A Cloudflare vs. Zscaler comparison of Zero Trust, SSE, SASE, and beyond

Comparison overview

This is a functional comparison for Cloudflare's and Zscaler's overall offering aligned to transformational network and security trends including Zero Trust (ZT), Security Service Edge (SSE), and Secure Access Service Edge (SASE). 37 criteria are organized into five groups: Internet-native network platform; cloud-native service platform; services to adopt a SASE architecture; services to extend ZT, SSE SASE, and beyond (the current definitions of these market trends); and network on-ramps. Some comparisons require more context and clarity, which are so footnoted on the last page.

For a more conceptual comparison, please visit cloudflare.com/products/zero-trust/cloudflare-vs-zscaler

Internet-native network platform

Criteria	Cloudflare	Zscaler	FN
Data center cities available to any customer	285	55	1
Distinct clouds (control planes) across data centers	1	~8	2
Uptime service level agreement	100%	99.99-99.999%	3
Single-pass inspection across all edge services	YES	NO	4
Threat research lab	YES	YES	-

Cloud-native service platform

Criteria	Cloudflare	Zscaler	FN
Composable architecture	YES	NO	5
Single-pane management interface	YES	NO	6
Serverless compute development platform	YES	NO	7
FedRAMP authorized	YES	YES	-

Services to adopt a SASE architecture

Criteria	Cloudflare	Zscaler	FN
Zero Trust Network Access (ZTNA)	YES	YES	-
Cloud Access Security Broker (CASB)	YES	YES	-
Secure Web Gateway (SWG)	YES	YES	-
Firewall as a Service (FWaaS)	YES	YES	-
WAN as a Service with L3-7 traffic acceleration	YES	NO	8
On-premise SD-WAN	NO - partner	NO - partner	9

Services to extend ZT, SSE, SASE, and beyond

Criteria	Cloudflare	Zscaler	FN
Cloud Email Security (CES)	YES	NO	-
Remote Browser Isolation (RBI)	YES	YES	10
Data Loss Prevention (DLP)	YES	YES	-
Intrusion detection system (IDS)	YES	YES	11
Network and application DDoS protection	YES	NO	12
Application security: WAF and bot detection	YES	NO	13
Application performance: CDN, DNS, and LB	YES	NO	-
Cloud security: CWPP, CPSM, and CIEM	NO	YES	14
Cyber defense: sandboxing and deception	NO	YES	-
Digital Experience Monitoring (DEM)	YES	YES	-
In-browser terminals for privileged remote access	YES	YES	15
SSH command logging	YES	NO	-

Network on-ramps

Criteria	Cloudflare	Zscaler	FN
Clientless browser-based access	YES	YES	-
Device client software	YES	YES	-
Application connector software	YES	YES	16
Branch connector software	NO	YES	17
Anycast DNS, GRE, IPsec, QUIC, Wireguard tunnels	YES	NO	18
Private network interconnect for data centers & offices	YES	NO	-
Inbound IP transit (BYOIP)	YES	NO	-
IPv6-only connection support	YES	NO	19
Recursive DNS resolvers	YES	YES	-
Device clients and DNS resolvers freely open to public	YES	NO	20

Comparison results

Group Score	Criteria	Cloudflare	Zscaler
Overall	**37**	**33**	**18**
Internet-native network platform	5	5	1
Cloud-native service platform	4	4	1
Services to adopt SASE	6	5	4
Services to extend ZT, SSE, SASE and beyond	12	10	7
Network on-ramps	10	9	5

Footnotes (FN)

1. Per cloudflarestatus.com and cloudflare.com/network, Cloudflare has public data centers in 275+ cities. Many cities are served by more than one data center. As of Jan 2022, per trust.zscaler.com and config.zscaler.com, Zscaler has 73 public data centers in 55 cities with 13 data centers in no published clouds and 11 data centers with auto geo proximity disabled. The other claimed 77 data centers do not appear to be publicly documented and/or available to any customer.
2. Per config.zscaler.com/zscaler.net/cenr, ZIA has seven distinct clouds, ZPA has two different distinct clouds, and other products like ZDX has more distinct clouds.
3. Most services are supported with a 99.999% uptime SLA, but their DNS resolver only offers a 99.99% uptime SLA (source).
4. For example, a request from a remote user to a private self-hosted application can be inspected in one pass on the same server within the same data center by SWG, RBI, ZTNA, and app security services.
5. Composable architecture requires being able to adopt any service offered in the platform in any order and have it be concurrently interoperable with previously deployed services. Zscaler has architectured some of its services to run separately on unique architecture that prevents such composability, which theses Zscaler articles demonstrate (source 1, source 2).
6. Cloudflare acquired Area 1 in April 2022. It is on the roadmap to integrate Area 1's email security management into the Cloudflare Zero Trust management interface. Zscaler does not offer email security, such that this is not an equivalent gap. However, Zscaler has separate management interfaces for their ZIA and ZPA offerings as well as many of their add-ons such as RBI.
7. Cloudflare Zero Trust is built on Cloudflare Workers powered by V8 isolate technology at our edge. Zscaler uses an older container-based architecture, which slows development time and adds overhead costs when shipping new features.
8. Zscaler does not claim to be able to smartly route and accelerate traffic from data center to data center over its own network backbone.
9. While Zscaler does offer branch connector software, it does not provide full on-prem SD-WAN functionality and it does not appear in analyst research for WAN edge infrastructure.
10. Zscaler's standard RBI technology sends a stream of pixels, whereas Cloudflare's patented network vector rendering technology sends a stream of draw commands. Also, as of June 2022, Zscaler only runs RBI in 4 data centers. The combination results in a poor user experience with many Internet and SaaS applications.
11. Cloudflare Intrusion Detection is available today in our private beta program. Contact your account team to inquire about joining.
12. Zscaler does not offer a DDoS protection service. All cloud-native service providers have some measure of DDoS protection built into their architecture, but this will not effectively mitigate a modern DDoS attack. While implementing Zero Trust does keep your applications from being directly exposed on the Internet, it does not stop contractors or other users with granted access from attacking the application via the ZTNA providers' network.
13. In March 2022, Zscaler announced that it added inline application protection into its ZTNA offering – ZPA. However, this is not equivalent to a full Web Application Firewall (WFA) for both public and private addressable applications. And it also lacks bot detection capabilities.
14. In 2020-21, Zscaler acquired Edgewise Networks for cloud workload protection platform (CWPP), Cloudneeti for cloud security posture management (CSPM), and Trustdome for cloud infrastructure entitlement management (CIEM). It has not integrated these cloud security services into its Zero Trust services.
15. Cloudflare provides in-browser terminals for SSH and VNC, whereas Zscaler provides in-browser terminals for SSH and RDP. Many Cloudflare customers use Apache Guacamole to run RDP in the browser.
16. Zscaler requires virtual machine infrastructure to run its image, whereas Cloudflare offers a daemon that can run with or without VMs.
17. Zscaler requires virtual machine infrastructure to run its image, and traffic can only pass through ZIA or ZPA, but not both in one pass.
18. Zscaler supports Anycast only for DNS resolution. For GRE or IPsec tunnels, customers must use an unique IP address per Zscaler data center. And it's app connector and device client rely on non-Anycast DTLS tunnels.
19. Zscaler's device client does not support IPv6-only connections per their community forums (source)
20. Zscaler does not offer free public DNS resolution (e.g. 1.1.1.1) and encrypted IP communication (e.g. WARP).