한눈에 보기

이점

- Cisco Web Security 소프트웨어 번들 및 개별 라이선스 구매 시 Cisco Web Security Appliance의 소프트웨어 버전이 무료로 함께 제공됩니다.
- 전 세계적인 위협 텔레메트리 네트워크인 Cisco Talos Security Intelligence and Research Group을 통해 모든 디바이스를 어디서든 항상 보호할 수 있습니다.
- 멀티레이어 검사 및 레이어 4 트래픽 모니터링, Advanced Malware Protection, URL 필터링, 동적 콘텐츠 분석, 애플리케이션 가시성 및 제어를 비롯한 다양한 기능을 이용할 수 있습니다.
- Cisco AnyConnect Security Mobility Client 및 Cisco Identity Services Engine으로 로밍 사용자에게도 보호 기능을 적용할 수 있습니다.

Cisco Web Security Virtual Appliance

효과적인 웹 보안 즉시 구현하기

Cisco® Web Security Virtual Appliance는 특히 고도로 분산된 네트워크 환경에서 웹 보안 구축 비용을 대폭 절감해 주는 올인원 웹 보안 솔루션입니다. 어떻게 가능할까요? 관리자가 필요한 위치에서 필요한 시점에 보안 인스턴스를 생성할 수 있기 때문입니다.

이 가상 어플라이언스는 Cisco Web Security Appliance의 소프트웨어 버전으로, Cisco Web Security 소프트웨어 번들 및 개별 라이선스 구매 시 무료로 함께 제공됩니다. 이 가상 어플라이언스를 사용할 경우 관리자는 트래픽 급증에 즉시 대응하고 용량 계획의 필요성을 없앨 수 있습니다. 새로운 하드웨어를 구매하고 조달할 필요가 없습니다. 데이터 센터의 복잡성이 증대되거나 새로운 물리적 요구 사항이 추가되는 일 없이 웹 트래픽의 증가를 지원할 수 있습니다.

강력한 보호

Cisco Talos Security Intelligence and Research Group(Talos)는 장소에 관계없이 모든 사용자에게 제로데이 위협 차단 서비스를 제공합니다. 세계 최대의 글로벌 위협 텔레메트리 네트워크 중 하나인 Talos는 Cisco 네트워크 보안 솔루션 제품군과 통합되어 Web Security Virtual Appliance가 지속적인 실시간 위협 차단 기능을 제공할 수 있도록 지원합니다.

Talos의 전문 연구 팀은 첨단 시스템을 활용하여 위협을 연구하고 있습니다. Talos 연구 팀은 알려진 위협과 새로운 위협 모두로부터 고객을 보호하기 위해 Cisco 제품을 위한 위협 인텔리전스를 구축합니다. Talos의 정교한 인프라와 시스템은 최고 수준의 텔레메트리 어그리게이션 및 분석을 통해 뛰어난 가시성을 제공합니다. 3~5분마다 자동 업데이트를 전송하여 글로벌 트래픽 활동을 24시간 동안 확인할 수 있으므로 Cisco에서는 이상 징후를 분석하고, 새로운 위협을 발견하고, 트래픽 트렌드를 모니터링할 수 있습니다. Talos 환경에는 다음 기능이 포함됩니다.

- 하루 100TB의 보안 인텔리전스 분석
- 방화벽, IPS, 웹, 이메일 어플라이언스를 포함하는 160만 대의 보안 디바이스 구축
- 하루 130억 개의 웹 요청
- 1억 5천만 개의 엔드포인트
- 전 세계 엔터프라이즈 이메일 트래픽의 35%

올인원 솔루션의 투자 가치

하나의 가상 머신에서 여러 보안 솔루션의 혜택 활용 가능 다른 솔루션은 복잡한 다중 디바이스 구축을 필요로 하지만 Web Security Virtual Appliance는 독립적 솔루션으로 작동하고, 단독 또는 기존 인프라와 통합하여 구축할 수 있습니다. Cisco S-Series Content Security Management Appliance를 사용하여 다중 어플라이언스를 제어할 수 있습니다. Cisco에서는 해당 어플라이언스의 모든 장점이 담긴 가상 버전도 제공하며, 관련된 Content Security Management Appliance 라이선스 구매 시 무료로 이용할 수 있습니다.

단일 소프트웨어 솔루션에서 여러 웹 보안 기능을 통합하여 웹 보안 구축을 간소화합니다. Web Security Virtual Appliance는 간소화된 아키텍처를 통해 관리, 지원, 유지 보수할 디바이스 수를 줄여 IT 비용을 절감합니다.

자세히 보기

자세한 내용은 http://www.cisco.com/go/wsa 를 참조하십시오.

Cisco 제품이 여러분 회사에 얼마나 효과적으로 적용될 수 있을지 Cisco 영업 담당자, 채널 파트너, 시스템 엔지니어와 함께 평가해 보십시오.

Web Security Virtual Appliance의 기능은 표 1에 자세히 설명되어 있습니다.

표 1. 어플라이언스 기능

기능	설명
실시간 악성코드 방어	Web Security Virtual Appliance는 악성코드 차단을 위한 다중 레이어를 사용합니다. Cisco Web Reputation Filters는 웹 트래픽을 분석하고 허용 임계값에 미달하는 URL을 차단합니다. 그런 다음 적응형 스캐닝을 통해 URL 평판, 콘텐츠 유형, 스캐너 효율성 등을 기준으로 가장 적절한 스캐너를 동적으로 선택하고 스캔 로드가 증가하는 동안 고위험 개체를 먼저 스캔하여 포착률을 개선합니다. 레이어 4 트래픽 모니터는 활동을 지속적으로 스캔하여 스파이웨어 "폰홈(phone-home)" 커뮤니케이션을 탐지 및 차단합니다.
AMP(Advanced Malware Protection)	AMP는 모든 Web Security Virtual Appliance 고객이 사용할 수 있는 라이선스가 부여된 추가 기능입니다. AMP는 고급 파일 평판 기능, 세부적인 파일 행동 보고, 지속적인 파일 분석, 회귀적 판단 경고 등의 기능을 통해 어플라이언스에서 이미 제공하는 악성코드 탐지 및 차단 기능을 보강합니다. Cisco Threat Grid 어플라이언스를 지원하는 AMP는 클라우드에 악성코드 샘플을 제출할 때 컴플라이언스 또는 정책 제한사항을 적용해야 하는 조직에 온프레미스 어플라이언스를 통한 악성코드 보호 기능을 제공합니다. Cognitive Threat Analytics에서는 환경을 적극적이고 지속적으로 모니터링하여 공격 확산을 차단함으로써 검색 시간을 단축합니다. 비정상적인 행동을 탐지하는 알고리즘과 신뢰 모델링을 통해 감염 징후를 찾아냅니다.
모든 디바이스에서 웹 트래픽 제어 가능	사용이 간편한 단일 관리 인터페이스에서 상황인식 검사를 사용하여 애플리케이션, 디바이스, 사용자 행동을 정밀하게 제어하고 정책을 집행합니다.
웹 사용 제어	전통적 URL 필터링과 실시간 동적 콘텐츠 분석을 통합하여 컴플라이언스, 의무 및 생산성 위험으로부터 조직을 보호합니다. Cisco 고유의 Cisco Dynamic Content Analysis 엔진은 알려지지 않은 URL을 실시간 분류하기 위해 해당 페이지의 콘텐츠를 분석합니다.
애플리케이션 가시성 및 제어	수백 개의 애플리케이션과 15만 개 이상의 마이크로 애플리케이션에 대한 정책을 간편하게 설정하고 사용을 제어할 수 있습니다. 정확한 정책 컨트롤로 관리자들은 Facebook이나 Dropbox와 같은 애플리케이션 사용을 허용하면서 문서 업로드나 사진 공유와 같은 활동을 하지 못하도록 차단할 수 있습니다.
Cisco AnyConnect® 및 Cisco Identity Services Engine	로밍 노트북 컴퓨터가 요청한 데이터를 보호합니다. AnyConnect®는 액세스를 허용하기 전 실시간 분석을 하기 위한 주요 웹 액세스 포인트로 민감한 정보를 전달하는 VPN을 동적으로 실행합니다. 또한 관리자는 가상 어플라이언스를 Identity Services Engine과 통합하여 엔진에서 수집한 프로파일 또는 멤버십 정보를 토대로 어플라이언스에 대한 정책을 생성할 수 있습니다.
데이터 유출 방지	기본 DLP를 위한 상황 기반 규칙을 생성하여 기밀 데이터가 네트워크에서 유출되는 것을 방지합니다. 이 가상 어플라이언스는 첨단 보호 기능을 제공하기 위해 타사 DLP 솔루션과 통합할 수 있는 ICAP(Internet Content Adaptation Protocol)를 사용합니다.

C45-727197-02 09/15