Cisco Stealthwatch System

이점

- **가시성 확보** 내부 위협과 외부 위협을 모두 탐지할 수 있도록 클라이언트 간, 서버 간, 클라이언트-서버 간 트래픽을 비롯한 모든 네트워크 상호작용에 대한 가시성 확보
- **첨단 보안 분석 수행** 공격을 의미할 수 있는 다양한 이례적인 움직임을 탐지 할 수 있도록 첨단 보안 분석을 실시하고 심층적인 상황 정보 확보
- **위협 탐지 가속화 및 개선** 전체 네트워크에서 위협 탐지, 사고 대응, 포렌식 가속화 및 개선
- **심층 포렌식 조사 지원** 네트워크 활동에 대한 감사 기록을 통해 더욱 심층적인 포렌식 조사 지원
- **컴플라이언스 간소화** 컴플라이언스, 네트워크 분할, 성능 모니터링, 용량 계획 간소화

네트워크 전 범위로 가시성을 확대하여 더 효과적인 보안 분석 및 위협 탐지 지원

오늘날 엔터프라이즈 네트워크는 그 어느 때보다도 더 복잡하고 분산되어 있습니다. 매일은 아니더라도 매주 새로운 보안 과제가 등장합니다. 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.

네트워크에서 이례적인 움직임이 발생하는지 여부를 확인하려면 알려지거나 알려지지 않은 모든 트래픽 플로우, 애플리케이션, 사용자 및 디바이스를 들여다봐야 합니다. 정교한 행동 분석 기술을 사용하는 Cisco Stealthwatch 시스템은 기존 인프라의 데이터를 실행 가능한 인텔리전스로 전환합니다. 더 우수한 네트워크 가시성 및 보안 분석으로 신속하게 사고에 대응할 수 있습니다.

사고 대응 및 포렌식 가속화를 위한 지속적인 네트워크 트래픽 분석

Cisco Stealthwatch 시스템은 중단 없이 실시간으로 모든 네트워크 트래픽을 모니터링하고 포괄적으로 조명합니다. 네트워크 전반의 의심스러운 사고에 대한 가시성, 보안 및 대응 시간을 획기적으로 개선합니다.

보안 운영 팀은 모든 사용자, 디바이스, 트래픽을 대상으로 현재 상황을 실시간으로 파악함으로써 보안 사고 전/중/후에 빠르고 효과적으로 위협에 대응할 수 있습니다.

Cisco Stealthwatch 시스템은 상황 인식 분석을 적용하여 비정상적인 행동을 자동으로 탐지합니다. 악성코드, 제로 데이 공격, DDoS(Distributed Denial-of-Service) 공격, APT(Advanced Persistent Threat), 내부자 위협을 비롯한 다양한 공격을 식별할 수 있습니다.

클라우드로 가시성 확대

워크로드를 오프프레미스와 클라우드 환경으로 이동하는 추세가 두드러지고 있습니다. 이를 통해 조직에는 유연성이 확대되지만, 이러한 가상 인스턴스 내에서 트래픽 플로우를 보는 기능이 저해되기도 합니다. 그러나 Stealthwatch Cloud License가 있으면 퍼블릭, 프라이빗 및 하이브리드 클라우드 환경에서 Cisco Stealthwatch의 모든 네트워크 가시성, 위협 탐지 및 분석 기능을 이용할 수 있습니다. Stealthwatch Cloud License는 Cisco Stealthwatch에 대한 가상 라이선스 애드온이며 센서로서의 네트워크를 클라우드로 확장합니다. 인프라 전 범위에서 실시간으로 상황을 인식하고 더 강력한 보안을 제공할 수 있습니다.

이 라이선스는 클라우드 컴퓨팅 서비스인 AWS(Amazon Web Services)에도 설치가 가능합니다. 현재 다음과 같은 호스트 운영 체제를 지원합니다.

- Linux
- CentOS 5, 6, 7(x64 전용)
- Red Hat Enterprise Linux 5, 6, 7(x64 전용)

엔드포인트로 가시성 확대

커넥티드 세상에서는 이동성이 무엇보다 중요합니다. 그러나 모든 네트워크 활동을 제대로 모니터링하려면 보안 팀은 네트워크 에지에서 실행되는 애플리케이션 및 프로세스를 원격 디바이스까지 포괄하는 범위에서 볼 수 있어야 합니다. Cisco Stealthwatch 엔드포인트 솔루션으로 의심스러운 행동을 나타내는 사용자 시스템을 풍부한 상황 정보에 기초하여 더 효율적으로 조사할 수 있습니다.

Cisco AnyConnect® Network Visibility Module과의 강력한 통합을 지원하는 Stealthwatch Endpoint License는 네트워크 가시성을 제공할 뿐 아니라 엔드포인트에 대한 조사를 확장합니다. 보안 분석가는 엔드포인트 애플리케이션 및 필요한 정보에 손쉽게 액세스하여 더 신속하게 사고에 대응하고 정책 위반을 처리할 수 있습니다.

엔드포인트 솔루션 구성 요소

- **StealthwatchEndpoint License:** Stealthwatch 콘솔에서 분석된 엔드포인트 데이터에 대한 가시성을 제공합니다.
- **Stealthwatch Endpoint Concentrator:** Cisco AnyConnect Visibility Module로부터 IPFIX 데이터를 수집합니다. 모든 엔드포인트 디바이스로부터 데이터를 수집하고 Endpoint Concentrator를 거쳐 StealthwatchFlow Collector로 전달합니다.

프록시 서버 전 범위로 가시성 확대

보안을 강화하고 웹 정책을 적용하기 위해 프록시 서버를 사용하는 곳이 많습니다. 이는 해당 기업에게 유익하지만 가시성을 저해하고 공격자에게 은거지를 제공할 수도 있습니다. Cisco Stealthwatch 솔루션은 프록시 로그를 사용하고 이를 플로우 레코드에 통합하는 방법으로 그 허점을 해결합니다. Proxy License는 프록시의 반대편으로부터 해당 통신에 대한 추가 상황 정보를 수집합니다. 프록시 로그를 통합하고 이를 사용자, 애플리케이션, RUL 데이터가 보존되는 적합한 흐름과 연계함으로써 프록시 서버가 방해 요인이 아닌 유용한 보안 장치로 바뀝니다. 트래픽 모니터링이 프록시 전반에 유지되어 조사 시간이 단축될 뿐 아니라 Stealthwatch 분석 엔진에도 정보를 제공하므로 보안 운영 팀이 더 빠르고 정확하게 위협 활동을 파악할 수 있습니다.

Proxy License 기능에서 지원하는 웹 프록시는 다음과 같습니다.

- Cisco® Web Security Appliance
- Blue Coat
- McAfee
- Squid

브랜치 환경으로 가시성 확대

네트워크를 보호하려면 브랜치 전반의 트래픽뿐 아니라 브랜치 간의 트래픽까지 모니터링하는 것이 중요합니다. Cisco Stealthwatch Learning Network License는 Cisco ISR(Integrated Services Router)을 보안 센서로 사용하여 특정 브랜치 라우터의 트래픽 플로우를 면밀하게 모니터링합니다. 또한 머신 러닝 기반의 행동 분석을 수행하고 패킷을 수집하며 로컬의 브랜치 레벨에서 즉시 위협을 탐지합니다. Learning Network License는 알고리즘 기반의 이상 탐지 솔루션입니다. Cisco Stealthwatch 솔루션은 기록 및 통계를 통해 이상 요인을 탐지합니다. 이러한 솔루션을 함께 사용하면서 브랜치 레벨에서 광범위하고 깊이 있는 가시성을 확보합니다.

Cisco Stealthwatch는 다음 기능을 수행합니다.

- 네트워크 경계, 내부, 데이터 센터, 프라이빗/퍼블릭 클라우드와 엔드포인트까지 포괄하여 면밀하게 모니터링
- 이례적인 행동을 정확하게 찾아낼 수 있는 기준을 설정하도록 NetFlow를 사용하여 정상적인 움직임을 간편하게 파악
- 분산된 네트워크에서 디바이스, 애플리케이션 및 사용자를 지속적으로 모니터링
- 공격을 의미할 수도 있는 다양한 움직임을 탐지하는 최신 보안 분석 및 인텔리전스
- 실시간 위협 탐지를 통해 더 빨라진 사고 대응 시간
- 포괄적인 네트워크 감사 추적을 통한 탁월한 포렌식 조사
- 네트워크 분할, 컴플라이언스 검증, 트러블슈팅, 진단을 위한 간소화된 기능

"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 백그라운드에서 중단 없이 감시하고 있습니다."

— Phil Agcaoili.
CISO, Elavon

"[Stealthwatch]로 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 아키텍트

"[Stealthwatch]는 네트워크 내에서 실제로 발생하고 있는 일들에 대한 인사이트를 제공하고, 표준 플로우 데이터를 사용하여 보고 이력과 향상된 문제 알림을 최적의 조합으로 결합하는 제품입니다. 뛰어난 지원, 세일즈 및 마케팅, 고객과의 적극적인 협업도 빼놓을 수 없는 최상의 솔루션입니다."

— Steve Mould.
선임 IT 설계자, Experian

Cisco 포트폴리오 전 범위에서의 통합

Cisco Stealthwatch는 Cisco의 "Security Everywhere" 전략을 확장하고 확대된 엔터프라이즈 환경 전 범위에서 네트워크 보안 및 가시성을 지원합니다.

Network as a Sensor 및 Network as an Enforcer 이니셔티브의 핵심 구성 요소인 Cisco Stealthwatch는 NetFlow 데이터를 실행 가능한 인텔리전스로 바꿔 놓습니다. 네트워크를 센서로 활용할 수 있게 합니다. 모든 네트워크 트래픽을 면밀하게 모니터링하면서 잠재적 네트워크 위협을 찾아낼 수 있습니다.

Cisco Stealthwatch와 Cisco Identity Services Engine의 조합으로 360도 전방위적 관점에서 위협에 신속하게 대응하며 성장하는 디지털 비즈니스를 보호할 수 있습니다. 이 두 솔루션을 함께 사용한다면 각 디바이스의 세부 사항, 즉 유형, 운영 체제, 컴플라이언스 상태, 연결 방법, 지리적 위치 등을 확인할 수 있습니다. 해당 환경에서 이상 트래픽을 발견하고 개별 사용자의 행동이 정확히 언제부터 의심스러워졌는지 파악합니다.

이제 Cisco는 NetFlow 분석 및 패킷 분석 기능을 통합하여 제공합니다. 즉 Cisco Stealthwatch 솔루션과 Cisco Security Packet Analyzer를 통합했습니다. 두 기술 유형 모두 보안 및 네트워크 사고의 트러블슈팅을 지원하지만, 대개 예산 문제 또는 리소스 부족 때문에 둘 중 하나만 선택하곤 했습니다. Cisco의 접근 방식은 문제의 패킷만 저장하여 스토리지 비용을 줄이는 한편 네트워크의 상태에 대해 더 세부적인, 상황에 기초한 정보를 제공하는 것입니다. NetFlow가 제공하는 향상된 가시성 및 보안 상황 정보가 더 정밀하고 비용 효과적인 패킷 레벨 데이터 수집 방식과 접목되어 필요한 시점에 특정 문제를 더 심도 있게 조사할 수 있도록 지원합니다.

다음 단계

Cisco Stealthwatch는 아무리 크고 동적인 네트워크에서도 포괄적인 가시성과 보호를 제공하기 위해 대용량의 네트워크 데이터를 수집 및 분석합니다. 자세한 내용은 http://www.cisco.com/go/Stealthwatch를 참조하거나 현지 Cisco 어카운트 담당자에게 문의하십시오.

C45-736510-01 03/17