NETSCOUT

NETSCOUT Arbor DDoS 공격 방어 솔루션이 더 좋은 이유

NETSCOUT Arbor DDoS 공격 방어 솔루션은 왜 특별한가요?

당사 솔루션은 온프레미스 및 클라우드 내 DDoS 공격 보호를 결합하는 지능적으로 자동화된 완전 관리형 솔루션입니다. 글로벌 위협 인텔리전스는 정기적으로 지속적으로 업데이트됩니다.

1. 온프레미스에서 NETSCOUT Arbor Edge Defense (AED) 제품은 머신 러닝 기반 지능형 DDoS 보호 기능을 통하여 다음과 같은 모든 유형의 DDoS 공격을 장비 스스로 분석하여 자동으로 감지하고 차단할 수 있는 상시 작동 인라인 DDoS 보호 솔루션입니다.
   - 최대 200Gbps의 볼륨메트릭 공격
   - TCP 세션 고갈 공격 및 애플리케이션 공격
   - 암호화된 트래픽 공격
2. Arbor Edge Defense는 동급 최고의 DDoS 보호 기능 이상을제공합니다. 수백만 개의 평판 기반 침해 지표(IoC) 및 NETSCOUT의ATLAS® Intelligence Feed 또는 제3자(STIX/TAXII 지원을 통해)의 기타위협 인텔리전스를 갖춘 AED는 조직 내 악성코드 확산을 차단하는 데도움이 될 수 있습니다. AED는 상태 비저장 패킷 처리 기술을 사용하여손상된 내부 장치에서 알려진 불량 사이트로의 인바운드 IoC 및아웃바운드 통신을 차단하여 데이터 침해를 방지할 수도 있습니다.
3. Intelligent Cloud Signaling은 AED가 현재 또는 미래의 공격에 사용하기 위해 클라우드 기반 완화 서비스(예: ISP, CDN 공급자 또는 NETSCOUT의 Arbor Cloud)에 대한 맞춤형 로컬 공격 정책 정보를 지속적으로(무장 해제) 가능하게 합니다. 대규모 공격이 발생하면 공격 트래픽이 분석 및 완화를 위해 적절한 클라우드 스크러빙 센터로 자동 라우팅됩니다. 이전에 전송된 AED 로컬 공격 정책을 포함하여 사전 구성된 공격 대응책은 몇 분 안에 DDoS 공격을 자동으로 차단합니다.
4. Arbor Cloud는 전 세계 15개 스크러빙 센터를 통해 15Tbps 이상의 완화 용량을 제공하는 연중무휴 완전관리형 DDoS 공격 보호 서비스입니다.
5. 공격 후 모든 공격 활동을 자세히 설명하는 포괄적인 보고서 세트가 자동으로 생성됩니다. 그리고 이러한 모든 제품과 서비스는 ATLAS 및 ASERT를 기반으로 하는 글로벌 위협 인텔리전스로 완벽하게 관리되고 지속적으로 무장하고 있습니다.

현재와 미래의 지능형 DDoS 공격으로부터 가장 포괄적인 방법인 클라우드, 온프레미스 DDoS 공격 방어에 대한 자동화된 조합을 제공하는 유일한 벤더입니다.

Arbor는 모든 규모의 조직이 기술 및 재정 상황에 적합한 솔루션을 맞춤 제작할 수 있도록 업계 최대의 DDoS 공격 방지 제품 및 서비스 포트폴리오를 제공하고 있습니다.

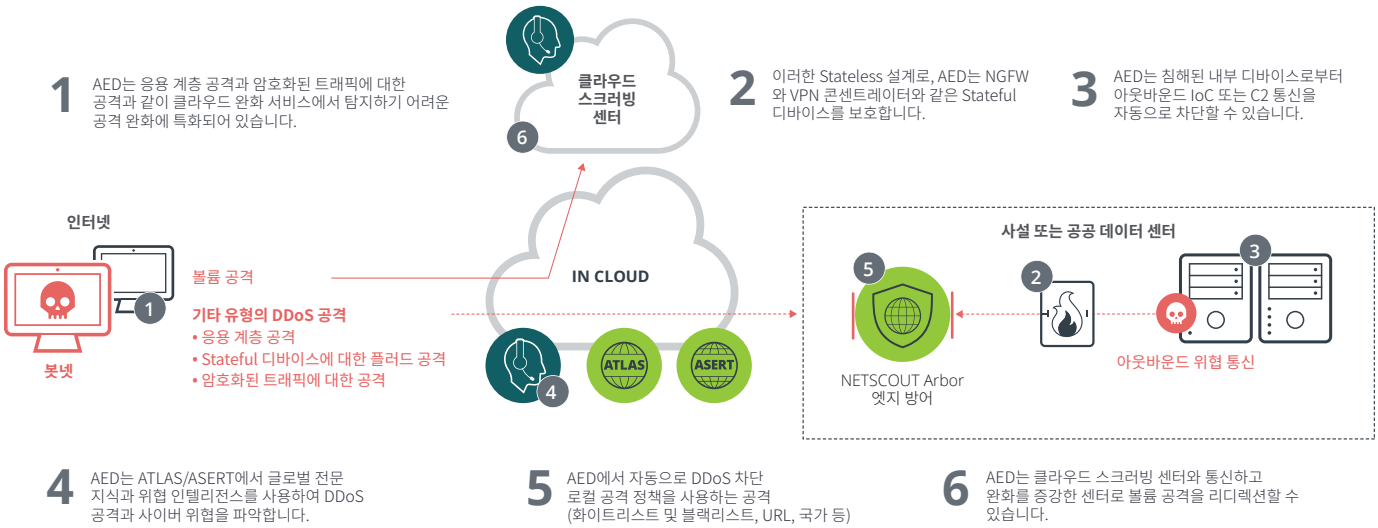

그림 1: Arbor의 지능적 자동화 실행.

NETSCOUT AED and AEM

효과적인 첫 번째이자 마지막 자동 경계 방어선을 제공하기 위해 다이나믹하게 변화하는 DDoS 공격에 적응하는 머신러닝기반 지능형 DDoS 보호 솔루션

DDoS 공격은 진화하고 있습니다. 요즘 선호되는 DDoS 공격은 다중 벡터 동적 직접 경로 공격입니다. 이는 기존 DDoS 방어를 지속적으로 회피하기 위해 벡터와 수법을 조정합니다. 여기에 랜섬웨어, 피싱시도, 손상된 IoT 디바이스까지 더하면 조직이 모든 유형의 고급 사이버 위협으로 인한 지속적인 위험에 노출되어 있다는 것을 알 수 있습니다. 이렇게 발전하는 위협을 해결하기 위해 보안 팀은 네트워크에 출입하고 변화하는 공격에 다이나믹하게 적응할 수 있는 솔루션이 필요합니다. 또한 중요한 점은 이러한 솔루션이 조직의 기존 보안 스택에 통합 및/또는 기능을 통합하여 비용, 복잡성, 위험을 줄일 수 있어야 한다는 것입니다.

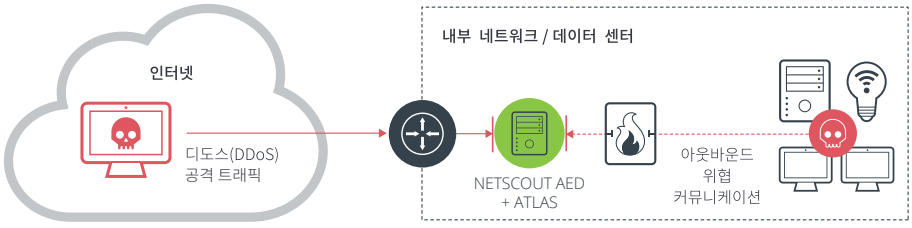

그림 2: 네트워크 엣지에서 AED의 고유한 위치 + Stateless 패킷 처리 엔진 + ATLAS 글로벌 위협 인텔리전스 = 첨단 사이버 위협으로부터의 첫 번째이자 마지막 방어선

NETSCOUT Arbor Edge Defense(AED)는 상시 가동되는 첫 번째이자 마지막 인라인 방어선을 제공하기 위해 네트워크 엣지에서 특별한 위치(예: 인터넷 라우터와 방화벽 사이)를 차지합니다. Stateless 패킷처리, 지속적인 글로벌 위협 인텔리전스, 수십 년 동안의 DDoS 완화 전문 지식, 머신러닝 기반 지능형 DDoS 방어 기술을 사용하여 AED는 자동으로 인바운드, 다이나믹하게 변화하는 DDoS 공격 그리고 위협 행위자 명령 및 제어(C2) 인프라와 통신하는 손상된 내부 디바이스에서 비롯된 아웃바운드 커뮤니케이션을 차단할 수 있습니다. Arbor Enterprise Manager는 모든 AED 관리를 위한 중앙 집중화되어 있으며 확장 가능한 단일창 방식의 콘솔을 제공합니다.

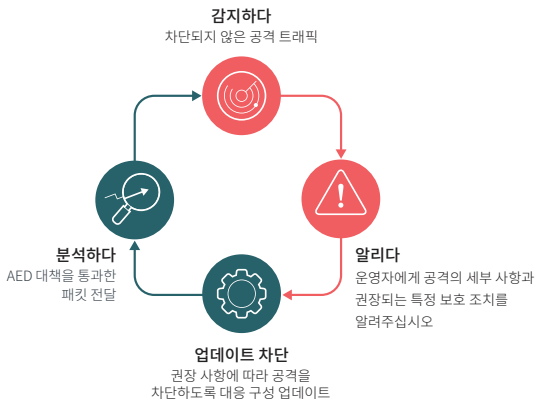

그림 3: Arbor Adaptive DDoS Protection은 이 단순하고 효율적인 워크플로우에 의해 구동됩니다.
참고: 머신러닝 기반 지능형 DDoS 보호는 AED 8100 및 가상 AED에서 지원됩니다. AEM도 필요합니다.

주요 기능 및 혜택

머신러닝 기반 지능형 DDoS 보호

자동으로 새로운 공격 기술을 탐지하고 표적화된 완화를 제공하여 합법적인 서비스에 영향을 주지 않은 채로 끊임없이 변화하는 DDoS 공격을 효과적으로 탐지하고 완화합니다. 동적 트래픽 분석 기술, 글로벌 공격 가시성, 머신러닝 기반 지능형 인텔리전스 및 수십 년 동안의 DDoS 분야 전문 지식을 바탕으로 탄생했습니다.

엔터프라이즈 규모 및 심층적인 다층 방어

Arbor Enterprise Manager를 통해 단일창에서 배포된 모든 AED를 관리하기 위한 중앙 집중화되어 있으며 확장 가능한 가시성. 지능적으로 포괄적인 하이브리드 DDoS 공격 방어를 위해 Arbor Cloud와 통합됩니다.

AWS에서 자산 보호

AWS에서 가상 AED를 배포하고 AWS(AWS 클라우드 외부 및 VPC 사이의 클라우드 내부)에서 자산을 대상으로 한 공격을 탐지 및 완화합니다.

첫 번째이자 마지막 방어선

독보적인 위협 인텔리전스와 내장된 보안 분석 전문 지식으로 네트워크 엣지에서 원치 않는 악성 인바운드 및 아웃바운드 트래픽(맬웨어, 스캐닝 및 피싱 시도 포함)을 자동으로 확실하게 차단합니다.

기존 보안 스택 및 프로세스와 통합

NETSCOUT AED의 REST API, Syslog(CEF, LEEF)에 대한 지원 및 STIX/TAXII는 NETSCOUT AED를 조직의 기존 보안 스택 및 프로세스에 완벽하게 통합된 구성 요소로 만듭니다.

NETSCOUT Systems Korea
서울시 강남구 테헤란로 521
파르나스타워 29층
전화 : 02-2097-8150
이메일 : netscout-kr-ent@netscout.com

(주)이롭 서울시 구로구 디지털로31길 38-21,
208호(구로동, E&C벤처드림타워3차) 08376
전화 : 02-3282-2303
이메일 : sales@erop.co.kr
http://www.erop.co.kr