



Cisco M-Series Content Security Management Appliance for Email & Web Security Appliances

Cisco M-Series Content Security Management Appliance는 어떤 가치를 제공합니까?

Cisco M-Series Content Security Management Appliances는 단일 관리 인터페이스에서 정책 및 런타임 데이터를 통합하여 Cisco Email & Web Security Appliance의 모든 보고 및 감사 작업을 해결할 중앙 집중식 플랫폼을 제공합니다. 통합 보고 기능으로 웹 사용량, 이메일 활동 및 추이를 모니터링하고 분석함으로써 IT 관리자가 새로운 위협에 신속하게 대처할 수 있습니다.

Cisco M-Series Content Security Management Appliance는 어떤 문제를 해결합니까?

Cisco M-Series Content Security Management Appliance는 리소스 제약을 겪는 현재 IT 팀의 부담을 덜어줍니다. 관리자는 보안부터 통신 시스템까지 다양한 영역에서 전문성을 발휘하고 각 영역의 여러 제품과 시스템을 잘 알며 사용할 수 있어야 합니다. 조직이 커지면 관리의 오버헤드도 기하급수적으로 증가할 수 있습니다.

Cisco M-Series Content Security Management Appliance는 지리적 경계 없이 Cisco X-Series 및 C-Series(이메일 보안), Cisco S-Series(웹 보안) 어플라이언스의 전 범위에 대해 중앙에서 일관성 있는 정책을 적용할 수 있게 합니다. 강력한 Cisco AsyncOS® 운영 체제를 기반으로 하는 Cisco M-Series 어플라이언스는 업계 최고의 확장성과 지원 기능으로 대규모 엔터프라이즈 및 ISP 고객을 수월하게 지원할 수 있습니다.

Cisco M Series Appliance에서 어떤 유형의 이메일 보고를 이용할 수 있습니까?

Cisco M-Series Content Security Management Appliance는 2가지 유형의 이메일 보고를 제공합니다.

- **고급 메시지 추적(Advanced Message Tracking)**— 관리자가 이메일 통신이 발생한 위치와 시점을 파악할 수 있습니다. 여러 이메일 보안 어플라이언스에 대한 메시지 텔레메트리를 발신자, 수신자, 메시지 제목, 기타 고급 매개변수에 따라 검색할 수 있습니다. 그러면 관리자는 전체 검사 결과, 이를테면 스팸/바이러스 판정 또는 정책 위반 및 배달 정보(예: 이메일 인증) 등 모든 검사 결과를 보고할 수 있습니다.
- **Cisco Spam Quarantine**—이 셀프서비스 솔루션은 편리한 웹 기반 또는 이메일 기반 인터페이스를 제공하며 기존 디렉토리 및 메일 시스템과도 간단하게 통합됩니다. 작업은 자동으로 수행되고 자율적으로 관리되므로 용량 오버로드의 위험이 없습니다. 무엇보다도 이 솔루션은 관리자나 최종 사용자에 의한 유지 보수가 필요하지 않습니다. 최종 사용자는 회사 LDAP 디렉토리를 사용하여 인증하거나 표준 기반 IMAP 또는 POP 서버의 경우 정규 이메일 비밀번호를 사용하여 인증할 수 있습니다. 격리 메시지 다이제스트에서 원클릭 인증을 통해 메시지 배포 목록을 관리할 수 있습니다.

M-Series Appliance는 어떤 웹 보고 및 추적 기능을 제공합니까?

Cisco M-Series Appliance는 특별한 위협 상관성 분석 엔진을 통해 현재의 운영 데이터에 대한 전례 없는 통찰력을 제공합니다. IT 관리자는 이를 통해 어떤 규모의 네트워크에서도 정책을 조정하고 인프라를 계획하고 생산성을 평가할 수 있습니다. 여러 이메일 또는 웹 보안 어플라이언스에서 보낸 보고 데이터가 거의 실시간으로 취합됩니다. 이를 중앙에서 통합하여 완벽한 통합형 보안 보고를 수행할 수 있습니다. 모든 M-Series Appliance는 다음 기능을 제공합니다.

- **포괄적인 웹 보고** - 악성코드 위협, 잠재적 감염, 봇넷 활동을 신속하게 파악하여 해결합니다.
- **중앙 웹 보고 보기** 가장 큰 네트워크 위협, 대부분의 사용자에게 차단 또는 경고가 발생하여 있는지 그리고 웹 사이트 및 URL 범주가 가장 큰 위험을 표시합니다.
- **실행 가능한 보고서** - 상세하고 정확한 정보를 생성하며, 이를 조직의 모든 단계에서 이용 가능한 대화형 보고서에 통합합니다.
- **면밀한 가시성** - 어떤 사용자가 AUP(acceptable use policies)를 위반했는지 파악하고 부서 또는 사이트 전 범위에서 정책 위반을 추적하고 리소스 소비가 많은 Facebook, YouTube, 인스턴트 메시징과 같은 애플리케이션의 사용량을 모니터링합니다.



표 1 캡션 추가?

모델	Cisco M1070	Cisco M670	Cisco M170
			
사용 시나리오			
어플라이언스별 사용자 수	10,000명 이상	최고 10,000	최대 1,000
새시			
폼 팩터	2 RU	2 RU	1RU
크기(H x W x D)	3.5 x 17.5 x 26.8인치 (8.9 x 44.5 x 68.1cm)	3.5 x 17.5 x 26.8인치 (8.9 x 44.5 x 68.1cm)	1.67 x 16.9 x 15.5인치 (4.24 x 42.9 x 39.5cm)
총 중량:	57.5lb	52.2lb	26.96lb
전원 공급 장치	870W, 100/240V	870W, 100/240V	400W, 100/240V
이중 전원	예	예	예
프로세서, 메모리, 디스크			
CPU	2x4(쿼드 코어 2개)	2x4(쿼드 코어 2개)	1x2(쿼드 코어 1개)
메모리	4GB	4GB	4GB
디스크 공간 및 카운트	3.6TB(600 * 6)	1.8TB(300 * 6)	500GB(250 * 2)
핫 스왑 가능 하드 디스크	예	예	예
RAID 레벨 및 컨트롤러	RAID 10, 하드웨어	RAID 10, 하드웨어	RAID 1, 하드웨어



Cisco M-Series에는 어떤 모델이 있습니까?

Cisco M-Series Content Security Management Appliance는 다양한 규모의 조직에서 요구 사항을 해결하고 모든 Cisco Email & Web Security Appliance를 보완하도록 설계되었습니다.



Cisco M1070

Cisco Content Security Management Appliance M1070: 이 통합형 관리 어플라이언스는 세계에서 가장 까다로운 네트워크의 요구 사항도 해결하도록 설계되었습니다. 네트워크 게이트웨이에서 유연한 관리와 철저한 보안 제어를 수행합니다.



Cisco M670

Cisco Content Security Management Appliance M670: 이 경제적인 모델은 여러 개의 게이트웨이 보안 어플라이언스가 있고 사용자 수가 최대 10,000명인 조직을 위한 제품입니다. M1070과 같은 기능과 기능을 갖추고 있습니다.



Cisco M170

Cisco Content Security Management Appliance M170: 이 경제적인 모델은 여러 개의 게이트웨이 보안 어플라이언스가 있고 사용자 수가 최대 1,000명인 조직을 위한 제품입니다. 전체 M-Series 제품군과 동일한 기능을 갖추고 있습니다.

Cisco M-Series의 장점

Cisco M-Series는 한군데서 전사적 범위의 모든 정책 설정 및 감사 정보를 모니터링하면서 모든 애플리케이션 보안 게이트웨이의 성능을 극대화하고 관리자의 워크로드 부담을 줄입니다. 선택적 기능을 적용하면 단일 어플라이언스에서 일상 보안 업무를 모두 실행하거나 여러 어플라이언스에 분산 배치할 수 있습니다. 중앙 집중식 보고 기능으로 여러 이메일 보안 어플라이언스의 트래픽 데이터를 취합하고 완벽하게 통합된 보고 기능을 제공할 수 있습니다. 관리자는 이메일 통신 및 감사 기능을 사용하여 특정 이메일 통신이 일어난 위치와 시간을 확인할 수 있습니다.

또한 네트워크 운영 팀은 중앙의 웹 보고 기능으로 시스템 용량 보고서를 작성하여 장기적 시스템 동향을 추적하고 시스템 용량을 계획할 수 있습니다. 웹 사용량은 차츰 증가하기 마련입니다. 적절한 모니터링을 통해 추가적인 용량 또는 구성 변경 사항을 미리 적용할 수 있습니다.

네트워크 관리자는 웹 보안 어플라이언스가 권장 CPU 용량을 초과한 시점, 초당 트랜잭션 수, 레이턴시, 응답 시간, 프록시 버퍼 메모리까지 추적할 수 있습니다. 이를 통해 관리자는 구성 최적화 또는 추가 어플라이언스가 필요한 시점을 결정할 수 있습니다.

왜 Cisco인가?

네트워크에 있어서 보안은 그 어느 때보다도 중요합니다. 위협과 위험이 상존하고 기밀 유지와 제어의 문제가 우려되는 상황에서 사업의 연속성을 제공하고 가치있는 정보를 보호하며 브랜드 명성을 유지하고 새로운 기술을 채택하려면 보안이 필수입니다. 안전한 네트워크에서는 직원들이 이동 중에도 적절한 정보에 안전하게 연결할 수 있습니다. 또한 고객과 파트너가 회사와 더 편리하게 사업을 수행할 수 있습니다.

Cisco만큼 네트워크 보안을 잘 아는 조직은 어디에도 없습니다. 시장을 이끄는 리더십, 위협으로부터의 최상의 보호 및 예방, 혁신적인 제품 및 긴 수명으로 인정받는 Cisco는 귀사의 보안 요구에 꼭 필요한 공급업체입니다.

추가 정보를 얻으려면 어디로 가야 합니까?

Cisco M-Series의 장점을 이해하는 가장 좋은 방법은 구매 전 시험 사용(Try Before You Buy) 프로그램에 참여하는 것입니다. 회사 네트워크에서 무료로 30일간 시험해볼 수 있도록 완전한 기능을 갖춘 평가 어플라이언스를 받으려면 <http://www.cisco.com/go/esa> 를 방문하십시오.