업계 최초로 암호화된 상태로 트래픽을 분석하는
시스코의 최신 혁신기술

cisco

암호화된 트래픽의 증가

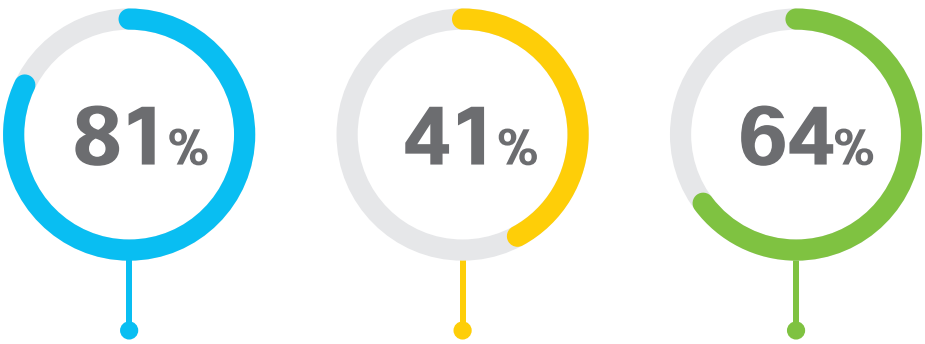
비즈니스가 디지털화됨에 따라 정보 보호와 보안을 강화하기 위해서 암호화 기술을 사용합니다. 암호화 기술은 검색, 소셜 미디어, 전자상거래 등의 웹사이트 뿐 아니라 인증서, 보안 키 등을 사용하는 애플리케이션 등에서도 널리 활용됩니다.

세계적인 IT리서치 기관인 가트너가 2019년까지 기업의 웹 트래픽 중 80% 이상이 암호화될 것이라고 예측하고 있습니다.

암호화된 트래픽이 보안의 과제

트래픽이 암호화 된다는 것은 보안이 상당히 강화된다 의미이기도 하지만, 정상적인 트래픽을 가장한 공격자들의 공격 행위를 탐지하기 어렵게 만듭니다.

글로벌 보안평가기관인 NSS Lab(NSS 연구소)의 자료에 따르면 2019년 보안 공격의 70% 이상이 명령, 제어, 데이터 유출 등의 활동을 숨기기 위해 암호화 기술을 사용할 것이라고 예측했습니다.



사이버 공격을 경험한 조직

탐지를 피하기 위해 암호화를 사용한 공격

암호화된 공격의 미 감지율

해결을 위해서는 암호화된 상태로 트래픽을 분석할 수 있는 솔루션 필요

하지만, 대다수의 기업은 암호화된 트래픽을 분석하는 솔루션을 갖추고 있지 못하며, 솔루션이 있더라도 대량의 트래픽에 대한 암호를 해독, 분석, 재 암호화하는 과정에서 정보 노출의 위험이 클 뿐 아니라 다양한 고성능의 장비나 솔루션을 도입해야하는 비용 부담이 큽니다.

따라서, 트래픽이 흘러가는 관문인 네트워크 전반에서 암호화된 상태로 사용자에게 위협이 되는 공격인지 정상적인 트래픽인지를 판단할 수 있다면 가장 경제적이고, 효율적인 방법이 될 것입니다.

게다가 분석하는 과정에서 네트워크의 속도를 저하시키지 않으면서, 네트워크 인프라 전체에 적용할 수 있어야 더욱 효율적인 방법입니다.

업계 최초로 암호화된 상태로 트래픽을 분석하는
시스코 ETA(Encrypted Traffic Analytics)

시스코 ETA는 업계 최초로 암호화된 트래픽을 해독하는 과정없이 분석해서, 정상적인 트래픽으로 가장한 악성코드를 탐지하는 혁신적인 솔루션으로, 내부 테스트 결과 99.999%의 높은 정확도를 보였습니다.

시스코의 다년간의 네트워크 경험과 지식, 방대한 정보가 축적된 분석엔진, 이 모든 것을 연계하는 솔루션이 유기적으로 통합되어 만들어진 것으로, 특히, 시스코의 보안인텔리전스 연구그룹인 시스코 탈로스(Talos)의 사이버 인텔리전스와 연결해, 머신러닝을 기반으로 한 패킷의 길이, 전달 시간, 순서, 바이트 분포, 최초 데이터 패킷의 암호화 정보 등을 사용해서 암호화된 트래픽을 분석합니다.

네트워크의 다양한 정보를
수집, 악성코드 탐지

암호 해독 과정없이
분석함으로써 보안성 확보

머신러닝 기반의
높은 정확도의 탐지 능력

시스코 ETA의 강점

공격 대응 시간 단축

감염된 장비와 사용자를 신속하게 감지

비용 절감

네트워크 장비를 보안 센서로 활용하여, 추가적인 보안 투자 비용을 최소화

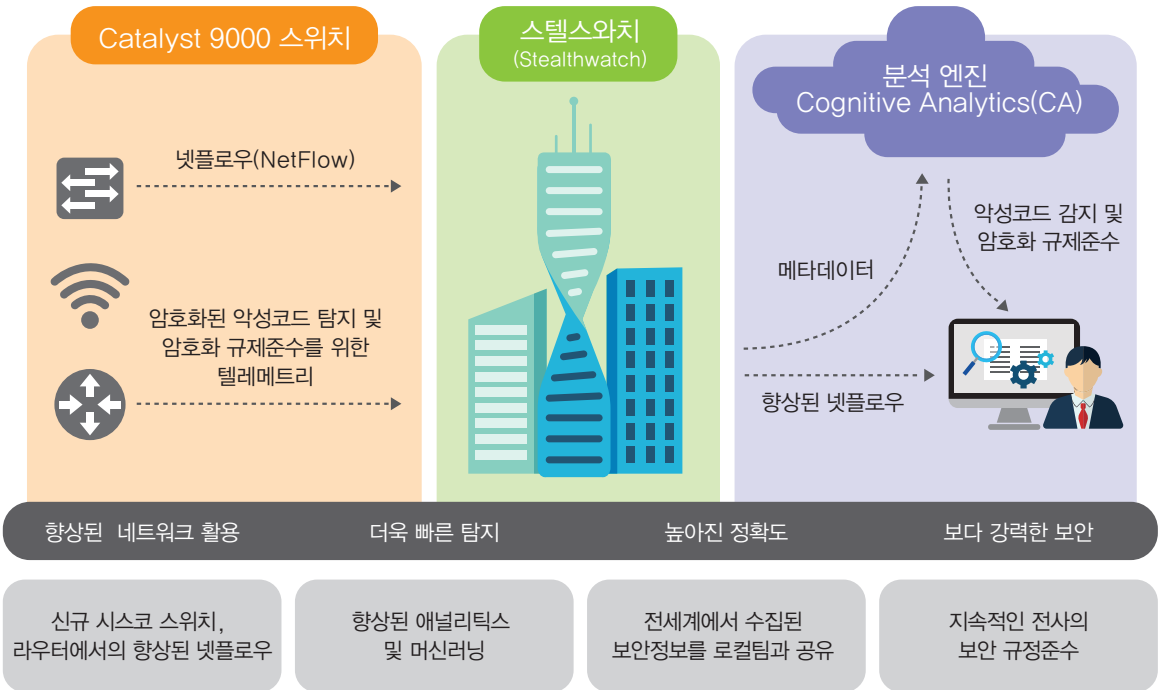
가시성 확보

네트워크 기반 분석을 통해 암호화 된 트래픽의 위협에 대한 가시성 확보.
사용자 및 장비의 상관 관계 분석을 통해 상황 별 위협 정보 제공

암호화 상태 평가

기업이 암호화 프로토콜을 준수하고 있는지,
네트워크에서 암호화 된 것과 되지 않는 항목에 대한 현황 파악

시스코 ETA의 주요 구성요소



Catalyst 9000 스위치

시스코 Catalyst 9000 스위치는 시스코 디지털 네트워크 아키텍처(DNA)를 기반으로 기초부터 새롭게 설계된 제품으로, 유무선 액세스 네트워크의 다양한 정보를 수집하고 손쉽게 관리할 수 있을 뿐 아니라 엔드-투-엔드 보안을 제공합니다.

또한, 네트워크 엣지부터 클라우드까지 포괄하는 정책 기반 자동화를 제공해서, 네트워크 서비스 및 사용자 액세스 구축, 변경하는 데 소요되는 시간을 단축시키며, 필요에 따라 네트워크를 사용자 그룹에 맞는 맞춤형 네트워크로 간편하게 구성할 수 있도록 합니다.

스텔스와치(Stealthwatch)

시스코 스텔스와치는 방화벽, 스위치, 라우터를 포함한 네트워크 장비에서 생성하는 넷플로우 정보를 기반으로 네트워크 전반에 대한 비정상적인 트래픽이나 이상 징후를 모니터링하며, 위협요소 발견시 차단하거나 격리할 수 있습니다.

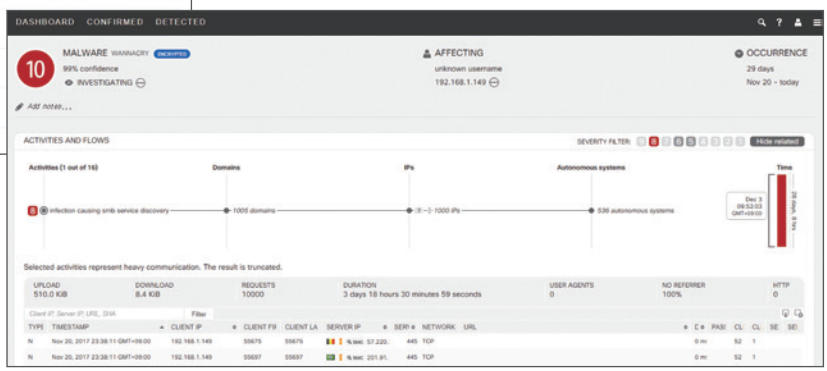
스텔스와치를 활용하면 이상 행위를 하는 내부 사용자가 얼마나 있는지, 명령 · 제어(C&C) 서버와 통신하고 있는 의심 단말이 무엇인지, 공격에 악용되는 장비, DDoS공격 소스, 내부 데이터 수집이나 유출하는 현황 등을 파악할 수 있습니다.

분석 엔진 Cognitive Analytics(CA)

시스코 스텔스와치에 적용돼있는 클라우드 기반의 분석엔진인 Cognitive Analytics(CA)는 머신러닝과 통계 모델링을 적용하여 메타데이터를 분석하게 함으로써, 웹과 네트워크 트래픽에 대한 가시성을 제공합니다.

CA는 암호화된 트래픽에서 위협적인 패턴을 찾아내고, 영향을 받는 사용자 및 경로를 자세히 제공해서 보안사고에 빠르게 대처할 수 있도록 합니다.

▶ 유입되는 트래픽을 분석엔진으로 분석한 결과 화면



▶ 위험도가 높은 트래픽을 클릭했을 경우 제공되는 대시보드 화면

THE NETWORK.
INTUITIVE.

스스로 판단하고 진화하는 네트워크

시스코 시스템즈 코리아 Cisco Systems Korea Ltd.

서울특별시 강남구 영동대로 517 아셈타워 5층 (우)06164 5F ASEM Tower, 517, Yeongdong-daero, Gangnam-gu, Seoul, Korea

Tel 02.3429.8000 **Fax** 02.3453.0851 **제품 및 구매문의** 080.808.8082 **홈페이지** www.cisco.com/kr

twitter twitter.com/CiscoKR facebook facebook.com/ciscokorea **Blog** www.ciscokrblog.com YouTube Cisco korea