

Cequence AI Gateway

Segurança, governança e controle para IA agêntica

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 agênticas 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 os agentes e, em seguida, autoriza cada ação que eles executam. O gateway aplica as políticas diretamente no caminho da solicitação, durante toda a sessão e em cada chamada de ferramenta (tool call). O Dr. Chase Cunningham e a Anthropic descreveram, de forma independente, essa abordagem como a correta; é a mesma arquitetura que a Cequence já havia desenvolvido.



Acesso de Privilégio Mínimo com Agent Personas

Uma descrição da função em linguagem simples garante que os agentes tenham acesso apenas às ferramentas, chamadas de API, LLMs, habilidades e dados específicos de que realmente precisam — todo o restante permanece fora de alcance. As personas funcionam imediatamente, desde a primeira chamada de ferramenta, sem a necessidade de um período de aprendizado.



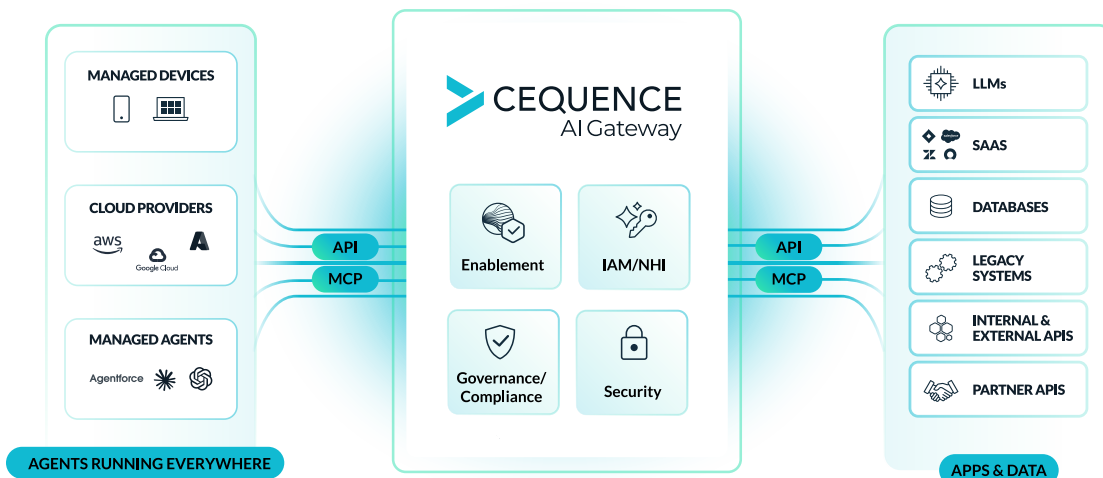
Monitoramento de Intenção Comportamental

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

Deteção, 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.

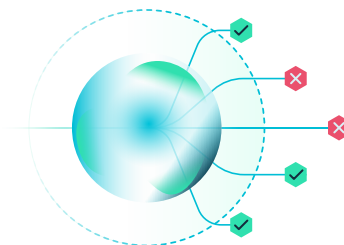


O Cequence AI Gateway fornece a segurança e a governança necessárias para que empresas implementem workflows de IA agêntica com confiança e em escala.

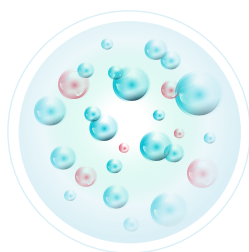
Recursos do AI Gateway

Governança de IA Agêntica

Personas de Agente. Cada agente recebe uma descrição da função que determina seu acesso às ferramentas, gerenciado por um Registro de Habilidades centralizado que define quais habilidades estão vinculadas a cada persona. Cada persona é associada a um único endpoint virtual, e as políticas são aplicadas em tempo real no AI Gateway. As Personas de Agentes disponibilizam apenas as ferramentas, APIs, LLMs, habilidades e permissões exigidas pela função. Assim, o agente recebe uma lista curta e relevante, em vez de centenas de opções em cada solicitação, reduzindo o consumo de tokens e melhorando o desempenho, pois o modelo seleciona a ferramenta correta logo na primeira tentativa.



Proteção de Dados Sensíveis. Muitas ações passam pelas verificações de permissão e ainda assim podem exfiltrar dados sensíveis. Por isso, o AI Gateway inspeciona todas as solicitações e respostas dos agentes de IA em tempo de execução. Monitore, masque e bloqueie dados sensíveis usando mais de 100 tipos de detecção prontos para uso. Integra-se facilmente à infraestrutura de DLP existente.

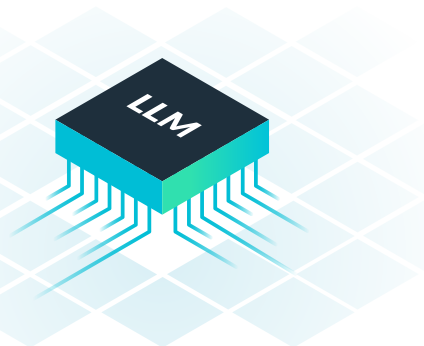


Descoberta de IA. Só é possível governar aquilo que se conhece. A Cequence oferece visibilidade sobre o uso existente de agentes e IA, descobrindo tanto soluções aprovadas quanto Shadow AI. Identifica todos os agentes, servidores MCP e provedores de LLM em toda a organização a partir dos logs existentes do SIEM.

Monitoramento e Visibilidade. Cada solicitação registra o agente, o usuário, a ferramenta utilizada, o horário e o resultado, produzindo uma trilha de auditoria completa exigida por estruturas de conformidade e processos de resposta a incidentes. Os dados e logs podem ser exportados no formato OTEL para integração com plataformas SIEM e GRC.

Registros Corporativos de MCP e APIs. O Registro MCP fornece um catálogo confiável de servidores MCP validados, criados tanto a partir de APIs oficiais de aplicações quanto de MCPs personalizados para suas próprias aplicações, todos provisionados centralmente com recursos de IAM. O AI Gateway gerencia as atualizações do protocolo MCP, eliminando a necessidade de alterações de código à medida que o padrão evolui. O Registro de APIs permite que os agentes acessem sistemas corporativos aprovados sem manter as credenciais de origem.

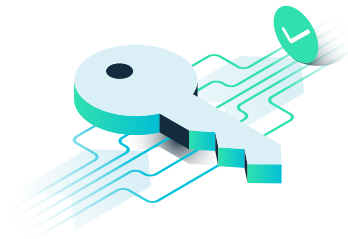
Registro de LLM e Prompt Guard. O Registro de LLMs fornece uma conexão controlada com cada provedor de LLM aprovado, gerencia as credenciais e o acesso aos modelos e aplica limites à taxa de consumo de tokens e aos gastos. O Prompt Guard protege contra injeções de prompt — incluindo padrões de jailbreak e de extração do prompt do sistema — antes que elas cheguem ao modelo.



Segurança

Detecção de Anomalias Comportamentais. Linhas de base comportamentais por persona, por usuário e por ferramenta permitem identificar padrões que a inspeção de chamadas individuais não consegue detectar. Um agente que leia 200 chamados consecutivos antes de abrir uma ferramenta de e-mail pode passar por todas as verificações individuais de permissão; no entanto, é a sequência de ações que representa a violação. O gateway limita ou interrompe a ação em tempo real de acordo com a política definida.

Guardrails e Limites de Taxa. Limites de taxa por agente e por ferramenta, com circuit breakers para interromper loops descontrolados, pontuação automática de risco das ferramentas e controles de rede, incluindo restrições por IP CIDR, geofencing e IP pinning, que exige que os tokens sejam utilizados apenas a partir do endereço IP para o qual foram emitidos, de acordo com cada persona.



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

Autenticação Corporativa. Suporte a múltiplos provedores de identidade (IdP), OAuth 2.1, PKCE, registro dinâmico, integração com OIDC e suporte a mecanismos de autenticação legados, aplicando a política de identidade da organização tanto para identidades humanas quanto não humanas.

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 os endpoints que deseja expor como ferramentas. O gateway gera um servidor MCP em minutos, sem necessidade de programação, e cada servidor criado herda automaticamente o escopo por persona, o monitoramento comportamental e os guardrails. A implantação pode ser totalmente gerenciada na Cequence Cloud ou autogerenciada por meio de um chart Helm.



Registro de Habilidades. O Registro de Habilidades fornece um catálogo central para distribuir instruções e padrões operacionais aprovados pela organização. Ele facilita o uso de Habilidades aprovadas pelos agentes e permite que a empresa acompanhe e audite as ações executadas pelos agentes de IA.

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 agênticas. 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.