CEQUENCE

DATASHEET

Cequence Bot Management

봇 탐지, 완화 및 사기 방지

오늘날 웹 트래픽의 거의 절반은 정상적인 봇과 악성 봇을 포함한 자동화된 봇에 의해 생성됩니다. 과거에는 악성 봇이 주로 웹사이트와 애플리케이션을 공격했지만, 이제는 애플리케이션을 우회하여 API를 직접 공격하는 경우가 점점 더 많아지고 있습니다.

API는 높은 접근성, 사용 편의성, 유연성, 그리고 광범위한 활용으로 인해 공격자들의 주요 표적이 되었습니다. 적절하게 개발된 API라 하더라도 대규모 계정 탈취(Account Takeover, ATO)나 구매 봇 캠페인의 일부로 비즈니스 로직 악용 공격에 노출될 수 있습니다.

대량의 가짜 계정 생성과 콘텐츠 스크래핑 또한 애플리케이션과 API를 대상으로 지속적으로 수행되고 있습니다. 따라서 기업은 애플리케이션과 API를 겨냥한 자동화 공격을 탐지 및 차단하고, 손쉽게 배포할 수 있으며 즉각적인 효과를 제공하는 솔루션이 필요합니다.

Bot Management 한눈에 보기

- **CAPTCHA 불필요**
  네트워크 기반 접근 방식으로 에이전트, JavaScript 또는 SDK 연동이 필요 없음
- **네이티브 완화 기능**
  WAF와 같은 타사 인프라에 의존하지 않고 공격을 탐지 및 차단
- **강력한 완화 옵션**
  차단, 속도 제한(Rate Limiting), 헤더 삽입, 디셉션(Deception) 기능 제공
- **빠른 가치 실현**
  신속한 구축과 즉각적인 효과
- **유연한 배포 모델**
  온프레미스, SaaS 및 하이브리드 환경 지원
- **API 사기 방지**
  조직별 요구사항에 맞는 세분화된 맞춤형 정책 지원

Cequence Bot Management 개요

Cequence는 웹, 모바일 및 API 애플리케이션을 기존 봇 공격부터 AI 기반의 고도화된 봇 공격까지 모든 유형의 자동화 공격으로부터 보호하여 데이터 유출, 정보 탈취 및 사기를 방지합니다.

머신러닝 기반 분석 엔진은 애플리케이션 및 API 트랜잭션의 행위를 실시간으로 분석하여 정상적인 요청과 악성 요청을 구분합니다. 이를 통해 공격을 네이티브 방식으로 완화하고 서비스 중단, 브랜드 신뢰도 하락, 왜곡된 매출 분석, 인프라 비용 증가와 같은 비즈니스 영향을 제거합니다.

Bot Management 주요 기능

애플리케이션 수정 없이, 사용자 경험 그대로

Cequence의 네트워크 기반 접근 방식은 에이전트 설치나 JavaScript, 모바일 SDK 연동과 같은 애플리케이션 수정이 필요하지 않습니다.

이 접근 방식은 CAPTCHA와 같은 기존 봇 방어 기술이 초래하는 사용자 불편을 제거하며, 계측이 가능한 애플리케이션뿐만 아니라 모든 애플리케이션과 API까지 보호 범위를 확장합니다.

또한 네트워크 기반 보호는 애플리케이션 계측에 필요한 개발 및 테스트 작업을 제거하여 시간과 비용을 절감합니다.

많은 조직은 자신들이 봇 문제를 겪고 있다는 사실조차 인식하지 못합니다. 봇은 단순히 공격을 대규모로 자동화하는 수단이기 때문입니다. Cequence는 다음과 같은 다양한 공격을 탐지하고 완화합니다.

계정 탈취(ATO)

BOLA 취약점 공격

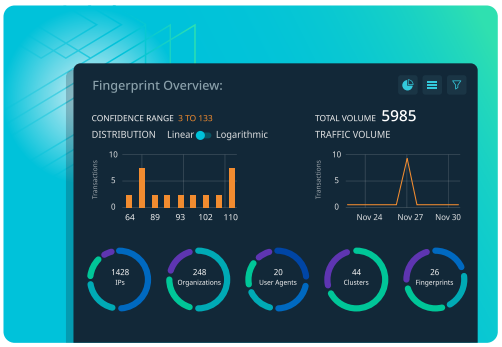
플래시 세일, 한정 판매 및 스니커 드롭 (Sneaker Drop) 공격

민감 데이터 노출

기프트 카드 및 로열티 프로그램 악용

가짜 계정 생성

지속적 행위 기반 위협 탐지 및 대응



Cequence의 머신러닝 기반 분석 엔진은 웹, 모바일 및 API 트래픽 전반에 걸쳐 행위 의도(Behavioral Intent)를 분석하여 IP 주소뿐 아니라 실제 행위를 기반으로 정상 트래픽과 악성 트래픽을 식별합니다. 이를 통해 생성된 행위 지문(Behavioral Fingerprint)은 공격자가 탐지를 회피하기 위해 전술을 변경하더라도 정교한 공격을 지속적으로 추적할 수 있습니다. 이 접근 방식은 기존 자동화 공격뿐 아니라 AI 기반 봇 공격에도 매우 효과적입니다.

실시간 완화

Cequence는 AI를 활용하여 공격을 탐지하고 위협 완화 규칙과 정책을 자동으로 생성합니다. 생성된 정책은 자동 적용하거나 보안 담당자의 검토 후 적용할 수 있습니다. 네이티브 완화 기능은 실시간으로 수행되며 차단, 속도 제한, 헤더 삽입 및 디셉션 기능을 포함합니다.

끊김 없는 사용자 인증

기존의 봇 방어 기술은 한계에 도달했습니다. 오늘날 머신러닝 모델은 이미지 기반 CAPTCHA를 일반 사용자보다 더 높은 정확도로 해결할 수 있으며, SMS 팜(SMS Farm)은 이동통신 인프라를 악용하여 일회용 인증 코드를 대규모로 가로채고 있습니다. Cequence의 Biometric Check는 완전히 다른 접근 방식을 제공합니다. 퍼즐을 제시하거나 인증 코드를 전송하는 대신 의심스러운 세션을 Face ID, Touch ID 또는 Windows Hello와 같은 디바이스의 기본 인증 방식으로 자동 연결합니다. 그 결과 사용자의 경험을 방해하지 않으면서도 실제 사용자가 요청을 수행하고 있음을 거의 즉시 확인할 수 있습니다.

빠른 가치 실현

Cequence는 애플리케이션 수정 없이 쉽게 구축할 수 있으며 즉시 효과를 제공합니다.또한 SaaS, 온프레미스 및 하이브리드 배포 옵션을 지원하여 모든 조직의 요구사항에 유연하게 대응합니다.

비즈니스에 최적화된 사기 방지

Cequence Bot Management는 업종 및 비즈니스 환경에 특화된 사기 방지 시나리오를 지원하기 위해 세분화된 맞춤형 정책 기능을 제공합니다. 정의된 사기 정책과 일치하는 활동은 실시간으로 탐지 및 차단되며, 각 사기 캠페인에 대한 상세 분석 정보도 함께 제공됩니다.

Cequence AI Gateway와 연동

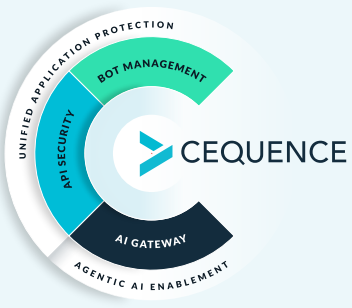
Cequence AI Gateway는 코딩 없이도 몇 분 만에 내부 시스템, 외부 서비스 및 SaaS 애플리케이션에 대한 에이전틱 AI(Agentic AI)의 안전한 접근을 제공합니다. Bot Management는 기업의 애플리케이션과 API를 악성 AI 에이전트로부터 보호합니다.

Bot Management는 Cequence 플랫폼의 일부입니다

Cequence 플랫폼은 웹, 모바일, API 및 AI 채널을 공격, 비즈니스 로직 악용 및 사기로부터 보호하는 동시에 안전한 에이전틱 AI 도입을 지원합니다.

사용자, 엔터티 및 AI 에이전트의 행동에 대한 깊은 이해를 바탕으로 Cequence는 안전하고 신뢰할 수 있는 에이전틱 AI 접근을 구현하며, 기업이 AI 기반 생산성과 성장의 잠재력을 최대한 활용할 수 있도록 지원합니다.

Cequence 플랫폼은 조직이 본연의 비즈니스 목표에 집중할 수 있도록 필요한 보안, 거버넌스 및 제어 기능을 제공합니다.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai