CEQUENCE

DATASHEET

Cequence AI Gateway

Segurança, governança e controle para IA agentiva

A Cequence desenvolveu a solução de gerenciamento de bots mais eficaz do mercado e atualmente protege mais de 10 bilhões de chamadas de API e 200 milhões de interações agentivas todos os dias. O mecanismo de intenção comportamental que está no centro da nossa plataforma diferencia usuários legítimos, bots autorizados e agentes maliciosos analisando a intenção, e não apenas a identidade. O AI Gateway estende essa tecnologia comprovada aos agentes de IA: cada agente recebe uma função claramente definida, cada ação é continuamente validada em relação a essa função e a confiança nunca é concedida apenas com base em uma credencial.

Como a aplicação das políticas acontece no AI Gateway, e não no modelo ou no endpoint, a governança permanece centralizada independentemente de onde os agentes estejam sendo executados: dispositivos gerenciados, plataformas em nuvem ou serviços SaaS de agentes, como ChatGPT Workspaces e Agentforce. Modelos frontier, open-weight e auto-hospedados são todos protegidos. A identidade permite que o agente entre; o AI Gateway governa o que ele pode fazer em seguida e verifica cada ação de acordo com sua função.

O que diferencia o Cequence AI Gateway

Arquitetura Agentic Zero Trust

O AI Gateway autentica agentes e, em seguida, autoriza cada ação que eles executam. O gateway aplica políticas inline no caminho da requisição, durante toda a sessão e em cada chamada de ferramenta. Pesquisas independentes do Dr. Chase Cunningham e da Anthropic chegaram à mesma arquitetura que a Cequence já havia desenvolvido.

Acesso de Privilégio Mínimo com Agent Personas

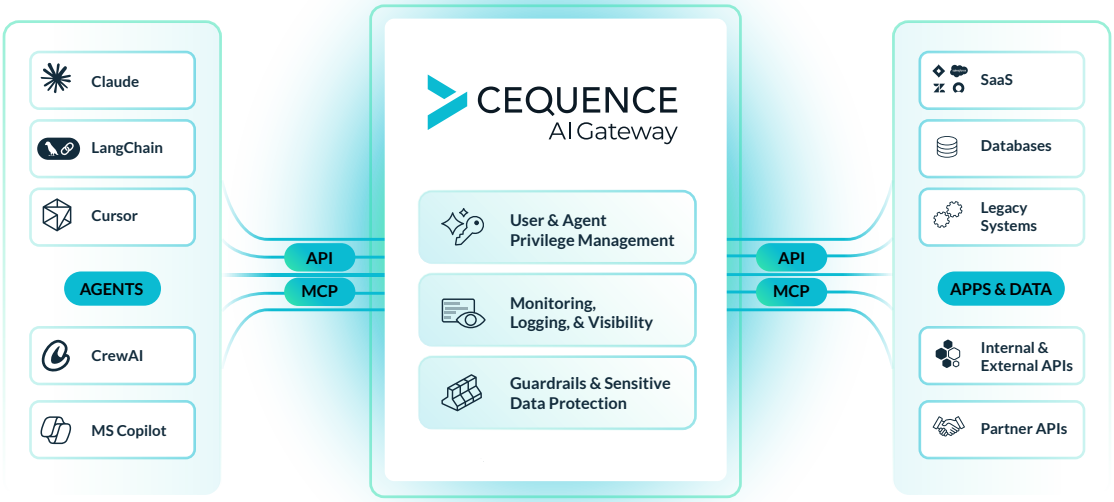
Uma descrição de função em linguagem natural é transformada em um papel de negação por padrão (default deny), com permissões definidas para cada chamada de ferramenta: ferramentas MCP específicas, operações de API e objetos de dados autorizados, e nada além disso. As Personas entram em vigor imediatamente desde a primeira chamada de ferramenta, sem necessidade de período de aprendizado.

Monitoramento de Intenção Comportamental

O mecanismo de intenção comportamental da Cequence analisa a sequência de ações executadas por um agente, e não apenas chamadas isoladas, comparando-as com linhas de base específicas para cada Persona e interrompendo ações que se desviam do comportamento esperado.

Proteção de Dados Sensíveis

Detecção, mascaramento, redação e bloqueio inline em todas as requisições e respostas, com mais de 100 tipos de detecção integrados para apoiar conformidade com PCI-DSS, PHI, SOC 2 e HIPAA.



O Cequence AI Gateway fornece a segurança e a governança necessárias para que empresas implementem workflows de IA agentiva com confiança e em escala.

Recursos do AI Gateway

Gerenciamento de Identidade e Acesso para Agentes

Agent Personas. Cada agente recebe uma descrição de função que determina seu acesso a ferramentas, governada por um Skill Registry centralizado que define quais capacidades são associadas a quais Personas. Cada Persona é vinculada a um endpoint virtual único e a aplicação das políticas acontece inline no AI Gateway. As Agent Personas expõem apenas as ferramentas necessárias para a função desempenhada, permitindo que o agente receba uma lista reduzida de ferramentas em vez de centenas em cada requisição. Isso reduz o consumo de tokens e melhora o desempenho ao permitir que o modelo selecione a ferramenta correta logo na primeira tentativa.

Isolamento de Credenciais. O agente se autentica no gateway usando uma credencial que concede acesso apenas ao próprio gateway. Nem o agente nem o modelo têm acesso a segredos de backend, impedindo que um agente comprometido ou um prompt manipulado exponha credenciais dos seus sistemas.

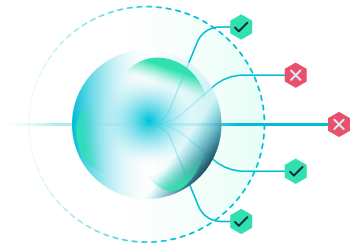
Autenticação Empresarial. Suporte a múltiplos provedores de identidade (IdPs), OAuth 2.1, PKCE, registro dinâmico, integração OIDC e mecanismos legados de autenticação, garantindo conformidade com as políticas corporativas de identidade e autorização para identidades humanas e não humanas.

Governança e Conformidade

Monitoramento e Visibilidade. Cada requisição registra o agente, usuário, ferramenta, horário e resultado, criando uma trilha de auditoria imutável exigida por estruturas de conformidade e processos de resposta a incidentes. Dados e logs podem ser exportados em formato OTEL para integração com plataformas SIEM e GRC.

Proteção de Dados Sensíveis. Uma ação pode passar pelas verificações de permissão e ainda assim exfiltrar dados sensíveis. Por isso, o gateway inspeciona todas as requisições e respostas em trânsito. Ele bloqueia a movimentação de dados sensíveis entre ferramentas autorizadas, identifica padrões de coleta gradual de informações comparando-os às linhas de base de cada Persona, mascara credenciais presentes em argumentos de ferramentas e impede que dados de produção sejam enviados para ambientes de desenvolvimento ou ferramentas externas. Integra-se facilmente às infraestruturas DLP existentes.

Segurança



Detecção de Anomalias Comportamentais. Linhas de base comportamentais por Persona, usuário e ferramenta permitem identificar padrões que inspeções de chamadas individuais não conseguem detectar. Um agente que leia 200 tickets consecutivos antes de abrir uma ferramenta de e-mail passaria por todas as verificações de permissão individualmente. Nesse caso, a sequência de ações é a própria violação, e o gateway pode limitar ou interromper a atividade de acordo com as políticas definidas.

Guardrails e Limites de Taxa. Limites de utilização por agente e por ferramenta, circuit breakers para impedir loops descontrolados, avaliação automatizada de risco de ferramentas e controles de rede que incluem restrições IP CIDR, geofencing e IP pinning, exigindo que tokens sejam utilizados apenas a partir do endereço IP para o qual foram emitidos, de acordo com cada Persona.

Habilitação

Criação de Servidores MCP Sem Código. Faça upload de uma especificação OpenAPI ou Swagger existente, ou selecione APIs descobertas em suas aplicações, e escolha quais endpoints deseja expor como ferramentas. O gateway gera um servidor MCP em minutos, sem necessidade de desenvolvimento, e cada servidor herda automaticamente controles de Persona, monitoramento comportamental e guardrails. Implante em modo totalmente gerenciado no Cequence Cloud ou em modo autogerenciado por meio de um Helm chart.

Registro Empresarial de MCP. Elimine servidores MCP não autorizados ou fora de governança com um catálogo confiável de servidores validados construídos a partir de APIs oficiais de aplicações, além de MCPs personalizados para seus próprios sistemas, todos provisionados centralmente com recursos de IAM. O gateway gerencia atualizações e revisões do protocolo MCP, eliminando a necessidade de alterações de código à medida que o padrão evolui.

Comprovado em Produção

Uma grande operadora global de telecomunicações identificou que o agente de desenvolvimento de software de um desenvolvedor legítimo executou uma tarefa durante o fim de semana, encontrou dependências que impediram sua conclusão e, em seguida, realizou 2,5 milhões de chamadas de ferramentas tentando contornar o bloqueio. O agente criou caminhos de arquivos fictícios, manipulou hashes SHA e buscou permissões de escrita. Todas as credenciais permaneceram válidas durante todo o processo. O Cequence AI Gateway detectou o comportamento anômalo, alertou as equipes de segurança e gerou a trilha de auditoria completa e o relatório de análise de causa raiz necessários para a investigação.

Desenvolvido para Empresas

Implante a plataforma como SaaS completo com um tenant dedicado para cada cliente ou em ambiente on-premises, onde dados sensíveis nunca deixam sua infraestrutura. Controle de acesso baseado em funções (RBAC), monitoramento contínuo de ambientes e modos separados para pré-produção e produção estão incluídos como recursos padrão. A plataforma possui certificação ISO 27001, conformidade com PCI DSS e atestado SOC 2 Tipo II. A integração com Cequence API Security e Bot Management adiciona especificações de API enriquecidas que aumentam a precisão dos agentes e oferecem proteção contra ataques, abusos e fraudes impulsionados por agentes.

Resumo

Todos os roadmaps corporativos de inteligência artificial apontam para a mesma direção: mais agentes, mais autonomia e acesso a mais aplicações e dados. O Cequence AI Gateway torna essa evolução governável. Cada agente é provisionado como uma nova contratação, com um papel de negação por padrão, seu comportamento é monitorado em tempo real em relação a esse papel e agentes cujas ações se desviam da função atribuída são imediatamente interrompidos. A Cequence é coautora do CIS Model Context Protocol Companion Guide e copreside a iniciativa AI-Native Blueprint do TM Forum, contribuindo para definir os padrões de segurança para interações agentivas. Esteja você avaliando plataformas de agentes ou já operando agentes em produção, a Cequence oferece a segurança, a governança e o controle que as organizações exigem.

CEQUENCE

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