CLOUDFLARE

RESUMO DA SOLUÇÃO

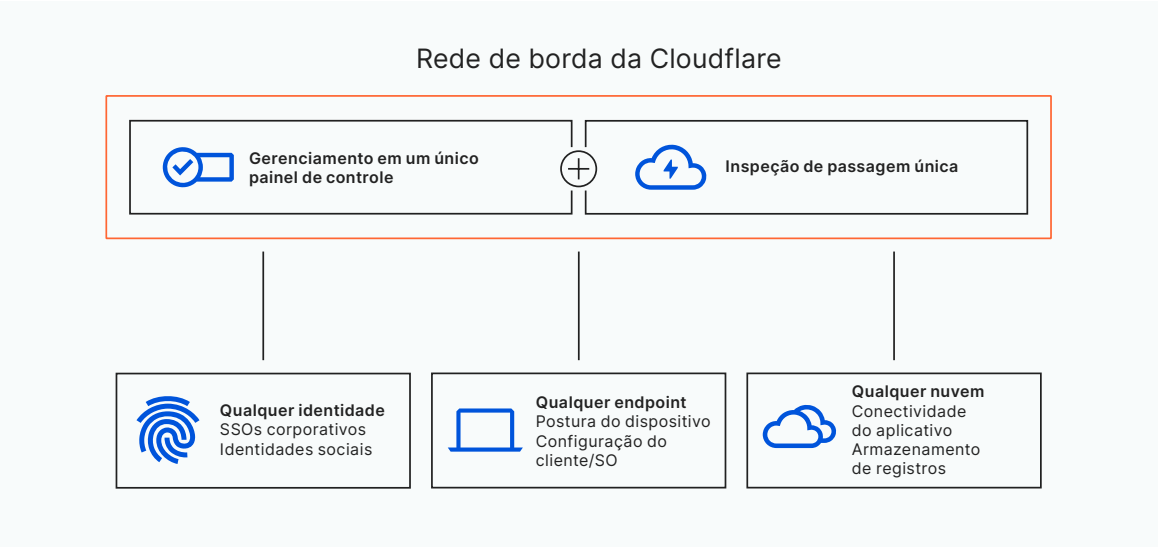
Integrações com o Zero Trust da Cloudflare

Desenvolva com os provedores de identidade, endpoint e nuvem que você já usa

Fazer malabarismos com vários provedores de identidade, endpoint e nuvem dentro de uma organização é inevitável, mas não precisa ser oneroso. Na Cloudflare, nosso objetivo é fortalecer sua organização com segurança mais robusta da maneira mais fácil de usar. Ao contrário de outros fornecedores, não temos nenhum interesse em provedores específicos nessas categorias com os quais você trabalha hoje ou no futuro.

Somos independentes. Portanto, nossa estratégia de longa data tem sido projetar o Zero Trust da Cloudflare para se integrar com o maior número possível de outras soluções.

Por meio de integrações, a Cloudflare agrega sinais em vários provedores e fornece um único painel de controle para aplicar políticas granulares e ricas em contexto em toda a nossa rede global. Além disso, essas integrações não requerem pesquisa de documentação técnica densa; elas são pré-criadas como fluxos de trabalho para um gerenciamento de painel único mais simples.



Destacamos três princípios que seguimos para atender os clientes onde quer que estejam:

- **Independente de identidade:** autenticar usuários em vários tipos de provedores de identidade para acesso sem atrito para todos os usuários sem problemas de configuração.
- **Independente de endpoint:** enriquecer as verificações de postura do dispositivo de maneiras mais granulares e adaptáveis com sinais de seus provedores de endpoint favoritos e de nosso cliente de dispositivo.
- **Independente de nuvem:** aplicativos seguros em qualquer nuvem pública ou privada (no local) para evitar o aprisionamento tecnológico no longo prazo.

Agregue várias identidades à Cloudflare

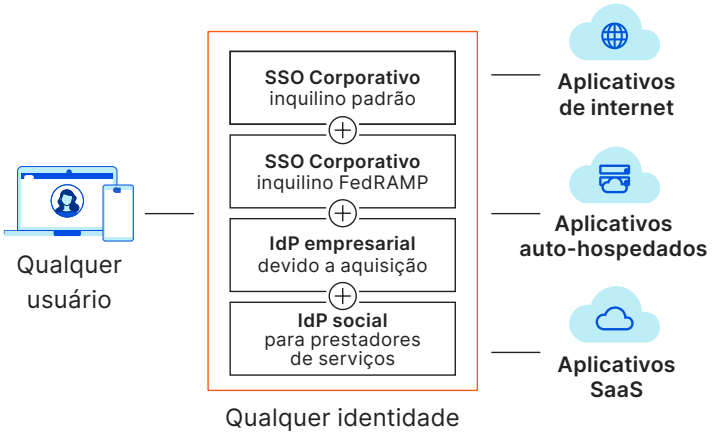
Multi-SSO

A Cloudflare criou uma das primeiras soluções de acesso Zero Trust para oferecer suporte a vários provedores de identidade (IdPs) simultaneamente. Hoje, integramos os principais IdPs corporativos (como Okta ou Azure AD), bem como identidades sociais (como LinkedIn ou Github) e padrões de código aberto (como SAML ou OIDC). Além disso, somos compatíveis com várias instâncias do mesmo IdP: por exemplo, uso de Okta com e sem FedRAMP.

Federe várias identidades de uma só vez

Nossa capacidade de federar identidades nos diversos IdPs pode agilizar o processo de criação de políticas sensíveis a identidades. As organizações já não precisam desenvolver integrações personalizadas entre seus IdPs.

As organizações em estágio de crescimento com pessoal de infosec mais limitado podem considerar a federação uma ferramenta particularmente poderosa para escalar uma abordagem Zero Trust sem o incômodo de consolidar um diretório centralizado único.



Principais recursos

- A Cloudflare integra-se com vários IdPs simultaneamente, os melhores da categoria
- Federar vários provedores e várias instâncias de cada provedor
- Integração mais rápida para usuários terceirizados e parceiros de fusões e aquisições

Caso de uso:

Fazer com que usuários terceirizados se sintam cidadãos de primeira classe

A abordagem independente de identidade da Cloudflare é particularmente útil ao colaborar com terceiros fora de sua organização, como prestadores de serviços, empresas adquiridas ou parceiros. As regras de acesso com menos privilégios podem ser configuradas em minutos com base nas identidades que esses usuários já trazem para a mesa.

Essa flexibilidade descomplicada evita as ineficiências e os riscos de segurança do provisionamento de licenças de SSO, implantação de VPNs ou criação de permissões únicas.

Os melhores parceiros de proteção de endpoints da categoria

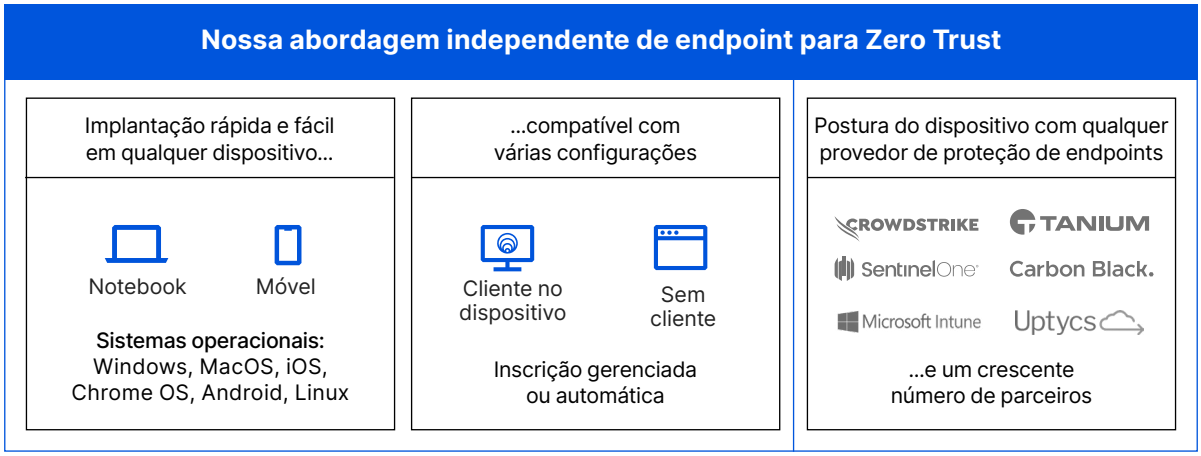
Parcerias

A Cloudflare é parceira da CrowdStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs e Microsoft Intune.

Os clientes podem integrar vários provedores de proteção de endpoints de uma só vez e aproveitar os sinais de segurança e os recursos de avaliação de risco dessas soluções.

Configuração

A configuração de qualquer um desses provedores requer apenas alguns cliques no painel de controle da Cloudflare com fluxos de trabalho predefinidos. Depois de configurada, a Cloudflare pode verificar se os dispositivos estão executando seu software de endpoint preferido para fornecer monitoramento contínuo contra malware e outras ameaças antes de permitir ou negar o acesso a um aplicativo protegido.



Integrações aprimoradas pelo nosso cliente de dispositivo (WARP)

Aumentar o nível de segurança geralmente requer um cliente de dispositivo, que pode enriquecer as verificações de postura do dispositivo com atributos adicionais. Otimizamos deliberadamente o nosso para uma adoção flexível e sem esforço.

É implantado na maioria dos sistemas operacionais

- Nosso cliente corporativo, WARP, funciona em uma lista crescente de sistemas operacionais mais populares (por exemplo, Windows, macOS, Linux, iOS, ChromeOS e Android).
- Nossa arquitetura WireGuard moderna requer apenas pequenos ajustes de código, específicos do sistema operacional.
- Nosso cliente corporativo tem uma versão para consumidores usada diariamente por milhões em todo o mundo. Ser testado por tantos usuários individuais significa que o WARP está mais preparado para o combate do que a maioria dos clientes usados para o Zero Trust.

Opções de inscrição gerenciada ou automática

- Para dispositivos gerenciados, documentamos implantações com qualquer método baseado em script em softwares populares de gerenciamento de dispositivos móveis (MDM).
- A autoinscrição do WARP pode ser útil para usuários de terceiros e leva apenas alguns minutos em qualquer desktop ou telefone celular.

Evite a dependência de provedores de nuvem

Problema

Alguns fornecedores mais monolíticos estão interessados principalmente em aumentar o consumo de seus serviços em nuvem, principalmente nas camadas de armazenamento e computação.

Não é de surpreender que suas soluções de segurança complementares não se integram tão bem quanto deveriam com outros provedores de nuvem. Pequenos inconvenientes como documentação mais fraca e bugs se acumulam. Essa dependência da pilha de tecnologia torna a vida das suas equipes de infosec mais difícil.

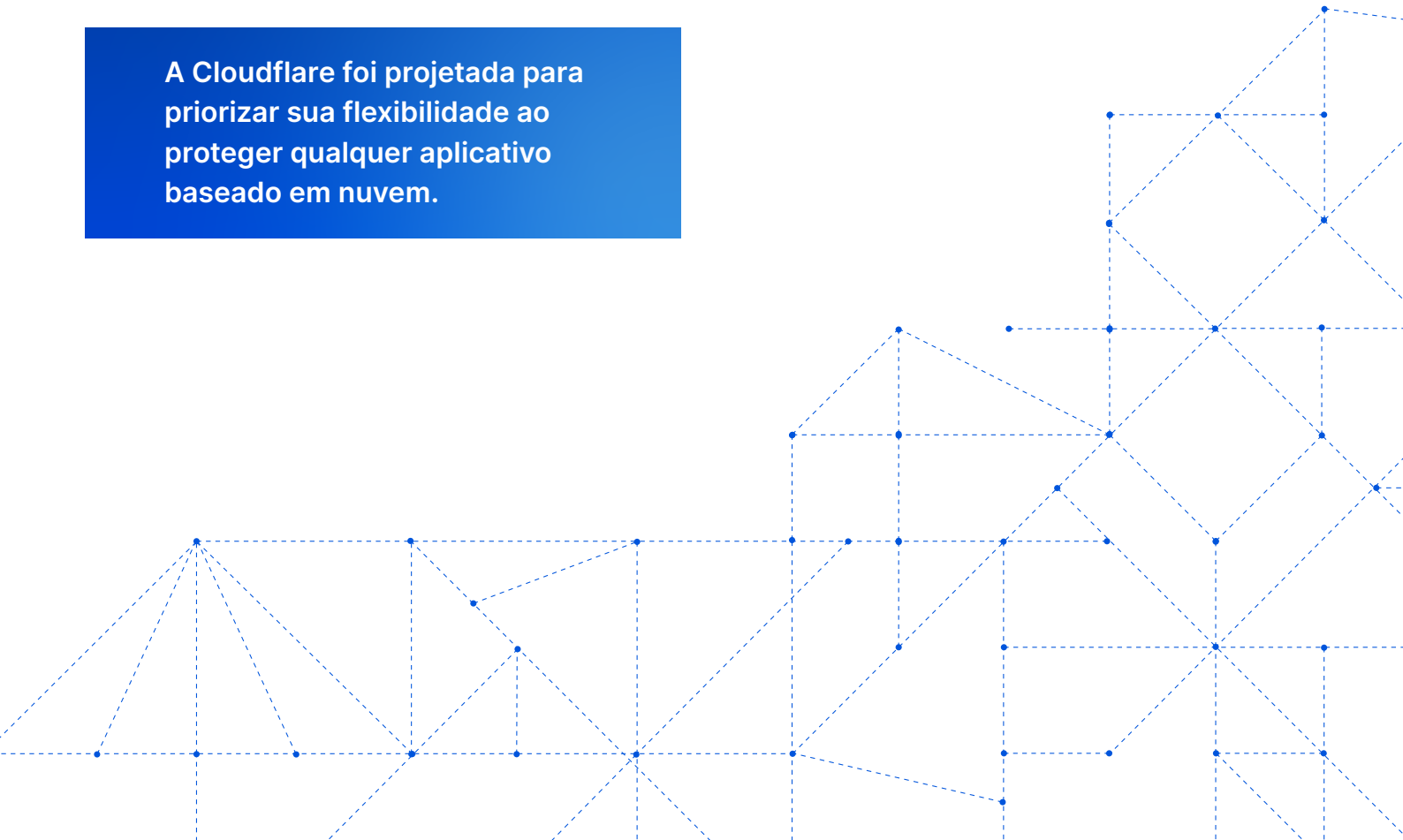
Solução

Por outro lado, nosso foco estratégico é sua segurança, não seu consumo de nuvem. A Cloudflare é independente de nuvem: protegemos o acesso a qualquer recurso em qualquer ambiente de nuvem pública, privada ou SaaS.

A Cloudflare foi projetada para priorizar sua flexibilidade ao proteger qualquer aplicativo baseado em nuvem.

Principais recursos

- Acesso Zero Trust em ambientes de nuvens públicas, privadas e SaaS
- Sem dependência de fornecedor para destinos de armazenamento ou computação em nuvem
- Conectores de aplicativos, parceiros de acesso à rede e integrações de armazenamento que facilitam a interação com aplicativos em qualquer nuvem



Pontos fortes da Cloudflare

Estender conexões para aplicativos em qualquer nuvem

Nosso conector de aplicativo leve funciona em todas as nuvens

- Executa a ferramenta de linha de comando como serviço no Linux e em outros sistemas operacionais
- Pacotes predefinidos como um contêiner do Docker
- Suporte de réplica para ambientes Kubernetes modernos
- O túnel pode ser configurado e monitorado por meio da IU

Amplas interconexões com provedores de nuvem

- Conexões rápidas para usuários habilitadas por 11.000 interconexões entre nossa rede e outros provedores de nuvem, 50 das quais são interconexões privadas com data centers da Microsoft, Amazon e Google

Diversos parceiros de acesso de rede que não são específicos de nuvem

- Conecte facilmente qualquer ambiente de nuvem pública e privada à nossa rede usando seu método de roteamento SD-WAN existente (por exemplo, VMware) ou interconecte-se de forma privada em mais de 1.600 locais de provedores de colo (por exemplo, Equinix)

Envie dados de registro para qualquer nuvem

Os dados de registros podem ser armazenados em nuvens ou enviados diretamente para provedores de análise de dados

- Compatibilidade integrada para um ou mais destinos de armazenamento simultâneos, incluindo AWS, Azure, Google Cloud e qualquer API compatível com S3 (por exemplo, Digital Ocean Spaces)
- Integrações incorporadas com ferramentas de análise de dados e SIEM como Sumo Logic, Splunk e Datadog.

Segurança em qualquer nuvem pública ou privada

Lista de parceiros de integração Zero Trust

Com o tempo, a Cloudflare vai agregar sinais a partir de uma lista ainda mais ampla de seus provedores preferidos, todos reforçados pela inteligência de nossa plataforma Zero Trust e rede global.

Provedores de identidade

SSOs corporativos

- Centrify
- Citrix ADC
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- Ping Identity

Identidades sociais

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Open Source

- OIDC
- SAML 2.0

Provedores de endpoints

Provedores de proteção de endpoints

(para postura de segurança do dispositivo)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

Provedores de gerenciamento de endpoints

(para implantação no cliente)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

Parceiros de rampas de acesso à rede

Parceiros de interconexão física

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Parceiros de interconexão de malha

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

Provedores de nuvem

Destinos para armazenamento em nuvem

- AWS S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- Outros fornecedores com API compatível com S3

Parceiros de análise de dados em nuvem e SIEM

- Azure Sentinel
- Datadog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

Para saber mais sobre o Zero Trust da Cloudflare e solicitar uma demonstração ou POC de um representante de vendas, acesse: https://www.cloudflare.com/pt-br/products/zero-trust/.

CLOUDFLARE

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-3795.2022SEP26