Cisco Stealthwatch Learning Network 라이선스

Cisco® Stealthwatch Learning Network 라이선스는 지사 위협에 대해 개선된 보안을 제공합니다.

이 솔루션은 Cisco Stealthwatch 제품군의 일부입니다. 또한 Cisco 네트워크 내에서 의심스러운 트래픽 패턴을 식별하여 지능형 위협에 대한 향상된 가시성을 제공합니다.

Learning Network 라이선스는 Cisco ISR(Integrated Services Router)을 보안 센서로 활용하여 NetFlow, NBAR(Network-Based Application Recognition), 머신 학습을 사용하는 지능형 센서 및 패킷 캡처를 통해 지사 트래픽을 모니터링합니다. 트래픽 패턴의 베이스라인을 분석하여 이상 징후를 탐지하고 효과적인 브랜치 보안 정책을 구축하는 데 도움을 줍니다. Cisco 관리자를 통해 ISR 에 의심스러운 패킷을 삭제하도록 지시하여 지사에서 직접 위협을 완화할 수 있습니다.

제품 개요

Cisco Stealthwatch Learning Network 라이선스는 라우터를 보안 디바이스로 전환하여 네트워크 인프라에 보안을 포함합니다. 또한 지사 네트워크 전체 및 지사 간에 더욱 심층적인 가시성을 제공합니다. 이 제품은 강화된 네트워크 보호 기능을 제공하며 위협에 신속하게 대응합니다. 네트워크 성능에 영향을 미치지 않으면서 지사로 보안 범위를 확장합니다.

Learning Network 는 2 가지 구성 요소로 구성됩니다.

1. 분산된 학습 에이전트는 ISR 지사 라우터에서 네트워크 에지에 배치됩니다. 에이전트는 Cisco IOS® XE Software 및 컨테이너 기능을 갖춘 소프트웨어 에이전트로 구현될 수 있습니다. 옵션으로 Cisco UCS® 블레이드와 함께 ISR 에 설치될 수 있습니다.
2. 에이전트는 중앙 모니터링 에이전트에서 관리됩니다. 관리자는 특정 가상 머신 서버에 설치됩니다. 각 에이전트는 정상(베이스라인) 항목을 파악하고 결과적으로 이상 징후를 탐지하기 위해 머신 학습 알고리즘 및 기술을 사용하여 환경에 고유하게 맞춤화될 수 있습니다. 각 에이전트는 NetFlow 레코드, 원시 패킷(예: DNS 패킷)의 DPI(Deep Packet Inspection) 및 심지어 지사 라우터 또는 스위치에서 사용 가능한 로컬 상태 등 다양한 데이터 피드를 활용하여 트래픽 특성을 자율적으로 모델링합니다.

에이전트는 자체 모델을 구축하고 중앙 집중식 분석을 위해 WAN 을 통해 과부하 트래픽 전달을 방지합니다. 또한 메모리 및 CPU 소비 측면에서 경량으로 설계되었습니다.

관리자는 Learning Network 라이선스 솔루션에 대한 사용자의 진입점 역할을 합니다. 이것은 데이터 센터에서 실행 중인 확장성이 뛰어난 애플리케이션입니다. 또한 에이전트를 “오케스트레이션”합니다. 또한 제공하는 정보를 집계 및 저장하고 다른 소스의 정보를 사용하여 컨텍스트를 강화합니다. (여기에는 Cisco pxGrid 및 Cisco Identity Services Engine 의 위협 인텔리전스, Talos 의 인텔리전스, DNS 트랜잭션 세부 정보 등이 포함될 수 있습니다.) 관리자는 모든 정보를 검색하여 분석하는 방법을 제공하며, 사용자가 시스템을 제어하고 피드백을 제공할 수 있도록 지원합니다.

기능 및 장점

기능	장점
이상 징후 탐지	“이상 징후 탐지”는 Learning Network 등의 시스템에서 정상 트래픽에 대한 복합적인 표현(모델링)을 구축하는 기능을 의미합니다. 이 기능은 잠재적으로 여러 가지 수치(시각, 트래픽 특성, 플로우당 패킷 수, 플로우 기간, 보이지 않는 트래픽 등)를 세부적으로 캡처합니다. 이러한 모델은 보안 공격 및 취약점을 나타낼 수 있는 “이상값” 또는 이상 징후를 탐지하는 데 사용됩니다. 이러한 시스템은 일반적으로(전적으로는 아님) 감독 되지 않는 머신 학습 알고리즘을 광범위하게 사용합니다.
관련성 학습	관련성 학습은 자가 학습 네트워크의 핵심 개념입니다. “긍정 오류”는 일반적으로 이상 징후 탐지에 의해 이상 징후로 잘못 판단된 이벤트를 의미합니다. 예를 들어, 차량을 인식하도록 설정된 시스템이 자전거를 차량으로 잘못 분류한 경우 이러한 분류를 긍정 오류라고 합니다. 사용자 관련성은 사용자가 제공한 레이블(예: “좋아하는 항목” 또는 “싫어하는 항목”)을 활용하여 시스템에서 동적으로 학습됩니다. 이상 징후를 받는 즉시 사용자는 좋아하는 항목/싫어하는 항목 피드백을 제공할 수 있습니다. h Learning Network 라이선스는 이 피드백을 사용하여 시스템에서 제기한 이상 징후의 관련성을 지속적으로 개선합니다.
완화 작업	분산된 학습 에이전트는 이상 징후 탐지뿐만 아니라 이상 징후 완화에도 사용될 수 있습니다. 각 에이전트가 관리자에게 이상 징후를 자세히 보고합니다. 사용자가 이상 활동을 이해한다면 나쁜 영향을 줄 수 있는 이상 트래픽이 네트워크를 통해 전달되는 것을 방지할 수 있습니다. 예를 들어, 사용자는 탐지 에이전트 근처에 있는 로컬 라우터에서 이상 트래픽을 삭제할 수 있습니다. 또는, 네트워크의 어느 위치에서 발생하든 관계없이 이상 호스트로 이동하거나 이상 호스트에서 나온 모든 트래픽을 삭제할 수 있습니다. 관리자는 ISR 로 다시 액세스 제어 목록을 보낼 수 있습니다.
외부 시스템의 ISE 와의 통합	Learning Network 라이선스는 네트워크에서의 이상 활동에 대한 추가적인 통찰력을 제공하기 위해 네트워크에서 사용 가능한 위협 인텔리전스 정보를 활용합니다. Cisco ISE(Identity Services Engine)를 구축한 경우, 에이전트는 pxGrid API 를 통해 ISE 와 통신하며 네트워크 사용자, 사용자 위치 및 기타 특성과 관련된 수많은 개인화된 정보를 수집합니다. 이상 활동이 네트워크에서 탐지된 경우 관리자는 문제 호스트에 대한 더욱 상세한 정보를 제공할 수 있습니다. 또한 사용자의 이름, 현재 위치(사용자와 연결된 스위치 및 스위치 포트) 등을 식별할 수도 있습니다.
외부 시스템의 Talos 데이터베이스와 통합	관리자가는 해당 활동의 특성을 포함하여 과거 이상 활동과 관련된 것으로 알려진 IP 주소를 포함하는 Talos 데이터베이스를 활용합니다. Talos 데이터베이스는 각 이상 징후에 적용된 위협 인텔리전스 정보에 대한 또 다른 소스입니다.
패킷 캡처	이상 징후 탐지에서 이벤트 세부 정보를 캡처할 수 있는 것도 중요합니다. Integrated Services Router 의 기능을 사용하여 관리자는 라우터에 특정 이벤트의 패킷을 캡처하도록 지시할 수 있습니다. 사고 대응 및 디바이스 레벨 완화를 더 빠르게 수행할 수 있습니다. 패킷 캡처는 ISR 의 하드 드라이브 스토리지 기능에 의해 제한됩니다.

플랫폼 지원

Stealthwatch Learning Network 라이선시는 새로운 Cisco 4000 Series Integrated Services Router 및 Cisco IOS XE 모듈 아키텍처를 활용하도록 특별히 설계되었으며 이를 통해 에이전트가 Cisco IOS XE 컨테이너에서 소프트웨어 에이전트로 설치될 수 있습니다. 또한 에이전트는 Cisco UCS E-Series 블레이드에 설치될 수 있습니다. (자세한 내용을 확인하려면 http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-e-series-servers/index.html 로 이동하십시오.)

모든 4451 또는 4431 ISR 에 Stealthwatch Learning Network 라이선스를 추가할 수 있습니다. 그러나 4000 Series AX 또는 AXV ISR 번들을 주문하는 것이 좋습니다. 이 번들은 Stealthwatch Learning Network 라이선스에 필요한 AppX 라이선스와 함께 제공되며 IWAN(Intelligent WAN)을 포함한 모든 보안 기능을 포함합니다. 번들 주문 설명서(Cisco 4000 Series Integrated Services Router 제품군 주문 가이드)를 참조하십시오. 또한 SLN 을 완벽하게 지원하는 Cisco ONE WAN 번들(C1-CISCO4431/K9 및 C1-CISCO4451/K9)을 참조하십시오(http://www.cisco.com/c/en/us/products/software/one-wan/wan-part-numbers.html).

제품군	지원되는 플랫폼	지원되는 Cisco IOS 이미지(기능 세트)
Cisco 4000 Series ISR	4431 및 4451 ISR* 에이전트는 소프트웨어 전용 설치 에이전트로 지원되며 옵션으로 Cisco UCS E-Series 블레이드에서 지원됩니다. *다른 ISR 모델은 이후에 지원될 예정입니다.	Universal 및 AppX(Application Experience) 라이선스 또는 AppX 라이센스를 포함하는 AX 또는 AXV 번들이 있는 IOS XE 3.16.0S 이상.
Cisco UCS E-Series 서버 모듈	Cisco UCS E140S M2 Software 이상(예: E160).	ESXi 5.5
Cisco 2900 및 3900 Series ISR	2921, 2951 및 3945 ISR. Cisco UCS E-Series 블레이드에서만 지원됩니다.	Cisco IOS 릴리스 15.5(3) M1 이상 및 NBAR(2) 프로토콜 팩

라이선싱

Cisco Stealthwatch Learning Network 라이선스는 Smart Software Licensing 이 지원되는 제품입니다. 에이전트는 1 년 및 3 년 기간 라이선스로 판매됩니다. 관리자는 영구 라이선스를 보유합니다. 아직 Smart License 어카운트가 없는 경우, 설정하려면 Cisco 담당자에게 문의하십시오. Smart Software Licensing 에 대한 자세한 내용을 확인하려면 http://www.cisco.com/web/ordering/smart-software-licensing/index.html 로 이동하십시오.

시스템 요구 사항

Cisco IOS XE Software 의 에이전트	에이전트가 Cisco IOS XE 컨테이너에서 실행되는 경우, 최소 8MB RAM 이 필요합니다. 패킷 캡처를 사용하려는 경우, 플래시 포함 500MB 로 제한됩니다. 사용량을 높이기 위해 패킷 캡처를 사용하려는 경우, SSD 의 NIM 캐리어 카드로 ISR 에 스토리지를 추가해야 합니다.
Cisco UCS E-Series Server 의 에이전트	Cisco UCS E-Series OVA(Open Virtualization Archive)는 155GB 디스크, 5GB 메모리, 4 개의 vCPU 및 ESXi 5.5 를 사용하도록 구성되었습니다.
부서장	관리자는 4 개의 vCPU, 24GB RAM 및 200GB 스토리지가 포함된 ESXi 5.5 이상이 필요합니다. 관리자는 최대 1000 개의 에이전트를 지원할 수 있습니다. 50 개 이상의 에이전트를 설치하려면 64Gb 의 메모리, 16 개의 vCPU 및 4Tb 의 스토리지가 권장됩니다.

주문 정보

부품 번호	제품 설명
L-SW-LN-44-1Y-K9	4400 Series 용 Cisco Stealthwatch Learning Network 라이선스(1 년 기간)
L-SW-LN-44-3Y-K9	4400 Series 용 Cisco Stealthwatch Learning Network 라이선스(3 년 기간)
L-SW-LN-UCS-1Y-K9	UCS Series 용 Cisco Stealthwatch Learning Network 라이선스(1 년 기간)
L-SW-LN-UCS-3Y-K9	UCS Series 용 Cisco Stealthwatch Learning Network 라이선스(1 년 기간)
L-SW-SCA-K9	Cisco Stealthwatch Learning Network 중앙 집중식 에이전트 관리자

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital® 파이낸싱을 통해 목표를 달성하는 데 필요한 기술을 도입하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI 를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital 은 100 여 개 국가에서 이용할 수 있습니다. 자세히 보기.

추가 정보

Cisco Stealthwatch Learning Network 라이선스에 대해 자세히 알아보려면 http://www.cisco.com/go/stealthwatch 로 이동하십시오.

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 C78-737494-02 09/16