

Comparação entre Cloudflare e Zscaler: Zero Trust, SSE, SASE e mais

Visão geral da comparação

Esta é uma comparação funcional da oferta geral da Cloudflare e da Zscaler, alinhada às tendências transformadoras de rede e segurança, incluindo Zero Trust (ZT), Serviço de Segurança de Borda (SSE) e Serviço de Acesso Seguro de Borda (SASE). Os 37 critérios são organizados em cinco grupos: plataforma de rede nativa na internet, plataforma de serviços nativa em nuvem, serviços que devem adotar a arquitetura SASE, serviços para ampliar a Zero Trust, SSE, SASE e mais (as definições atuais dessas tendências de mercado) e acessos à rede. Algumas comparações precisam de mais contexto e clareza, por isso, consulte as notas de rodapé na última página.

Para ver uma comparação mais conceitual, visite cloudflare.com/products/zero-trust/cloudflare-vs-zscaler

Plataforma de rede nativa na internet

Critérios	Cloudflare	Zscaler	NR
Cidades com data center disponível para qualquer cliente	270	55	1
Nuvens diferentes (planos de controle) em data centers	1	Cerca de 8	2
Contrato de Nível de Serviço com tempo de atividade	100%	99,99% a 99,999%	3
Inspeção de passagem única em todos os serviços de borda	SIM	NÃO	4
Laboratório de pesquisas de ameaças	SIM	SIM	-

Plataforma de serviços nativos

Critérios	Cloudflare	Zscaler	NR
Arquitetura combinável	SIM	NÃO	5
Interface de gerenciamento em um painel único	SIM	NÃO	6
Plataforma de desenvolvimento de computação sem servidor	SIM	NÃO	7
FedRAMP em andamento ou autorizado	SIM	SIM	8

Serviços para adotar uma arquitetura SASE

Critérios	Cloudflare	Zscaler	NR
Acesso à Rede Zero Trust (ZTNA)	SIM	SIM	-
Agente de segurança de acesso à nuvem(CASB)	SIM	SIM	-
Gateway da web seguro (SWG)	SIM	SIM	-
Firewall como serviço (FWaaS)	SIM	SIM	-
WAN como serviço com aceleração de tráfego para camadas 3 e 7	SIM	NÃO	9
SD-WAN local	NÃO - Parceiro	NÃO - Parceiro	10

Serviços para ampliar a Zero Trust, SSE, SASE e mais

Critérios	Cloudflare	Zscaler	NR
Segurança de e-mail em nuvem (CES)	SIM	NÃO	-
Isolamento de Navegadores Remotos (RBI)	SIM	SIM	11
Prevenção de perda de dados (DLP)	SIM	SIM	12
Sistema de detecção de intrusão (IDS)	SIM	SIM	13
Proteção contra DDoS para aplicativos e redes	SIM	NÃO	14
Segurança para aplicativos: WAF e detecção de bots	SIM	NÃO	15
Desempenho para aplicativos: CDN, DNS e LB	SIM	NÃO	-
Segurança para nuvem: CWPP, CPSM e CIEM	NÃO	SIM	16
Defesa cibernética: sandbox e fraude	NÃO	SIM	-
Monitoramento de experiência digital (DEM)	NÃO	SIM	-
Terminais no navegador para acesso remoto com privilégios	SIM	SIM	17
Registro de comando SSH	SIM	NÃO	-

Acessos à rede

Critérios	Cloudflare	Zscaler	NR
Acesso baseado em navegador sem cliente	SIM	SIM	-
Software de cliente de dispositivo	SIM	SIM	-
Software de conector de aplicativos	SIM	SIM	18
Software de conector de filiais	NÃO	SIM	19
DNS Anycast, GRE, IPsec, QUIC, túneis Wireguard	SIM	NÃO	20
Interconexão de rede privada para data centers e escritórios	SIM	NÃO	-
Trânsito de IP de entrada (BYOIP)	SIM	NÃO	-
Suporte para conexões apenas IPv6	SIM	NÃO	21
Resolvedores de DNS recursivos	SIM	SIM	-
Clientes de dispositivo e resolvedores DNS abertos ao público	SIM	NÃO	22

Resultados da comparação

Pontuação do grupo	Critérios	Cloudflare	Zscaler
Geral	37	32	18
Plataforma de rede nativa na internet	5	5	1
Plataforma de serviços nativos em nuvem	4	4	1
Serviços para adotar o SASE	6	5	4
Serviços para ampliar a Zero Trust, SSE, SASE e mais	12	9	7
Acessos à rede	10	9	5

Notas de rodapé (NR)

1. De acordo com cloudflarestatus.com e cloudflare.com/network, a Cloudflare tem data centers públicos em mais de 270 cidades. Muitas cidades são atendidas por mais de um data center. A partir de janeiro de 2022, de acordo com trust.zscaler.com e config.zscaler.com, a Zscaler possui 73 data centers públicos em 55 cidades, com 13 data centers sem nuvens publicadas e 11 data centers com proximidade geográfica automática desativada. Os outros 77 data centers declarados não parecem estar documentados publicamente e/ou disponíveis para clientes.
2. De acordo com config.zscaler.com/zscaler.net/cenr, a ZIA tem sete nuvens diferentes, a ZPA tem duas nuvens diferentes e outros produtos como ZDX têm mais nuvens diferentes.
3. A maioria dos serviços têm um SLA de tempo de atividade de 99,999%, mas o resolvidor DNS só oferece um SLA com tempo de atividade de 99,99% ([fonte](#)).
4. Por exemplo, uma solicitação de um usuário remoto a um aplicativo auto-hospedado privado pode ser inspecionada em uma passagem no mesmo servidor dentro do mesmo data center por SWG, RBI, ZTNA e serviços de segurança de aplicativos.
5. Uma arquitetura combinável requer a capacidade de adotar qualquer serviço oferecido na plataforma em qualquer ordem e ter interoperabilidade simultânea com serviços implantados anteriormente. A Zscaler projetou alguns de seus serviços para execução em separado em uma arquitetura única que impede essa composição, o que você pode ver nestes artigos da Zscaler ([fonte 1](#), [fonte 2](#)).
6. A Cloudflare adquiriu a Area 1 em abril de 2022. Está no nosso plano de ação integrar o gerenciamento de segurança para e-mail da Area 1 à interface de gerenciamento de Zero Trust da Cloudflare. A Zscaler não oferece segurança para e-mail, portanto, não é uma lacuna equivalente. No entanto, a Zscaler tem interfaces de gerenciamento separadas para as ofertas de ZIA e ZPA, bem como para muitos complementos, como RBI.
7. A Zero Trust da Cloudflare foi criada com base no Cloudflare Workers com tecnologia V8 isolada em nossa borda. A Zscaler usa uma arquitetura mais antiga baseada em contêiner, que desacelera o desenvolvimento e acrescenta custos à entrega de novos recursos.
8. Desde junho de 2022, a Cloudflare está com a autorização FedRAMP em andamento, já a Zscaler tem autorização FedRAMP.
9. A Zscaler não declara ser capaz de rotear e acelerar com inteligência o tráfego entre data centers em seu próprio backbone de rede.
10. Embora a Zscaler ofereça software para conectar filiais, não fornece funcionalidade SD-WAN totalmente local e não aparece na pesquisa de analistas por infraestruturas de borda WAN.
11. A tecnologia RBI padrão da Zscaler envia um fluxo de pixels, enquanto a tecnologia de renderização de vetor de rede patenteada da Cloudflare envia um fluxo de comandos de desenho. Além disso, desde junho de 2022, a Zscaler só executa RBI em quatro data centers. A combinação resulta em uma experiência do usuário ruim com muitos aplicativos SaaS e de internet.
12. Desde 2021, a Cloudflare está criando um serviço DLP nativamente em nossa plataforma Zero Trust. Uma versão beta privada foi iniciada em julho de 2022, entre na [lista de espera para saber mais](#). A versão beta pública vai começar em agosto.
13. A Detecção de Intrusão da Cloudflare já está disponível em nosso programa beta privado. Entre em contato com sua equipe de conta para saber como participar.
14. A Zscaler não oferece um serviço de proteção contra DDoS. Todos os provedores de serviços nativos em nuvem têm algum nível de proteção contra DDoS integrado na arquitetura, mas isso não mitiga com eficiência um ataque DDoS moderno. Embora a implementação da Zero Trust impeça a exposição de seus aplicativos na internet, ela não evita que prestadores de serviços ou outros usuários com acesso concedido ataquem o aplicativo pela rede do fornecedor de ZTNA.
15. Em março de 2022, a Zscaler anunciou a inclusão de proteção para aplicativo inline à oferta de ZTNA — ZPA. No entanto, isso não é equivalente a um firewall de aplicativos web (WFA) completo para aplicativos públicos e privados. E também faltam recursos de detecção de bots.
16. Em 2020 e 2021, a Zscaler adquiriu a Edgewise Networks para plataforma de proteção de carga de trabalho em nuvem (CWPP), Cloudneeti para gerenciamento de postura de segurança em nuvem (CSPM) e Trustdome para gerenciamento de direitos de infraestrutura em nuvem (CIEM). Esses serviços de segurança em nuvem ainda não foram integrados aos serviços Zero Trust.
17. A Cloudflare oferece terminais no navegador para SSH e VNC, enquanto a Zscaler fornece terminais no navegador para SSH e RDP. Muitos clientes da Cloudflare usam o Apache Guacamole para executar RDP no navegador.
18. A Zscaler exige uma infraestrutura de máquina virtual para executar sua imagem, já a Cloudflare oferece um daemon que pode ser executado com ou sem VMs.
19. A Zscaler exige infraestrutura de máquina virtual para executar sua imagem e o tráfego só pode passar por ZIA ou ZPA, mas não em uma única passagem.
20. A Zscaler é compatível com Anycast somente para resolução DNS. Para túneis GRE ou IPsec, os clientes devem usar um endereço de IP exclusivo para cada data center da Zscaler. E o conector de aplicativo e o cliente de dispositivo dependem de túneis DTLS não Anycast.
21. O cliente de dispositivo da Zscaler não é compatível com conexões apenas IPv6 de acordo com os fóruns da comunidade ([fonte](#)).
22. A Zscaler não oferece resolução DNS pública grátis (por exemplo, 1.1.1.1) e comunicação criptografada por IP (por exemplo, WARP).