CLOUDFLARE

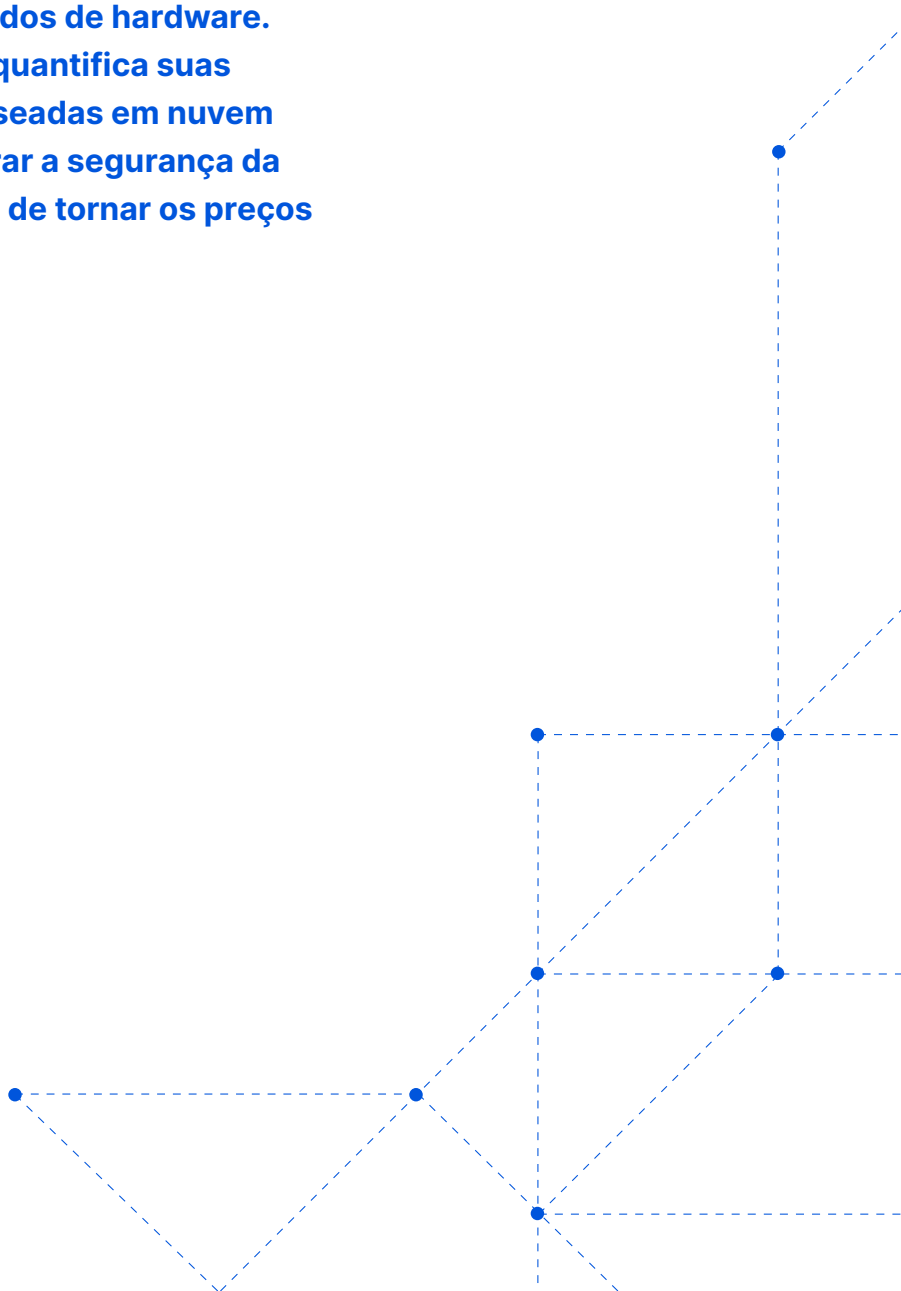
ARTIGO TÉCNICO

# O fim dos dispositivos de hardware de rede

Por que chegou a hora de se libertar do hardware de rede

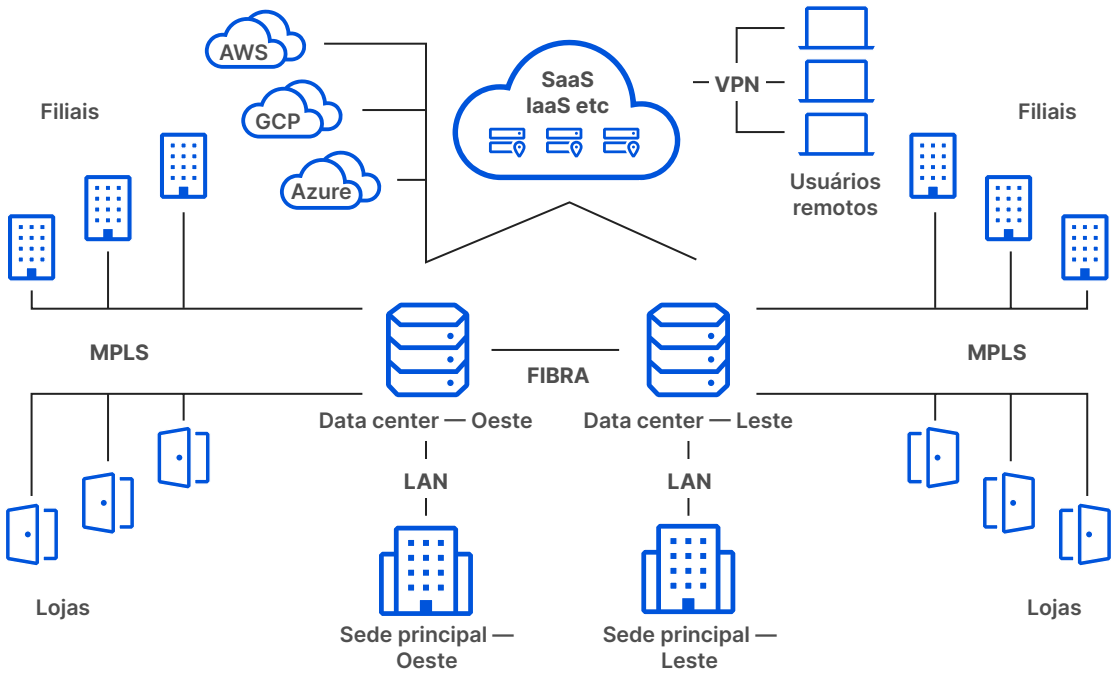
# Sumário executivo

**Embora o armazenamento e a computação tenham migrado para a nuvem, muitas funções de rede continuam no local, criando limitações de capacidade, alto custo total de propriedade, dificuldades de suporte e falhas de segurança. As organizações estão lutando para garantir que uma capacidade adequada e uma segurança eficaz para o trabalho híbrido se tornem padrão. Muitos projetos de transformação estão emperrados há mais de um ano devido a filas de espera para pedidos de hardware. Este artigo descreve esses desafios, quantifica suas consequências e propõe soluções baseadas em nuvem para aumentar a velocidade e aprimorar a segurança da infraestrutura de nuvem híbrida, além de tornar os preços mais acessíveis.**



# Introdução

Migrar para a nuvem tem comprovado ser uma estratégia eficiente para reduzir custos de infraestrutura, aumentar a disponibilidade de dados e aplicativos e aprimorar a agilidade operacional. No entanto, a migração raramente acontece de uma só vez. Muitas organizações de grande porte acabam se vendo com uma mistura complexa de infraestrutura local e em nuvem.




Esse tipo de infraestrutura híbrida não é necessariamente ruim, mas cria complicações. Especificamente, cria situações em que várias funções de rede — como mitigação de DDoS, balanceamento de carga, firewall e VPN — permanecem no local.

Esses dispositivos de hardware de rede obsoletos não estão à altura de sua tarefa de proteger e acelerar a infraestrutura crítica em um mundo com foco na nuvem. Na verdade, sempre foram um incômodo, uma confusão de equipamentos caros e desorganizados conectados a um emaranhado de cabos. Assim que a nuvem é adicionada a esse estado de coisas, as falhas de segurança, a deterioração da performance e mais desafios de suporte surgem rapidamente.

Este artigo descreve os riscos e armadilhas da opção de manter o hardware de rede em um mundo que está migrando para os serviços baseados em nuvem, além de oferecer estratégias para desenvolver uma rede mais segura e mais eficaz.

# Os riscos do hardware em um mundo em nuvem

Os dispositivos de hardware de rede abarcam uma variedade de funções específicas e são usados de modo diferente por cada organização.

Veja alguns exemplos comuns:

### Segurança

- Proteção contra DDoS
- Firewall
- Rede Privada Virtual
- Políticas configuráveis

### Performance e confiabilidade

- Balanceamento de carga
- Aceleração de tráfego/ Otimização de WAN
- Filtragem de pacotes
- Análises de dados de tráfego

Quando esse hardware é implantado no local, a arquitetura resultante geralmente fica exposta a cinco categorias de risco: **pressões da cadeia de abastecimento, limitações de capacidade, alto custo total de propriedade, dificuldades de suporte** e **falhas de segurança**.

As três primeiras categorias sempre impuseram desafios até mesmo para as mais sofisticadas redes e equipes de segurança. As outras duas são exacerbadas pela migração para a nuvem.

## Pressões da cadeia de abastecimento

Como qualquer tipo de produto físico, o hardware de rede é vulnerável a diversas dificuldades da cadeia de abastecimento. Quando os custos de matéria prima sobem, determinados materiais e componentes se tornam mais difíceis de obter ou os provedores de frete ficam sobrecarregados, o hardware de rede se torna mais difícil de adquirir ou substituir.

Infelizmente, tais dificuldades têm sido comuns ultimamente, em grande parte devido aos efeitos da pandemia de COVID-19. De acordo com a Gartner Research, "Antes da pandemia o comum eram prazos de entrega de 4-6 semanas. Agora, prazos de 200-300 se tornaram comuns e já vimos uma estimativa de mais de 430 dias informada aos clientes em cotações por escrito".

Esses atrasos se devem a diversos fatores:

- **Dificuldades de logística:** os modelos históricos de cadeia de abastecimento têm diversos pontos de falha, forças de trabalho reduzidas ao mínimo e uma forte dependência de tecnologias que podem ou não ser seguras — desafios que cobraram seu preço recentemente. Durante a pandemia, muitas fábricas foram fechadas, empresas de frete enfrentaram atrasos e muitos tipos de trabalhadores da cadeia de abastecimento se tornaram difíceis de contratar e reter. Todos esses desafios resultam em um prazo mais longo para a fabricação e entrega de hardware. Talvez o aspecto mais difícil de qualquer logística do qual devemos nos lembrar é que o processo se parece a uma corrida de revezamento: o fato de que sua empresa em particular não estar enfrentando dificuldades não significa que você não será afetado por um elo rompido mais à frente na sua cadeia.
- **Custo mais alto de matérias primas:** os dispositivos de hardware de rede dependem de uma série de matérias primas. Devido à sua alta demanda e à sua oferta limitada, os preços dos materiais dispararam, o que significa que não apenas as empresas estão esperando mais para receber os dispositivos necessários para sua rede, mas também pagando quantias significativamente mais altas por eles. Infelizmente, devido a esses desafios, a Gartner espera que os prazos de entrega de dispositivos de hardware continuem longos até o início de 2023 (fonte).

Todos esses desafios resultam em consequências adicionais. Continuarmos com o foco em adquirir, manter e substituir caixas de hardware significa despesas gerais mais altas, mais tempo gasto em planejar ao invés de executar e preocupações extras de segurança quando se trata de garantir e proteger uma cadeia de abastecimento física durante épocas de incerteza. Em vez de manter o foco em logística, prazos de entrega, aquisição e armazenamento de caixas de hardware, as organizações poderiam estar se concentrando nas necessidades de seus clientes.

## Limitações de capacidade

Não é surpresa que, por natureza, os dispositivos de hardware de rede podem ficar sobrecarregados durante picos de tráfego inesperados — seja esse tráfego legítimo ou não. Mas diversas tendências recentes indicam que atingir esses limites é uma preocupação mais comum.

Pense na mitigação de DDoS (Negação de Serviço Distribuída). O maior ataque de DDoS da história, de acordo com a Microsoft, ocorreu em novembro de 2021 e alegou ter alcançado um volume máximo de 3.47 Tbps (fonte). Esses ataques de DDoS teriam sobrecarregado e excedido em muito as caixas de hardware de mitigação de DDoS mais avançadas do mercado, que, de modo geral, fornecem apenas uma fração da capacidade necessária para mitigá-los.

**Em novembro de 2021, o maior ataque de DDoS da história alegou ter atingido o volume máximo de 3,47 Tbps.**

Nem todas as organizações irão atrair ataques dessa magnitude, mas nem todas as organizações tampouco podem ou irão implementar o mais avançado hardware de mitigação de DDoS. Um relatório da Cloudflare descobriu que os ataques volumétricos apresentaram aumento no 1° trimestre de 2021. Na verdade, os ataques acima de 10 Mpps (milhões de pacotes por segundo) aumentaram mais de 300% trimestre a trimestre e os ataques acima de 100 Gbps mais de 645% trimestre a trimestre (fonte). Esse acentuado aumento dos ataques de DDoS não apenas é alarmante, como também esses tipos de ataque teriam sobrecarregado muitas soluções de mitigação baseadas em hardware teoricamente de alta capacidade.

Além disso, o volume do ataque não leva em conta o tráfego legítimo que pode alcançar seu data center ao mesmo tempo.

Caso um ataque menor ocorresse durante um período de tráfego elevado — como o fim de semana de compras da Black Friday, quando em média os pageviews do comércio eletrônico costumam dobrar da noite para o dia (source) — o aumento de tráfego resultante poderia continuar sendo suficiente para forçar o hardware de segurança a ultrapassar seu limite e entrar em colapso.

A mitigação de DDoS é somente um exemplo das limitações de capacidade do hardware local.

Outros exemplos incluem:

**Balanceadores de carga:** um balanceador de carga individual no local pode facilmente ficar sobrecarregado por picos repentinos de tráfego legítimo. Quando isso acontece, pode levar muito tempo para provisionar e instalar um hardware adicional. A alternativa é manter uma capacidade suficiente para as piores situações, mas essa abordagem exige que a organização execute constantemente uma grande quantidade de hardware a um custo muito elevado.

**Redes Privadas Virtuais (VPNs):** o uso de VPNs se tornou muito mais difícil de prever com antecedência. Para muitas organizações, o trabalho totalmente remoto e híbrido se tornou o novo normal, mas a abordagem de uma VPN tradicional requer um planejamento, manutenção e gerenciamento cuidadosos, já que muitas VPNs não foram projetadas para o uso contínuo por uma organização inteira. Quando muitos funcionários usam uma VPN, a conectividade e a confiabilidade são afetadas. Além disso, podem surgir questões de segurança, simplesmente devido à natureza das VPNs e o modo como são projetadas sem nenhum controle Zero Trust. Mais ainda, se uma VPN ficar sobrecarregada, as organizações podem "dividir os túneis" de tráfego de forma que o tráfego destinado à internet não passe pela VPN — tornando difícil monitorar e gerenciar a atividade de um funcionário na web.

Quando esses problemas surgem, uma solução é comprar mais hardware, mais novos e de maior capacidade. Mas essa abordagem cria muitas outras dificuldades.

## Custos de propriedade

Assim como ocorre com as limitações de capacidade, o fato de um hardware de data center ser caro não é nenhuma surpresa. Por exemplo, o hardware necessário para obter aproximadamente 100 Gbps de capacidade de mitigação de DDoS pode custar entre US$ 400 e 500 mil pagos adiantadamente.

Além disso, esses custos são apenas uma parte do custo total de propriedade dos dispositivos de hardware.

Pense também nas seguintes despesas:

- Despesas com a equipe: comprar, operar e manter hardware para se defender contra ameaças em todas as camadas do modelo OSI — e oferecer o nível de performance e confiabilidade esperado dos sites e aplicativos de internet modernos — requer a presença de membros da equipes que sejam especialistas em cada uma dessas funções de rede. Desenvolver uma equipe com essa amplitude e profundidade de conhecimentos é uma proposta cara, especialmente em se tratando de um dos mercados de trabalho mais restritos jamais vistos. Uma pesquisa feita pela ISACA em 2022 descobriu que, entre as 2.000 empresas profissionais de segurança cibernética que participaram da pesquisa anual, 63% dos cargos de segurança cibernética estavam vagos — 8% de aumento com relação ao ano anterior (fonte).
- Custos de manutenção: a vida útil média de uma peça de hardware de rede no local é de apenas 3 a 5 anos. Além disso, as garantias para esses períodos costumam requerer gastos extras. Se levarmos em conta o ritmo das inovações tecnológicas, fica claro que, inevitavelmente, a vida útil dessas caixas no local continuará a encurtar. A alternativa são consertos inesperados — e, portanto, não previstos no orçamento — executados pelo fabricante original ou por um terceiro. Um defeito de hardware também pode resultar em tempo de inatividade no data center, cujo custo médio em termos de oportunidade é de mais de US$ 8.800 por minuto (fonte).
- Custos de reposição: substituir um dispositivo de hardware a cada três anos requer que as organizações não apenas precisem pagar novamente o valor do investimento inicial, mas também destinar recursos aos custos de frete e instalação do novo hardware. Adiar essas reposições muitas vezes resulta em defeitos mais frequentes e, portanto, em custos adicionais de manutenção.

Compare esse modelo com os serviços de rede em nuvem. É possível ter uma equipe operacional mais ágil, sem custos de manutenção e frete e sem precisar escolher entre upgrades caros e aumento do mau funcionamento.

**Defeitos de hardware podem resultar em tempo de inatividade no data center, cujo custo médio em termos de oportunidade é de mais de US$ 8.800 por minuto.**

## Desafios de suporte

Oferecer suporte a dispositivos de hardware de rede, além de caro, é um desafio logístico. O hardware precisa de correções frequentes para acompanhar as vulnerabilidades e as táticas de ataque mais recentes. Como esse processo muitas vezes é realizado manualmente, está suscetível a erro humano.

Quanto mais dispositivos de hardware uma organização usa, maiores são as chances de que, eventualmente, deixe passar a necessidade de um patch de segurança devido à falta de atenção ou medo de afetar sistemas vitais. Em uma recente Consultoria Conjunta de Segurança Cibernética, a Agência de Segurança Nacional (NSA), a Agência de Segurança Cibernética e Infraestrutura (CISA) e o Departamento Federal de Investigação (FBI) relataram que 16 falhas publicamente conhecidas em dispositivos de rede sem patches de segurança foram exploradas em campanhas amplamente disseminadas (fonte). As explorações afetaram vários dispositivos no local, desde roteadores de pequenas empresas a VPNs de corporações, possivelmente concedendo aos invasores a capacidade de manipular o tráfego de rede e exfiltrar dados das redes visadas.

Apesar do fato de as 16 falhas listadas serem classificadas como críticas, a aplicação de patches e correções não é uma tarefa simples. Na verdade, a aplicação de patches de segurança pode ser tão complexa que existe toda uma categoria de softwares para ajudar as empresas a se manterem atualizadas (source).

E as consequências da não aplicação de apenas um patch podem ser significativas. Não apenas o hardware permanece desprotegido mas, quando um patch é lançado, a vulnerabilidade correspondente se torna um alvo muito mais visível para os invasores oportunistas. Compare essa situação aos serviços de segurança baseados em nuvem, nos quais a correção de vulnerabilidades e a instalação de atualizações ocorrem automaticamente por padrão e podem levar somente 30 segundos para se propagar, dependendo da velocidade da rede do provedor de nuvem.

Outros desafios de manutenção do hardware:

- **Solução de problemas:** em um cenário somente de hardware, frequentemente a solução de problemas força as equipes de TI a passarem pelo árduo processo de desconectar balanceadores de carga, firewalls e outros dispositivos locais, um de cada vez, para descobrir onde está o problema.

  Esse processo fica ainda mais complicado com o uso simultâneo dos serviços de nuvem. As organizações que confiam em hardware muitas vezes gerenciam o acesso a esses serviços por meio de um data center centralizado e todos os dispositivos individuais que ele inclui. Quando os funcionários não conseguem acessar um serviço específico, as equipes de TI têm um local a mais para conferir ao diagnosticar problemas. Se levarmos em conta uma pesquisa recente da Productiv mostrando que 56% dos aplicativos SaaS se encaixam na categoria de Shadow IT — aplicativos não aprovados ou não gerenciados adquiridos sem o conhecimento da equipe de TI — veremos que o problema se agrava rapidamente, tanto em termos de escopo quanto de escala (fonte).
- **Manutenção física:** quando um dispositivo de hardware chega a quebrar, as equipes de TI precisam desconectá-lo fisicamente, encomendar a reposição, testar a reposição e reinstalá-lo — mais um processo difícil. Se levarmos em conta a escala de muitas corporações globais, esses dispositivos carecendo de atenção poderiam estar do outro lado do mundo.

## Falhas de segurança

Mesmo que uma organização tivesse os recursos necessários para provisionar e manter continuamente o hardware local mais recente e de mais alta capacidade, a infraestrutura resultante ainda sofreria com deficiências de segurança críticas, especialmente em um mundo que está migrando para a nuvem.

Pense no gerenciamento de acesso dos funcionários. Embora o hardware de VPN crie túneis criptografados entre dispositivos de funcionários remotos e aplicativos hospedados em um data center interno, ele não monitora nem protege a atividade do usuário depois disso.

Se o dispositivo do funcionário se tornar comprometido por malware ou um ataque de phishing comprometer suas credenciais de VPN, um invasor poderá ser capaz de usar o acesso à VPN para obter uma ampla variedade de informações sensíveis. Tanto o phishing quanto o malware continuam a representar sérios riscos e a gerar ganhos monetários significativos para os perpetradores das ameaças. Em 2021, foram perdidos US$ 6,9 bilhões devido a crimes cibernéticos, de acordo com o FBI. Especificamente, o Comprometimento de E-mails Comerciais (BEC) custou às empresas perdas da ordem de US$ 2,4 bilhões (source).

**Se o dispositivo do funcionário tiver malware ou se um ataque de phishing comprometer as credenciais de VPN dele, um invasor poderá usar o acesso à VPN para conseguir uma grande variedade de informações sensíveis.**

Os serviços de nuvem e aplicativos SaaS complicam ainda mais a segurança de uma infraestrutura centrada em hardware. Em um modelo de nuvem híbrida, por exemplo, uma organização opera uma mistura de infraestruturas no local e na nuvem. A organização não pode, simplesmente, enviar um hardware de segurança para um provedor de nuvem. Se desejar continuando a usar hardware no local para seu próprio data center, diferentes partes da infraestrutura serão protegidas de maneiras distintas, reduzindo a visibilidade e o controle que as equipes de segurança obtêm dos ataques recebidos.

Os serviços baseados em nuvem conseguem superar esses dois desafios com a unificação de data centers e serviços em nuvem em uma única camada definida por software.

Uma explicação detalhada dessa abordagem excede o escopo deste artigo. Para saber mais, explore os artigos a seguir:

- O que é uma rede Zero Trust?
- O que é Serviço de Acesso Seguro de Borda?

# Segurança baseada em nuvem e serviços de desempenho: vantagens e desafios

Oferecer serviços de rede por meio da nuvem evita muitos dos problemas associados ao hardware: pressões da cadeia de abastecimento, limitações de capacidade, custos, dificuldades de suporte e falhas de segurança.

- **Cadeia de abastecimento:** Muitos provedores de serviços de rede baseados em nuvem são projetados para se ampliar com arquiteturas globais modernas, reduzindo a gravidade dos problemas da cadeia de abastecimento.
- **Capacidade:** por causa da natureza distribuída e definida por software da nuvem, as organizações podem provisionar mais capacidade facilmente conforme o negócio cresce.
- **Custos:** os custos adicionais de hardware simplesmente não existem ou podem ser mais fáceis de se planejar com antecedência. Melhor ainda, os serviços de nuvem costumam ser classificados como despesas operacionais, não despesas de capital, o que permite vantagens fiscais e contábeis para várias empresas.
- **Suporte:** as necessidades logísticas e de recursos são administradas pelo provedor de serviços, e não há chance de uma correção ser ignorada, porque as atualizações são automáticas.
- **Segurança:** os serviços de rede definidos por software podem unificar infraestruturas diferentes em uma camada de proteção.

No entanto, os serviços de rede em nuvem têm seus próprios riscos se não forem implantados com atenção:

| Risco | Descrição |
|---|---|
| **Latência** | Algumas funções de rede baseadas em nuvem dependem de data centers especializados baseados em nuvem, como, por exemplo, centros de depuração de mitigação de DDoS. Fazer o backhaul do tráfego para esses data centers pode aumentar a latência de modo significativo, dependendo de sua localização em relação ao servidor de destino.<br><br>Esse problema se agrava quando uma organização usa provedores diferentes para funções de rede diferentes. Quando o tráfego precisa saltar de provedor em provedor, a latência pode ser medida em centenas de milissegundos. |
| **Suporte** | Quando uma organização usa provedores diferentes para funções distintas, a solução de problemas continua sendo um problema. Pode ser difícil identificar qual provedor é a causa de congestionamento ou interrupções. |
| **Custos** | Quando uma organização usa provedores diferentes para funções distintas, o tempo (e consequentemente o custo) exigido para gerenciá-los pode ser longo. |

## Para evitar esses problemas, siga estas estratégias:

- **Procure provedores que funcionem tanto com infraestruturas em nuvem quanto locais.**
  Esse recurso permite que equipes de TI e de segurança definam controles e monitorem o tráfego global em um só lugar. Também ajuda a construir uma arquitetura mais resiliente, na qual suas equipes podem mudar de estratégia rapidamente em resposta a flutuações nas condições do mercado.
- **Procure provedores de nuvem que ofereçam várias funções de rede funcionando juntas.**
  Isso geralmente reduz o número de saltos de rede que o tráfego precisa fazer, o que resulta em redução da latência e, consequentemente, em uma melhor experiência do usuário final. A solução dos problemas de rede também fica mais fácil quando você precisa ligar para uma empresa, e não para várias. Além disso, agrupar diversas funções costuma resultar em custos mais baixos.
- **Procure provedores de nuvem que possam realizar várias funções de rede em todos os locais de sua rede.**
  Provedores que expandem seus portfólios de serviços por meio de aquisições nem sempre integram totalmente esses novos serviços, o que significa que determinadas funções só podem ser fornecidas por data centers específicos. Pense em contratar provedores que oferecem essas funções em toda a sua rede para evitar os problemas mencionados acima.
- **Procure provedores de nuvem com uma ampla presença global.**
  Esse recurso facilita o anterior e garante que os usuários finais estejam sempre próximos da rede, independentemente do local onde estiverem. Além disso, cria uma ampla superfície de rede para absorver o tráfego de DDoS e conduzir outras funções de rede que requeiram uma grande capacidade.

# Como a Cloudflare pode ajudar

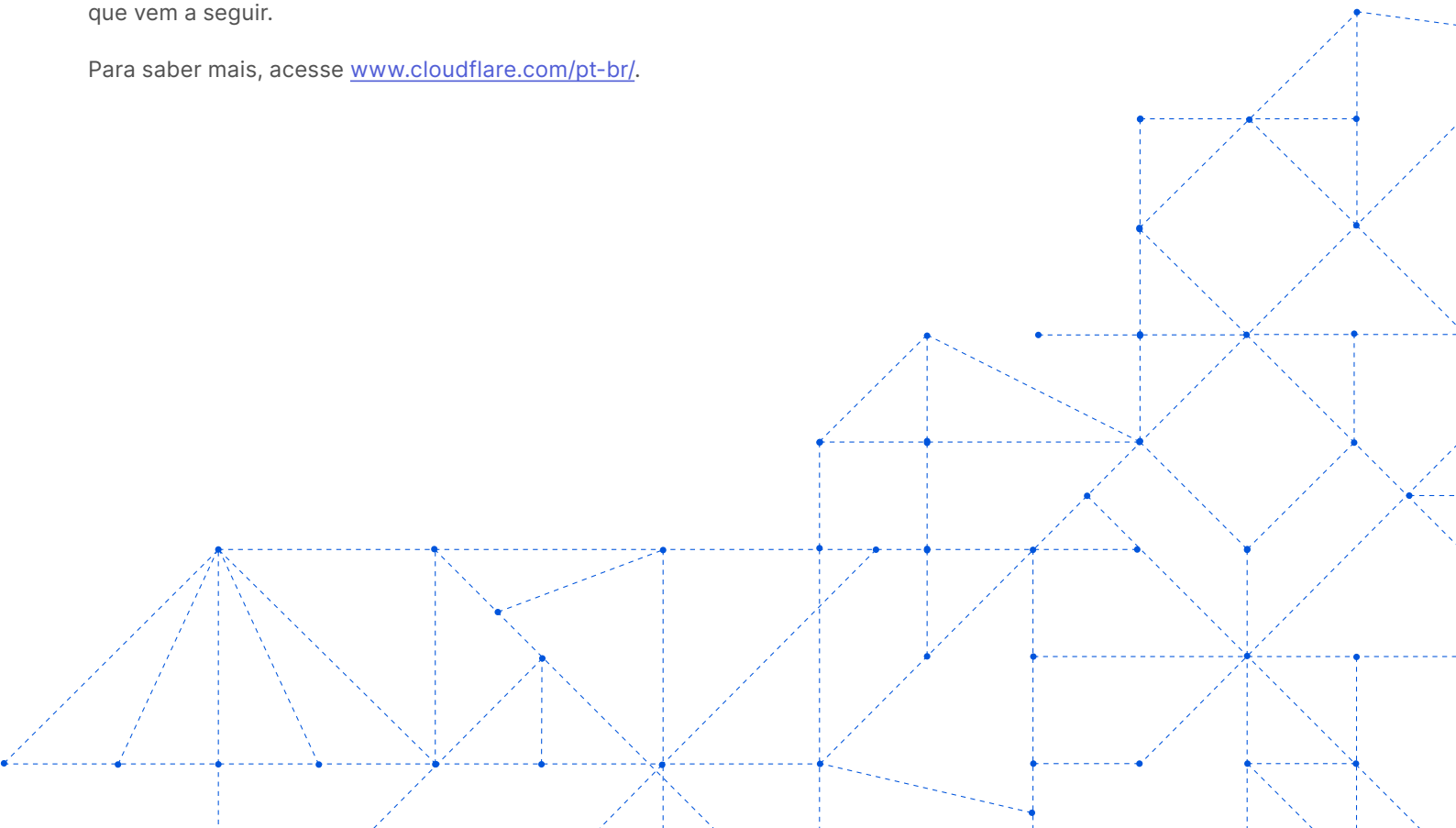
O que as organizações podem fazer para acelerar sua transformação de rede sem ficar aguardando a chegada de um hardware ou desperdiçar mais dinheiro em caixas que duram somente alguns poucos anos?
Usar a Cloudflare.

A Cloudflare é uma plataforma global na nuvem que oferece uma grande variedade de serviços de rede para tornar as organizações mais seguras, melhorando a performance de aplicativos e eliminando o custo e a complexidade de gerenciar um hardware de rede individual. Essa plataforma oferece um painel de controle unificado, escalável e fácil de usar para proporcionar segurança, performance e confiabilidade a todos os seus aplicativos locais, híbridos, na nuvem e de software como serviço (SaaS).

O crucial é que todos os data centers na rede global da Cloudflare em mais de 270 cidades podem oferecer todos esses serviços, reduzindo a latência que pode complicar as implementações de nuvem. Simplifique sua pilha de rede, acelere a transformação e equipe sua rede com o que vem a seguir.

Para saber mais, acesse www.cloudflare.com/pt-br/.

> "Recentemente, a Dropbox se tornou uma organização que coloca o virtual em primeiro lugar. Exploramos a forma como essa estratégia de negócios afeta a nossa abordagem de segurança e a nossa arquitetura de rede. Somos gratos pelo apoio da Cloudflare, que nos ajudou e a outras organizações que, como nós, priorizam o trabalho remoto, a aprendermos o que fazer para nos adaptar a esse 'novo normal'."
>
> Konstantin Sinichkin
> **Gerente de Engenharia da Dropbox**



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

REV:BDES-3313.2022JUN10