

SASE 和 SSE 平台

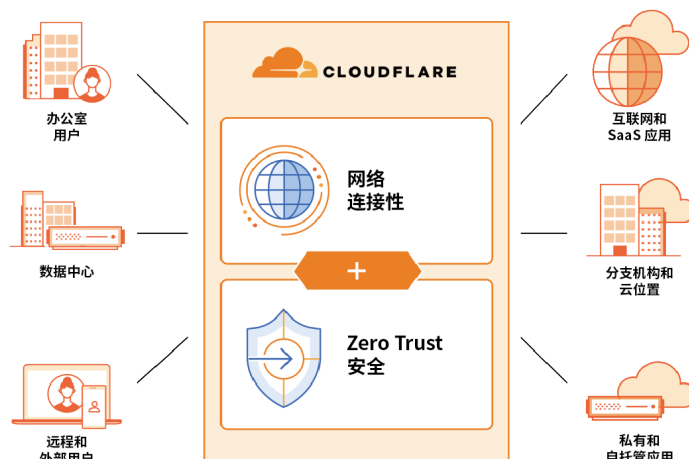
扩展 Cloudflare 全球连通云的覆盖范围——通过可组合的 Zero Trust 网络连接服务降低网络风险并现代化您的网络

立即融合安全与网络

为了减少 IT 复杂性并重新获得控制，[88% 的 IT 领导者](#)已经在整合和优化其技术栈。作为一个重要的架构趋势，SASE 融合了安全性和网络连接，以提供简单、安全的访问，同时提升业务敏捷性。

简单、安全地将任何用户连接到任何资源，无需 VPN 或 MPLS 回传

准备好加速您的 Zero Trust 部署并进一步提高互联网流量速度了吗？利用连接和保护 Web 应用的同一[全球连通云](#)来连接、保护企业应用和 Web 浏览。**Cloudflare One** 是我们的单一供应商[安全访问服务边缘 \(SASE\)](#) 平台，支持以任意顺序采用的可组合入口和服务。许多客户从 Zero Trust 安全服务边缘 (SSE) 开始，以减少他们的攻击面，阻止网络钓鱼或勒索软件，防止横向移动，并保护数据。



采用 Zero Trust 架构的最快路径

在用户进入企业网络后，不再隐式信任，避免授予过度访问权限。使用代理对进入、离开和网络实体之间的每个请求进行身份验证和授权，明确验证身份、设备态势和业务上下文。



提高运营效率

简化策略管理，更快地解决问题，并改善用户体验——将连接相关 IT 工单减少 **80%**。



降低网络风险

利用源于 **20%** 的 Web——DNS、电子邮件、应用、API 等——的广泛威胁情报获得实时洞察，并部署应对措施。



为企业赋能

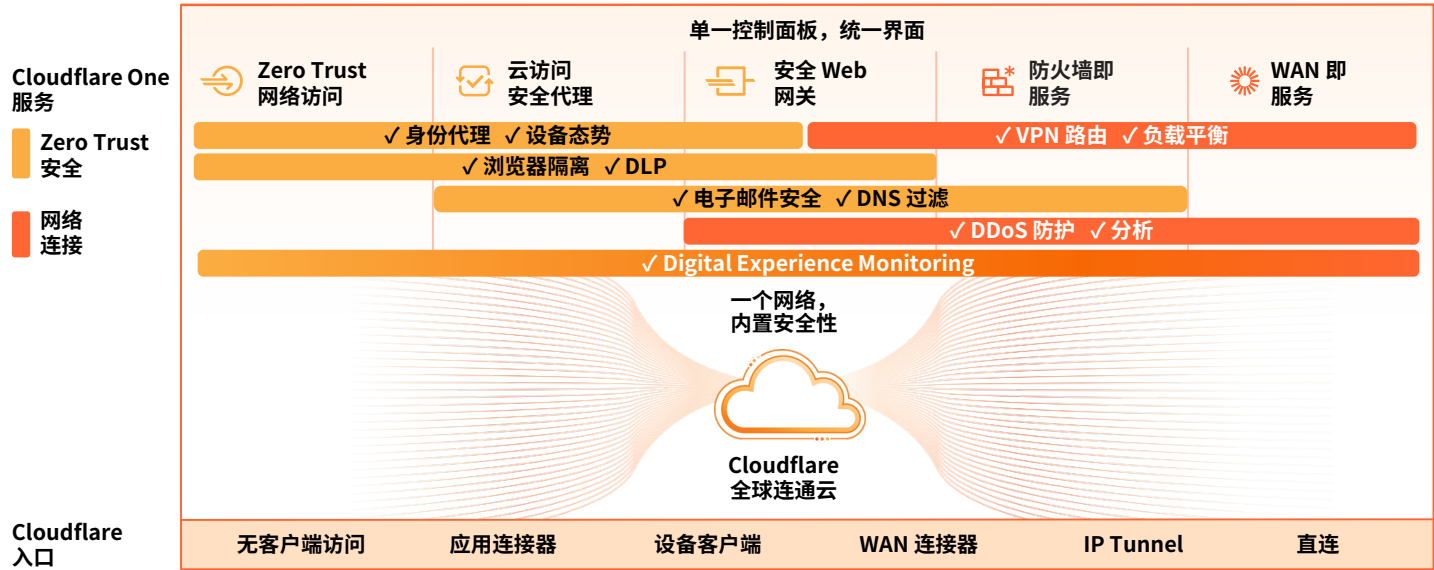
利用可组合的内联安全服务，提供对网络流量的整体可视性，帮助加速数字成熟，减少硬件资本支出，整合单点产品。



Everywhere Security

所有服务都设计成在 **330+** 城市的数据中心运行，让所有流量都在最接近来源的地方进行检查，从而在任何地方提供一致的速度和规模。

Cloudflare One 如何工作



为任何团队提供灵活的入口，更快设置任意对任意连接

- **IT 和安全团队：**保护所有用户到应用的流量、双向流量和站点到站点流量。
- **网络团队：**利用现代化架构简化站点到站点连接并降低 TCO。
- **DevOps 团队：**保护现代服务到服务工作流并简化网状/点到点连接。

通过全球连通云集成**超越 SASE 的服务**

Cloudflare One 融合了 SASE 平台通常不具备的安全和性能，从而进一步降低了复杂性。例如：

- **云电子邮件安全：**拦截通过电子邮件传播的威胁。
- **Auth DNS、负载均衡和 DDoS 防护：**我们的反向代理和网络服务内置于所有应用访问控制中。

优先用例 及从何开始



为什么使用 Cloudflare for SASE?

通过您已信赖的 Cloudflare 服务，帮助推进您的安全访问服务边缘 (SASE) 部署。

无论您当前正在使用 Cloudflare [加速和保护 Web 应用](#)、[构建全栈和 AI 应用](#)，还是[简化数据合规流程](#)，在我们的网络上整合均可帮助您重获 IT 控制权，同时降低供应商复杂性和成本。

所有 Cloudflare 服务，包括 Cloudflare One，都基于我们的[全球连通云](#)打造。这是一个可编程、可组合的一站式服务平台，用于实现网络、云、应用和用户之间的任意互连。

一项[独立成本效益分析](#)显示，我们的全球连通云在三年内为一个代表受访客户的合成组织实现了如下效益：

- ✓ **238% ROI**，回报期不超过六个月
- ✓ **安全团队效率提高 29%**，得益于增强保护、服务整合、加快事件响应和集中可见性
- ✓ **IT 团队效率提高 13%**，得益于简化、自动化或消除手动 IT 任务
- ✓ **泄露风险降低多达 25%**，得益于 Cloudflare 识别并更好地保护了众多攻击面



得到分析师认可的 SASE 平台

Gartner®

在 2024 年 Gartner® 单一供应商 SASE 魔力象限™ 中首次得到认可

连续第二年得到 Gartner® 安全服务边缘魔力象限™ 认可

FORRESTER

2021 年第一季度 Forrester Wave™ 安全服务边缘 (SSE) 解决方案报告中获评为“表现卓越者”

2023 年第三季度 Forrester Wave™ Zero Trust 平台 (ZTP) 报告中获评为“卓越表现者”

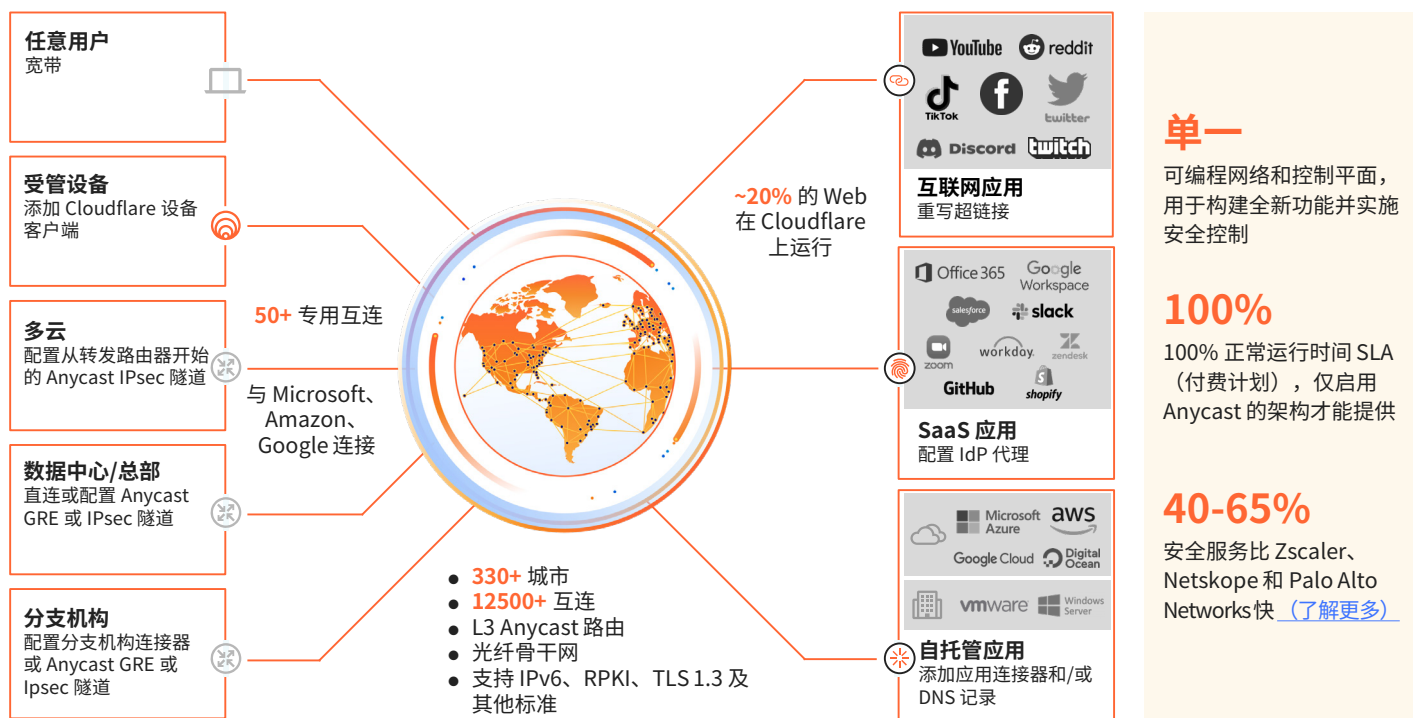
Forrester Wave™ 企业电子邮件安全, 2023 年第二季度报告中的领导者

IDC

IDC MarketScape 2023 年 Zero Trust 网络访问 (ZTNA) 报告中获评为“领导者”

IDC MarketScape 2023 年网络边缘安全即服务报告中获评为“领导者”

通过灵活的接入方式开始使用



Cloudflare 支持与专业服务



您得到了强有力的支持



Cloudflare 获评为 2024 年 [Gartner® Peer Insights™](#) 客户之声：Zero Trust 网络访问的“客户之选”



财富 500 强
[阅读案例研究](#)

10 万+

混合劳动力
保护互联网和应用访问。



Delivery Hero

电子商务
[阅读案例研究](#)

4.4 万+

全球劳动力受到保护
以 Zero Trust 取代混合
办公员工的 VPN。



第一大求职网站
[阅读案例研究](#)

3 个月

替代 VPN
1.3 万名员工和 2000 名承包商



美国政府
[了解更多](#)

100+

美国民事机构
的办公室使用 Cloudflare 与
Accenture 合作的 DNS 过滤进
行保护。

准备好加速您的 SASE & SSE 部署了吗？
立即联系您的 Cloudflare 代表。

欢迎阅读我们的 [SASE 参考架构](#) 以了解更多信息，或者观看 [我们的 Zero Trust 平台交互演示](#) 以了解其如何工作。

Gartner, Zero Trust 网络访问“客户之声”，由同行评选，2024 年 1 月 30 日
Gartner 安全服务边缘魔力象限，作者：Charlie Winckless、Thomas Lintemuth 和 Dale Koeppen，2024 年 4 月 15 日

GARTNER 是 Gartner, Inc. 和/或其附属公司在美国 and 全球的注册商标和服务商标，MAGIC QUADRANT 和 PEER INSIGHTS 均为注册商标，The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE 徽章是 Gartner, Inc. 和/或其附属公司的商标，在此经许可使用。保留一切权利。Gartner® Peer Insights 内容包含最终用户基于自身体验而提出的主观意见，这些意见不应视为事实陈述且不代表 Gartner 或其附属公司的观点。Gartner 不支持本内容中描述的任何供应商、产品或服务，也不就本内容的准确性或完整性作出任何明示或暗示保证，包括对任何适销性或适合某一特定目的的保证。Gartner 不支持其研究出版物中提及的任何供应商、产品或服务，也不建议技术用户只选择那些获得最高评分或其他称号的供应商。Gartner 研究出版物包含 Gartner 研究和顾问组织的意见，不应被视为事实陈述。Gartner 对本研究不承担任何明示或暗示担保，包括任何针对特定用途的适销性或适用性的担保。