CLOUDFLARE

保护和连接应用服务的三大挑战

传统架构为何失败 —— 全球连通云能提供什么帮助

内容

概述

Web 应用和 API 是现代企业增长的基础。2023 年，维持 Web 存在的企业占比跃升至 71%，同时另一项研究估计目前 28% 的业务活动是在线进行的。[1]

从移动电子商务平台到内部生产力工具、应用（以及使其能够运行的API）不仅允许企业向客户提供动态、个性化的内容，还连接全球员工团队、提高用户生产力并加快开发人员持续创新的步伐。然而，随着企业规模扩大，维持应用的最佳性能和安全性变得越来越重要，而且更难确保：

- **API 易于使用，但难以保护。**一项研究发现，API 不安全性（API 错误或被利用导致的泄露）每年造成的损失达到约 410-750 亿美元[2]
- **即使短短几秒钟的延迟也会严重损害用户体验、参与度和转化率。**流量激增、宕机和应用性能低劣会导致客户流失；据估计，88% 的在线用户在经历负面体验后将不再访问网站[3]
- **应用泛滥、复杂性和供应商挑战阻碍了业务增长。**随着企业规模扩大，管理不断增长的应用组合——通常跨越多个环境和供应商——会带来成本上升、控制丧失以及更大的安全和 IT 问题

对抗这些问题——而不减缓业务运营——需要比传统硬件或多供应商、单一解决方案云服务更灵活的解决方案。**全球连通云**旨在连接和保护 IT 环境中的所有内容，可以帮助企业整合关键的应用服务并促进业务增长。

挑战一：网络攻击复杂且代价高昂

Web 应用和 API 使企业能够更灵活地运作，提供优质的用户体验，并比以往更快地进行创新——它们也代表着一个日益扩大的攻击面。DDoS 攻击、API 威胁、恶意机器人和零日漏洞都有可能影响业务运营，降低客户信任，有时甚至带来毁灭性的后果。

攻击比以往任何时候更大、更复杂

随着企业规模扩大和客户基础增加，它们成为全球网络攻击者日益增长和诱人的目标：

- 应用层攻击在 2023 年暴增多达 80%
- 在 2023 年第三季度，Cloudflare 应对了一场创纪录的 DDoS 攻击，每秒请求数高达 2.01 亿次
- 数据泄露的平均成本飙升至 445 万美元——比 2020 年增加了 13%

攻击不仅比以往任何时候规模更大，而且由于采用了日益复杂的策略，其后果也变得更加严重。正如组织采用更先进的安全技术来保护其应用程序、基础设施和数据免受破坏一样，现代网络犯罪分子也利用人工智能和机器学习工具来发动定制、自适应的攻击。[4]

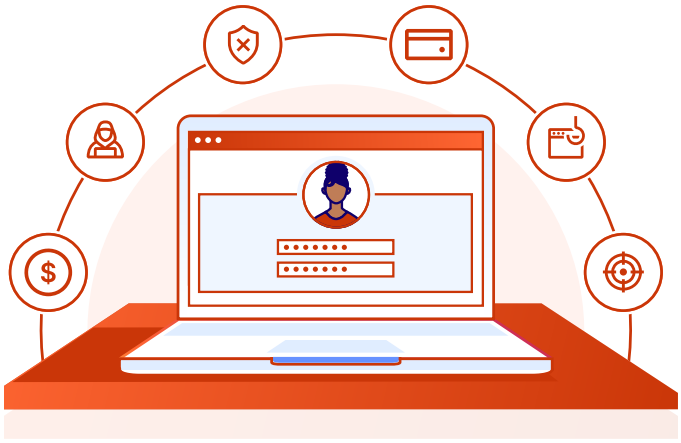
此类成功攻击可能会危及保密的用户数据，严重影响收入、品牌声誉和客户信任，并导致严重的合规罚款和高昂的补救成本。

API 泄露的成本正在上升

近年来，API 经历了爆炸式增长，使企业能够将其灵活性和创新速度提高到前所未有的水平。但 API 开发的快速增长也使得检测和修补它们所包含的每一个漏洞变得几乎不可能，特别是当开发人员和工程师未能在推出之前与安全团队进行沟通的情况下。

如果企业缺乏保护其 API 环境安全所需的内部资源，则后果可能会很严重。在最近的一项调查中，53% 的受访者由于 API 令牌暴露而导致其应用程序和网络造成数据泄露。[5] 专家还发现，全球范围内，脆弱或不安全的 API 每年给企业造成了 410 亿至 750 亿美元的损失。[6]

然而，确保 API 的安全远非一个简单的过程。现有的应用安全工具集，包括 Web 应用防火墙 (WAF)、DDoS 缓解和机器人管理服务，并非为防御 API 威胁而专门设计的，而且许多仍然没有提供为 API 防范针对性威胁所需的细粒度控制。



挑战二：应用性能低劣导致用户流失

对于各种线上业务和移动应用而言，消费者任何时候都期望流畅快速的体验。不幸的是，流量激增、服务器超载和意外宕机都会影响应用的可用性和性能，从而导致客户参与度和信任度下降。为了对抗这些问题，企业需要可靠的应用服务，可以保证快速加载时间和可用性，同时轻松扩展丰富、动态的用户体验。

延迟问题会导致销售额下降——达到数十亿

根据《福布斯》的数据，在 2023 年，大约 71% 的全球企业维持着一定形式的 Web 存在，估计 28% 的业务是在线进行的。[7] 换言之：消费者有大量选择，这给企业带来了额外的压力，要求他们提供闪电般快速、始终可用且易于使用的体验。

在所有性能基准中，对流畅成功的在线体验而言，延迟是最清晰的指标之一。加载缓慢的 Web 体验不仅会让客户感到沮丧，通常还会对转化率产生不利影响。

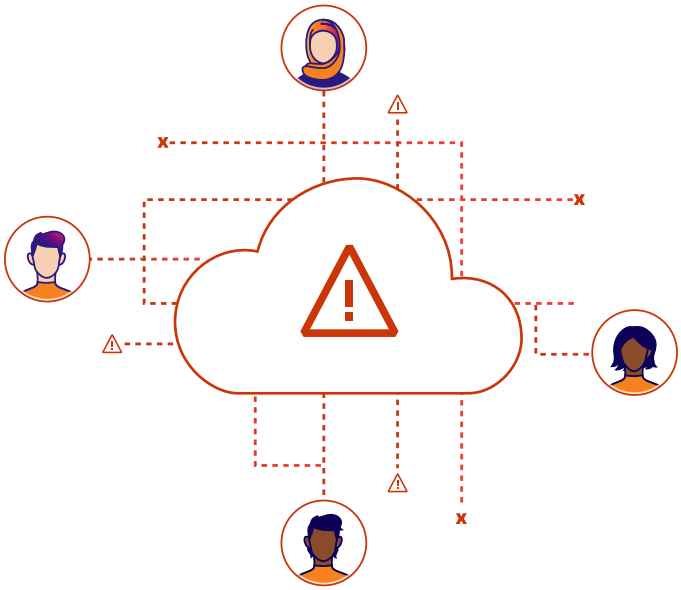
一份报告发现，如果网站加载时间超过 3 秒，高达 40% 的用户会离开。[8] 而且用户参与度的损失还在不断增加：每年由于加载缓慢而损失的销售额估计达到 26 亿美元。[9]

网站的不可预测性会在企业最需要用户的时候疏远他们

当今的在线企业已经非常熟悉在假日流量峰值和爆发增长期间维持流畅消费者体验的挑战。

假日购物者的突然涌入很容易会让电商应用不堪重负，当购物车意外清空或产品页面无法快速加载时，用户会感到沮丧。或者，紧急服务网页可能无法满足大量用户的需求，在最关键的时刻导致长时间的服务中断。

没有足够的流量优化和可靠性措施，企业有可能会失去大部分用户群。据估计，61% 的 Web 用户希望 5 秒内在网站上找到他们所需的东西；否则，他们会去其他地方寻找。[10] 这对很多企业来说是一个承担不起的风险。



挑战三：应用服务存在可扩展性挑战

保护和加速 Web 应用和 API 对于现代企业的成功至关重要。然而，随着这些企业不断扩大其内部运营和客户群，关注重点很快就从确保应用的安全和性能转向*规模化*。

管理复杂的架构可能会减缓业务增长，并损害控制。

在 2023 年，连接和保护复杂的数字环境对许多企业来说是一个复杂的过程。关键的数据和应用存在于日益扩大的本地基础设施、公共云和 SaaS 环境的组合中，超过 40% 的安全和 IT 团队刚开始承担管理和保护它们的任务。[11]

随着这些应用组合增长，对其进行适当配置、保护和维护所需的时间也在增加。企业很快发现自己缺乏时间和资源来做到这一点，导致他们失去对整个应用环境的可见性和控制。

Cloudflare 和 Forrester Consulting[12] 进行的一项调查发现，这种失控是由四个主要因素驱动的：

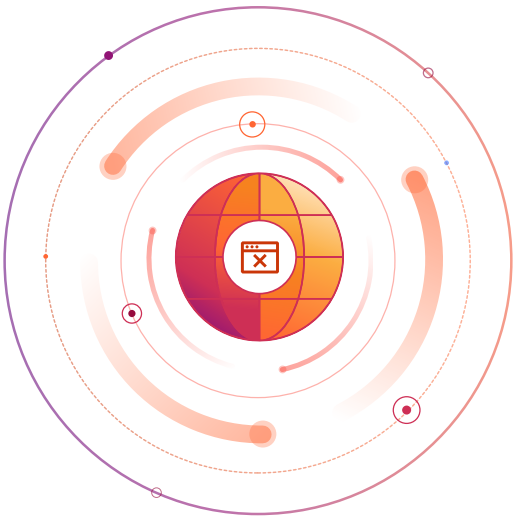
1. 组织要负责更多应用 (66% 的受访者回答 “是”) 。
2. 应用存在于更多位置 (62%)。
3. 组织已将运营从本地位置转移到云环境 (54%)。
4. 组织已转向远程或混合办公模式 (49%)。

如果无法控制环境的各个方面，企业可能会面临实施延迟，导致应用容易受到威胁，或发现很难以高效的方式扩展业务 (和竞争优势) 。

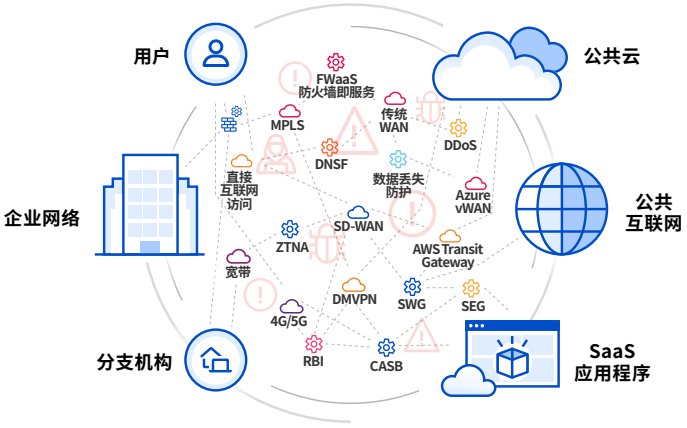
现有的应用服务并非为灵活性和业务增长而设计。

更糟糕的是，提供集成应用服务的云供应商可能会将企业困在使其处于不利地位的合同中，尤其是在它们尝试扩展规模时。企业可能会从供应商最初的产品中获益，但会被锁定在数据存储的低效定价模式中，或者缺乏在多个供应商之间灵活混合和匹配服务的能力。

在面临供应商锁定、灵活性降低和业务增长受阻的情况下，98% 的受访组织表示，如果如果有一个云原生平台可以为他们的用户、应用程序、数据、设备、网络和云环境提供安全、高性能的 “任意对任意” 连接，他们将能从中发现价值。[13] 这样的平台不仅有助于缩小企业的整体攻击面，还有超过 50% 的受访者表示它还将有助于加速上市时间和增加收入。



传统硬件和云解决方案不足之处



优化 Web 应用和 API 需要一系列专门的服务，包括本地和全局负载平衡、等候室、内容优化和视频流式传输服务，以及 Web 应用防火墙 (WAF)、API 保护、机器人管理和 DDoS 保护。然而，传统硬件和基于云的单点解决方案都无法提供企业所需的简化保护和性能，以确保竞争性增长、保持客户满意度、有效管理风险、保护品牌声誉和提高内部生产力。

硬件设备无法优化和保护云中的内容

本地硬件设备从未设计为支持云计算需求和满足现代业务需求。

这些传统解决方案成本高昂且难以扩展，导致在安全性和性能之间权衡，可能对应用程序的性能和可用性以及客户体验产生不利影响。

而且这往往会加重安全和 IT 团队的负担，他们必须处理几乎不可能的任务，即管理和保护一个由硬件和虚拟化设备、混合和多云环境以及从根本上互不兼容的 SaaS 应用构成的复杂网络。不可避免的是，这些团队不得不努力寻找解决方案，满足日益严格的合规要求，并避免引入安全漏洞——而不会损失生产力或使最终用户感到沮丧。

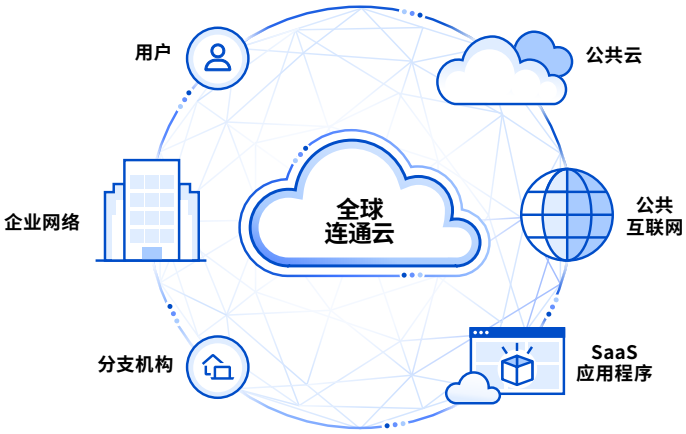
多供应商云服务引入了复杂性和供应商锁定

总的来说，基于云的应用服务使企业能够更灵活、更敏捷地运营，但这些服务不可避免存在自身的性能、安全性和可扩展性问题。随着业务需求持续增长，以及应用程序格局日益复杂化，找到在 Web 应用程序安全和性能优化方面均表现出色的云供应商并非易事。

声称提供集成服务的供应商并不总是在“底层”提供真正的集成，而是选择打包各种不同的解决方案，这些解决方案仍然难以实施、维护和扩展。

如今，大多数基于云的解决方案供应商倾向于将客户锁定在其生态系统中，这使得他们的解决方案与采用混合或多云部署的客户不兼容。这迫使企业要么整合于某个云供应商上（通常是一项复杂且昂贵的任务），要么维护多个应用安全和管理堆栈——这是 IT 的噩梦。

隆重推出全球连通云：整合应用服务的全新方式



现代企业需要在不牺牲应用性能和安全性的前提下无缝扩展。这需要比硬件或基于云的单点解决方案更灵活的应用服务方式。

这种全新方式就是“**全球连通云**”：一个云原生服务的统一平台，旨在帮助企业重新控制其 IT 环境。由智能、可编程的全球云网络驱动，全球连通云提供无与伦比的安全性、性能、可见性和可靠性。

传统的云供应商（如 AWS、GCP 等）只为托管在其云平台上的应用程序提供服务，而全球连通云则旨在与任何应用程序配合使用，无论其托管在何处。

在其核心，全球连通云提供四个关键功能：

1. **一种可组合和可编程的架构。**全球连通云旨在提供灵活性和易用性，使企业能够轻松管理其专有基础设施、云系统、合规需求和特定配置，而不会损害用户体验或管理流程。

2. **原生、无处不在的互联网集成。**全球连通云与互联网和企业网络均原生集成，在每个用户、应用程序和基础设施之间提供安全、低延迟、可无限扩展的连接。

3. **内置平台情报和创新。**一个具备良好架构的全球连通云在基础层面内置了广泛的服务，分析巨量且多样性的流量，以便自动更新情报模型，而不会导致低效或安全漏洞。

4. **统一、简化的界面。**全球连通云通过单一的视图管理大部分 IT 环境，显著减少工具泛滥、仪表板过载和警报疲劳。

主要能力	技术效益	商业效益
无限可互操作性	通过在相同的服务器上构建支持 API 的无服务器函数，可以与任何第三方系统编排和自动化服务。	释放内部资源，降低组织成本
可自定义的联网	完全支持 API 编程的 L1-7 连接，以满足合规、隐私和主权要求	满足本地法规要求，而不牺牲生产力或效率
原生互联网集成	将企业网络和资源连接到互联网——完全掌控从业务请求源到目的地的全过程。	确保全球任何地点始终可用的应用连接和性能
全球网络连接	与互联网连接的所有用户、应用和网络基础设施均实现低延迟	创造更佳客户体验，增强企业竞争优势
无限网络可扩展性	按需扩展，无需客户配置、硬件或虚拟设备支持	轻松地发展业务，没有复杂的配置或隐藏成本
真正一次性内置服务处理	内置安全、性能和隐私功能——连接永远不会中断或遭到入侵	提高应用的安全性、性能和可靠性，无需权衡取舍
平台情报驱动的创新	平台情报提升对所有互联网路径的可见性，并帮助通过最快的路径加速代码、数据和流量	重新获得对环境的控制和可见性，无论应用和数据位于何处
加快供应商整合	整合供应商服务、日志和客户服务能力，并从统一的管理界面进行交付	降低复杂性，优化跨多个供应商和服务的应用管理
加速数字转型	完全连接您当前和未来的网络环境，涵盖所有用户、应用、系统和位置	通过连接您的环境、应用和用户，提高生产力、效率和灵活性

Cloudflare 如何提供连接和控制

Cloudflare 是世界上第一款全球连通云。Cloudflare 的全球网络覆盖 120+ 国家/地区逾 310 城市，拥有独特的架构，提供企业所需的连接，以实现最佳的应用安全和性能，而无需依赖过时的解决方案或向威胁敞开大门。

使用 Cloudflare 整合应用服务

联系我们

> **最终用户的体验非常流畅，而且使用像 Cloudflare 这样的集中式服务来管理应用访问策略，使我们的IT和安全团队更轻松。此外，我们现在可以看到谁在使用我们的每项服务，这有助于我们全面提高安全性。”**
>
> João Pedro Gonçalves，全球首席信息安全官，EQT

参考资料

1. Forbes Advisor。“2023 年最热门网站统计数据。” https://www.forbes.com/advisor/business/software/website-statistics/。访问日期：2023 年 10 月 20 日。
2. Tech Wire Asia。“API 漏洞每年给企业造成高达 750 亿美元的损失。” https://techwireasia.com/2022/06/api-vulnerabilities-costing-businesses-up-to-us75-billion-annually/。访问日期：2023 年 10 月 20 日。
3. Forbes Advisor。
4. McKinsey & Company。“网络安全趋势：展望未来。” https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon。访问日期：2023 年 10 月 23 日。
5. VentureBeat。“50% 的组织报称因 API 密钥泄露而遭遇数据泄露。” https://venturebeat.com/security/data-breaches-api/。访问日期：2023 年 10 月 23 日。
6. Tech Wire Asia。“API 漏洞每年给企业造成高达 750 亿美元的损失。” https://techwireasia.com/2022/06/api-vulnerabilities-costing-businesses-up-to-us75-billion-annually/。访问日期：2023 年 10 月 20 日。
7. Forbes Advisor。“2023 年最热门网站统计数据。” https://www.forbes.com/advisor/business/software/website-statistics/。访问日期：2023 年 10 月 20 日。
8. Forbes Advisor。
9. Forbes Advisor。
10. Forbes Advisor。
11. Cloudflare 和 Forrester Consulting。“新研究揭示云巨头正在束博企业。” https://www.cloudflare.com/press-releases/2023/new-study-reveals-cloud-giants-are-holding-businesses-captive/。访问日期：2023 年 10 月 20 日。
12. Cloudflare 和 Forrester Consulting。
13. Cloudflare 和 Forrester Consulting。

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-5435.2024JAN10