이메일 및 웹 보안용 Cisco Content Security Management Appliances

Cisco Content Security Management Appliances의 가치란?

조직은 제한된 직원과 예산을 바탕으로 지리적으로 분산된 팀 사이에서 다수의 보안 어플라이언스를 관리하는 업무를 수행해야 합니다. 이러한 과제를 해결하기 위해 Cisco® Content Security Management Appliance(SMA)는 여러 Cisco Email Security Appliances와 Cisco Web Security Appliances 사이에서 관리 및 보고 기능을 중앙 집중화하고 있습니다. 이러한 통합은 관리와 기획을 간소화하고, 준법 모니터링을 개선하며, 정책을 일관성 있게 이행하고, 위협 방지를 강화합니다.

보고 및 추적을 위해 최적화된 강력한 플랫폼을 바탕으로 구축된 Cisco SMA는 오래 지속되는 투자 가치를 위해 높은 성능과 확장성을 제공합니다.

중앙 집중식 관리

Cisco SMA는 단일 관리 콘솔에서 다수의 Cisco Web 및 Email Security Appliances에 이르는 구성을 게시하여 관리를 간소화합니다. 업데이트 및 설정은 개별 어플라이언스가 아닌 SMA 콘솔에서 중앙 관리합니다. 규모가 큰 구축인 경우, 대안으로 기업들은 개별 애플리케이션을 처리하도록 특정 어플라이언스를 지정할 수 있습니다.

중앙 보고

완전히 통합된 보고를 통해 여러 Cisco Email 및 Web Security Appliances에서 실시간으로 트래픽 데이터를 통합할 수 있습니다. Cisco SMA의 보고 기능에는 다음이 포함됩니다.

- **메시지 추적:** 발신자, 수신자, 메시지 제목, 기타 매개변수를 기준으로 분류된 데이터를 포함하여 여러 Cisco Email Security Appliances에서 데이터를 취합합니다. 스팸, 바이러스 판정과 같은 스캔 결과도 정책 위반 여부와 함께 표시됩니다.
- **웹 추적:** 개별 웹 트랜잭션의 기록이 IP 주소, 사용자 이름, 도메인 이름, 액세스 시간, 기타 상세 정보와 함께 보관됩니다. Facebook, YouTube 및 인스턴트 메시징과 같은 Web 2.0 애플리케이션을 직원이 사용하는 것에 대한 정보도 제공됩니다.
- **웹 보고:** 웹 추적 정보는 실시간으로 수집되며 수준 높고 사용이 간편한 그래픽 형식으로 표시됩니다. 보고 기능으로 관리자는 직원이 회사 장치에서 액세스할 수 있는 웹 사이트, URL 카테고리, 애플리케이션 등을 결정할 수 있습니다.

향상된 위협 방지

Cisco SMA는 기업의 보안 업무에 대한 종합적인 상황을 제공하여 더 나은 위협 인텔리전스, 방어 및 리미디에이션을 제공합니다. 위협 방지 기능에는 다음이 포함됩니다.

- **스팸 격리:** 스팸 및 마케팅 메시지는 사용이 간편한 셀프 서비스 Cisco Spam Quarantine 솔루션을 통해 중앙에서 보관됩니다. Cisco Email Security Appliances를 다수 보유한 대기업에서는 추적을 용이하게 하기 위해 스팸 트래픽을 하나의 장소에 오프로드하고 직원 액세스를 위한 단일 지점을 제공할 수 있습니다.
- **위협 모니터링:** 대부분의 차단 또는 경고를 접하는 사용자, 가장 위험이 큰 웹 사이트와 URL 카테고리 등을 포함한 웹 기반 위협에 대한 데이터가 실시간으로 제공됩니다. 악성코드와 기타 Cisco Web Security Appliances가 감지하고 차단한 위협도 보고됩니다.
- **평판 점수:** 이 기능은 사용자가 액세스하는 웹 사이트의 평판 점수에 대한 자세한 정보를 제공합니다. 이러한 점수는 웹 서버 행동을 분석하고 각 URL에 악성코드를 포함할 가능성을 반영하는 점수를 할당하는 Cisco Web Security Appliances가 제공한 데이터를 기준으로 합니다.
- **데이터 손실 방지:** 정책 위반, 필터 매치, 사용자 활동, 몇 개월 또는 몇 년 전에 발생한 이벤트에 대한 상세 정보를 확인할 수 있습니다. 장기적 가시성으로 관리자는 리미디에이션 및 방지를 위한 주요 활동과 동향을 식별 및 처리할 수 있습니다.
- **봇네트 감지:** 잠재적 악성코드 연결이 포함된 포트와 시스템이 표시됩니다. Cisco Web Security Appliances의 레이어 4 트래픽 모니터링 기능의 데이터는 기업이 봇넷 감염 호스트를 감지하고 리미디에이션하는데 도움이 됩니다.

준법 모니터링 및 시행

중앙 집중화된 보고 및 추적으로 사용자 정책을 위반하는 사용자를 확인할 수 있습니다. 이 기능은 또한 모든 부서나 사이트의 정책 위반을 식별하고 Facebook과 YouTube와 같은 Web 2.0 애플리케이션의 사용을 모니터링하고 "도박" 또는 "스포츠"와 같은 카테고리의 URL 방문 수를 모니터링하는 데에도 도움이 됩니다.

여러 어플라이언스의 관리를 중앙 집중화하여 관리자들은 조직 전체에서 일관성 있게 정책을 사용하도록 할 수 있습니다.

간소화된 관리 및 기획

Cisco SMA는 사용이 간편한 직관적 인터페이스를 제공합니다. 업그레이드와 새로운 기능은 Cisco에서 직접 제공하여 고객의 승인을 받고 그 후 자동으로 설치되고 관리됩니다.

또한 관리자는 보안 어플라이언스가 권장 용량을 초과했을 때 통지를 받을 수 있습니다. Cisco SMA는 초당 트랜잭션 수와 시스템의 지연, 응답 시간, 프록시 버퍼 메모리 등을 보고합니다. 이 정보로 관리자는 시스템을 재구성하거나 추가 어플라이언스를 설치해야 할 때를 결정할 수 있습니다.

우수한 성능 및 확장성

Cisco SMA는 하나의 일반적 데이터베이스가 아니라 보고 및 추적을 위해 최적화된 2개의 독점적 데이터베이스를 가지고 있습니다. 실시간 보고서의 신속한 생성을 위해 각 쿼리에 적절한 연산이 적용됩니다.

고성능 Cisco AsyncOS 운영체제를 기반으로 한 Cisco SMA는 대기업과 서비스 제공업체의 수요에 부합하기 위해 업계 최고의 확장성을 제공합니다.

Cisco Content Security Management Appliance 모델

Cisco SMA 플랫폼은 다양한 규모의 조직 요건에 부합하고 모든 Cisco Email 및 Web Security Appliances를 지원하도록 만들어졌습니다.

구축	사용자 수*	모델	설명
대기업	10,000명 이상	Cisco SMA 1070	Cisco Email 및 Web Security Appliances를 다수 보유한 대기업
		Cisco SMA M680	가장 까다로운 구축을 위한 Cisco SMA 제품군의 최고 성능 모델
중견 기업	1,000 ~ 10,000	Cisco SMA M670	Cisco Email 및 Web Security Appliances 다수 보유, 최고 10,000명의 사용자가 있는 기업
		Cisco SMA M380	중간 규모의 구축, 최신 세대의 어플라이언스 하드웨어 기반
소규모 기업 및 지사 사무소	최고 1,000	Cisco SMA M170	사용자 수가 1,000명 미만인 기업 및 지사 사무소

추가 정보

Cisco SMA 플랫폼에 대한 자세한 정보는 http://www.cisco.com/go/sma를 방문하거나 Cisco 현지 영업 담당자에게 문의하십시오.

Cisco SMA 플랫폼의 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/esa를 방문하십시오.

C45-720312-01 10/13