Cloudflare Access

O acesso à rede Zero Trust (ZTNA) verifica o contexto, como identidade e postura do dispositivo, para proteger o acesso em todo o seu ambiente, sem necessidade de VPN.

Modernize o acesso remoto

Acesso à rede Zero Trust rápido e confiável

Os ambientes de trabalho distribuídos exigem uma abordagem distribuída para a segurança. O "perímetro" não existe mais e as soluções tradicionais de acesso remoto, como VPNs, não conseguem atender às expectativas modernas de segurança ou desempenho.

O serviço ZTNA da Cloudflare fornece acesso simples e seguro entre qualquer usuário e recurso, em qualquer dispositivo, em qualquer local, verificando continuamente o contexto granular, como identidade e postura do dispositivo, para cada solicitação. Com uma abordagem nativa de nuvem, não existe mais um "ato de equilíbrio" entre segurança e experiência do usuário. O ZTNA permite que sua empresa tenha acesso contínuo a aplicativos e infraestrutura, ao mesmo tempo que protege os dados.

Também ajuda as organizações a permanecerem ágeis e a navegar pelas mudanças com mais facilidade, seja para integração de novos prestadores de serviços, ou dispositivos não gerenciados, ou navegar pelo acesso durante uma migração para a nuvem ou uma atividade de fusão e aquisição (M&A). A Cloudflare pode se tornar o centro da estratégia Zero Trust ou de modernização da segurança de uma organização, fornecendo ZTNA em nossa nuvem de conectividade global e programável.

"A Cloudflare simplifica a forma como distribuímos o Zero Trust em toda a nossa organização, o que nos ajuda a mitigar riscos de forma mais eficaz com menos esforço."

Anthony Moisant
SVP, CIO e CISO
indeed

Capacite sua empresa com acesso modernizado

Fortalecer a experiência do usuário

Melhore a produtividade da equipe com segurança modernizada que faz com que os aplicativos locais pareçam aplicativos SaaS. Chega de VPNs lentas e desajeitadas ou reclamações de funcionários.

Eliminar o movimento lateral

Reduza o risco cibernético e sua superfície de ataque concedendo acesso baseado em contexto com menos privilégios por recurso, em vez de acesso em nível de rede.

Escalar o Zero Trust sem esforço

Melhore a eficiência tecnológica protegendo aplicativos ou grupos de usuários de alto risco e, em seguida, expanda o ZTNA nativo da internet para proteger toda a sua organização.

Principais casos de uso do Access

Adotar Zero Trust e proteger o trabalho híbrido

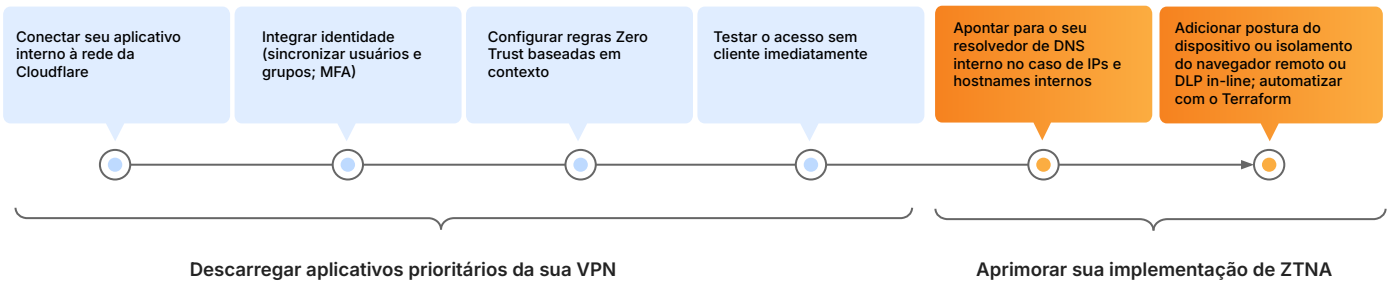
- **Aumento e substituição de VPN** — O Access é mais rápido e seguro do que VPNs tradicionais. Comece a descarregar usuários e aplicativos críticos para melhorar a segurança e a experiência do usuário final.
- **Acesso de prestadores de serviços/BYOD** — Autorize usuários ou funcionários terceirizados em máquinas pessoais com opções de acesso baseadas em navegador.
- **Acesso à infraestrutura** — Forneça acesso privilegiado à infraestrutura confidencial, sem interromper os fluxos de trabalho dos desenvolvedores.

Habilitar a modernização digital

- **Acelere fusões e aquisições** — Evite uma fusão de rede tradicional totalmente. Integre-se com vários provedores de identidade e forneça acesso interno por aplicativo durante fusões e aquisições.
- **Apoie migrações para a nuvem** — Forneça continuidade de acesso durante projetos de modernização de aplicativos usando o ZTNA em ambos os lados de uma migração.
- **Proteja fluxos de trabalho de DevOps** — Proteja fluxos de trabalho entre serviços com conectividade mesh/peer-to-peer, compatível com tráfego bidirecional.

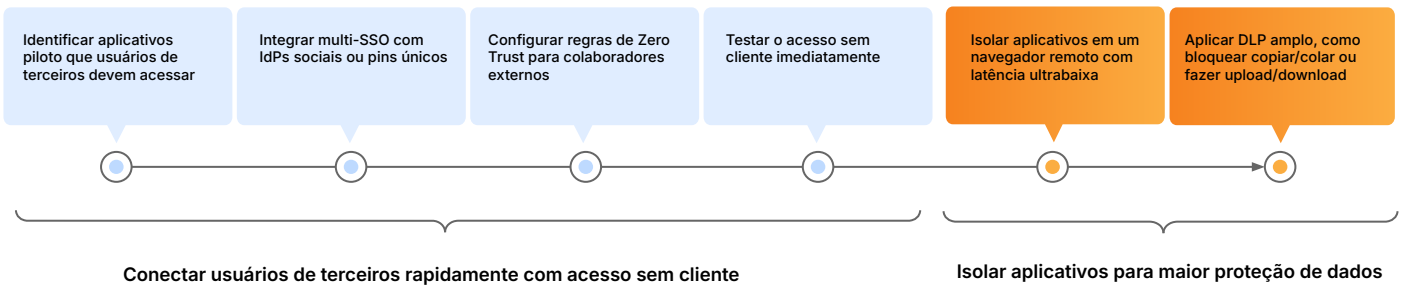
Iniciar o aumento e a substituição da VPN

Priorize aplicativos críticos ou usuários de risco para um piloto de ZTNA para aumentar sua VPN. Use acesso sem cliente a aplicativos web para ajudar a agilizar os testes. Avance gradualmente em direção à substituição completa da VPN ao longo do tempo e adote serviços in-line adicionais para aprimorar sua implantação de SSE ou SASE com sinais mais contextuais ou controles de dados.



Iniciar o acesso de prestadores de serviços/BYOD

Forneça acesso com menos privilégios a usuários de terceiros ou dispositivos não gerenciados e, ao mesmo tempo, mitigue os riscos de movimento lateral ou exfiltração de dados. Configure opções simples de autenticação para prestadores de serviços. Não é necessário software de usuário final. Aplique controles de dados em um navegador isolado para aprimorar sua implementação.



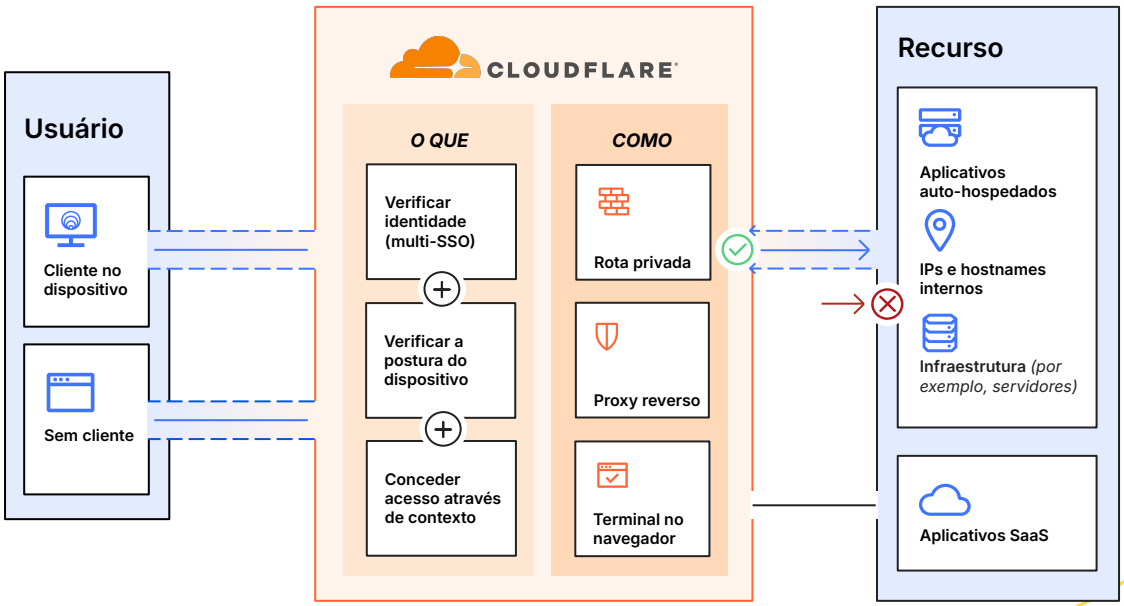
Como o Access funciona

Simplifique e proteja o acesso a todos os recursos de sua organização individualmente, criando um perímetro definido por software usando o Cloudflare Access. Nosso serviço ZTNA é uma camada de agregação flexível que verifica continuamente o contexto granular, como identidade e postura do dispositivo. Quando um usuário se autentica e atende a todos os critérios da política de acesso, o Access emite um JSON Web Token (JWT) assinado, válido por uma duração de sessão especificada. Realizamos a inspeção de passagem única em todas as solicitações de usuários por meio de nossa plataforma SASE combinável e nossa experiência centralizada de administração de políticas aplica as alterações de políticas globalmente em segundos.

A operação unificada, sem cliente e baseada em cliente, lida com todos os tipos de dispositivos. Utilizamos um único cliente de dispositivo em nossa plataforma que criptografa o tráfego para nossa rede a fim de manter a privacidade dos dados de nossos clientes. Também oferecemos acesso simples e seguro a dispositivos fora da empresa por meio de nossa configuração sem cliente. Nossos serviços de proteção ZTNA, DNS e os serviços líderes WAF e proteção contra DDoS trabalham juntos para criar e proteger hostnames públicos acessíveis a usuários terceirizados e a uma força de trabalho híbrida em qualquer dispositivo. Nossas opções de autenticação sem usuário (tokens ou certificados mTLS) também atendem a casos de uso de serviços automatizados e dispositivos IoT.

Para controles Zero Trust, os recursos usam hostnames públicos para proxy reverso para aplicativos auto-hospedados (em nuvem/no local) ou SSH/RDP baseados em navegador, proxy de identidade para aplicativos SaaS ou roteamento privado baseado em cliente/túnel via camadas proxy de encaminhamento nas camadas 4-7 para qualquer recurso web ou não web (por exemplo, destino de infraestrutura ou TCP/UDP arbitrário) em uma sub-rede privada. Nosso software de rede global e conector de aplicativos combinados são compatíveis com qualquer ambiente de computação, nuvem pública, incluindo Kubernetes e contêineres ou recursos de rede local legados, sem exigir infraestrutura de máquinas virtuais e sem limitações de taxa de transferência.

Mantenha-se ágil e crie junto com as ferramentas que os administradores já usam. Ferramentas de identidade de terceiros, endpoints, vias de acesso à rede, registro/análise de dados e SIEM são integrados no painel unificado da Cloudflare, com opções nativas também fornecidas para nosso cliente de dispositivo e analytics.



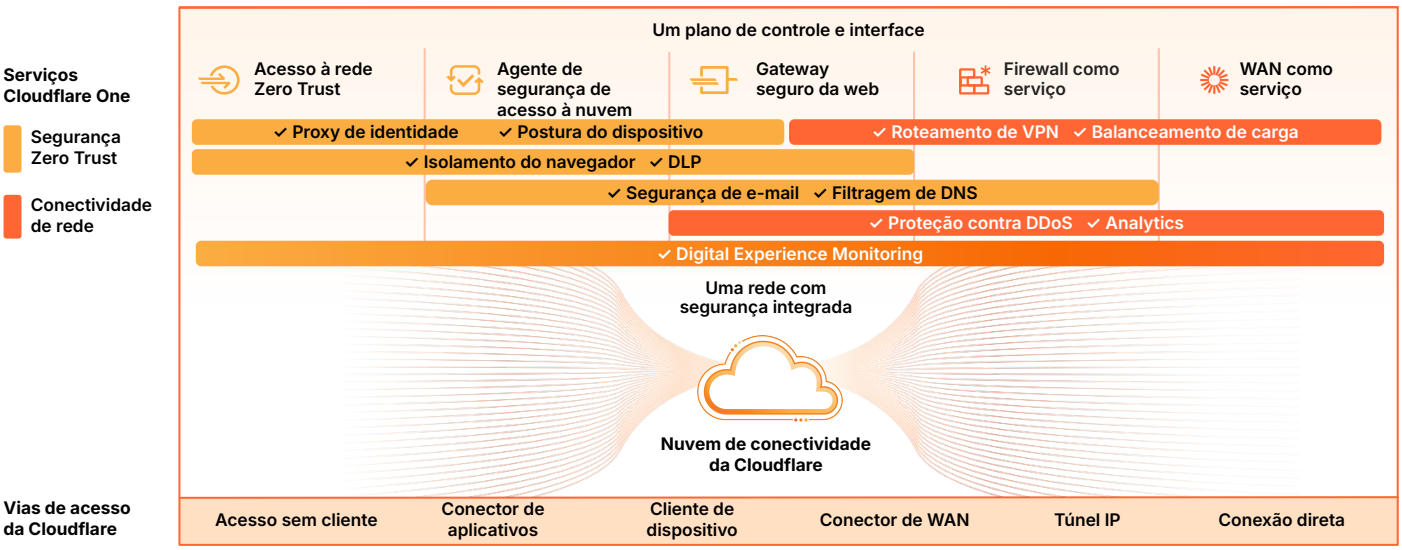
Access como parte da plataforma SSE e SASE da Cloudflare

SSE e SASE costumam ser uma jornada estratégica de vários anos. No entanto, as organizações frequentemente começam com o ZTNA para demonstrar rapidamente o valor comercial multifuncional. As organizações que buscam proteger o trabalho híbrido, defender-se contra ameaças e proteger seus dados no caminho para a consolidação, cada vez mais escolhem a Cloudflare como sua parceira de confiança, quer estejam apenas começando a modernizar o acesso remoto ou retomando um projeto Zero Trust paralisado.

A flexibilidade de implantação e a arquitetura combinável da Cloudflare permitem que qualquer organização proteja e acelere o desempenho de dispositivos, aplicativos e redes inteiras para manter o trabalho híbrido seguro e produtivo. Para isso, oferecemos suporte à integração sem agente para usuários finais, isolamento da web sem cliente para conter tráfego inseguro e um painel de gerenciamento unificado que permite visibilidade de todos os serviços de segurança e de rede, independentemente de onde os administradores ou usuários estão se conectando. A amplitude da rede global da Cloudflare permite que a segurança seja aplicada mais perto dos usuários finais, minimizando a latência e proporcionando uma experiência melhor aos funcionários. Nossa arquitetura Anycast resiliente ajuda a contornar interrupções na internet, mantendo as equipes on-line e ajudando a garantir a continuidade dos negócios.

Reforce sua postura de segurança com implementação simplificada e manutenção de políticas. O contexto compartilhado entre nossas políticas ZTNA, CASB, DLP e SWG fornece fluxos de trabalho de administração consistentes. Os mesmos atributos de identidade e postura do dispositivo podem informar decisões de políticas em todos os serviços.

ZTNA, isolamento do navegador remoto e segurança de e-mail também podem ser usados juntos para fornecer acesso condicional a recursos e, ao mesmo tempo, isolar os usuários de conteúdo malicioso (links, anexos) em ferramentas de e-mail e colaboração. Prestadores de serviços ou funcionários terceirizados em dispositivos pessoais podem ter acesso com menos privilégios a recursos corporativos isolados com controles de dados baseados em navegador (por exemplo, políticas DLP ou controles amplos, como desabilitar fazer upload/download, copiar/colar, entrada de teclado).



Você está em boas mãos

Gartner Peer Insights Customers' Choice 2024™

A Cloudflare foi eleita uma Customers' Choice no Gartner® Peer Insights™ Voice of the Customer: Zero Trust Network Access de 2024[1]

+ de 100 mil

trabalhadores híbridos têm acesso protegido à internet e aos aplicativos.

Fortune 500
Ler o estudo de caso

+ de 44 mil

trabalhadores globais protegidos e substituiu a VPN pelo Zero Trust para força de trabalho híbrida.

Comércio eletrônico
Ler o estudo de caso

3 meses

para substituir a VPN para 13 mil funcionários e 2 mil prestadores de serviços.

site de empregos nº 1
Ler o estudo de caso

1 semana

para migrar políticas e substituir o Zscaler para mais de 7 mil trabalhadores para simplificar as operações.

Comércio eletrônico
Ler o estudo de caso

"O Cloudflare Access foi disponibilizado bem a tempo de evitar que tivéssemos que passar pelo trabalho de implantar uma VPN. Foi uma escolha fácil para nós e surpreendentemente simples de implantar."

Conor Sherman
Diretor de segurança

ezcater

"Antes da implementação do Cloudflare Access, a preparação de um aplicativo para implantação segura era um projeto de duas a quatro semanas. Com o Cloudflare Zero Trust, economizamos 90% desse tempo."

Ricardo Girardelli
Network Engineering Team Lead

creditas

Recursos do Access

Criação/edição de políticas Zero Trust para acesso seguro	
Políticas de acesso granulares e personalizadas	A definição de aplicativos unificada permite uma experiência consistente de administração de políticas. Os aplicativos web são protegidos em nível de subdomínio e caminho com suporte a caracteres curinga e vários hostnames e são compatíveis com solicitações CORS. As alterações nas políticas serão aplicadas globalmente em questão de segundos. Inclui testador de política.
Amplitude de recursos: o que podemos proteger e como	Os recursos usam hostnames públicos para proxy reverso para aplicativos auto-hospedados (nuvem/local) ou SSH/RDP baseado em navegador, proxy de identidade para aplicativos SaaS ou roteamento privado baseado em cliente/túnel via proxy de encaminhamento nas camadas 4-7 para qualquer recurso web/não web (por exemplo, alvo de infraestrutura ou TCP/UDP arbitrário) dentro de uma sub-rede privada. Também é compatível com recursos/fluxos de trabalho com tráfego bidirecional (por exemplo, pipeline VoIP/SIP ou CI/CD).
Identidade	Autenticar por meio de todos os principais provedores de identidade empresarial e social (IdPs), incluindo vários IdPs simultaneamente. Também pode usar conectores SAML e OIDC genéricos. Suporta (e pode aplicar) qualquer método de autenticação fornecido pelo IdP, autenticação temporária, justificativa de finalidade, intervalos de re-AuthN em base global ou por sessão de política/aplicativo e opção de revogação imediata de sessão por aplicativo ou por usuário. Pode usar o dispositivo cliente (WARP) como método de autenticação (identidade armazenada em cache por sessão WARP).
Postura do dispositivo	Verificar a postura do dispositivo usando cliente de dispositivo e integrações com o provedor de proteção de endpoints (EPP) de terceiros. Usar integrações entre serviços (ou integração personalizada com qualquer API) para incluir pontuações de risco de EPP em políticas Zero Trust.
Sinais contextuais para políticas	Configurar sinais como grupo de e-mail, intervalos de IP, geolocalização, método de login (por exemplo, tipo de MFA, tipo de IdP), certificado mTLS ou SSH válido, token de serviço, lista de números de série, atributos de postura do dispositivo, cliente do dispositivo instalado, duração da sessão, aplicação de regras SWG ou sinais de chamadas de APIs externas. Também pode fazer referência direta aos contextos de autenticação de acesso condicional do Microsoft Entra ID.
Outras compatibilidades relacionadas	• **SCIM:** provisiona/desprovisiona automaticamente usuários para sincronizar as alterações em todos os IdPs • **DNS interno:** configura o substituto do domínio local e resolve solicitações de rede privada • **Túneis divididos:** inclui/exclui IPs para redes privadas ou em execução junto com uma VPN • **Autenticação mTLS:** autenticação baseada em certificado para IoT e outros casos de uso de mTLS • **Isolamento de aplicativos:** com uma única caixa de seleção, isole aplicativos em nosso navegador remoto ultrarrápido*
Vias de acesso e de saída	
Conector de aplicativos	A orquestração simples de nosso conector de aplicativo leve (Cloudflare Tunnel) agiliza a conexão de recursos à Cloudflare, sem exigir infraestrutura de VM e sem limitações de rendimento. Inclui monitoramento, redes virtuais (para sobreposições de IP) e recursos de redundância e failover.
Cliente de dispositivo: quando usar	• **Sem cliente:** estender as políticas Zero Trust a usuários terceirizados em dispositivos não gerenciados; também combina com isolamento do navegador remoto sem cliente para impor controles de dados (por exemplo, bloquear/baixar, copiar/colar) e políticas DLP na camada 7 por meio do navegador. Compatível com aplicativos web e SSH, RDP e VNC baseados em navegador. • **Baseado em cliente:** nosso cliente de dispositivo (WARP) estende o acesso seguro a redes privadas, permite integrações de postura do dispositivo entre serviços e reconhece a localização para aplicar políticas personalizadas para usuários do escritório. Compatível com o modo multiusuário em dispositivos Windows e usa o protocolo MASQUE para um melhor gerenciamento do portal cativo. Pode conectar dois ou mais dispositivos executando o WARP para criar redes privadas. Os usuários podem se autoinscrever ou implantar via MDM.
Extensibilidade e visibilidade	
Personalização de página	Fazer upload de HTML personalizado para telas de bloqueio e inicializadores de aplicativos de acordo com sua marca ou transmite instruções de acesso específicas para agilizar a experiência do usuário final.
Logging	Logging abrangente em eventos de autenticação e solicitações para caminhos URI/alvos de infraestrutura protegidos. Inclui logs SSH. Pode usar logpush ou API para integração com ferramentas de SIEM, orquestração e análise existentes. A descoberta de TI invisível fornece visibilidade em aplicativos SaaS autorizados e não autorizados e origens de rede privada.
Automação	APIs intuitivas e provedor Terraform disponíveis para gerenciar programaticamente todos os aspectos de uma implementação Zero Trust. Pode usar tokens de serviço para sistemas automatizados sem usuário.

**usando recursos em outras partes da plataforma SSE/ SASE*

Por que a Cloudflare?

Implantação mais rápida e simples

Comece a usar o ZTNA rapidamente, simplifique o gerenciamento diário e escale facilmente em todos os locais com vias de acesso flexíveis e um painel e API unificados.

Melhor experiência global do usuário final

Garanta uma aplicação de políticas rápida e consistente perto dos usuários finais devido à enorme escala da Cloudflare e à arquitetura de rede Anycast com resiliência integrada.

Arquitetura ágil para o futuro

Simplifique seu plano de modernização de longo prazo com uma rede e um plano de controle unificados de serviços combináveis e nativos de nuvem projetados para funcionarem juntos.

Vamos conversar sobre acesso simples e seguro para sua organização

Solicite um workshop

CLOUDFLARE

Ainda não está pronto para uma conversa ao vivo?

Continue aprendendo mais sobre nossa arquitetura de referência SASE, ou veja como ela funciona em um tour interativo por nossa plataforma Zero Trust.

1. Gartner, Voice of the Customer for Zero Trust Network Access, 30 de janeiro de 2024, colaboradores parceiros. GARTNER, PEER INSIGHTS e o selo Gartner Peer Insights Customers' Choice são marcas registradas da Gartner, Inc. e/ou de suas afiliadas e são usados aqui com permissão. Todos os direitos reservados. O conteúdo do Gartner Peer Insights é constituído das opiniões de usuários finais individuais com base em suas próprias experiências com os fornecedores listados na plataforma; não deve ser interpretado como declarações de fato e não representa as opiniões da Gartner ou de suas afiliadas. A Gartner não endossa nenhum fornecedor, produto ou serviço representado nesse conteúdo e não oferece garantias, expressas ou implícitas, com relação ao conteúdo e sua exatidão ou completude, incluindo garantias de comercialização ou adequação a um propósito específico.

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