Proteger o trabalho híbrido

Reduzir o risco e aumentar a visibilidade para todos os usuários, dentro e fora da rede

Proteja todas as conexões de todos usuários, em todos os dispositivos, em qualquer lugar

Nosso futuro com trabalho em qualquer lugar: anos após a pandemia global e com uma recessão iminente, o trabalho híbrido parece ter vindo para ficar. As equipes de TI e segurança devem fornecer proteção e experiências consistentes para todos os usuários e dispositivos, sejam remotos ou no escritório e as ferramentas tradicionais centradas em localização (como VPNs e controles baseados em IP) não estão conseguindo cumprir a tarefa.

Segurança moderna para uma força de trabalho moderna: em resposta, muitas organizações estão reimaginando sua arquitetura de TI e segurança e adotando segurança fornecida em nuvem que se adapta às necessidades das forças de trabalho distribuídas e segue as práticas recomendadas de Zero Trust.

A Cloudflare simplifica a proteção de todas as conexões, para que usuários em qualquer dispositivo ou local permaneçam seguros e produtivos ao acessar aplicativos ou a internet.

O que a Gartner® diz:

> *Até 2026, 75% dos trabalhadores continuarão a dividir o tempo entre casa e escritórios tradicionais, um pouco abaixo dos 77% no auge da pandemia em 2021.[1]*

> *Os projetos de segurança de rede baseados em vários dispositivos de segurança de perímetro são inadequados para atender às necessidades dinâmicas em qualquer lugar e qualquer hora de uma empresa digital moderna e sua força de trabalho digital híbrida.[2]*

Sumário por página

Oportunidades de modernização de segurança

Acesso seguro a aplicativos sem VPN

Com usuários tão dispersos, o tráfego de backhaul por meio de dispositivos locais, como VPNs, diminui o desempenho e cria o risco de que as ameaças se espalhem lateralmente pela rede corporativa.

A alternativa é recuperar a visibilidade de todas as solicitações e aplicar controles baseados em identidade oferecidos mais perto dos usuários para manter a produtividade. Sem necessidade de backhaul.

Simplifique a segurança de SaaS

Mais do que nunca, as forças de trabalho dependem de aplicativos SaaS fora dos controles das redes corporativas tradicionais.

Em resposta, as organizações precisam de visibilidade e controle mais abrangentes sobre seus aplicativos SaaS para definir políticas de acesso, aplicar controles de proteção de dados, mitigar a TI invisível e verificar aplicativos em busca de configurações incorretas.

Proteger dados e usuários contra ameaças na internet

Ransomware, phishing e outras ameaças da internet estão sempre presentes e cada vez mais sofisticados.

A adoção de inspeção e isolamento baseados em nuvem para tráfego de saída mantém os usuários protegidos contra malware. Além disso, os administradores podem aplicar controles para impedir que dados confidenciais cheguem a dispositivos locais não gerenciados.

Trabalho híbrido para empresas maduras

Para as empresas maduras modernizarem a segurança para o trabalho híbrido com confiança

Desafio: ambientes legados complexos

As organizações estão experimentando modelos de trabalho no escritório. Mas manter as proteções consistentes e as experiências do usuário é um desafio nesses cenários híbridos.

Essas empresas geralmente estão mais estabelecidas com investimentos mais densos no local, já existentes (muitas vezes complexos) e legados. Iniciar um novo projeto de segurança diante dos ventos contrários da recessão pode parecer muito arriscado e difícil.

Oportunidade: caminho mais simples para a modernização

As organizações merecem buscar a transformação digital em seu próprio ritmo, sem precisar de um orçamento infinito, "provas de conceito" caras, fases de implementação complexas ou serviços em cadeia.

Para ajudar essas empresas maduras a atender às suas necessidades de trabalho híbrido, a Cloudflare foi projetada para ser mais fácil e rápida de implantar do que outros provedores de serviços Zero Trust, como a Zscaler.

Amostras de casos de uso

Telecomunicações

Situação: uma empresa de telecomunicações europeia com mais de 100 anos e mais de US$ 20 bilhões em receita anual queria um único fornecedor para implantar filtragem de internet e autenticar o acesso a aplicativos legados que haviam sido recentemente migrados para vários ambientes em nuvem.

Solução: a empresa selecionou a Cloudflare para consolidar serviços e usar uma plataforma unificada para proteger o acesso a aplicativos e à internet entre seus mais de 100 mil funcionários.

Governo federal

Situação: o Departamento de Segurança Interna dos EUA (DHS) lidera os investimentos em proteção contra ameaças da internet em escritórios federais, locais e infraestrutura.

Solução: o DHS selecionou a Cloudflare e a Accenture Federal Services para desenvolver uma solução conjunta para filtrar consultas de DNS para destinos maliciosos e arriscados que será usada em todas as agências federais.

Mídia e publicidade

Situação: um conglomerado de mídia (receita de mais de US$ 10 bilhões e mais de 100 mil funcionários em todo o mundo) enfrenta ataques cibernéticos na infraestrutura interna, incluindo uma nota de resgate.

Solução: a Cloudflare protege centenas de aplicativos web e fora da web com regras Zero Trust baseadas em identidade. A empresa implementa proteção para 50 mil funcionários em 3 meses e tem projeto para expandir para toda a força de trabalho em 9 meses.

Energia

Situação: um fornecedor de gás natural da Fortune 500 buscou proteção aprimorada contra ameaças cibernéticas crescentes direcionadas ao setor para seus data centers distribuídos e mais de 1.500 funcionários.

Solução: a empresa selecionou a Cloudflare para substituir a Zscaler, citando melhor confiabilidade e consistência na proteção de aplicativos e acesso à internet e, no longo prazo, um caminho mais fácil para adotar controles avançados com isolamento do navegador remoto.

CITAÇÕES DE CLIENTES

> *A Cloudflare é um multiplicador de forças em nossa jornada Zero Trust.*

John McLeod
CISO, National Oilwell Varco

> *A Cloudflare permite que o Ziff Media Group disponibilize nosso conjunto de ferramentas internas de forma transparente e segura para funcionários em todo o mundo em qualquer dispositivo, sem a necessidade de configurações de rede complicadas.*

Josh Butts
SVP de produtos e tecnologia, Ziff Media Group

> *Com a Cloudflare, conseguimos reduzir nossa dependência de VPNs e listas de permissões de IP para ambientes de desenvolvimento.*

Alexandre Papadopoulos, Diretor de segurança cibernética, INSEAD

Força de trabalho remota para nativos digitais

Para nativos digitais priorizarem a segurança ágil para oferecer suporte à flexibilidade do trabalho remoto

Desafio: dimensionar e automatizar a segurança em nuvem

Muitas organizações estão adotando a contratação remota. De forma geral, elas tendem a ser mais jovens, adotantes iniciais da nuvem com infraestrutura local limitada e com modelos de negócios baseados em serviços digitais seguros, rápidos e confiáveis.

Permitir a flexibilidade do trabalho de qualquer lugar pode ser um diferencial, mas exige ferramentas de segurança igualmente flexíveis à medida que os usuários se movem e dependem de dispositivos pessoais.

Oportunidade: segurança combinável ajustada à escala

Com menos TI legada para ser depreciada, esses nativos digitais podem aproveitar nossa arquitetura nativa da internet e flexibilidade de implantação para permanecerem ágeis em sua modernização de segurança.

Nossos serviços compostos, design de API em primeiro lugar e gerenciamento em painel único facilitam a introdução e a adaptação da segurança. A velocidade, escala e confiabilidade de nossa rede global atendem às necessidades de uma força de trabalho totalmente remota.

Amostras de casos de uso

SaaS B2B

Situação: a plataforma australiana de design gráfico, Canva, (avaliada em US$ 40 bilhões em 2021) implantou a Cloudflare antes da pandemia para simplificar o acesso para usuários de terceiros e evitar os aborrecimentos de implementar uma VPN.

Solução: com o tempo, a Canva implementou políticas de acesso a aplicativos Zero Trust em toda a sua crescente força de trabalho, além de estender a filtragem e a inspeção da internet.

Fintech e blockchain

Situação: a BlockFi, uma plataforma de gerenciamento de patrimônio série D com tecnologia blockchain, precisava aumentar a segurança diante de ameaças cibernéticas contra seus crescentes ativos sob gestão e força de trabalho remota.

Solução: a Cloudflare possibilitou que a BlockFi fizesse a transição para a autenticação baseada em identidade para acesso a aplicativos e sem controles demorados baseados em IP.

Rede social

Situação: uma plataforma global de rede social sofreu uma violação de alto nível que explorou o acesso interno a aplicativos e as configurações de VPN.

Solução: em resposta, a empresa decidiu reformular sua abordagem de acesso remoto adotando a solução Acesso à Rede Zero Trust (ZTNA) da Cloudflare para 13 mil funcionários e contratados, removendo suas implantações de VPN.

Comércio eletrônico

Situação: uma plataforma global de comércio eletrônico (receita de mais de US$ 4 bilhões e mais de 15 mil funcionários) buscou melhor proteção para usuários remotos que navegam na internet e acessam aplicativos SaaS confidenciais fora da rede.

Solução: a empresa implanta a Cloudflare para criar camadas de recursos de proteção contra ameaças, como filtragem de DNS e ao mesmo tempo fornecer visibilidade aprimorada do uso dos aplicativos SaaS.

CITAÇÕES DE CLIENTES

> *Na Delivery Hero, sempre nos esforçamos para proporcionar uma experiência incrível aos nossos clientes. A Cloudflare nos ajuda a fazer o mesmo para nossas equipes internas: oferecendo a elas um ambiente de trabalho seguro em todo o mundo e uma maneira fácil de criar aplicativos rápidos, confiáveis e que respeitam a privacidade.*

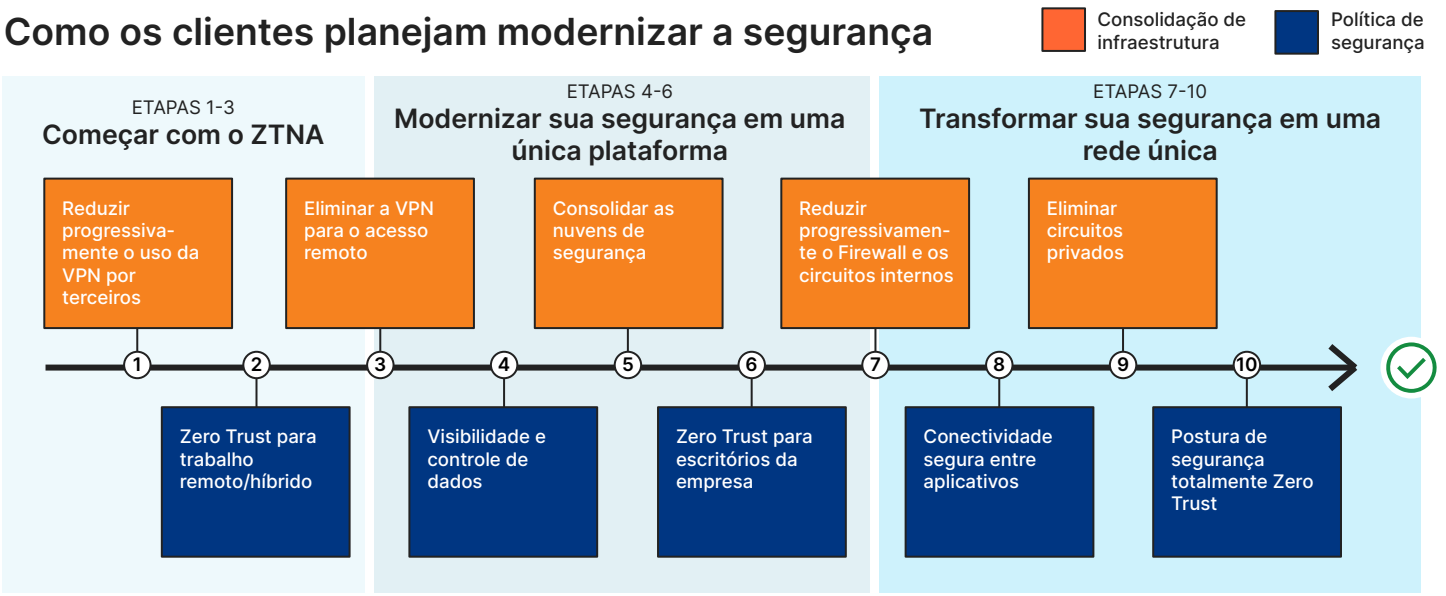
Christina von Hardenberg
CTO, Delivery Hero

> *A Cloudflare é essencial para proteger nossa força de trabalho remota e em rápido crescimento. A adoção do Zero Trust para acesso a aplicativos deu aos nossos administradores visibilidade aprimorada e controles granulares que eles nunca poderiam obter com ferramentas legadas anteriores.*

Marccio Alcaide
Diretor de segurança de TI, Facily

Roteiro ilustrativo de trabalho híbrido

Como os clientes planejam modernizar a segurança



Roteiro de modernização de segurança

O roteiro acima ilustra a abordagem que observamos as organizações adotarem ao modernizar sua segurança para se adaptar ao trabalho híbrido. Este roteiro tem dois objetivos principais:

1) **Linha superior (em laranja):** consolidar a conectividade e infraestrutura de segurança sem produtos pontuais e hardware para uma plataforma nativa de nuvem.
2) **Linha inferior (em azul):** ganhar visibilidade e controles para adotar a segurança Zero Trust entre usuários e recursos em qualquer dispositivo, em qualquer local.

Fases 1 - 5: proteger o aplicativo e o acesso à internet

Para muitos, a adaptação ao trabalho híbrido significa primeiro modernizar a forma como as forças de trabalho chegam aos recursos corporativos.

Fase 1: muitas vezes, o primeiro passo é começar a descarregar o tráfego da VPN e fazer a transição para controles nativos da internet para usuários selecionados, como contratados, desenvolvedores, parceiros ou equipes recém-adquiridas. A Cloudflare torna particularmente fácil proteger aplicativos auto-hospedados acessíveis por meio de um navegador sem a necessidade de implantar qualquer software em endpoints.

Fase 2: essas ferramentas modernas permitem a visibilidade necessária para criar políticas por aplicativo com base em função, MFA e requisitos de chave física e identidade e postura do dispositivo.

Fase 3: à medida que as equipes ganham confiança nessa abordagem, elas migram para o abandono total da VPN e a proteção das redes privadas legadas e fora da web com Zero Trust.

Fase 4: o foco então muda para melhorar a visibilidade e os controles para aplicativos SaaS, incluindo a mitigação de TI invisível, gerenciamento de locatários e prevenção de exfiltração de dados.

Fase 5: com aplicativos internos e SaaS agora gerenciados a partir de uma única plataforma, as organizações buscam expandir os controles para acesso de saída à internet e consolidar ferramentas de proteção contra ameaças, como filtros de DNS e Gateways seguros da web.

Fases 6 a 10: Mudar a conectividade para a nuvem

As fases restantes do roteiro estão em planejamento para a maioria das organizações, mas sua aspiração é mudar toda a conectividade e segurança de rede para uma rede unificada em nuvem.

Fase 6: aqui, as organizações procuram estender o Zero Trust consistente a qualquer local da rede, como sede, filiais, data centers e escritórios satélites para dar suporte ao trabalho híbrido.

Fase 7: à medida que o tráfego dos escritórios é cada vez mais enviado à Cloudflare para fins de segurança, as organizações podem eliminar os firewalls locais tradicionais e outros dispositivos da rede privada.

Fase 8: esses casos de uso avançados se concentram em proteger a conectividade de aplicativo para aplicativo em ambientes multinuvem híbridos, o que prepara a equipe de infraestrutura de rede para encerrar os contratos MPLS de telecomunicações na **Fase 9**.

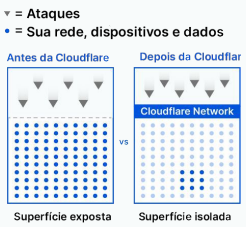
Fase 10: na realidade, embora a modernização nunca termine, a aspiração é que o Zero Trust, agora, se estenda a todos os usuários, dispositivos, dados, aplicativos e ambientes.

Resultados de negócios e segurança

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

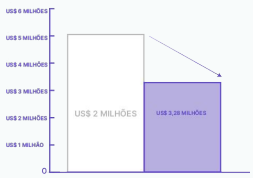
Reduzir superfície de DDoS

91% ↓



Reduzir VIOLAÇÃO da computação

35% ↓



Acelerar a integração de funcionários

60% ↑

Reduzir a carga de tickets de TI

80% ↓

Reduzir a latência para os usuários

39% ↓

Outros impulsionadores de negócios

Desbloquear a produtividade da força de trabalho

Para administradores

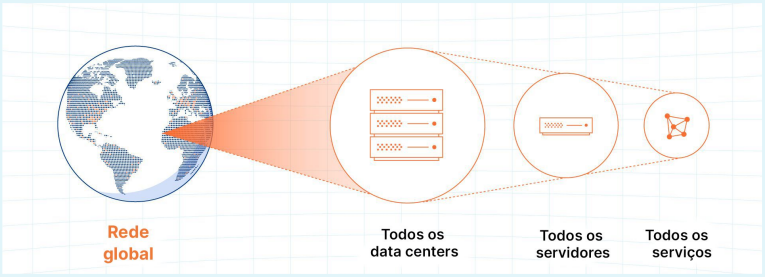
- Simplificar a configuração com uma única interface de gerenciamento para definir políticas entre aplicativos e acesso à internet
- Configurar todas as integrações com provedores de identidade, proteção de endpoints, provedores de nuvem e acessos à rede a partir da mesma interface de gerenciamento

Para usuários finais

- Autenticação sem atrito e experiências de navegação nativas com segurança que fica fora do caminho

Reduzir os custos em serviços legados

- Substituir ou aumentar seus dispositivos de rede privada virtual (VPN) e adotar o Acesso à Rede Zero Trust (ZTNA)
- Transição do proxy ou firewall da web local para serviços de segurança nas camadas 3-7 nativos de nuvem
- Descarregar casos de uso da infraestrutura de desktop virtual com Isolamento do navegador remoto (RBI)
- Trocar o gateway de e-mail seguro tradicional pela segurança moderna do e-mail em nuvem



Velocidade e escala consistentes para proteger todos os usuários remotos ou do escritório

Todas as funções de segurança, desempenho e confiabilidade foram desenvolvidas para serem executadas em cada um dos servidores de todos os data centers da Cloudflare em nossa rede que atualmente abrange mais de 275 cidades.

Acelere seu roteiro Zero Trust Experimente agora Fale conosco

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

REV: PMM-2022JUL

[1] *Top Network Practices to Support Hybrid Work,* Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 08/04/2022
[2] *2022 Strategic Roadmap for SASE Convergence,* Gartner, Neil MacDonald, Andrew Lerner, John Watts 24/06/2022