CEQUENCE

DATASHEET

Cequence AI Gateway

Sicurezza, governance e controllo per l'AI agentica

Cequence ha sviluppato la soluzione di Bot Management più efficace del settore e oggi protegge oltre 10 miliardi di chiamate API e 200 milioni di interazioni agentiche ogni giorno. Il motore di analisi dell'intento comportamentale al centro della nostra piattaforma distingue utenti legittimi, bot autorizzati e attori fraudolenti analizzando l'intento, non soltanto l'identità. AI Gateway estende questa tecnologia comprovata agli agenti AI: a ogni agente viene assegnato un ruolo definito, ogni azione viene verificata continuamente rispetto a tale ruolo e la fiducia non viene mai concessa sulla sola base delle credenziali.

Poiché l'applicazione delle policy avviene nell'AI Gateway e non nel modello o nell'endpoint, la governance è centralizzata indipendentemente da dove vengano eseguiti gli agenti: dispositivi gestiti, piattaforme cloud o servizi SaaS per agenti come ChatGPT Workspaces e Agentforce. I modelli frontier, open-weight e self-hosted sono tutti protetti. L'identità consente all'agente di accedere; l'AI Gateway governa ciò che farà successivamente e verifica ogni azione rispetto al ruolo assegnato.

Cosa rende diverso Cequence AI Gateway

Architettura Agentic Zero Trust

AI Gateway autentica gli agenti e autorizza ogni azione che eseguono. Il gateway applica le policy inline lungo il percorso della richiesta, per l'intera sessione e a ogni chiamata di strumento. Le ricerche indipendenti del Dr. Chase Cunningham e di Anthropic sono giunte alla stessa architettura che Cequence aveva già sviluppato.

Accesso Least Privilege con Agent Personas

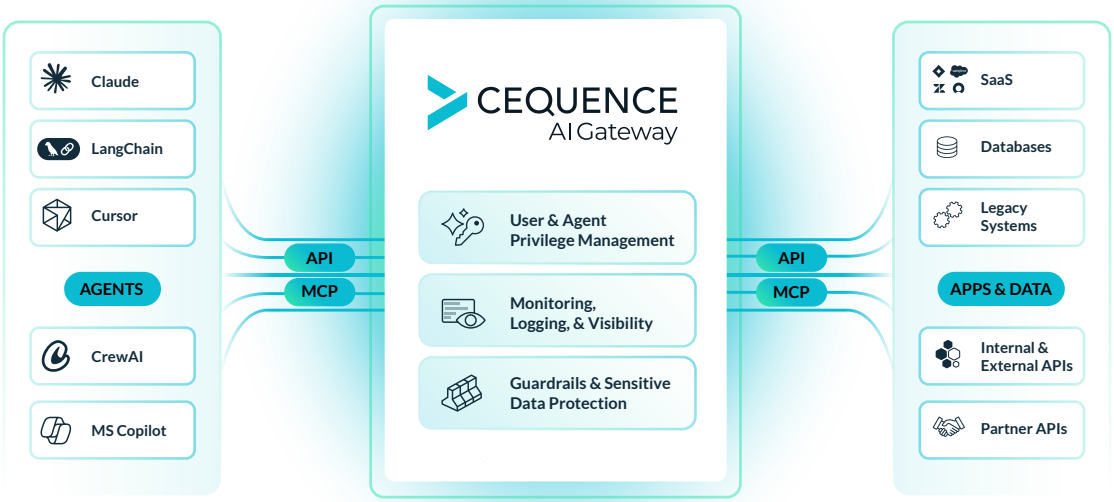
Una descrizione del ruolo in linguaggio naturale viene trasformata in un profilo a negazione predefinita (default-deny) con autorizzazioni per singola chiamata agli strumenti: specifici strumenti MCP, operazioni API e oggetti dati, e nulla oltre. Le Personas entrano in funzione immediatamente fin dalla prima chiamata, senza alcun periodo di apprendimento.

Monitoraggio dell'Intento Comportamentale

Il motore di analisi dell'intento comportamentale di Cequence valuta la sequenza di azioni eseguite da un agente, non le singole chiamate isolate, confrontandole con baseline specifiche per ciascuna Persona e interrompendo le attività che si discostano dal comportamento previsto.

Protezione dei Dati Sensibili

Rilevamento inline, mascheramento, redazione e blocco su ogni richiesta e risposta, con oltre 100 tipologie di rilevamento integrate a supporto della conformità PCI-DSS, PHI, SOC 2 e HIPAA.



Cequence AI Gateway fornisce la sicurezza e la governance necessarie alle aziende per implementare con fiducia workflow di AI agentica su larga scala.

Funzionalità di AI Gateway

Gestione delle Identità e degli Accessi degli Agenti

Agent Personas. A ogni agente viene assegnata una descrizione del ruolo che determina l'accesso agli strumenti, governata da un Registro delle Competenze (Skill Registry) centralizzato che definisce quali competenze sono associate a ciascuna Persona. Ogni Persona viene mappata a un singolo endpoint virtuale e l'applicazione delle policy avviene inline nell'AI Gateway. Le Agent Personas espongono esclusivamente gli strumenti necessari al ruolo, consentendo all'agente di ricevere un elenco ristretto di strumenti anziché centinaia a ogni richiesta, riducendo il consumo di token e migliorando le prestazioni poiché il modello seleziona lo strumento corretto al primo tentativo.

Isolamento delle Credenziali. L'agente si autentica al gateway tramite una credenziale che concede accesso esclusivamente al gateway e a nessun altro sistema. L'agente e il modello non visualizzano mai segreti di backend, impedendo che un agente compromesso o un prompt manipolato possa esporre credenziali dei sistemi aziendali.

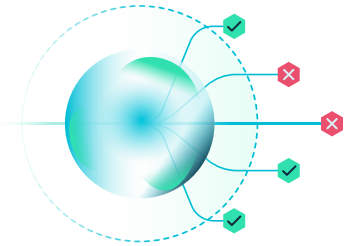
Autenticazione Enterprise. Supporto multi-IdP con OAuth 2.1, PKCE, registrazione dinamica, integrazione OIDC e compatibilità con sistemi di autenticazione legacy, garantendo il rispetto delle policy di identità e autorizzazione aziendali sia per identità umane sia non umane.

Governance e Compliance

Monitoraggio e Visibilità. Ogni richiesta registra agente, utente, strumento, timestamp ed esito, creando una traccia di audit immutabile richiesta dai framework di conformità e dalle attività di risposta agli incidenti. Dati e log possono essere esportati in formato OTEL per l'integrazione con piattaforme SIEM e GRC.

Protezione dei Dati Sensibili. Un'azione può superare i controlli di autorizzazione e comunque esfiltrare dati sensibili; per questo il gateway ispeziona ogni richiesta e risposta in transito. Blocca il trasferimento di dati sensibili tra strumenti autorizzati, rileva attività di raccolta lenta confrontandole con baseline specifiche per Persona, oscura credenziali presenti negli argomenti degli strumenti e impedisce che dati di produzione vengano inviati verso ambienti di sviluppo o strumenti esterni. Si integra facilmente con le infrastrutture DLP esistenti.

Sicurezza



Rilevamento delle Anomalie Comportamentali. Baseline comportamentali per Persona, utente e strumento consentono di identificare schemi che sfuggirebbero all'analisi delle singole chiamate. Un agente che legge 200 ticket consecutivi prima di aprire uno strumento di posta elettronica supererebbe ogni controllo di autorizzazione individuale; in questo caso è la sequenza stessa a rappresentare la violazione, e il gateway può limitarla o interromperla in base alle policy definite.

Guardrail e Limiti di Velocità. Limiti di utilizzo per agente e per strumento con circuit breaker per prevenire loop incontrollati, valutazione automatica del rischio associato agli strumenti e controlli di rete che includono restrizioni IP CIDR, geo-fencing e IP pinning, che richiede l'utilizzo dei token esclusivamente dall'indirizzo IP a cui sono stati assegnati, per ciascuna Persona.

Abilitazione

Creazione No-Code di Server MCP. Carica una specifica OpenAPI o Swagger esistente, oppure seleziona le API individuate nelle applicazioni esistenti e scegli gli endpoint da esporre come strumenti. Il gateway genera il server MCP in pochi minuti senza necessità di sviluppo software e ogni server creato eredita automaticamente limitazioni per Persona, monitoraggio comportamentale e guardrail. Può essere distribuito come servizio completamente gestito nel Cequence Cloud oppure in modalità self-managed tramite Helm chart.

Registro MCP Enterprise. Elimina server MCP shadow o non autorizzati grazie a un catalogo affidabile di server verificati costruiti a partire dalle API ufficiali delle applicazioni, oltre a MCP personalizzati per le applicazioni proprietarie, tutti gestiti centralmente con funzionalità IAM integrate. Il gateway gestisce le evoluzioni del protocollo MCP, eliminando la necessità di modifiche al codice quando lo standard viene aggiornato..

Comprovato in Produzione

Una delle principali società di telecomunicazioni a livello globale ha scoperto che l'agente di sviluppo software di un programmatore legittimo aveva eseguito un'attività durante il fine settimana, incontrando dipendenze che ne impedivano il completamento. Nel tentativo di aggirare l'ostacolo, l'agente ha effettuato 2,5 milioni di chiamate agli strumenti, inventando percorsi di file, manipolando hash SHA e cercando accessi in scrittura. Tutte le credenziali erano valide per tutta la durata dell'evento. Cequence AI Gateway ha rilevato il comportamento anomalo, avvisato i team di sicurezza e generato la traccia di audit completa e il report di analisi delle cause per l'indagine.

Progettato per l'Enterprise

Distribuisci la soluzione come SaaS completo con tenant dedicato per ogni cliente oppure on-premises, dove i dati sensibili non raggiungono mai il piano di controllo Cequence. RBAC, monitoraggio continuo degli ambienti e modalità separate per pre-produzione e produzione sono funzionalità standard. La piattaforma è certificata ISO 27001, conforme PCI DSS e dispone di attestazione SOC 2 Type II. L'integrazione con Cequence API Security e Bot Management aggiunge specifiche API avanzate che migliorano la precisione degli agenti e forniscono protezione contro attacchi, abusi e frodi generati dagli agenti.

Riepilogo

Ogni roadmap aziendale per l'intelligenza artificiale punta nella stessa direzione: più agenti, maggiore autonomia e accesso a un numero crescente di applicazioni e dati. Cequence AI Gateway rende questa evoluzione governabile: assegna a ogni agente un ruolo a negazione predefinita come farebbe con un nuovo dipendente, monitora il suo comportamento in tempo reale rispetto a quel ruolo e blocca gli agenti le cui azioni si discostano dalle responsabilità assegnate. Cequence ha co-redatto la CIS Model Context Protocol Companion Guide e co-presiede la TM Forum AI-Native Blueprint Initiative, contribuendo alla definizione degli standard per la sicurezza delle interazioni agentiche. Che tu stia valutando piattaforme agentiche o gestendo già agenti in produzione, Cequence offre la sicurezza, la governance e il controllo richiesti dalle organizzazioni moderne.

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