

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 AI 에이전트를 인증한 후, 에이전트가 수행하는 모든 작업을 지속적으로 권한 부여합니다. 게이트웨이는 요청 경로에서 정책을 인라인으로 적용하며, 세션 전체에 걸쳐 모든 툴 호출(tool call)에 대해 정책을 강제합니다. Dr. Chase Cunningham과 Anthropic은 각각 독립적으로 이러한 접근 방식을 올바른 아키텍처로 제시했으며, 이는 Cequence가 이미 구축해 온 동일한 아키텍처입니다.



Agent Personas 기반 최소 권한 접근 제어

일상적인 언어로 작성된 직무 설명을 기반으로 에이전트가 실제로 필요한 특정 도구, API 호출, LLM, 스킬 및 데이터에만 액세스하도록 보장하며, 그 밖의 모든 항목에 대한 액세스는 제한됩니다. 페르소나는 별도의 학습 기간 없이 첫 번째 도구 호출부터 즉시 작동합니다.



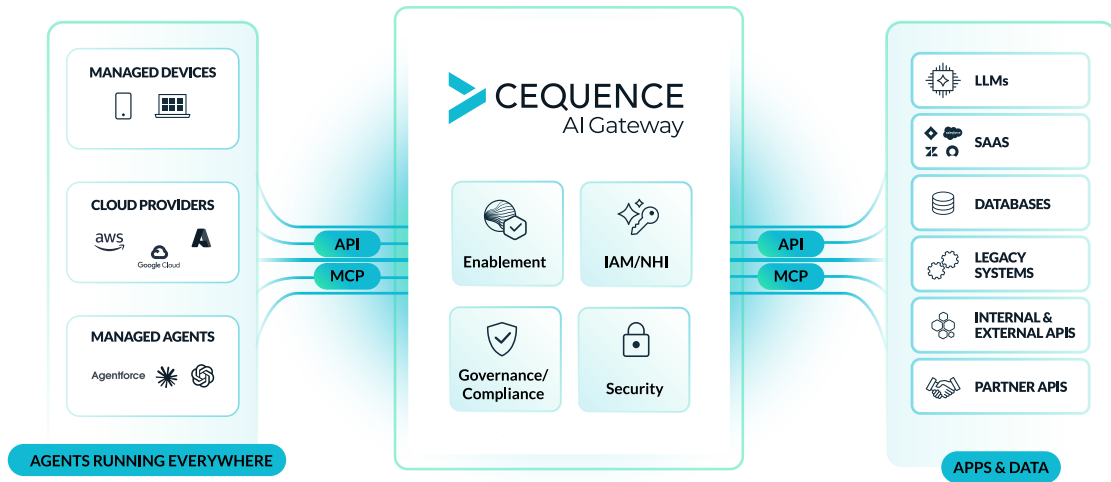
행위 의도 모니터링

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.

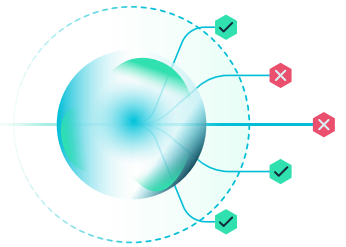


Cequence AI Gateway는 기업이 에이전틱 AI 워크플로우를 대규모로 안전하게 배포할 수 있도록 필요한 보안과 거버넌스를 제공합니다.

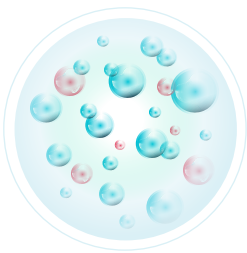
AI Gateway 주요 기능

에이전틱 AI 거버넌스

에이전트 페르소나. 각 에이전트에는 도구 액세스 권한을 결정하는 직무 설명이 부여되며, 어떤 스킬을 어떤 페르소나에 연결할지 정의하는 중앙 집중식 스킬 레지스트리를 통해 관리됩니다. 각 페르소나는 하나의 가상 엔드포인트에 매핑되고, 정책은 AI 게이트웨이에서 인라인으로 적용됩니다. 에이전트 페르소나는 직무 수행에 필요한 도구, API, LLM, 스킬 및 권한만 노출합니다. 따라서 에이전트는 요청마다 수백 개의 항목을 전달받는 대신, 간결하고 관련성 높은 목록만 받게 됩니다. 이를 통해 토큰 소비를 줄이고 모델이 처음부터 적절한 도구를 선택할 수 있도록 하여 성능을 향상합니다.



민감 데이터 보호. 많은 작업은 권한 검사를 통과하더라도 민감한 데이터를 유출할 수 있습니다. AI Gateway는 실행 시점 (Runtime)에 모든 AI 에이전트의 요청과 응답을 검사합니다. 100개 이상의 기본 제공 탐지 유형을 활용하여 민감 데이터를 모니터링하고, 마스킹하며, 차단할 수 있습니다. 또한 기존 DLP 인프라와 손쉽게 통합됩니다.

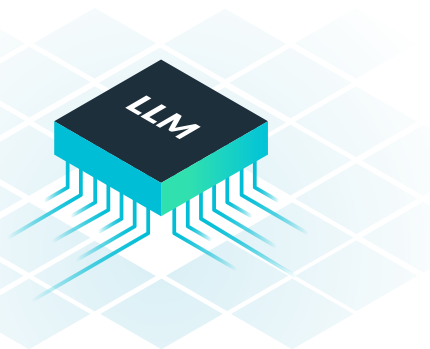


AI 탐지. 인지하고 있는 대상만 거버넌스할 수 있습니다. Cequence는 기존 에이전트 및 AI 사용 현황에 대한 가시성을 제공하며, 승인된 AI뿐 아니라 섀도우 AI(Shadow AI)까지 모두 발견합니다. 기존 SIEM 로그를 활용하여 조직 전반의 모든 에이전트, MCP 서버 및 LLM 제공업체를 식별합니다.

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

엔터프라이즈 MCP 및 API 레지스트리. MCP 레지스트리는 공식 애플리케이션 API와 자체 애플리케이션용 맞춤형 MCP를 기반으로 구축된 검증된 MCP 서버를 신뢰할 수 있는 중앙 카탈로그로 제공합니다. 모든 서버는 IAM 기능을 통해 중앙에서 프로비저닝됩니다. AI Gateway는 MCP 프로토콜의 변경 사항을 처리하므로 표준이 발전하더라도 코드 변경이 필요하지 않습니다. API 레지스트리를 통해 에이전트는 원본 시스템의 자격 증명을 보유하지 않고도 승인된 비즈니스 시스템을 호출할 수 있습니다.

LLM 레지스트리 및 프롬프트 보호. LLM 레지스트리는 승인된 각 LLM 제공업체에 대한 통제된 연결을 제공하고, 자격 증명과 모델 액세스를 관리하며, 토큰 사용량 및 지출 한도를 적용합니다. 프롬프트 가드는 탈옥 및 시스템 프롬프트 추출 패턴을 포함한 프롬프트 인젝션 공격이 모델에 도달하기 전에 차단합니다.



보안

행위 이상 탐지. 페르소나별, 사용자별, 도구별 행위 기준선을 구축하여 단일 요청 검사만으로는 발견할 수 없는 이상 패턴을 탐지합니다. 예를 들어 에이전트가 이메일 도구를 열기 전에 200개의 티켓을 연속으로 읽는 경우, 각각의 권한 검사는 모두 통과할 수 있습니다. 그러나 문제는 개별 요청이 아니라 이러한 행위의 순서이며, AI Gateway는 정책에 따라 실행 중인 작업을 제한하거나 즉시 중단할 수 있습니다.

보호 정책 및 속도 제한. 에이전트별·도구별 속도 제한, 무한 루프를 방지하는 회로 차단기(Circuit Breaker), 자동 도구 위험도 평가, 그리고 IP CIDR 제한, 지리적 접근 제한(Geo-fencing), IP 고정(IP Pinning) 등의 네트워크 제어 기능을 제공합니다. IP 고정은 각 페르소나에 대해 발급된 토큰이 발급 당시의 IP 주소에서만 사용되도록 강제합니다.



자격 증명 격리. 에이전트는 AI Gateway에만 접근 권한을 부여하는 자격 증명을 사용하여 인증합니다. 에이전트와 모델은 모두 백엔드 비밀 정보(Secrets)에 접근할 수 없으므로, 에이전트가 침해되거나 프롬프트가 조작되더라도 시스템 자격 증명에 노출되지 않습니다.

엔터프라이즈 인증. 다중 IdP 지원, OAuth 2.1, PKCE, 동적 등록(Dynamic Registration), OIDC 통합 및 레거시 인증 방식을 지원하여 사람과 비사람(Non-Human Identity) 모두에 대해 조직의 ID 정책을 일관되게 적용합니다.

활성화

노코드 MCP 서버 생성. 기존 OpenAPI 또는 Swagger 명세를 업로드하거나 검색된 애플리케이션 API를 선택한 후, 도구로 노출할 엔드포인트를 지정하면 됩니다. AI Gateway는 몇 분 안에 코딩 없이 MCP 서버를 생성하며, 생성된 모든 서버는 페르소나 범위 지정, 행위 모니터링 및 보호 정책을 자동으로 상속받습니다. Cequence Cloud에서 완전 관리형으로 배포하거나 Helm Chart를 사용하여 자체 관리형으로 배포할 수 있습니다.



기술 레지스트리. 기술 레지스트리는 기업에서 승인한 지침과 운영 패턴을 배포하기 위한 중앙 카탈로그를 제공합니다. 이를 통해 에이전트는 승인된 기술(Skill)을 보다 쉽게 활용할 수 있으며, 조직은 에이전트의 작업을 추적하고 감사할 수 있습니다.

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 톨 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, 에이전트 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.