# 告别传统硬件设备

用智能、可扩展的应用服务替换传统设备

## 传统硬件设备的问题

硬件设备无法满足现代网络业务的需求。虽然这些设备的购置本身就已经非常昂贵，但包括 DDoS 攻击在内的复杂现代网络攻击能轻而易举地压垮它们，让其无法发挥作用。

不幸的是，支出并不止步于购买一台硬件设备。由于硬件设备有一个硬性的性能上限，并且不能扩展到某个极限之外，因此企业被迫继续投资于更大、更好的设备，以满足其业务需求。设备的维护和管理也很昂贵，在维护期间需要停机，而且无法处理攻击或高需求导致的流量激增。企业还被迫每 3-7 年购买新的硬件，以跟上技术进步、软件更新和业务需求的步伐。在大多数硬件解决方案中，团队通常需要购买额外的硬件组件或设备，以便为其部署增加功能。加上运行这些硬件设备和维护数据中心的成本，基于硬件设备的解决方案的总拥有成本很容易飙升到极高水平。

最后，将解决方案和功能整合到硬件设备上可能会面临一些挑战，因为这些设备缺乏灵活性，由许多不同的组件组成，使用复杂，并且通常设计为强制供应商锁定。

转移到 Cloudflare 这样的边缘云平台来满足应用安全和性能需求，不仅帮助组织简化其基础设施和运营，还可以通过消除硬件更新、减少供应商臃肿和降低数据中心开销等方式大幅节省成本。

## Cloudflare 的不同之处

Cloudflare 的应用服务产品可以帮助企业轻松整合应用性能和安全需求。

Cloudflare 全球边缘服务器网络可以减少延迟并提高网站性能。借助 Cloudflare CDN、DNS、负载均衡（用于全球和本地流量管理）等行业领先解决方案，Cloudflare 确保 Web 应用和 API 始终可用且性能卓越。

Cloudflare 还提供一系列安全功能，以帮助防御各种基于 Web 的攻击，无论攻击规模大小，包括 DDoS 防护、Web 应用程序防火墙 (WAF) 和机器人保护。我们的云原生架构帮助企业跟上新兴威胁，即使前所未见的零日攻击，都能在 10-15 秒内获得防御能力。

Cloudflare 提供整合安全和性能的一站式服务。我们的统一应用服务解决方案帮助快速识别和响应事件，同时确保业务连续性和轻松扩展。

### 可扩展且易于使用

Cloudflare 允许组织按需使用资源，并实现更快的自动威胁调查和事件响应，最大程度地减少手动配置和管理。

我们的网络都可以轻松吸收流量激增，无论是由 DDoS 攻击还是高需求所致，并在多个位置和源服务器之间进行流量负载平衡，以确保您的应用对最终用户始终可用。

### 防御新型攻击

Cloudflare 的云原生安全解决方案由来自一个庞大全球网络的威胁情报支持，帮助组织直面新型和不断增长的网络攻击，无需等待安全补丁或昂贵且麻烦的设备升级。

### 具有成本效益的整合

Cloudflare 减少在配置和管理方面花费的宝贵工程时间，让您专注于最高优先级的计划上。

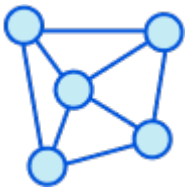
我们支持高效成长，让您仅在需要时为自己所用的资源付费，无需提前为高昂但不一定能充分利用的硬件投入成本。

## 为什么可扩展性如此重要

Cloudflare 允许用户自动、按需调用资源来应对高需求产品发布、假日购物季或网络攻击等所致的流量激增，例如试图使应用瘫痪的大规模、多手段 DDoS 攻击。

在遭遇这种流量峰值时，Cloudflare 负载平衡服务可以轻松将流量路由到其他区域的源服务器，或者将流量从特定区域或部署中不堪重负的服务器转移出去。在发生区域性故障时，负载平衡也可立即将流量转移到其他源，而不会造成延迟。

Cloudflare 还提供不计量 DDoS 防护和速率限制解决方案，让您无需担心费用飙升，也不用努力分配资源以保护应用免受大规模攻击破坏。我们的网络持续吸收甚至最大规模的 DDoS 攻击，让您的业务保持在线。



| | 传统硬件设备 | Cloudflare 应用程序服务 |
|---|---|---|
| **硬件成本** | 硬件成本，包括更新、升级和数据中心间接成本。 | 没有硬件成本。 |
| **专业服务成本** | 传统的硬件解决方案需要专业服务支持，多个小时的复杂脚本编写和维护开销可能会导致高昂的额外成本。 | 产品易于使用可减少用于管理一个供应商的工程时间，让工程师有更多的时间投入到更重要的项目上。 |
| **服务整合** | 将应用服务整合到传统的硬件设备上可能既昂贵、又复杂。<br>• 获得强大、可定制的安全性，但不够灵活<br>• 维护停机时应用处于无保护状态，且性能欠佳<br>• DDoS 攻击或流量激增会导致瓶颈，使下游安全解决方案和应用变得失效 | 在 Cloudflare 上整合应用服务简单且经济高效。使用 Cloudflare，企业能够：<br>• 将攻击检测时间缩短超过 50%<br>• 将应用性能和网页加载时间提高 4 倍<br>• 将检测和应对入侵尝试的平均时间缩短 90%<br>• 吸收大规模 DDoS 攻击并将流量从超负荷的服务器转移出去 |
| **会计影响** | 传统设备是基于资本支出 (CapEx) 模式销售的。这意味着：<br>• 解决方案需要前期的购置投资，这些投资会随着时间的推移而折旧<br>• 企业需要购置硬件来满足峰值需求，但在所有其他时间设备将得不到充分利用 | Cloudflare 的运营支出 (OpEx) 模式消除了有关前期资本支出和折旧的担忧：<br>• Cloudflare 的会计优势使投资回报更加直接<br>• 企业可轻松扩展其环境以满足特定需求，而无需投资于硬件的前期成本 |
| **实施时间** | • 硬件交付时间（因供应链问题而延长）<br>• 繁琐、依赖专业服务的设置过程<br>• 通常需要编写中央管理脚本，以便在所有设备上一致地部署配置 | • 轻松集中管理所有域的性能和安全<br>• 相比设备提供商，Cloudflare 的价值实现时间至少快 10 倍，即使从硬件设备交付并就位开始计算 |

要进一步了解如何使用 Cloudflare 应用服务保护您的 Web 应用程序免受现代网络攻击、确保业务连续性并将业务提升到新的水平，请访问 https://www.cloudflare.com/zh-cn/lp/appliances-to-cloudflare/