Cisco AWSR(Advanced Web Security Reporting)

소개

Cisco® AWSR(Advanced Web Security Reporting) 애플리케이션은 Cisco WSA(Web Security Appliances) 및 Cisco CWS(Cloud Web Security)에서 생성되는 로그를 신속하게 색인화하고 분석하는 보고 솔루션입니다. 이 툴은 트래픽 및 스토리지 요구 사항이 많은 고객에게 알맞은 확장식 보고 기능을 제공합니다. 또한 관리자가 웹 사용 및 악성코드 위협에 대한 세부적인 통찰력을 수집할 수 있는 보고 기능도 제공합니다.

디렉토리 그룹 기반 보고

Advanced Web Security Reporting 애플리케이션을 통해 관리자는 Active Directory 같은 중앙 인증 서버 내에 정의된 그룹 또는 사용자 ID를 기준으로 보고서를 생성할 수 있습니다. 인증 그룹에 정의된 기능적 또는 지리적 경계에 따라 보고서를 손쉽게 생성할 수 있습니다. 관리자가 정의된 디렉토리 그룹(예를 들어 관리자가 관리하는 그룹)에 대한 보고서만 볼 수 있도록 역할을 생성하여, 해당 그룹에 속하지 않은 개인의 개인 정보를 보호할 수 있습니다.

상세한 L4TM(Layer 4 Traffic Monitor) 가시성

관리자는 nonweb 포트의 활동에 대한 보고서를 실행할 수 있습니다. 이러한 L4TM(Layer 4 Traffic Monitor) 보고서는 특정 포트 및 사용자와 연동된 호스트를 연결하며, 비표준 포트에서 수많은 기존의 웹 보안 솔루션을 회피하려는 악의적인 행동을 식별하는 데 사용될 수 있습니다.

SOCKS 보고

SOCKS(Socket Secure) 프록시 설정을 사용하는 고객의 경우, 관리자가 SOCKS 트래픽에 대한 정보를 얻을 수 있습니다.

데이터 내역 가져오기

내역이 기록된 로그는 포렌식 조사 중에 가져올 수 있습니다. 모든 기간의 로그를 보고 툴로 가져와 분석할 수 있으므로, 인사 담당자 및 법무 담당자는 몇 년에 걸친 기간을 지정하여 포렌식 조사를 수행할 수 있습니다. 필요한 경우, 관리자는 특정 사용자의 웹 활동을 집중적으로 살펴볼 수 있습니다.

Advanced Malware Protection 보고

WSA 및 CWS를 통과한 후에도 위협을 지속적으로 분석할 수 있도록 파일 평판 점수 및 차단, 정적 및 동적 파일 분석(샌드박싱), 파일 회귀 분석 등의 기능을 제공합니다. 이 보고 애플리케이션은 관리자가 웹 사용 및 악성코드 위협에 대한 상세한 통찰력을 얻을 수 있도록 더욱 심도 있는 분석을 위한 단일 창을 제공하는 Cisco Advanced Malware Protection 솔루션이 제공하는 데이터를 통합합니다.

Web Reporting은 누가 사용해야 합니까?

Cisco Web Security 및 Security Management Appliance에 내장된 보고 기능은 대부분의 Cisco 고객이 필요로 하는 보고 요구 사항을 충족해 줍니다. 트랜잭션 양이 증가하여 확장된 스토리지가 필요하거나 디렉토리 그룹 기반 보고 기능이 필요한 고객을 위한 대안적인 보고 솔루션으로 Advanced Web Security Reporting을 사용할 수 있습니다.

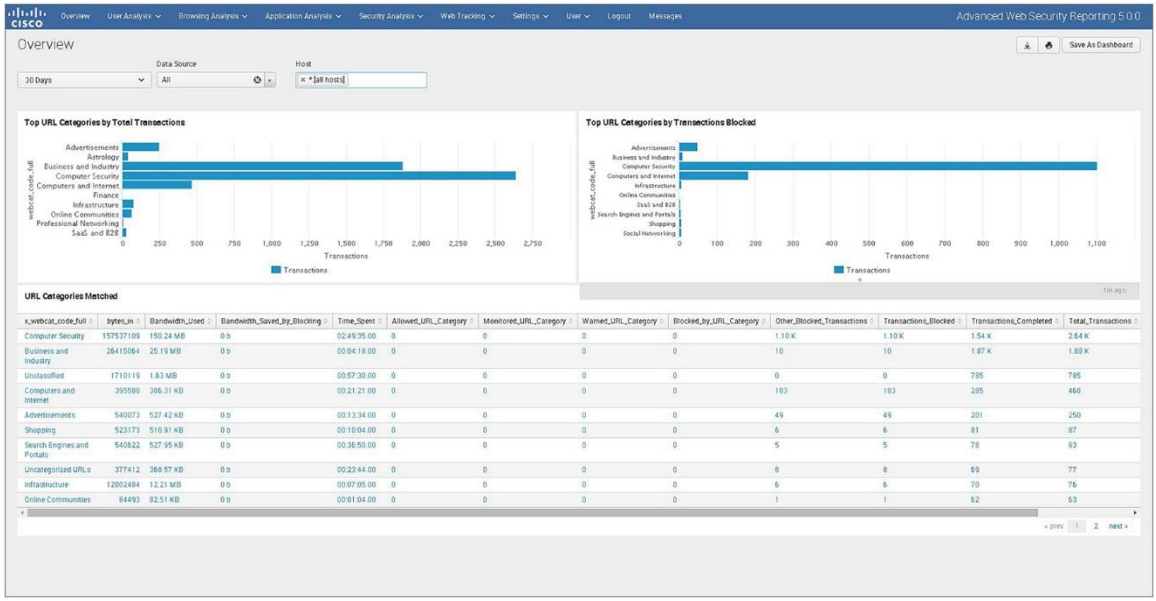
또한, 하이브리드 웹 보안 솔루션을 구축한 고객을 위한 "단일 창" 역할도 수행합니다. Cisco Web Reporting 보고서 형식은 이미 Cisco S-Series 및 M-Series어플라이언스에서 제공하는 보고서와 동일합니다.

Cisco Web Reporting의 최신 릴리스에는 어떤 기능이 포함되어 있습니까?

- **통합된 웹 보안 보고:** Cisco AWSR(Advanced Web Security Reporting) 애플리케이션은 구축 상태와 관계없이(그림 1) 더욱 쉽게 웹 보안을 모니터링할 수 있도록 다양한 정보를 단일 디스플레이에 통합해 줍니다. 보고 애플리케이션은 사전 정의된 보고서를 위해 여러 Cisco WSA 및 CWS에서 수집한 로그 데이터를 폴링합니다. 고객은 플래시 타임라인 보기 및 웹 추적 양식을 사용하여 애드혹 검색을 수행할 수도 있습니다.
- **규모와 성능:** Cisco Advanced Web Security Reporting 애플리케이션 릴리스 4.0은 시트 대역 전반의 데이터 계층 도입에 맞게 조정하여 일일 로그 볼륨 요구 사항에 따라 유연하게 구매할 수 있습니다.
- 하위 계층: 이 버전은 현재 고객의 제한된 데이터 요구 사항(사용자당 1일 2MB)을 충족합니다.
- 상위 계층: 이 버전은 데이터 요구 사항이 높은 사용자(사용자당 1일 6MB)를 보유한 하이브리드 웹 보안 및 엔터프라이즈 라이선스 계약(ELA) 고객을 위한 것입니다.

* 이러한 옵션에는 Web Security Reporting 라이선스만 포함됩니다. 이 제품에는 컨피그레이션 및 정책 관리 라이선스는 포함되지 않습니다. 예를 들어, 여기에는 독립 실행형 CWS 애플리케이션 보고 또는 이 솔루션을 사용하는 통합 Cisco WSA 및 CWS 보고에 필요한 Cisco WSA Log Extraction 라이선스인 SMA가 포함되지 않습니다.

그림 1. 차단된 URL 범주 및 트랜잭션에 대한 보고서



시스템 요구 사항

Advanced Web Security Reporting은 Microsoft Windows 및 Red Hat Linux에서 실행됩니다. Advanced Web Security Reporting 애플리케이션의 특정 릴리스의 시스템 요구 사항에 대한 자세한 내용은 릴리스 노트의 " Advanced Web Security Reporting 요구 사항" 섹션을 참조하십시오.

Cisco 어카운트 팀과 의논하고 문서를 참조하여 조직에서 Cisco Web Reporting 애플리케이션을 실행하는 데 필요한 하드웨어 사양을 숙지하시기 바랍니다.

Cisco Capital

시스코 금융 지원 솔루션
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 도입 편의성을 제공합니다. 또한, 정해진 일자에 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세한 내용은 관련 웹 사이트에서 알아보십시오.

추가 정보

자세한 내용은 주문 가이드, 릴리스 노트 및 사용 설명서를 참조하십시오.

시작하기: Linux 및 Windows용 단일 설치 프로그램을 다운로드하십시오.

문의: Cisco 파트너 고객 관리자에게 문의하십시오.

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

Printed in USA C78-729104-04 07/16