Cisco Web Security: 보호, 제어, 가치

이점

- **강력한 보호:** Cisco Talos Security Intelligence and Research Group(Talos)을 포함하는 정교한 글로벌 위협 인텔리전스 인프라를 통해 모든 디바이스를 보호합니다.
- **완벽한 제어:** 소셜 미디어 애플리케이션과 같은 동적 웹 콘텐츠를 비롯한 모든 웹 트래픽을 지능적으로 제어할 수 있도록 지원합니다.
- **투자 가치:** 유연한 구축 옵션, 기존 보안 및 네트워크 인프라와의 원활한 통합, 세계 최고 수준의 24시간 지원을 제공하여 보안 투자의 가치를 높이고 웹 보안의 TCO(Total Cost of Ownership)를 절감합니다.

월드 와이드 웹은 경이로운 공간입니다. 하지만 안전하지 않은 곳이기도 합니다. 그렇다면 소셜 미디어와 웹 애플리케이션을 사용하면서 디바이스와 리소스를 보호할 수 있는 방법은 무엇일까요?

하나의 솔루션으로는 역부족입니다. 빠르게 진화하는 오늘날의 사이버 위협을 차단할 수 있는 다양한 보호 기능이 필요합니다. 하지만 그로 인해 복잡성이 심화되고 IT 환경의 운영 워크로드가 늘어나는 것은 어떻게 해야 할까요? Cisco® WSA(Web Security Appliance)를 사용하면 이러한 문제가 없습니다(그림 1 참조). Cisco WSA는 고도로 보안된 일체형(all-in-one) 웹 게이트웨이로서 강력한 보호, 완벽한 제어, 투자 가치라는 이점을 제공합니다. 또한 경쟁력 있는 웹 보안 구축 옵션을 다양하게 제공하며, 각 옵션에는 Cisco의 업계 최고 글로벌 위협 정보 인프라가 포함되어 있습니다.

그림 1. Cisco Web Security Appliance

강력한 보호

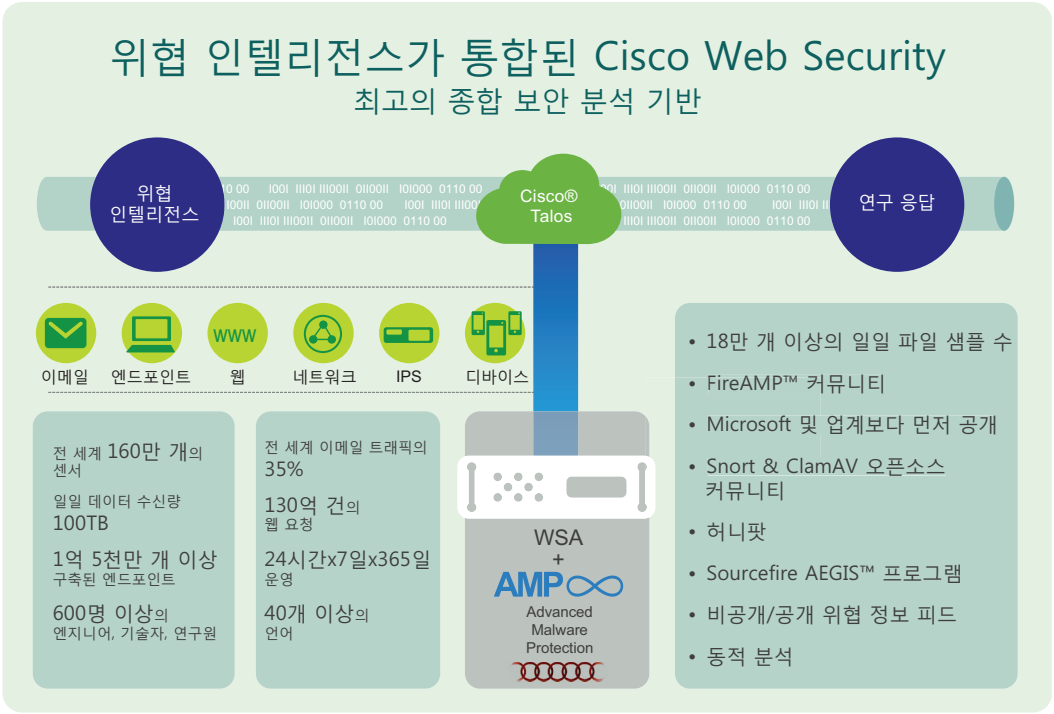
지능형 위협 방어

Cisco Web Security는 가장 광범위한 가시성 및 가장 큰 보호 범위를 갖춘 업계 최대의 실시간 위협 인텔리전스 모음인 Cisco Talos Security Intelligence and Research Group(Talos)을 기반으로 합니다. Talos는 여러 공격 벡터에서 막대한 양의 글로벌 정보를 수집하여 위협이 숨어 있는 위치를 발견합니다(그림 2 참조). 이러한 정보 수집에는 다음이 포함됩니다.

- 하루 100TB의 보안 인텔리전스
- 방화벽, 침입 방지 시스템(IPS), 웹, 이메일 어플라이언스 등을 포함한 160만 대의 보안 디바이스
- 1억 5천만 개의 엔드포인트
- 매일 130억 건의 웹 요청
- 수백 개의 애플리케이션 및 15만 개의 마이크로애플리케이션
- 전 세계 기업 이메일 트래픽의 35%

Talos는 조기 경보 인텔리전스, 위협 및 취약성 분석 기능을 제공하여 제로 데이 지능형 위협으로부터 조직을 보호할 수 있도록 지원합니다. Talos는 3분에서 5분 간격으로 업데이트되는 새로운 규칙을 지속적으로 생성하여 Cisco Web Security가 경쟁사 제품보다 몇 시간 내지 며칠 더 앞서 업계 최고의 위협 방어 기능을 제공할 수 있도록 합니다.

그림 2. Cisco Talos Security Intelligence and Research Group



최고의 웹사이트 평판 분석
Cisco WSA는 Cisco 네트워크에서 수집된 위협의 상관관계를 파악하여 조치를 취해야 할 행동 점수를 생성합니다. 상위 사이트 및 하위 사이트에서 웹 평판 점수를 적용하고 시행합니다.

적응형 보호 기능을 위한 통합 멀티레이어 악성코드 방어
예전에는 효과적인 웹 보안을 악성 URL 탐색 차단으로 생각했습니다. 하지만 지금은 합법적인 웹사이트를 통해 바이러스에 감염되거나 악성코드를 다운로드할 가능성이 높습니다. Cisco WSA는 Talos에서 3분에서 5분 간격으로 업데이트하는 여러 레이어의 악성코드 차단 기술과 인텔리전스를 사용하여 악성코드 및 지능형 지속 위협을 차단합니다. HTML에서 이미지, Adobe Flash 파일에 이르기까지 액세스되는 모든 웹 콘텐츠는 보안 및 상황 인식 검사 엔진을 사용하여 분석됩니다.

Cisco WSA는 높은 처리 속도를 유지하면서 트래픽을 실시간으로 분석하고, 기능적 요소로 분할하며, 검사를 위해 최상으로 설계된 악성코드 엔진에 요소를 푸시합니다(그림 3 참조).

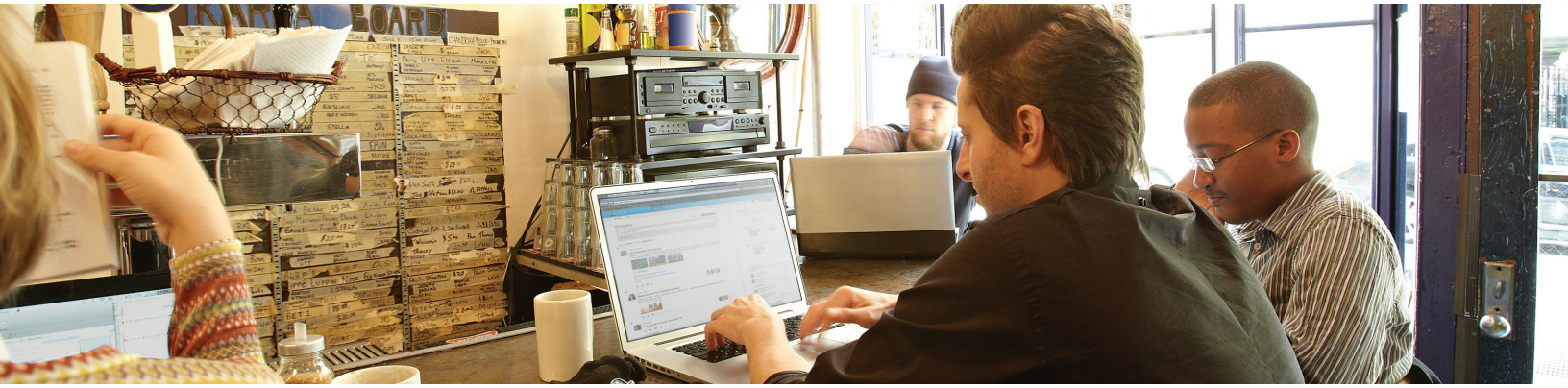
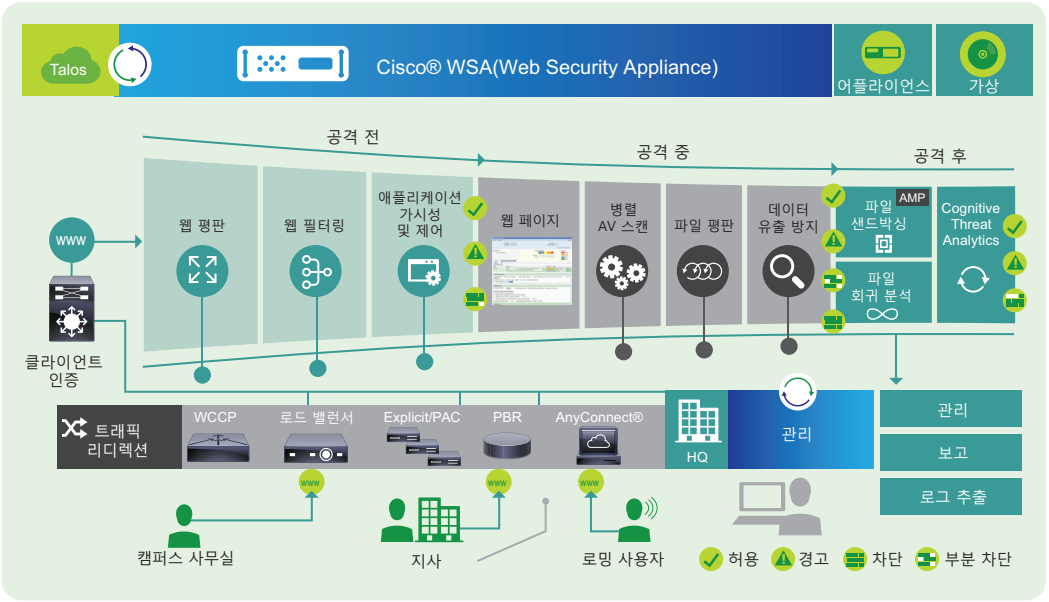


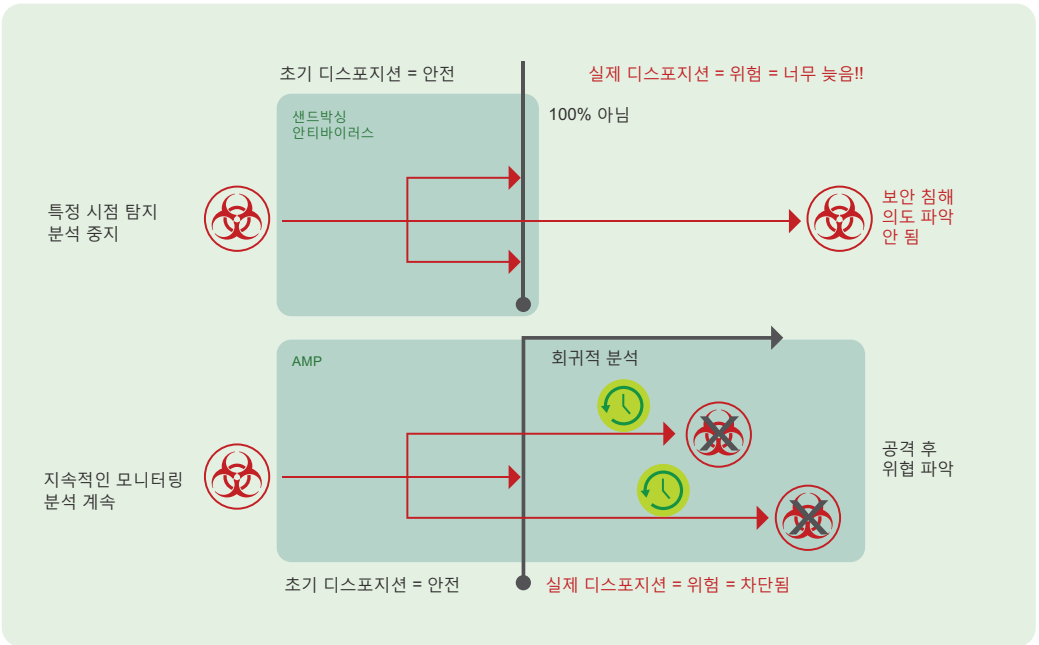
그림 3. Cisco WSA의 방어 레이어

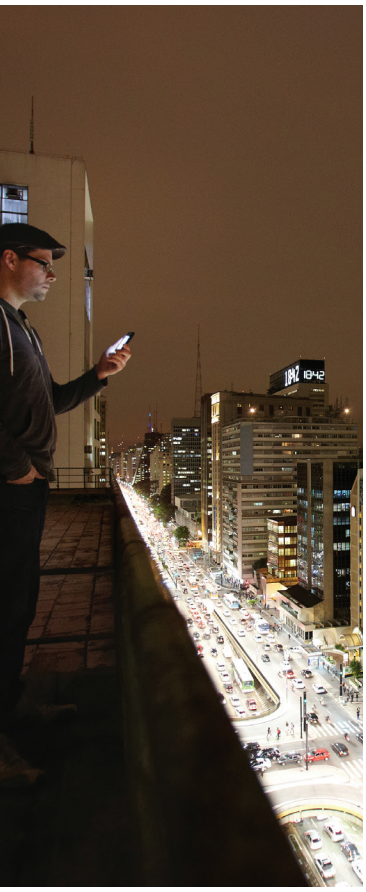


샌드박싱 및 지속적인 분석

AMP(Advanced Malware Protection)는 모든 Cisco WSA 고객이 사용할 수 있는 라이센스가 부여된 추가 기능입니다. AMP는 악성코드 탐지 및 차단, 지속적인 분석, 회귀적 알림 등의 기능을 제공하는 포괄적인 악성코드 차단 솔루션입니다(그림 4 참조). AMP는 향상된 파일 평판 기능, 세부적인 파일 동작 보고, 지속적인 파일 분석, 회귀적 판단 알림 등의 기능을 통해 Cisco WSA에서 이미 제공하고 있는 악성코드 탐지 및 차단 기능을 더욱 강화합니다. 이제 고객은 Windows PE(portable executable) 파일뿐만 아니라 PDF, Microsoft Office 및 아카이브/압축 파일을 샌드박싱할 수 있습니다.

그림 4. AMP를 사용한 회귀적 분석





완벽한 제어

중앙 집중식 관리

Cisco WSA의 직관적인 관리 인터페이스는 정책 관리 및 보고를 중앙 집중화하여 사용이 간편한 단일 인터페이스에서 글로벌 제어 기능을 제공합니다.

심층적인 웹 사용 및 애플리케이션 가시성

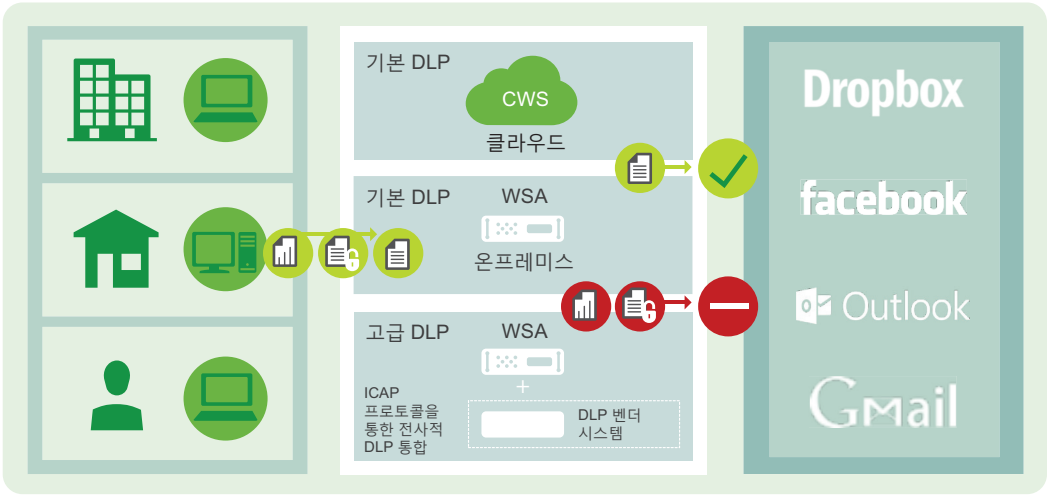
Cisco WSA에서는 진화하는 애플리케이션 및 마이크로애플리케이션 콘텐츠에 대한 심층적인 가시성이 제공됩니다. 특히, Cisco WSA는 Facebook과 같이 가장 관련성이 크고 널리 사용되는 웹 및 모바일 애플리케이션과 Facebook 게임과 같은 15만 개 이상의 마이크로애플리케이션을 식별하고 분류합니다. 이는 ID, 시간, 콘텐츠, 위치, 아웃바운드 컴플라이언스 데이터를 결합하여 애플리케이션 정책을 구축하고 유지 관리함으로써 수행됩니다.

이러한 가시성과 함께 Cisco WSA는 애플리케이션 및 사용 행동에 대한 정밀한 제어 기능을 제공합니다. 사용자의 위치 또는 프로필과 디바이스 유형에 따라 대역폭 소비를 통제하고 조절(throttling)과 같은 조건적 제어를 적용할 수 있습니다. 또한 Cisco WSA는 사용자 프로필, 디바이스, 액세스 메커니즘에 따라 애플리케이션에 대한 사용자 액세스를 동적으로 상황에 기반하여 제어합니다. Salesforce.com, WebEx와 같은 SaaS 애플리케이션을 제어하기 위한 정책을 설정할 수도 있습니다.

데이터 유출 방지

Cisco WSA는 민감한 정보가 안전한 네트워크 외부로 유출되는 것을 차단하여 규정준수를 보장하고 위험을 줄일 수 있도록 지원합니다(그림 5 참조). 이 기능은 파일 공유 애플리케이션과 같은 아웃바운드 콘텐츠에 대한 제어 기능 외에 추가로 제공됩니다. iCloud, Dropbox 등의 클라우드 기반 파일 공유 서비스에 업로드하는 것을 방지할 수 있습니다. 기본적인 DLP(Data Loss Prevention)를 위한 상황 기반 규칙을 생성하거나, ICAP(Internet Content Adaptation Protocol)를 통해 서드파티 DLP 솔루션과 통합하여 콘텐츠 심층 검사 및 DLP 정책 적용을 수행함으로써 기밀 데이터가 네트워크 외부로 유출되는 것을 막을 수도 있습니다.

그림 5. Cisco WSA를 사용한 데이터 유출 방지



투자 가치

총 소유 비용 절감

새로운 특징 및 기능을 위해 추가 디바이스가 필요한 경우가 많은 다른 솔루션과는 달리, Cisco WSA는 단일 어플라이언스에서 통합 솔루션을 제공합니다. 99.999% 가용성 및 가동 시간으로 문제 해결에 소요되는 시간이 줄어듭니다. Talos의 자동 업데이트를 통해 시간을 절약하고 직접 개입하지 않고도 최신 위협 차단 기능을 구현할 수 있습니다. 마지막으로, Cisco WSAV(Web Security Virtual Appliance)를 숫자에 제한 없이 구축하여 기존 VMware 인프라를 사용할 수 있습니다.

사용 가능한 모델 및 옵션

표 1부터 표 4까지에는 Cisco WSA, Cisco WSAV(Web Security Virtual Appliance), Cisco M-Series Content Security Management Appliance에 대한 사양이 나와 있습니다.

표 1. Cisco WSA 성능 사양

	사용자 수*	모델	디스크 공간	RAID 미러링	메모리	CPU
대규모 기업	6,000~12,000명	S680	4.8TB(8 x 600GB SAS)	예(RAID 10)	32GB	16(옥타 코어 2개) 2.70GHz
중견기업	1,500~6,000명	S380	2.4TB(4 x 600GB SAS)	예(RAID 10)	16GB	6(헥사 코어 1개)
중소기업(SMB) 및 지사	1,500명 미만	S170	500GB(2 x 250GB SATA)	예(RAID 1)	4GB	2(듀얼 코어 1개) 2.80GHz

* 현재 및 예상 요구사항을 충족하는 솔루션을 구축할 수 있도록 Cisco 콘텐츠 보안 전문가에게 크기 조정에 대한 조언을 받으시기 바랍니다.

표 2. Cisco WSA 하드웨어 사양

	S680	S380	S170
하드웨어 플랫폼			
폼 팩터	2RU(2개 랙 유닛)	2RU	1RU
규격	3.5 x 19 x 29인치 (8.9 x 48.3 x 73.7cm)	3.5 x 19 x 29인치 (8.9 x 48.3 x 73.7cm)	1.64 x 19 x 15.25인치 (4.2 x 48.3 x 38.7cm)
예비 전원 공급 장치	예	예	아니요
원격 전원 주기	예	예	아니요
DC 전원 옵션	예	예	아니요
운영 중 교체 가능한 하드 드라이브	예	예	예
파이버 옵션	예(액세서리)	아니요	아니요
이더넷	4기가비트 NIC, RJ-45	4기가비트 NIC, RJ-45	2기가비트 NIC, RJ-45
속도(Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate

표 3. Cisco WSAV 사양

웹 사용자	모델	디스크	메모리	코어
1,000명 미만	S000v	250GB	4GB	1
1,000 ~ 2,999명	S100v	250GB	6GB	2
3,000 ~ 6,000명	S300v	1024GB	8GB	4
서버				
Cisco UCS 		**ESXi 5.0, 5.1 및 5.5 하이퍼바이저** vmware KVM		

표 4. Cisco M-Series Content Security Management Appliance

모델	Cisco M680	Cisco M380	Cisco M170
사용자 수(근사치)	10,000명 이상	최대 10,000명	최대 1,000명

다음 단계

자세한 정보는 http://www.cisco.com/go/wsa를 참조하십시오. Cisco WSA가 귀사에 얼마나 효과적으로 적용될 수 있을지 Cisco 영업 담당자, 채널 파트너 또는 시스템 엔지니어와 함께 평가해 보십시오.

미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트 **www.cisco.com/go/offices**에서 확인하십시오.

C02-733921-00 2/15