Cisco Cloud Web Security

Cisco® Cloud Web Security는 기존 솔루션과는 다른 더욱 포괄적인 클라우드 기반 웹 방어 솔루션입니다. 웹 사용 정책의 실행을 통해 업계 최고의 실시간 보호 기능을 제공합니다.

제품 개요

해킹은 널리 알려진 산업이 되었으며 교묘하게 충분한 자금으로 운영되는 범죄 기업이 이용하고 있습니다. 공격 역시 지속적으로 진화하여 갈수록 더 큰 피해를 유발할 뿐만 아니라 탐지하기가 더욱 어려워지고 있습니다. 전통적인 웹 보안 솔루션은 알려진 위협을 차단할 수는 있지만 변화하는 위협 환경에 적응하지 못하고 있습니다. 또한 지능형 악성코드를 처리할 수 없습니다.

경계 방어로 사용자가 정보 및 리소스에 액세스하는 방법을 처리할 수 없습니다. 이제 조직 외부의 사용자만이 우려의 대상이 아닙니다. 조직 내부의 사용자가 과도한 대역폭을 소비하거나 조직을 위험에 빠뜨릴 수 있는 부적절한 콘텐츠에 액세스할 수도 있습니다. 조직 내부 사용자의 개인 디바이스를 통해 방화벽 내부에서 악성코드가 퍼질 수도 있습니다.

업계 최고의 글로벌 위협 가시성 네트워크를 기반으로 구축된 Cloud Web Security는 지능형 위협과 표적 위협을 매우 효과적으로 차단합니다. 또한 네트워크와 파일 동작을 모두 지속적으로 모니터링하고, Cisco AMP(Advanced Malware Protection) 및 Cognitive Threat Analytics를 사용하여 네트워크 환경에서 작동하는 위협을 식별합니다.

Cloud Web Security는 웹 사용을 제어하고 시그니처, 평판 및 콘텐츠 분석을 기반으로 사이트를 차단합니다. 또한 위협을 차단하기 위해 각 웹 페이지 구성 요소를 실시간으로 분석하는 휴리스틱스(heuristics) 기반 엔진인 보안 침해 인텔리전스를 통해 동급 최고의 악성코드 검사 기능을 제공합니다.

Cisco AMP는 파일 회귀 분석을 사용하여 시간 경과에 따른 파일의 속성을 추적함으로써 지능형 악성코드 위협을 차단합니다. Cognitive Threat Analytics는 보안 침해 증상을 지속적으로 검사하여 경계 방어를 우회하는 위협을 발견하는 데 걸리는 시간을 단축합니다.

클라우드 서비스인 Cloud Web Security는 뛰어난 유연성을 제공합니다. 기존 인프라를 사용하면서 여러 연결 옵션을 통해 서비스를 간편하게 구축하고 확장할 수 있습니다. 단일 관리 인터페이스를 통해 사용자의 위치 또는 디바이스와 관계없이 조직 전체에 세부적인 웹 사용 정책을 실행할 수 있습니다. Cisco AnyConnect® Secure Mobility Client를 통해 Cloud Web Security는 로밍 중인 노트북 컴퓨터 사용자에게 강력한 보호 기능을 제공할 수 있으며 동일한 온프레미스 정책을 실행합니다.

Cisco의 고급 글로벌 위협 가시성 네트워크는 최신 위협에 대항하여 Cloud Web Security를 지속적으로 업데이트하고, 실행 가능성이 가장 높은 클라우드 기반 인텔리전스 보고를 제공하여 웹 사용에 대한 뛰어난 가시성을 보장합니다. 전 세계 23곳에 위치한 최고 수준의 데이터 센터 시설에서 99.999% 업타임의 SLA(Service-Level Agreement)를 제공하므로 상시 정보를 사용할 수 있습니다. 또한 Cloud Web Security에는 수상 경력에 빛나는 Cisco의 24시간 지원이 제공됩니다.

라이센스에 따른 기능 및 장점

몇 가지 라이센스를 사용할 수 있습니다. Cloud Web Security Essentials는 신규 고객과 갱신 고객을 위한 기본 제품입니다. 다른 번들 및 개별 옵션도 제공됩니다. 각 라이센스의 주요 기능은 표 1~5에 나와 있습니다.

표 1. Essentials 라이센스

기능	설명
웹 필터링	75개 이상의 웹 범주 목록으로부터 필터를 적용하여 5천만 개 이상의 알려진 웹 사이트에 대한 웹 액세스를 제어합니다.
악성코드 스캔	웹 트래픽을 기능적 요소로 나누며 효율적으로 실시간 분석하는 인텔리전트 멀티스캔 기술을 사용하여 차단율을 높입니다.
보안 침해 인텔리전스(Outbreak Intelligence)	휴리스틱스(heuristics) 기반 악성코드 차단 엔진을 통해 알 수 없는 비정상적인 동작과 제로 아워(zero-hour) 발생을 식별합니다. 보안 침해 인텔리전스는 사용자 액세스를 허용하기 전에 가상 에뮬레이션 환경에서 웹 페이지 구성 요소를 실행합니다. Java, PDF, 실행 파일 등에 대해 전용 "scanlet" 엔진을 사용하여 보안 침해 인텔리전스는 웹 페이지의 개별 구성 요소를 열어 각 구성 요소가 동작하는 방식을 파악하고 악성코드를 차단합니다.
웹 평판	사이트 평판에 기반하여 웹 사이트 액세스를 제한합니다. 도메인 소유자, 호스팅 서버, 생성된 시간, 요청된 사이트 유형, 50개 이상의 기타 개별 매개변수 등의 데이터를 분석하여 요청된 사이트에 대한 평판 점수를 제공합니다.[1]
애플리케이션 가시성 및 제어	웹 페이지, 개별 웹 파트 또는 마이크로애플리케이션에 대한 액세스를 제어하여 직원들이 불필요하게 주의가 분산되지 않고 업무에 필요한 사이트에 액세스할 수 있도록 함으로써 직원 생산성을 높입니다. 동시에 부적절한 콘텐츠에 대한 액세스를 방지합니다.
동적 콘텐츠 분석	전통적인 URL 필터링을 실시간 DCA(Dynamic Content Analysis)와 결합하여 규정준수, 책임 및 생산성 위험으로부터 보호합니다. DCA 엔진은 페이지 자체의 콘텐츠를 분석하고, 웹 범주(예: 외설, 불쾌한 표현, 도박, 불법 다운로드)에 대한 관련성 점수를 매기며, 웹 보안 정책과 충돌하는 경우 해당 페이지를 차단하여 알 수 없는 URL의 콘텐츠를 자동으로 분류합니다.
중앙 집중식 관리 및 보고	모든 위협, 데이터, 애플리케이션을 대상으로 실행 가능한 정보를 제공받습니다. 강력한 중앙 집중식 툴이 보안 운영(예: 관리)과 네트워크 운영(예: 대역폭 소비 분석)을 모두 제어합니다. 관리자는 미리 정의된 다양한 보고서에 액세스하고 맞춤형 대시보드를 생성하고 알림을 설정할 수 있습니다. 모든 보고서는 클라우드에서 생성되고 저장되므로 몇 시간이 아니라 몇 초 만에 제공할 수 있습니다. 또한 자동으로 제공되도록 보고서를 저장하고 예약할 수 있습니다. 이러한 기능을 통해 사용자 수준까지 세부 정보를 제공하여 유연성을 구현하고, 관리자가 잠재적인 문제를 신속하게 파악할 수 있도록 합니다.
로밍 중인 노트북 컴퓨터 사용자 보호	Cisco AnyConnect를 통해 동일한 사내(in-house) 정책으로 로밍 사용자를 보호합니다. AnyConnect는 모든 로밍 웹 트래픽을 SSL 터널을 통해 가장 가까운 Cisco 클라우드 프록시에 직접 라우팅하고 온프레미스에서와 동일한 보안 기능을 실행합니다. VPN을 통해 웹 트래픽을 백홀하지 않아도 되므로 Cloud Web Security는 본사의 웹 정체 현상을 해소하여 대역폭 사용을 줄이고 최종 사용자 경험을 개선합니다.

[1] Cisco Web Reputation 기술 페이지의 "URL 기반 위협으로부터 보호"를 참조하십시오.

표 2에 나와 있는 Cloud Web Security Premium 라이센스에는 Cloud Web Security Essentials 번들의 모든 기능이 포함될 뿐만 아니라 AMP와 Cognitive Threat Analytics가 추가됩니다.

표 2. Premium 라이센스

기능	설명
Cisco AMP (별도 구매 가능)	AMP의 탐지 및 차단, 지속적인 분석, 소급 경보(retrospective alerting)를 통해 최신 지능형 악성코드를 차단합니다. AMP는 Cisco와 (현재 Cisco가 인수한) Sourcefire의 광범위한 클라우드 보안 인텔리전스 네트워크를 모두 사용합니다. AMP는 향상된 파일 평판 기능, 세부적인 파일 샌드박싱 및 파일 회귀 분석을 통해 Cloud Web Security에서 이미 제공되는 악성코드 탐지 및 차단 기능을 보강합니다. 이러한 모든 기능을 갖춘 유일한 솔루션인 Cisco AMP는 네트워크 경계 내부에서 시간 경과에 따라 파일의 처리를 추적합니다. 파일이 나중에 악성으로 확인되는 경우 파일 회귀 분석을 통해 해당 파일이 들어온 위치와 이동한 위치를 식별하여 교정 프로세스를 지원합니다. 자세히 보기
Cognitive Threat Analytics (별도 구매 가능)	네트워크 내부에서 작동하는 위협의 발견 시간을 단축합니다. Cognitive Threat Analytics는 동작 분석 및 이상 징후 탐지를 통해 악성코드 감염이나 데이터 보안 침해의 증상을 파악하여 경계 기반 방어의 허점을 보완합니다. 전통적인 모니터링 시스템과 달리 CTA는 고급 통계 모델링 및 기계 학습을 사용하여 독립적으로 새로운 위협을 식별하고 파악한 내용을 학습하며 시간을 두고 적응합니다. 자세히 보기

표 3. Advanced Threat Detection 및 개별 선택 라이센스

기능	설명
Log Extraction API	S3 호환 HTTPS API를 사용하여 웹 사용 데이터를 신속하게 자동으로 풀링하여 매우 안전한 분석을 수행합니다. 로그 데이터는 SIEM(Security Information and Event Management)과 같은 다양한 보고 및 분석 툴을 사용하여 기존 데이터와 상관 관계가 있을 수 있는 W3C 텍스트 형식으로 컴파일됩니다. 일반적으로 20개 이상의 특성으로 구성된 로그 정보를 이벤트 발생 후 15분 이내에 사용할 수 있습니다. Log Extraction은 기존의 모든 Cloud Web Security 라이센스에 추가할 수 있습니다. 사용자 수가 4,000명 이상인 고객에게 이상적입니다.
AMP	표 2 참조
Cognitive Threat Analytics	표 2 참조
데이터 보존	차단된 웹 요청 데이터(정책 또는 악성코드 차단)는 1년 동안 보존되고, 허용되는 데이터는 45일 동안 보존됩니다. 고객은 서브스크립션 조건에 맞게 더 긴 기간 동안 데이터를 보관할 수 있습니다.

Advanced Threat Detection은 Cisco AMP 및 Cognitive Threat Analytics를 포함하는 애드온 라이센스(위 표의 설명 참조)로, 현재 Cloud Web Security Essentials 라이센스가 있는 고객이 사용할 수 있습니다.

표 4. 웹 보안 번들

기능	설명
웹 보안 번들	웹 보안 번들은 Cisco Web Security Appliance와 Cloud Web Security로 구성되어 있습니다. 고객은 클라우드 또는 온프레미스 전반에서 Cisco Web Security를 사용할 수 있습니다. 번들에는 다음이 포함됩니다. • **Web Security Appliance Premium:** URL 필터링 방어를 심층적 콘텐츠 검사(웹 사용 제어, 웹 평판, Sophos Anti-malware, Webroot Anti-malware, 소프트웨어 서브스크립션 지원)와 결합하며, Web Security Virtual Appliance에 대한 라이센스를 포함합니다. 자세한 내용은 Web Security Appliance 데이터 시트를 참조하십시오. • **Cloud Web Security Essentials:** 표 1 참조 • **웹 보고 애플리케이션(선택 사항):** Cisco Web Security 보고 애플리케이션은 구축에 상관없이 웹 보안을 모니터링할 수 있는 단일 창구를 제공합니다. 여기에는 투명하게 설치되는 맞춤형 애플리케이션이 포함됩니다. 또한 미리 정의된 보고서에 대해 여러 Web Security Appliance 및 Cloud Web Security에서 수집된 로그 데이터를 폴링합니다. 고객은 플래시 타임라인 보기 및 웹 추적 양식을 사용하여 검색할 수도 있습니다. • **Log Extraction(선택 사항):** 표 3 참조 • **AMP:** 표 2 참조

이러한 혜택은 모든 Cloud Web Security 라이센스에 포함됩니다.

Talos Security and Research Group: 글로벌 트래픽 활동에 대한 24시간 가시성을 통해 Talos는 이상 징후를 분석하고, 새로운 위협을 발견하며, 트래픽 트렌드를 모니터링합니다. Talos는 3분에서 5분 간격으로 새로운 규칙을 생성하고 업데이트하여 경쟁업체보다 몇 시간 또는 며칠 앞서 위협 방어 조치를 취합니다. 다음에 기반한 가장 광범위한 가시성과 가장 큰 설치 범위를 통해 세계 최대 위협 탐지 네트워크 중 하나에서 지원하는 신속하고 포괄적인 웹 보호 정보를 제공받습니다.

- 매월 Cloud Web Security에서 서비스하는 1,300억 건의 웹 요청
- 매월 Cloud Web Security를 통해 펌핑되는 3.6페타바이트의 대역폭
- 매일 수집되는 100TB의 인텔리전스
- 매월 49억 건의 안티 바이러스 및 웹 필터링 차단
- 160만 개의 센서
- 모든 주요 운영 체제 및 플랫폼에서 지원

세계 최고 수준의 지원: JD Power 수상 경력에 빛나는 10개 이상의 보안 지원 센터를 통해 24시간 액세스 가능한 Cisco 전문가에게 직접 문의하여 신속하게 문제를 해결합니다. Cloud Web Security 소프트웨어 서브스크립션에 대한 지원에는 다음이 포함됩니다.

- 최신 기능 집합으로 애플리케이션의 최적 성능을 유지하기 위한 소프트웨어 업데이트 및 주요 업그레이드
- 신속한 전문 지원을 위해 Cisco TAC(Technical Assistance Center)에 액세스
- 사내 전문 지식을 구축 및 확대하고 비즈니스 민첩성을 증대할 수 있는 온라인 툴

업계 최고의 업타임: 99.999% 업타임의 SLA를 제공하는 최고 수준의 데이터 센터 시설을 통해 데이터 보호를 보장합니다. Talos에서 제공하는 자동 업데이트를 통해 Cloud Web Security는 항상 최신 위협 정보를 활용할 수 있습니다. 항상 보안 상태가 유지되므로 직원들이 다른 우선 순위 업무에 집중할 수 있습니다.

구축

Cloud Web Security 트래픽 리디렉션 연결 방법

Cloud Web Security에서는 Cisco 어플라이언스에 구애받지 않는 유연한 구축 옵션을 제공합니다. 트래픽을 Cloud Web Security 웹 프록시로 다양한 방법으로 리디렉션할 수 있습니다. Cisco Adaptive Security Appliances(물리 및 가상), Cisco ISR(Integrated Services Routers) G2, Cisco 4000 Series Integrated Services Routers(IPsec을 통한 일반 라우팅 캡슐화) 및 Web Security Appliances(물리 및 가상)를 통해 리디렉션을 수행할 수 있습니다. 이를 통해 Cloud Web Security로 트래픽을 리디렉션하여 웹 보안 기능을 확보합니다.

차세대 방화벽(Cisco Adaptive Security Appliances, 물리 및 가상): Cloud Web Security를 통해 콘텐츠 검사 기능을 Cisco의 클라우드에 오프로드하여 Adaptive Security Appliance 투자를 활용합니다. 기업, 그룹 또는 개별 사용자에게 제한적 사용 정책을 적용합니다.

Web Security Appliance(물리 및 가상): ID 정보를 클라우드로 보낼 수 있도록 Cloud Web Security와 Web Security Appliance를 통합합니다. 또한 다른 온프레미스 엔터프라이즈 기능을 Cloud Web Security 고객에게로 확장합니다.

Cisco ISR G2: 지사에서 클라우드로 직접 인터넷 트래픽을 지능적으로 리디렉션하여 보안 및 제어 정책을 실행하여 대역폭, 비용 및 리소스를 절감하고 지점의 인터넷 속도를 개선합니다. 위치에 관계없이 모든 사용자에게 제한적 사용 정책을 적용합니다.

Cisco 4000 Series ISR: ISR G2를 통해 리디렉션할 때와 동일한 이점을 제공합니다. 동시에 안정적이고 잘 알려지고 발전된 산업 표준 GRE over IPsec 기술을 도입하여 유지 보수 비용을 절감합니다. 자세한 내용은 제어된 가용성 알림을 참조하십시오.

AnyConnect Secure Mobility Client: 최종 사용자가 기업 네트워크를 벗어날 때마다 웹 트래픽을 인증하고 리디렉션합니다. Cloud Web Security는 사용자가 사무실 외부에 있거나 VPN을 통해 연결하는 경우 캐시된 사용자 자격 증명 및 디렉토리 정보를 사용하여 동일한 웹 사용 정책이 적용되도록 합니다.

독립형 구축: 추가 하드웨어가 필요하지 않은 간단한 웹 보안 솔루션을 구축합니다. 기존 브라우저 설정 및 PAC(Proxy Auto-Configuration) 또는 WPAD(Web Proxy Auto-Discovery) 파일을 사용하여 Cloud Web Security 서비스에 연결합니다.

모든 Cloud Web Security 구축 옵션에는 최종 사용자 식별을 향상하는 디렉토리 인증 방법이 포함되어 있어 관리자가 사용자 또는 그룹 수준에서 정밀한 필터 제어를 적용하고 세부적인 로그 보고서를 실행할 수 있습니다.

서브스크립션

모든 Cisco Cloud Web Security 서브스크립션은 1년, 3년 또는 5년의 기간 기반 서브스크립션입니다.

사용자 수 기반 서브스크립션

Cisco Web Security 포트폴리오에는 디바이스가 아니라 사용자 수에 기반한 계층형 가격이 적용됩니다. 영업 및 파트너 담당자가 각 고객 구축에 대해 올바른 계층을 결정할 수 있도록 도와드립니다.

대역폭 기반 서브스크립션

고객은 다양한 구축 사이트에서 Cloud Web Security 데이터 센터로 전달될 전체 트래픽을 집계하여 대역폭을 기반으로 Cloud Web Security를 사용할 수 있습니다.

Security Enterprise License Agreement

Cisco Security ELA(Enterprise Licensing Agreement)는 단일 계약을 통해 간소화된 라이센스 관리 기능과 라이센스 비용 절감 효과를 제공합니다. 추가 비용 없이 ELA v3 보유 고객은 Cloud Web Security Essentials를 추가할 수 있고, ELA v4 보유 고객은 Cloud Web Security Premium을 추가할 수 있습니다. Security Enterprise License Agreement에 대한 자세한 내용은 Cisco 어카운트 담당자에게 문의하십시오.

소프트웨어 서브스크립션 지원

모든 Cloud Web Security 서브스크립션에는 다음과 같은 지원 혜택도 포함됩니다.

- Cisco 클라우드에 패치, 소프트웨어 업데이트 및 유지 보수를 자동으로 적용하여 애플리케이션 및 플랫폼 소프트웨어를 최신 상태로 유지
- 일주일에 7일, 하루 24시간 Cisco TAC(Technical Assistance Center) 액세스 가능
- 애플리케이션 툴, 기술 문서 및 교육이 포함된 온라인 리포지토리에 액세스 가능
- 온라인 기술 정보 및 서비스 요청 관리를 위한 Cisco.com에 대한 등록된 액세스

서비스

Cisco는 보안에 대해 위협 중심의 접근 방식을 사용하여 네트워크상의 네트워크 인프라와 자산을 보호합니다. Cisco의 서비스는 설치한 보안 어플라이언스 및 시스템을 최대한 활용할 수 있도록 지원합니다.

Cisco Branded Services

Cisco에서는 성공적인 보안 구축을 위해서는 평가, 통합, 최적화, 관리 등 4가지 작업이 필수적이라는 사실을 확인했습니다. 이러한 서비스를 활용하여 해당 작업을 구현할 수 있습니다.

Cisco Security Planning and Design Service: 다음을 통해 신속하고 비용 효율적으로 강력한 보안 솔루션을 개발 및 구현할 수 있도록 지원합니다.

- 기술 준비도 평가
- 설계 개발
- 구현 엔지니어링
- 지식 이전

Cisco Web Security Configuration and Installation Service: 다음을 구현하기 위한 설치, 구성 및 테스트를 통해 웹 보안 위험을 완화할 수 있도록 지원합니다.

- AUP(Acceptable-Use Policy) 제어
- 평판 및 악성코드 필터링
- 데이터 보안
- 애플리케이션 가시성 및 제어

Cisco Security Optimization Service: 위협을 방지, 탐지 및 차단할 수 있는 네트워크 기능을 평가하고 강화할 수 있도록 지원합니다. 이 서비스에서는 네트워크 보안 평가, 설계, 지원, 학습 활동을 하나의 포괄적인 서브스크립션 패키지에 통합하여 제공합니다.

Cisco Managed Threat Defense: 알려진 취약성 및 지능형 지속 위협을 차단할 수 있도록 동적인 실시간 탐지 및 교정 기능을 제공합니다. Cisco는 글로벌 보안 운영 센터 네트워크를 통해 서브스크립션 기반 모델로 위협 방어 기능을 제공할 수 있는 하드웨어, 소프트웨어 및 전문 지식을 제공합니다.

협업/파트너 서비스

계획, 설계, 구현 및 최적화 라이프사이클 전체에서 Cisco 파트너가 제공하는 다양하고 가치있는 서비스를 사용할 수 있습니다. 암호화 맵은 다음을 포함합니다.

Cisco Network Device Security Assessment: Cisco 네트워크 인프라 보안상의 허점을 찾아내 더 강력한 네트워크 디바이스 환경을 구현 및 유지할 수 있도록 지원합니다.

Smart Care Service(Cisco Certified Partner가 제공): 능동적인 네트워크 모니터링, 평가, 소프트웨어 수리 및 기술 지원을 통해 네트워크 유지 보수를 간소화할 수 있도록 지원합니다.

기타 서비스

Cisco PSIRT(Product Security Incident Response Team): PSIRT는 Cisco 제품 및 네트워크와 관련된 보안 취약성 정보의 접수, 조사 및 공개 보고를 관리하는 전담 글로벌 팀입니다.

Cisco SDL(Secure Development Lifecycle): Cisco 제품의 복원력 및 신뢰성을 높이도록 설계된 반복 및 측정 가능한 프로세스입니다.

시스코 서비스에 대한 자세한 내용은 http://www.cisco.com/en/US/products/hw/vpndevc/services.html을 참조하십시오.

워런티 정보

보증 정보는 Cisco.com의 제품 보증 페이지에서 확인하십시오.

Cisco Capital

목표 달성을 지원하는 파이낸싱

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기

추가 정보

자세한 내용은 http://www.cisco.com/go/cws를 참조하십시오. Cloud Web Security가 여러분 회사에 얼마나 효과적으로 적용될 수 있을지 Cisco Sales Representative, 채널 파트너, 시스템 엔지니어와 함께 평가해 보십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

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. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-729637-07 12/15