Cloudflare 和 Zscaler 的比较 —— Zero Trust、SSE 和 SASE 等

比较概述

这是根据变革性的网络和安全趋势——包括 Zero Trust、安全服务边缘（SSE）和安全访问服务边缘（SASE），对 Cloudflare 和 Zscaler 整体产品的功能进行的比较。37 个比较标准分为 5 个类别：互联网原生平台；云原生服务平台；采用 SASE 架构的服务；扩展 Zero Trust、SSE、SASE 及更多（超越这些市场趋势当前定义的）的服务；以及网络入口。部分比较需要更多背景和说明，请参见最后一页的脚注。

如需更概念性的比较，请访问 cloudflare.com/products/zero-trust/cloudflare-vs-zscaler

互联网原生网络平台

标准	Cloudflare	Zscaler	FN
对任何客户开放的数据中心城市	270	55	1
各数据中心所属的不同云（控制平面）	1	~8	2
正常运行时间服务级别协议	100%	99.99-99.999%	3
在所有边缘服务上单次通过检查	是	否	4
威胁研究实验室	是	是	-

云原生服务平台

标准	Cloudflare	Zscaler	FN
组合式架构	是	否	5
单面板管理界面	是	否	6
无服务器计算开发平台	是	否	7
FedRAMP 授权过程中或已授权	是	是	8

采用 SASE 架构的服务

标准	Cloudflare	Zscaler	FN
Zero Trust 网络访问（ZTNA）	是	是	-
云访问安全代理（CASB）	是	是	-
安全 web 网关（SWG）	是	是	-
防火墙即服务（FWaaS）	是	是	-
WAN 即服务，提供 L3-7 流量加速	是	否	9
本地 SD-WAN	无 - 合作伙伴	无 - 合作伙伴	10

扩展 ZTNA、SSE、SASE 及更多的服务

标准	Cloudflare	Zscaler	FN
云电子邮件安全（CES）	是	否	-
远程浏览器隔离（RBI）	是	是	11
数据丢失防护（DLP）	是	是	12
入侵检测系统（IDS）	是	是	13
网络和应用 DDoS 保护	是	否	14
应用安全：WAF 和机器人检测	是	否	15
应用性能：CDN、DNS 和负载平衡	是	否	-
云安全：CWPP、CPSM 和 CIEM	否	是	16
网络防御：沙箱与欺骗	否	是	-
数字体验监测（DEM）	否	是	-
用于特权远程访问的浏览器内终端	是	是	17
SSH 命令日志记录	是	否	-

网络入口

标准	Cloudflare	Zscaler	FN
基于浏览器的无客户端访问	是	是	-
设备客户端软件	是	是	-
应用连接器软件	是	是	18
分支连接器软件	否	是	19
Anycast DNS、GRE、IPsec、QUIC、Wireguard 隧道	是	否	20
适用于数据中心和办公室的专用网络互连	是	否	-
入站 IP 传输（BYOIP）	是	否	-
纯 IPv6 连接支持	是	否	21
递归 DNS 解析器	是	是	-
设备客户端和 DNS 解析器免费对公众开放	是	否	22

比较结果

类别得分	标准	Cloudflare	Zscaler
总体	37	32	18
互联网原生网络平台	5	5	1
云原生服务平台	4	4	1
采用 SASE 的服务	6	5	4
扩展 ZTNA、SSE、SASE 及更多的服务	12	9	7
网络入口	10	9	5

脚注（FN）

1. 根据 cloudflarestatus.com 和 cloudflare.com/network，Cloudflare 在 270 多个城市设有公共数据中心。很多城市由超过一个数据中心提供服务。截至 2022 年 1 月，根据 trust.zscaler.com 和 config.zscaler.com，Zscaler 在 55 个城市拥有 73 个公共数据中心，其中 13 个数据中心在未发布的云中，11 个数据中心禁用了自动地理邻近功能。其声称拥有的另外 77 个数据中心似乎并没有公开记录和/或不对任何客户开放。
2. 根据 config.zscaler.com/zscaler.net/cenr，ZIA 有 7 个不同的云，ZPA 有两个不同的云，ZDX 等其他产品有更多不同的云。
3. 大多服务由 99.999% 正常运行时间 SLA 支持，但其 DNS 解析器仅提供 99.99% 正常运行时间 SLA（来源）。
4. 例如，远程用户对私有自托管应用的请求可以通过 SWG、RBI、ZTNA 和应用安全服务在同一数据中心的同一服务器上进行一次性检查。
5. 可组合的架构要求能够以任何顺序采用平台提供的任何服务，并能与之前部署的服务并发互操作。在 Zscaler 的架构中，部分服务在独特的架构上独立运行，从而妨碍了这种可组合性。有关详情，参见这些 Zscaler 文章（来源 1，来源 2）
6. Cloudflare 在 2022 年 4 月 1 日收购 Area 1。该公司已在路线图中规划将 Area 1 的电子邮件安全管理集成到 Cloudflare Zero Trust 管理界面中。Zscaler 不提供电子邮件安全服务，因此这并非一个可比的差距。然而，Zscaler 为其 ZIA 和 ZPA 产品以及很多附加组件（如 RBI）提供独立的管理界面。
7. Cloudflare Zero Trust 建立在 Cloudflare Workers 之上，由我们边缘的 V8 隔离技术驱动。Zscaler 使用更老的基于容器的架构，这减慢了开发时间，并增加推出新功能时的间接成本。
8. 截至 2022 年 6 月，Cloudflare 正处于获得 FedRAMP 授权的过程中，而 Zscaler 已经获得 FedRAMP 授权。
9. Zscaler 并没有声称能够通过自己的骨干网络智能地路由和加速从数据中心到数据中心的流量。
10. 虽然 Zscaler 提供分支机构连接器软件，但其没有提供完整的本地 SD-WAN 功能，也没有出现在 WAN 边缘基础设施的研究分析中。
11. Zscaler 的标准 RBI 技术发送像素流，而 Cloudflare 的专利网络矢量渲染技术发送绘制指令流。此外，截至 2022 年 6 月，Zscaler 仅在 4 个数据中心运行 RBI。这种组合导致很多互联网和 SaaS 应用的用户体验很差。
12. 2021 年以来，Cloudflare 在我们的 Zero Trust 平台内原生构建 DLP 服务。内测于 2022 年 7 月开始，欢迎加入等候名单以了解更多。公测将于 8 月开始。
13. Cloudflare 入侵检测今天推出内测。请联系您的账户团队以了解如何加入。
14. Zscaler 不提供 DDoS 保护服务。所有云原生服务提供商都在其架构中内置了某种 DDoS 保护措施，但这不足以有效缓解现代 DDoS 攻击。虽然实施 Zero Trust 确实能防止您的应用直接暴露在互联网上，它并不能阻止具有访问权限的承包商或其他用户通过 ZTNA 提供商的网络对应用进行攻击。
15. 在 2022 年 3 月，Zscaler 宣布在其 ZTNA 产品 —— ZPA 中增加了内联应用保护。然而，这并不等同于为公共和私有可寻址应用提供一个完备的 Web 应用程序防火墙（WAF）。而且该系统不具备机器人检测能力。
16. 在 2020-21 年，Zscaler 收购了 Edgewise Networks 作为云工作负载保护平台（CWPP），收购 Cloudneeti 作为云安全态势管理（CSPM），收购 Trustdome 作为云基础设施授权管理（CIEM）。该公司没有将这些云安全服务集成到其 Zero Trust 服务中。
17. Cloudflare 为 SSH 和 VNC 提供浏览器内终端，而 Zscaler 为 SSH 和 RDP 提供浏览器内终端。很多 Cloudflare 客户使用 Apache Guacamole 来在浏览器中运行 RDP。
18. Zscaler 需要虚拟机基础设施来运行其映像，而 Cloudflare 提供了一个后台进程，有无虚拟机均可运行。
19. Zscaler 需要虚拟机基础设施来运行其映像，且流量仅能通过 ZIA 或 ZPA，但不能一次通过两者。
20. Zscaler 仅对 DNS 解析支持 Anycast。对于 GRE 或 IPsec 隧道，客户必须为每个 Zscaler 数据中心使用唯一的 IP 地址。而且其应用连接器和设备客户端依赖于非 Anycast DTLS 隧道。
21. 根据其社区论坛，Zscaler 的设备客户端不支持纯 IPv6 连接。（来源）
22. Zscaler 不提供免费的公共 DNS 解析（例如 1.1.1.1）和加密 IP 通信（例如 WARP）。