네트워크 가시성 및 보안 분석으로 보안 위협에 대한 방어를 강화하는 Cisco Stealthwatch

이점

- 내부 위협과 외부 위협을 모두 탐지할 수 있도록 클라이언트 간, 서버 간, 클라이언트-서버 간 트래픽을 비롯한 모든 네트워크 상호작용에 대한 가시성 확보
- 공격을 의미할 수 있는 다양한 이례적인 행동을 탐지할 수 있도록 첨단 보안 분석을 실시하고 심층적인 상황 정보 확보
- 기업 리스크를 감소할 수 있도록 네트워크 전반에서 위협 탐지, 사고 대응, 포렌식 가속화 및 개선
- 네트워크 활동에 대한 감사 기록을 통해 더욱 심층적인 포렌식 조사 지원
- 네트워크 전반의 가시성을 확장하여 컴플라이언스, 네트워크 분할, 성능 모니터링 및 용량 계획 간소화

내부 네트워크와 분산형 네트워크에서 포괄적인 네트워크 가시성을 찾고 있다면, 이제 더 알아볼 필요가 없습니다. Cisco Stealthwatch™ System은 정교한 행동 분석을 사용하여 데이터를 실행 가능한 인텔리전스로 바꿔줍니다. 이제 보안을 강화하는 동시에 사고에 신속하게 대응할 수 있습니다.

오늘날 엔터프라이즈 네트워크는 그 어느 때보다도 더 복잡하고 분산되어 있습니다. 매주 새로운 보안 당면 과제가 발생합니다. 지속적으로 발전하는 위협 환경과 클라우드 컴퓨팅, IoT(Internet of Things) 등과 같은 트렌드로 인해 상황은 더욱 복잡해지고 있습니다. 안타깝게도, 점점 더 많은 사용자와 디바이스가 네트워크에 추가되면서 네트워크에 일어나는 일을 파악하는 것이 더욱 어려워졌습니다. 또한 보이지 않는 것을 보호할 수는 없습니다.

Cisco Stealthwatch는 가장 동적이며 초대형 네트워크에도 종합적인 내부 가시성과 보호를 제공할 수 있도록 대량의 데이터를 수집 및 분석합니다. 보안 운영 팀이 위협에 신속하고 효과적으로 대응할 수 있도록 확장 네트워크에서 모든 사용자, 디바이스 및 트래픽에 대한 실시간 상황을 인식하도록 도와줍니다.

지속적인 모니터링 및 인텔리전스를 활용하면 다양한 공격을 탐지할 수 있습니다. 제로 데이 악성코드, 내부자 위협, APT(Advanced Persistent Threat), DDoS(Distributed Denial-of-Service) 공격 및 여타 공격으로 인해 네트워크가 대혼란에 빠지기 전에 이와 관련된 행동을 탐지할 수 있습니다. 다른 보안 모니터링 솔루션과 달리 StealthWatch에서는 네트워크를 오고 가는 트래픽뿐만 아니라 네트워크 악용 및 내부자 위협을 파악할 수 있도록 네트워크 내에서 수평으로 이동하는 이스트 웨스트 트래픽(east west traffic)도 모니터링합니다.

더 많은 공격, 줄어든 가시성

오늘날 공격 표면은 그 어느 때보다 크고 복잡합니다. 네트워크는 도처에 있고 기업들은 끊임없이 새로운 기업을 인수하고 새로운 지역으로 뻗어나가며 지점을 열고 있습니다. 사용자는 장소에 구애받지 않고 각자의 스마트 디바이스로 네트워크에 접속할 수 있습니다. 기업의 앱, 서버, 데이터가 클라우드에 있습니다. 네트워크가 계속 확장되면 네트워크의 현재 상황을 파악하는 가시성을 확보하기가 더욱 힘들어집니다.

뿐만 아니라 공격자는 그 어느 때보다 정교하고 민첩하며 조직화되었으므로 가시성을 확보하여 네트워크에서 의심스러운 행동이 발생하는 위치를 파악하는 것은 공격을 방어하는 데 매우 중요합니다. 보안에서는 가시성 확보가 이해의 출발입니다.

더 효과적인 보안을 구현하려면 네트워크 전반의 상황을 이해할 수 있도록 가시성을 확보하는 것이 필요합니다. 가시성 부재는 네트워크 진단 및 컴플라이언스 검증 능력을 제한합니다. 그리고 네트워크 내외 위협으로부터 네트워크 내부를 보호하는 데 복잡성이 가중됩니다. 네트워크에 대한 가시성은 복잡한 엔터프라이즈 보안에 매우 중요합니다. 이상 행동이 발생하는지 여부를 확인하려면 알려지거나 알려지지 않은 트래픽 흐름, 애플리케이션, 사용자, 디바이스를 확인해야 합니다.

Cisco Stealthwatch는 네트워크 전반에서 네트워크 가시성, 보안, 대응력을 획기적으로 향상시킵니다. 보안 운영팀이 위협에 신속하고 효과적으로 대응할 수 있도록 확장 네트워크, 데이터 센터, 클라우드에서 모든 사용자, 디바이스 및 트래픽에 대한 실시간 상황을 파악하도록 도와줍니다.

아키텍처 및 구성 요소

Flow Collector, Flow Sensor, Management Console은 Cisco Stealthwatch 시스템에서 네트워크 전반의 가시성을 제공하는 데 필요한 핵심 요소입니다. 이 요소는 물리적 또는 가상 어플라이언스의 형태로 해당 라이선스와 함께 제공할 수 있습니다.

Flow Collector는 네트워크 디바이스 및 메커니즘의 텔레메트리를 수집합니다. 여기에는 Cisco NBAR(Network Based Application Recognition), NSEL(NetFlow Security Event Logging), NetFlow, syslog 등이 포함됩니다. 데이터가 수집, 분석, 저장됩니다. 하나 이상의 컬렉터가 필요하며 하나의 구축에서 최대 25개의 Flow Collector를 지원할 수 있습니다.

Flow Sensor는 디바이스가 기본적으로 NetFlow를 지원하지 않는 네트워크 영역에서 유용합니다. Flow Sensor는 비즈니스 크리티컬, 피어 투 피어, 소셜 미디어, 모바일 애플리케이션으로부터 애플리케이션 정보 및 패킷 레벨의 성능 통계를 수집합니다. Flow Sensor가 수집하는 플로우 기록에 URL 정보도 있습니다. 트래픽 데이터를 Flow Sensor에 보내면 여기서 Flow Collector에 보냅니다.

Flow Collector의 이 모든 정보는 중심점인 Management Console로 취합됩니다. 수집된 모든 데이터를 시각적으로 나타내는 데 하나의 콘솔만 있으면 됩니다.

> "회사에 들어서면 지금까지의 상황 또는 현재 상황을 기본적으로 이해하고 있음을 확신합니다. Stealthwatch가 항상 함께하니까요. Stealthwatch는 우리 팀의 가장 큰 자산입니다. 아무도 주목하지 않을 때도 Stealthwatch는 눈에 띄지 않는 곳에서 항상 주시하고 있습니다."
>
> **— Phil Agcaoili, CISO, Elavon**

지속적인 네트워크 모니터링

규모나 업종과는 상관없이 모든 기업에서는 네트워크에서 일어나는 모든 것을 심층 모니터링하면서 신속하게 해당 환경의 정상 행동 기준을 정할 수 있습니다. 이렇게 이해한 기준으로 의심스러운 행동을 손쉽게 식별할 수 있습니다. 액세스 컨트롤과 보호를 개선하도록 중요 네트워크 자산을 식별하고 적절하게 세분화할 수 있습니다.

사후 포렌식

Cisco Stealthwatch 시스템은 실시간 위협 탐지를 개선하는 데 머무르지 않습니다. 사고 대응 시간을 대폭 단축하며, 대개 트러블슈팅 시간을 며칠 또는 몇 달에서 몇 분으로 줄여 줍니다. 네트워크 데이터를 몇 개월 또는 몇 년 동안 저장할 수 있기 때문에 모든 네트워크 활동에 대한 중요한 감사 흔적을 제공하므로, 사고 후 심층적 포렌식 조사를 수행하는 데 핵심적인 역할을 합니다.

Cisco Stealthwatch는 네트워크 트래픽에 대한 포괄적인 가시성을 제공할 뿐 아니라 추가적인 보안 상황도 제공합니다. 여기에는 사용자 및 디바이스 인식, 클라우드 가시성, 애플리케이션 인식 및 위협 피드 데이터가 포함됩니다.

Cisco Stealthwatch와 기타 보안 기술의 비교

Cisco Stealthwatch에서는 기존 라우터, 스위치 및 방화벽을 통한 플로우(NetFlow sFlow, JFlow 등)와 같은 네트워크 텔레메트리를 수집 및 분석하여 네트워크 및 사용자 행동을 모니터링합니다. StealthWatch에서는 공격을 의미할 수 있는 비정상적인 행동을 자동으로 탐지하도록 네트워크 데이터에 대해 정교한 독점 분석을 진행합니다.

Cisco Stealthwatch는 종종 SIEM이나 풀 패킷 캡처와 같은 여타 모니터링 솔루션과 비교되곤 합니다. SIEM 기술은 네트워크 자산으로부터 시스템 로그를 추적하여 시그니처 기반 툴에서 경보 및 알림을 발생시킵니다. 하지만 불행히도 공격당한 시스템에서 시작된 시스템 로그는 신뢰할 수 없으며, 시그니처 기반 모니터링 툴은 액세스 권한이 있는 사항만 확인할 수 있기 때문에 행동 변화를 놓칠 수밖에 없습니다.

한편 풀 패킷 캡처는 비싼 비용과 복잡성 때문에 네트워크의 제한적인 영역에만 구축할 수 있습니다. 종합적인 행동 기반 모니터링으로 이러한 정보 소스를 보완하는 것은 위험한 보안 틈새를 없애는 데 매우 중요합니다. 또한 Cisco Stealthwatch는 Cisco® Security Packet Analyzer와 함께 사용하면서 Cisco Stealthwatch 알람에서 생성되는 이례적인 트래픽 플로우와 관련된 패킷을 캡처하고 조사할 수도 있습니다.

Cisco Stealthwatch는 확장성이 뛰어나기 때문에 그 기능이 경쟁사의 보안 기술(여타 플로우 기반 모니터링 툴 포함)을 능가합니다. 단방향 플로우 기록을 중복 제거하고 결합할 수 있는 능력을 갖추고 있으므로 규모가 크고 매우 복잡한 엔터프라이즈 네트워크에서도 비용 효율적인 플로우 모니터링과 저장이 가능합니다.

> "[Stealthwatch로] 저희 글로벌 엔터프라이즈 네트워크 전반에서 향상된 가시성을 얻게 되었습니다. 실시간에 가까운 데이터 보고 및 경보 기능을 통해 저희 팀은 보안 사고가 발생하자마자 신속하게 탐지하고 대응할 수 있게 되었습니다."
>
> **— Jeff DeLong, 정보 보안 설계자, Westinghouse Electric Company**

구성 요소

Cisco Stealthwatch 시스템은 맞춤 설정할 수 있으나 그 핵심 구성 요소는 Flow Collector, Flow Sensor, Management Console입니다. 앞서 설명한 것처럼 적합한 라이선스와 함께 물리적 또는 가상 어플라이언스로 제공됩니다. 해당 구성 요소들은 다음과 같은 방식으로 함께 작동합니다.

- Flow Collector는 기존 인프라의 NetFlow, IPFIX 및 기타 텔레메트리 데이터를 사용합니다.

  이를 통해 엔터프라이즈 네트워크 전반에 비용 효율적인 엔드 투 엔드 가시성이 제공됩니다.
- Management Console은 전사에 걸친 실시간 보안 및 네트워크 인텔리전스의 연관성을 볼 수 있도록 모든 Cisco StealthWatch 제품을 관리, 조정하고 환경을 설정합니다.
- Flow Sensor는 네트워크에서 사용 중인 애플리케이션과 프로토콜을 식별하기 위해 DPI(Deep Packet Inspection)와 행동 분석을 조합하여 사용합니다. 이는 또한 NetFlow가 지원되지 않는 네트워크 영역에서 쓰입니다.
- UDP Director는 여러 위치에서 핵심적인 네트워크 및 보안 정보를 수신하는 고속, 고성능 어플라이언스입니다. 수신한 정보를 하나의 데이터 스트림으로 Flow Collector와 같은 하나 이상의 대상에 전달합니다.
- Threat Intelligence License는 글로벌 위협 정보를 제공합니다. 의심스러운 커뮤니케이션을 경고할 수 있도록 이벤트의 Concern Index와 경보를 생성하여 이 신속하게 조사할 수 있도록 합니다.
- Proxy License는 프록시 기록을 주입하고 이를 플로우 기록에 연결합니다. 각 플로우의 원래 사용자, 애플리케이션 및 URL 정보를 전송하여 웹 프록시를 통과하는 네트워크 상호작용을 모니터링할 수 있습니다.
- 엔드포인트 솔루션 구성 요소로는 Endpoint License와 Endpoint Concentrator가 있습니다. Endpoint Concentrator는 Cisco AnyConnect® Visibility Module로부터 IPFIX 데이터를 수집합니다. 모든 엔드포인트 디바이스에서 데이터를 수집하여 Endpoint Concentrator를 거쳐 Flow Collector에 전달하면 Management Console에서 분석된 엔드포인트 데이터에 대한 가시성을 제공합니다.
- Cloud License는 Cisco Stealthwatch 시스템에 대한 가상 라이선스 애드온입니다. Cloud License는 네트워크를 센서로 클라우드까지 확장하여, 사용자가 Management Console 내에서 가상 인스턴스의 플로우를 파악할 수 있도록 합니다.

- Cisco Stealthwatch Learning Network License는 Cisco IS(Integrated Services Router)을 보안 센서로 사용하면서 특정 브랜치 라우터의 트래픽 플로우에 대한 심층 가시성을 확보합니다. 또한 머신 러닝 기반의 행동 분석을 수행하고 패킷을 수집하며 브랜치 레벨에서 즉시 위협을 탐지합니다.

활용 사례

모든 업계	• 확장된 네트워크를 지속적으로 모니터링 • 실시간 위협 탐지 • 사고 대응 및 포렌식 시간 단축 • 네트워크 세그멘테이션 간소화 • 컴플라이언스 요건 충족 • 네트워크 성능 및 용량 계획 개선
유통	• 보안 및 성능 문제 파악을 위해 수백 개의 원격 시스템 모니터링 • POS(point-of-sale) 단말기 보호 • PCI 컴플라이언스 유지
의료	• 환자 기록 보호 • 인명 구조용 의료 장비에 대한 사이버 공격 차단 • HIPAA 컴플라이언스 유지 • 지적 재산 보호 • 높은 레벨의 성능 유지 • 새로운 네트워크 디바이스를 신속한 발견하고 보호
금융 서비스	• 외부자 및 내부자 위협 탐지 • 고객 데이터 보호 • 엄격한 컴플라이언스 요건 충족 • 중요한 금융 정보에 대한 24시간 액세스 유지 • 위협 및 성능 문제 발생 전에 해결 방안 모색 및 적용
정부 기관	• 지능형 공격이 존재하는지 네트워크를 지속적으로 모니터링 • 기밀 정보 보호 • 엄격한 보안 규제로 컴플라이언스 유지 • 내부자 위협 탐지
교육 강화	• 모바일 디바이스 보호 • P2P 파일 공유 탐지 • 민감한 정보 보호 • 네트워크 악용 및 오용 방지 • 높은 레벨의 가용성 및 성능 유지 • 보안 워크플로 간소화 • 컴플라이언스 요구 사항 충족

Cisco를 선택해야 하는 이유

NetFlow를 발명한 Cisco는 네트워크 가시성에 플로우 데이터를 사용하는 보안 솔루션을 제공하는 유일한 입지를 갖추고 있습니다. 2000년부터 Lancope는 StealthWatch를 사용하여 깊이 있는 네트워크와 보안 인사이트를 확보하는 데 텔레메트리 데이터를 처음으로 사용하기 시작했습니다. StealthWatch는 NetFlow, IPFIX, 기타 네트워크 텔레메트리 데이터 유형을 수집하고 분석하여 네트워크를 상시 가동하는 가상 센서가 되게 하고 전 세계 수백 개 기업의 보안 상태를 개선할 수 있도록 정교한 행동 분석 기법을 적용하여 다양한 공격을 신속하게 탐지합니다. 이제 Cisco StealthWatch는 필적할 만한 이 두 가지 기술 개발 노력의 최고 결과물을 선사하고자 합니다.

간편하고 전문적으로 StealthWatch 구축

공인 전문 서비스 기관과 인증 파트너들이 수년간에 걸친 Cisco StealthWatch 제품군의 설계, 구축, 관리 경험을 바탕으로 서비스를 제공합니다. 외부 서비스 팀은 다양한 고객 및 업계 경험을 바탕으로 기업이 구체적인 비즈니스 요건을 충족하고 생산성을 제고하고 위험을 감소할 수 있도록 최적화를 지원합니다. 이들은 오늘날의 지능형 위협 환경의 까다로운 요구를 충족할 수 있도록 전문적인 네트워크 및 보안 기술을 사용하여 Cisco StealthWatch 시스템을 신속하고 효과적으로 구현합니다.

Cisco 전문 서비스에는 초기 설치, 상태 확인 및 튜닝, 호스트 그룹 자동화, 프록시 통합, 시스템 교육은 물론 맞춤형 컨설팅과 통합 서비스가 포함됩니다.

> "[StealthWatch]는 내부 네트워크 가시성을 확보할 수 있도록 해 주며... 특정 트래픽 유형이 네트워크 외부로 유출되지 않도록 보안 영역에 대한 감사를 손쉽게 실행합니다."
>
> **— Ryan Laus, 네트워크 관리자, Central Michigan University**

Cisco Capital

목표 달성을 지원하는 파이낸싱

Cisco Capital® 금융 지원 솔루션을 통해 여러분이 비즈니스 목표를 달성하는 데 필요한 기술을 도입하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 구입 시 Cisco Capital의 금융 지원 솔루션을 유연하게 활용할 수 있습니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기.

다음 단계

자세한 내용은 http://www.cisco.com/go/stealthwatch를 참조하거나 현지 Cisco 어카운트 담당자에게 문의하십시오.

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.

인쇄지: 미국

C22-736505-01 03/17