한눈에 보기

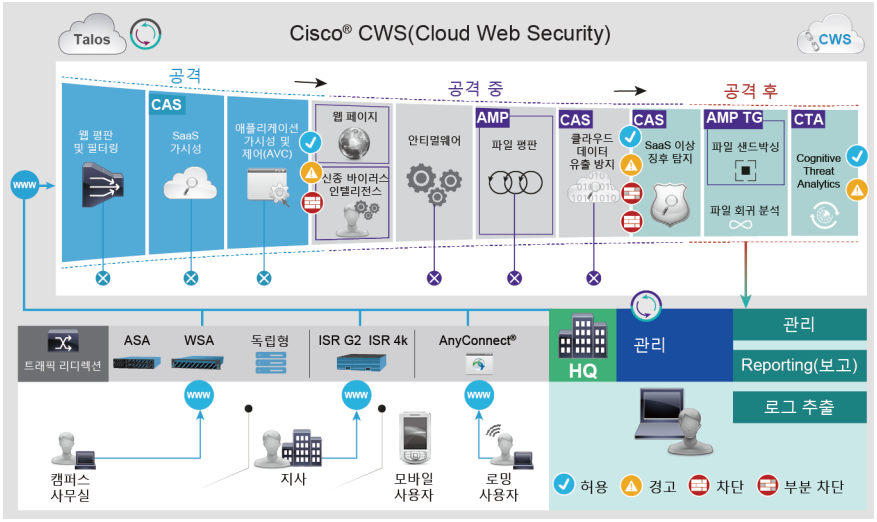
혜택

- **세분화된 웹 사용 정책:** 애플리케이션, 웹 사이트 및 특정 웹 페이지 콘텐츠의 전체 환경에서 설정하고 실행합니다.
- **간편한 통합:** 유연한 네트워크 통합 옵션으로 Cisco CWS(Cloud Web Security)를 기존의 인프라에 연결할 수 있습니다.
- **실시간 위협 인텔리전스:** 분석 엔진이 웹 기반 공격에 대항하여 업계 최고의 안티멀웨어 및 제로데이 위협 차단 기능을 제공합니다. 새로운 위협으로부터 보호하기 위해 Cisco의 어드밴스드 글로벌 위협 텔레메트리 네트워크는 Cisco CWS를 지속적으로 업데이트합니다.
- **중앙 집중식 관리 및 보고:** 웹 사용 및 위협 정보에 대한 가시성을 향상합니다.

Cisco Cloud Web Security

SaaS(Security as a Service) 제공

클라우드 서비스로 포괄적인 웹 보안을 제공하는 Cisco의 차별화된 보안 접근 방식을 만나 보십시오. Cisco는 Cisco CWS(Cloud Web Security) 솔루션을 통해 실제 환경에 맞는 인텔리전트 사이버 보안 기능을 제공합니다. 공격 전, 공격 중, 공격 후의 전 범위에서 탁월한 가시성, 일관된 제어력 그리고 지능형 위협 차단을 제공합니다.



클라우드 기반 웹 보안 솔루션으로서 Cisco CWS는 광범위한 SaaS(Security as a Service)를 제공합니다. 간단하고 신속하게 구축할 수 있으며, 유지 보수 또는 업그레이드가 필요하지 않습니다.

Cisco CWS를 사용하여 관리자는 전체 환경에서 특정 웹 사용 정책을 설정하고 실행할 수 있습니다. 사용자는 유연한 네트워크 통합 옵션을 통해 Cisco CWS를 기존 인프라에 연결할 수 있습니다. Cisco CWS는 SaaS 애플리케이션과 웹 페이지 및 애플리케이션의 특정 콘텐츠와 웹 사이트에 대한 액세스를 제어합니다. Cisco의 분석 엔진은 웹 기반 공격에 대항하여 지속적으로 업계 최고의 안티 멀웨어 및 제로 데이 위협 차단 기능을 제공합니다. 최신 위협에 대항하여 Cisco의 어드밴스드 글로벌 위협 텔레메트리 네트워크는 Cisco CWS를 지속적으로 업데이트합니다.

Cisco AMP(Advanced Malware Protection)는 지능형 악성코드를 차단하고 악성 파일의 이동 경로를 알 수 있도록 시간 경과에 따라 파일 속성을 추적합니다. CTA(Cognitive Threat Analytics)는 웹 트래픽에서 감염의 증상을 스캔하고 경계 방어를 우회하는 위협을 해결합니다. CAS(Cloud Access Security)는 SaaS 앱에서 발생하는 증가하는 위험으로부터 보호합니다. 또한 중앙 집중식 관리 및 보고 기능을 제공하여 웹 사용 및 위협 정보에 대한 가시성을 향상합니다.

Cloud Web Security Pillars

포괄적인 방어

웹 필터링 및 웹 평판 점수를 통해 Cisco CWS는 75개 이상의 콘텐츠 카테고리 목록의 필터를 적용하여 5천만 개 이상의 알려진 웹 사이트에 대한 액세스를 제어합니다. Cisco의 애플리케이션 가시성 및 제어 기능은 직원 생산성 및 규정준수를 향상시키는 사용 제한 정책과 SaaS 가시성을 포함합니다. 직원이 업무에 필요한 사이트에 액세스할 수 있도록 이러한 제어에는 웹 페이지, 개별 웹 요소, SaaS 애플리케이션 및 마이크로애플리케이션 내의 활동에 대한 액세스가 포함됩니다. 중앙 집중식 정책 관리를 통해 언제 어디서나 액세스 할 수 있는 하나의 중앙 집중식 위치에서 모든 사용자와 전 지사의 모든 솔루션을 관리하고 정책을 시행할 수 있습니다.

실시간 악성코드 차단 기능은 휴리스틱스(heuristics) 기반 안티멀웨어 엔진을 통해 알려지지 않았으며 비정상적인 동작 및 제로아워 보안 침해를 식별하는 것에 기반을 둡니다. 보안 침해 인텔리전스는 보안 수준이 높은 가상 에뮬레이션으로 웹 페이지 구성 요소를 실행하여 각 구성 요소가 어떻게 동작하고 악성코드를 차단하는지 확인합니다. 로밍 사용자는 회사 사무실에 있는 Cisco CWS에서 사용할 수 있는 것과 동일한 보안 기능을 실행하는 Cisco AnyConnect®로 보호됩니다. 보안 모바일 브라우저에서는 모바일 디바이스를 보호합니다.

지능형 위협 차단

Cisco AMP 및 Threat Grid는 공격 전, 공격 중, 공격 후의 전 범위에서 네트워크 환경을 보호합니다. 파일 평판 기능을 통해 Cisco는 각 파일이 고객 네트워크를 통과할 때 해당 파일의 핑거프린트를 캡처할 수 있습니다. 이러한 핑거프린트는 평판 판단을 위해 AMP의 클라우드 기반 인텔리전스 네트워크에 전송됩니다.

공격 후, 파일 회귀 분석을 사용하여 파일이 해당 환경에 들어온 후 시간 경과에 따라 변한 속성을 추적할 수 있습니다. 악성코드로 확인될 경우, 해당 파일이 어디로 들어와서 현재 어디에 있는지 파악하여 앞으로의 침입을 차단할 수 있습니다.

Cisco의 클라우드 기반 CTA 기능은 지속적인 노력을 통해 위협 식별 시간을 분 단위로 단축시켜 줍니다. CTA는 동작 분석, 이상 징후 탐지 및 기계 학습을 통해 악성코드 감염 증상을 적극적으로 식별합니다. 또한 세계 최대의 위협 탐지 네트워크 중 하나인 Cisco Talos Security Intelligence Research Group을 통해 최고 수준의 연구자와 시스템이 전 세계 네트워크, 엔드포인트, 모바일 디바이스, 가상 시스템, 웹 및 이메일에 대한 위협 추적을 기반으로 Cisco CWS에 보안 인텔리전스를 지속적으로 제공합니다.

CAS는 제어를 클라우드 앱으로 확장하므로, 사용자가 클라우드 앱과 데이터를 공유하도록 허용하는 방법을 규제하는 정책을 설정할 수 있습니다. 또한 비정상적인 트래픽을 탐지하고 사고의 근본 원인을 식별할 수 있습니다.

뛰어난 유연성

Cisco CWS는 99.999% 업타임에 기반한 SLA(Service-Level Agreement)를 사용하는 전세계 네트워크 및 23개 데이터 센터가 지원합니다. 자신의 웹 사용 가사성을 10분 간격으로 업데이트되는 10,000개 이상의 맞춤형 보고서를 사용하여 맞춤화 할 수 있으며 사용자 트래픽과 애플리케이션 트래픽을 분류할 수 있는 기능도 지정할 수 있습니다. 웹 사용 데이터를 신속하게 액세스 할 수 있으며 SIEM(Security Information and Event Management)과 같은 다양한 보고 및 분석 툴을 사용하여 높은 보안 수준으로 액세스할 수 있습니다.

또한 Cisco Integrated Router G2 및 ISR 4000, Cisco Adaptive Security Appliance(ASA 및 ASAv) 차세대 방화벽, Cisco Web Security Appliance(WSA 및 WSAV), Cisco AnyConnect Web Security Module과 같은 기존 Cisco 제품을 통해 Cisco CWS에 트래픽을 리디렉션하여 시간과 비용을 절감할 수 있습니다. 독립형 구축에서도 Cisco CWS에 연결할 수 있습니다.

다음 단계

자세한 내용은 http://www.cisco.com/go/cloudwebsecurity를 참조하십시오.

C45-730902-02 10/15