Cloudflare 與 Zscaler 在 Zero Trust、SSE、SASE 等方面的比較

比較概況

這是 Cloudflare 和 Zscaler 在轉型網路與網路安全趨勢方面（包括 Zero Trust (ZT)、安全服務邊緣 (SSE) 和安全存取服務邊緣 (SASE)）的整體方案功能比較。將 37 個準則分為五組：網際網路原生網路平台；雲端原生服務平台；採用 SASE 架構的服務；延伸 ZT、SSE、SASE 等（目前市場趨勢的定義）的服務；以及網路入口。有些比較需要更多背景資訊與說明，因此在最後一頁加上此類註腳。

如需更多概念上的比較，請造訪 cloudflare.com/products/zero-trust/cloudflare-vs-zscaler

網際網路原生網路平台

準則	Cloudflare	Zscaler	FN
可供任何客戶使用的數據中心所在城市	270	55	1
不同數據中心使用不同的雲端（控制平面）	1	~8	2
100% 正常運作時間服務等級協定	100%	99.99-99.999%	3
對所有邊緣服務執行單遍式貫通檢測	是	否	4
威脅研究實驗室	是	是	-

雲端原生的服務平台

準則	Cloudflare	Zscaler	FN
可組合的架構	是	否	5
單一面板管理介面	是	否	6
無伺服器運算開發平台	是	否	7
FedRAMP 進行中或已授權	是	是	8

採用 SASE 架構的服務

準則	Cloudflare	Zscaler	FN
Zero Trust 網路存取 (ZTNA)	是	是	-
雲端存取安全性代理程式 (CASB)	是	是	-
安全 web 閘道 (SWG)	是	是	-
防火牆即服務 (FWaaS)	是	是	-
具有 L3-7 流量加速的 WAN 即服務	是	否	9
內部部署 SD-WAN	無 - 合作夥伴	無 - 合作夥伴	10

延伸 ZT、SSE、SASE 等的服務

準則	Cloudflare	Zscaler	FN
雲端電子郵件安全性 (CES)	是	否	-
遠端瀏覽器隔離 (RBI)	是	是	11
資料丟失預防 (DLP)	是	是	12
入侵偵測系統 (IDS)	是	是	13
網路與應用程式 DDoS 防護	是	否	14
應用程式安全性：WAF 和機器人偵測	是	否	15
應用程式效能：CDN、DNS 和 LB	是	否	-
雲端安全性：CWPP、CPSM 和 CIEM	否	是	16
網路防禦：沙箱和騙術	否	是	-
數位體驗監控 (DEM)	否	是	-
特殊權限遠端存取適用的瀏覽器內終端	是	是	17
SSH 指令紀錄	是	否	-

網路入口

準則	Cloudflare	Zscaler	FN
零用戶端瀏覽器型存取 (agentless)	是	是	-
裝置用戶端軟體	是	是	-
應用程式連接器軟體	是	是	18
分支機構連接器軟體	否	是	19
Anycast DNS、GRE、IPsec、QUIC、Wireguard 通道	是	否	20
適用於資料中心與辦公室的私有網路互連	是	否	-
用戶 IP 網段接入 (BYOIP)	是	否	-
對僅限 IPv6 連線的支援	是	否	21
遞迴 DNS 解析程式	是	是	-
裝置用戶端和 DNS 解析程式對大眾任意開放	是	否	22

比較結果

群組分數	準則	Cloudflare	Zscaler
整體	37	32	18
網際網路原生網路平台	5	5	1
雲端原生的服務平台	4	4	1
採用 SASE 架構的服務	6	5	4
延伸 ZT、SSE、SASE 等的服務	12	9	7
網路入口	10	9	5

註腳 (FN)

1. 根據 cloudflarestatus.com 和 cloudflare.com/network，Cloudflare 在超過 270 座城市擁有公共資料中心，且許多城市都有多個資料中心為其提供服務。截至 2022 年 1 月，根據 trust.zscaler.com 和 config.zscaler.com，Zscaler 在 55 座城市擁有 73 個公有資料中心，其中有 13 個資料中心位於未發佈的雲端，11 個資料中心則是已停用自動地理鄰近性。其他聲稱擁有的 77 個資料中心似乎並未公開記錄和/或提供給任何客戶使用。

2. 根據 config.zscaler.com/zscaler.net/cenr，ZIA 有七個相異的雲端，ZPA 有兩個不同的相異雲端，其他像是 ZDX 等產品擁有更多相異雲端。

3. 大部分的服務支援 99.999% 正常運作時間 SLA，但是其 DNS 解析程式僅提供 99.99% 正常運作時間 SLA（來源）。

4. 例如，遠端使用者對私人自我裝載應用程式所提出的要求，可能會由 SWG、RBI、ZTNA 和應用程式安全服務，在相同資料中心內同一部伺服器的單一通路中進行檢查。

5. 可組合的架構必須能夠以任何順序採用平台中提供的任何服務，並使該服務與先前部署的服務同時互通。Zscaler 已將其部分服務架構化，以便在唯一的架構上單獨執行；而該架構無法擁有此類可組合性（正如這些 Zscaler 文章所說明）（來源 1、來源 2）。

6. Cloudflare 已在 2022 年 4 月 1 日收購 Area 1。藍圖中的規劃，就是將 Area 1 的電子郵件安全性管理整合至 Cloudflare Zero Trust 管理介面。Zscaler 並未提供電子郵件安全性，因此這並非對等差異。但是，Zscaler 對於其 ZIA 和 ZPA 方案以及多個附加服務（例如 RBI）具有不同的管理介面。

7. Cloudflare Zero Trust 建構在 Cloudflare Workers 之上，後者由我們邊緣的 V8 隔離技術提供支援。Zscaler 使用較舊的容器式架構，會使開發時間變慢，在推出新功能時也會增加開支成本。

8. 截至 2022 年 6 月，Cloudflare 是正在進行 FedRAMP，Zscaler 則是 FedRAMP 已授權。

9. Zscaler 並未聲稱能夠在其自有的網路骨幹上，以智慧方式來路由和加快資料中心對資料中心的流量速度。

10. 雖然 Zscaler 提供分支機構連接器軟體，卻未提供完整的內部部署 SD-WAN 功能，也並未顯示在 WAN 邊緣基礎結構的分析研究中。

11. Zscaler 的標準 RBI 技術會傳送一個像素串流，而 Cloudflare 的專利網路向量渲染技術則是傳送一個繪製命令串流。截至 2022 年 6 月，Zscaler 僅在 4 個資料中心內執行 RBI。此結果導致多個網際網路和 SaaS 應用程式的使用者體驗不佳。

12. Cloudflare 自 2021 年起開始在我們的 Zero Trust 平台內原生建構 DLP 服務。我們已在 2022 年 7 月開始推出私人測試，請加入等候名單以瞭解詳情。公開測試將在 8 月開始。

13. 現在，我們的私人測試計畫中已可使用 Cloudflare 入侵偵測。請聯絡您的客戶團隊以詢問加入相關事宜。

14. Zscaler 並未提供 DDoS 防護服務。所有雲端原生服務提供者都有某種內建在其架構中的 DDoS 防護措施，但這樣無法有效地緩解新式的 DDoS 攻擊。雖然實作 Zero Trust 會避免讓您的應用程式直接暴露在網際網路上，但這樣無法防止承包商或其他擁有存取權限的使用者透過 ZTNA 提供者的網路來攻擊應用程式。

15. 2022 年 3 月，Zscaler 宣布已將內嵌應用程式保護新增到其 ZTNA 方案 (ZPA) 中。但是，這並不等同於同時適用於公共和私人可定址應用程式的完整 Web 應用程式防火牆 (WFA)。此外，它也缺乏機器人偵測功能。

16. 2020 至 2021 年間，Zscaler 收購了 Edgewise Networks 以提供雲端工作負載保護平台 (CWPP)，收購了 Cloudneeti 以提供雲端安全狀態管理 (CSPM)，以及收購了 Trustdome 以提供雲端基礎結構權利管理 (CIEM)。他們並未將這些雲端安全服務整合到其 Zero Trust 服務中。

17. Cloudflare 為 SSH 和 VNC 提供瀏覽器內終端，Zscaler 則為 SSH 和 RDP 提供瀏覽器內終端。許多 Cloudflare 客戶會使用 Apache Guacamole 在瀏覽器中執行 RDP。

18. Zscaler 需要虛擬機器基礎結構才能執行其影像，Cloudflare 則是提供精靈，無論有無虛擬機器都可以執行。

19. Zscaler 需要虛擬機器基礎結構才能執行其影像，而且流量僅能流經 ZIA 或 ZPA，無法單遍同時流經二者。

20. Zscaler 僅針對 DNS 解析支援 Anycast。對於 GRE 或 IPsec 通道，客戶必須依據各個 Zscaler 資料中心來使用專屬的 IP 位址。此外，其應用程式連接器和裝置用戶端必須仰賴非 Anycast DTLS 通道。

21. 根據 Zscaler 的社群討論區，Zscaler 的裝置用戶端並不支援僅限 IPv6 的連線（來源）

22. Zscaler 不提供免費的公用 DNS 解析（例如 1.1.1.1）和加密的 IP 通訊（例如 WARP）。