



# Cisco Network as a Sensor

## Cisco 네트워크를 강력한 보안 센서로 사용

네트워크는 끊임없는 지능형 사이버 공격에 대응해야 합니다. 이제 해킹은 수십억 달러 규모의 복잡한 대규모 글로벌 사업으로 발전했습니다. 한편 클라우드 서비스, 모빌리티 및 IoT(Internet of Things)의 급속도 확산으로 인해 연결되는 장치의 수는 폭발적으로 증가하고 있습니다. 이와 같은 모든 연결은 네트워크 공격을 위한 잠재적 진입점이 될 수 있습니다.

전통적인 엔터프라이즈 네트워크 경계를 넘어 발생하는 수많은 액세스 시도를 차단하려면 전 범위적인 보안이 필요합니다. 다행히 Cisco 네트워크는 이러한 위협에 대응할 수 있는 솔루션을 이미 포함하고 있습니다. 바로 Cisco® Network as a Sensor 솔루션입니다. Cisco 네트워크에 포함된 보안 기능의 간단한 활성화를 통해 네트워크 및 네트워크와 네트워크 간에 연결된 모든 항목에 대한 광범위한 가시성을 제공하는 완벽한 보안 모니터링 시스템으로 바꿀 수 있습니다.

## 혜택

- **네트워크 전반에 걸친 가시성 확보:** 전체 네트워크를 보안 센서로 사용
- **상황별 위협 인텔리전스 활용:** 실시간 NetFlow 데이터 사용
- **위험 감소:** 사용자 및 디바이스가 네트워크에 연결하는 방법, 시간, 위치 및 이유 파악 가능
- **시간 단축 및 제어 비용 절감:** 네트워크 인프라의 기존 보안 투자를 기반으로 사용

Cisco가 분석한 비즈니스 네트워크 모두(100%)에서 악성코드를 호스팅하는 웹 사이트로 이동하는 트래픽이 발견되었습니다.

Cisco 2014 Annual Security Report(2014년 연례 보안 보고서)

## 개선된 가시성: 볼 수 없으면 차단할 수도 없다.

네트워크 위협을 볼 수 없으면 방어할 수도 없습니다. Cisco Network as a Sensor 솔루션은 이러한 문제를 정면으로 타개합니다. Cisco [IOS® Flexible NetFlow](#)의 상세한 보안 분석을 통해 글로벌 네트워크에 대한 가시성을 제공하고, Cisco [ISE\(Identity Services Engine\)](#)을 통해 상황별 데이터를 제공하는 한편 파트너 기술인 Lancope StealthWatch를 통해 실시간 모니터링 및 알림을 제공합니다.

이 솔루션은 네트워크의 기준 프로필을 결정합니다. 이를 통해 비정상적인 데이터 이동, 의심스러운 트래픽, 지능형 위협 등 환경의 모든 위치에서 발생하는 악의적인 활동을 신속하게 탐지합니다. 트래픽의 흐름, 네트워크에 액세스하는 디바이스 및 네트워크에서 발생하는 악의적인 활동에 대한 정보를 제공합니다.

## 적시에 제공되는 효율적인 지능형 위협 정보

이 솔루션을 사용하면 IP 주소 뒤에 숨어 있는 사용자, 장치, 위치 및 기타 중요한 속성의 소스와 대상에 대한 정보를 빠르게 식별할 수 있습니다. 이러한 정보는 네트워크에서 일어나는 악의적인 활동의 검색 및 식별하는데 필요한 시간을 극적으로 단축하는 데 도움이 됩니다.

## 다음 단계

Cisco Network as a Sensor 솔루션에 대한 자세한 내용은 [Cisco Enterprise Network Security](#) 페이지를 참조하십시오.