CLOUDFLARE

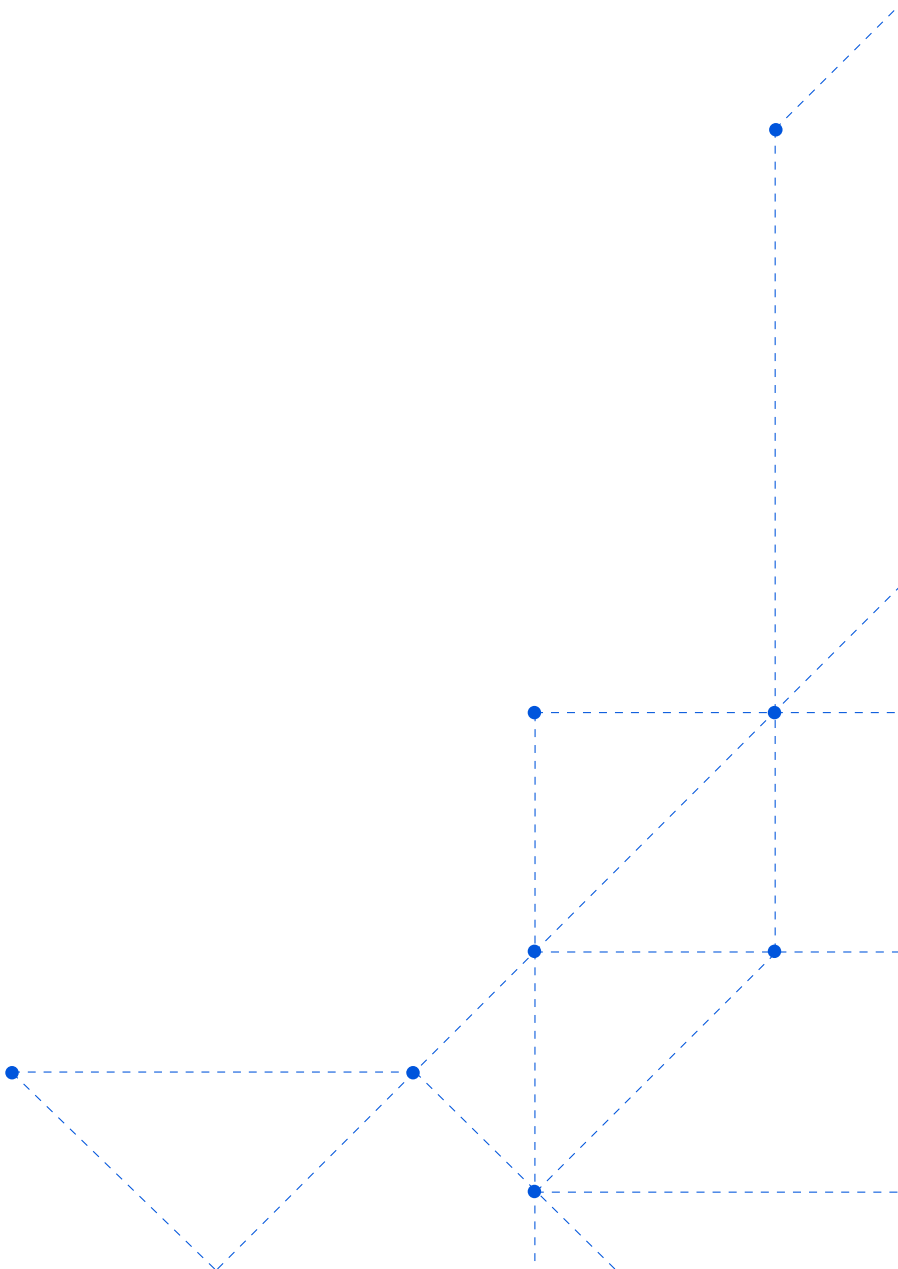
白皮书

网络硬件设备的消亡

为什么现在正是淘汰网络硬件的时候

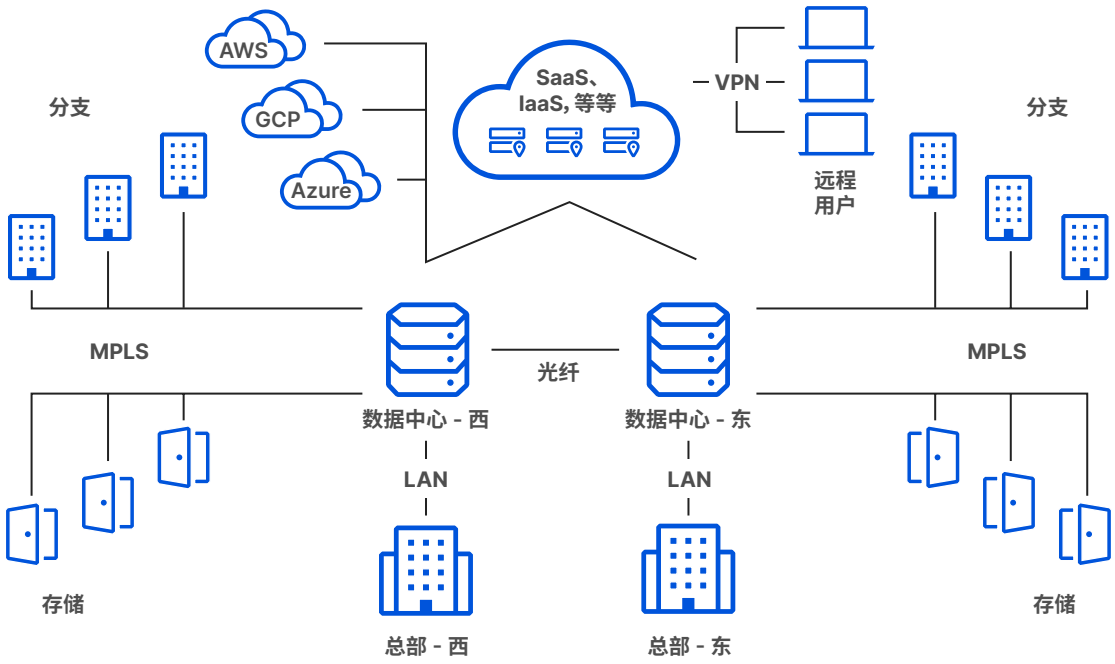
摘要

尽管存储和计算已迁移到云中，但许多网络功能仍留在企业内部，造成容量限制、高总体拥有成本、支持挑战和安全缺口等问题。在混合工作成为常态的情况下，各个组织都在努力确保足够的容量和有效的安全性。许多转型项目由于硬件积压远远超过一年而停滞。本文概述这些挑战，对其后果进行量化，并提出通过基于云的解决方案来提高混合云基础设施的速度、可负担性和安全性。



简介

事实证明，云迁移是降低基础设施成本、提高数据和应用程序可用性以及提高运营敏捷性的有效策略。不过，这种迁移极少能够一步到位。许多大型组织发现自己混合部署了多云和内部基础设施，形成一种复杂的结构：



这种混合基础设施不一定是坏事，但确实带来了麻烦。具体来说，它会造成各种网络功能（例如 DDoS 缓解、负载平衡、防火墙和 VPN）留在本地的情况。

在以云为中心的世界中，传统网络硬件设备不能胜任保护和加速关键基础设施的任务。这些设备一直是麻烦所在，成本高昂且往往杂乱无章，通过蛛网般的线缆连接在一起。一旦让云加入进来，安全漏洞、性能损失和其他支持挑战便会迅速出现。

本文描述在迁移到云的世界中维护网络硬件的风险和缺陷，并提供了建立一个更安全和有效的网络的策略。

云世界中的硬件风险

网络硬件设备具有多种特定功能，其使用方式在不同组织之间也有一定程度的差异。

常见的示例包括：

安全

- DDoS 防护
- 防火墙
- 虚拟专用网络
- 可配置的策略

性能和可靠性

- 负载平衡
- 流量加速/WAN 优化
- 数据包过滤
- 流量分析

这类硬件部署到本地时，所形成的架构通常会面临五类风险：**供应链压力、容量限制、高总体拥有成本、支持挑战**和**安全漏洞**。

前三类对于哪怕最先进的网络和安全团队都始终会带来挑战，后两类则因为云迁移而加剧。

供应链压力

与任何种类的物理产品类似，网络硬件容易面临各种供应链困难。材料成本上升时，一些材料和组件更难获得，或者运输提供商负担过重，网络硬件更难购买和更换。

不幸的是，这类困难最近很普遍，很大一部分原因是新冠疫情。根据 Gartner 研究：“疫情之前，订货交付时间常常需要 4-6 个星期。现在，200–300 天很常见，我们在向客户询问时还发现超过 430 天的情况。”

这些延迟源于多个因素：

- **物流困难：**历史上的供应链模型有多个故障点，要求最低限度的员工数量，并极度依赖不一定安全的技术——这些挑战近期开始发酵。在疫情期间，许多工厂停工，运输公司遭遇延迟，企业更难招到并留住许多类型的供应链工人。所有这些挑战都使得生产和交付硬件所需时间更长。也许物流中最有挑战性的方面就是，这就像是一场接力赛，自身没有遇到挑战的组织也可能因为供应链上游某个链条中断而受到影响。
- **更高的材料成本：**网络硬件设备依赖于各种原材料。由于需求旺盛、供应有限，材料价格飞涨，这意味着，不仅企业要等待更长时间才能获得其网络所需的东西，而且所支付的价格也高了许多。不幸的是，由于这些挑战，Gartner 预计硬件设备订货交付时间一直到 2023 年初都会保持高位（来源）。

所有这些挑战都会带来深远的影响。如果继续以采购、维护和更换硬件设备为工作重心，就会带来更高的开销成本，花费更多时间进行规划而不是执行，并且在动荡时期增加了对于保护物理供应链的安全性担忧。各个组织的工作重心应当从硬件设备的物流、订货交付时间、采购和存储转移到确保满足客户的需要之上。

容量限制

鉴于网络硬件设备的本质，在流量意外激增时网络硬件可能会变得不堪重负——无论流量是否合法，这一点已经不足为奇。但近期的一些趋势表明，流量意外激增已经是一个常见问题。

以分布式拒绝服务 (DDoS) 缓解为例。据 Microsoft 称，史上最大的 DDoS 攻击发生于 2021 年 11 月，最大流量达到 3.47 Tbps (来源) 。即便是对于市面上最先进的 DDoS 缓解硬件设备，这些 DDoS 攻击造成的负担也是它们承受能力的许多倍，这些硬件设备通常仅提供缓解此类攻击所需容量的一小部分。

据称，在 2021 年 11 月，史上最大 DDoS 攻击的最大流量达到了 3.47 Tbps。

并非所有组织都会招来如此规模的攻击，但同样并非所有组织都能够或已经实施最先进的 DDoS 缓解硬件。一份 Cloudflare 报告发现，容量耗尽攻击在 2022 年第 1 季度有所增加。事实上，超过 10 Mpps (百万数据包/秒) 的攻击按季度环比增长了 300%，超过 100 Gbps 的攻击按季度环比增长了 645% (来源) 。不仅仅是 DDoS 攻击的数量激增令人担忧，而且这些类型的攻击还会让许多所谓基于高容量硬件的缓解解决方案不堪重负。

此外，攻击流量并没有计入可能同时访问您的数据中心的合法流量。

在电商大促等流量高峰时段，平均来说，电子商务每日页面浏览量会在一夜之间翻倍 (来源) ，如果此时发生较小的攻击，产生的流量激增仍可能足以超出安全硬件的可承受极限。

DDoS 缓解只是本地硬件容量限制的一个示例。

其他示例包括：

负载平衡器： 独立的本地负载平衡器很容易因合法流量猛然激增而超负荷。发生这种情况时，可能需要很长时间才能置备和安装额外硬件。替代方案是保持可应对最坏状况的充足容量，但这种方法需要组织以高昂代价持续运转大量硬件。

虚拟专用网络 (VPN)： 如今，提前预测 VPN 使用量的难度提高了许多。对于许多组织来说，完全远程和混合工作成了新常态，但传统的 VPN 方法需要仔细规划、维护和管理，因为许多 VPN 不适用于整个组织连续使用。有太多员工在使用某个 VPN 时，连接和可靠性都会变差。此外，可能会出现安全问题，因为 VPN 在设计时并没有实施 Zero Trust 控制措施。还有，如果 VPN 不堪重负，组织可能“拆分隧道”来传输流量，如此一来，访问 Web 的流量不会经过 VPN——这样就很难跟踪和管理员工的 Web 活动。

面对这些问题，一种应对方法是购置更多、更新、更高容量的硬件。但这样的方法会带来许多其他问题。

拥有成本

与容量限制一样，数据中心硬件价格昂贵也不足为奇。例如，要获得约 100 Gbps 的 DDoS 缓解能力，所需硬件的前期投入可能介乎 40 万到 50 万美元之间。

而且，这些费用只是硬件设备总体拥有成本的一部分。请考虑以下支出：

- 团队成本：购买、运行和维护硬件以抵御 OSI 模型中每一层的威胁，并提供现代网站和互联网应用程序应有的性能和可靠性，这需要团队成员在每一种网络功能方面达到专家水平。组建具有如此广度和专业知识的团队是一项代价昂贵的提议，尤其是在全世界有史以来劳动力市场最紧张的时期。2022 年的一项 ISACA 调查发现，在参与年度调查的 2,000 位网络安全专业人士中，有 63% 的人反映有空缺的网络安全职位——比前一年增加了 8%（来源）。
- 维护成本：本地网络硬件的使用寿命平均为 3 到 5 年，然而这整个周期的质量担保常常需要额外的支出。如果考虑到技术创新的步伐，这些本地设备的使用寿命还会进一步缩短。替代方案是由厂商或第三方进行计划外——因此也没有预算——的维修。硬件故障也可能导致数据中心停机，其平均机会成本超过每分钟 8,800 美元（来源）。
- 更换成本：倘若每三年更换一次硬件设备，组织不仅需要重新支付其初始投资，还要投入资源来运送和安装新硬件。延迟更换通常会导致故障更加频繁，进而造成维护成本增多。

云交付的网络服务与这种模式形成鲜明对比。它们有可能通过一个更灵活的团队来运行，不会产生维护和运输成本，也不会迫使组织在代价高昂的升级和更频繁的故障之间权衡取舍。

硬件故障可能导致数据中心停机，平均机会成本超过每分钟 8,800 美元。

支持挑战

为网络硬件设备提供支持不仅是一项昂贵的提议，也是一个后勤上的挑战。硬件需要经常打补丁，才能应对最新的漏洞和攻击手段，这一过程通常依靠手动实施，因此容易受到人为错误的影响。

组织使用的硬件设备越多，因为疏忽大意或担心影响重要系统而最终疏于安装补丁的几率就越高。在最近的联合网络安全公告中，美国国家安全局 (NSA)、网络安全和基础设施安全局 (CISA) 和联邦调查局 (FBI) 报告称，在广为传播的网络攻击中利用了未安装补丁的网络设备中的 16 个公开已知缺陷（来源）。这些漏洞会影响从小型商务路由器到企业 VPN 在内的各种本地设备，而且可能使攻击者能够操控网络流量并从目标网络中渗漏数据。

尽管列出的这 16 个缺陷大部分被评级为紧急，安装补丁和补救措施并不容易。事实上，对硬件安装补丁可能相当复杂，因而有一整套的软件来帮助公司保持更新（来源）。

并且，哪怕只是遗漏一个补丁，后果也可能非常严重。这不仅是因为硬件仍然存在漏洞，还因为一旦发布了补丁，相应漏洞就会成为机会主义攻击者更高调的目标。与之形成对比的是基于云的安全防护服务，后者默认自动修复漏洞并安装更新，而且传播时间可以短至 30 秒，具体因云提供商网络速度而异。

硬件的其他维护挑战包括：

- **故障排除：**在仅有硬件的场景中，故障排除通常会迫使 IT 团队经历一次艰辛的过程，逐一拔掉负载平衡器、防火墙和其他本地设备，如此才能发现问题所在。

  同时使用云服务时，会使此过程更加复杂。依赖硬件的组织往往通过集中式数据中心及其所有独立设备来管理对这些服务的访问。当员工无法访问某项服务时，IT 团队还要检查一个额外位置来诊断问题。Productiv 最近的一份报告显示，所有 SaaS 应用程序中有 56% 属于影子 IT，也就是在 IT 部门不知情的情况下获取的未经批准、未受到管理的应用程序，这个问题的范围和规模正在迅速增长（来源）。
- **物理维护：**当硬件设备发生损坏时，IT 团队必须断开其物理连接，订购替换设备，测试替换设备并安装到位。这又是一个艰难的过程。考虑到许多跨国企业的规模十分庞大，这些需要关注的设备有可能位于地球另一端。

安全漏洞

即使组织具备所需的资源来持续置备和维护最新、最大容量的本地硬件，所形成的基础设施仍将面临严重的安全缺陷，尤其是在云计算已成为全球趋势的大环境中。

以员工访问管理为例。尽管 VPN 硬件可以在远程员工设备和运行于内部数据中心的应用程序之间建立加密隧道，但在建立此隧道后，它无法监控和保护用户活动。

如果员工的设备受到恶意软件入侵，或者网络钓鱼攻击窃取了他们的 VPN 凭据，则攻击者可能利用该 VPN 连接来访问各种敏感信息。网络钓鱼和恶意软件仍旧构成严重风险，并为威胁行为者带来丰厚的金钱收益。2021 年，FBI 报道称网络犯罪造成了 69 亿美元的损失。其中商业电子邮件威胁 (BEC) 给企业造成了 24 亿美元的损失（来源）。

如果员工的设备受到恶意软件入侵，或者网络钓鱼攻击窃取了他们的 VPN 凭据，则攻击者或可利用该 VPN 连接来访问各种敏感信息。

云服务和 SaaS 应用程序进一步增加了以硬件为中心的基础设施的安全性保障难度。例如，在混合云模型中，组织会同时运行本地和云基础设施。组织无法简单地将安全硬件发送给云提供商。如果组织想要继续将本地硬件用于其自己的数据中心，基础设施的不同部分将以不同的方式受到保护，从而使安全团队对传入攻击的可见性和控制力度降低。

基于云的服务将数据中心和云服务统一在由软件定义的单个层下，从而克服这两项挑战。

对这种方法的详细说明不在本文讨论范畴。若要了解更多信息，可以浏览以下文章：

- 什么是 Zero Trust 网络?
- 什么是安全访问服务边缘?

基于云的安全和性能服务：优势和挑战

通过云交付网络服务能够避免许多与硬件相关的问题，如供应链压力、容量限制、成本、支持挑战和安全漏洞。

- **供应链：**许多基于云的网络提供商旨在利用现代全球架构进行扩展，从而缓解供应链问题。
- **容量：**由于云具有广泛分布和软件定义的性质，组织可随业务规模扩大而轻松置备更多容量。
- **成本：**硬件的追加成本要么不存在，要么更容易提前计划。此外，云服务通常被归类为运营支出，而不是资本支出，这为许多企业带来税务和会计方面的好处。
- **支持：**后勤和资源需求由服务提供商解决。此外，也不会有遗漏补丁的可能，因为更新是自动进行的。
- **安全：**软件定义的网络服务可以在单个保护层下统一不同的基础设施。

但若部署不周全，云网络服务也会面临自身的风险：

风险	描述
延迟	一些基于云的网络功能依赖于专门的云数据中心，例如用于缓解 DDoS 的清理中心。将流量回传到这些数据中心可能会大幅增加延迟，具体取决于它与目标服务器的相对位置。 如果组织针对不同的网络功能使用不同的提供商，这个问题会更加严重。如果流量必须在不同提供商之间传递，延迟可能达到数百毫秒。
支持	当组织为不同功能采用不同提供商时，故障排除仍然是个问题。很难判断哪个提供商是拥塞或中断的起因。
成本	当组织为不同功能采用不同提供商时，仍然需要花费大量时间（和资金）对其进行管理。

要避免这些问题，请考虑以下策略：

- **寻找同时适用于云和本地基础设施的提供商。**
  这种能力让 IT 和安全团队能够设置一致的控制并从一个地方监控全局流量。这还有助于构建更有韧性的架构——在这种架构中，团队能够迅速对市场状况的波动做出应对。
- **寻找提供能协同工作的多种网络功能的云提供商。**
  这通常会减少流量必须进行的网络跳转次数，从而缩短延迟，进而改善最终用户体验。此外，在对网络问题进行故障排除时，您只需要联络一家公司就可以解决问题。另外，将多种功能捆绑在一起通常可以降低成本。
- **寻找可以从其网络中每一个位置执行多种网络功能的云提供商。**
  通过收购来扩展其服务组合的提供商不一定会全面整合这些新服务，导致某些功能只能由某些数据中心交付。因此，要考虑在整个网络中提供这些功能的提供商，从而避免上文列出的问题。
- **寻找网络覆盖全球的云提供商。**
  这一能力为上一项能力提供支持，确保最终用户无论身在何处都始终接近其网络。同时也能形成一个大型网络表面，既可吸收 DDoS 流量，又能执行其他需要大容量的联网功能。

Cloudflare 如何提供协助

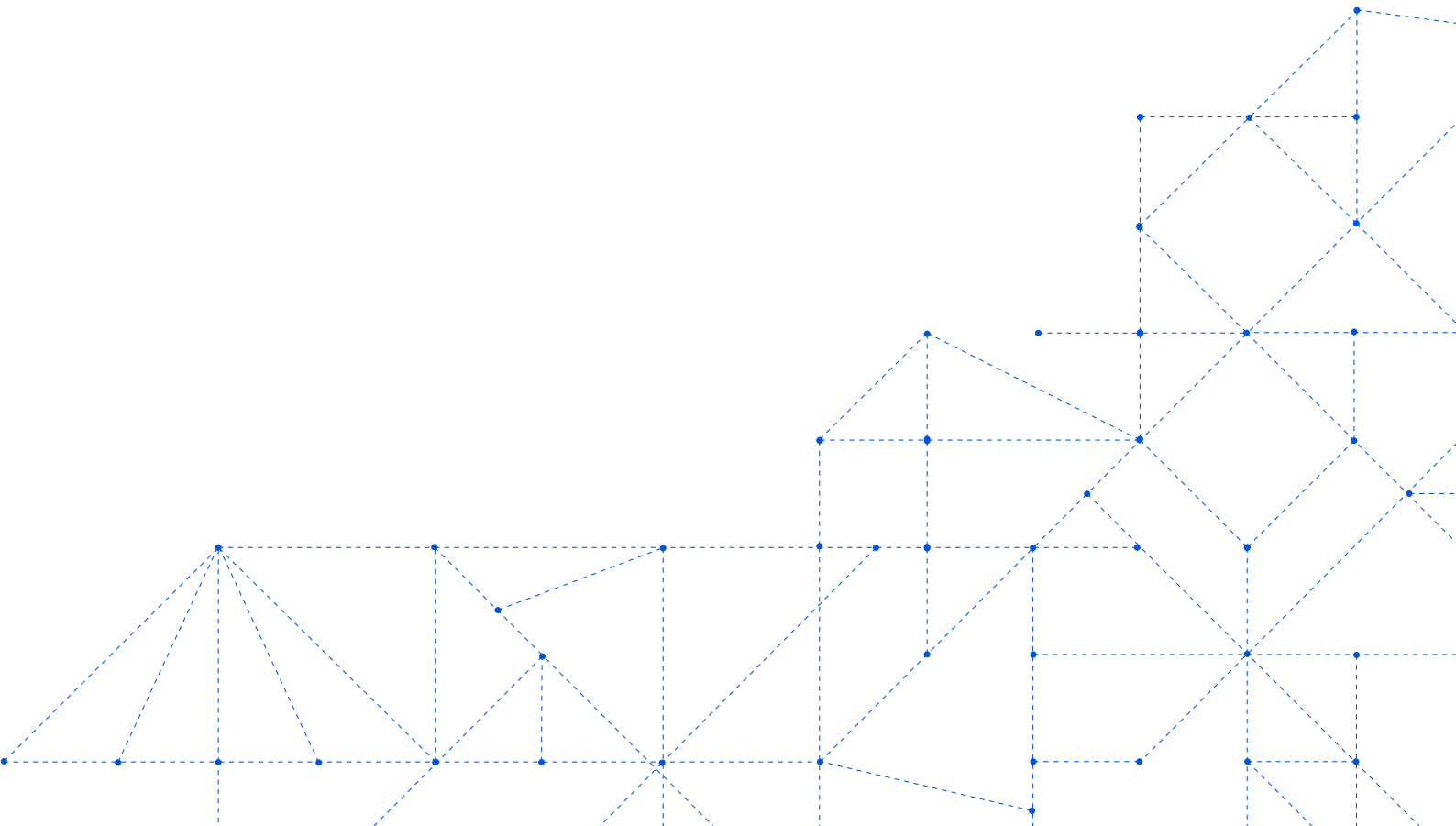
组织如何加速网络转型，而不必等待硬件送达，也不必投入更多资金采购只能使用几年的设备？
使用 Cloudflare。

Cloudflare 建设了一个提供广泛服务的全球云平台，帮助企业增强安全性，提高应用程序的性能，并消除管理单个网络硬件的成本与复杂性。这个平台充当一个可扩展、易于使用的统一控制面，为本地、混合、云和软件即服务 (SaaS) 应用程序提供极佳的安全、性能和可靠性。

至关重要的是，在 Cloudflare 覆盖 270 多个城市的全球网络中，每个数据中心都能提供这些服务中的每一项，减少了使云实施复杂化的延迟。简化您的网络堆栈，加速转型，并让您的网络做好应对未来的准备。

如需进一步了解，请访问：www.cloudflare.com。

> “Dropbox 最近成了‘虚拟优先’的公司。我们一直在探索这种业务战略会对我们的安全性方法和网络架构带来何种影响。Cloudflare 提供了大力支持，帮助我们和其他像我们这样的远程优先组织学习如何适应这种‘新常态’，对此我们深表感激。”
>
> Konstantin Sinichkin
> **Dropbox 工程经理**



010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3313.2022JUN10