CLOUDFLARE

RESUMO DA SOLUÇÃO

Cloudflare AI Security Suite

Proteja as interações de IA ao controlar dados e gerenciar riscos durante todo o seu ciclo de vida da IA.

Escale a IA com confiança

Os riscos da IA exigem segurança moderna

Suas equipes estão usando a IA para inovar mais rapidamente, mas isso cria riscos de segurança críticos. A antiga estratégia de bloquear a IA ou adicionar soluções pontuais complexas está falhando porque sufoca a inovação e ignora a realidade:

- **85% dos funcionários** usam ferramentas de IA antes que o departamento de TI possa avaliá-las.[1]
- **93% admitem** colocar dados da empresa em IA sem aprovação.[2]
- **63% das organizações violadas** não têm políticas de governança de IA.[1]

Aprenda a capacitar suas equipes e a aproveitar os benefícios de produtividade da IA, mantendo a segurança e o controle que sua empresa precisa.

Uma plataforma unificada para proteger IA agêntica e generativa

A Cloudflare oferece uma plataforma única para que sua organização adote a IA com confiança. Capacitamos líderes de segurança para gerenciar riscos, equipes de tecnologia para desbloquear a produtividade e engenheiros de plataforma para criar com segurança, garantindo que todos possam inovar juntos de forma segura.

Comece a usar o Cloudflare AI Security Suite

O Cloudflare AI Security Suite é fornecido em uma plataforma unificada para proteger o uso de ferramentas de IA no espaço de trabalho e aplicativos voltados para o público. Descubra a IA oculta, proteja os modelos contra violações e o acesso de agentes além de evitar a exposição de dados em prompts. Assim, sua empresa pode inovar com segurança e eficiência, com maior visibilidade e controle.

Amplie a visibilidade

em aplicativos de IA, endpoints de API e conexões de agentes de IA.

Mitigue o risco

com proteções, controle de postura e mitigação de ameaças em tempo real

Proteja dados

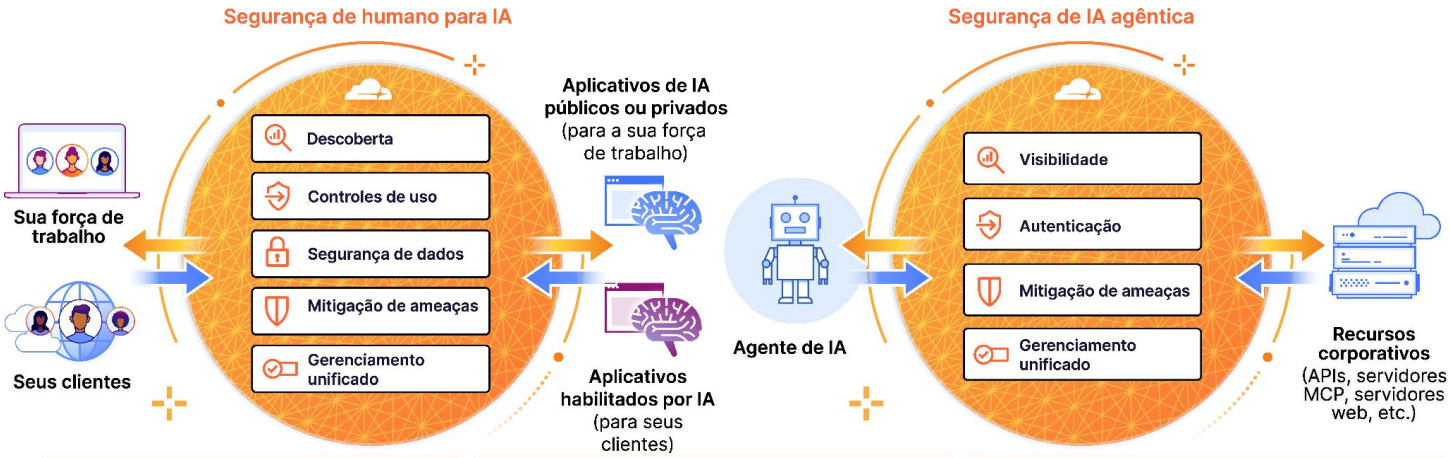
com proteções de prompts e controles de acesso para funcionários e agentes de IA

A segurança é integrada
ao desenvolver IA na Cloudflare.

 +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/ REV:PMM-OCT2025

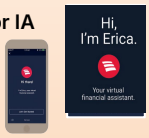
Proteja a comunicação entre IA generativa e agêntica com o Cloudflare AI Security Suite

Proteja todas as comunicações de IA ao controlar os dados que sua força de trabalho utiliza na IA generativa e ao gerenciar os riscos de segurança apresentados por agentes autônomos.



- **Sua força de trabalho:** funcionários, prestadores de serviços, desenvolvedores etc.
- **Seus clientes:** visitantes de seus sites e aplicativos

- **Aplicativos de IA generativa:** independentes ou integrados
  Gemini, Claude, ChatGPT, Copilot
- **Aplicativos habilitados por IA**
  Ex: Chatbot de IA do Bank of America, Erica



- **APIs** e **servidores MCP** para qualquer aplicativo.
  Google Workspace
- **Servidores web** para inferência e geração aumentada de recuperação (RAG)

Acelere a adoção da IA com segurança por design em todo o ciclo de vida da IA

Uso seguro de IA pela força de trabalho

Implemente controles de uso de IA e gerenciamento de postura de segurança de IA (AI-SPM) para mitigar riscos e proteger dados.

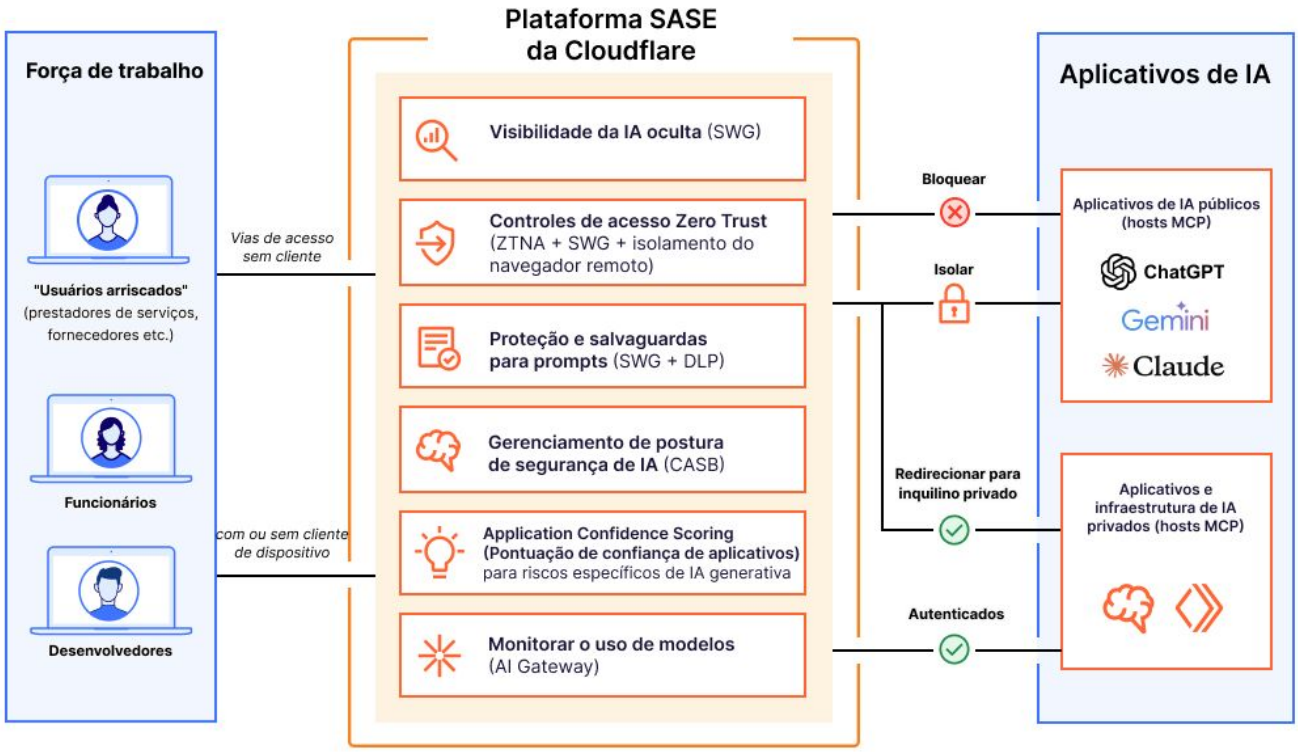
Proteja aplicativos com tecnologia de IA

Proteja seus aplicativos e APIs de IA contra injeção de prompts e vazamento de dados em tempo real.

Crie IA com segurança

Capacite desenvolvedores para proteger aplicativos de IA com observabilidade, limitação de taxa e proteções de IA em linha integradas.

Proteja o uso de aplicativos e cargas de trabalho de IA pela força de trabalho com a plataforma SASE da Cloudflare



SSE para proteger a comunicação entre humanos e IA

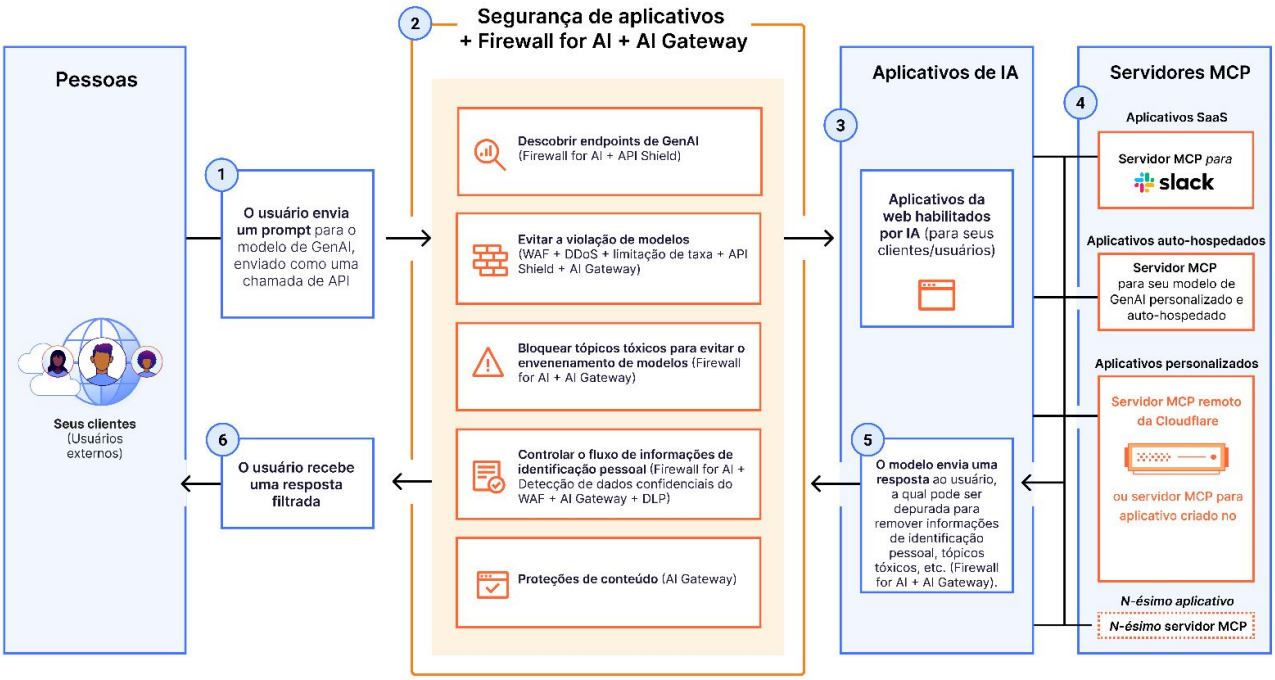
- **Visibilidade:** descubra e analise o uso de IA oculta por meio da inspeção de tráfego em linha. Avalie os riscos representados por aqueles aplicativos de IA com pontuação transparente.
- **Controles de acesso:** bloquear, isolar, redirecionar ou permitir conexões de usuários. Imponha regras de Zero Trust baseadas em identidade por aplicativo.
- **Proteção de prompts e salvaguardas:** detecte e bloqueie prompts de usuários com base na intenção (por exemplo, tentativas de jailbreak, violação de código, solicitações de informações de identificação pessoal).
- **Segurança de dados:** acabe com a exposição de dados confidenciais com detecções de DLP (prevenção contra perda de dados) com tecnologia de IA para informações de identificação pessoal, código-fonte e muito mais.
- **Gerenciamento de postura de segurança de IA:** integre ferramentas de GenAI por meio de API para verificar configurações incorretas com nosso agente de segurança de acesso à nuvem (CASB). Disponível agora para ChatGPT, Claude e Google Gemini.

Portais do servidor MCP para proteger a comunicação IA-recurso

- **Visibilidade:** agregue todos os logs de solicitações do Model Context Protocol (MCP) para auditoria e análise. Analise e aprove cada servidor MCP antes de adicioná-lo ao portal.
- **Autenticação:** autentique o acesso de usuários ao portal com base na identidade. Defina o escopo do acesso aos servidores MCP com base no princípio do menor privilégio.
- **Conexões:** conecte todos os servidores MCP acessíveis com um único URL, em vez de configurar individualmente cada servidor MCP.
- **Gerenciamento unificado:** imponha as mesmas políticas de acesso granular para conexões de IA que você usa para usuários humanos.

Observação: os portais de servidores MCP em negrito são compatíveis com qualquer servidor MCP, incluindo (mas não se limitando a) servidores MCP remotos criados ou implantados na Cloudflare. Esse recurso está disponível como um controle de acesso à rede Zero Trust (ZTNA).

Proteja aplicativos e cargas de trabalho habilitados por IA com a segurança in-line independente de modelo da Cloudflare.



Proteja a IA voltada para o público com segurança de aplicativos e Firewall for AI

- **Descubra endpoints de GenAI:** descubra automaticamente todos os modelos e APIs de IA em seus ativos da web.
- **Proteja os modelos de IA contra violações:** use nosso Firewall for AI, criado especificamente, para bloquear injeção de prompts, envenenamento de modelo, uso excessivo e outras ameaças que podem contornar as proteções de segurança tradicionais.
- **Controle o fluxo de informações de identificação pessoal:** analise os prompts de usuários e as respostas do modelo para impedir a exposição de dados confidenciais, ajudando você a manter a conformidade.
- **Proteções de conteúdo:** Bloqueie prompts inseguros ou tóxicos usando modelos integrados como o Llama Guard. Crie regras WAF personalizadas para bloquear ou registrar facilmente interações de IA suspeitas.

Proteja a IA que você cria com a plataforma para desenvolvedores e o AI Gateway

- Plano de controle de IA **unificado:** gerencie todos os seus aplicativos de IA em um único painel. Direcione solicitações, armazene respostas em cache, controle custos e monitore o desempenho.
- **Proteja as credenciais na borda:** armazene com segurança chaves de API e segredos na borda, evitando a exposição do lado do cliente e simplificando a rotação de chaves entre provedores.
- **Imponha proteções de segurança de conteúdo:** identifique e bloqueie/edite automaticamente conteúdo prejudicial e informações de identificação pessoal em prompts e respostas.

A Cloudflare é a única fornecedora que protege seus ambientes de IA públicos e privados

Implemente as proteções adequadas para adotar a IA com confiança, garantindo que a segurança acelere sua inovação, e não a dificulte.

- **Proteção unificada do ecossistema de IA:** pilhas de segurança complexas aumentam o risco. Use uma única plataforma para proteger dados e garantir a conformidade em todo o ciclo de vida da IA.
- **Arquitetura global preparada para o futuro:** evite os desafios do futuro hoje mesmo com uma rede segura pós-quântica que se adapta a qualquer volume de tráfego, se ajusta constantemente a novas ameaças e é programável para novos casos de uso.
- **Segurança com tecnologia de IA:** nossas defesas com tecnologia de IA inspecionam prompts e respostas para detecção de ameaças em tempo real.
- **Liderança comprovada em IA:** inove com confiança em uma plataforma utilizada por 80% das 50 maiores empresas de GenAI.
- **Implantação independente de modelo:** os controles de segurança funcionam para todos os modelos de IA em seu ambiente, fornecendo uma abordagem unificada para controlar as implantações de IA.

O que os clientes estão dizendo

indeed

Site de empregos nº 1 do mundo
Ler estudo de caso

Identificar e controlar a IA oculta

Em paralelo com o projeto de substituição de VPN

APPLIED

Tecnologia para seguros
Ler estudo de caso

Isolar ferramentas públicas de IA generativa como o ChatGPT

para bloquear copiar e colar dados confidenciais

Empresa de SaaS habilitada por IA

Proteger informações de identificação pessoal

ao evitar que os clientes enviem informações confidenciais para endpoints de GenAI voltados para o público

Cyndx

Fintech orientada por IA

95% de redução nos custos de inferência

ao adotar a Cloudflare para armazenar em cache e executar respostas de provedores de modelos de IA

Pronto para discutir suas necessidades de segurança de IA?

Fale com um especialista

1. 2025 Manage Engine research: Fonte
2. Relatório IBM, Cost of a Data Breach de 2025: Fonte

