐지 및 차단, 지속적인 분석, 회귀적 알림 등의 기능을 제공하는 포괄적인 악성코드 방어 솔루션입니다. Advanced Malware Protection은 파일 평판 점수 및 차단, 정적 및 동적 파일 분석(샌드박싱), 파일 회귀

	분석을 통해 이메일 게이트웨이를 통과한 후에도 위협을 지속적으로 분석하여 Cisco Email Security Appliances에서 이미 제공되는 악성코드 탐지 및 차단 기능을 보강합니다. 모든 필수 하드웨어를 구매할 경우, AMP Threat Grid의 무제한 라이선스를 받게 됩니다. 또한 Threat Grid 어플라이언스와 함께 AMP 시스템은 AMP 프라이빗 클라우드 라이선스를 사용하여 온프레미스에 완벽하게 구축될 수 있습니다. 이것은 AMP 퍼블릭 클라우드의 사용을 허용하지 않는 엄격한 정책 요구 사항을 지닌 고객에게 중요합니다.
그레이메일 안전 수신 거부	정말로 안전한 "수신 거부" 옵션으로 그레이메일에 태그를 지정할 수 있습니다. 이 태그는 엔드 유저를 대신하여 "수신 거부" 작업을 매우 안전하게 관리합니다. 또한 여러 가지 다른 그레이메일 수신 거부 요청도 모니터링합니다. 이러한 모든 요청을 LDAP 그룹 정책 레벨에서 관리할 수 있습니다.

소프트웨어 라이선스 계약

Cisco End-User License Agreement 및 Web Security Supplemental End-User License Agreement가 각 소프트웨어 라이선스 구매 시 제공됩니다.

소프트웨어 서브스크립션 지원

모든 이메일 보안 라이선스에는 비즈니스 크리티컬 애플리케이션을 사용 가능하고, 매우 안전하며, 최고 성능으로 운영되도록 하는 데 필수적인 소프트웨어 서브스크립션 지원이 포함됩니다. 이 지원을 통해 고객은 구매한 소프트웨어 서브스크립션의 전체 기간 동안 다음과 같은 서비스를 이용할 수 있습니다.

- 최신 기능으로 애플리케이션의 최고 성능을 유지하기 위한 소프트웨어 업데이트 및 주요 업그레이드
- 신속하고 전문적인 지원을 제공하는 Cisco Technical Assistance Center
- 사내 전문 지식을 구축 및 확대하고 비즈니스 민첩성을 증대할 수 있는 온라인 툴
- 추가 지식 및 교육 기회를 제공하는 협업 방식 학습

Cisco Services

표 7 에는 Cisco 이메일 보안 솔루션에 대해 사용할 수 있는 Cisco Services가 요약되어 있습니다.

표 7. Cisco Services

서비스	설명
Cisco branded services	• Cisco Security Planning and Design Service: 강력한 보안 솔루션을 신속하고 비용 효율적으로 구축할 수 있도록 지원 • Cisco Email Security Configuration and Installation Remote Service: 솔루션을 설치, 구성 및 테스트하여 보안 위험 완화 • Cisco Security Optimization Service: 설계, 성능 조정, 시스템 변경 지원 등을 통해 새로운 보안 위협에 대응할 수 있도록 진화하는 보안 시스템 지원
협업 및 파트너 서비스	• Cisco Collaborative Professional Services Network Device Security Assessment Service: 보안상의 허점을 찾아내 더 강력한 네트워크 환경을 유지할 수 있도록 지원 • Cisco Smart Care Service: 네트워크 성능에 대한 매우 안전한 가시성에 기반한 인텔리전스를 사용하여 사전 예방적으로 모니터링함으로써 비즈니스를 최상의 상태로 실행 가능 • Cisco 파트너는 계획, 설계, 구현 및 최적화 라이프사이클 전체에서 다양한 추가 서비스도 제공
Cisco 파이낸싱	Cisco Capital®에서 비즈니스 요구사항에 부합하는 금융 지원 솔루션을 맞춤화하여 제공할 수 있습니다. 조속히 Cisco 기술을 활용하여 더욱 신속하게 비즈니스 혜택을 누리십시오.

Cisco Smart Net Total Care 지원 서비스

기술 투자의 가치를 극대화하려면 Cisco Smart Net Total Care™ Service를 구매하여 이메일 보안 어플라이언스와 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. 자세한 내용은 https://www.cisco.com/c/en/us/services/support/smart-net-total-care.html을 참조하십시오.

Cisco Email Security Appliance 를 평가하는 방법

Cisco Email Security Appliance C-Series 및 X-Series 플랫폼의 장점을 알아보려면 구매 전 시험 사용(Try Before You Buy) 프로그램을 이용하는 것이 가장 좋습니다. 기업 네트워크에서 무료로 45일간 시험해 볼 수 있도록 완전한 기능을 갖춘 평가 어플라이언스를 받으려면 이 페이지를 방문하십시오.

Cisco Cloud Email Security Services를 평가하는 방법

클라우드 기반 솔루션은 이메일 보안을 위한 유연한 구축 모델을 제공하는 모든 것이 포함된 신뢰할 수 있는 서비스입니다. 이 솔루션을 사용하면 온사이트 이메일 보안 인프라 없이 공동 관리를 통해 개인 비용을 절감할 수 있습니다. 담당 Cisco 어카운트 팀 또는 리셀러가 무료 45일 평가 설치를 도와드릴 수 있습니다.

Cisco Email Security Virtual Appliance를 평가하는 방법

1. https://www.cisco.com/go/esa로 이동합니다.
2. 오른쪽에 있는 "Support(지원)" 아래에서 "Software Downloads, Release and General Information(소프트웨어 다운로드, 릴리스 및 일반 정보)"을 클릭합니다. "Download Software(소프트웨어 다운로드)"를 클릭한 다음 모델에 대한 링크를 클릭하면 제공되는 다운로드 가능한 가상 머신 이미지가 표시됩니다. 또한 다운로드 가능한 XML 평가 라이선스도 확인할 수 있습니다. 이미지 및 XML 평가 라이선스 중 하나를 다운로드해야 합니다.
3. Cisco.com에서 다음 설명서를 다운로드합니다.
   a. Cisco Security Virtual Appliance 설치 가이드
   b. Cisco AsyncOS® 9.5 for Email 릴리스 노트
4. Cisco Security Virtual Appliance Installation Guide의 지침에 따라 사용을 시작합니다. Cisco Content Security Virtual Appliance 평가는 Cisco SMARTnet Total Care Service에 포함되지 않으므로 지원되지 않습니다.

워런티 정보

워런티 정보는 Cisco.com의 제품 워런티 페이지에서 확인하십시오.

왜 Cisco를 선택해야 할까요?

네트워크에 있어서 보안은 그 어느 때보다도 중요합니다. 위협과 위험이 상존하고 기밀 유지와 제어의 문제가 우려되는 상황에서 사업의 연속성을 제공하고 가치 있는 정보를 보호하며 브랜드 명성을 유지하려면 보안이 필수입니다. 기업 네트워크에 촘촘히 구축된 Cisco의 통합 보안 솔루션은 운영 중단 없이 비즈니스를 보호할 수 있는 강화된 가시성과 제어력을 제공합니다. 시장 주도력, 공격 전, 중, 후 전 단계에 구현되는 지능형 위협 차단, 혁신적인 제품, 긴 제품 수명을 모두 갖춘 Cisco는 여러분의 보안 요구사항에 가장 적합한 공급업체가 될 것입니다.

Cisco Capital

시스코 금융 지원 솔루션

Cisco Capital 파이낸싱을 통해 목표를 달성하는 데 필요한 기술을 습득하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 구입 시 Cisco Capital의 금융 지원 솔루션을 유연하게 활용할 수 있습니다. 또한, 정해진 일자에 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세히 알아보십시오.

추가 정보

자세한 내용은 https://www.cisco.com/go/emailsecurity를 참조하십시오. 또는 Three Ways to Try Email Security for Free를 통해 잘 알려진 솔루션을 이용해 보십시오.

미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

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 C78-729751-17 09/17