CLOUDFLARE

RESUMO DO PRODUTO

Zero Trust da Cloudflare

A plataforma Zero Trust mais rápida
para navegação e acesso a aplicativos

Riscos além do perímetro

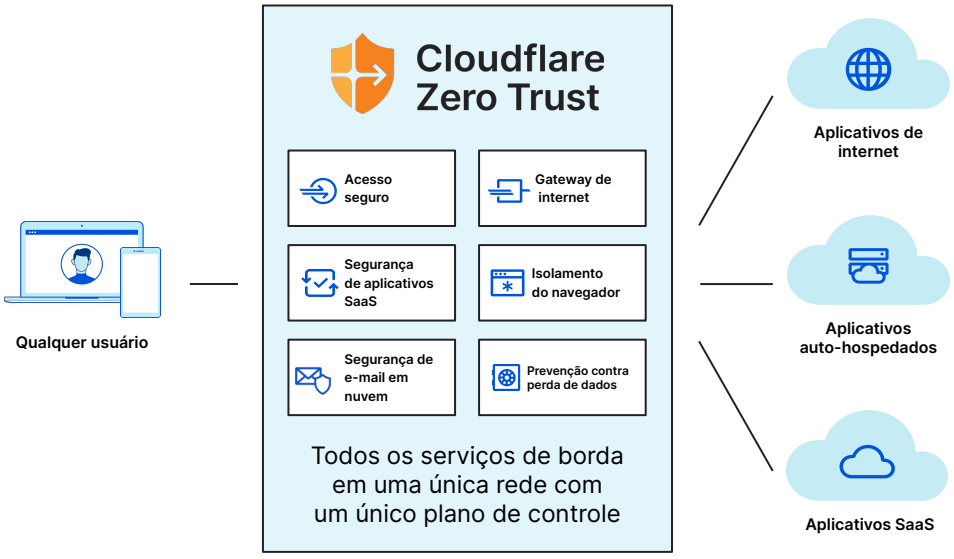
Quando aplicativos e usuários precisaram extrapolar os perímetros corporativos, as equipes de segurança tiveram de se comprometer para manter os dados seguros. Os métodos de segurança de tráfego centrados na localização (como VPNs, firewalls e proxies da web) falharam sob pressão, deixando as organizações com visibilidade limitada, configurações conflitantes e risco excessivo.

Com os riscos agora persistindo em todos os lugares, as organizações estão se voltando para o Zero Trust entregue em nuvem para se adaptar.

Adote o Zero Trust nativo da internet

O Zero Trust da Cloudflare é uma plataforma de segurança que aumenta a visibilidade, elimina a complexidade e reduz os riscos à medida que usuários remotos e no escritório se conectam a aplicativos e à internet. Com sua arquitetura de passagem única, o tráfego é verificado, filtrado, inspecionado e isolado das ameaças.

Ele é executado em uma das redes Anycast mais rápidas do mundo, em mais de 275 cidades em mais de 100 países, para implantar mais rapidamente e ter um desempenho melhor do que outros provedores.



Acesso seguro
simplifique e proteja o acesso entre todos os usuários e aplicativos, em qualquer dispositivo, em qualquer local

Defesa contra ameaças
mantenha seus usuários e dados protegidos contra ameaças da web, de e-mail e multicanais

Proteja com a Microsoft
visibilidade e controle de todos os pacotes SaaS na Microsoft, no Google e em muitos outros

Proteja o trabalho híbrido
melhore a produtividade da equipe, reduza o risco cibernético e aumente a eficiência da tecnologia

Benefícios para os negócios

Reduza o excesso de confiança

Proteja aplicativos com regras de Zero Trust baseadas em identidade e contexto. Bloqueie phishing, ransomware e outras ameaças on-line. Isole os endpoints dos riscos mantendo o código não confiável longe dos dispositivos e a atividade do usuário não confiável longe dos dados.

Elimine a complexidade

Reduza a dependência de produtos pontuais legados e aplique controles de segurança padrão a todo o tráfego, independentemente de como essa conexão seja iniciada ou em que ponto da pilha de rede esteja.

Restaure a visibilidade

Registros abrangentes para atividade de DNS, HTTP, SSH, rede e TI invisível. Monitore a atividade dos usuários em todos os aplicativos. Envie registros para várias de suas ferramentas de análise de dados e armazenamento em nuvem preferidas.

Acesso seguro (ZTNA)

Uma maneira mais rápida, fácil e segura para conectar qualquer usuário a qualquer aplicativo

Desafio: Acesso lento, complexo e arriscado

Os controles de acesso tradicionais baseados em perímetro (como as VPNs) têm uma deficiência cada vez maior. O desempenho lento prejudica a produtividade do usuário final, os administradores lutam com configurações complicadas e o movimento lateral é difícil de conter.

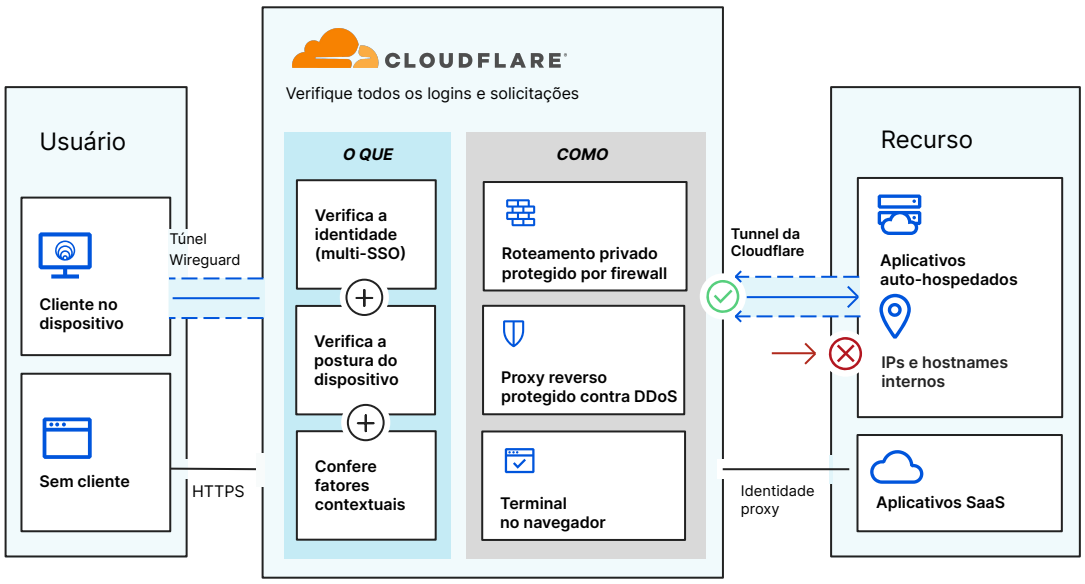
A adoção acelerada da nuvem e o trabalho híbrido expuseram ainda mais essas falhas e tornaram as VPNs mais vulneráveis.

Acesso à Rede Zero Trust (ZTNA)

O Access, serviço ZTNA da Cloudflare, aumenta ou substitui os clientes VPN protegendo qualquer aplicativo, em qualquer rede local, nuvem pública ou ambiente SaaS.

O ZTNA da Cloudflare trabalha com seus provedores de identidade e plataformas de proteção de endpoint para impor regras de negação padrão e Zero Trust que limitam o acesso a aplicativos corporativos, espaços de IP privados e hostnames.

Como funciona



Implantação sem cliente para aplicativos auto-hospedados baseados na web, SSH ou VNC, acessíveis por meio de um navegador.

Implante com o cliente de dispositivo da Cloudflare para conectar-se a IPs internos, nomes de host e aplicativos fora da web.

Principais casos de uso

Apoiar iniciativas de trabalho remoto e BYOD

Verifique o acesso de todos os usuários, onde quer que estejam, com base na identidade, postura do dispositivo, método de autenticação e outros fatores contextuais.

Aplique essas políticas Zero Trust junto à sua força de trabalho híbrida. Dê suporte a iniciativas de BYOD (traga seu próprio dispositivo), protegendo dispositivos gerenciados ou não.

Simplificar o acesso de terceiros com flexibilidade

Acelere a configuração de acesso para terceirizados, fornecedores, agências, colaboradores etc.

Integre vários provedores de identidade (IdPs) de uma só vez. Defina regras de menor privilégio com base nos IdPs que já usam.

Evite provisionar licenças de SSO, implantar VPNs ou criar permissões únicas.

Simplificar a configuração administrativa e o suporte

Adicione novos usuários, provedores de identidade ou regras de Zero Trust em minutos.

Desbloqueie a nova produtividade, reduzindo o tempo de integração de colaboradores (eTeacher Group) e deixando de lado a configuração de acesso baseada em IP (BlockFi). Não há necessidade de contratar colaboradores dedicados para gerenciar VPNs (ezCater).

Defesa contra ameaças (SWG e RBI)

Filtros, inspeção e isolamento do tráfego que chega da internet.

Desafio: o cenário de ameaças em evolução

Aumentar o nível de segurança e manter os usuários produtivos nunca foi tão complicado. Trabalho remoto significa mais dispositivos não gerenciados armazenando mais dados confidenciais, localmente. Enquanto isso, ransomware, phishing, TI invisível e outras ameaças baseadas na internet estão explodindo em volume e sofisticação.

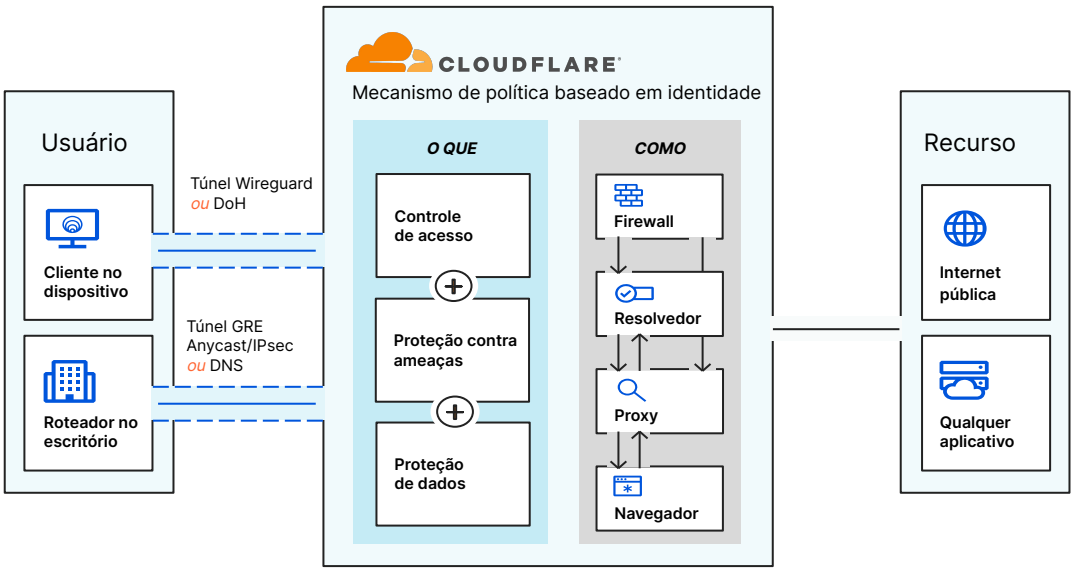
Confiar em soluções pontuais legadas e backups de dados é uma estratégia arriscada para se proteger contra a próxima ameaça multicanal.

SWG com navegação Zero Trust

O Gateway da Cloudflare, nosso Gateway seguro da web (SWG), protege os usuários com filtragem da web baseada em identidade, além de isolamento do navegador remoto (RBI) integrado nativamente.

Comece com a filtragem de DNS para obter um tempo de retorno rápido para usuários remotos ou no escritório. Em seguida, aplique uma inspeção HTTPS mais abrangente e, por fim, estenda os controles de RBI para adotar o Zero Trust para todas as atividades na internet.

Como funciona



Sem backhaul.
Envie tráfego das camadas 4-7 por meio da Cloudflare em vez de dispositivos legados.

Filtros, inspeção e isolamento podem ser aplicados ao tráfego de recursos internos e vinculados à internet.

Principais casos de uso

Pare o ransomware

Bloqueie sites e domínios de ransomware com base em nossa inteligência de rede global. Isole a navegação em sites arriscados para reforçar a proteção.

Combine filtragem SWG e RBI com ZTNA de negação padrão para mitigar o risco de infecção por ransomware se espalhar lateralmente e aumentar privilégios em sua rede.

Bloqueie o phishing

Filtre domínios de phishing conhecidos e "novos"/"recentemente vistos". Isole a navegação para impedir que cargas perigosas sejam executadas localmente. Interrompa o envio de informações confidenciais em sites de phishing suspeitos por meio dos controles de entrada do teclado do RBI.

Além disso, em breve, os administradores poderão ativar a filtragem de e-mail com um único clique – desenvolvido pelo Area 1.

Evite o vazamento de dados

Implemente a prevenção contra perda de dados (DLP) com controles de tipo de arquivo que podem impedir que os usuários carreguem arquivos para sites.

Implante a navegação Zero Trust para controlar e proteger os dados que residem em aplicativos baseados na web. Controle as ações do usuário no navegador: baixar, carregar, copiar e colar, entradas de teclado e funcionalidades de impressão

Proteja com a Microsoft (CASB)

Simplifique a segurança SaaS para mais visibilidade e controle, com menos sobrecarga

Desafio: proliferação de aplicativos SaaS

As forças de trabalho modernas dependem de aplicativos SaaS como o Microsoft 365, agora mais do que nunca. Mas cada aplicativo SaaS requer considerações de segurança diferentes e opera fora das salvaguardas do perímetro tradicional.

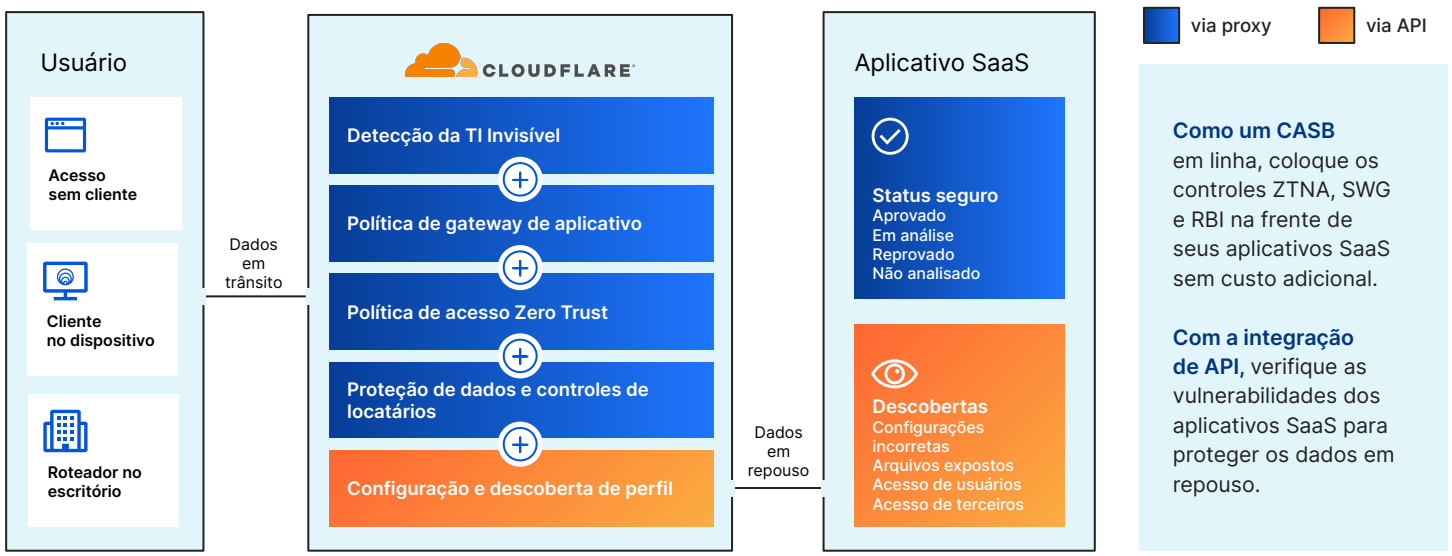
À medida que as organizações adotam dezenas de aplicativos SaaS, torna-se cada vez mais desafiador manter segurança, visibilidade e desempenho consistentes.

Agente de segurança de acesso à nuvem(CASB)

O serviço CASB da Cloudflare oferece visibilidade e controle abrangentes sobre aplicativos SaaS, para que você possa facilmente evitar vazamentos de dados e violações de conformidade.

Bloqueie ameaças internas, compartilhamento de dados arriscado e agentes mal-intencionados. Registre todas as solicitações HTTP para revelar aplicativos SaaS não autorizados. Analise aplicativos SaaS para detectar configurações incorretas e atividades suspeitas.

Como funciona



Como um CASB em linha, coloque os controles ZTNA, SWG e RBI na frente de seus aplicativos SaaS sem custo adicional.

Com a integração de API, verifique as vulnerabilidades dos aplicativos SaaS para proteger os dados em repouso.

Principais casos de uso

Aplique controles de proteção de dados e locatários

Aplique o controle de locatários por meio de políticas de gateway HTTP para evitar que os usuários acessem e armazenem dados nas versões erradas de aplicativos SaaS populares, inadvertidamente ou maliciosamente.

Controle as ações do usuário (por exemplo, copiar/colar, downloads, impressão etc.) em aplicativos SaaS baseados na web para minimizar o risco de perda de dados.

Mitigue e controle a TI invisível

Minimize os riscos introduzidos por aplicativos SaaS não aprovados.

A Cloudflare agrega e categoriza automaticamente todas as solicitações HTTP em nosso registro de atividades por tipo de aplicativo. Os administradores podem definir o status e acompanhar o uso de aplicativos aprovados e não aprovados em sua organização.

Identifique novas ameaças e configurações incorretas

Conecte-se a aplicativos SaaS populares (Google Workspace, Microsoft 365 etc.) por meio da API e verifique os riscos.

Capacite suas equipes de TI e segurança com visibilidade de permissões, configurações incorretas, acesso impróprio e problemas de controle que podem colocar seus dados e colaboradores em risco.

Proteção contra phishing (CES)

Estenda o Zero Trust ao e-mail para proteção abrangente contra ameaças

Desafio: o e-mail é o vetor nº 1 de ameaças

O e-mail é a forma nº 1 de comunicação entre as equipes, mas também a forma de comunicação nº 1 dos invasores. De fato, um estudo recente descobriu que 91% de todos os ataques cibernéticos começam com um e-mail de phishing.

Os invasores frequentemente visam e exploram, com sucesso, o alto nível de confiança que geralmente é depositado na comunicação por e-mail.

Integrando a segurança de e-mail nativa em nuvem

Adicionar a segurança de e-mail em nuvem (CES) do Area 1 como parte de uma estratégia abrangente de Zero Trust remove a confiança implícita no e-mail para interromper preventivamente os ataques de phishing e comprometimento de e-mail corporativo (BEC).

Todo o tráfego do usuário, incluindo e-mail, é verificado, filtrado, inspecionado e isolado de ameaças conhecidas e desconhecidas. O Area 1 ajuda os clientes a bloquear ameaças transmitidas por e-mail, adotar uma postura de segurança proativa e reduzir os tempos de resposta a incidentes de phishing em 90%.

Como funciona: Zero Trust para todo o tráfego de e-mail, web e rede

Principais casos de uso

Previna BEC e fraudes baseadas em e-mail

Impeça ataques sofisticados de comprometimento de e-mail corporativo (BEC) e controles de contas de fornecedores por meio de análise de sentimentos, gráficos sociais de parceiros, classificação de mensagens e análise de origem de campanha.

Bloqueie, coloque em quarentena e escale automaticamente comunicações financeiras fraudulentas.

Proteja-se contra ataques multicanal

Bloqueie, sem esforço, campanhas de ataque que visam indivíduos por meio de vários canais de comunicação, como e-mail e web, permitindo que os usuários carreguem com segurança links suspeitos ou desconhecidos em um navegador remoto e isolado.

Capture ataques de phishing adiados que armam links após a entrega com a classificação do link no momento do clique.

Acelere a triagem e a resposta ao phishing

Libere os ciclos de investigação de segurança, obtenha informações úteis sobre seu ambiente de e-mail e reduza os tempos de resposta com recursos dedicados que reforçam sua equipe existente para que possa neutralizar rapidamente as ameaças de phishing.

Obtenha suporte adicional e experiência em segurança com serviços de segurança de e-mail gerenciados.

Trabalho híbrido seguro: a diferença da Cloudflare

Segurança moderna para uma força de trabalho moderna

Implantação simples

A Cloudflare fornece uma plataforma uniforme e componível para maior facilidade de configuração e operação. Com conectores somente de software e integrações necessárias uma única vez, nossos acessos de entrada e serviços de borda na Cloudflare trabalham todos em conjunto.

Isso resulta em uma melhor experiência para os seus profissionais de TI e seus usuários finais.

Resiliência de rede

Nossa automação de tráfego de ponta a ponta garante conectividade confiável e escalável, com proteção consistente em qualquer local.

Com a Cloudflare, cada serviço de borda é criado para ser executado em todos os locais da rede e está disponível para todos os clientes, o que não ocorre com outros fornecedores

Velocidade de inovação

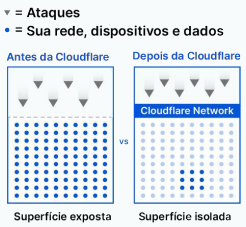
Nossa arquitetura preparada para o futuro nos ajuda a desenvolver e enviar novos recursos de segurança e de rede muito rapidamente.

Quer seja por nossa rápida adoção de novos padrões de segurança e de internet ou por desenvolver novos casos de uso orientados por clientes: nosso histórico de destreza fala por si e nossa base proporciona uma extrema diversidade de opções.

5 maneiras pelas quais o Zero Trust economiza tempo e dinheiro da sua empresa

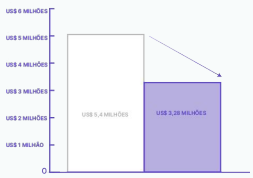
Reduz a superfície de DDoS

91% ↓



Reduz os custos de violaçao

35% ↓



Acelera a integração de funcionários

60% ↑

Reduz a carga de tickets de TI

80% ↓

Reduz a latência para o usuário

39% ↓

Otimizado para usabilidade

Uma interface de gerenciamento

Simplifique a configuração com um painel construído nativamente para políticas de acesso à internet e aplicativos.

Use um painel para integração com provedores de identidade, proteções de endpoints e acessos de rede.

Uma plataforma consolidada

Substitua uma colcha de retalhos de clientes VPN, firewalls locais e outras soluções de segurança pontuais por uma plataforma e um plano de controle.

Reduza os custos e a complexidade, ao levar a segurança para a borda.

Experiência do usuário incomparável

A Cloudflare fica mais próxima de seus usuários e serviços e direciona as solicitações mais rapidamente, utilizando roteamento otimizado e orientado por inteligência em nossa vasta rede Anycast, com mais de 275 locais, em mais de 100 países ao redor do mundo.

Acelere sua jornada Zero Trust

Experimente agora | Fale conosco