CLOUDFLARE

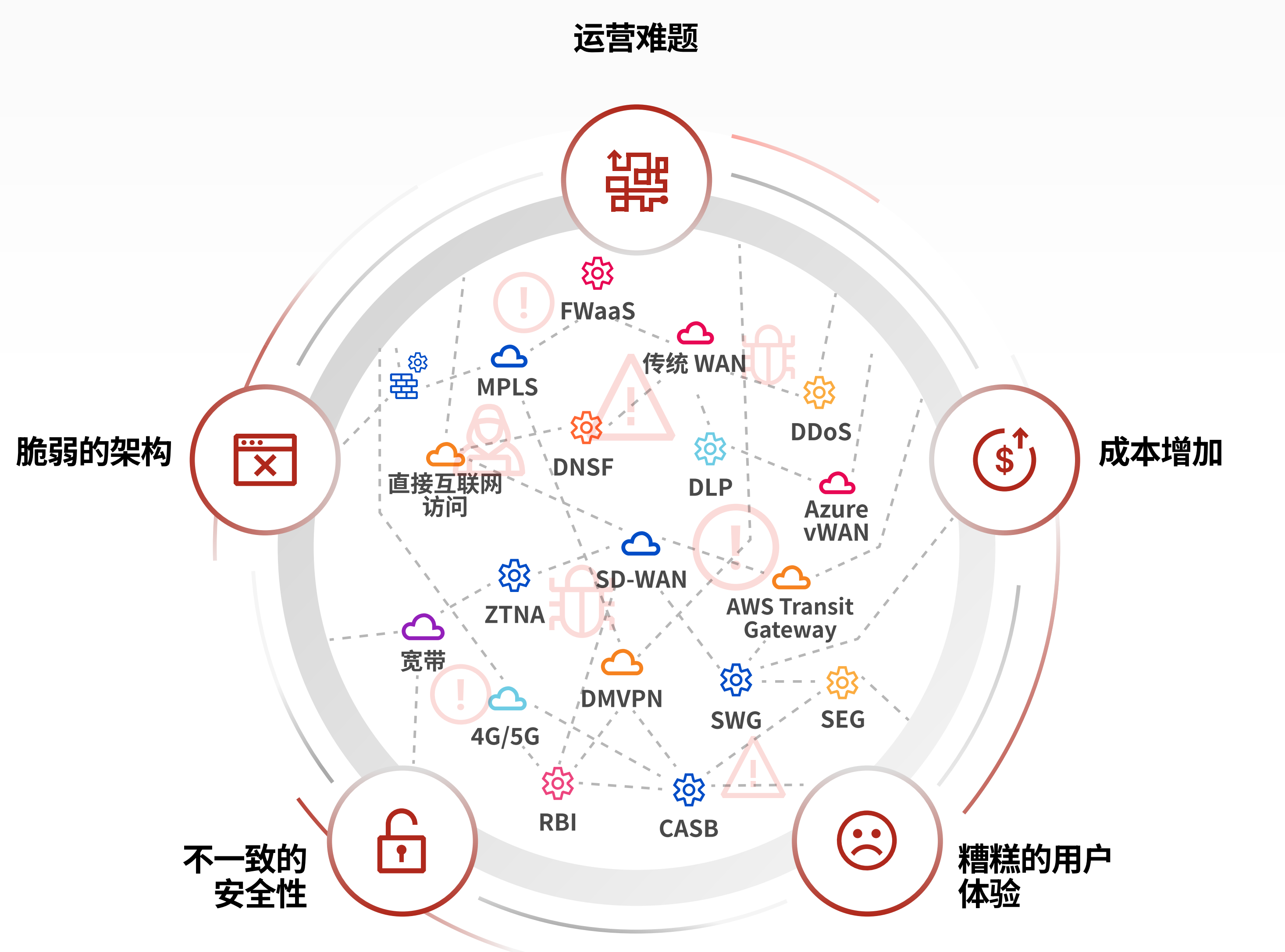
每一条路径都很重要

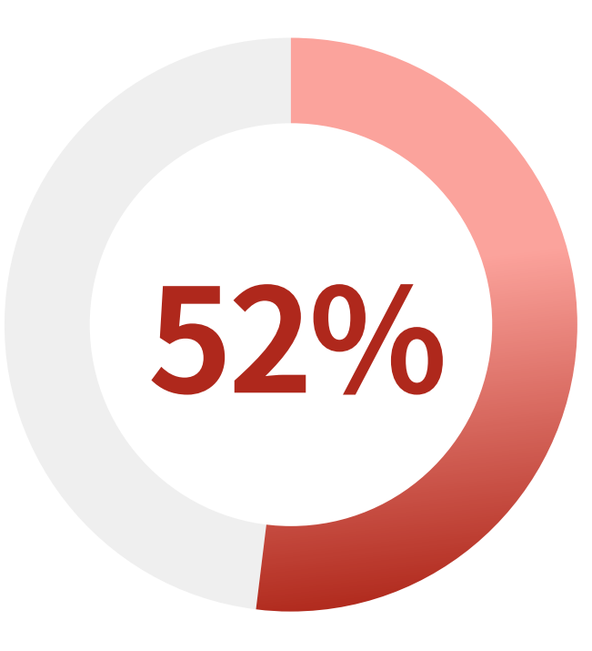
是时候重新规划网络流量路由了吗？

传统企业网络仅专注于内部连接和安全。然而，混合办公、云部署应用和快速数字现代化投资已经彻底改变了网络数据流动的地点和方式。

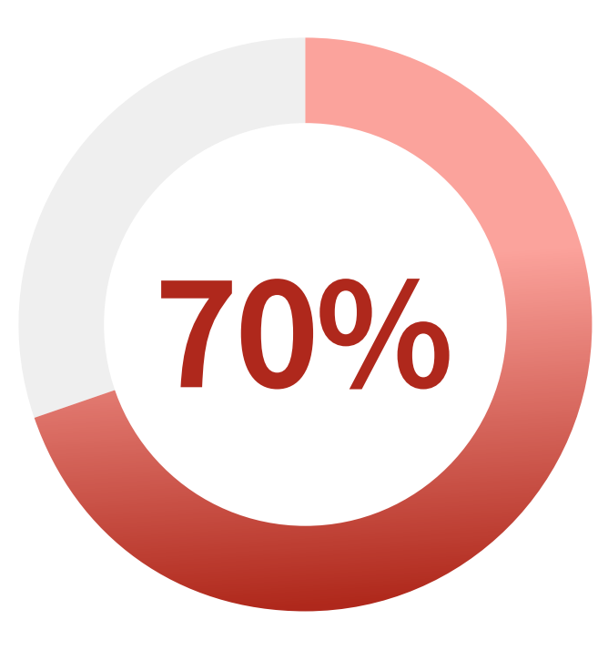
如果网络基础设施未准备好以满足当今的业务需求，会发生什么？

传统企业网络经常遇到：





52% 的高管表示**复杂性是安全运营的最大障碍**[1]



全球 70%的 CEO 表示，他们的**网络成熟度正在对业务交付产生负面影响**[2]

平台化企业的平均 ROI 达到 101%，相比之下，非平台化企业平均 ROI 仅为 28%[1]

传统架构使用数十种不同的解决方案来覆盖四种网络流量，这也增加了复杂性

流量路径	所需产品	挑战
入站流量 来自互联网	传统上由本地防火墙、VPN、DMZ 基础设施和 ISP 过滤覆盖	• DoS 和 DDoS 攻击 • Zero-day 漏洞利用 • 网络钓鱼 • 恶意软件
出站流量 到互联网和云应用	传统上由本地防火墙和代理覆盖	• 横向移动 • 数据暴露 • 勒索软件传播 • 僵尸网络参与
WAN 网络 连接园区和分支机构	传统上由物理/虚拟化网络、SD-WAN、私有互连和 MPLS 覆盖	• 资本支出/运营支出较高 • 网络延迟 • 带宽限制 • 用户体验欠佳
多云 适用于跨多个云平台的应用	传统上由 DIY 产品覆盖	• 可见性和策略执行问题 • 监管复杂性

必须做出什么改变？

对比

传统网络

- 插入设备以增加新功能或扩展覆盖范围——这会导致停机和服务中断
- 将用户和分支机构连接并保护到托管于数据中心的应用
- 网络边界内的隐式“受信任”流量
- 为支持办公室员工而优化

现代网络

- 部署可组合服务而非设备，降低复杂性并减少中断
- 必须在任何地方支持云、SaaS 和私有云应用
- 必须假定所有实体“不可信任”，包括分布式用户、设备、应用及数据
- 不能假定用户的位置，必须支持在任何地方工作的用户

如何在处理所有流量类型的同时满足现代要求？

不再为每个流量路径使用互不关联的解决方案，利用一个全球连通云全面解决网络现代化问题。

入站流量	出站流量	WAN 网络	多云流量
保护网络和应用免受 DDoS 和其他互联网传播的威胁损害	保护用户和办公室以防威胁，执行一致策略，并管控应用中的数据	连接和保护办公室、用户、设备、数据中心和基础设施	提供网络服务，以在公共云/混合云环境中连接、保护和构建应用

Cloudflare 的全球连通云使用可组合、可编程的架构，为您的用户以及基于云的业务基础设施和应用提供网络和安全服务。

- 无需扩展或扩充私有数据中心
- 使用基于云的网络和安全服务，而不是设备
- 借助 Zero Trust 减少对网络的过度“信任”

详细了解如何使用 Cloudflare 简化和加速网络现代化

了解更多

---

1. Ali, Mohamad 和 Jenkins，BJ。“捕捉网络安全红利”。IBM，https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform？访问日期：2025 年 6 月 26 日。
2. “NTT 的新研究发现，70% 的 CEO 表示他们的网络正在拖慢业务增长。” Business Wire，2022 年 10 月 20 日，https://www.businesswire.com/news/home/20221020005120/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds。新闻稿。

010 8524 1783 | enterprise@cloudflare.com | Cloudflare.com
REV:BDES-7841.2025JUL31

CLOUDFLARE