CEQUENCE

DATASHEET

Cequence AI Gateway

에이전틱 AI를 위한 보안, 거버넌스 및 제어

Cequence는 업계에서 가장 효과적인 봇 관리(Bot Management) 솔루션을 구축했으며, 현재 매일 100억 건 이상의 API 호출과 2억 건 이상의 에이전틱 상호작용을 보호하고 있습니다. Cequence 플랫폼의 핵심인 행위 의도(Behavioral Intent) 엔진은 단순한 신원이 아닌 의도를 분석하여 정상 사용자, 정상 봇, 그리고 악의적 행위자를 구분합니다. AI Gateway는 이러한 검증된 기술을 AI 에이전트 환경으로 확장합니다. 모든 에이전트에는 명확한 역할이 부여되며, 모든 행위는 해당 역할에 부합하는지 지속적으로 검증됩니다. 자격 증명만으로는 신뢰를 부여하지 않으며, 모든 신뢰는 지속적인 검증을 통해 확인됩니다.

정책 집행은 모델이나 엔드포인트가 아닌 AI Gateway에서 수행되므로, 에이전트가 관리형 디바이스, 클라우드 플랫폼 또는 ChatGPT Workspaces 및 Agentforce와 같은 SaaS 에이전트 서비스 어디에서 실행되더라도 거버넌스는 중앙에서 유지됩니다. Frontier 모델, Open-Weight 모델, 자체 호스팅 모델 모두 동일하게 보호됩니다. 신원(Identity)은 에이전트의 접근을 허용하는 역할을 수행하지만, AI Gateway는 에이전트가 이후 수행하는 모든 행위를 해당 역할(Role)에 따라 통제하고, 모든 행위가 역할에 부합하는지 지속적으로 검증합니다.

Cequence AI Gateway의 차별점

Agentic Zero Trust 아키텍처

AI Gateway는 에이전트를 인증한 후 수행하는 모든 행위를 개별적으로 승인합니다. Gateway는 요청 경로 상에서 정책을 인라인으로 적용하며, 세션 전체와 모든 툴 호출(Tool call)에 대해 지속적으로 제어합니다. Dr. Chase Cunningham과 Anthropic의 독립적인 연구는 Cequence가 이 분야에서 유일하게 제품 아키텍처로 구현되었음이 검증된 것입니다.

Agent Personas 기반 최소 권한 접근 제어

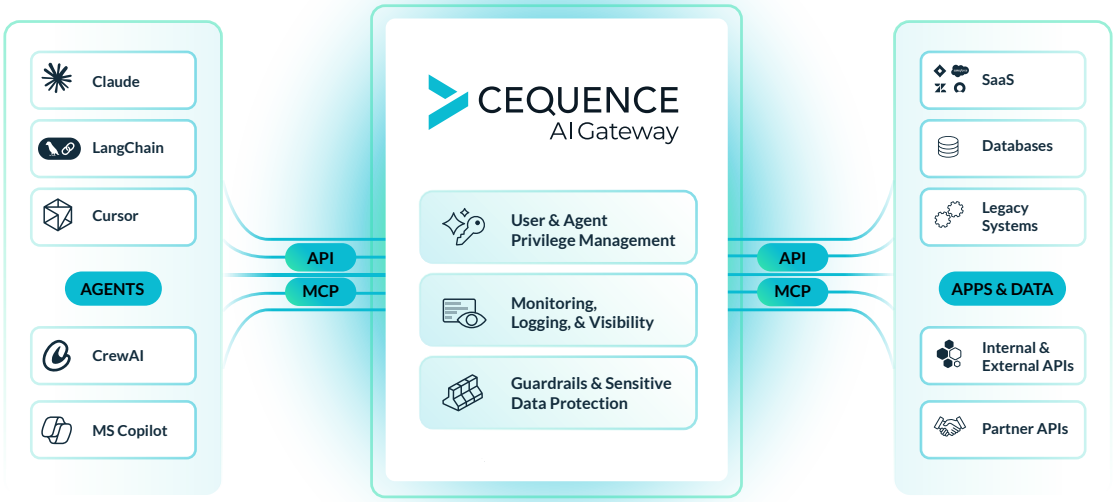
자연어로 작성된 직무 설명(Job Description)은 기본 거부(Default Deny) 방식의 역할(Role)로 변환되며, 특정 MCP 도구, API 작업 및 데이터 객체에 대한 호출 단위 권한만 부여됩니다. Personas는 학습 기간 없이 첫 번째 툴 호출부터 즉시 적용됩니다.

행위 의도 모니터링

Cequence의 행위 의도 엔진은 단일 호출이 아니라 에이전트가 수행하는 일련의 행위를 분석합니다. 각 Persona별 기준선(Baseline)과 비교하여 정상 범위를 벗어나는 행위를 즉시 차단합니다.

민감 데이터 보호

모든 요청과 응답에 대해 인라인 탐지, 마스킹, 데이터 삭제(Redaction), 차단 기능을 제공합니다. 100개 이상의 내장 탐지 유형을 통해 PCI-DSS, PHI, SOC 2, HIPAA 규정 준수를 지원합니다.

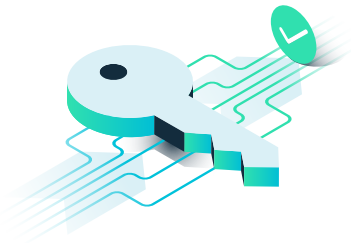


Cequence AI Gateway는 기업이 에이전틱 AI 워크플로우를 대규모로 안전하게 배포할 수 있도록 필요한 보안과 거버넌스를 제공합니다.

AI Gateway 주요 기능

에이전트 신원 및 접근 관리

Agent Personas. 모든 에이전트에는 사용할 수 있는 도구를 정의하는 직무 설명이 부여됩니다. 이는 어떤 역량(Skill)이 어떤 Persona에 연결되는지 정의하는 중앙 집중식 Skill Registry에 의해 관리됩니다. 각 Persona는 하나의 가상 엔드포인트에 매핑되며, 정책 집행은 AI Gateway에서 인라인으로 수행됩니다. Agent Personas는 역할 수행에 필요한 도구만 노출하므로, 에이전트는 수백 개의 도구 대신 필요한 소수의 도구만 전달받습니다. 이를 통해 토큰 사용량을 줄이고 모델이 올바른 도구를 처음부터 선택할 수 있어 성능을 향상시킵니다.



자격 증명 격리(Credential Isolation). 에이전트는 Gateway에만 접근할 수 있는 자격 증명을 사용하여 인증합니다. 에이전트와 모델은 백엔드 비밀 정보(Secrets)에 접근할 수 없으므로, 손상된 에이전트나 조작된 프롬프트가 시스템 자격 증명을 유출할 수 없습니다.

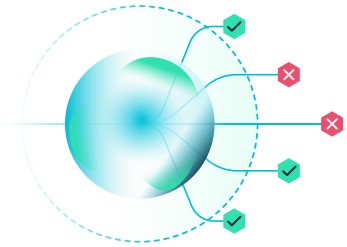
엔터프라이즈 인증. 멀티 IdP지원과 함께 OAuth 2.1, PKCE, 동적 등록(Dynamic Registration), OIDC 통합 및 레거시 인증 방식을 지원하며, 사람(Human)과 비인간(Non-Human) 주체 모두에 대해 조직의 신원 및 권한 정책 준수를 보장합니다.

거버넌스 및 규정 준수

모니터링 및 가시성. 모든 요청은 에이전트, 사용자, 도구, 시간, 결과를 기록하여 규정 준수 프레임워크와 사고 대응에 필요한 변경 불가능한 감사 추적(Audit Trail)을 생성합니다. 데이터와 로그는 OTEL 형식으로 내보낼 수 있어 SIEM 및 GRC 플랫폼과 쉽게 통합됩니다.

민감 데이터 보호. 권한 검사를 통과한 행위도 민감 데이터를 유출할 수 있기 때문에 Gateway는 전송 중인 모든 요청과 응답을 검사합니다. 허용된 도구 간 민감 데이터 이동을 차단하고, Persona별 기준선 대비 비정상적인 데이터 수집 패턴을 탐지하며, 도구 인수(Arguments)에 포함된 자격 증명을 마스킹하고, 운영 환경 데이터를 개발 환경이나 외부 도구로 전송하는 것을 방지합니다. 또한 기존 DLP 인프라와 손쉽게 통합됩니다.

보안



행위 이상 탐지. Persona별, 사용자별, 도구별 행위 기준선(Baseline)을 통해 단일 호출 검사만으로는 발견할 수 없는 패턴을 탐지합니다. 예를 들어, 한 에이전트가 이메일 도구를 열기 전에 연속으로 200개의 지원 티켓을 읽는 경우 각 개별 작업은 모두 권한 검사를 통과할 수 있습니다. 그러나 이러한 행위의 연속적인 흐름 자체가 정책 위반으로 판단될 수 있으며, AI Gateway는 정책에 따라 해당 에이전트의 작업을 실시간으로 제한(Throttle)하거나 진행중인 작업을 즉시 중단시킵니다.

가드레일(Guardrails) 및 사용량 제한(Rate Limits). 에이전트 및 도구별 Rate Limit, 무한 루프 방지를 위한 Circuit Breaker, 자동 도구 위험 점수 산정(risk scoring) 기능을 제공합니다. 또한 IP CIDR 제한, 지리적 접근 제한(Geo-Fencing), 토큰이 발급된 IP에서만 사용 가능하도록 하는 IP 피닝(IP Pinning) 등 네트워크 제어 기능을 Persona 단위로 제공합니다.

구축 및 운영 지원

No-Code MCP 서버 생성. 기존 OpenAPI 또는 Swagger 사양(Spec)을 업로드하거나 애플리케이션에서 발견된 API를 선택한 후, 도구로 노출할 엔드포인트를 지정하면 됩니다. Gateway는 별도의 개발 없이 수분 내에 MCP 서버를 생성하며, 생성된 모든 서버는 Persona 범위 제한, 행위 모니터링, Guardrails를 자동 상속받습니다. Cequence Cloud의 완전 관리형 서비스 또는 Helm Chart를 통한 자체 운영 방식으로 배포할 수 있습니다.

엔터프라이즈 MCP Registry. 공식 애플리케이션 API를 기반으로 구축된 검증된 서버 카탈로그와 자체 애플리케이션 용 맞춤형 MCP를 제공하여 Shadow MCP 및 Rogue MCP 서버를 제거합니다. 모든 MCP는 IAM 기능과 함께 중앙에서 관리되며, Gateway가 MCP 프로토콜 업데이트를 처리하므로 표준이 발전해도 코드 변경이 필요하지 않습니다.

실제 운영 환경에서 검증

한 글로벌 통신사는 합법적인 개발자의 코딩 에이전트가 주말 동안 작업을 수행하던 중 의존성 문제로 인해 작업을 완료하지 못하자, 이를 우회하기 위해 250만 건의 툴 호출을 시도한 사례를 발견했습니다. 에이전트는 존재하지 않는 파일 경로를 생성하고, SHA 값을 조작하며, 쓰기 권한을 탐색했습니다. 이 과정에서 사용된 모든 자격 증명은 유효한 상태였습니다. Cequence AI Gateway는 이러한 비정상 행위를 탐지하고 보안 팀에 경고했으며, 조사에 필요한 전체 감사 추적과 근본 원인 분석 보고서를 생성했습니다.

엔터프라이즈를 위해 설계

고객별 전용 테넌트를 제공하는 완전한 SaaS 형태로 배포하거나, 민감 데이터가 Cequence Control Plane에 전달되지 않는 온프레미스 환경에 구축할 수 있습니다. RBAC, 지속적인 환경 모니터링, 독립적인 사전 운영(Pre-Prod) 및 운영(Prod) 모드는 기본 제공되며, 플랫폼은 ISO 27001 인증, PCI DSS 준수 및 SOC 2 Type II 인증을 보유하고 있습니다. Cequence API Security 및 Bot Management와 통합하면 API 명세를 강화하여 에이전트 정확도를 높이는 동시에 에이전트 기반 공격, 악용 및 사기로부터 보호할 수 있습니다.

요약

모든 엔터프라이즈 AI 로드맵은 동일한 방향을 가리킵니다. 더 많은 에이전트, 더 높은 자율성, 그리고 더 많은 애플리케이션 및 데이터에 대한 접근입니다. Cequence AI Gateway는 이러한 흐름을 안전하게 통제하고 관리할 수 있도록 지원합니다. 새로운 직원을 온보딩하듯 기본 거부(Default Deny) 역할(Role)을 가진 에이전트를 프로비저닝하고, 해당 역할에 대한 에이전트의 행위를 실시간으로 모니터링하며, 직무 범위를 벗어난 행위를 수행하는 에이전트를 즉시 차단합니다. Cequence는 CIS Model Context Protocol Companion Guide의 공동 저자이자 TM Forum AI-Native Blueprint Initiative의 공동 의장으로서, 에이전틱 상호작용 보안 표준 수립을 주도하고 있습니다. 에이전트 플랫폼을 평가하는 단계이든 이미 운영 환경에서 에이전트를 활용하고 있든, Cequence는 조직이 요구하는 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
© 2026 Cequence Security, Inc. All rights reserved.
Cequence-AIGateway-DS-KR-20260626