



The bridge to possible



2021 全球网络趋势报告

业务弹性专题研究: 解析在困难时期有助实现灵活性和弹性的五大技术趋势

目录

序言 - 业务弹性 3

网络技术的五大发展趋势 5

1. 员工 - 远程、安全 7

2. 工作场所 - 安全、可靠 9

3. 工作负载 - 多云 11

4. 运维 - 自动化 13

5. 运维 - AI 支持 15

结语 18



序言 - 业务弹性

序言: 从业务连续性到业务弹性

席卷全球的新冠疫情给人们的工作和生活带来了翻天覆地的变化。无论是对企业还是对个人来说，其影响范围之广、持续时间之长都是始料未及的。就在一夜之间，所有上班族都开始远程办公。一些企业尽其所能将产品和服务搬到线上，也有一些企业摒弃了原有的战略性供应链，转而采用新供应商和新地理布局。

可以想见，新冠疫情给每一个国家、地区、城市和组织敲响了警钟。但这带来了什么变化呢？要知道，许多企业都经历过大风大浪。过去五年里，70% 的组织曾至少一次陷入重大危机，95% 的组织确信他们今后还会遇到重大危机。¹



过去五年里，70% 的组织曾至少一次陷入重大危机。

来源：“普华永道：2019 全球危机调查”

人为原因造成的业务中断（如网络攻击、法规要求和社会动荡）变得越来越常见。与此同时，全球因飓风、森林火灾、洪水等自然灾害造成的业务中断也日益增多，而且这类业务中断事件可能会定期发生。

要顺利度过今后可能发生的业务中断事件，IT 主管必须转换思路。具体而言，就是摒弃传统业务连续性战略所依赖的被动式规范化方法，将侧重点转移到 IT 敏捷性上，建立业务弹性。二者的最大区别在于，业务弹性战略可以让组织做到未雨绸缪，对各种意外事件做好准备。



¹ 普华永道，“PwC's Global Crisis Survey 2019”（普华永道 2019 全球危机调查）。

业务连续性与业务弹性

业务连续性：发生业务中断事件后，组织继续以最初订立的验收标准提供产品或服务的能力。*

业务弹性：组织通过掌握和适应环境变化，持续实现目标、平稳度过危机并实现茁壮成长的能力。**

* 国际标准化组织，“Security and Resilience – Vocabulary”（安全性和弹性 – 术语），ISO 22300-2018

** 国际标准化组织，“Security and resilience – Organizational resilience – Principles and attributes”（安全性和弹性 – 组织弹性 – 原则和属性），ISO 22316-2017



图 1. 从业务连续性到业务弹性

网络技术的五大发展趋势

网络: 有助打造业务弹性的五大发展趋势

如今，重要的业务流程往往依赖各种全数字化技术，这些技术日益丰富完善，为组织打造弹性战略提供了基础。



在用户和设备日益动态化、分散化的当下，应用和工作负载也变得越来越分工明确。网络可以作为单一平台，统一约束、保护并支持用户、设备、应用和工作负载，因此在组织打造弹性战略的过程中发挥着核心作用。

这也意味着单纯注重保障网络连接和正常运行时间的网络弹性战略已无法再满足当前需求。企业需要利用具备以下能力的高级网络平台建立更高层次的弹性战略：迅速对任何情况做出响应；支持新型业务模式和服务；与 IT 流程集成；保护员工、核心业务活动、客户和品牌。事实上，这与支持全数字化转型所需的高级网络不谋而合。

业务连续性与业务弹性

网络弹性：特定电信网络在遇到影响正常运营的故障或困难时，利用事先准备的设施满足并维持可接受服务级别的能力。*

业务弹性网络：专门设计的网络，旨在确保组织能够快速、安全、有效地应对计划内和计划外的业务中断事件。

* 国际电信联盟，“Requirements for Network Resilience and Recovery”（网络弹性和恢复能力要求）。



面向员工、工作场所、工作负载和运维打造灵活性和弹性

为了帮助网络主管有的放矢地思考如何支持组织的弹性战略，我们将重点探讨五个趋势。这五大趋势都有助于提升组织在以下 4 个主要领域的弹性：员工、工作场所、工作负载和 IT 运维。

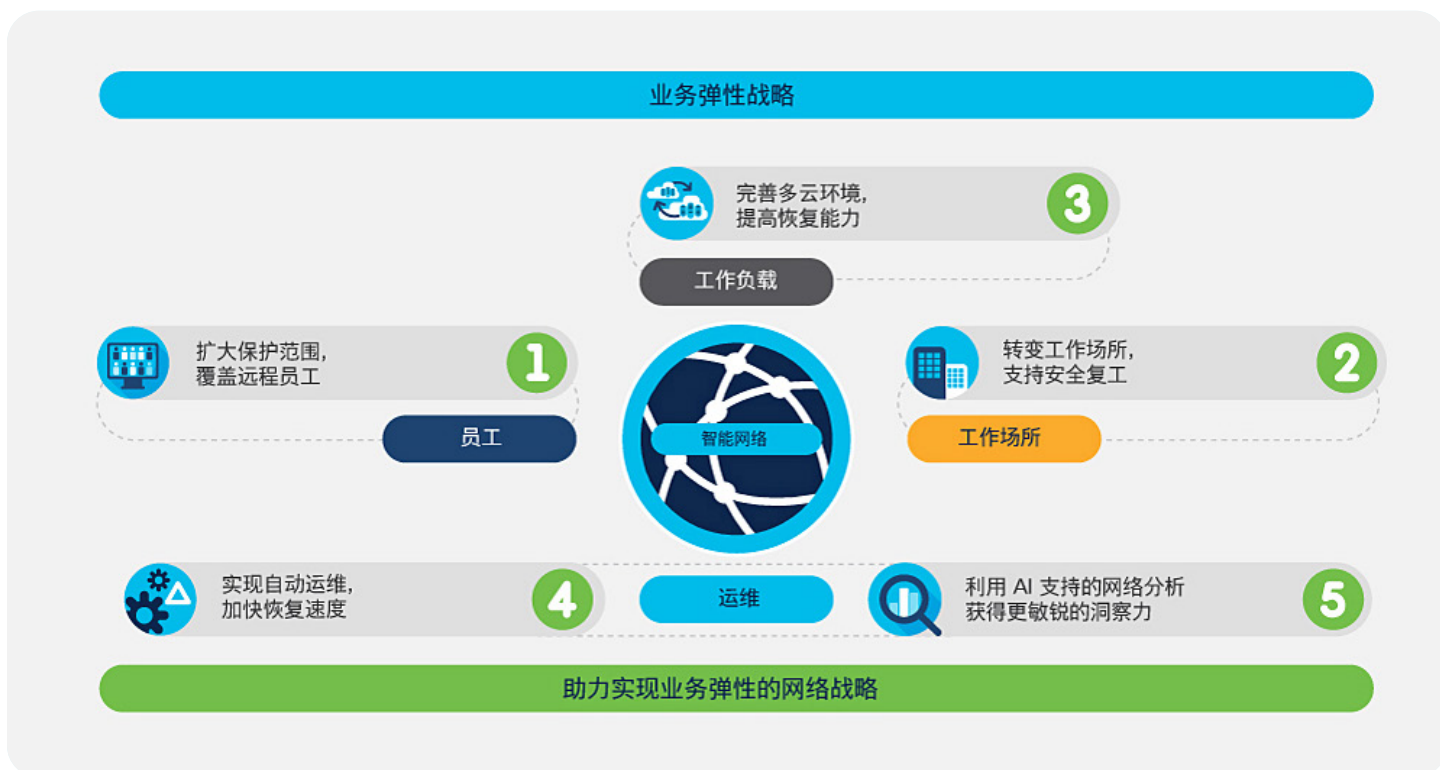
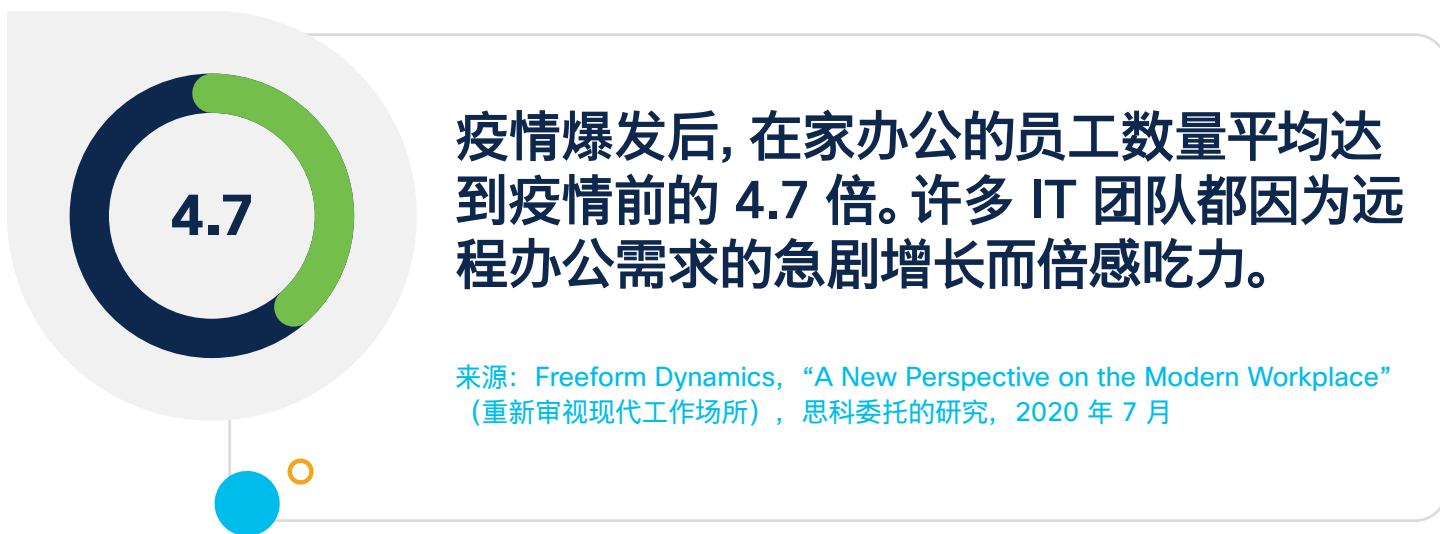


图 2. 有助提升员工、工作场所、工作负载和运维弹性的网络基础

员工 - 远程、安全

趋势 1: 员工 - 扩大保护范围, 覆盖远程员工

大多数组织已经意识到, 为员工提供更加灵活的全新工作方式将成为新常态。

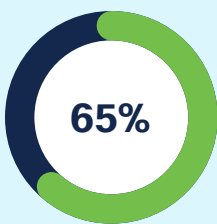


为此, IT 将面临一系列新的业务要求

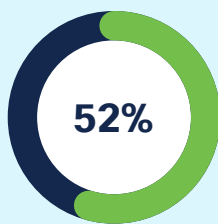
- 赋能员工, 确保他们随时随地都能高效工作并开展协作
- 针对每一名员工优化 IT 性能、成本和安全性
- 将企业级 IT 运维和管理工作延伸到在家办公的员工

但是, 满足这些要求并不是一件轻松的事。尤其是远程员工安全性和终端用户行为, 一直是大多数 IT 组织持续关注但很难解决的问题。

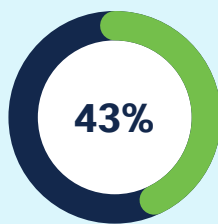
IT 支持远程办公面临的 4 大挑战:



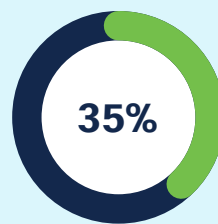
安全性 (65%)



终端用户行为 (52%)



应用性能 (43%)



IT 运维 (35%)²

² “2020 Cisco Business Resilience Networking Survey” (2020 思科业务弹性网络调查)。

远程员工在使用个人设备和私人网络访问企业应用和数据时，特别容易遭到网络安全攻击。许多员工会绕过 VPN 并直接访问公共云中的服务和应用，这一直是网络防御的最薄弱环节。³

网络设计注意事项：要大规模保护在家办公的员工，IT 团队应考虑采用以下部分或所有策略：

- **扩展 VPN，保护远程员工：**要让企业级控制和保护更广泛地覆盖到远程员工，使用企业 VPNs 不失为一种快捷高效的途径。
- **使用多因素身份验证 (MFA) 保护应用：**MFA 会要求用户验明身份，才允许他们访问组织网络或敏感的应用和数据，是保护组织的重要武器。
- **部署安全访问服务边缘 (SASE)，保护多云访问：**基于云的安全功能和 SASE 可帮助防御基于互联网的威胁，而且不受连接、用户设备和云环境限制。

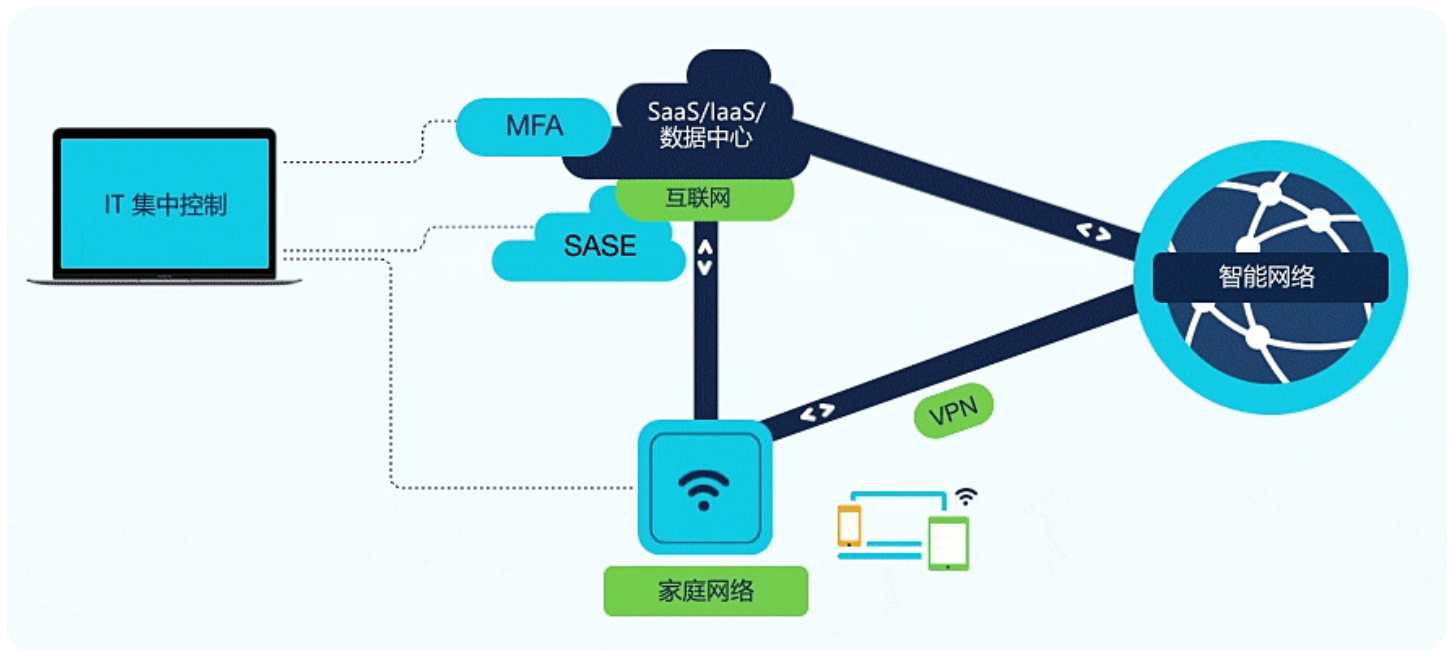


图 3. 结合使用 VPN、MFA 和 SASE 保护远程员工

深入了解如何支持和保护远程员工

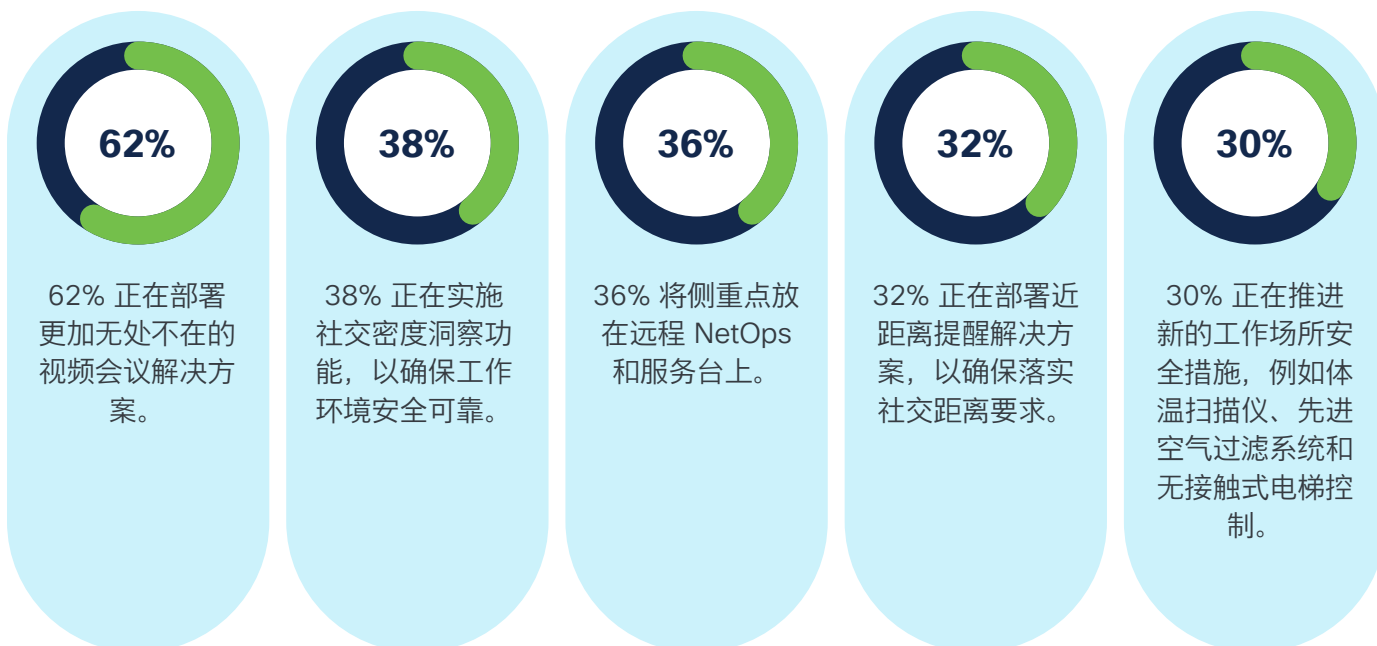
³ Cisco Umbrella, “2019 Cybersecurity Trends” (2019 网络安全趋势)。

工作场所 - 安全、可靠

趋势 2: 工作场所 - 转变工作场所, 支持安全复工

尽管还有很多问题尚待解决, 但毫无疑问, 随着新冠疫情持续蔓延, 员工和工作场所也会不断演变。不计其数的企业正在扩大视频会议和基于位置的 Wi-Fi 等现有服务的部署规模。也有一些企业开始着手部署新型服务和保护措施, 例如社交距离监控、近距离提醒、办公场所自动化, 乃至辅助员工工作交流的机器人。

网络团队如何为安全复工提供支持



来源: “2020 Cisco Business Resilience Networking Survey” (2020 思科业务弹性网络调查)。



网络设计注意事项：要让员工安全顺畅地重返办公室工作，敏捷的现代化网络是关键。

- **对网络进行压力测试：**在很多情况下，网络会连续数周运转失常。不要想当然地认为网络能一直为员工提供所需的有线和无线服务。
- **实现自动化的基于身份的安全访问：**无论访问组织网络及服务的用户和设备使用的是本地连接、家庭连接，还是公共网络，组织都应以一致的方式对用户和设备进行管理、保护和分段。
- **借助基于位置的分析提高员工和客户的安全感：**组织应使用现有 Wi-Fi 网络来支持工作场所监控、预警和洞察技术，以保护员工、合作伙伴、访客和客户的健康与安全

深入了解如何打造安全的工作场所

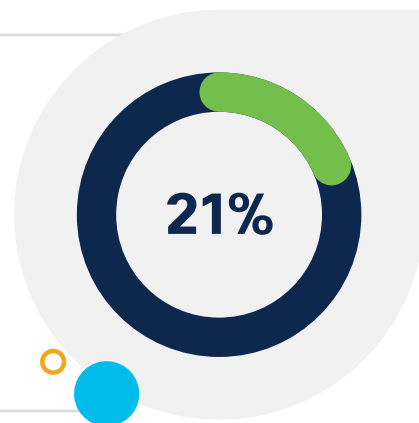
工作负载 - 多云

趋势 3: 工作负载 - 完善多云环境, 提高恢复能力

全球疫情爆发后, 许多 IT 主管都将云服务作为提高业务弹性的手段。越来越多的组织开始采用多云模式来降低成本, 提高灵活性, 并预防和分散灾难性故障带来的风险。多云模式是指将应用、工作负载和数据分布在多个本地数据中心和公共云中。

“受疫情相关的资本支出影响, 21% 的组织正在将更多工作负载迁移到公共云。”

来源: IDC, “COVID-19 Impact Survey, Wave 5” (第 5 次新冠疫情影响调查), 2020 年



网络设计注意事项: 要确保用户和 DevOps 团队获得始终如一的经验, 组织需要采用具有前瞻性的多云网络战略, 确保网络设计与云、安全和 IT 运维方面的优先事项保持一致。

多云网络战略能否成功取决于三个主要因素:

- **工作负载:** 针对跨本地数据中心、多种分散的云和其他**计算**环境分布的工作负载和服务, 采用云操作模型来简化策略实施、保护和管理工作。
- **访问:** 采用 **SD-WAN** 和 **SASE** 模型来确保企业网络和公共网络中的用户和设备无论位于何处 (园区、分支机构、家中或路上), 都能始终如一地安全访问多云环境 (包括 **SaaS**)。
- **安全:** 降低因用户、设备和应用分布在多个云或其他计算环境中而造成的风险。



图 4. 多云网络：工作负载、访问和安全

深入了解如何制定安全、高效的多云网络战略

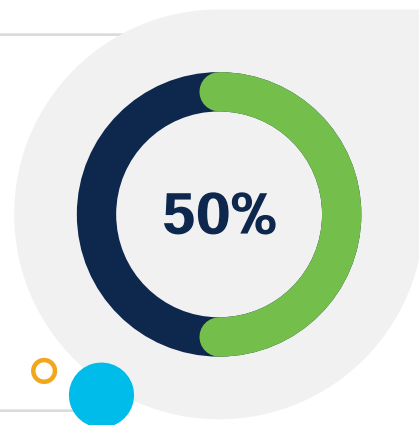
运维 - 自动化

趋势 4: 运维 - 实现自动运维, 加快恢复速度

异地分布的远程员工数量呈爆炸性增长仅仅是导致当今 NetOps 团队压力陡增的原因之一。在新冠疫情的影响下, 客户端数量、应用流量模式, 以及对新使用案例 (例如线上学习、视频会议、虚拟大型活动、远程医疗、流程自动化和其他依赖网络的服务) 的需求都出现了井喷式增长, 让本已严峻的形势雪上加霜。

为了解决燃眉之急, 摆脱业务中断, 50% 的组织将网络自动化提上日程。

来源: 2020 思科业务弹性网络调查



因此, 不难理解为什么有一半的网络专业人士将网络自动化视为摆脱业务中断, 维持服务和运营正常运转的关键所在。

来源: 思科, 2020 全球网络趋势报告

网络设计注意事项: NetOps 团队可以逐步采取以下措施来不断优化网络环境, 并快速应对日益增加的业务中断风险和网络安全威胁:

- 将重复性的管理任务自动化, 例如网络调配、配置和映像管理。这有助于减轻管理负担, 并加强各个网域的合规性。
- 实现网络接入、自行激活和网络分段的全面自动化, 分组保护分散的用户和事物, 阻止网络安全攻击蔓延。
- 在企业数据中心推进网络策略自动化, 借助基于应用的分段技术保护应用和数据, 并对工作负载加以跟踪。
- 将策略自动化从数据中心扩展到云端, 借助云操作模型跨本地和混合云环境实施一致的应用策略。
- 实现基于策略的自动化端到端多域分段, 针对包括用户、事物和工作负载在内的所有对象建立一致的端到端零信任访问模式。

35% 的组织计划在 2022 年以前打造覆盖所有域的基于意图的网络，这一数字在 2019 年仅为 4%。

来源：思科，2020 全球网络趋势报告

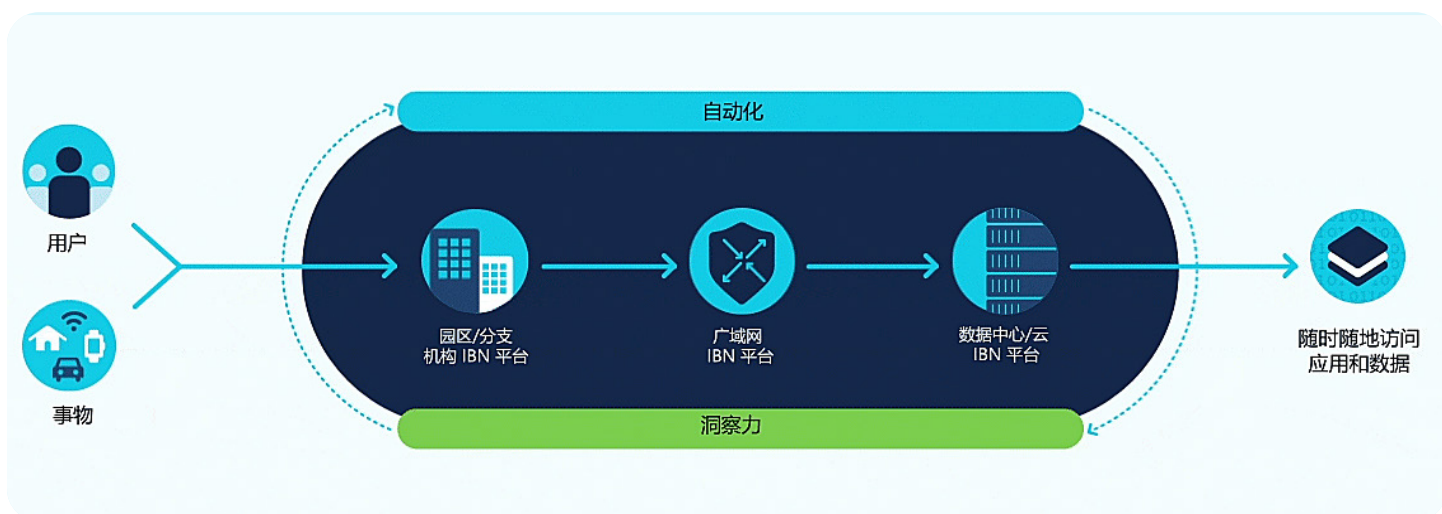
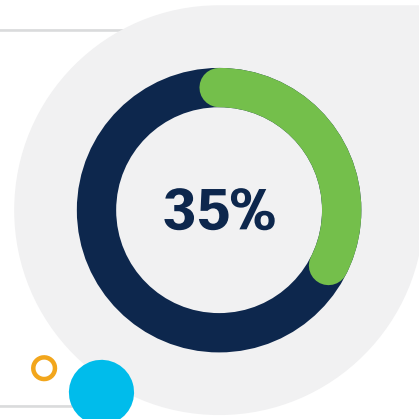


图 5. 从员工到工作负载，实现无处不在的自动化和洞察

深入了解如何跨多个网域实现策略自动化

运维 - AI 支持

趋势 5: 运维 - 利用 AI 支持的网络分析获得更敏锐的洞察力

无论是规模庞大、纷繁复杂的现代网络，还是由多种独立式监控平台发出的海量事件和问题警报，在管理上都十分困难而耗时，在发生网络中断事件时更是如此。

4,400 - 每个企业网络中每月出现的无线网络相关事件的平均数量。*

来源：思科遥测数据：Cisco DNA Center, 2020 年

4400

* 基于超过 600 个企业网络的遥测数据。事件包括自行激活失败/超时、无线吞吐量问题和 DHCP 响应超时/失败。事件数量为采用 AI 支持的动态基准技术减少后的数量。

显然，NetOps 团队需要借助高级分析技术，才能及时作出明智的补救决策。

诸如 AI 支持的网络分析和机器学习技术，都可以帮助 NetOps 团队有效解决更多问题。

260万

Cisco AI Network Analytics 是 Cisco DNA Center 中提供的一款全球适用的应用，可将每月 260 万个“事件”解析为 15,080 个可供解决的“问题”，使警报数量减少了 99.4%! *

来源：思科遥测数据：Cisco DNA Center, 2020 年

* 基于全球 700 多个企业网络的遥测数据。

通过大幅减少警报数量，NetOps 团队可以专注于真正重要的事情，并集中精力处理可能给业务带来不利影响的问题。

更重要的是，安全问题已不再局限于企业网络内部。如今，大多数网络事务都始于或止于传统企业网络外部，因此 NetOps 团队也必须对组织网络所连接的公共网络了如指掌，并能对其进行分析。在类似当前疫情这样的非常时期，这种能力尤为重要。

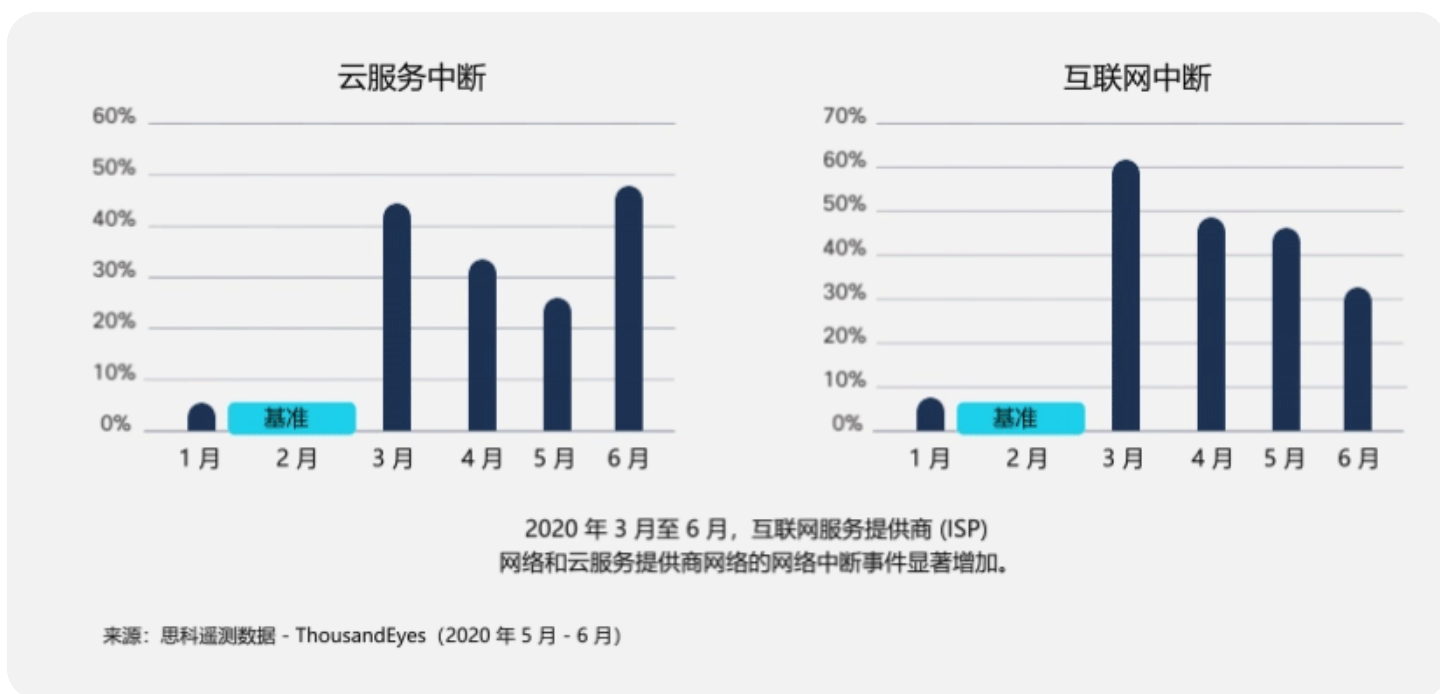


图 6. 疫情期间，云和互联网服务中断事件的增长情况

Cisco ThousandEyes 发现，在 2020 年 2 月至 3 月的一个个月内，互联网服务提供商 (ISP) 网络的网络中断事件增加了 61%，云服务提供商网络的网络中断事件增加了 44%。

来源：Cisco ThousandEyes, “Internet Performance Report: COVID-19 Impact Edition” (互联网性能报告：新冠疫情的影响专题报告)，2020 年

61%



网络设计注意事项: 要从海量警报中理清头绪, NetOps 团队需要借助 AI 支持的网络分析和网络状态感知系统来实现以下目标:

- **提高检测精度:** 在同一网域内和不同网域间提高问题和异常检测的精准度。
- **加快补救速度:** 关联不同事件, 以探查并明确描述最有可能造成相关问题和异常的根本原因。
- **实现自动化策略管理:** 识别设备、应用和趋势, 并提供策略更新建议。
- **减少服务降级:** 识别模式和趋势并提供基于情景的洞察力, 帮助尽快开展预防措施、纠正措施和保护措施。
- **分享同行情报:** 提供情报和分析数据, 使网络管理员能够对比全球、行业和地区基准评估自身网络的性能。

深入了解如何利用基于 AI 的洞察力更好地管理您的网络:

面向数据中心的网络洞察

结语

结论: 借助高级网络平台提高业务弹性

只要我们从事这个行业, 就难免会遇到影响业务的网络中断事件。我们应该趁现在行动起来, 重新思考如何将网络战略与业务弹性战略相接轨, 并确定最迫切需要的新型网络功能, 以便从容应对下一次重大事件。

基于意图的网络提供的自动化功能和基于 AI 的洞察力可以作为您的有力武器, 让您游刃有余地应对任何情况。这些技术可以为您提供所需的敏捷性、安全性、洞察力和行动力, 围绕以下 4 个方面打造弹性战略:

- **员工:** 赋能员工, 确保他们无论在家中、在办公室, 还是在路途中, 都能安全访问所需应用, 并畅享企业级性能
- **工作场所:** 借助 Wi-Fi 支持的监控、预警和洞察技术, 支持员工安全复工
- **工作负载:** 推行多云弹性模式, 确保无论工作负载位于公共云还是本地数据中心, 都能为数据和应用提供保护
- **运维:** 部署自动化端到端网络策略和分段解决方案, 帮助简化管理任务、提高可视性、减少警报数量并加快补救速度

在当前的新常态下, 拥有一个能够灵活调整、无往不利的网络至关重要。在思考业务弹性战略时, 请仔细考虑如何让网络在您的战略中发挥关键作用。

深入了解业务弹性

相关推荐

业务弹性

网络研讨会

思科全数字化网络架构 (Cisco DNA)