CLOUDFLARE

ARTIGO TÉCNICO

Esperança no horizonte: Como construir uma postura de segurança cibernética melhor durante a incerteza econômica

Conteúdo

Sumário executivo

As organizações estão enfrentando incertezas econômicas à medida que as perspectivas se tornam mais imprevisíveis. Essa incerteza, muitas vezes exemplificada por orçamentos reduzidos, pressiona CIOs e líderes técnicos para encontrar novos caminhos a seguir.

Felizmente, líderes que criam estratégias para enfrentar a tempestade realinhando orçamentos, redefinindo processos para eficiência e continuando o crescimento planejado proativamente, sem um aumento substancial de recursos, ainda vão estar em uma posição vantajosa quando os tempos de incerteza passarem.

Nas seções a seguir, vamos definir e expandir os diversos fatores que criam essas circunstâncias e condições de mercado. A partir desses insights, definimos cinco etapas que líderes podem seguir para encontrar oportunidades de obter eficiência em suas práticas de segurança sem comprometer sua postura de segurança. Ao alinhar a estratégia de infraestrutura de TI ao novo ambiente econômico, líderes podem preparar suas organizações para o sucesso no futuro.

Introdução

Nos últimos anos, líderes de TI têm lidado com uma crise após outra enquanto planejam e executam sua estratégia. Tiveram que reagir a uma pandemia global e seus efeitos secundários como a escassez na cadeia de suprimentos, um conflito crescente na Europa Oriental e o que pode se tornar uma recessão. Nas palavras do economista de Stanford, Paul Romer, "É terrível desperdiçar uma crise" (fonte). As escolhas que CIOs fizeram para apoiar sua força de trabalho remota vão trazer benefícios duradouros e não intencionais, tornando seus locais de trabalho atraentes ao oferecer suporte ao trabalho remoto. Da mesma forma agora, à medida que líderes enfrentam uma perspectiva econômica pior, as escolhas que fazem sobre segurança, rede, acesso remoto, armazenamento, desenvolvimento e infraestrutura vão fazer com que surjam mais fortes e com melhor posicionamento para um crescimento seguro e sustentável no futuro.

A ascensão do trabalho remoto foi acompanhada por um explosão de ransomware e ameaças cibernéticas sofisticadas que estabeleceram novos padrões de impacto, escala e sofisticação na receita (fonte). A evaporação do que restava do perímetro da rede, aliada aos aumentos históricos na rotatividade de funcionários, gerou falhas na segurança e atrasos em projetos estratégicos de TI. Isso forçou as organizações a repensar não apenas sua abordagem de contratação e retenção, mas também sua abordagem de controle de acesso a seus sistemas e máquinas. Embora a pandemia tenha causado um aumento dramático no eCrime (fonte), ela também abriu os olhos das organizações e seus conselhos para a necessidade urgente de uma cibersegurança eficaz. Agora é a hora de as organizações adotarem uma abordagem mais estratégica para o longo jogo de habilitar uma infraestrutura de trabalho híbrida segura, produtiva e disponível.

Aqui estão cinco coisas que você pode fazer para reduzir o risco de sua empresa, dentro do orçamento, e aumentar a capacidade de sua organização de lidar com as ameaças emergentes que surgem no horizonte:

1. Audite as ferramentas de segurança existentes para descobrir recursos sobrepostos

As organizações têm muito a ganhar consolidando seus fornecedores de segurança. Embora nenhuma ferramenta jamais seja a solução "definitiva" que CISOs adorariam ter, uma grande quantidade de operadores de segurança disseram acreditar que sua empresa está desperdiçando dinheiro com muitas ferramentas que ainda não oferecem uma defesa ideal. Ser compatível com várias ferramentas de vários fornecedores significa que seus funcionários estão gastando um tempo valioso em aquisição, implementação, gerenciamento, solução de problemas e suporte a um grande número de sistemas desconectados, em vez de proteger sua infraestrutura e dados. Na verdade, uma pesquisa realizada em junho de 2022 na RSA Conference anual constatou que "metade (53%) das empresas entrevistadas sente que desperdiçou mais de 50% de seu orçamento de segurança cibernética e ainda não consegue remediar as ameaças. Quarenta e três por cento dos entrevistados dizem que seu desafio número um na detecção e remediação de ameaças é uma superabundância de ferramentas, enquanto 10% das organizações carecem de ferramentas eficazes para remediar ameaças de segurança cibernética" (fonte). Se você eliminar apenas algumas dessas ferramentas, poderá melhorar a segurança e economizar o tempo valioso dos funcionários.

Ao transferir os investimentos de despesas de capital para despesas operacionais, você também pode fazer melhorias imediatas no fluxo de caixa no curto prazo e evitar se prender a investimentos de capital plurianuais que impedem a agilidade dos negócios. E um jeito de simplificar é diminuir a dependência do hardware tradicional. Uma mudança de equipamentos antigos para soluções oferecidas como serviço garante que suas iniciativas de maior prioridade permaneçam consolidadas, mesmo que os orçamentos diminuam. Adquirir o modelo como serviço também significa que você se beneficia dos ciclos de inovação inerentemente mais rápidos do software e elimina o problema inevitável de corrigir frequentemente o hardware legado. Ficar livre da preocupação com correções e inovação permite que suas equipes se concentrem em atividades que realmente diferenciam sua empresa. Ao enfrentar a incerteza, a simplificação e a consolidação estratégica podem ajudar a alcançar o sucesso no longo prazo.

2. Concentre-se nos dados, não apenas nas ferramentas

As equipes de liderança devem considerar mudar o foco para melhor integrar não apenas as ferramentas, mas também os dados, em todos os seus conjuntos de ferramentas de segurança para melhor descobrir padrões e anomalias. Historicamente, as equipes de segurança continuaram adicionando mais e mais conjuntos de ferramentas ao longo do tempo sem considerar os impactos no longo prazo de muitos conjuntos de dados em muitos lugares. Muitas vezes, o resultado é uma colcha de retalhos de produtos com pouca ou nenhuma interoperabilidade e opacidade nos dados, o que resulta em insights mais fracos com níveis mais baixos de precisão, introduzindo oportunidades para erro humano. Sem mencionar que a quantidade de tempo que pode levar para uma equipe extrair vários conjuntos de dados, mesclá-los e executar as consultas não é apenas uma perda de tempo, mas também de recursos. Em vez disso, esses recursos poderiam estar focados em iniciativas de negócios mais estratégicas.

Embora as equipes possam encontrar soluções criativas para resolver desafios de interoperabilidade, como mesclagem manual de conjuntos de dados ou importação e exportação de CSVs, é importante considerar que, deixando de lado a eficiência, o valor das ferramentas de segurança está nos dados que esses sistemas digerem , criam e disponibilizam para defensores. Se seus dados estiverem em todos os lugares, não classificados, não protegidos e não gerenciados com cuidado, eles podem distorcer o que poderia ter sido insights impactantes derivados de tais dados, especialmente se houver dados em instâncias de TI invisível que podem ter sido totalmente deixadas de fora. Ao consolidar conjuntos de ferramentas e considerar cuidadosamente a interoperabilidade de sua pilha de segurança, você pode reduzir o erro humano e proteger melhor seus dados. Porque mesmo que você tenha investido nas melhores ferramentas disponíveis hoje, os conjuntos de dados isolados e os conjuntos de dados invisíveis levam a insights mais fracos.

Em termos de eficiência, é importante considerar que na era do Zero Trust (“nunca confie, sempre verifique”), mais ferramentas significam que as equipes também estão gastando mais tempo fazendo login, autenticando e obtendo acesso aos sistemas antes mesmo que possam começar a fazer o seu trabalho. Quanto menos sistemas um determinado funcionário precisar ter contato, maior a economia de tempo e isso permite que se movam mais rapidamente. É extremamente importante considerar que os dados contidos nesses sistemas, bem como quantos sistemas precisam acessar para concluir uma determinada tarefa, são, em última análise, o que permitirá ou impedirá a capacidade das equipes de responder, em vez de reagir, a ameaças de forma oportuna.

3. Procure modelos de nuvem como serviço para maximizar a inovação e minimizar a complexidade

Toda empresa precisa inovar para se manter competitiva, mas qualquer empresa que não esteja no ramo de segurança cibernética não tem tempo, orçamento ou recursos para acompanhar os últimos CVEs, tendências de ataque e correções essenciais necessárias para manter toda sua infraestrutura segura. A adoção de modelos como serviço, quando viável, permite que líderes se beneficiem da inovação contínua sem ter que se preocupar em fazer compensações ou decisões difíceis em relação à dívida técnica.

Também é importante considerar que alguns serviços de segurança cobram taxas a mais por ultrapassar as limitações de tráfego e alguns cobram taxas de largura de banda. Considere analisar o que sua organização está pagando mensalmente ou anualmente para entender se você está pagando mais do que imagina. Se estiver, aproveite para buscar outras soluções que não cobrem excedentes para ajudar não só a economizar, mas também a ter um gasto mais previsível no longo prazo, o que permite que sua equipe se planeje melhor para o futuro.

Os serviços dessa natureza fornecidos em nuvem também permitem que sua organização cresça e diminua conforme necessário, sem ter que se comprometer com racks de hardware caros e todo o problema de gerenciamento do ciclo de vida que vem com eles. Em tempos de incerteza, as empresas precisam permanecer ágeis e responder rapidamente às mudanças nas condições de mercado. Quando o fluxo de caixa é uma preocupação, a capacidade de minimizar custos, ou eliminá-los como um todo, é uma vantagem estratégica que pode significar a diferença entre simplesmente sobreviver e prosperar, independentemente das condições de mercado.

4. Melhore a experiência dos funcionários

De acordo com a Forbes, “Nossa pesquisa descobriu que processos de login complexos e com várias etapas estão frustrando trabalhadores, desperdiçando seu tempo, prejudicando a produtividade e fazendo com que desistam de tarefas essenciais relacionadas ao trabalho... Em última análise, quase 40% dos trabalhadores disseram que procrastinou, delegou ou pulou completamente a configuração de novos aplicativos de segurança de trabalho devido a processos de login complicados. É como proteger sua casa com o portão mais forte, alto e seguro que o dinheiro pode comprar, fortificado com dragões que respiram laser, apenas para deixá-lo destrancado à noite. Além de ser ineficiente e difícil para os defensores rastrear quais ferramentas abrigam cada função, muitos painéis e muitos locais onde os dados ficam podem criar grandes riscos de segurança e lacunas de visibilidade para qualquer organização. As empresas que desejam ficar à frente das ameaças de segurança cibernética devem considerar que cada clique e pressionamento de tecla consomem tempo, energia e foco valiosos na resposta a eventos críticos. Para criar uma experiência de funcionário melhor e mais simplificada, é fundamental que a liderança analise com atenção quantas ferramentas defensores precisam usar para realizar seu trabalho com eficiência, bem como o que pode ser eliminado ou consolidado para reduzir os custos o tempo que cada defensor leva para responder, não apenas reagir, a um evento crítico de segurança.

Quando se trata de funcionários não técnicos ou que não desempenham funções de defensores, também é importante considerar que, à medida que trabalhadores remotos buscam acelerar sua produtividade pessoal, eles podem recorrer à TI invisível ou a métodos alternativos. Embora os controles Zero Trust tenham fornecido um caminho promissor para a construção de organizações mais seguras, especialmente em um ambiente remoto, não há como negar que nem todas as abordagens Zero Trust são criadas iguais. Quanto mais complexo for para um funcionário obter acesso ao que precisa, mais provável será que encontre uma maneira de burlar os controles de segurança em vez de obedecê-los. Líderes devem procurar entender não apenas a eficácia dos produtos de segurança, mas também levar em consideração a facilidade de uso, porque ignorar a experiência do funcionário aumenta o risco organizacional geral.

5. Procure serviços de segurança que não comprometam o desempenho da rede

Não é apenas sobre as ferramentas, mas como você configura e gerencia as ferramentas, que pode fazer toda a diferença. Considere fazer com que suas equipes façam uma auditoria das configurações e personalizações atuais para descobrir oportunidades que possam ajudar a melhorar o desempenho. Se não for possível melhorar o desempenho, considere buscar soluções que sejam criadas para o desempenho desde o início, já que o desempenho pensado de forma tardia, raramente atinge as metas que líderes esperam atingir. Quando se trata de desempenho de rede, é importante ter em mente que uma arquitetura ruim não pode ser resolvida com código. Da mesma forma que as plantas de um edifício têm pouca possibilidade de serem reprojetadas depois que a fundação foi construída, as redes devem ser projetadas desde o início para o melhor desempenho.

Aproveitar o poder de uma rede de borda global que processa e lida com dados mais próximos da fonte dará às organizações uma vantagem estratégica hoje e no futuro. De acordo com o MIT Technology Review, “Processar volumes de dados pode levar a problemas de desempenho. Em resposta, muitas organizações estão recorrendo à computação de borda, que processa dados próximos à fonte para permitir análises e respostas rápidas e em tempo real, mantendo os requisitos de privacidade e segurança” (fonte). Ao escolher estrategicamente soluções que já estão baseadas nas arquiteturas do futuro, você pode dar às suas equipes a vantagem estratégica de melhor desempenho de rede sem sacrificar os elementos críticos de privacidade e segurança.

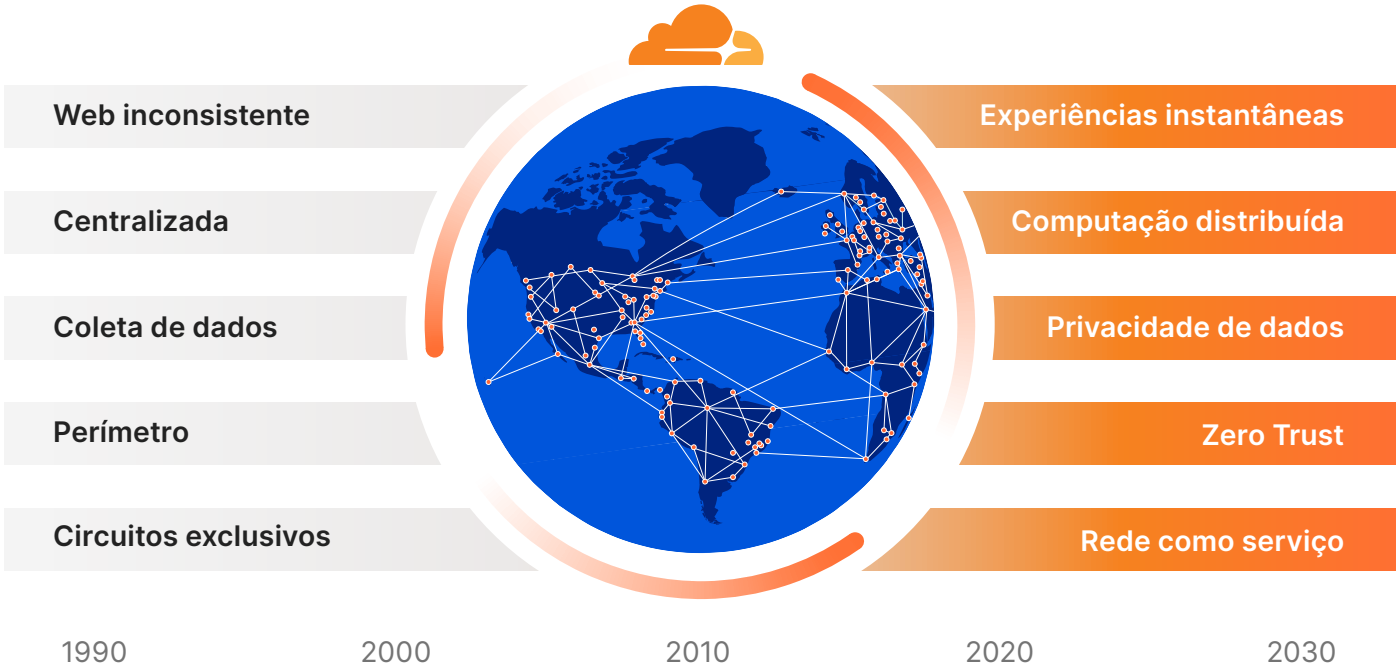
Em resumo, as etapas que você pode seguir para criar uma postura de segurança cibernética melhor durante tempos incertos são:

1. **Auditar as ferramentas de segurança existentes para descobrir recursos sobrepostos**
   - Consolide ferramentas sobrepostas
   - Mude os investimentos de CapEx para OpEx
2. **Concentrar-se nos dados, não apenas nas ferramentas**
   - A interoperabilidade das ferramentas leva a conjuntos de dados melhores e mais precisos
   - Conjuntos de dados e relatórios mais precisos levam a insights melhores, que são essenciais para atingir as metas da empresa
3. **Procurar modelos de nuvem como serviço para maximizar a inovação e minimizar a complexidade**
   - Se você não está no negócio de segurança cibernética, tem muito a ganhar ao ficar livre de correções, manutenção e atualizações mudando para ofertas como serviço
   - Os modelos em nuvem e como serviço oferecem a flexibilidade de que você precisa para ser ágil em um ambiente econômico flutuante
4. **Melhorar a experiência dos funcionários**
   - Muitas ferramentas em muitos lugares podem criar pontos cegos de segurança e frustração dos funcionários. Consolidar e simplificar vai ajudar a otimizar sua experiência
   - A otimização para a facilidade de uso do funcionário vai ajudar na retenção de funcionários e evitar que recorram à TI invisível para realizar seu trabalho
5. **Procurar custos ocultos e oportunidades de aprimoramento de desempenho em sua pilha de segurança cibernética atual**
   - Audite as ferramentas existentes para descobrir oportunidades de otimizar o desempenho, mas lembre-se de que não é possível otimizar uma arquitetura ruim.
   - A adoção de ferramentas desenvolvidas em escala global mais próximas de onde você prevê que seus clientes estão localizados vai permitir que sua organização ofereça uma experiência de cliente superior e segura

Como a Cloudflare pode ajudar

A Cloudflare foi fundada em 2010, após a crise econômica de 2008, para liderar a transformação da infraestrutura no local para a nuvem. Projetamos a plataforma da Cloudflare com um objetivo audacioso: ajudar a construir uma internet melhor. O conjunto de produtos da Cloudflare protege e acelera qualquer coisa conectada à internet sem adicionar hardware, instalar software ou alterar uma linha de código.

Os ativos da internet habilitados pela Cloudflare têm todo o tráfego da web roteado por meio de nossa rede global inteligente, que fica melhor a cada solicitação. Ajudamos nossos clientes a trabalhar com mais inteligência, desenvolver melhor, funcionar mais rápido e crescer com segurança. Hoje, a Cloudflare protege e acelera milhões de ativos da internet.



Controle

Aproveite a capacidade de uma rede global integrada que oferece conectividade, segurança e computação abrangentes e deixa você no controle das políticas.

Flexibilidade

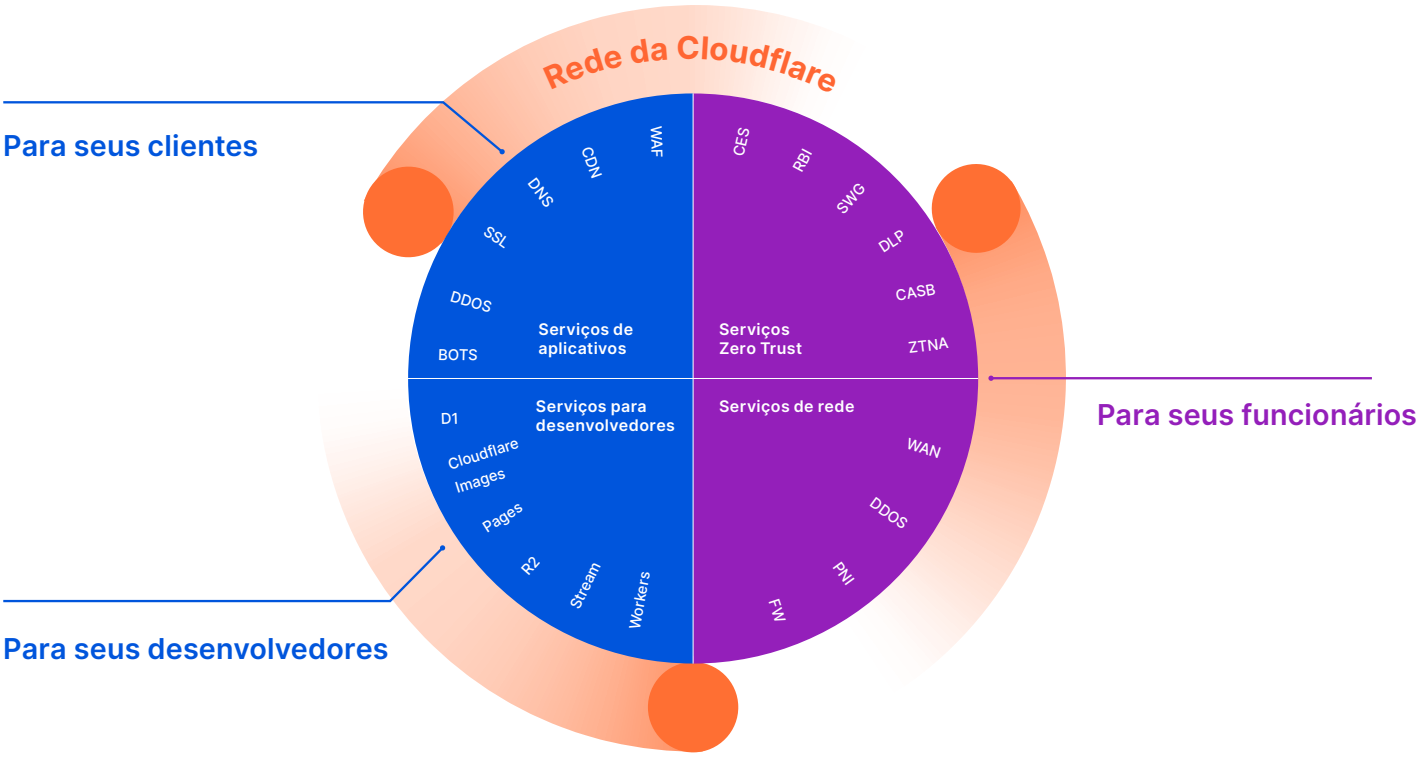
Serviços nativos de nuvem não exigem investimento antecipado em CapEx. Aumente ou diminua o uso facilmente para alinhar com as flutuações dos negócios.

Previsibilidade

Faturamento previsível, sem custos inesperados, como taxas de saída ilimitadas. Sem necessidade de gastar CapEx agora com hardware a ser entregue no ano que vem.

A Cloudflare é uma rede global desenvolvida para tornar tudo o que você conecta à internet mais seguro, privado, rápido e confiável

- **Proteja** seus sites, APIs e aplicativos de internet.
- **Proteja** redes corporativas, funcionários e dispositivos.
- **Escreva** e **implante** código para ser executado na borda de rede.



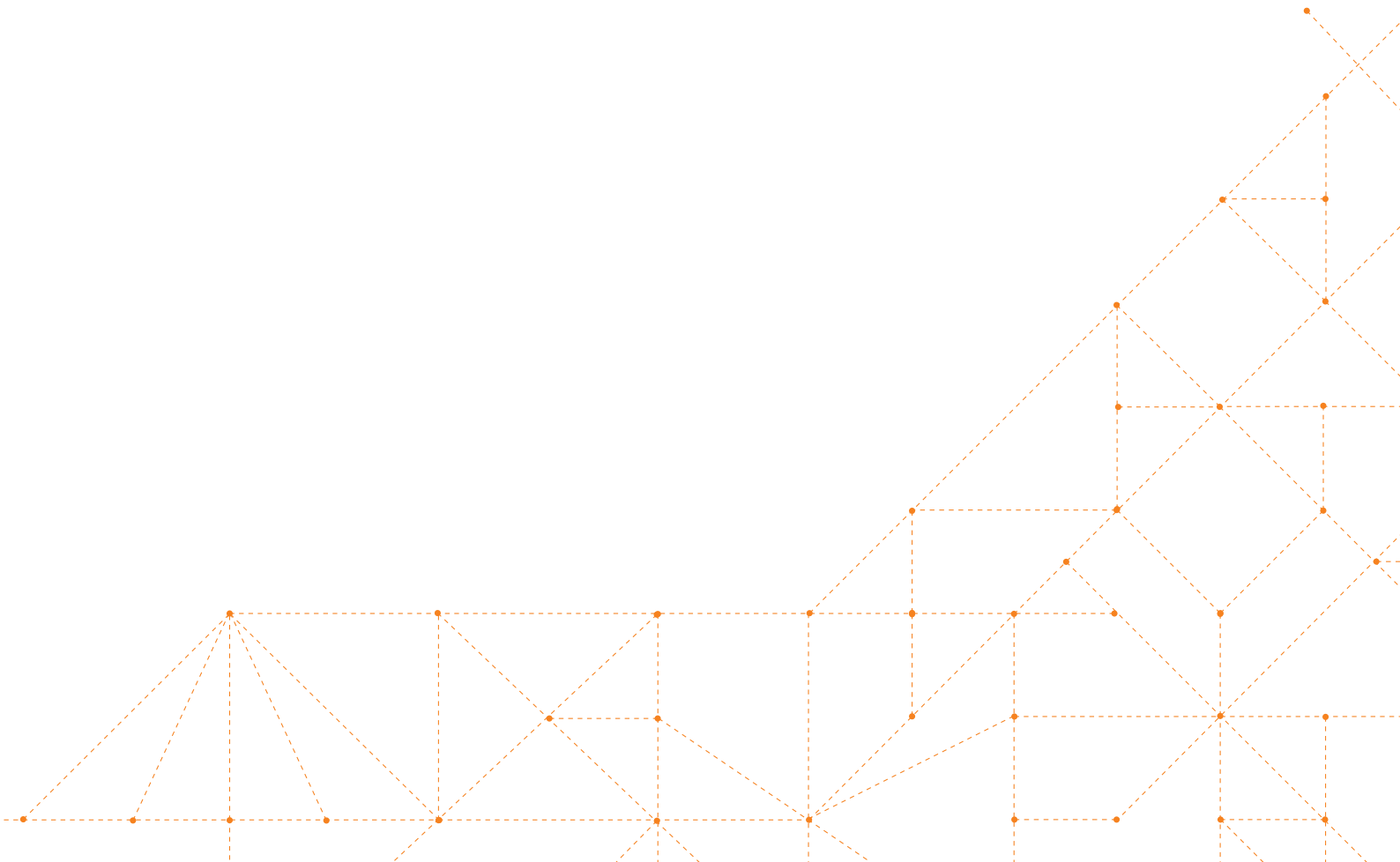
Nossa plataforma

Sobre a Cloudflare

A Cloudflare foi lançada em 2010 para liderar a transformação das infraestruturas locais migrando-as para a nuvem. Desenvolvemos a plataforma da Cloudflare partindo do zero e plenamente cientes de como era audacioso o nosso plano de ajudar a construir uma internet melhor. O conjunto de produtos da Cloudflare protege e acelera qualquer aplicativo de internet on-line sem adicionar hardware, instalar software ou alterar uma linha sequer de código.

Todo o tráfego dos ativos da internet habilitados pela Cloudflare é roteado por meio de sua rede global inteligente, que fica mais inteligente a cada solicitação. Ajudamos nossos clientes a trabalhar com mais inteligência, desenvolver melhor, funcionar mais rápido e crescer com segurança. Hoje, a Cloudflare protege e acelera milhões de ativos da internet.

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



CLOUDFLARE

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

REV:BDES-4327.2023MAR10