

Cequence AI Gateway

Sicurezza, governance e controllo per l'AI agentic

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 singola azione che eseguono. Il gateway applica le policy direttamente nel percorso della richiesta, per l'intera durata della sessione e a ogni chiamata di strumento (tool call). Il Dr. Chase Cunningham e Anthropic hanno descritto indipendentemente questo come l'approccio corretto; è la stessa architettura che Cequence aveva già realizzato.



Accesso Least Privilege con Agent Personas

Una descrizione del ruolo formulata in un linguaggio semplice garantisce che gli agenti possano accedere esclusivamente agli strumenti, alle chiamate API, agli LLM, alle competenze e ai dati specifici di cui hanno effettivamente bisogno; tutto il resto rimane inaccessibile. Le persona sono operative fin dalla prima chiamata a uno strumento, senza alcun periodo di apprendimento.



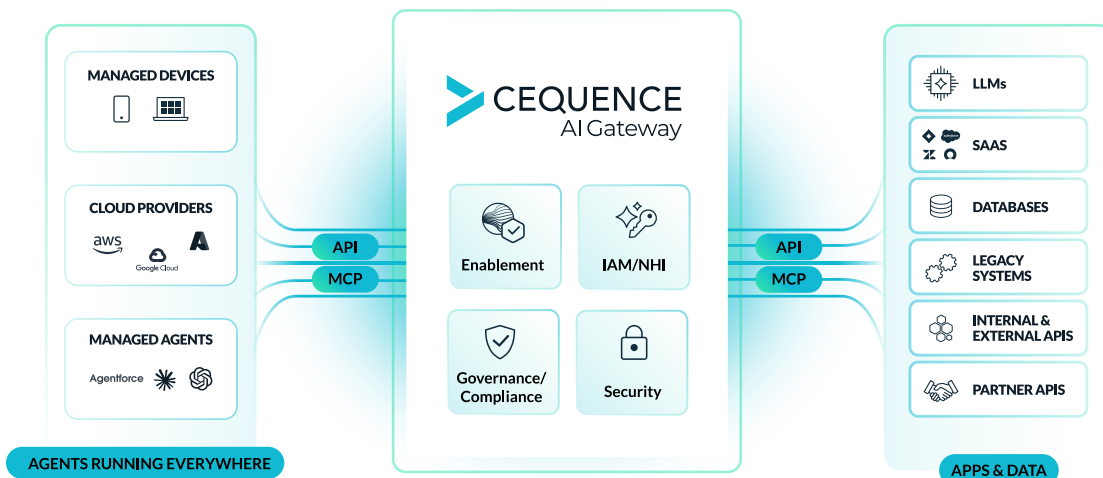
Monitoraggio dell'Intento Comportamentale

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.

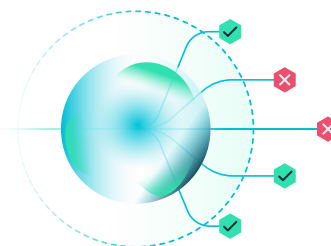


Cequence AI Gateway fornisce la sicurezza e la governance necessarie alle aziende per implementare con fiducia workflow di AI agentica su larga scala.

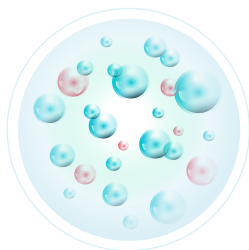
Funzionalità di AI Gateway

Governance dell'AI Agentica

Personas degli Agenti. A ogni agente viene assegnata una descrizione del ruolo che determina l'accesso agli strumenti, regolato da uno Skill Registry centralizzato che definisce quali competenze sono associate a ciascuna persona. Ogni persona è collegata a un singolo endpoint virtuale e i controlli vengono applicati in linea a livello dell'AI Gateway. Le Agent Persona espongono esclusivamente gli strumenti, le API, gli LLM, le competenze e le autorizzazioni richiesti dal ruolo. In questo modo, l'agente riceve un elenco breve e pertinente, anziché centinaia di opzioni a ogni richiesta, riducendo il consumo di token e migliorando le prestazioni, poiché il modello seleziona lo strumento corretto fin dal primo tentativo.



Protezione dei Dati Sensibili. Molte azioni superano i controlli delle autorizzazioni e possono comunque causare l'esfiltrazione di dati sensibili. Per questo motivo, AI Gateway ispeziona ogni richiesta e risposta degli agenti AI in fase di esecuzione. Monitora, maschera e blocca i dati sensibili utilizzando oltre 100 tipi di rilevamento predefiniti. Si integra facilmente con l'infrastruttura DLP esistente.

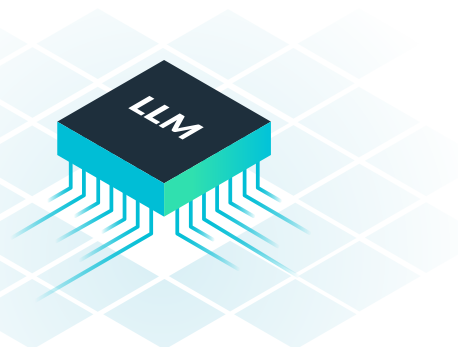


Rilevamento dell'AI. È possibile governare solo ciò di cui si è consapevoli. Cequence offre visibilità sull'utilizzo esistente di agenti e AI, individuando sia le implementazioni autorizzate sia la Shadow AI. Rileva tutti gli agenti, i server MCP e i provider LLM presenti nell'intera organizzazione utilizzando i log SIEM esistenti.

Monitoraggio e Visibilità. Ogni richiesta registra l'agente, l'utente, lo strumento utilizzato, l'orario e il risultato, producendo una traccia di audit completa richiesta dai framework di conformità e dai processi di risposta agli incidenti. Dati e log possono essere esportati in formato OTEL per l'integrazione con piattaforme SIEM e GRC.

Registri Enterprise MCP e API. Il Registro MCP fornisce un catalogo affidabile di server MCP verificati, creati sia dalle API ufficiali delle applicazioni sia da MCP personalizzati per le proprie applicazioni, tutti gestiti centralmente con funzionalità IAM. AI Gateway gestisce l'evoluzione del protocollo MCP, eliminando la necessità di modifiche al codice quando lo standard viene aggiornato. Il Registro API consente agli agenti di accedere ai sistemi aziendali approvati senza conservare le credenziali di origine.

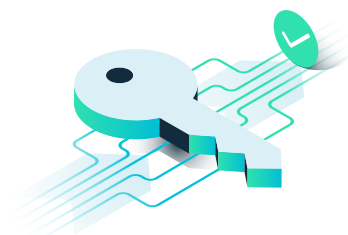
Registro LLM e Protezione dei Prompt. L'LLM Registry fornisce una connessione regolamentata a ciascun provider di LLM approvato, gestisce le credenziali e l'accesso ai modelli e applica limiti alla frequenza di utilizzo dei token e alla spesa. Prompt Guard protegge dagli attacchi di prompt injection, inclusi i pattern di jailbreak e di estrazione del prompt di sistema, prima che raggiungano il modello.



Sicurezza

Rilevamento delle Anomalie Comportamentali. Baseline comportamentali per persona, utente e strumento consentono di individuare schemi che l'analisi delle singole richieste non è in grado di rilevare. Ad esempio, un agente che legge 200 ticket consecutivi prima di aprire uno strumento di posta elettronica può superare ogni singolo controllo delle autorizzazioni; tuttavia, è la sequenza delle azioni a rappresentare la violazione. AI Gateway può limitare o interrompere l'azione in tempo reale in base ai criteri definiti.

Guardrail e Limiti di Velocità. Limiti di velocità per agente e per strumento, circuit breaker per arrestare i loop fuori controllo, valutazione automatica del rischio degli strumenti e controlli di rete che includono restrizioni IP CIDR, geofencing e IP pinning, che impone l'utilizzo dei token esclusivamente dall'indirizzo IP al quale sono stati emessi, in base alla persona.



Isolamento delle Credenziali. L'agente si autentica su AI Gateway utilizzando una credenziale che concede l'accesso esclusivamente al gateway. Né l'agente né il modello hanno accesso ai segreti del backend, impedendo che un agente compromesso o un prompt manipolato possano esporre le credenziali dei sistemi aziendali.

Autenticazione Enterprise. Supporto per più provider di identità (IdP), OAuth 2.1, PKCE, registrazione dinamica, integrazione OIDC e meccanismi di autenticazione legacy, applicando le policy di identità dell'organizzazione sia alle identità umane sia a quelle non umane.

Abilitazione

Creazione di Server MCP Senza Codice. Carica una specifica OpenAPI o Swagger esistente oppure seleziona tra le API delle applicazioni individuate gli endpoint da esporre come strumenti. AI Gateway genera un server MCP in pochi minuti senza richiedere codice e ogni server creato eredita automaticamente l'ambito delle personas, il monitoraggio comportamentale e i guardrail. È possibile distribuire la soluzione completamente gestita su Cequence Cloud oppure in modalità self-managed tramite un chart Helm.



Registro delle Skill. Il Registro delle Skill fornisce un catalogo centrale per distribuire istruzioni e modelli operativi approvati dall'azienda. Consente agli agenti di utilizzare più facilmente le skill approvate e permette all'organizzazione di tracciare e verificare le azioni eseguite dagli agenti AI.

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

Distribuisce 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.