CLOUDFLARE

E-BOOK

Guia sobre adoção de SASE para CISOs

Como avaliar plataformas de SASE para casos de uso de alta prioridade

A missão de alcançar a resiliência cibernética

O Instituto Nacional de Padrões e Tecnologia (NIST) define resiliência cibernética como a capacidade de antecipar, resistir, recuperar e adaptar-se a condições adversas, tensões, ataques ou comprometimentos em sistemas que usam ou são habilitados por recursos cibernéticos.

No entanto, o reforço da resiliência cibernética, ao mesmo tempo que reduz os custos de mitigação de violações, também apresenta vários desafios:

- **Os cibercriminosos continuam a evoluir suas táticas:** à medida que os invasores desenvolvem ferramentas, técnicas e procedimentos mais sofisticados, a proteção do cenário de ameaças se torna ainda mais difícil para as organizações.
- **Os ambientes de TI estão se tornando mais complexos:** devido ao grande número de dispositivos e aplicativos conectados em arquiteturas multicloud, proteger esses ambientes é um processo caro e complicado
- **As equipes internas estão sobrecarregadas:** as organizações podem enfrentar restrições de recursos, à medida que os orçamentos ficam mais apertados e as equipes internas ficam sobrecarregadas

Para superar esses desafios, muitos CISOs estão recorrendo a uma estrutura de serviço de acesso seguro de borda (SASE). Ao contrário das abordagens de rede anteriores, uma arquitetura SASE unifica a segurança e a rede em uma plataforma em nuvem para visibilidade e controle consistentes. O SASE coloca controles de rede na borda da nuvem, e não no data center corporativo, para permitir que as empresas forneçam acesso simples e seguro a qualquer usuário, aplicativo, dispositivo ou rede, independentemente da localização.

Este guia aborda alguns dos casos de uso mais comuns de SASE e descreve as principais etapas para iniciar sua implementação de SASE, para que você possa fortalecer sua resiliência cibernética e obter ganhos rápidos.

Caso de uso n.º 1:

Adotar acesso à rede Zero Trust (ZTNA)

Depender da segurança tradicional baseada em perímetro para arranjos de trabalho híbridos, ambientes multicloud e dispositivos não gerenciados deixa as organizações com visibilidade limitada, configurações conflitantes e riscos excessivos. Uma abordagem Zero Trust, na qual controles de acesso granulares garantem que nenhuma entidade seja confiável por padrão, pode ajudar a modernizar sua estratégia de segurança das seguintes maneiras:

Substituindo a segurança tradicional baseada em hardware

Os controles de perímetro de rede tradicionais, como redes privadas virtuais (VPNs), podem ser difíceis de escalar, afetar a visibilidade e dificultar a detecção e a correção de ataques pelas equipes de segurança. Um modelo SASE oferece uma alternativa segura ao implementar o acesso à rede Zero Trust (ZTNA), ao mesmo tempo em que roteia e processa o tráfego de rede em uma rede global em nuvem, ajudando a reduzir o atrito do usuário final e o movimento lateral.

Gerenciando o acesso ao dispositivo

Conceder acesso a usuários terceiros, como prestadores de serviços, agências e fornecedores, pode apresentar riscos quando as organizações acidentalmente fornecem privilégios em excesso ou concedem acesso a dispositivos não gerenciados. O SASE permite que as organizações definam políticas Zero Trust sem cliente, garantindo assim que usuários terceiros tenham acesso apenas ao que precisam.

Prevenção contra ataques de ransomware

O ransomware pode se espalhar rapidamente por uma rede inteira e, em alguns casos, pode até se espalhar por várias redes e organizações. O SASE ajuda a prevenir a propagação de ataques de ransomware, revogando o acesso à rede e ao aplicativo assim que uma infecção é detectada. Apoiada pelo princípio Zero Trust de “controle de acesso com privilégios mínimos”, essa abordagem dificulta que os invasores aumentem os privilégios e se movam lateralmente dentro de uma rede.

Limitando a exposição de dados

A exposição e a exfiltração de dados podem representar uma séria ameaça para as organizações, à medida que os usuários fazem upload ou distribuem informações confidenciais em aplicativos sancionados e não sancionados. As políticas Zero Trust do SASE podem ajudar a prevenir a exposição de dados, limitando os aplicativos aos quais cada usuário tem acesso, ao mesmo tempo em que verificam suítes SaaS populares em busca de dados confidenciais e configurações incorretas.

ESTUDO DE CASO

Adotar o Zero Trust

Um provedor de telecomunicações da Fortune 500 usou a plataforma SASE da Cloudflare para proteger seu ambiente de trabalho híbrido para mais de cem mil funcionários, em centenas de aplicativos hospedados na AWS, no Azure e outros ambientes em nuvem. Com uma arquitetura de rede Zero Trust baseada em identidade, gateway seguro da web e controles de acesso unificados, eles conseguiram proteger os usuários contra ameaças sem a necessidade de conciliar diversas interfaces de criação de políticas, VPNs e serviços de filtragem de internet.

Caso de uso n.º 2:

Proteger superfícies de ataque

A transformação digital e o trabalho remoto expandiram a superfície de ataque, com usuários mais dispersos e dispositivos não gerenciados que precisam de acesso a recursos internos. Mas estender firewalls no local para a nuvem e escalar redes por meio de VPNs pode aumentar a exposição a ameaças externas e internas e, ao mesmo tempo, reduzir a visibilidade. Com uma arquitetura SASE, as organizações podem ampliar a visibilidade e os controles para dar suporte a um modelo “sem perímetro” e impor proteção consistente das seguintes maneiras:

Evitar o phishing multicanal

Os invasores costumam lançar ataques de phishing em canais onde os usuários tendem a baixar a guarda sobre onde clicam, especialmente aquelas ferramentas que normalmente não são protegidas por controles de segurança de e-mail. Uma plataforma SASE unificada permite proteção abrangente em todos os seus ambientes para mitigar o risco de roubo de credenciais, controle de conta e exfiltração de dados.

Defender trabalhadores remotos

O trabalho remoto exige que os usuários se conectem a partir de vários locais e dispositivos, muitas vezes fora dos limites das organizações que os empregam. Uma arquitetura SASE permite que as organizações protejam o acesso de funcionários e terceiros a ambientes e dados críticos, ajudando a garantir uma abordagem de trabalhar de qualquer lugar protegida e produtiva.

Melhorar as experiências do usuário

As abordagens tradicionais para depurar o tráfego de escritórios geralmente exigem o backhaul do tráfego para data centers corporativos centralizados, o que pode aumentar a latência e prejudicar a produtividade. Mas a alternativa, dar aos usuários acesso direto à internet, introduz riscos de segurança e cria experiências do usuário inconsistentes. O SASE gerencia e otimiza de forma inteligente conexões diretas com qualquer destino em nuvem ou na internet e aplica políticas e proteções o mais próximo possível dos usuários finais.

Proteger redes de longa distância (WANs)

Algumas WANs contornam a segurança em nuvem para o tráfego entre filiais, portanto, as reivindicações de integração entre serviços de segurança e WANs definidas por software podem não ser o que parecem inicialmente. O SASE permite que as organizações simplifiquem e protejam a forma como se conectam através de WANs, filtrando e inspecionando o tráfego entre escritórios, data centers, nuvens públicas e outros locais dentro e fora da internet mais ampla.

ESTUDO DE CASO

Proteger superfícies de ataque em expansão

A Werner Enterprises implantou serviços de SASE perfeitamente durante a migração para a nuvem, sem interrupções críticas de negócios ou de atendimento ao cliente. Após a implantação, eles reduziram os e-mails maliciosos em mais de 50% e, ao mesmo tempo, minimizaram os esforços manuais de triagem de e-mails em várias horas por dia, para que a equipe de segurança pudesse se concentrar em objetivos mais estratégicos da empresa.

Caso de uso n.º 3:

Proteger dados em qualquer lugar

À medida que os dados abrangem mais ambientes, as organizações muitas vezes acham difícil rastreá-los. Os dados confidenciais podem ser expostos através do uso não autorizado de inteligência artificial generativa e TI invisível, levando a comprometimentos ou violações cuja correção pode ser cara. O SASE converge visibilidade e controles de dados em ambientes web, SaaS e de aplicativos privados, ajudando as organizações a realizar o seguinte:

Simplificar a conformidade com as regulamentações de privacidade de dados

Com o surgimento de modelos de linguagem grandes (LLMs) e outras ferramentas de IA, os padrões de conformidade precisam evoluir para proteger os dados dos usuários. O SASE mantém os dados seguros e privados ao unificar os controles de dados, para que as equipes de segurança possam bloquear classes de dados regulamentadas, reduzir o risco de violações e garantir a conformidade contínua com requisitos de dados rígidos.

Gerenciar a TI invisível

A TI invisível são aplicativos não sancionados que não são gerenciados ou protegidos pelas organizações que os utilizam, ela pode apresentar riscos à medida que dados confidenciais são transferidos para ou através desses aplicativos. O SASE ajuda a minimizar esse risco ao fazer proxy do tráfego por meio de agentes de segurança de acesso à nuvem (CASB) in-line, que registram todas as conexões e solicitações para revelar a presença de aplicativos não sancionados e, em seguida, permitem que as organizações controlem como esses aplicativos são acessados e usados.

Usar a IA generativa com segurança

À medida que mais organizações adotam a IA, o risco de exposição de dados confidenciais também aumenta. Com um gateway seguro da web e um agente de segurança de acesso à nuvem in-line, uma abordagem SASE permite que as equipes de segurança detectem e aprovem o uso de aplicativos de IA, verifiquem configurações incorretas que possam causar vazamento de dados ou executem aplicativos de IA em navegadores web isolados para restringir entradas e saídas de dados.

Proteger dados confidenciais

Uma arquitetura SASE permite que as organizações detectem e controlem como os dados confidenciais entram, circulam e saem de seus ambientes de TI. Isso inclui a verificação de aplicativos e a inspeção do tráfego em busca de dados pessoais e propriedade intelectual regulamentados, o bloqueio de ameaças da internet, como phishing e ransomware, e a implementação de proteções adicionais contra roubo de dados e vazamentos inadvertidos.

ESTUDO DE CASO

Proteger dados em qualquer lugar

A Applied Systems adotou serviços de SASE para proteger o acesso a aplicativos e infraestrutura auto-hospedados para mais de 2.500 funcionários. Essa nova abordagem dá à equipe de segurança a flexibilidade de aplicar controles rigorosos para atender às diferentes necessidades dos usuários, ao mesmo tempo que controla como seus dados são compartilhados com ferramentas de IA.

Escolher uma solução SASE:

Consolidação de fornecedor único versus várias soluções pontuais

Um provedor SASE de fornecedor único converge recursos de rede e segurança em um único serviço fornecido em nuvem. Isso permite que as empresas consolidem diferentes produtos pontuais, eliminem dispositivos e garantam a aplicação consistente de políticas. Embora uma implementação SASE de vários fornecedores possa alcançar resultados semelhantes a uma abordagem de fornecedor único, muitas vezes ela aumenta a complexidade e o custo, ao mesmo tempo que reduz a visibilidade e a flexibilidade internas.

A consolidação desses recursos em uma plataforma unificada permite que você cumpra a verdadeira promessa do SASE: uma rede simplificada e eficiente e uma infraestrutura de segurança que reduz o custo total de propriedade e se adapta facilmente para atender às crescentes necessidades da empresa.

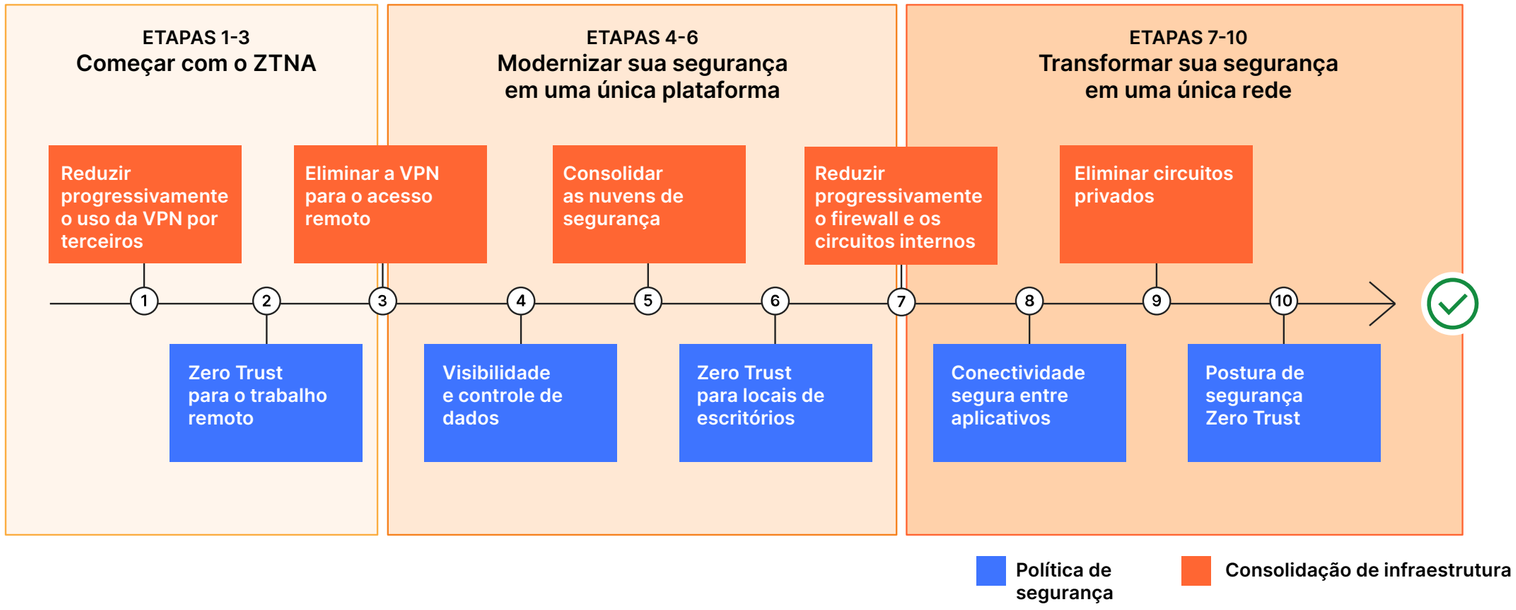
Ao avaliar possíveis fornecedores de SASE, tenha em mente as seguintes questões:

1. O tráfego de aplicativos é descriptografado e inspecionado por mecanismos de detecção de ameaças e dados confidenciais em uma única passagem? Há alguma advertência na implantação?
2. Todos os fluxos de dados e comunicações por meio de suítes SaaS estão protegidos em todos os canais (atividades de e-mail e web in-line e fora de banda)?
3. O isolamento do navegador remoto está habilitado para todos os usuários e aplicativos? Como isso afeta a produtividade? Incorre em taxas adicionais?
4. Alguma função de segurança é ignorada com base em qualquer via de acesso da rede?
5. É possível garantir que o tráfego do cliente seja isolado e privado em uma arquitetura de nuvem multilocatário?
6. Quais recursos de localização de dados estão disponíveis? A ativação da localização de dados adiciona latência para usuários remotos que se conectam fora da sua região localizada?
7. Você pode integrar seus feeds de inteligência contra ameaças à arquitetura deles? Como a plataforma reduz os falsos positivos dos feeds de inteligência contra ameaças?
8. Que tipo de pontuação e análise de risco de usuários/dispositivos está disponível? As pontuações de risco podem ser aplicadas uniformemente em todos os aplicativos?

Como a Cloudflare fornece o SASE

Para completar a jornada rumo a uma plataforma SASE unificada, muitas empresas confiam na Cloudflare. Somos o único fornecedor de SASE a começar com uma arquitetura de rede Zero Trust com identidade e conectividade baseada em contexto integradas de forma consistente em toda a nossa plataforma.

Seu roteiro de longo prazo para uma arquitetura SASE completa pode seguir um fluxo semelhante ao exemplo abaixo:



Ligue para: +55 (11) 3230.4523
e-mail: enterprise@cloudflare.com
Acesse: www.cloudflare.com/pt-br/

Apoiada por uma rede global que abrange mais de 310 cidades em todo o mundo, a Cloudflare ajuda os CISOs a obter segurança, resiliência e desempenho de nível empresarial. Nosso plano de controle único converge soluções pontuais em vários domínios de segurança, para que as organizações possam simplificar suas operações de segurança e garantir proteção consistente contra ameaças em evolução.

Visite nosso site para saber mais sobre a Cloudflare e a plataforma SASE da Cloudflare.