종합적인 가시성 및 보안으로 위협 방어를 개선하는 StealthWatch

혜택

- 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 이상 징후를 탐지 할 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 규정준수, 네트워크 분할, 성능 모니터링 및 용량 계획 간소화

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

오늘날 엔터프라이즈 네트워크는 그 어느 때보다도 더 복잡하고 분산되어 있습니다. 새로운 보안 문제가 매주 발생합니다. 지속적으로 발전하는 위협 환경과 더불어 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.

StealthWatch는 이러한 문제를 덜어드립니다. StealthWatch는 가장 동적이며 초대형 네트워크에도 종합적인 내부 가시성과 보호를 제공할 수 있도록 대량의 데이터를 수집 및 분석합니다. StealthWatch는 보안 운영팀이 위협에 신속하고 효과적으로 대응할 수 있도록 확장 네트워크에서 모든 사용자, 디바이스 및 트래픽에 대한 실시간 상황을 인식하도록 도와줍니다.

StealthWatch의 지속적인 모니터링 및 인텔리전스를 활용하면 다양한 공격을 탐지할 수 있습니다. 제로 데이 악성코드와 내부자 위협, APT(Advanced Persistent Threat), DDoS(Distributed Denial-of-Service) 공격 및 여타 공격으로 인해 네트워크가 대혼란에 빠지기 전에 차단할 수 있습니다. 다른 보안 모니터링 솔루션과 달리 StealthWatch에서는 네트워크를 오고 가는 트래픽뿐만 아니라 네트워크 악용 및 내부자 위협을 파악할 수 있도록 네트워크 내부의 측면, 즉 동서 방향의 트래픽도 모니터링합니다.

더 많은 공격, 줄어든 가시성

오늘날 정부 및 기업은 갈수록 증가하는 사이버 공격의 대홍수에 직면해 있습니다. 안타깝게도 방화벽, 안티바이러스 툴, IPS(Intrusion Prevention System)와 같은 기존의 보안 솔루션이 공격자들의 손으로부터 기밀 데이터를 지켜내기에 역부족이라는 사실은 분명합니다. 네트워크 에지에 수많은 기술을 구축한다 해도 침입자들은 또 다른 공격 방법을 고안해 냅니다. 이들은 제로 데이 공격, 도난한 액세스 자격 증명, 감염된 모바일 디바이스, 취약한 비즈니스 파트너 등의 수단을 사용합니다.

또한 갈수록 많은 공격자들이 더 이상 해킹을 하지 않습니다. 이들은 손쉽게 확보할 수 있는 자격 증명을 사용하여 간단하게 로그인합니다. 교묘하게 조정할 수 있는 직원 한 명만 찾아내면 내부 사용자와 동일한 권한을 갖게 됩니다. 이러한 소셜 엔지니어링 트렌드의 결과, 직원들은 흔히 자신의 의지와 상관없이 내부자 위협이 되곤 합니다. 기업은 경계 보안에 너무 많은 신경을 쓰고 네트워크 내부에 존재하는 공격자를 탐지하는 데 너무 오래 걸리기 때문에 피해를 입게 됩니다.

사이버 전쟁에서 승리를 거두기 위해서는 경계 밖 상황을 파악하는 것뿐만 아니라 네트워크 내부 상황을 제대로 파악할 수 있어야 합니다. 이는 오늘날과 같은 현실에서 더욱 그러합니다. 네트워크 트래픽의 80% 이상이 데이터 센터 내에서 동에서 서로 이동하며 절대 경계를 넘어가지 않습니다. 하지만 안타깝게도 SIEM(Security Information and Event Management) 시스템이나 풀 패킷 캡처와 같은 기존의 보안 기술은 내부 네트워크에 대한 가시성이 제한적입니다. 게다가 이러한 접근 방식은 제한적인 구축 환경 너머로 확장하기 어려운 경우가 많습니다.

StealthWatch 아키텍처 및 구성 요소

StealthWatch의 2-tier 아키텍처는 StealthWatch FlowCollector와 StealthWatch Management Console 어플라이언스로 구성됩니다. 플로우 콜렉션 라이센스와 함께 물리 또는 가상 어플라이언스로 제공됩니다.

StealthWatch FlowSensor는 DPI(Deep Packet Inspection)를 통해 네트워크 및 서버 성능 메트릭에 대한 포괄적인 가시성을 제공합니다. 조직의 네트워크에서 NetFlow가 지원되지 않는 경우, 네트워크 텔레메트리 데이터를 생성하는 어플라이언스로 FlowSensor를 구축합니다. FlowSensor의 텔레메트리 데이터는 FlowCollector로 전송 전송되며, 여기에서 행동 분석을 진행합니다. FlowCollector는 보안, 네트워크 운영 및 애플리케이션 성능 최적화를 위해 애플리케이션과 프로토콜을 식별합니다.

StealthWatch는 FlowCollector를 사용하여 초당 최대 240,000개의 플로우 유지 속도로 최대 4,000개의 텔레메트리 데이터 소스를 저장 및 분석합니다. 동일한 네트워크에 초당 최대 6백만 플로우의 속도로 최대 25개의 FlowCollector가 집계될 수 있습니다.

> "StealthWatch 는 문제 해결 시간을 며칠에서 몇 초로 단축합니다. StealthWatch 를 사용하면 잠재적인 공격과 보안 침해에 앞서 대응할 수 있습니다"
> **— Edge Web Hosting**

주요 기능

StealthWatch는 전체 엔터프라이즈 네트워크에 진정으로 포괄적인 가시성과 보안 인텔리전스를 제공하는 데 기존의 인프라 투자를 활용합니다.

지속적인 네트워크 모니터링

네트워크 전반에서 일어나는 모든 상황에 대한 심층적인 인사이트를 사용하여 크고 작은 각양각색의 조직에서는 사내 환경의 정상적인 행동에 대한 기준을 도출할 수 있습니다. 이렇게 이해한 기준으로 의심스러운 행동을 손쉽게 식별할 수 있습니다. 조직에서는 액세스 컨트롤과 보호를 개선하도록 중요 네트워크 자산을 식별하고 적절하게 나눌 수 있습니다.

초기 위협 탐지

StealthWatch에서는 이상 행동을 자동으로 탐지할 수 있도록 상황 인식 보안 분석을 적용합니다. StealthWatch에서는 악성코드, 제로 데이 공격, DDoS, APT, 내부자 위협을 비롯한 다양한 공격을 식별할 수 있습니다. StealthWatch에서는 다른 보안 모니터링 솔루션과 달리 네트워크를 오고 가는 트래픽뿐만 아니라 측면(동서) 트래픽도 모니터링합니다. 이를 통해, 네트워크 악용 및 오용은 물론 네트워크 내부에서 활동 중인 공격자를 찾아냅니다.

보안 사고 후 포렌식

StealthWatch는 실시간 위협 탐지 기능을 개선할 뿐 아니라 사고 대응 시간을 대폭 단축하며, 많은 경우 트러블슈팅 시간을 며칠 또는 몇 달에서 몇 분으로 줄여 줍니다. StealthWatch는 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.

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

StealthWatch와 기타 보안 기술의 비교

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

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.

확장성이 뛰어나기 때문에 StealthWatch의 기능은 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.

"Lancope 솔루션으로 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, Westinghouse Electric Company, LLC 정보 보안 설계자

StealthWatch 구성 요소

StealthWatch는 맞춤형 구성이 가능하나 핵심 구성요소는 FlowCollector와 Management Console입니다. 앞에서 언급한 바와 같이 이는 물리 또는 가상 어플라이언스로 제공됩니다. 해당 구성 요소들은 다음과 같은 방식으로 함께 작동합니다.

- FlowCollector는 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 StealthWatch 제품을 관리, 조정하고 환경을 설정합니다.
- FlowSensor는 네트워크에서 사용 중인 애플리케이션과 프로토콜을 식별하기 위해 DPI와 행동 분석을 조합하여 사용합니다.
- UDP Director는 여러 위치에서 핵심적인 네트워크 및 보안 정보를 수신하는 고속, 고성능 어플라이언스입니다. UDP Director는 수신한 정보를 하나의 데이터 스트림으로 FlowCollector와 같은 하나 이상의 목적지로 전달합니다.
- SLIC(StealthWatch Labs Intelligence Center) Threat Feed는 글로벌 위협 인텔리전스를 활용합니다. 의심스러운 커뮤니케이션을 경고할 수 있도록 이벤트의 Concern Index와 경보를 생성하여 이 신속하게 조사할 수 있도록 합니다.
- ProxyWatch는 프록시 기록을 주입하고 이를 플로우 기록에 연결합니다. 각 플로우의 원래 사용자, 애플리케이션 및 URL 정보를 전송하여 웹 프록시를 통과하는 네트워크 상호작용을 모니터링할 수 있습니다.

활용 사례

모든 업계	• 확장된 네트워크를 지속적으로 모니터링 • 실시간 위협 탐지 • 사고 대응 및 포렌식 시간 단축 • 네트워크 세그멘테이션 간소화 • 규정 준수 요건 충족 • 네트워크 성능 및 용량 계획 개선
유통	• 보안 및 성능 문제 파악을 위해 원격으로 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 규정준수 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 규정준수 유지 • 내부자 위협 탐지
고등 교육	• 모바일 디바이스 보호 • P2P 파일 공유 탐지 • 민감한 정보 보호 • 네트워크 악용 및 오용 방지 • 높은 레벨의 가용성 및 성능 유지 • 보안 워크플로 간소화 • 규정준수 요구 사항 충족

왜 시스코를 선택해야 할까요?

NetFlow를 발명한 Cisco는 네트워크 가시성에 플로우 데이터를 사용하는 보안 솔루션을 제공하는 유일한 입지를 갖추고 있습니다. 2000년부터 Lancope는 StealthWatch를 사용하여 깊이 있는 네트워크와 보안 인사이트 확보하는 데 텔레메트리 데이터를 처음으로 사용하기 시작했습니다. StealthWatch는 NetFlow, IPFIX 및 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 제품으로 편입된 StealthWatch는 같은 종류의 두 가지 기술 개발 노력의 최고 정점을 제공합니다.

간편하고 전문적으로 StealthWatch 구축

공인 전문 서비스 기관과 인증 파트너들이 수년간에 걸친 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 StealthWatch 최적화를 지원합니다. 이들은 오늘날의 지능형 위협 환경의 까다로운 요구를 충족할 수 있도록 전문적인 네트워크 및 보안 기술을 사용하여 StealthWatch를 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, Central Michigan University 네트워크 관리자

Cisco Capital

목표 달성을 지원하는 파이낸싱

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 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기.

다음 단계

StealthWatch에 대한 자세한 내용을 알아보려면 http://www.cisco.com/go/stealthwatch 를 방문하거나 현지 Cisco 어카운트 담당자에게 문의하시기 바랍니다.

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 C22-736505-00 01/16