ARTIGO TÉCNICO

CLOUDFLARE

Comece a usar o SASE: Um guia para proteger e agilizar sua infraestrutura de rede

O SASE, ou serviço de acesso seguro de borda simplifica a arquitetura de rede tradicional ao combinar os serviços de rede e de segurança em uma única rede global. Este artigo explora a evolução da segurança de rede que levou ao SASE, descreve a amplitude de serviços incluídos em uma solução SASE e oferece etapas práticas para avançar em direção à adoção do SASE.

INTRODUÇÃO

Criado pela Gartner em 2019, o serviço de acesso seguro de borda, ou “SASE”, foi inicialmente posicionado como um avanço fundamental no processo de transformação digital: serviços de rede e segurança altamente personalizáveis integrados perfeitamente na estrutura de uma plataforma de nuvem global. Com uma taxa de adoção de 20% esperada até 2023, a Gartner afirmou que a demanda por recursos SASE “redefine a arquitetura de rede corporativa e de segurança de rede e reformula o cenário competitivo”. [1]

Desde então, o termo se espalhou rapidamente pelo espaço de TI e segurança corporativa. À medida que os provedores de segurança de rede e os fornecedores de SD-WAN lutam para se posicionar como líderes SASE, as empresas se veem em meio a um conjunto confuso e montado às pressas de serviços de rede e segurança que se aproxima, mas geralmente não abrange totalmente, uma estrutura SASE.

Uma plena adoção do SASE requer mais do que apenas juntar soluções pontuais existentes em um pacote —exige também que sua empresa repense completamente sua infraestrutura de rede. Manter um perímetro de rede local rígido não é mais suficiente para proteger uma força de trabalho móvel e distribuída, ao mesmo tempo em que conciliar vários serviços de segurança para proteger uma infraestrutura híbrida pode ser caro, criar dores de cabeça para que as equipes de TI implantem e gerenciem e deixar enormes lacunas de segurança.

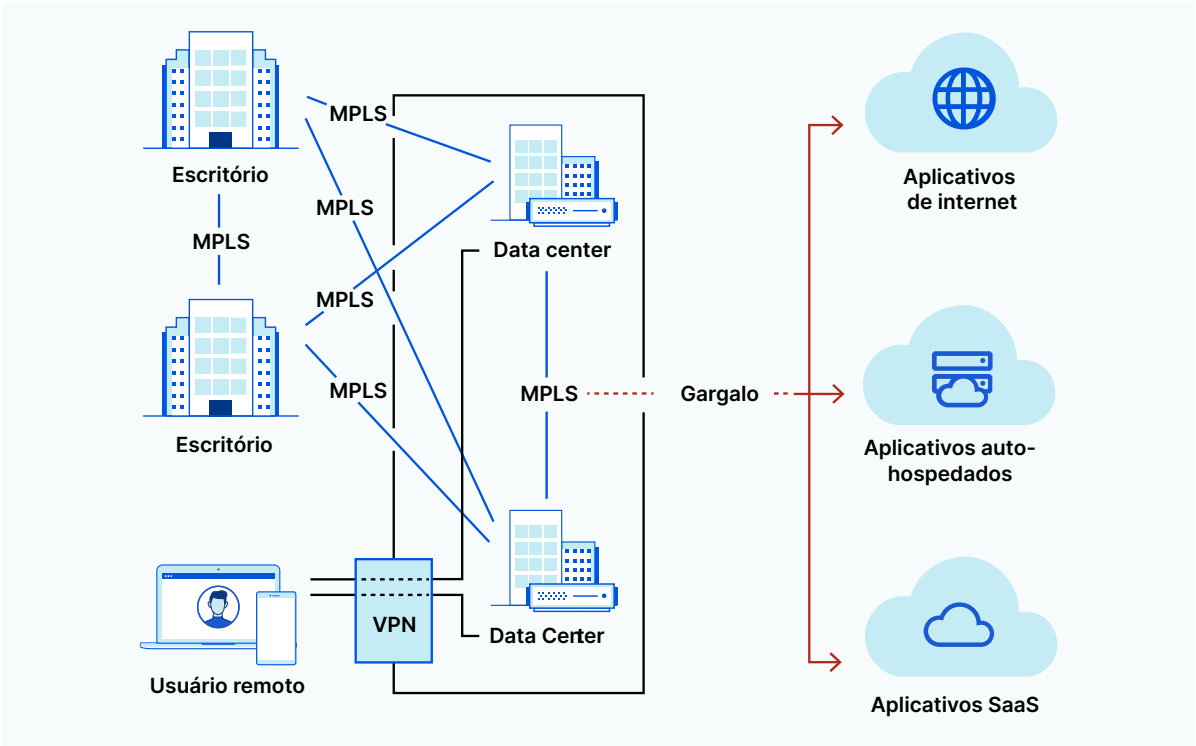
O SASE aborda esses desafios ao mudar o perímetro da rede de data centers centralizados para o usuário. Ao consolidar serviços de rede e de segurança de rede e fornecê-los a partir de uma única plataforma nativa da nuvem com base nos princípios Zero Trust, o SASE elimina as lacunas de segurança entre os serviços, oferece às equipes de TI maior visibilidade da atividade da rede e simplifica o processo de migração para a nuvem.

AS ORIGENS DO SASE — MODELO ANTIGO

Para entender a mudança essencial que o SASE representa, é importante examinar a evolução gradual da infraestrutura e segurança de rede.

Antes da adoção generalizada da computação em nuvem, recursos corporativos, dados e aplicativos viviam dentro de instalações locais protegidas por firewalls de hardware e dispositivos DDoS. Os funcionários de um escritório corporativo acessavam recursos internos por meio de conexões privadas filtradas por firewalls de rede. Os usuários que se conectavam de locais remotos geralmente o faziam através de uma VPN, que era propensa a latência e sobrecarga para evitar superlotação, vulnerabilidades de patch e experiências móveis ruins.

A base dessa configuração era o medo da internet aberta — uma ferramenta que foi construída principalmente para resiliência, com pouca consideração pela performance empresarial e pelas necessidades de segurança. Como a internet provou ser inerentemente vulnerável a ataques, as organizações optaram por estabelecer suas próprias redes privadas que protegeram (muitas vezes de forma ineficaz) dados, aplicativos e recursos corporativos com caixas de firewall físicas e dispositivos DDoS e criaram o efeito trombone em todo o tráfego de entrada por meio de data centers para inspeção e filtragem.



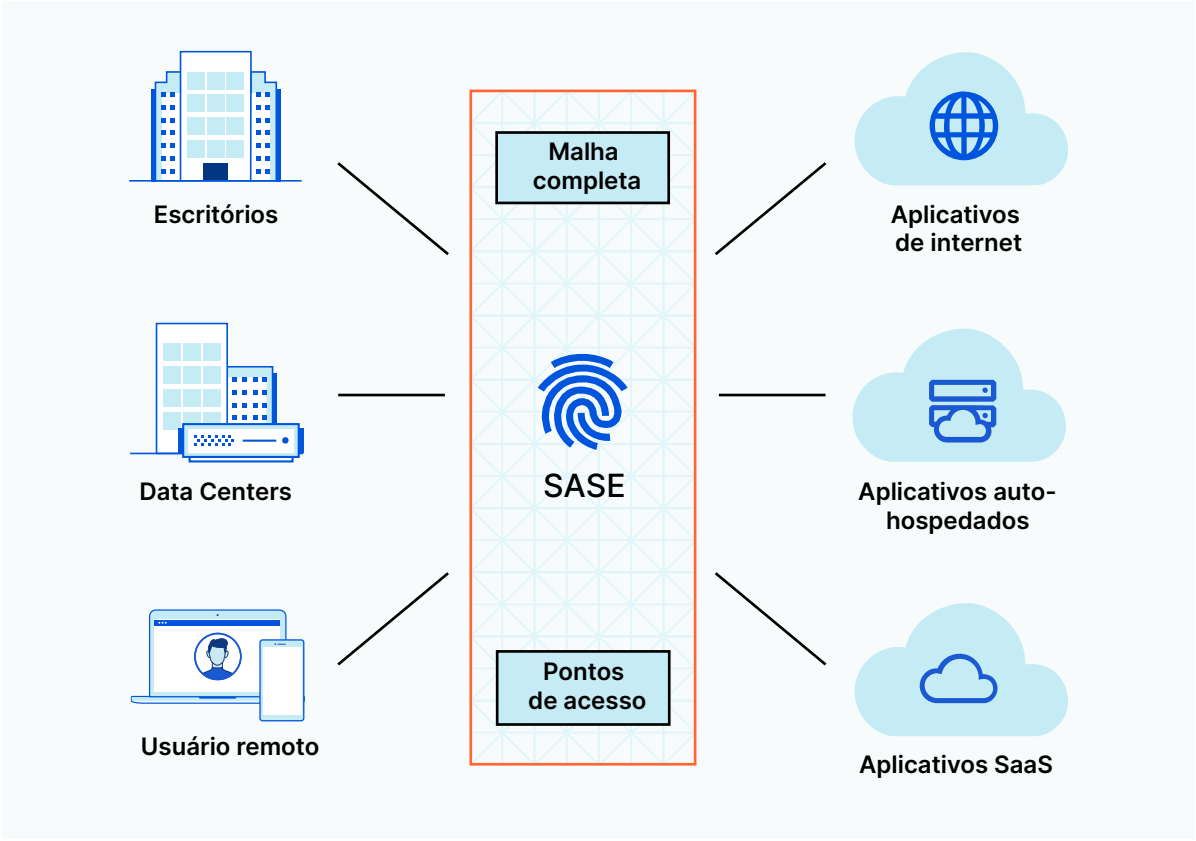
Esse modelo de segurança de rede era caro e complexo e ainda deixava as organizações vulneráveis a invasão de dados e ameaças internas. Uma vez que um invasor violava o perímetro da rede, ele podia causar danos significativos em uma organização espalhando ransomware, assumindo o controle das contas de usuários[2] e roubando dados importantes de clientes. [3]

Com o advento dos serviços de nuvem e SaaS, as organizações têm mais liberdade e flexibilidade para reimaginar sua infraestrutura de rede, já que aplicativos, dados e funcionários não precisam mais residir exclusivamente nas instalações locais.

AS ORIGENS DO SASE — MODELO NOVO

No entanto, com essa liberdade surgem novos desafios de segurança. As equipes de TI têm a tarefa de proteger uma mistura de serviços locais e baseados em nuvem, além de garantir uma força de trabalho cada vez mais móvel e remota.[4] Fazer isso com sucesso geralmente requer manutenção de hardware cara e serviços de segurança em camadas de ponto único de vários fornecedores, o que pode ser demorado para implementar e difícil de gerenciar.

A próxima evolução da segurança de rede provavelmente não se assemelhará ao hardware que protegeu a tradicional infraestrutura de "hub-and-spoke" ou as soluções alternativas complexas exigidas por uma arquitetura de nuvem híbrida. Em vez disso, ela se assemelhará a uma estrutura SASE, que consolida serviços de rede e segurança e os entrega como um serviço integrado.



Em vez de depender de dispositivos de hardware ineficazes ou juntar serviços de segurança em silos, o SASE oferece uma abordagem simplificada para a segurança de rede. Ele substitui o backhauling complicado pela borda da internet, permitindo que as empresas encaminhem, acelerem, verifiquem, filtrem, isolem e inspecionem o tráfego em uma única passagem. Junto com conectividade WAN de malha completa, políticas de acesso Zero Trust e proteção contra ameaças no nível de rede, o SASE elimina a necessidade de VPNs obsoletas e circuitos MPLS, bem como firewalls de hardware, proxy e dispositivos de proteção contra DDoS, oferecendo às empresas mais visibilidade e controle sobre suas configurações de segurança de rede.

DEFINIÇÃO DO ESCOPO DO SASE — PRINCIPAIS RECURSOS

O SASE é um modelo de segurança baseado em nuvem que combina redes de longa distância definidas por software com os principais serviços de segurança de rede e os entrega na borda da nuvem. A maioria das ofertas SASE são caracterizadas por cinco recursos principais:

Construir e gerenciar redes

Uma rede de longa distância definida por software (SD-WAN) permite que as organizações estabeleçam redes corporativas privadas sem a assistência de roteadores de hardware ou circuitos de comutação de etiquetas multiprotocolo (MPLS). Essa arquitetura virtual baseada em software oferece às empresas maior flexibilidade ao criar e manter sua infraestrutura de rede, embora também venha com algumas vulnerabilidades de segurança incorporadas.

Filtragem de tráfego

Um gateway seguro da web (SWG): evita ameaças cibernéticas e invasão de dados, filtrando o conteúdo indesejado do tráfego da web, bloqueando comportamentos não autorizados do usuário e implementando as políticas de segurança da empresa. Geralmente inclui filtragem de URL, detecção e bloqueio de malware e controle de aplicativos, entre outros recursos.

Proteção de dados

Um agente de segurança de acesso à nuvem ou CASB, desempenha várias funções de segurança para serviços hospedados na nuvem (por exemplo aplicativos SaaS, IaaS e PaaS). Os CASBs padrão garantem a confidencialidade de dados através do controle de acesso e prevenção de perda de dados, revela TI invisível e garante a conformidade com os regulamentos de privacidade de dados.

Conectar usuários a aplicativos

O acesso à rede Zero trust (ZTNA) requer verificação em tempo real de cada usuário para cada aplicativo protegido, a fim de proteger recursos internos e se defender contra possíveis invasão de dados. Com uma abordagem “Zero trust”, nenhuma entidade é automaticamente confiável até que sua identidade seja autenticada — mesmo se ela já estiver dentro do perímetro de uma rede privada.

Proteger aplicativos e infraestrutura

Os firewalls baseados em nuvem (FWAAs) protegem a infraestrutura e os aplicativos em nuvem contra ataques cibernéticos por meio de um conjunto de recursos de segurança que inclui filtragem de URL, prevenção de intrusões e gerenciamento de políticas uniforme.

DEFINIÇÃO DO ESCOPO DO SASE — MELHORES RECURSOS DA CATEGORIA

Embora uma solução SASE convencional inclua os cinco serviços descritos acima, a lista é mais um ponto de partida do que um conjunto rigoroso de requisitos. O SASE, essencialmente, converge dois recursos fundamentais e separados — arquitetura de rede baseada em software e serviços de segurança baseados em nuvem — além disso, os fornecedores podem adicionar ou subtrair serviços adicionais conforme necessário.

Embora a SD-WAN ajude os clientes a gerenciar a última milha da conectividade de rede, ela não pode garantir diretamente a segurança, a performance e a confiabilidade da milha intermediária entre usuários e aplicativos. Na melhor das hipóteses, ela pode otimizar as conexões de ponta a ponta confiando em várias redes globais e encadeando vários serviços de segurança, o que é complexo e caro. Um provedor SASE que cria uma WAN como serviço do zero -- com ou sem SD-WAN -- permite que os clientes gerenciem apenas uma rede global com segurança, performance e confiabilidade integrados por padrão. SWG, CASB e ZTNA juntos reduzem muito os riscos de segurança, mas a combinação ainda deixa muitas lacunas na proteção de ameaças e dados em todos os casos de uso. Um provedor SASE que cria o isolamento remoto do navegador do zero para integrar nativamente com SWG, CASB e ZTNA em cada data center elimina essas lacunas.

BENEFÍCIOS DE UMA ABORDAGEM SASE

À medida que continua a evoluir, a implementação do SASE pode variar consideravelmente de fornecedor para fornecedor e organização para organização. A maioria das soluções SASE, no entanto, compartilha várias vantagens importantes em relação às configurações de segurança de rede híbrida e local:

Implementação simplificada

Ao consolidar serviços de rede e segurança, o SASE elimina a necessidade de serviços de integração baseados em nuvem, de configurar dispositivos locais e de investir tempo, dinheiro e recursos internos para manter ambos atualizados contra as ameaças mais recentes.

Gerenciamento de políticas simplificado.

O SASE permite que as organizações configurem, monitorem, ajustem e implementem políticas de acesso para todos os locais, usuários, dispositivos e aplicativos. Ataques e ameaças recebidas podem ser identificados e mitigados a partir de um único portal, ao invés de monitorados e gerenciados individualmente com várias ferramentas de segurança de finalidade única.

Acesso à rede baseado em identidade

O SASE se apoia profundamente em um modelo de segurança Zero Trust, no qual a identidade do usuário e o acesso é concedido com base em uma combinação de fatores: localização do usuário, hora do dia, padrões de segurança corporativos, políticas de conformidade e uma avaliação contínua de risco/confiança. Esse nível de segurança — um avanço significativo em relação à VPN excessivamente permissiva e inerentemente vulnerável — protege contra invasões de dados externas e internas e outros ataques.

Latência reduzida

O SASE reduz a latência e melhora a performance ao rotear o tráfego de rede através de uma rede de borda extensa cujo tráfego é processado o mais próximo possível do usuário. As otimizações de roteamento podem ajudar a determinar o caminho de rede mais rápido com base no congestionamento da rede e em outros fatores.

Rede global

Uma estrutura SASE é construída sobre uma única rede global, permitindo que as organizações expandam seu perímetro de rede para qualquer usuário remoto, filial, dispositivo ou aplicativo e ganhe mais visibilidade e controle em toda a sua infraestrutura de rede.

NOÇÕES BÁSICAS DE SASE

Para empresas que investiram muito tempo, recursos e dinheiro em elaboradas configurações locais, gerenciam redes complexas de serviços de segurança baseados em nuvem ou ainda estão se ajustando ao futuro do trabalho remoto, a adoção do SASE pode parecer assustadora — mas não tem que ser.

Aqui estão cinco etapas práticas que você pode seguir para começar a usar o SASE:

1. Proteger sua força de trabalho remota.

Implemente uma solução ZTNA que permitirá reduzir a dependência ou até mesmo substituir sua VPN, proteger dados corporativos e recursos contra ameaças internas e externas e melhorar a experiência do usuário. Ao trazer seu gateway seguro de web, firewall e navegadores de dispositivos para a borda, você pode filtrar, isolar e inspecionar o tráfego sem backhaul através de um data center central.

2. Colocar filiais atrás de um perímetro de nuvem.

Aplique uma arquitetura Zero Trust às filiais que removerá a necessidade de dispositivos de segurança no local (gerenciamento unificado de ameaças, etc.), que podem ser dispendiosos para manter e ineficazes contra um cenário de ameaças em rápida evolução.

3. Mover a proteção contra DDoS para a borda.

Livre-se de dispositivos DDoS e defenda as redes corporativas contra ataques com proteção contra DDoS na camada de rede nativa de nuvem, que pode detectar e mitigar ameaças em tempo real.

4. Migrar aplicativos para a nuvem.

À medida que sua organização se expande, mova aplicativos auto-hospedados de seus data centers para a nuvem e certifique-se de aplicar políticas de segurança de rede consistentes em todo o tráfego.

5. Substitua os dispositivos de segurança no local por aplicação de políticas unificadas e nativas de nuvem.

Reduza o custo e a complexidade da manutenção de dispositivos de hardware de rede mudando a aplicação de políticas para a borda, onde você pode monitorar em uma única passagem e gerenciar em um único painel todo o tráfego, padrões de ataque e políticas de segurança.

O SASE DA CLOUDFLARE É O CLOUDFLARE ONE

O Cloudflare One é uma plataforma de rede como serviço Zero Trust que conecta dinamicamente os usuários aos recursos corporativos, com controles de segurança baseados em identidade entregues próximos aos usuários, onde quer que estejam.

Com os serviços de rede do Cloudflare One, as equipes de infraestrutura podem:	Com os serviços Zero Trust do Cloudflare One, as equipes de segurança de TI podem:
• Use a rede global da Cloudflare como sua WAN. • Substitua dispositivos obsoletos por um firewall de rede nativo de nuvem. • Melhore a performance do aplicativo e a reduza a latência para o usuário final.	• Conecte usuários a recursos de forma simples e segura, sem VPN. • Bloqueie movimento lateral, ransomware, malware e phishing. • Melhore a experiência do usuário final e o esforço de administração, especialmente o tempo de integração.

Por que a Cloudflare?

Implantação e gerenciamento simples

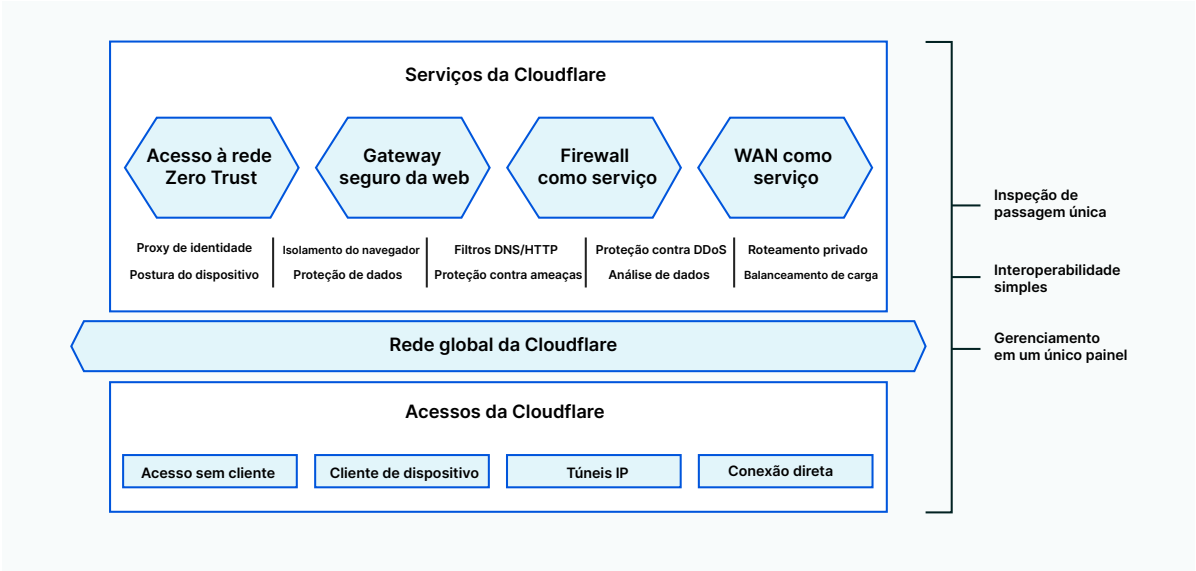
Todos os serviços do Cloudflare One são executados em cada uma das nossas mais de 250 cidades ao redor do mundo. Não é preciso integrar manualmente vários produtos pontuais ao progredir para um modelo SASE.

Segurança e velocidade consistentes em qualquer lugar do planeta

Todos os data centers da Cloudflare oferecem inspeção de tráfego de passagem única e roteamento, o que protege os usuários em qualquer lugar do planeta da mesma forma — sem perder velocidade devido à latência ou ao "efeito de trombone".

Se conecta com as ferramentas que você já usa

A Cloudflare administra a Rede mais poderosa e com maior troca de tráfego do mundo e o Cloudflare One dá suporte à identidade, endpoint e aos provedores de nuvem que você já usa. Fácil de usar, integração única.



O SASE DA CLOUDFLARE É O CLOUDFLARE ONE

O Cloudflare One oferece os recursos de segurança e conectividade de que você precisa para conectar usuários, aplicativos e filiais em um mundo de trabalho remoto.

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>Acesso à rede Zero Trust
Conecte qualquer usuário a qualquer aplicativo e rede privada com mais rapidez e segurança que a VPN por meio da imposição de regras baseadas em identidade e contexto e da limitação do movimento lateral.

Principais recursos do SASE:
• Conectar usuários a aplicativos
• Proteção de dados</td><td>WAN como serviço
Habilite todos os tipos de conectividade com uma performance mais rápida, segurança integrada e mais resiliência substituindo a arquitetura WAN obsoleta pelo nosso backbone privado global.

Principal recurso do SASE:
• Construir e gerenciar redes</td></tr>
<tr><td>Gateway seguro da web
Bloqueie ameaças conhecidas e desconhecidas da internet — e controle facilmente os fluxos de dados — pela imposição de regras de DNS, HTTP, rede e isolamento do navegador com inspeção SSL ilimitada.

Principais recursos do SASE:
• Filtrar e inspecionar o tráfego
• Proteção de dados</td><td>Firewall como serviço
Controle o acesso — e bloqueie ataques DDoS e outras ameaças — com a imposição de regras de inspeção com estado em todo o tráfego de entrada e saída, ao mesmo tempo em que mantém uma performance rápida.

Principal recurso do SASE:
• Proteger aplicativos e infraestrutura</td></tr>
<tr><td colspan="2">Rede global da Cloudflare
A 50 ms de 95% da população conectada à internet, nossa Rede opera em mais de 250 cidades com mais de 100 Tbps de capacidade, mais de 10 mil interconexões e um SLA de 100% de tempo de atividade.</td></tr>
<tr><td>Acesso sem cliente
Integre qualquer usuário ou dispositivo em questão de minutos — incluindo terceiros e BYOD — com acesso seguro baseado em navegador a aplicativos SaaS e auto-hospedados, além de HTTP.</td><td>Túneis IP
Integre sub-redes IP públicas e privadas inteiras por meio de anúncios de rota BGP Anycast com túneis GRE ou nosso próprio conector de túnel na nuvem ou em ambientes locais.</td></tr>
<tr><td>Cliente de dispositivo
Integre dispositivos Windows, macOS, iOS, Android, ChromeOS e Linux para acesso seguro baseado em cliente a qualquer aplicativo, rede privada ou destino da internet.</td><td>Conexão direta
Integre sua infraestrutura de rede, física ou virtualmente, a mais de 1.600 instalações de colocation — em vez de na internet pública — para ter uma experiência mais confiável e segura.</td></tr>
</table>

RESULTADOS COMERCIAIS COM O USO DO CLOUDFLARE ONE

↓91%

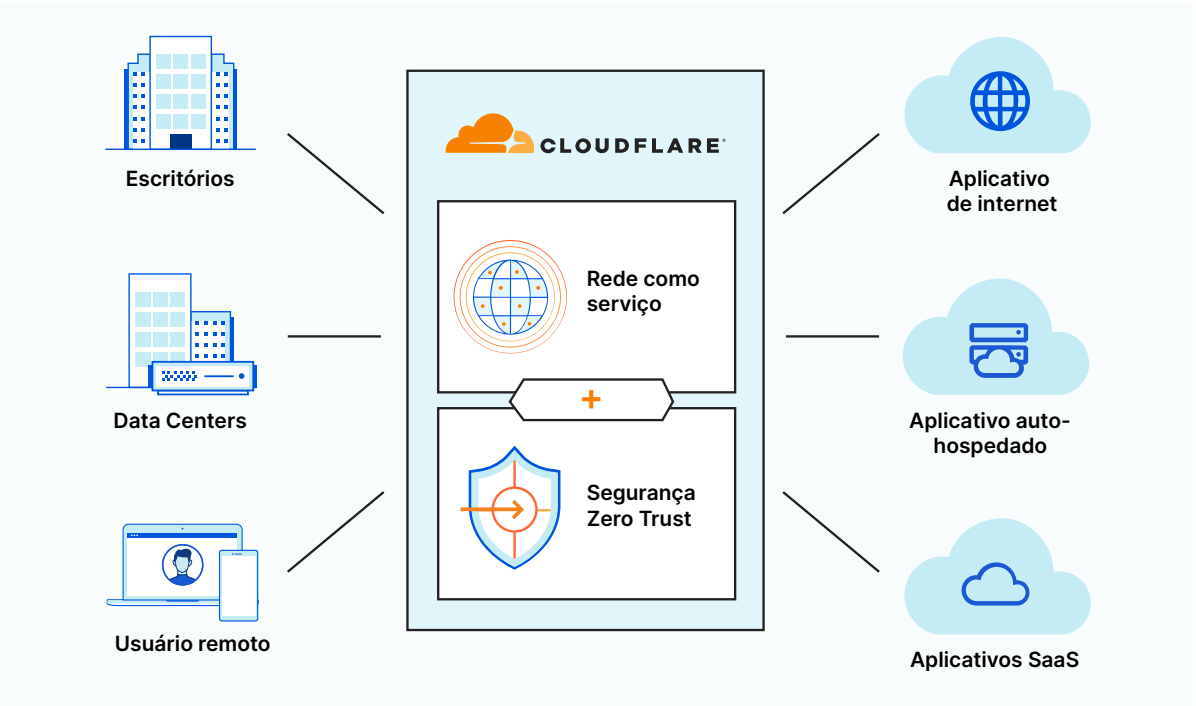
Diminua a superfície de ataque em até 91% ao isolar a navegação de alto risco dos sistemas do usuário final e isole o acesso a aplicativos a partir das redes.

10 → 1

TCO menor e negócios acelerados com a consolidação de até dez produtos pontuais em uma plataforma.

↑60%

Integre novos funcionários e terceiros até 60% mais rápido conectando usuários a recursos por meio da Cloudflare em vez de uma VPN.



Saiba mais sobre o Cloudflare One

Clique aqui

REFERÊNCIAS

1. Gartner, “The Future of Network Security Is in the Cloud.” Analista(s): Neil MacDonald, Lawrence Orans, Joe Skorupa. 30 de agosto de 2019. Gartner.

2. Twitter Inc. “An update on our security incident.” Twitter. Acessado em 27 de outubro de 2020.

3. Marriott International News Center. “Marriott International Notifies Guests of Property System Incident.” Marriott. Acessado em 27 de outubro de 2020.

4. Bursztynsky, Jessica. “Dropbox is the latest San Francisco tech company to make remote work permanent.” CNBC. CNBC. Acessado em 27 de outubro de 2020.