한눈에 보기

이점

- **지능형 위협 탐지:** Cisco Advanced Malware Protection, Cisco Cognitive Threat Analytics, 클라우드 액세스 보안 제품과의 통합
- **손쉬운 솔루션 구축:** 빠르고 유연한 구축 옵션과 자동 업데이트
- **세부적인 웹 액세스 제어를 통한 강화된 보안:** 업계 최고의 Cisco Identity Services Engine 사용
- **비용 절감:** 기존 보안 인프라에 손쉽게 통합
- **올인원 솔루션 구축:** 단일 상자로 지원되는 웹 보안과 프록시 기능

Cisco Web Security Appliance

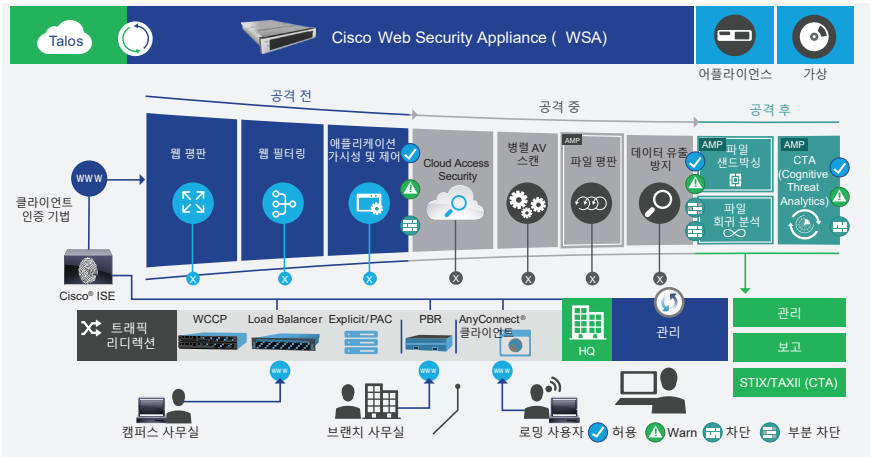
강력한 올인원 네트워크 보안

지능형 웹 보안 위협에 맞서기 위해서는 모든 엔드포인트와 그 사이의 모든 영역에 강력한 보호와 일관성 있는 제어가 이루어져야 합니다. 여기에는 모바일 디바이스, 웹 및 모바일 애플리케이션, 웹 브라우저가 포함됩니다. Cisco® Web Security Appliance가 필요한 이유입니다. 이 제품을 통해 웹 트래픽의 보안 및 제어 문제를 쉽고 빠르게 해결할 수 있습니다.

Web Security Appliance는 AMP(Advanced Malware Protection), CTA(Cognitive Threat Analytics), AVC(Application Visibility and Control, 애플리케이션 가시성 및 제어), AUP(Acceptable-use policies), 인사이트 보고, 고도의 보안 모빌리티를 통합하여 제공합니다(그림 1). 사용하기 쉬운 단일 플랫폼을 제공합니다.

물리적 어플라이언스인 Web Security Appliance는 레이턴시 감소와 더불어 낮은 운용 비용 등 유지보수에 대한 요구사항이 적습니다. 고도로 분산된 네트워크의 경우 Cisco Web Security Virtual Appliance를 통해 필요할 때 언제, 어디서든 가상 버전으로 동일한 웹 보안을 구축할 수 있습니다.

그림 1. 공격 전, 중, 후의 전 단계에서의 위협 중심 보안



로밍 사용자 보호

Web Security Appliance는 로밍 노트북에서 요청한 데이터를 보호합니다. 네트워크 액세스를 허용하기 전에 실시간 분석을 위해 민감한 트래픽을 기본 웹 액세스 포인트로 보내는 VPN을 시작합니다. 또한 관리자는 어플라이언스를 Cisco ISE(Identity Services Engine)와 통합해 엔진에서 수집한 사용자 프로필 또는 멤버십 정보를 토대로 어플라이언스에 대한 정책을 생성할 수 있습니다. 차원이 다른 사용자 제어 및 보고 기능을 제공합니다. 또한 통합 SSO(Single Sign-On)와 같은 간소화 기능을 통해 BYOD(bring-your-own-device) 환경에서 훨씬 뛰어난 사용자 환경을 제공합니다.

© 2016 Cisco and/or its affiliates. All rights reserved.

애플리케이션 가시성 및 제어

Web Security Appliance를 통해 사용이 간편한 단일 관리 인터페이스에서 상황인식 검사를 사용하여 애플리케이션과 사용자 행동을 정밀하게 제어하고 정책을 시행합니다. 수백 개의 애플리케이션과 15만 개 이상의 마이크로 애플리케이션에 대해 정책을 간편하게 설정하고 사용 방식을 제어할 수 있습니다. 따라서 Facebook이나 Dropbox와 같은 애플리케이션 사용을 허용하면서 채팅이나 문서 업로드와 같은 활동을 하지 못하도록 차단할 수 있습니다. 또한 사용자, 그룹, 정책별로 맞춤형 대역폭 및 시간 할당량을 지정할 수도 있습니다. 클라우드 액세스 보안과 통합하여 클라우드 애플리케이션에 대한 사용자 액세스를 제어함으로써 명시적인 조직의 승인을 받지 않고 조직 내에서 구축 및 사용되는 IT 시스템 및 솔루션인 "섀도우 IT" 문제를 해결합니다.

웹 사용 제어

Web Security Appliance를 통해 기존의 URL 필터링과 동적으로 업데이트된 기존 URL 데이터베이스를 통합하여 컴플라이언스, 책임 및 생산성 위험을 줄일 수 있습니다. Cisco Dynamic Content Analysis 엔진이 알려지지 않은 URL의 페이지 콘텐츠를 실시간으로 평가하고 분류합니다. 이러한 분류는 Cisco Talos Security Intelligence and Research Group에서 3~5분마다 동적으로 업데이트됩니다. Talos는 정교한 시스템을 활용하여 전 세계의 위협, 악성코드, 침입을 분석하는 업계 최고의 위협 연구가들로 구성되어 있습니다.

데이터 유출 방지

기밀 데이터가 네트워크를 벗어나지 못하도록 기본 DLP(Data Loss Prevention, 데이터 유출 방지)에 대한 상황 기반 규칙을 생성합니다. WSA는 첨단 보호 기능을 제공하기 위해 타사 DLP 솔루션과의 통합할 수 있는 ICAP(Internet Content Adaptation Protocol)를 사용합니다.

물리/가상 어플라이언스의 기능과 이점은 표 1에서 확인할 수 있습니다.

표 1. 기능 및 이점

기능	이점
Talos	130억 건의 일일 웹 요청으로 처리되는 100테라바이트의 보안 데이터, 1억 5천만 개의 엔드포인트, 구축된 160만 개의 보안 디바이스 등 업계 최대의 실시간 위협 인텔리전스를 통해 조기 경보 기능과 더불어 취약점 분석 기능을 제공합니다. Talos는 3분에서 5분 간격으로 자동 업데이트를 보내 지속적으로 실시간 위협을 차단할 수 있습니다.
웹 평판 필터	웹 평판 필터는 Talos의 위협 정보와 결합하여 동적 평판 분석을 통해 제로데이 웹 악성코드를 차단합니다. 이 기능은 URL 평판, 콘텐츠 유형, 스캐너의 실효성을 기준으로 가장 적합한 스캐너를 실시간으로 선택하고, 검사량이 많을 경우 고위험 개체를 일차적으로 스캔하여 탐지율을 높입니다.
AMP(Advanced Malware Protection)	AMP는 모든 Web Security Appliance 고객이 사용할 수 있는 라이선스가 부여된 추가 기능입니다. AMP는 어플라이언스에서 이미 지원하는 악성코드 탐지 및 차단 기능을 보강합니다. 고급 파일 평판 기능, 세부적인 파일 행동 보고, 지속적인 파일 분석, 회귀적 판단 경고를 제공합니다. AMP Threat Grid 어플라이언스를 지원하는 AMP는 클라우드에 악성코드 샘플을 제출할 때 컴플라이언스 또는 정책 제한사항을 적용해야 하는 조직에 온프레미스 어플라이언스를 통한 악성코드 보호 기능을 제공합니다.
CTA(Cognitive Threat Analytics)	클라우드 기반 침입 탐지 및 분석을 통해 웹 프록시를 보안 센서로 활용합니다. Cisco CTA(Cognitive Threat Analytics)는 네트워크 내에서 작동하는 위협의 검색 시간을 단축하는 클라우드 기반 솔루션입니다. 행동 분석 및 이상 징후 탐지를 통해 악성코드 감염이나 데이터 보안 침해의 증상을 파악하여 경계 기반 방어의 허점을 보완합니다. Cisco Web Security Appliance의 AMP 애드온 라이선스에 포함된 CTA(Cognitive Threat Analytics)를 이용할 수 있습니다. 복잡성을 낮추면서도 계속 변화하는 위협 환경과 함께 진화하는 탁월한 보호 기능을 제공합니다. Cisco CTA(Cognitive Threat Analytics)에 대한 자세한 내용은 www.cisco.com/go/cognitive 를 참조하십시오.
CnC(Command and Control) 트래픽 모니터링	레이어 4 트래픽 모니터는 지속적으로 활동을 스캔하여 스파이웨어 "폰홈(phone-home)" 통신을 탐지해 차단합니다. 모든 네트워크 애플리케이션을 추적하여 전형적인 웹 보안 솔루션을 우회하려는 악성코드를 효과적으로 차단합니다. 또한 알려진 악성코드 도메인의 IP 주소로 악성 개체 목록을 자동으로 업데이트합니다.
간소화된 구축	Web Security Appliance(물리/가상)는 여러 웹 보안 기능을 단일 어플라이언스에 결합하여 구축을 간소화한 올인원 솔루션입니다. 간소화된 아키텍처를 통해 관리, 지원 및 유지보수를 담당할 몇 개의 디바이스만 마련하면 되므로 IT 비용을 절감합니다.

다음 단계

Cisco Web Security Appliance에 대한 자세한 내용은 http://www.cisco.com/go/wsa 를 참조하십시오.

Cisco 영업 담당자, 채널 파트너 또는 시스템 엔지니어와 함께 여러분 회사에 얼마나 효과적으로 Cisco 제품을 적용할 수 있는지 평가해 보십시오.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-730937-03 10/16