

Cequence Platform

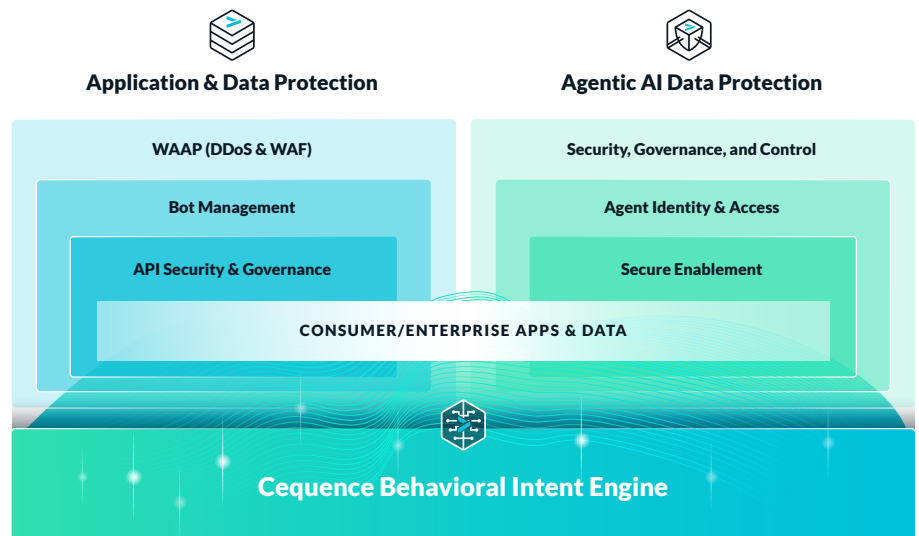
애플리케이션, API 및 AI를 위한 행위 기반 보호

계속 확장되는 공격 표면

클라우드 도입 확대, 시스템 간 통합의 가속화, 제3자 공급망 의존성 증가, 그리고 AI의 등장으로 인해 기업의 공격 표면은 급격히 확장되고 있으며, 이에 따라 애플리케이션과 데이터가 다양한 보안 위협에 노출되고 있습니다. 애플리케이션과 API는 지속적으로 증가하고 있으며, AI는 공격자가 취약점을 탐지하고 기계 수준의 속도로 공격을 수행할 수 있도록 지원하고 있습니다. 또한 통제되지 않는 AI 에이전트는 데이터 유출과 권한 오·남용의 새로운 위협을 초래하고 있습니다. 조직은 AI 기반 생산성과 성장의 잠재력을 실현하는 동시에, 애플리케이션, API 및 데이터를 공격, 비즈니스 로직 악용, 그리고 사기로부터 보호할 수 있는 솔루션이 필요합니다.

Cequence만의 차별화된 접근 방식

모든 애플리케이션, API 및 에이전트형 AI의 상호작용은 그 행위를 통해 의도를 드러냅니다. 행위 의도(Behavioral Intent)는 Cequence 플랫폼의 핵심 기반입니다. Cequence는 애플리케이션, API 및 데이터와 상호작용하는 모든 사용자, 봇 및 AI 에이전트의 행위를 프로파일링하여 정상적인 자동화와 악성 활동을 구분할 수 있는 디지털 ID를 구축합니다. 이러한 기능은 이제 에이전트형 AI까지 확장되었습니다. Cequence는 에이전트와 애플리케이션 간의 트래픽에 행위 분석을 적용하여, 에이전트가 수행할 수 있는 작업과 접근할 수 있는 데이터를 실시간으로 제어하고, 허용된 범위를 벗어나는 행위가 발생할 경우 즉각적인 대응 조치를 수행합니다.



Cequence 제품



AI Gateway

에이전트형 AI 워크플로우를 연결하고 보호



Bot Management

자동화 공격 및 사기로부터 애플리케이션과 API 보호



API Security

API 엔드포인트를 탐지, 인벤토리화, 테스트 및 보호



WAAP

Bot Management, API Security, WAF 및 DDoS 방어를 통합 제공

Cequence AI Gateway는 조직이 애플리케이션과 데이터를 AI 에이전트가 쉽고 안전하게 사용할 수 있도록 지원합니다. 가시성과 모니터링을 위한 중앙 관리 지점을 제공하며, 신뢰할 수 있는 MCP, API, LLM 및 스킬 레지스트리와 기업이 승인한 애플리케이션 카탈로그를 제공합니다. 또한 최소 권한 접근 (Least Privilege Access), 속도 제한(Rate Limiting), 민감 데이터 보호와 같은 기능을 포함한 거버넌스와 가드레일을 기본 제공하여 AI 에이전트의 행동을 안전하게 제어합니다.

AI Gateway에는 최소 권한 접근(Least Privilege Access), 속도 제한(Rate Limiting), 민감 데이터 보호와 같은 기능을 기반으로 에이전트의 행위를 제어하기 위한 거버넌스 및 가드레일이 기본적으로 내장되어 있습니다.

또한 제로 트러스트 원칙을 기반으로 런타임 환경에서 에이전트의 행위를 지속적으로 검증하고 유효성을 확인합니다. 이러한 가드레일과 제어 체계를 통해 조직은 거버넌스를 유지하면서도 신속한 혁신을 추진할 수 있으며, 단순한 솔루션에서 흔히 발생하는 기술 부채와 확장성 제약 없이 프로토타입 단계에서 운영 환경(Production)까지 원활하게 전환할 수 있습니다.

Cequence API Security는 API를 탐지, 인벤토리화 및 테스트하는 AI 우선(AI-first) 솔루션으로, 포괄적인 API 보안 태세 관리(API Security Posture Management)를 제공합니다. 내부 API, 외부 API, 서드파티 API는 물론 엣지, 인프라, 게이트웨이 및 호스팅 제공업체까지 폭넓게 탐지합니다.

Inside-Out 및 Outside-In 탐지를 결합하여 공격 표면과 내부 API 모두에 대한 가시성과 인벤토리를 제공합니다. Cequence API Security는 API를 통해 전달되는 민감 데이터를 자율적으로

식별하고 런타임에서 이를 마스킹하여 원치 않는 데이터 유출을 방지합니다. 또한 보안 담당자를 지원하는 AI Assistant와 내부 에이전트형 AI 워크플로우와 연동할 수 있는 내장 MCP 서버를 제공합니다.

Cequence Bot Management는 광범위한 자동화 공격을 탐지하고 실시간으로 대응 정책을 적용하여 데이터 유출, 탈취 및 사기를 방지합니다. Bot Management는 네트워크 기반으로 동작하므로 기존 인프라와 손쉽게 통합할 수 있으며, 별도의 에이전트, JavaScript 또는 SDK가 필요하지 않습니다.

행위 기반 핑거프린팅과 다차원 분석은 비즈니스 컨텍스트를 심층적으로 이해하여 공격을 실시간으로 식별하고 네이티브 방식으로 차단합니다. 또한 비즈니스 로직 공격, 취약점 악용 공격, 자동화된 봇 활동, 온라인 사기 및 OWASP API Security Top 10 위협을 포함한 다양한 사이버 공격을 완화합니다.

Cequence Web Application and API Protection (WAAP)은 Bot Management와 API Security를 WAF 및 DDoS 방어 기능과 통합하여 단일 SaaS 테넌트로 제공합니다.

공유 트래픽 파이프라인 내에서 통합된 구성 요소들은 멀티벤더 환경에서 흔히 발생하는 보안 사각지대와 트래픽 라우팅 불일치를 제거합니다. 단일 애플리케이션 보호 포털을 통해 WAF, Bot Management 및 API Security를 통합 운영할 수 있으며, 관리 복잡성을 줄이는 동시에 모든 애플리케이션 및 API 상호작용에 대해 일관되고 연계된 방어 체계를 제공합니다.

주요 활용 사례



에이전트형 AI 보안 및 거버넌스

에이전트형 AI 워크플로우에 대한 가시성, 모니터링, 가드레일 및 제어



JavaScript 및 SDK 불필요

애플리케이션 수정 없이 배포 가능



어디서나 배포 가능 온프레미스, SaaS 또는 하이브리드 환경 지원



봇 공격 방어

웹, 모바일 및 API 애플리케이션 전반에 걸친 효과적인 공격 방어



블랙박스가 아닌 투명성

공격 트래픽, 정책 및 데이터에 즉시 접근 가능



안전한 에이전트형 AI 도입

엔터프라이즈 및 SaaS 애플리케이션을 안전하게 에이전트 지원 환경으로 전환



개방형 아키텍처

데이터를 가져와 분석을 강화하고 SIEM 및 WAF로 내부 워크플로우를 개선



취약점 악용 방지

제로데이 공격 차단 및 OWASP API Security Top 10, PCI DSS 요구사항 대응



API 인벤토리 및 위험 평가

내부, 외부 및 제3자 API를 지속적으로 평가하고 관리



민감 데이터 유출 방지

민감 데이터를 자동 식별 및 마스킹하여 유출 차단

Cequence 플랫폼 주요 기능

행위 인텔리전스와 정밀한 식별

Cequence는 사용자와 엔터티의 행동을 분석하여 풍부한 디지털 아이덴티티를 구축함으로써, 조직이 악성 봇의 위험 없이 생산적인 AI 에이전트를 안전하게 활용할 수 있도록 지원합니다. 사람과 봇을 정확하게 구분하고, 정상적인 자동화와 위협을 구별합니다. 또한 한층 강화된 인증이 필요한 경우, Cequence Biometric Check는 CAPTCHA와 같은 불필요한 사용자 불편을 추가하는 대신 방문자의 기기에 내장된 Secure Enclave를 활용하여 인증을 수행할 수 있습니다.

런타임 보호 및 실시간 대응

Cequence는 런타임 환경에서 동작하며, 공격이 발생하는 즉시 이를 탐지하고 피해가 발생하기 전에 동적으로 대응합니다. 정적인 규칙이나 사후 분석에 의존하지 않고, 실시간 트래픽을 지속적으로 평가하여 위협을 실시간으로 식별하고 즉각적이고 정밀한 대응 조치를 수행합니다. 이를 통해 정상 사용자의 서비스 이용을 방해하지 않으면서 애플리케이션, API 및 데이터를 보호합니다.

모듈형 아키텍처와 유연한 배포

Cequence는 전 세계 주요 금융, 리테일 및 통신 기업 환경에서 매일 100억 건 이상의 애플리케이션 및 API 상호작용을 분석하고 보호합니다. 조직은 현재 필요한 Cequence 제품부터 도입하고, 요구사항 증가에 따라 점진적으로 확장할 수 있습니다. SaaS, 온프레미스 및 하이브리드 환경 전반에서 제공되는 빠르고 유연한 배포 옵션을 통해 플랫폼이 고객의 인프라 환경에 맞춰 적응하며, 고객이 플랫폼에 맞춰 인프라를 변경할 필요가 없습니다.

통합 플랫폼과 일관된 보호

Cequence 플랫폼은 처음부터 통합을 고려하여 설계되었습니다. 네이티브 통합 아키텍처는 개별 포인트 솔루션을 연결할 때 발생하는 보안 사각지대와 운영 오버헤드를 제거하며, 봇, API 및 AI 전반에 걸쳐 조직에 단일하고 일관된 방어 체계를 제공합니다.

“저는 위협 행위자들을 기업 경계 내부에서 상대하고 싶지 않습니다. 가능한 한 보안 경계를 외부로 확장하고 싶습니다. Cequence는 위협 행위자로부터 발생하는 악성 트래픽을 기업 경계 밖에서 사전에 차단할 수 있습니다. 이러한 기능을 통해 우리 조직의 보안 태세는 크게 향상되었습니다.”

Maria Ng
CISO

