Cisco Secure Network Analytics (이전 이름 Stealthwatch)

Contents

Cisco Secure Network Analytics

이 문서에서는 Cisco Secure Network Analytics(이전 명칭 Stealthwatch Enterprise)에 대한 정보를 설명합니다. Cisco Secure Cloud Analytics(이전 이름 Stealthwatch Cloud) 데이터시트를 여기에서 검토할 수 있습니다.

자세한 내용은 https://cs.co/sna를 참조하십시오.

솔루션 개요

Cisco Secure Network Analytics는 위협을 실시간으로 탐지하고 대응할 수 있도록 전사적 네트워크 가시성을 제공합니다. 이 솔루션에서는 네트워크 활동을 지속적으로 분석하여 정상적인 네트워크 행동의 베이스라인을 생성합니다. 그런 다음 이 베이스라인과 함께 비시그니처 기반의 고급 분석과 함께 행동 모델링과 머신 러닝 알고리즘과 전역 위협 인텔리전스를 포함하는 고급 분석을 함께 사용하여 이상 징후를 식별하고 실시간으로 위협을 탐지하고 대응합니다. Secure Cloud Analytics는 명령 및 제어(C&C) 공격, 랜섬웨어, 분산 서비스 거부(DDoS) 공격, 불법 크립토마이닝, 알 수 없는 악성 코드, 내부자 위협 등의 위협을 빠르고 확실하게 탐지할 수 있습니다. 에이전트 없는 솔루션을 사용하면 전체 네트워크 트래픽(암호화된 트래픽 포함)에 대한 포괄적인 위협 모니터링을 수행할 수 있습니다.

기업에서는 이미 IT 인프라와 보안에 많은 투자를 하고 있습니다. 하지만 위협은 계속해서 침투할 방법을 찾고 있습니다. 더욱이, 보안 침해를 탐지하는 데는 몇 달, 심지어 몇 년이 걸리는 경우도 있습니다. 이러한 가시성 부족은 지속적으로 증가하는 네트워크 복잡성과 끊임없이 진화하는 위협의 결과입니다. 리소스가 제한적이고 도구가 분산되어 있는 보안팀은 할 수 있는 일이 한정되어 있습니다. 거의 모든 조직에는 방화벽과 같은 보안 솔루션이 있지만, 이러한 툴이 올바르게 작동하고, 관리되며, 설정되어 있는지 어떻게 알 수 있을까요? 고객이 이러한 툴이 필요한 작업을 수행하고 있음을 어떻게 알 수 있을까요?

우리는 문제를 근본적으로 해결하기로 결정했습니다. 기존 투자인 네트워크를 활용하여 조직을 보호하는 것은 어떨까요? 네트워크 텔레메트리는 누가 조직에 연결하고 무엇을 하고 있는지에 대한 귀중한 인사이트를 제공할 수 있는 풍부한 데이터 소스입니다. 모든 것이 네트워크와 연결되므로 이러한 가시성은 본사에서 브랜치, 데이터 센터, 로밍 사용자, 스마트 디바이스(프라이빗 및 퍼블릭 클라우드로 확장)에 이르기까지 확장됩니다. 이 데이터를 분석하면 기존 제어를 우회하는 방법을 찾아낸 위협이 큰 영향을 미치기 전에 탐지하는 데 도움이 될 수 있습니다.

솔루션은 Secure Network Analytics이며, 이는 네트워크를 참여시켜 온프레미스는 물론 프라이빗 및 퍼블릭 클라우드에서 트래픽의 엔드 투 엔드 가시성을 제공합니다. 이러한 가시성에는 모든 호스트를 파악하고, 특정 시점에 누가 어떤 정보에 액세스하는지를 확인하는 것이 포함됩니다. 이때부터 특정 사용자 또는 "호스트"의 정상적인 행동이 무엇인지 파악하고, 사용자 행동의 변경 사항에 대한 알림을 받을 수 있는 베이스라인을 설정하는 것이 중요합니다.

Secure Network Analytics는 하드웨어 어플라이언스 또는 가상 머신의 두 가지 구축 모델을 제공합니다. Secure Cloud Analytics(이전 이름 Stealthwatch Cloud)는 Secure Network Analytics의 SaaS(Software-as-a-Service) 버전입니다. 프라이빗 네트워크를 모니터링하는 것 외에도 Secure Cloud Analytics를 구축하여 퍼블릭 클라우드에서 위협 및 설정 문제를 탐지할 수 있습니다.

주요 활용 사례

실시간 위협 탐지

간단히 말해서, 가장 포괄적이고 상황이 다양한 네트워크 가시성을 제공하는 Secure Network Analytics는 오랜 기간 동안 검증된 업계 최고의 보안 분석과 결합함으로써 가장 광범위하고 정확도 높은 행동 기반 위협 탐지 기능을 통해 다음과 같은 점을 크게 개선합니다.

- 알 수 없는 위협 탐지: 통신 및 악성 도메인과 같이 기존의 시그니처 기반 툴에서는 누락되는 의심스러운 행동 기반 네트워크 활동을 식별합니다.
- 내부자 위협 탐지: 데이터 호딩, 데이터 유출, 의심스러운 외부 이동에 대해 경보를 받습니다.
- 암호화된 악성코드 탐지: 다층 머신러닝을 활용하고, 해독 없이 암호화된 웹 트래픽으로 가시성을 확장합니다.
- 정책 위반: 다른 툴에 설정된 보안 및 컴플라이언스 정책이 시행되는지 확인합니다.
- 사고 대응 및 포렌식: 위협 활동에 대한 철저한 지식, 포렌식을 위한 네트워크 감사 추적, SecureX 및 기타 Cisco Secure 솔루션과의 통합을 통해 빠르고 효과적으로 대응합니다.

원격 근무자 모니터링

Secure Network Analytics에서는 AnyConnect NVM(Network Visibility Module)의 엔드포인트 레코드 텔레메트리 데이터를 기본 텔레메트리 소스로 설정했습니다. 이를 통해 엔드포인트별 사용자 및 디바이스 컨텍스트를 광범위하고 세밀하게 추가로 캡처하여 사용자가 단일 VPN 세션을 사용하여 작업하는지, 분할 터널링을 사용하여 원격 작업 환경을 최적화하는지 또는 VPN 연결이 완전히 끊어졌는지 여부에 관계없이 모바일 원격 근무자의 엔드포인트 활동에 대한 완전하고 지속적인 가시성을 조직에 효과적으로 제공할 수 있습니다. 따라서 패치가 필요한 취약성이 있는 이전 운영 체제 버전을 실행 중인 직원, 데이터 호딩 또는 데이터 유출 작업에 종사하는 직원 등 이전에는 파악할 수 없었던 작업을 파악할 수 있어 조직의 보안 상태를 강화할 수 있습니다.

그룹 기반 정책 보고

사용자는 그룹 통신을 시각화하는 새로운 방법을 제공하는 그룹 기반 정책 보고서를 생성함으로써 그룹 기반 정책 도입 노력을 가속화하기 위해 Cisco Secure Network Analytics와 Cisco Identity Services Engine의 통합을 활용할 수 있습니다. 그룹 기반 정책 보고서를 통해 사용자는 그룹 간 커뮤니케이션을 손쉽게 시각화, 분석 및 드릴다운하고, 정책의 효과를 검증하고, 환경의 필요에 따라 올바른 정책을 채택하고, 관련 흐름 및 관련 IP에 대한 인사이트를 통해 정책 위반 조사를 간소화할 수 있습니다. 자세한 내용은 요약을 참조하십시오.

암호화된 트래픽 분석

암호화된 트래픽이 급격하게 증가하면서 위협 환경도 변화하고 있습니다. 암호화는 데이터 프라이버시 및 보안에 탁월한 방식이지만, 사이버 범죄가 악성코드를 숨기고 탐지를 우회할 수 있는 기회가 되기도 합니다. 오늘날, 모든 웹 트래픽의 약 95%가 암호화되며, 공격의 70% 이상이 암호화를 사용할 것으로 예상됩니다. 성능 및 리소스와 관련된 이유로 인해 대량 암호 해독, 분석 및 재암호화를 수행하는 기존의 위협 검사를 사용할 수 없는 경우도 있습니다. 또한 개인 정보 보호 및 데이터 무결성을 손상시킵니다. 네트워크 인프라 시장에서의 전문성을 보유한 Cisco는 암호 해독 없이 암호화된 트래픽을 분석할 수 있는 획기적인 기술을 도입했습니다. 이를 통해 조직은 1) 암호화된 트래픽에서 위협을 탐지하고 2) 암호화 규정 준수를 보장할 수 있습니다. 자세한 내용을 보려면 https://www.cisco.com/go/eta로 이동하십시오.

주요 이점

- **사각지대는 더 이상 없습니다.** Secure Network Analytics는 모든 위치에 센서를 구축하지 않고도 프라이빗 네트워크 전반에 걸쳐 퍼블릭 클라우드에 대한 포괄적인 가시성을 제공할 수 있는 유일한 보안 분석 솔루션입니다. 또한 해독 없이 암호화된 트래픽에서 악성코드를 탐지하는 최초의 솔루션입니다.
- **노이즈가 아닌 인시던트에 집중:** 행동 모델링, 다층 머신러닝 및 글로벌 위협 인텔리전스의 강력한 기능을 사용하여 Secure Network Analytics는 환경에 영향을 미치는 중요한 위협에 대한 오탐 및 알람을 크게 줄입니다.
- **공격이 시작되는 순간 포착:** Secure Network Analytics는 네트워크를 지속적으로 모니터링하여 지능적인 위협을 실시간으로 탐지합니다. 은밀한 공격은 일반적으로 포트 스캐닝, 지속적인 Ping, 정찰 전술과 같은 활동이 수행됩니다. 이 솔루션은 시스템에서와 같은 조기 경고 징후와 경보를 인식하여 공격자를 조기에 차단합니다. 위협이 식별되면 사용자는 포렌식 조사를 수행하여 소스를 정확히 찾아내서 어디가 전파되었는지를 확인할 수 있습니다.
- **투자 극대화:** 에이전트 없는 솔루션을 통해 기존 네트워크 인프라에서 생성되는 풍부한 텔레메트리를 사용하여 보안 태세를 개선합니다.
- **비즈니스 성장에 따른 보안 확장:** 이제 비즈니스의 변화에 따라 보안을 타협할 필요가 없습니다. 새로운 브랜치나 데이터 센터를 추가하든, 워크로드를 클라우드로 이동하든, 단순히 디바이스를 추가하든 Secure Network Analytics 구축은 네트워크의 필요에 맞게 확장하여 커버리지를 쉽게 제공할 수 있습니다. 온프레미스 또는 클라우드에 구축할 수 있고, SaaS 기반 또는 라이선스 기반 솔루션으로 사용할 수 있으며, 자동 역할 분류 기능을 제공하여 네트워크에 추가되는 새로운 디바이스를 자동으로 분류합니다.
- **보안 에코시스템과 SecureX 통합: 이 솔루션은 SecureX** 플랫폼이 내장된 상태로 제공되어 확장된 위협 조사 및 대응 기능을 제공합니다. Secure Network Analytics는 SecureX와 통합되어 가시성을 통합하고 위협 대응을 간소화하며 모든 위협 벡터 및 액세스 포인트에서 자동화를 지원합니다.

솔루션 구성 요소

Secure Network Analytics의 핵심에는 필수 구성 요소인 매니저, 플로우 컬렉터 및 플로우 속도 라이선스가 있습니다. 또한 플로우 센서, Cisco Telemetry Broker 및 데이터 저장소와 같은 선택적 구성 요소를 제공하여 유연하고 강력한 아키텍처를 제공합니다.

시스템의 필수 구성 요소

매니저

Secure Network Analytics Manager는 최대 25개의 플로우 컬렉터, Cisco Secure Network Access(이전 이름 Cisco Identity Services Engine) 및 기타 소스의 분석을 집계, 구성 및 제공합니다. 종합적인 분석을 위해 네트워크 트래픽, 신원 정보, 사용자 지정 요약 보고서, 통합 보안 및 네트워크 인텔리전스를 그래픽으로 표시합니다.

매니저의 수용력에 의해 분석되고 표시 가능한 텔레메트리 데이터의 용량이 결정될 뿐만 아니라 구축 가능한 Flow Collector 수도 결정됩니다. 매니저는 하드웨어 어플라이언스 또는 가상 머신으로 제공됩니다. 표 1에는 매니저의 이점이 정리되어 있습니다.

표 1. 매니저의 주요 이점

이점	설명
실시간 최신 데이터	의심스러운 네트워크 동작을 파악할 수 있도록 수백 개 네트워크 세그먼트에서 트래픽을 동시에 모니터링하기 위한 데이터 흐름을 제공합니다. 이 기능은 엔터프라이즈 레벨에 특히 유용합니다.
보안 위협 탐지 및 우선순위 지정 기능	보안 위협을 신속하게 탐지하여 우선순위 지정, 네트워크 오용 및 최적화되지 않은 성능 파악, 엔터프라이즈 전반의 이벤트 대응 관리 등과 같은 작업이 하나의 컨트롤 센터에서 모두 이루어집니다.
어플라이언스 관리	Flow Collector, Flow Sensor, UDP Director를 비롯한 Cisco Network Analytics 어플라이언스를 구성, 조정, 관리합니다.
다양한 유형의 플로우 데이터 사용	Netflow, IPFIX, sFlow를 비롯한 다양한 유형의 플로우 데이터를 사용합니다. 결과: 비용 효율적인 행동 기반 네트워크 보호를 실현합니다.
확장성	아무리 큰 네트워크 수요도 지원합니다. 초고속 환경에서도 잘 작동하며 크기에 상관없이 IP 연결이 가능한 네트워크의 모든 부분을 보호할 수 있습니다.
네트워크 트랜잭션에 대한 감사 추적	보다 효율적인 포렌식 조사를 위해 모든 네트워크 트랜잭션에 대한 전체적인 감사 추적을 제공합니다.
맞춤화가 가능한 실시간 관계형 플로우 맵	조직 트래픽의 현재 상태에 대한 그래픽 보기를 제공합니다. 관리자는 위치, 기능, 가상 환경 등과 같은 기준에 따라 네트워크의 맵을 쉽게 구성할 수 있습니다. 2개의 호스트 그룹을 연결하면 운영자가 이러한 그룹 간의 트래픽 이동을 빠르게 분석할 수 있습니다. 또한 해당 데이터 포인트를 선택하면 특정 시점에 발생하는 일들에 대한 심층적인 인사이트를 확보할 수 있습니다.
유연한 구축 옵션	모든 규모의 조직에 적합한 확장형 디바이스인 물리적 어플라이언스를 주문할 수 있습니다. 또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 또는 KVM Hypervisor 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다.

매니저 사양

- Secure Network Analytics 매니저 2210 – 부품 번호: ST-SMC2210-K9
- Secure Network Analytics 매니저 2300 – 부품 번호: ST-SMC2300-K9
- Secure Network Analytics 매니저 Virtual Edition - 부품 번호: L-ST-SMC-VE-K9

플로우 컬렉터

플로우 컬렉터는 라우터, 스위치, 방화벽, 엔드포인트 및 기타 네트워크 인프라 디바이스와 같은 기존 인프라에서 NetFlow, IPFIX(Internet Protocol Flow Information Export), NVM, SYSLOG와 같은 엔터프라이즈 텔레메트리 유형을 수집하고 저장합니다. 또한 플로우 컬렉터는 프록시 데이터 소스에서 텔레메트리를 수집할 수 있습니다. 이는 클라우드 기반 머신 러닝 엔진으로 분석할 수 있습니다(전역 위협 알림).

텔레메트리 데이터를 분석하여 네트워크 활동에 대한 완전한 그림을 제공합니다. 몇 개월 또는 몇 년 동안의 데이터를 저장할 수 있으며, 포렌식 조사 및 컴플라이언스 이니셔티브를 개선하는 데 사용할 수 있는 감사 추적을 생성할 수 있습니다. 네트워크에서 수집할 수 있는 텔레메트리의 용량은 구축된 Flow Collector의 총 결합 용량에 따라 결정됩니다. Flow Collector를 여러 대 설치할 수 있습니다. Flow Collector는 하드웨어 어플라이언스 또는 가상 머신으로 제공됩니다. 표 2에는 플로우 컬렉터의 이점이 요약되어 있습니다.

표 2. 플로우 컬렉터의 주요 이점

이점	설명
위협 탐지	프락시 기록을 수집한 후 플로우 기록과 연결하여 각 플로우에 대한 사용자 애플리케이션 및 URL 정보를 제공함으로써 상황 인식을 높입니다. 이 프로세스에서는 조직에서 위협을 파악하고 MTTK(Mean Time to Know)를 단축할 수 있도록 역량을 강화합니다.
플로우 트래픽 모니터링	의심스러운 네트워크 행동을 파악할 수 있도록 수백 개 네트워크 세그먼트를 통해 플로우 트래픽을 동시에 모니터링합니다. 이 기능은 엔터프라이즈 레벨에 특히 유용합니다.
확장된 데이터 보존	조직과 기관에서 많은 양의 데이터를 장기적으로 보관할 수 있습니다.
확장성	초고속 환경에서도 잘 작동하며 크기에 상관없이 IP 연결이 가능한 네트워크의 모든 부분을 보호할 수 있습니다.
중복 제거 및 스티칭	둘 이상의 라우터를 통과하는 플로우를 한 번만 계산하도록 중복을 제거합니다. 그런 다음 플로우 정보를 결합하여 네트워크 트랜잭션에 대한 전체 가시성을 제공합니다.
전달 방법 선택	모든 규모의 조직에 적합한 확장형 디바이스인 Appliance Edition을 주문할 수 있습니다. 또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 또는 KVM Hypervisor 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다. 이 솔루션은 할당된 리소스에 따라 동적으로 확장됩니다.

플로우 컬렉터 사양

- Secure Network Analytics 플로우 컬렉터 4210 — 부품 번호: ST-FC4210-K9
- Secure Network Analytics 플로우 컬렉터 5210 — 부품 번호: ST-FC5210-K9
- Secure Network Analytics 플로우 컬렉터 4300 — 부품 번호: ST-FC4300-K9
- Secure Network Analytics 플로우 컬렉터 Virtual Edition - 부품 번호: L-ST-FC-VE-K9

데이터 저장소

데이터 저장소는 하나 이상의 플로우 컬렉터의 용량을 초과할 정도로 높은 데이터 수집 용량 레벨 또는 장기 보존 시간이 필요한 환경을 위한 솔루션을 제공합니다. 데이터 저장소 클러스터는 Secure Network Analytics Manager와 플로우 컬렉터 사이에 추가할 수 있습니다. 이처럼 크고 방대한 네트워크의 경우 하나 이상의 플로우 컬렉터가 플로우 데이터를 수집 및 중복 제거하고, 분석을 수행한 다음, 플로우 데이터와 그 결과를 데이터 저장소로 직접 전송합니다. 그런 다음 이 플로우 데이터는 최소 3개의 데이터 노드 어플라이언스로 구성된 데이터 저장소에 동일하게 배포됩니다. 데이터 저장소는 분산형 모델의 여러 플로우 컬렉터에 분산시키는 것과 달리 플로우 데이터 저장을 용이하게 하며, 모든 네트워크 텔레메트리를 하나의 중앙 집중식 위치에 보관합니다. 이 새로운 중앙 집중식 모델은 분산형 모델에 비해 더 큰 스토리지 용량, 흐름 속도 수집 및 향상된 복원력을 제공합니다.

표 3. 데이터 저장소의 주요 이점

이점	설명
데이터 수집 용량 증가	데이터 저장소를 결합하여 단일 데이터 노드 클러스터를 만들 수 있습니다. 이는 3백만 FPS(초당 플로우)를 모니터링하는 데 도움이 됩니다. 이는 플로우 볼륨이 많은 조직의 수집 대역폭 문제를 완화하는 데 도움이 됩니다.
엔터프라이즈급 데이터 복원력	텔레메트리 데이터는 단일 노드 장애 시 원활한 데이터 가용성을 허용하기 위해 노드 전체에 이중 저장되므로, 텔레메트리 데이터 손실을 방지하는 데 도움이 됩니다. 데이터 저장소가 두 개 이상인 구축에서는 데이터 노드 손실의 최대 50%를 지원하면서 계속 작동할 수 있습니다.* 데이터 저장소는 이중 상호 연결 스위치를 지원하여 네트워크 업그레이드 및 예기치 않은 중단에서도 완벽하게 작동합니다. * 하드웨어 구성 및 설치에 따라 다릅니다.
쿼리 및 보고 응답 시간의 상당한 개선	데이터 저장소는 다른 표준 구축 모델이 제공하는 것보다 10배 이상 빠른 쿼리 성능 및 보고 응답 시간을 제공합니다. 또한 API 또는 Secure Network Analytics Manager 웹 UI를 통해 더욱 많은 동시 쿼리를 수행할 수 있습니다. 이러한 쿼리 개선으로 운영 효율성이 크게 향상됩니다. 데이터 저장소를 사용하면 보고서를 실행하고 더 빠르게 답변을 얻을 수 있으므로 위협을 더욱 빠르게 파악하고 대응하여 분류, 조사 및 치료 워크플로를 신속하게 처리할 수 있습니다.
스토리지 확장성	데이터 저장소는 네트워크가 성장 중인 조직에 추가 데이터베이스 클러스터를 추가하는 기능을 통해 데이터 스토리지 확장성에 대한 향상된 유연성을 제공합니다.
장기간 데이터 보존	확장 가능한 장기 텔레메트리 스토리지 기능을 통해 플로우 컬렉터를 추가하지 않고도 최대 1~2년치 데이터의 장기 플로우 보존이 가능합니다. 이는 규정 요구 사항을 충족하고, 서드파티 스토리지 솔루션 또는 추가 플로우 컬렉터의 구매 및 통합과 관련된 비용 및 복잡성을 줄이는 데 도움이 됩니다.

데이터 저장소 사양

- Cisco Secure Network Analytics 데이터 저장소 6200 — 부품 번호: ST-DS6200-K9
- Cisco Secure Network Analytics 데이터 저장소 6300 — 부품 번호: ST-DN6300-K9
- Cisco Secure Network Analytics 가상 데이터 저장소 - 부품 번호: L-ST-DS-VE-K9

자세한 내용은 Secure Network Analytics 데이터 저장소 솔루션 개요를 참조하십시오.

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,
The Netherlands

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 https://www.cisco.com/go/offices에서 확인하십시오.

인쇄지: 미국 06/23