Cisco Cloud Security:
올바른 이메일 보안 구축 방식 선택

목차

Executive Summary

규모에 상관없이 모든 기업은 증가하는 메일 볼륨 및 갈수록 진화하는 새로운 위협이라는 동일한 당면 과제를 안고 있습니다. Cisco Cloud Security 서비스 제품군은 Fortune 선정 1000대 기업 중 40%를 인바운드 위협 및 아웃바운드 데이터 유출 가능성으로부터 보호하는 업계 최고의 이메일 기술의 안정적 토대를 기반으로 구축된 최고의 구축 모델을 고객에게 제공합니다.

오늘날의 이메일 기반 위협은 바이러스, 스팸, 오탐, DDoS(distributed denial-of-service) 공격, 스파이웨어, 피싱(사기), 규정 준수 위반, 데이터 유출 등으로 구성되어 있습니다. Cisco® Cloud Security는 쉽게 구축 및 관리할 수 있는 예방 및 사후 대응형 보안 조치를 통합함으로써 대규모/소규모 기업에서 발생하는 문제를 해결합니다.

이메일 위협이 지속적으로 증가하고 진화하면서 조직은 IT 팀에 보다 철저한 보호, 높은 효율성 및 유연성을 요구하고 있습니다. IT 팀은 이러한 요구를 충족하기 위해 비즈니스 규정을 준수하는 솔루션을 설계할 수 있도록 유연성을 높여야 합니다. 유연성을 높이면 이메일 보안을 위한 구축 옵션을 적절하게 선택할 수 있습니다. 유연성을 높여야 하는 고객은 크게 세 가지 범주로 구분할 수 있습니다. 첫째로, 클라우드 또는 SaaS(Software as a Service) 솔루션을 사용함으로써 스팸 문제를 아웃소싱하여 운영 효율성을 개선하려는 고객이 있습니다. 둘째로, 온프레미스(구내 장비) 이메일 보안 인프라를 구축하여 민감한 아웃바운드 정보에 대한 통제력을 최대한 유지하려는 고객이 있습니다. 세 번째 범주에는 하이브리드(분할형) 방식을 사용하려는 고객이 포함됩니다. 이러한 방식에는 클라우드 솔루션을 사용하여 효율성을 높이는 동시에 온프레미스(구내 장비) 어플라이언스 기반 구축의 이점은 계속 활용하는 방식이 포함됩니다.

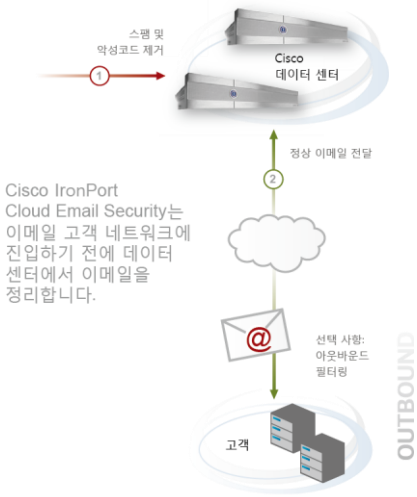
솔루션과 벤더를 선택할 때는 조직의 기존/향후 비즈니스 요구 사항을 기반으로 하여 적절한 선택을 해야 합니다. 이메일 보호의 경우 고객은 Cisco Cloud Security 서비스를 통해 사용 가능한 모든 폼 팩터 중에서 선택할 수 있습니다. 이러한 폼 팩터는 모두 동일한 업계 최고의 Cisco IronPort® 이메일 보안 기술을 기반으로 구축되었으며 Cisco SenderBase® Network를 통해 지원됩니다. 또한 모든 이메일 관리자의 요구를 충족하기에 적합합니다.

- Cisco IronPort Cloud Email Security
- Cisco IronPort Hybrid Email Security
- Cisco IronPort Managed Email Security

이 문서에서는 Cisco Cloud Security에서 제공하는 다양한 이메일 보안 서비스 옵션과, 조직의 비즈니스 요구에 가장 적합한 솔루션을 선택하는 방법을 설명합니다.

Cloud Email Security

Cisco IronPort Cloud Email Security는 지리적으로 분산된 여러 Cisco 관리 데이터 센터에 구축된 이메일 인프라를 통해 업계 최고의 이메일 보안 기술을 제공합니다.



클라우드 이메일 보안 솔루션은 다음과 같은 이점을 원하는 조직에 적합합니다.

- 데이터 센터 사용 공간을 줄여 랙 공간, 전력/냉각 수요 및 관리 오버헤드 감소
- TCO(총 소유 비용) 절감
- 현재 및 향후 용량 요건에 맞게 구축 시간 단축

클라우드 솔루션을 선택할 때는 이러한 비즈니스 요소를 반드시 고려해야 합니다. 하지만 기존 클라우드 이메일 보안 솔루션의 경우 솔루션의 효율성을 심각하게 제한할 수 있는 여러 가지 단점이 있습니다. 아래 섹션에서는 이러한 제한에 대해 간략하게 살펴보고 Cisco IronPort Cloud Email Security에서 이러한 문제를 해결하는 방식에 대해 설명합니다.

안티 스팸 효율성

스팸의 양은 매년 2배씩 증가해 왔습니다. 그 결과 조직에서는 스팸 차단 효율성이 높은 안티 스팸 벤더를 찾고 있습니다. 놓치는 스팸의 비율이 증가하면서 사용자의 받은 편지함에 배달되는 실제 메시지 수가 매년 2배로 증가하고 있습니다. 스팸 차단율도 높아야 할 뿐 아니라 합법적 이메일 메시지가 스팸으로 분류되는 오탐률도 낮아야 합니다. 기존 이메일 보안 벤더의 차단율은 약 95%이지만 오탐률이 매우 높습니다. 이로 인해 최종 사용자는 받은 편지함에서 스팸 메시지를 직접 확인해야 하며, 최악의 경우에는 관리자에게 계속 전화를 걸어 합법적인 업무 이메일이 이메일 보안 벤더에 의해 스팸으로 분류되어 격리되었을 가능성이 의심됨을 보고해야 합니다.

Cisco는 안티 스팸 기술 업계를 선도하는 기업으로, 완벽에 가까운 수치인 99% 이상의 차단율을 일관되게 제공하는 동시에 메시지 1백만 건당 오탐 1건 미만이라는 업계 최고의 오탐률을 제공합니다. 이는 Cisco 솔루션의 주요 차별화 요소 중 하나이며, 고객이 경쟁업체의 제품이 아닌 Cisco 제품을 지속적으로 선택하는 핵심적인 이유이기도 합니다.

최대한의 데이터 보호

Cisco 클라우드 기반 이메일 보안은 각 고객의 인프라를 완벽하게 격리한다는 점에서 고유합니다. 이로 인해 최고 레벨의 데이터 보호 기능이 제공될 뿐 아니라, 일반적인 클라우드 기반 이메일 보안 벤더에서 겪어 온 다운타임, 데이터 오염 등의 문제도 방지할 수 있습니다.

이 서비스는 고객 이메일과 데이터를 물리적으로 분리하므로 클라우드 폼 팩터에서 데이터 오염 위험을 최고 레벨로 보호합니다.

아웃바운드 제어

DLP(데이터 유출 방지)는 보안 사고 건수 및 그에 따른 비용이 증가하고 있는 만큼 기업에게 중대한 과제입니다. 데이터 손실은 악의적인 시도이든 실수에 의한 것이든 기업의 브랜드 가치와 주주 가치를 떨어뜨리고 영업권과 평판에도 타격을 줄 수 있습니다. 또한 조직은 민감한 데이터를 처리해야 하는 방법에 대해 엄격한 요건을 적용하는 다양한 규정도 준수해야 합니다.

조직이 비즈니스 문제를 적절하게 해결할 수 있도록 Cisco는 완벽하게 통합된 이메일 DLP 솔루션을 제공합니다. 이 솔루션은 HIPAA, SOX, GLBA 및 주 프라이버시 관련 법률을 비롯하여 100개가 넘는 사전 정의된 템플릿을 제공합니다. 또한 통합 암호화 기능도 추가적인 치료 레벨을 제공합니다. Cisco IronPort Email DLP 및 Cisco IronPort Email Encryption을 사용하면 민감한 데이터를 빠르고 정확하게 보호하고 클라우드 또는 하이브리드 폼 팩터에서 규정을 준수할 수 있습니다.

고급 제어

아주 작은 규모의 조직이라도 바이러스, 스팸, 오탐, DDoS 공격, 스파이웨어, 피싱, 규정 준수 위반, 데이터 유출 등의 이메일로 인한 위협을 매일 경험하고 있습니다. 하지만 기존의 클라우드 이메일 보안 벤더는 매우 기초적인 이메일 보안 제어 기능만을 제공합니다. 이로 인해 고객은 벤더가 제공하는 기능의 범위 내에서만 이메일 보안을 유지할 수 있습니다.

Cisco IronPort Cloud Email Security는 이메일 보안을 강화하기 위해 활용 가능한 엔터프라이즈급 고급 제어 기능 집합을 고객에게 제공합니다. 여기에는 바운스 확인, SPF, DKIM, TLS, 규정 준수 사전, 스마트 식별자, 다양한 고급 콘텐츠 필터 규칙 등의 기능이 포함됩니다. 이러한 모든 고급 제어 기능은 추가 비용 없이 제공됩니다.

메시지 추적

보안 요소의 성능과 정확성도 중요하지만 메시지 추적 기능도 그와 동일하게 중요한 측면입니다. 이메일 관리자는 클라우드 이메일 보안 솔루션을 통과한 메시지의 특성을 즉시 확인할 수 있는 유연성을 원합니다. 기존 클라우드 이메일 보안 벤더를 이용하는 고객은 고객 지원을 위한 티켓을 연 다음 답변을 받을 때까지 때로는 몇 시간 동안 기다려야 합니다. 특히 CEO가 몇 시간 전에 배달되었어야 하는 비즈니스 크리티컬 이메일 메시지에 대해 문의 전화를 거는 등의 경우 이러한 과정은 관리자에게 대단히 번거로울 수 있습니다.

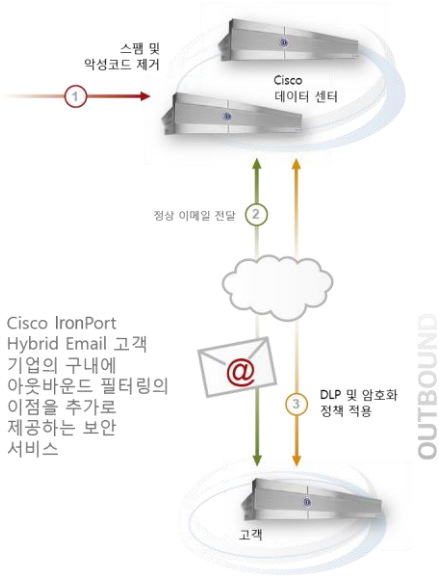
Cisco IronPort Cloud Email Security는 실시간으로 메시지를 검색할 수 있는 쉽게 사용 가능한 메시지 추적 인터페이스를 고객에게 제공합니다. 따라서 관리자는 벤더가 열린 티켓에 응답할 때까지 몇 시간씩 기다리는 대신 중요한 전화를 받아 몇 분 내에 답변을 할 수 있습니다.

보고

메시지 추적뿐 아니라 이메일 보안 보고 기능도 이메일 관리자에게는 매우 중요합니다. Cisco IronPort Cloud Email Security는 매우 정교한 관리, 모니터링 및 보고 툴을 제공합니다. 이 서비스에 포함된 고유한 보고 시스템은 조직 이메일 인프라를 이동하는 메일에 대해 실시간 정보와 이력 정보를 모두 제공합니다. 이러한 툴은 관리자가 실시간으로 중요한 보안 관련 결정을 내리는 데 필요한 정보를 제공하고, 다양한 그래픽이 표시되는 전문적인 보고서를 관리 작업에 사용할 수 있도록 내보내며, 보고서를 특정 이메일 주소로 자동 배달하도록 예약하는 기능도 제공합니다.

Hybrid Email Security

Cisco IronPort Hybrid Email Security는 고객이 비즈니스 요구를 가장 효율적으로 충족하는 방식으로 이메일 보안을 구축할 수 있는 솔루션을 선택할 수 있는 고유한 이메일 보안 서비스입니다. 이 아키텍처에는 클라우드 기반 폼 팩터와 온프레미스(구내 장비) 폼 팩터로 구분되는 이메일 보안 인프라가 포함됩니다. 조직은 대개 클라우드 인프라를 통해 안티 스팸, 안티바이러스 등의 인바운드 보안 제어 기능을 구축하는 동시에 온프레미스(국내 장비) 어플라이언스를 통해 암호화 및 DLP(데이터 유출 방지) 솔루션을 활용하여 민감한 정보를 보호합니다.



하이브리드 이메일 보안 솔루션은 다음 비즈니스 요건 중 일부를 충족하고자 하는 조직에 적합합니다.

- 클라우드 폼 팩터의 이점 활용
- 아웃바운드 데이터 온프레미스(구내 장비)의 제어 기능 유지
- 관리 간소화

고객은 비즈니스 계획 예측에 도움이 되는 동급 최고의 이메일 보안 솔루션을 사용하고자 합니다. 아래 섹션에서는 이러한 각 비즈니스 요건에 대해 살펴보고 Cisco IronPort Hybrid Email Security가 이러한 문제를 해결하는 방식에 대해 설명합니다.

아웃바운드 제어

클라우드 제품과 마찬가지로 하이브리드 폼 팩터에서도 온프레미스(구내 장비)에서 동일한 기능이 제공됩니다. 고급 콘텐츠 필터링용 온프레미스(구내 장비) 솔루션을 활용하고자 하는 고객은 클라우드 및 온프레미스(구내 장비) 어플라이언스 간의 제어 기능을 분할하여 이러한 목표를 달성할 수 있는 독특한 서비스인 Cisco IronPort Hybrid Email Security를 사용할 수 있습니다. 고객은 환경에 가장 적합한 방법을 선택할 수 있습니다.

간소화된 관리

하이브리드 구축 옵션은 사업적으로 효율적이기는 하지만, 이 옵션을 사용하는 경우에는 이메일이 두 구축 집합에서 이동하므로 두 폼 팩터에서 모두 데이터 추적 및 보고를 계속해서 처리해야 합니다. 가령 CEO가 이메일 관리자에게 전화를 걸어 2시간 전에 받았어야 하는 이메일에 대해 문의하는 경우 관리자는 두 인터페이스에 각각 별도로 로그인하여 메시지를 검색하거나 벤더에 대해 티켓을 열어 CEO 메시지 처리 방식을 확인해야 할 필요가 없어야 합니다. CEO에게 신속하게 답변을 제시하려면 두 구축에서 모두 메시지를 검색하는 인터페이스가 제공되어야 합니다. 마찬가지로, 여러 인터페이스로 이동하여 이메일 흐름에 대한 보고서를 보고 통계를 다운로드하는 대신 공통의 인터페이스를 사용할 수 있어야 관리자의 효율성을 크게 높일 수 있습니다.

Cisco IronPort Hybrid Email Security는 클라우드 및 온프레미스(구내 장비) 구축에서 모두 사용 가능한 간편한 인터페이스에서 실시간 메시지 추적 및 보고 기능을 고객에게 제공합니다. 관리자는 메시지 추적 인터페이스를 사용하여 관심 메시지의 상태를 즉시 파악할 수 있습니다. 또한 미리 작성된 많은 보고서를 확인하여 PDF 형식으로 다운로드하고 CSV 형식으로 내보낼 수 있으며 시간 환경 설정에 따라 이메일로 보고서를 배달하도록 예약할 수도 있습니다. 이러한 추적 및 보고 기능을 활용하면 관리 작업을 대폭 간소화할 수 있으므로 효율성을 크게 높일 수 있습니다.

비즈니스 계획 예측

조직은 솔루션을 선택할 때 기술적 측면뿐 아니라 사업적 측면도 평가해야 합니다. 오늘날에는 CFO가 IT 중역에게 비용을 줄이고 예측 가능성을 높이도록 요구하고 있습니다. 이러한 비용에는 초기 및 지속적으로 지출되는 하드웨어/소프트웨어 지출이 모두 포함됩니다. 또한 기업의 CapEx 예산액은 그다지 유동적이지 않습니다. 기존 클라우드 솔루션은 예측 가능한 사용자당 연간 가격 모델, 스팸 증가량을 충족하는 데 필요한 향후 용량 보장, 그리고 CapEx 모델에 비해 보다 유동적인 OpEx(운영비용) 모델을 비롯한 여러 이점을 고객에게 제공합니다.

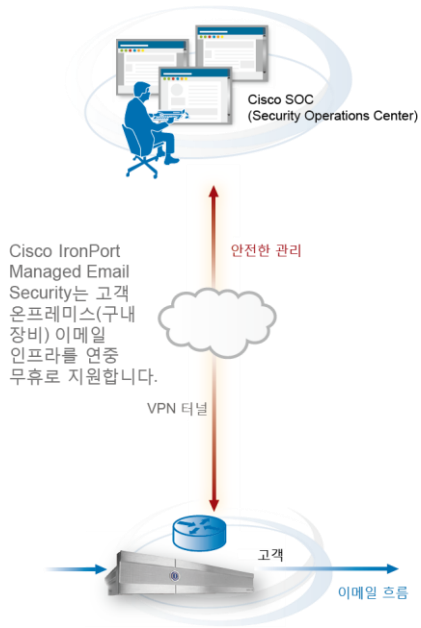
Cisco IronPort Hybrid Email Security는 기존 클라우드 벤더가 제공하는 것과 동일한 이점을 클라우드 및 온프레미스(구내 장비) 구축 폼 팩터에서 모두 제공합니다. 뿐만 아니라 간단한 사용자당 연간 가격으로 사용 가능한 전체 인프라에서 고객에게 다음과 같은 추가적인 이점이 제공됩니다.

- 초기 하드웨어 인프라
- 지속적인 용량
- 소프트웨어 라이센스
- OpEx(운영비용) 및 CapEx 대금 청구 방식 비교

Cisco IronPort Hybrid Email Security를 사용하는 경우에는 고유한 소프트웨어 라이센싱 방식이 적용됩니다. 고객은 단일 패키지에서 하드웨어, 지원 및 소프트웨어 라이센스를 받을 수 있습니다. 고객은 선택한 어떤 위치에나 소프트웨어 라이센스를 구축할 수 있으므로 라이센스 용량 중 일부는 클라우드에서, 나머지는 온프레미스(구내 장비)에서 사용할 수 있습니다. 예를 들어 대다수의 고객은 안티 스팸 및 안티바이러스를 클라우드에서 구축하고 암호화 및 콘텐츠 필터링은 온프레미스(구내 장비)에서 구축합니다. 그러나 아웃바운드 스캐닝의 경우 고객은 추가 비용 없이 온프레미스(구내 장비) 어플라이언스에도 안티바이러스 솔루션을 유동적으로 구축할 수 있습니다.

Managed Email Security

Cisco IronPort Managed Email Security는 IT 관리자가 전략적 이니셔티브에 주력할 수 있도록 조직의 이메일 배달 인프라를 모니터링 및 관리하는 서비스입니다. 이 서비스를 사용하는 경우 스팸 양 증가로 인한 추가 하드웨어 예산을 책정하고 직원을 지속적으로 교육할 필요가 없습니다. 고객은 온사이트 이메일 보안 어플라이언스에서 제공하는 최고 레벨의 데이터 보안 기능을 활용하는 동시에 일부 또는 모든 유지 및 관리 업무를 유동적으로 위임할 수도 있습니다.

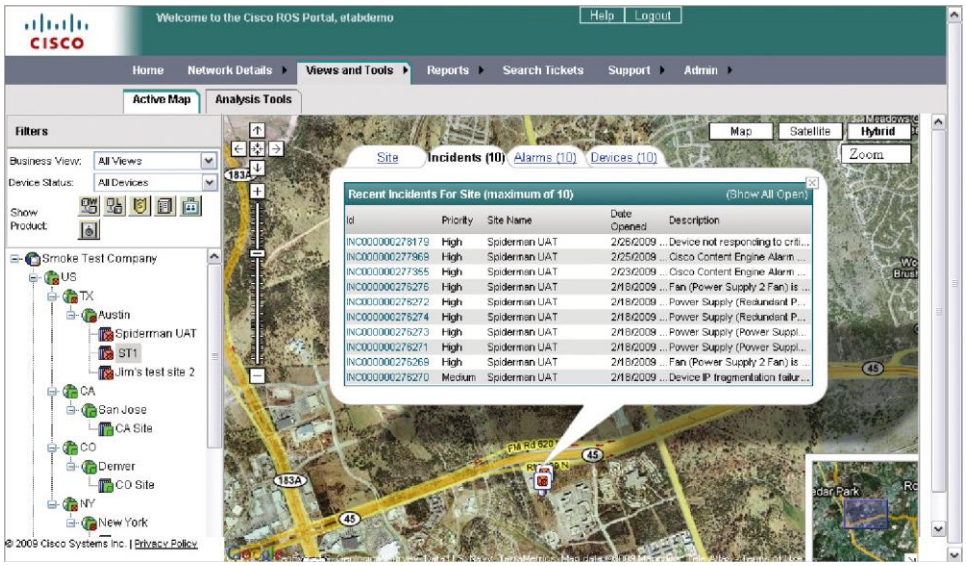


Managed Email Security 솔루션은 다음 문제를 해결해야 하는 조직에 적합합니다.

- 숙련된 직원을 찾기 어려운 조직
- 전략적 IT 이니셔티브에 주력하기 위해 리소스를 확보하려는 조직
- 예측 가능한 가격으로 온프레미스(구내 장비) 이메일 보안 솔루션을 사용하려는 조직

원격 모니터링 및 관리

Cisco IronPort Managed Email Security를 사용하는 경우 Cisco IronPort 어플라이언스는 고객 데이터 센터에 구축되며 Cisco Remote Management Services 팀의 이메일 보안 전문가에 의해 항상 원격으로 모니터링되고 관리됩니다. Cisco 팀은 우수성이 입증된 ITIL(Information Technology Infrastructure Library) 기반 방법과 프로세스를 사용하여 비즈니스 연속성을 보장하는 신뢰할 수 있는 솔루션을 제공합니다. 고객이 자체 네트워크를 최종적으로 제어할 수 있으며, 쉽게 사용 가능한 포털을 통해 네트워크의 상태를 실시간으로 확인할 수 있습니다.



고객 지원 포털의 사고 레코드 및 위치 이미지

유동적인 관리 모델

대부분의 관리되는 통신 사업자는 고객이 자체 구내에 구축된 이메일 인프라에 대한 관리를 제어하지 못하도록 제한합니다. 일부 고객의 경우에는 이러한 방식이 적합할 수도 있지만 대부분의 이메일 관리자는 이메일 배달 상태, 최근 추가된 콘텐츠 정책을 가장 많이 위반하는 직원 등의 문의에 대해 빠르고 간단한 응답을 제공할 수 있는 인프라에 액세스하고자 합니다. 관리 권한이 없으면 관리자는 아주 사소한 요청이라도 통신 사업자에게 문의하여 답변을 받아야 합니다.

Cisco IronPort Managed Email Security를 사용하는 경우 고객은 이메일 인프라를 가장 효율적으로 관리하는 방법을 선택할 수 있습니다. 이 서비스는 조직에 두 가지 옵션을 제공합니다.

- 공동 관리 모델: 이 모델에서는 고객 IT 팀이 확장되어 Cisco가 포함됩니다. 또한 조직의 요구에 따라 주요 이메일 보안 관리 및 모니터링 지원이 제공됩니다. 공동 관리 모델은 유동성이 뛰어나며 사용자 정의를 통해 비즈니스 프로세스에 맞게 조정할 수 있습니다. 고객은 Cisco 서비스 팀의 관리 지원을 통해 지원되는 방식으로 네트워크의 모든 Cisco IronPort 어플라이언스에 항상 모든 권한으로 액세스할 수 있습니다.
- 완전 관리 모델: 이 모델에서는 이메일 보안의 모든 측면을 Cisco 전문가가 원격으로 처리하는 "상시" 서비스를 제공합니다. 이 포괄적인 서비스에는 지속적인 컨피그레이션 지원, 사고 관리, 최신 티켓 추적, 보고 및 기타 운영 기능이 포함되므로 기업 이메일 인프라의 적절한 상태가 항상 보장됩니다.

비즈니스 계획 예측

앞에서 설명한 기타 구축 옵션과 마찬가지로 Cisco IronPort Managed Email Security는 단일 사용자별 연간 가격을 통해 비즈니스 계획 예측 기능을 제공합니다. 여기에는 다음 항목이 포함됩니다.

- 초기 하드웨어 인프라
- 지속적인 용량
- 소프트웨어 라이센스

따라서 고객은 CapEx 비용 모델이 아닌 OpEx(운영비용) 비용 모델을 통해 서비스를 유동적으로 제공받을 수 있습니다. Cisco IronPort Managed Email Security는 이메일 관리자가 원하는 유동적인 관리 모델을 사용하여 최고 레벨의 이메일 보안을 활성화합니다. 어떤 모델을 선택하든 이메일 전문가가 중요한 작업을 관리하고 모니터링합니다. 이 모델을 사용하는 경우 관리자는 사업 확장 등의 보다 전략적인 이니셔티브에 주력할 수 있습니다.

결론

Cisco Cloud Security를 사용하는 조직은 최고의 보안 업체인 Cisco의 이메일 보안 전문가가 지원하는 가장 적합한 이메일 보안 인프라를 선택할 수 있습니다. 비즈니스 요구에 따라 고객은 Cisco IronPort Cloud Email Security, Cisco IronPort Hybrid Email Security, Cisco IronPort Managed Email Security 등 여러 구축 옵션 중 하나를 선택할 수 있습니다. 구축 모델에 관계없이 고객에게는 하드웨어 용량 보장, 예측 가능한 예산 계획 및 간소화된 관리 이점이 제공됩니다. Cisco는 업계 최고의 지원 및 기업 안정성을 통해 지원되는 이메일 보안 서비스로 전 세계의 조직을 지원해 왔습니다.

Cisco Cloud Security에 대한 자세한 내용을 확인하려면 다음 페이지를 참고하십시오.
http://www.ironport.com/products/email_security_services.html

미주 본사
Cisco Systems, Inc.
San Jose, CA

아시아 태평양 본사
Cisco Systems (USA) Pte. Ltd
Singapore

유럽 본사
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco 는 전 세계에 200 개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 (www.cisco.com/go/offices)에 나와 있습니다.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, Cisco logo, DCE 및 Welcome to the Human Network는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 상표입니다. Changing the Way We Work, Live, Play 및 Learn and Cisco Store는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 서비스 마크입니다. Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, Cisco Certified Internetwork Expert 로고, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, Cisco Systems 로고, Cisco Unity, Collaboration Wzithout Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, IronPort 로고, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx 및 WebEx 로고는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 등록 상표입니다.

본 문서 및 웹사이트에 언급된 다른 모든 상표는 각 소유자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (0809R)