后疫情时代，企业需要应对的三大网络挑战

作者：Kartika Prihadi，思科亚太区企业网络总经理

如今的工作场所已不同往昔，推动这一变革的除了员工预期，还有其他许多因素。麦肯锡公司的一项全球调查显示，十位企业高管中九位表示其组织计划在疫情后继续推行远程和现场相结合的混合办公模式。此外，这些高管大多承认，其员工的工作效率在疫情期间有所提升。

身为 IT 主管，您很可能已经开始积极接受这场变革，采取相应的行动来应对突如其来的远程办公热潮，并为安全复工做准备。

但是，随着突如其来的变革逐渐成为一种新常态，您应早做准备，从根本上重新评估您的工作场所、员工和业务活动赖以维系的物理和数字基础设施。考虑到这场变革的性质和规模，您在重新评估时也应该考虑到将企业的一切人和事物联系在一起的基础设施，那就是您的网络。

为了帮助 IT 主管进行这项评估，我们发布了一系列文章，为您分析如何通过升级企业网络来迎合后疫情时代的要求。首先，我们总结了您将面临的三大挑战。

连接挑战

事实上，在疫情发生前，大多数企业的网络就已经超越了传统办公室和分支机构网络的范畴。许多办公室员工都已改为使用适合移动办公的工作站，能够自由地随时随地办公。如今，有更多人加入了远程办公的行列，改为完全或部分时间在家办公。

另一方面，疫情加快了数字技术的普及速度。从快递员到现场医疗专业人员，越来越多的职业开始在越来越多的地点使用数字技术。从制造业到农业，各行各业都开始采用新型物联网 (IoT) 应用，致使连接到数字网络的设备也不断增加。

对 IT 主管而言，支持所有远程员工和设备轻松而可靠的连接到网络无疑是一大挑战。企业网络还必须满足用户对性能和带宽日益增长的需求。

线上会议（通常是从多个位置连接的高清视频会议）将成为一种常态，而其他远程应用（例如远程医疗和技术支持应用）也开始越来越多地使用视频和其他大量占用带宽的媒体。此外，远程员工和物联网设备需要通过低延迟网络即时访问各种云应用。

安全挑战

IT 主管面临的另一个重要挑战是针对不断增长的分布式员工保护业务数据，否则将招致比以往更严峻的后果。据研究机构 IBM-Ponemon Institute 的 *2021 年数据泄露的损失*报告显示，目前企业数据泄露事件的平均损失为 424 万美元，创下了自该报告诞生 17 年来的新高。

究其原因，与远程办公有极其密切的联系。平均而言，与远程办公相关的泄露事件造成的损失比其他泄露事件多 107 万美元。

另一方面，物联网和其他自动化应用带动机器间 (M2M) 连接与日俱增。思科预测，到 2023 年，M2M 设备将占到全球联网设备总数的一半，而这一数字在 2018 年时为三分之一。

想想就觉得可怕：一方面，您的组织的受攻击面不断扩大；另一方面，许多终端附近可能没有专人来提供保护。

网络管理挑战

在终端设备不断增加的同时，企业也在使用越来越多样的系统和应用来加快全数字化进程。使用多种云服务便是一个具体的表现：据 IDC 最近的*云脉动调查*显示，69% 的组织采用了多云战略。

但是，许多企业网络的规模和复杂性不断增加，达到了网络设计意图始料未及的程度。传统网络技术和拓扑在本质上无法满足当今企业的需求，因为现在的企业不仅拥有多个有线和无线局域网、广域网、分支机构、数据中心和云服务，还有不计其数的远程连接。

虽然许多企业对网络进行了现代化升级，但通常是为了解决燃眉之急，所以企业的网络和 IT 环境仍需独立管理。要对访问网络的人和设备以及用户体验的质量了如指掌，简直难如登天。同样难以做到的，还有检测和诊断异常与威胁，以及应用一致的策略。

全栈解决方案可以一举多得

要解决上述挑战，您可能需要针对后疫情时代的特点重新设计企业网络。思科认为，实现这一目标的有效途径是采用着眼于整体的全栈策略来打造您的网络基础设施。

这种战略可以让您的组织:

- 打造全面覆盖的网络环境，让员工和设备自由地使用有线和无线网络随时随地轻松建立可靠的连接
- 通过持续的身份验证保护您的网络，确保只有授权用户和设备能够可靠地访问应用、服务和数据
- 借助人工智能 (AI) 和机器学习 (ML) 自动执行网络管理和协调任务，并通过分析整个网络中的设备、用户和应用活动获得端到端可视性和洞察力。

我们会发布更多内容，进一步探讨如何重构企业网络。从混合办公模式下的连接和互动，到构建新的网络运维模型，精彩内容陆续更新。

要深入了解思科如何帮助您重新构想企业网络，请参阅由 Cisco DNA 软件支持的 Catalyst 全栈解决方案简介。