CLOUDFLARE

RESUMO DA SOLUÇÃO

Serviço de segurança de borda (SSE)

Planejamento para a consolidação de serviços de segurança e adoção no seu próprio ritmo

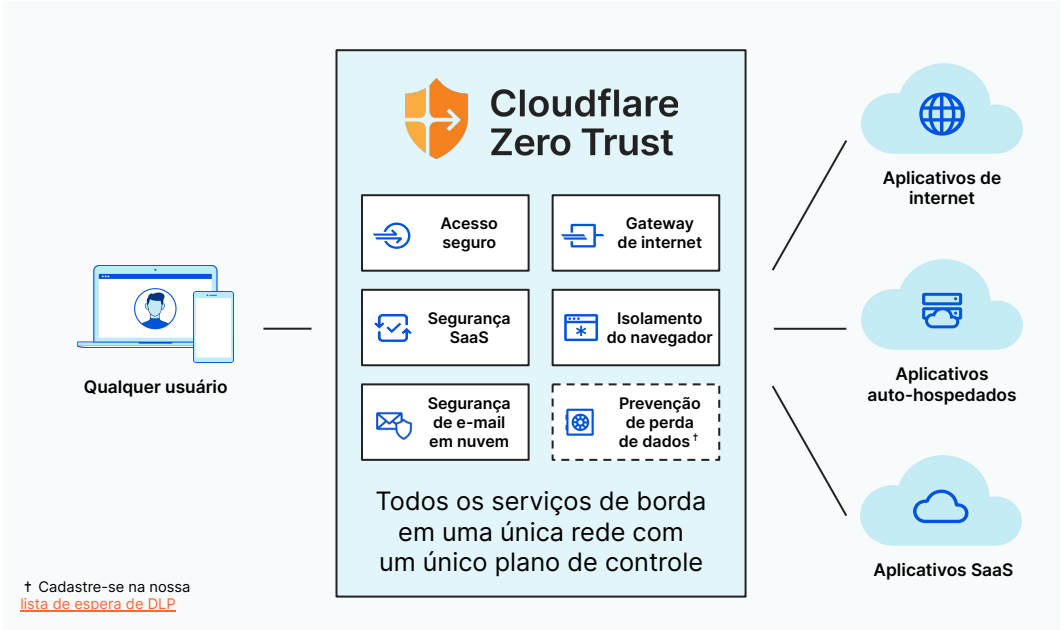
Convergência centrada em nuvem

A complexidade de se manter diversas soluções pontuais está levando a maioria das organizações a consolidar seus fornecedores favoritos. Atualmente, os "melhores recursos da categoria" e plataformas abrangentes não precisam se excluir mutuamente. Como a maioria dos compradores de TI tendem à consolidação, os fornecedores de segurança estão aproveitando a oportunidade para ampliar o valor de suas plataformas de segurança, indo além do que cada serviço poderia oferecer individualmente.

A abordagem SSE, que busca o equilíbrio entre produtos pontuais e a consolidação completa, tem um foco mais profundo em recursos de segurança do que a maioria das ofertas de Serviços de Acesso Seguro de Borda (SASE) por não estar vinculada a uma infraestrutura de rede. Em nossa opinião, nossa plataforma Zero Trust é comparável ao SSE da Gartner e converge produtos pontuais anteriormente distintos: ZTNA, VPN, SWG, Filtragem de DNS, CASB, RBI e Firewall como Serviço (FWaaS).

"Consolide seus fornecedores e reduza a complexidade e os custos à medida que seus contratos de SWG, CASB e VPNs (substituídos por uma abordagem ZTNA) são renovados. Tire proveito do mercado convergente que surge da combinação entre esses serviços." [1]

Gartner



† Cadastre-se na nossa lista de espera de DLP

Substituição de VPN
simplifica e protege a conexão de qualquer usuário a qualquer recurso

Segurança de SaaS
visibilidade e controle de aplicativos, incluindo e-mail

Proteção da internet
mantém seus dados a salvo de ameaças com qualquer porta e protocolo

Modernização da segurança
mais produtividade, operações mais simples, superfície de ataque reduzida

SSE como uma ponte para o SASE

Embora a convergência entre a segurança e os serviços da borda de rede seja o objetivo definitivo do SASE, algumas empresas poderão nunca atingir uma consolidação completa com um único fornecedor, com base em seu histórico e sua infraestrutura atual. Independentemente de sua estratégia de SASE no longo prazo, a Cloudflare pode ajudá-lo a modernizar sua segurança, transformar sua rede corporativa ou as duas coisas.

SASE de fornecedor único
Para as empresas que objetivam unificar totalmente seus serviços de segurança e de borda de rede com um único fornecedor, o Cloudflare One, nossa plataforma de SASE, fornece uma rede Zero Trust como serviço criada em nossa Rede global com mais de 275 cidades.

SASE multifornecedor
Para os que têm implantações de SD-WAN maduras ou equipes separadas de rede e segurança, a Zero Trust da Cloudflare pode ajudar a modernizar a segurança e a obter uma implementação de SSE tirando proveito de parcerias de SD-WAN para um SASE multifornecedor.

Adoção do SSE componível

A migração para um SSE baseado em nuvem não se faz da noite para o dia; a Zero Trust da Cloudflare ajuda as organizações a desativar o hardware em etapas, no ritmo que o cliente deseja. Muitas empresas optarão por iniciar sua jornada Zero Trust intensificando sua VPN com o ZTNA , como parte de um caminho para a substituição total. A simplificação da segurança SaaS vem logo em seguida, como uma segunda prioridade para a maioria, com estratégias mais amplas de proteção de dados e contra ameaças.

Nossa arquitetura uniforme e componível facilita uma adoção modular dos serviços de segurança. As empresas podem implantar combinações personalizadas entre serviços que se adaptem aos seus casos de uso prioritários, sem necessidade de uma mentalidade do tipo "tudo ou nada".

"Faça um inventário dos equipamentos e contratos para implementar uma desativação progressiva do perímetro de segurança no local e do hardware de segurança das filiais em favor do fornecimento de SSE baseado em nuvem, programada para durar vários anos. Tenha como meta a consolidação dos equipamentos no local, idealmente em um único dispositivo." [1]

Gartner

A integração alimenta a inovação

Todos os serviços da Cloudflare são executados em todos os servidores de cada data center ao longo de nossa gigantesca Rede global, de forma a não deixar nenhuma inconsistência nem lacuna na cobertura. Isso nos ajuda a fornecer uma inspeção de passagem única e a garantir o mais alto nível de segurança, desempenho e confiabilidade.

Serviços integrados nativamente também dão margem a oportunidades criativas de combinar funcionalidades ao longo de serviços diversos e fornecer aos nossos clientes os casos de uso desejados. À medida que essas linhas de produtos se mesclam, a interação entre serviços nos ajuda a resolver cenários mais avançados e a modernizar verdadeiramente a segurança.

Reforce a segurança de acesso de terceiros

- O ZTNA e o RBI se integram para fornecer acesso seguro a terceiros, como prestadores de serviços e parceiros
- Verifique informações contextuais para conceder autorização e distribua aplicativos em navegadores isolados para proteger os dados
- As operações sem cliente para ambos os serviços simplificam as implementações, sem necessidade de nenhum download

Visualize e faça a auditoria das sessões de SSH

- O ZTNA e o SWG se integram para fornecer visibilidade ao longo de sessões inteiras de SSH para monitorar o acesso privilegiado
- Simplifique o acesso SSH com sessões de SSH sem cliente e baseadas em navegador por meio do ZTNA
- Forneça visibilidade da sessão de SSH na camada de rede; registre cada comando usando o SWG como proxy

Simplifique os fluxos de trabalho corretivos de SaaS

- O SWG e o CASB se integram para habilitar um fluxo de trabalho do tipo "encontrar e corrigir"; bloqueie as atividades de SaaS suspeitas, no todo ou em parte, diretamente a partir dos achados de segurança do CASB
- Amplie a visibilidade de SaaS para ajudar a detectar e corrigir problemas que poderiam levar ao vazamento de dados ou a violações de conformidade

Melhor proteção contra phishing

- A segurança de e-mail e o RBI se integram para combater ataques de phishing sofisticados e comprometimento de e-mails corporativos (BEC)
- Nenhuma inteligência de ameaças preditiva é perfeita; ao abrir links de e-mails em um navegador isolado, você conta com uma camada extra de proteção

Comece sua jornada em direção a uma rede mais rápida, mais segura, mais confiável

Experimente agora

Ainda não está pronto para experimentar? Continue se informando sobre o Cloudflare One

[1] *Gartner Hype Cycle™ for Network Security, 2021*