Cisco Stealthwatch Cloud

퍼블릭 클라우드, 프라이빗 네트워크, 하이브리드 환경을 보호할 수 있는 우수한 가시성과 지속적인 위협 탐지 기능을 확보할 수 있습니다.

제품 개요

Cisco® Stealthwatch Cloud 는 프라이빗 네트워크부터 지사, 퍼블릭 클라우드에 이르는 분산 네트워크 전반의 보안을 강화해 주고 사고 대응 역량을 높여 줍니다. 또한, 이 솔루션은 네트워크 디바이스와 클라우드 리소스에 발생한 위협을 빠르게 식별해 내야 하는 디지털 기업의 요구 사항을 해결하며, 기업의 관리와 감독, 보안 인력도 거의 필요로 하지 않습니다.

네트워크는 날로 진화하고 있습니다. 점차 많은 IT 리소스가 클라우드로 이동하고 있습니다. 이와 동시에 프라이빗 네트워크에 연결된 디바이스 수가 급증하고 있습니다. 보안 요원은 어떤 엔티티가 조직에 위협을 가하는지의 문제는 고사하고 해당 환경 내에서 어떤 엔티티가 동작하고 있는지 파악하는 데에도 어려움을 겪고 있습니다.

Stealthwatch Cloud 는 에이전트를 사용하지 않고도 포괄적인 가시성 및 잡음 없는 고도로 정밀한 경고를 제공하여 이러한 문제를 해결합니다. 따라서 조직은 공격이 네트워크에서 발생하든, 클라우드에서 발생하든 두 환경 모두에서 발생하든 관계없이, 실시간으로 위협을 정확하게 탐지할 수 있습니다. Stealthwatch Cloud 는 클라우드 기반의 SaaS(Software-as-a-service) 배포 솔루션으로, 보안 침해를 나타내는 랜섬웨어 및 기타 악성코드, 데이터 유출, 네트워크 취약점, 역할 변경을 탐지합니다.

기능 및 이점

기능	이점
네트워크 가시성	네트워크 및 퍼블릭 클라우드에서 어떤 디바이스와 리소스가 작동하고 있는지 정확하게 파악할 수 있도록, 디바이스 레벨의 네트워크 트래픽과 통신 패턴을 완전히 자동화된 방식으로 실시간 분석
하이파이(Hi-Fi) 보안 경고	오탐율을 감소시키는 동시에 실행 가능한 인텔리전스를 제공하여 더욱 스마트한 보안 조치 가능
SaaS(Software as a Service)	더 유연하게 사용하고 구축할 수 있어 조직이 효율적으로 대규모 보안 구축
엔티티 모델링	네트워크의 모든 디바이스와 엔티티의 행동 모델을 제공하며, 이를 통해 위협을 나타내는 갑작스러운 행동 변화와 악의적인 활동을 자동으로 식별
자동 역할 분류	행동에 따라 자동으로 각 네트워크 디바이스와 클라우드 리소스의 역할을 식별
에이전트 없는 구축	특정 하드웨어나 소프트웨어 에이전트 필요 없이 네트워크 및 AWS(Amazon Web Services) 클라우드 인스턴스의 텔레메트리와 로그의 네이티브 소스를 사용

첨단 네트워크를 위한 보안

오늘날의 조직은 보안 '사각지대'로 인해 어려움을 겪고 있습니다. 프라이빗 네트워크에 연결되는 디바이스가 폭발적으로 늘어나고 있으며, 더욱 많은 워크로드가 퍼블릭 클라우드로 마이그레이션되고 있습니다. 한편, 보안 실무자는 쇄도하는 보안 경고를 관리할 수 없는 지경에 이르렀습니다. 2017 년 Cisco 연간 사이버 보안 보고서에 따르면 보안 경고의 56%만 조사되었으며, 그중 절반 이상은 해결되지 않은 상태로 남아 있다고 합니다.

공격자는 이러한 상황을 재빠르게 활용하여 네트워크 보안을 침해하고 탐지를 무력화합니다. 조직에게는 네트워크 활동을 확인하고, '정상적인' 엔티티 활동이 무엇인지 파악하며, 위협 징후를 식별할 수 있는 손쉬운 방법이 필요합니다. Stealthwatch Cloud 는 프라이빗 네트워크와 퍼블릭 클라우드의 텔레메트리 및 로그 소스를 기반으로 활동을 모델링하여 위협 활동을 식별함으로써, 조직의 그러한 문제를 해결합니다.

가시성 및 분석

이 텔레메트리는 Stealthwatch Cloud 내에서 처리되어, 프라이빗 네트워크, 지사 및 퍼블릭 클라우드를 포함하는 네트워크 전반의 모든 활성 엔티티에 대해 우수한 가시성을 제공합니다. Stealthwatch Cloud 는 엔티티 모델링을 사용하여 다양한 위협 활동을 아주 정확하게 탐지합니다. 하이파이(Hi-Fi) 보안 경고는 더욱 스마트한 보안 결정을 할 수 있도록 지원하며 오탐 경고의 수를 줄이고 조사에 할애하는 시간을 단축해 줍니다.

유연성 및 사용 용이성

Stealthwatch Cloud 는 SaaS(Software as a service)로 제공되어 사용이 쉽고 간단하게 구매할 수 있고 사용이 용이합니다. 특정 하드웨어를 구매할 필요가 없고 소프트웨어 에이전트도 구축할 필요가 없으며 특별한 전문 지식도 필요하지 않습니다.

Stealthwatch Cloud 에서 데이터를 받는 순간부터 더는 구성 작업이나 디바이스 분류 작업이 필요 없습니다. 또한, 모든 분석이 자동화됩니다. 이러한 기능 덕분에, Stealthwatch Cloud 운영에는 관리 지식이나 보안 지식이 거의 필요하지 않습니다.

첨단 위협 탐지를 위한 엔티티 모델링

텔레메트리가 수집되면, Stealthwatch Cloud 가 네트워크 또는 모니터링되는 퍼블릭 클라우드의 모든 활성 엔티티에 대한 일종의 시뮬레이션 같은 모델을 생성합니다. 이러한 모델링을 바탕으로 초기 단계의 보안 침해나 눈에 띄지 않는 보안 침해 지표를 신속하게 확인할 수 있습니다. 시그니처 목록을 업데이트하거나 소프트웨어 에이전트를 구축할 필요가 없습니다.

각 모델은 엔티티 활동에 대한 5 가지 핵심 요소로 구성됩니다.

- **예측:** 과거 활동을 바탕으로 엔티티 활동을 예측하고 이러한 예측과 관찰된 동작을 비교하여 평가합니다.
- **그룹화:** 해당 활동을 유사한 엔티티의 활동과 비교해 엔티티의 활동이 일관되는지 평가합니다.
- **역할:** 엔티티의 행동을 바탕으로 엔티티의 역할을 확인한 후 해당 역할에 부합되지 않는 활동을 탐지합니다.
- **규칙:** 프로토콜과 포트 사용, 디바이스와 리소스 프로파일 특성 및 블랙리스트에 있는 통신을 포함한 조직의 정책을 엔티티가 위반할 경우 이를 탐지합니다.
- **일관성:** 디바이스가 데이터 전송 및 액세스 특성과 관련하여 과거 행동에서 크게 벗어난 행동을 할 경우 이를 인지합니다.

이러한 모델링을 기반으로 잠재적 위협과 관련된 다양한 행동을 감지할 수 있습니다. 예를 들어, Stealthwatch Cloud 가 프린터를 자동 분류한 이후, 해당 프린터가 네트워크를 스캔하기 시작하고 외부 서버에 대한 하트비트 연결을 설정하는 경우가 있습니다. 전에 없던 이러한 통신 패턴은 프린터 또는 해당 디바이스의 특정 행동 모델과 일치하지 않으므로 보안 침해의 징후일 수 있습니다. Stealthwatch Cloud 는 이 같은 새로운 행동 등을 실시간에 가깝게 감지하고, 의심스러운 트래픽에 대한 상세 정보를 포함한 경고를 생성합니다.

예를 들어, Stealthwatch Cloud 는 DNS 남용, 지리적으로 특이한 원격 액세스, 지속적인 원격 제어 연결, 잠재적인 데이터베이스 유출에 대한 경고를 생성합니다. 또한, 트래픽 통계를 포함해 가장 빈번하게 사용되는 IP, 가장 많이 사용되는 포트, 활성 서브넷 등에 대한 네트워크 보고서를 제공합니다.

두 가지 서비스

Cisco Stealthwatch Cloud 는 두 가지의 기본 서비스인 퍼블릭 클라우드 모니터링 및 프라이빗 네트워크 모니터링으로 구성됩니다.

퍼블릭 클라우드 모니터링

Cisco Stealthwatch Cloud 의 퍼블릭 클라우드 모니터링은 AWS(Amazon Web Services) 및 Microsoft Azure 인프라에 대한 가시성과 위협 탐지를 제공합니다. 그리고 클라우드로 제공되는 SaaS 기반 솔루션이기 때문에 쉽고 빠르게 구축할 수 있습니다.

AWS 환경에서는 소프트웨어 에이전트 없이 VPC(Virtual Private Cloud) 플로우 로그 같은 AWS 의 텔레메트리 네이티브 소스를 활용해 Stealthwatch Cloud 를 배포할 수 있습니다. Stealthwatch Cloud 는 VPC 내부 트래픽이든 VPC 간 트래픽이든 외부 IP 주소로 전송되는 트래픽이든 관계없이, 조직 리소스와 기능에서 생성한 모든 IP 트래픽을 VPC 플로우 로그를 사용하여 모델링합니다. 그뿐 아니라, Stealthwatch Cloud 는 Cloud Trail, Cloud Watch, Config, Inspector, IAM(Identity and Access Management), Lambda 등의 추가 AWS 서비스와도 통합됩니다.

Microsoft Azure 환경에서 Stealthwatch Cloud 는 엔티티 모델링이 필요한 모든 Linux 서버에 구축해야 하는 소프트웨어 센서를 기반으로 작동합니다.

퍼블릭 클라우드 모니터링은 프라이빗 네트워크 모니터링 또는 Cisco Stealthwatch Enterprise 와 함께 사용하여 네트워크 전반의 가시성과 위협 탐지를 제공할 수 있습니다.

Amazon Web Services 에서 Stealthwatch Cloud 를 활성화하는 방법은 다음과 같습니다.

- 적합한 권한이 있는 정책을 생성해야 합니다.
- Stealthwatch Cloud 에 대한 역할을 생성해야 합니다.
- Amazon VPC 플로우 로그를 활성화해야 합니다.

Microsoft Azure 에서 Stealthwatch Cloud 를 활성화하려면, 플로우 로그를 생성할 수 있도록 소프트웨어 센서를 모든 Linux 서버에 구축해야 합니다. 현재 사용 가능한 Microsoft Windows 센서는 없습니다.

프라이빗 네트워크 모니터링

Cisco Stealthwatch Cloud 의 프라이빗 네트워크 모니터링은 클라우드 기반의 SaaS 솔루션에서 제공되며, 온프레미스 네트워크에 대한 가시성과 위협 탐지 기능을 제공합니다. 이 솔루션은 자본 지출과 운영 오버헤드는 줄이는 동시에, 온프레미스 환경에 대한 인식과 보안은 높이고자 하는 조직에 이상적입니다.

이 모니터링 솔루션은 가상 시스템이나 서버에 다양한 텔레메트리의 네이티브 소스를 사용하거나 네트워크 패킷 플로우에서 메타데이터를 추출할 수 있는, 경량의 가상 어플라이언스를 배포합니다. 그 메타데이터를 암호화하여 분석을 위해 Stealthwatch Cloud 분석 플랫폼으로 전송합니다. Stealthwatch Cloud 는 메타데이터만 사용합니다. 패킷 페이로드는 절대 네트워크 외부에 보존되거나 전송되지 않습니다.

네트워크 인터페이스	1 NetFlow, IPFIX 또는 JFlow 만 수집하는 경우, 2 SPAN 또는 미러 포트에 연결하는 경우
메모리	최소 2GB
CPU	최소 2 개의 코어
디스크 공간	최소 32GB

프라이빗 네트워크 모니터링의 경우 플로우 텔레메트리 수집, 관리 및 분석에 Flow Rate License 가 필요합니다. 또한 Flow Rate License 는 수집할 플로우 양을 규정하며, fps(flows per second) 기준으로 라이선스가 부여됩니다.

주문 정보

Cisco Stealthwatch 주문 가이드의 섹션 3 을 살펴보면, Stealthwatch Cisco 구성요소와 라이선스 유형을 파악할 수 있습니다. 주문하려면 Cisco 어카운트 담당자에게 문의하십시오.

보안을 위한 Cisco Software Support

Cisco Stealthwatch Cloud 서브스크립션에는 보안을 위한 Cisco Software Support 의 기본 온라인 지원 옵션이 제공됩니다. 기본 온라인 지원은 구매한 소프트웨어 서브스크립션의 전체 기간 동안 다음을 포함한 기본 지원을 제공합니다.

- 온라인 도구를 통해 지원에 액세스. (전화 액세스는 제공되지 않음)
- Cisco 담당자가 제출된 사례에 대해 다음 영업일의 표준 업무 시간 안에 응답.

Cisco Stealthwatch Cloud 서브스크립션을 주문하는 경우, 서브스크립션에 기본 온라인 지원이 포함되어 있습니다. 별도로 주문할 필요가 없습니다. 따라서 Cisco Stealthwatch Cloud 서브스크립션이 갱신되면 기본 온라인 지원도 동일한 기간으로 갱신됩니다. SaaS 서브스크립션으로 이러한 지원을 받기 위해서 추가 제품을 구입하거나 이용료를 내지 않아도 됩니다.

Cisco Software Support 에 관한 자세한 내용은 서비스 설명을 참조하십시오.

지금 바로 환경 보호

위험 부담이 전혀 없는 무료 평가판으로 지금 Stealthwatch Cloud 를 사용해 보십시오. 자세한 내용을 보려면, https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html 을 방문하거나 해당 지역 Cisco 어카운트 담당자에게 문의하십시오.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

0Cisco Capital 이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 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 이용 가능합니다. 자세히 알아보십시오.

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, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

미국에서 인쇄

C78-739619-00 09/17