CLOUDFLARE

VISÃO GERAL DA SOLUÇÃO

Uso seguro de IA generativa e agêntica pela força de trabalho

Capacite suas equipes para usar qualquer ferramenta de IA com segurança, com proteções aplicadas pela plataforma SASE da Cloudflare.

Recupere o controle, desbloqueie a produtividade

A pressa em adotar a IA está deixando um rastro de riscos crescentes, incluindo vazamentos de dados, violações regulatórias e uma superfície de ataque cada vez maior. Bloquear a IA de vez apenas sacrifica sua vantagem competitiva e experimentar soluções pontuais só aumenta a complexidade.

A Cloudflare protege o uso de IA pela sua organização, ampliando a visibilidade, mitigando riscos e protegendo dados de forma holística em ambientes de IA:

- **Descubra a IA oculta** e gerencie políticas para todas as ferramentas de IA autorizadas e não autorizadas.
- **Fortalecer a governança de IA** com controles de acesso baseados em identidade e gerenciamento de postura.
- **Evitar a perda de dados** bloqueando informações confidenciais em prompts de usuários, aplicando proteções tópicas e verificando se há configurações incorretas em ferramentas de IA.

Amplie a Cloudflare para adotar a IA com segurança, quer sua estratégia de IA envolva limitar o uso a aplicativos específicos ou experimentar uma gama mais vasta de ferramentas diversificadas.

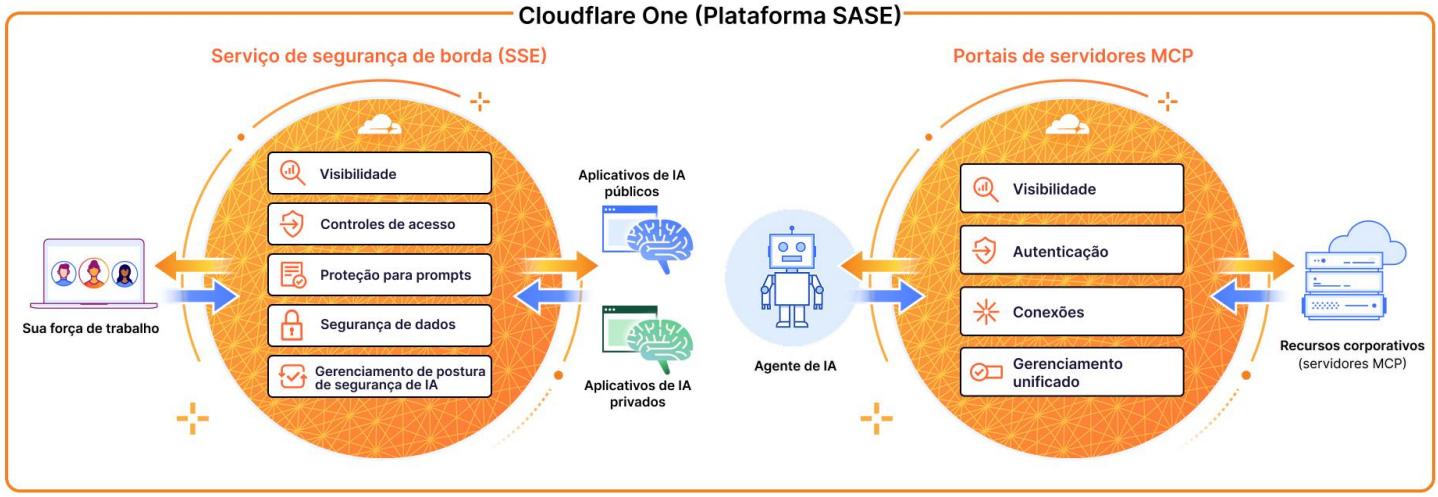
Por que o SASE protege o uso da IA pela força de trabalho

A plataforma SASE (serviço de acesso seguro de borda) da Cloudflare se situa entre sua força de trabalho e as ferramentas de IA. Isso faz do SASE um ponto de partida ideal para que muitos comecem a usar a IA com segurança.

Seja os funcionários conversando com o ChatGPT ou agentes de IA coletando informações em recursos corporativos, a plataforma SASE da Cloudflare impõe controles de segurança consistentes.

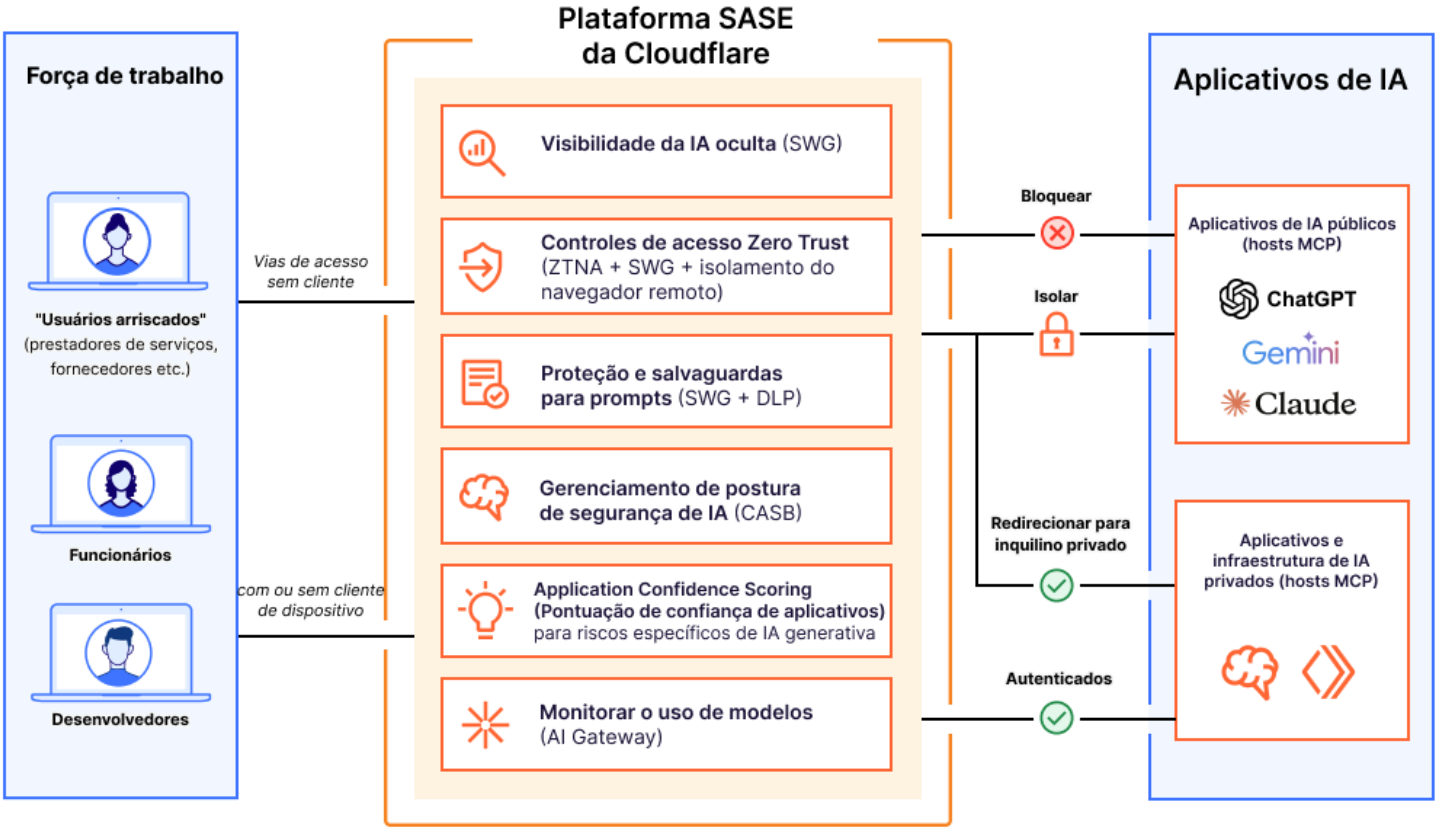
Proteger a comunicação entre IA generativa e agêntica

A plataforma SASE da Cloudflare fornece um painel e um plano de controle unificados para gerenciar as interações de humano para IA e de máquina para máquina em toda a sua organização.



Ao contrário de outros fornecedores de SASE, a Cloudflare também ajuda a conectar e proteger aplicativos e cargas de trabalho habilitados por IA voltados para o público (como o chatbot de IA ou os mecanismos de recomendação de seu site).

Proteger as comunicações de usuários com aplicativos de IA generativa
com controles de uso de IA na plataforma SASE da Cloudflare



- **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:** bloqueie, isole, redirecione ou permita conexões de usuários. Imponha regras de Zero Trust baseadas em identidade por aplicativo.
- **Proteção e salvaguardas para prompts:** 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 da postura de segurança de IA:** integre com as ferramentas de GenAI via API (disponível agora para ChatGPT, Claude, Google Gemini) para verificar se há erros de configuração usando nosso agente de segurança de acesso à nuvem (CASB).

Resultados de clientes

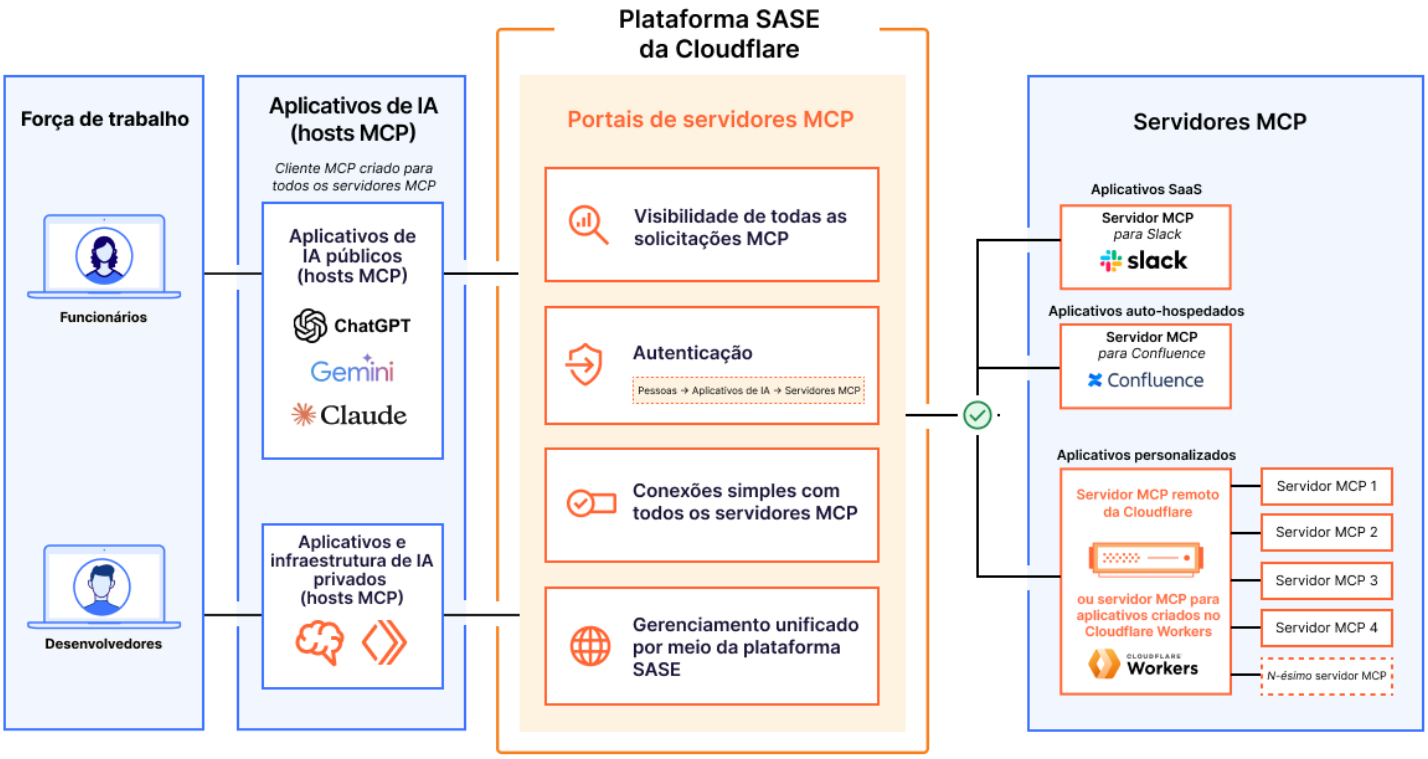
indeed
Site de empregos nº 1 do mundo

Identificar e controlar a IA oculta
em paralelo com o projeto de substituição de VPN

APPLIED
Tecnologia para seguros

Isolar ferramentas públicas de GenAI, como o ChatGPT,
para bloquear a função de copiar e colar dados confidenciais.

Comunicação segura de IA agêntica (de IA para recurso)
com portais de servidores MCP na plataforma SASE da Cloudflare



- **Visibilidade:** agregue todos os logs de solicitações MCP para auditoria e análise. Analise e aprove cada servidor MCP antes de adicioná-lo ao portal.
- **Autenticação:** autentique o acesso do usuário 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.
- **Personalizar ferramentas por portal:** escolha as ferramentas e os modelos de prompts específicos disponibilizados para cada usuário.

Observação: Os portais de servidores MCP da Cloudflare são compatíveis com qualquer servidor MCP, incluindo (mas não se limitando a) qualquer servidor MCP remoto criado ou implantado na Cloudflare. Esse recurso está disponível como um controle de acesso à rede zero trust (ZTNA).

Saiba mais sobre nossa visão nesse blog.

Quer descobrir como a Cloudflare pode proteger seu uso de IA?

Solicite um workshop

