Cisco Umbrella

과거에는 데스크탑, 비즈니스 애플리케이션 및 중요 인프라가 모두 방화벽 뒤에 배치됐지만 이제는 네트워크 밖에 배치되는 경우가 점차 늘고 있습니다. 다른 네트워크에서 인터넷을 통해 접속하는 기업 소유의 노트북, 로밍 사용자, 클라우드 앱이 증가하는 현실에서 사용자가 더 이상 기업 네트워크에만 의존하여 업무를 수행하지 않는다는 사실을 확인할 수 있습니다. 한편, 인터넷에 직접 연결하는 지사도 점점 더 늘어나고 있는 추세입니다.

2021년 무렵이면 기업 데이터 트래픽 중 평균 25%가 네트워크 경계를 우회할 것으로 Gartner는 예측합니다. 사용자가 네트워크 밖에 있을 경우 사용자는 더 취약해지고 기업의 가시성과 보호 능력은 저하되는데, 경계 보안에만 의존할 경우 철저한 보호가 여의치 않습니다. 그로 인한 보안 공백은 악성 프로그램, 랜섬웨어, 기타 공격에 실마리로 작용합니다.

1차 방어선

보안 인터넷 게이트웨이인 Cisco Umbrella는 사용자의 위치에 관계없이 인터넷에 존재하는 위협을 저지할 1차 방어선 역할을 합니다. Cisco Umbrella는 모든 위치, 장비, 사용자의 인터넷 활동을 완벽하게 파악하고 위협이 네트워크나 엔드포인트에 도달하기 전에 차단합니다. 클라우드 기반의 개방형 플랫폼인 Cisco Umbrella는 기존의 보안 솔루션과 원활하게 통합되며 기존의 위협과 신종 위협에 대한 위협 분석 정보를 실시간으로 제공합니다.

Cisco Umbrella는 인터넷 활동 패턴을 분석하고 학습함으로써 해커가 공격을 위해 준비한 인프라를 자동으로 발견하고 연결이 이뤄지기 전에 미리 악성 주소에 대한 요청을 차단하는데, 이 때 사용자의 대기 시간은 늘어나지 않습니다.

Cisco Umbrella를 사용하면 피싱 및 악성 프로그램 감염을 미연에 방지하고, 이미 감염된 장비를 더욱 빠르게 감지하며, 데이터 유출을 방지할 수 있습니다.

인터넷의 기본 요소로 구축되는 보안

DNS(Domain Name System)는 도메인 이름을 IP 주소에 매핑하는 인터넷의 기본 구성요소입니다. 사용자가 링크를 클릭하거나 URL을 입력하면 DNS 요청에 따라 장비를 인터넷에 연결하는 프로세스가 시작됩니다. 클라우드 플랫폼에 트래픽을 연결하는 주요 메커니즘으로 DNS를 사용하는 Cisco Umbrella는 보안을 강화할 목적으로도 DNS를 사용합니다.

DNS 요청을 수신한 Cisco Umbrella는 분석 정보를 사용하여 그 요청이 안전한지, 악성인지 또는 위험한지 판별하는데, 도메인에는 악성 컨텐츠와 합법적 컨텐츠가 모두 들어 있을 수 있기 때문입니다. 판별을 마친 Cisco Umbrella는 안전한 요청은 평소대로 라우팅하고, 악성 요청은 차단하며, 위험한 요청은 보다 심층적인 검사를 위해 클라우드 기반 프록시로 라우팅합니다. Cisco Umbrella 프록시는 Cisco Talos의 웹 평판과 다른 기업들의 피드를 사용하여 해당 URL의 악성 여부를 파악하고 안티 바이러스(AV) 엔진 및 Cisco AMP(Advanced Malware Protection)를 사용하여 위험한 사이트에서 다운로드하려고 시도한 파일을 검사한 뒤, 검사 결과에 따라 연결을 허용하거나 차단합니다.

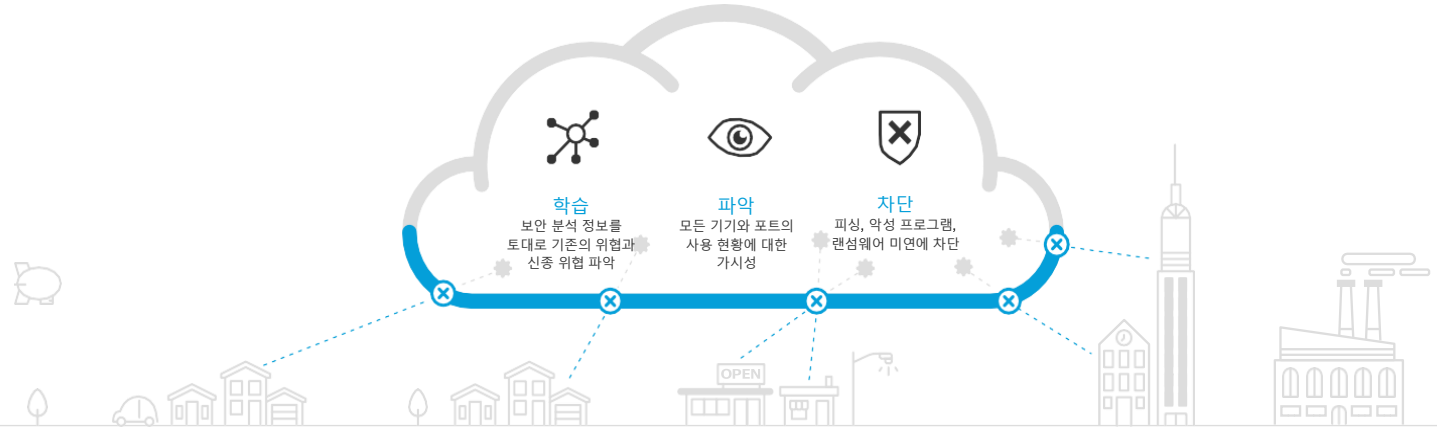
효과

치료 비용 및 데이터 유출 피해 감소: Cisco Umbrella는 1차 방어선 역할을 하기 때문에 보안 팀이 치료해야 할 악성 프로그램 감염 사례가 감소하며 피해가 발생하기 전에 공격을 저지할 수 있습니다.

위협을 감지하고 억제하는 데 소요되는 시간 감소: Cisco Umbrella는 포트 또는 프로토콜에 대한 명령 및 제어 콜백 기능을 갖추고 있으며 콜백 상황을 실시간으로 보고합니다.

모든 위치 및 사용자의 인터넷 활동에 대한 가시성 향상: Cisco Umbrella는 사고 대응에 중대한 영향을 미치는 가시성을 제공하므로 기업이 모든 상황을 확실하게 파악할 수 있습니다.

전사적으로 클라우드 앱 사용 현황 파악: Cisco Umbrella는 기업 전역에서 합법적 또는 무단으로 사용 중인 클라우드 서비스에 대한 가시성을 제공하므로 기업은 어떤 서비스가 새로 사용되고 있으며 누가 이 서비스를 사용하고 있는지 파악하고 잠재적 위험을 판별할 수 있습니다.



보안 분석 정보를 토대로 공격이 개시되기 전에 저지

시스코의 귀납적 DNS 서비스가 구축되는 네트워크인 Umbrella 글로벌 네트워크는 매일 수십억 건에 달하는 전 세계 수백만 사용자의 인터넷 요청을 해결합니다. 시스코는 이 엄청난 양의 데이터를 분석하여 패턴을 감지하고 공격자의 인프라를 파악합니다.

시스코는 글로벌 네트워크의 모든 인터넷 활동 데이터를 대용량 그래프 데이터베이스에 실시간으로 취합한 후, 이를 토대로 통계 및 머신러닝 모델링을 지속적으로 실시합니다. Umbrella 보안 연구원들은 지속적으로 이 정보를 분석하고 Cisco Talos의 보안 인텔리전스로 보완합니다. 시스코는 이러한 인간 지능과 머신러닝의 접목을 통해 도메인, IP 또는 URL 등 인터넷 전역의 모든 악성 사이트를 판별합니다.

다른 인프라와 적절한 조화

Cisco Umbrella는 보안 어플라이언스, 인텔리전스 플랫폼 및 CASB(Cloud Access Security Broker) 컨트롤러를 비롯한 기존의 보안 인프라와 통합됩니다. Cisco Umbrella는 인터넷 활동에 관한 로그 데이터를 SIEM이나 로그 관리 시스템에 전송할 수 있으며, 사용자는 API에서 Cisco Umbrella에 전송하도록 설정하여 악성 도메인을 차단할 수 있습니다. 기존의 투자 활용도를 극대화하고 보호 범위를 모든 곳으로 쉽게 확장할 수 있습니다.

몇 분만에 전사적 배치 완료

단 몇 분만에 배치를 완료할 수 있는 Cisco Umbrella는 모든 사용자를 가장 빠르고 손쉽게 보호할 수 있는 보안 솔루션입니다. Cisco Umbrella는 클라우드를 통해 지원되므로 하드웨어를 설치하거나 소프트웨어를 일일이 업데이트할 필요가 없습니다. BYOD 및 IoT를 비롯해서 네트워크에 연결된 모든 장비를 몇 분 내에 프로비저닝하고 기존 시스코 인프라[AnyConnect, ISR(Integrated Services Router) 4K 시리즈, 무선 LAN 컨트롤러 5520 및 8540]를 사용하여 수천 개의 네트워크 엔트포인트와 로밍 노트북을 단시간에 프로비저닝할 수 있습니다.

다음 단계

시스코 영업 담당자나 파트너에게 연락하여 Cisco Umbrella로 어떻게 모바일 장비와 클라우드로 연결된 조직을 정교한 위협으로부터 보호할 수 있는지 확인하십시오. 자세한 내용은 시스코 홈페이지 umbrella.cisco.com을 참조하십시오.

주요 특징

- 모든 지점에 대한 가시성 및 보호 체계 구축
- 보안 정보 분석을 토대로 조기에 공격 감지
- 간단한 배치 및 관리
- 통합하기 용이한 개방형 플랫폼
- ▪ 빠르고 안정적인 클라우드 인프라

주요 통계

- 일일 평균 인터넷 요청 건수 1,000억 건
- 사용자 수 6,500만 명
- 전 세계 데이터 센터 개수 25개
- DNS 계층에서 동시에 발생하는 악성 주소 700만 개