23.教主解读2020全球网络趋势报告

教主技术进化论

翻越下一座技术的高峰

主讲人：*现任明教教主*

PPT制作：*现任明教教主*

内容简介

1. 总览
2. 五大新型技术一: 自动化
3. 五大新型技术二: AI保障
4. 五大新型技术三: 多云环境
5. 五大新型技术四: 网络接入与无线
6. 五大新型技术五: 不断改变的网络安全角色

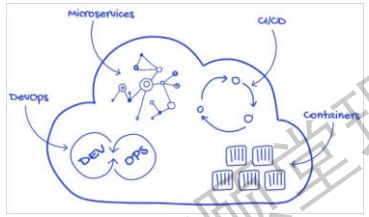
第一部分

总览

业务与技术趋势

云原生模型

https://www.infoq.cn/article/WR3YLpZ-X64AeWicO920



要点

趋势衍生出技术

- 全球化、数字化转型、业务自动化和弹性，以及可持续性等趋势正在塑造着对于新型网络的需求。
- 不断发展的技术领域——新兴的云原生模型、物联网、人工智能（AI）、手机、网络安全威胁，及沉浸式应用程序——都对打网络的架构和运营带来了显著的影响。
- 这些需求的规模、复杂性和动态性几近超出人类操作者的应对能力。

人类解决不了所以需要自动化

- 新型网络正通过人工智能（AI）、机器学习及自动化等新兴技术简化和保障运营，实现快速适应性，并提高人类的决策能力。

催生新型网络的全球业务和技术趋势

7亿	50%	146亿	42%	53%	12倍
到2021年的边缘托管容器数量[1]	到2021年，企业数据中心之外的工作负载占比[2]	到2022年，物联网（IoT）设备数量[3]	2017至2022年，业务移动流量每年增加量[3]	导致超过50万美元损失的网络安全攻击占比[4]	到2022年，增强现实（AR）/虚拟现实（VR）使用量增长[3]
容器技术	多云	物联网	5G与WIFI6	网络安全	AR/VR

高层前瞻

多种网络类型的整合

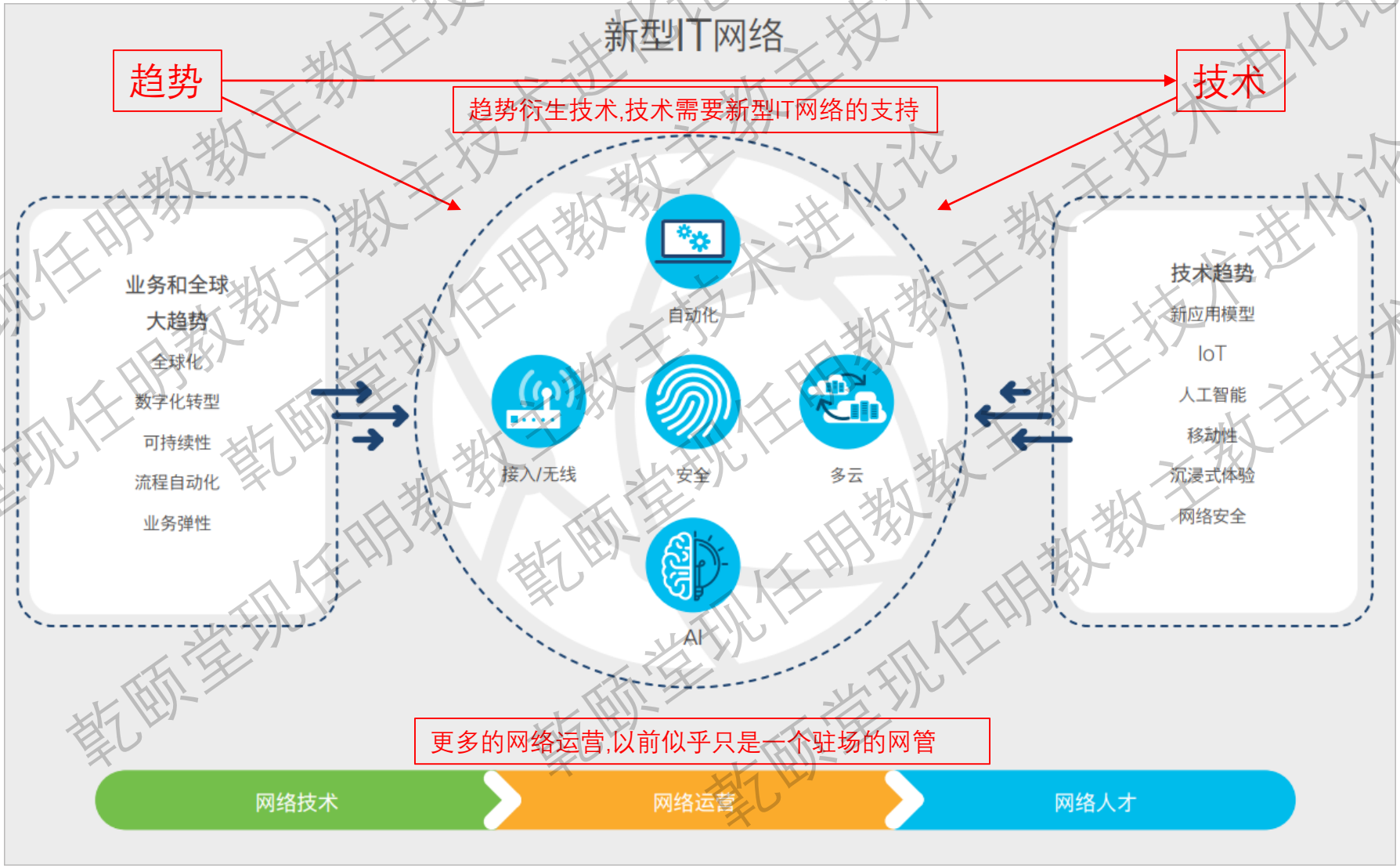
网络自动化

基于意图的网络

“到2025年，领先的网络团队将跨域（园区、分支机构、WAN、数据中心、云、服务提供商和安全等）运行基于意图的网络。他们的网络将能够理解业务和应用的需求，并将这些需求转化为网络和安全策略。藉由网络的智能自动化，其灵活性会得到显著提高，网络将以强大的反馈环运行，提供持续的监控、保障和优化。基于意图的网络将确保不间断提供业务服务并进行保护。这些进步将为企业乃至整个社会带来巨大益处。”

——思科企业网络首席技术官（CTO）
John Apostolopoulos

新型IT网络



容器,云与边缘计算1

应用程序和数据正迁离本地：应用程序和数据正被模块化为微服务，并移至多个公共云。在某些情况下，它们也被分发到网络边界，且被多个软件即服务 (SaaS) 提供商越来越多地使用。

容器云与边缘计算

应用程序是模块化的，并跨多个环境分布：在很多情况下，整体式应用程序正在分解为相互连接的微服务，并通过跨整个企业的一系列虚拟和物理工作负载 (包括容器) 交付。

物理-虚拟-容器-无服务器

应用程序得到持续高速构建：对于在内部开发和托管的应用程序，IT必需加速自身基础设施服务的创建和交付，以满足应用程序和用户的需求，同时控制运营成本。

应用程序正从物理向虚拟，再向容器和无服务器迁移：容器的兴起将应用程序的设计和部署模式置于更颠覆性的技术，即无服务器架构，该架构正迫使企业重新审视构建应用程序的方式、基础设施的作用，以及运营流程的设计。

据Uptime Institute估计，到2021年，所有工作负载的一半会在企业数据中心之外的云和数据中心基础设施内或网络边缘运行。[2]

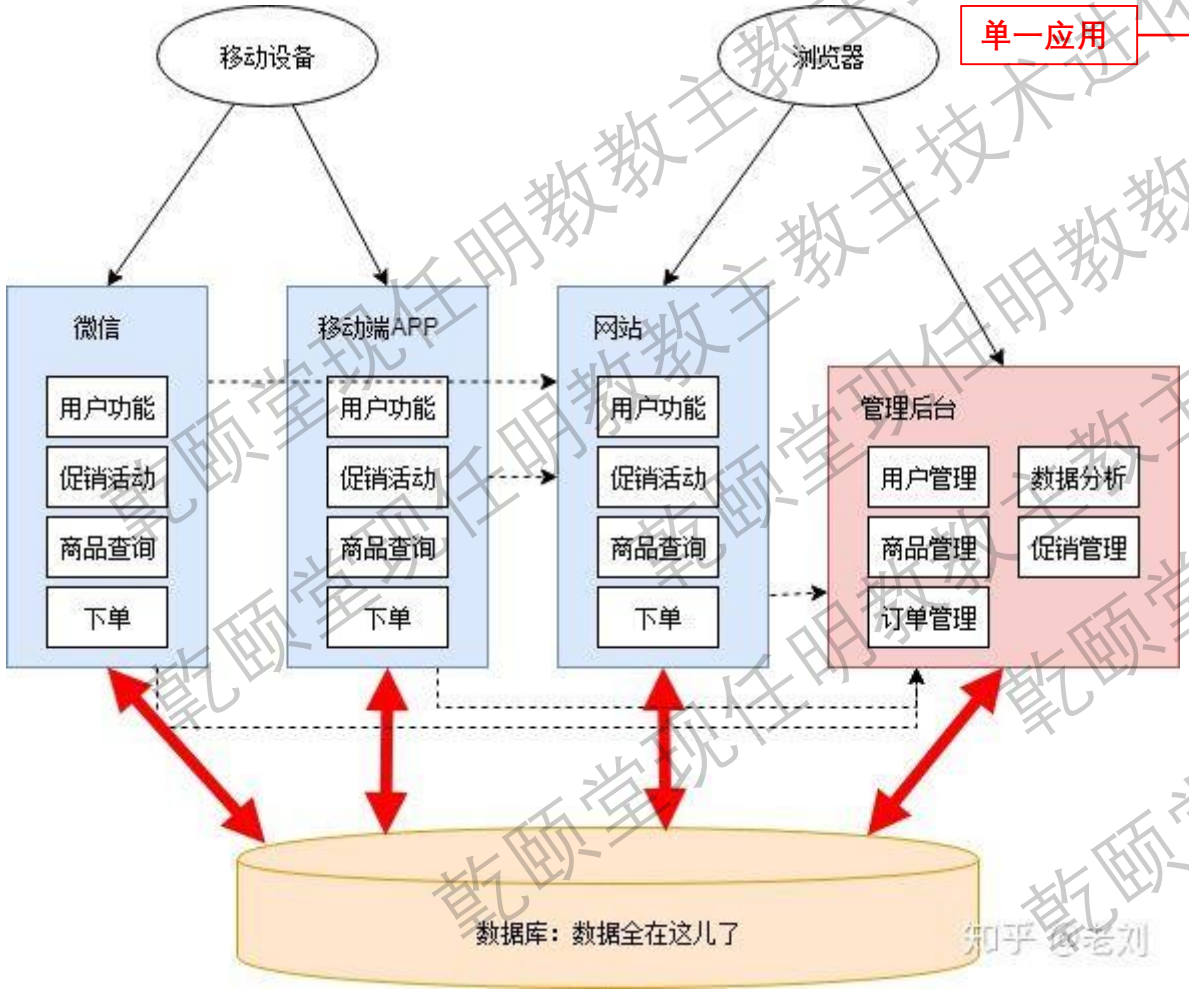
容器,云与边缘计算2

据估计，到2021年，已安装和正在使用的容器将超过35亿，其中20%以上运行在分布式位置，服务于边缘和物联网工作负载。[1]

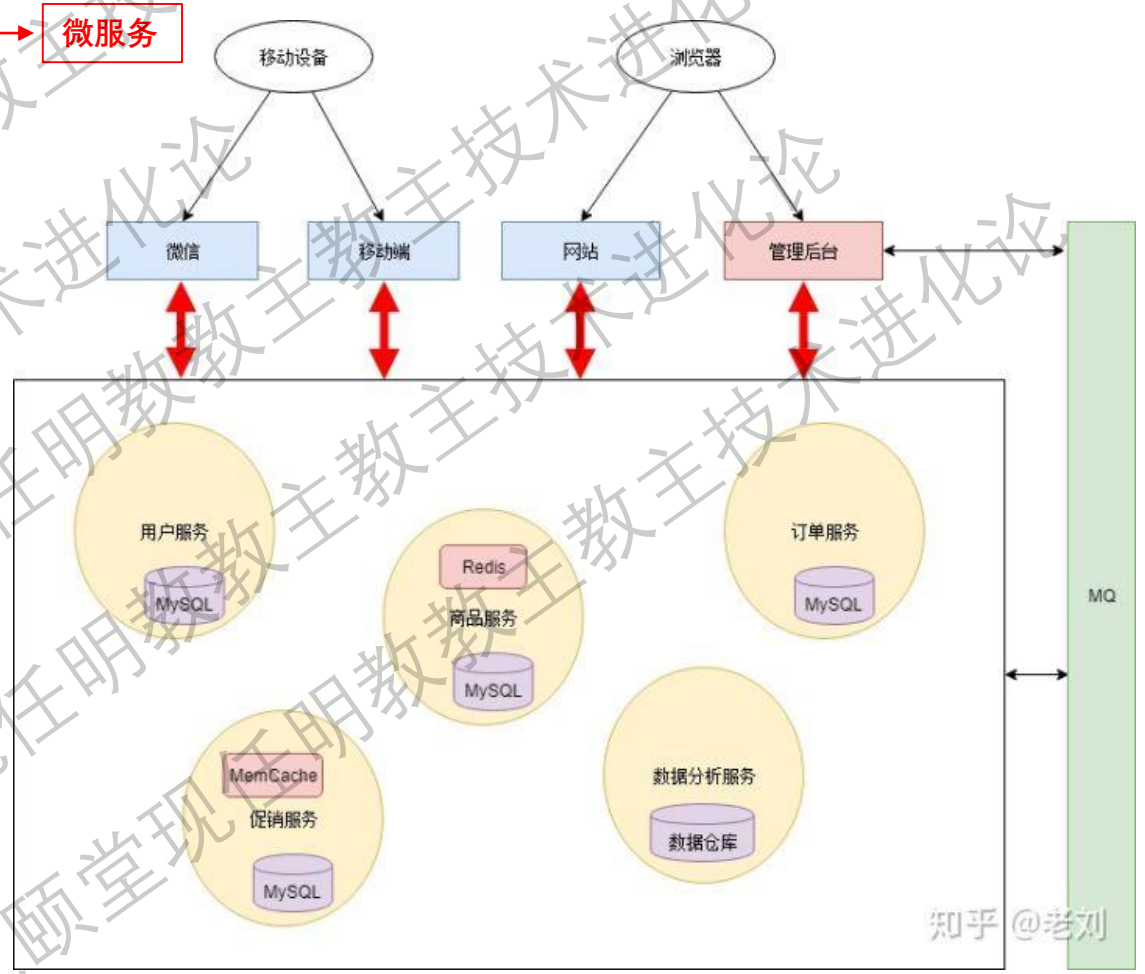
网络影响力

随着应用程序和微服务在所有领域如雨后春笋般涌现，更应将网络视为一组正在生长的互连“神经簇”，它们位于数据所在的位置，并可出现在边缘云统一体的任何位置。新型网络需能够稳固地连接在这些互连的“神经簇”之内和之间，并对这些新应用模型的工作方式有基本的了解，同时将整个网络的应用程序政策动态地扩展到托管应用程序的任何地方。

微服务



单一应用 → 微服务



物联网

物联网

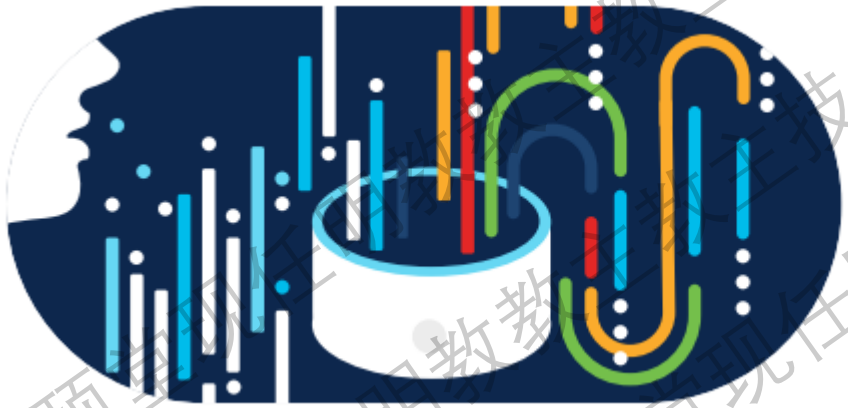
物联网设备、应用程序及相关数据的爆炸式使用正推动新型分布式计算机模型的建立，这些模型的规模和复杂性都呈指数级增长。据思科“VNI Forecast Highlights Tool”，到2022年，机对机（M2M）设备将占全球所有联网设备的51%（146亿）。[12]

网络影响力

除为极其多样的物联网设备提供连通性和安全性外，网络管理员还需要找到可扩展的高效方式，自动识别、分类和应用策略，并对它们进行监控，确保功能正常，不会影响或损害在网络上运行的其他设备。

高速增长如何保障与管理

AI



AI

以AI驱动的应用程序（无论面向业务还是消费者）的出现正引领人们迈入一个互联、智能和自动化设备无处不在的全新世界。

网络影响力

要释放AI在业务中的全部潜力，需要在更靠近边缘的地方完成更多的计算处理和决策。AI处理和数据的布置包括云到内部数据中心，再到网络边缘，取决于其性能、容量、隐私性，甚至成本考虑。

高效的网络,云和边缘计算是AI的底层依托

移动性

移动性

据思科"VNI Forecast Highlights Tool"，从2017年到2022年，全球业务移动数据流量将增长六倍，年增长率为42%。[12] 业务移动用户仍期待通过Wi-Fi及公共4G和5G网络在任何地点、任何时间和任何设备上实现即时高性能连接。同时，无线物联网设备会越来越普遍地出现在我们生活的各个方面。

网络影响力

使用公司和个人设备访问云应用程序的员工如果离开网络，会导致缺乏可见性和控制力，这是网络和安全管理员未曾面临的情况。物联网设备的涌现在规模、不同的流量模式和安全性方面增加了对无线网络的要求。

物联网和公有云的大量使用,促使了移动流量的激增

安全

安全

网络安全威胁变得日益复杂和危险，受攻击面更为广泛，且不再包含在明确并受保护的边界内。尤其是随着工作负载的向外迁移，IT有失去可见性的危险。

网络影响力

尽管在识别和遏制威胁方面网络仍是强大的同盟，但网络和安全运营需要分享数据、集成工具和工作流，以最佳方式抗击数量及复杂性不断增加的攻击。另外，网络能将IT的触及范围扩展到云环境中，以帮助保护应用程序和数据——即便不在这些环境的直接控制之下。

云,物联网,移动网络给安全带来了巨大挑战

沉浸式体验

沉浸式体验

为提升合作、培训、生产效率和远程工作体验，视频的使用日渐增加，虚拟现实 (VR) 和增强现实 (AR) 技术也随之兴起，这些都对企业的网络提出更高的要求。

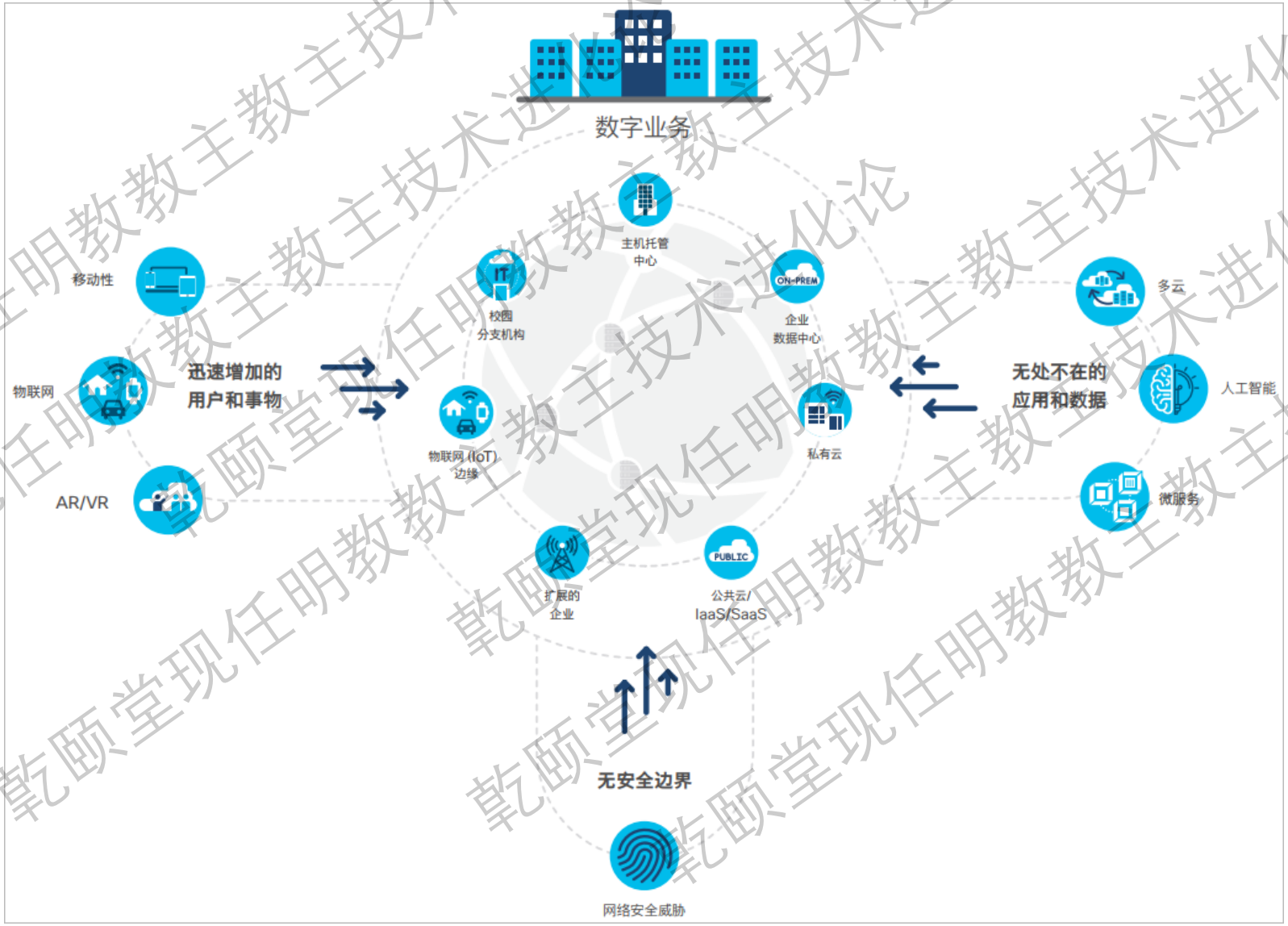
网络影响力

网络需要提供实现上述沉浸式体验所需的端到端宽带和低延时通信及动态性能控制。

网络需要保障带宽与延时

到2022年，互联网视频将占互联网全部业务流量的82%，VR/AR流量将增长12倍，互联网视频监视流量将增长7倍。[13]

驱动新型网络需求的技术



新型网络的四个基本目标

满足业务需求	简化复杂性	确保性能	降低风险
• 启动新的数字业务计划 • 动态满足快速变化的应用需求	• 简化IT运营，应对日益增长的需求 • 让IT能够集中资源创造业务价值	• 始终满足服务性能和用户体验要求 • 防止网络中断	• 在网络威胁造成损害前加以预防和遏制 • 满足合规和法规要求

新型网络实例

一家企业想使用无线IoT光学传感器为一项通过AR应用程序交付的新业务创新提供支持。以下为业务需求和意图如何被转化成网络行动的过程。

五级网络成熟度模型

催生新型网络的五大技术

第二部分

五大新型技术一:自动化

自动化的趋势

要点

- 软件定义网络（SDN）、基于意图的网络（IBN）、网络虚拟化、可编程性和开放平台网络控制器正在共同促进网络服务自动适应业务需求和IT流程的实现。
- IBN提高了SDN的自动化能力，使其能够将意图转化为策略、收集数据、提供可见性、纠正问题，并确保策略按意图如实执行。

大量的SDN

- IBN的目标是在整个网络中不断应用并保证服务性能要求、安全性及合规策略，以及IT运营流程。
- 开放平台控制器上的应用程序编程接口（API）允许控制器与相邻的网络及IT服务、其他IT域、业务应用和异构基础架构集成并交换智能。

API交换智能

关键调查结果

重大技术,自动化领先

- IT领导者认为，网络自动化（25%）、SDN（23%）和IBN（16%）是今后五年对网络影响最大的技术。
- 27%的IT领导者将接入、WAN、数据中心（DC）、云和安全域孤立的设计和运营方式视为他们适应先进网络技术的障碍。

网络技术需要整合

- 34%的IT领导者认为，与其他IT团队更好地进行网络协作和整合是改进的一个重要领域。

需要更好的协作

- 尽管当前仅4%的IT领导者和网络策略师认为他们的网络是基于意图的网络，但有35%计划在两年内将他们的网络改为基于意图的网络。

大规模网络自动化

网络自动化就是使网络中物理和虚拟设备的配置、管理、测试、部署和运营实现自动化的过程。为创建持续的服务增强，甚至网络自动化本身也可自动化。

据Gartner统计，“近70%的数据中心网络任务由人工完成，这不仅增加了用时、成本、出错几率，而且降低了灵活性。”[15]

人工操作,不仅费时,而且容易出错,并且费钱

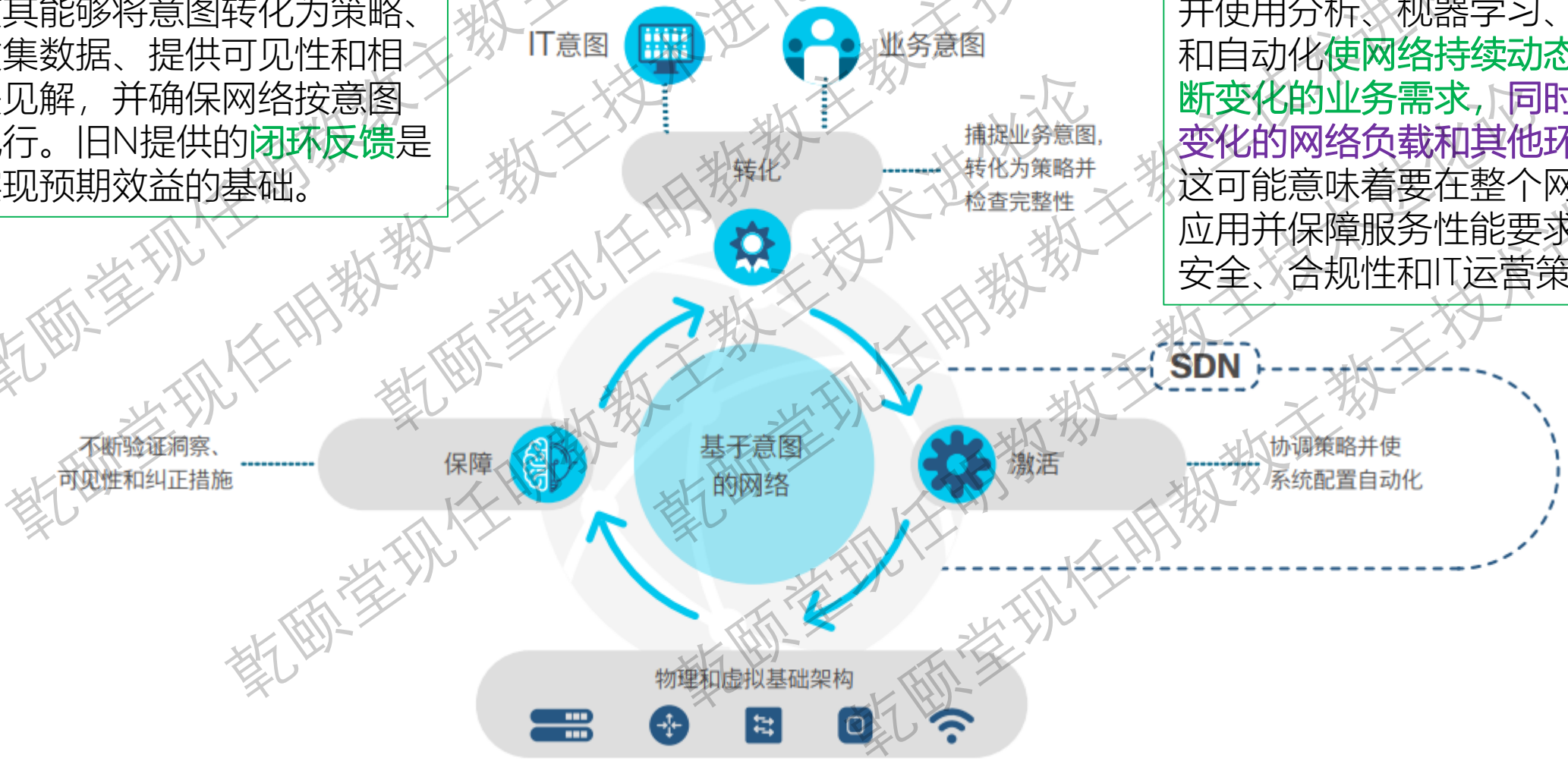
自动化可提高网络可用性，并将网络运营（NetOps）团队从耗时的日常任务中解脱出来，难怪当被问及未来五年哪些技术会对网络影响最大时，25%的IT领导者认为是网络自动化。[14]

如今，在SDN、基于意图的网络（IBN）、虚拟化、可编程性和开放平台控制器领域的创新正使网络自动化成为现实。

25%的IT领导者认为未来五年对网络影响最大的是自动化。[14]

基于意图的网络的构成

它提升了SDN的自动化能力，使其能够将意图转化为策略、收集数据、提供可见性和相关见解，并确保网络按意图执行。旧N提供的闭环反馈是实现预期效益的基础。



基于意图的网络可捕获业务的意图，并使用分析、视器学习、机器推理和自动化使网络持续动态地适应不断变化的业务需求，同时适应不断变化的网络负载和其他环境影响。这可能意味着要在整个网络中不断应用并保障服务性能要求及用户、安全、合规性和IT运营策略。

SDN与IBN

IDC的Rohit Mehra表示，“基于意图的网络是网络行业的重大进展。它不仅包含高级可见性、自动化和保障，而且是构建基于机器学习的新网络管理功能的平台。”[19]

开放平台IBN控制器:IT流程及业务整合

为采用更高效的自动化系统，IT团队要继续抛弃传统的基于命令行接口(CLI）的人工管理方式，而以数据模型驱动接口(DMI)取而代之。这些标准的基于模型的接口提供一致性、开放性、结构和效率。

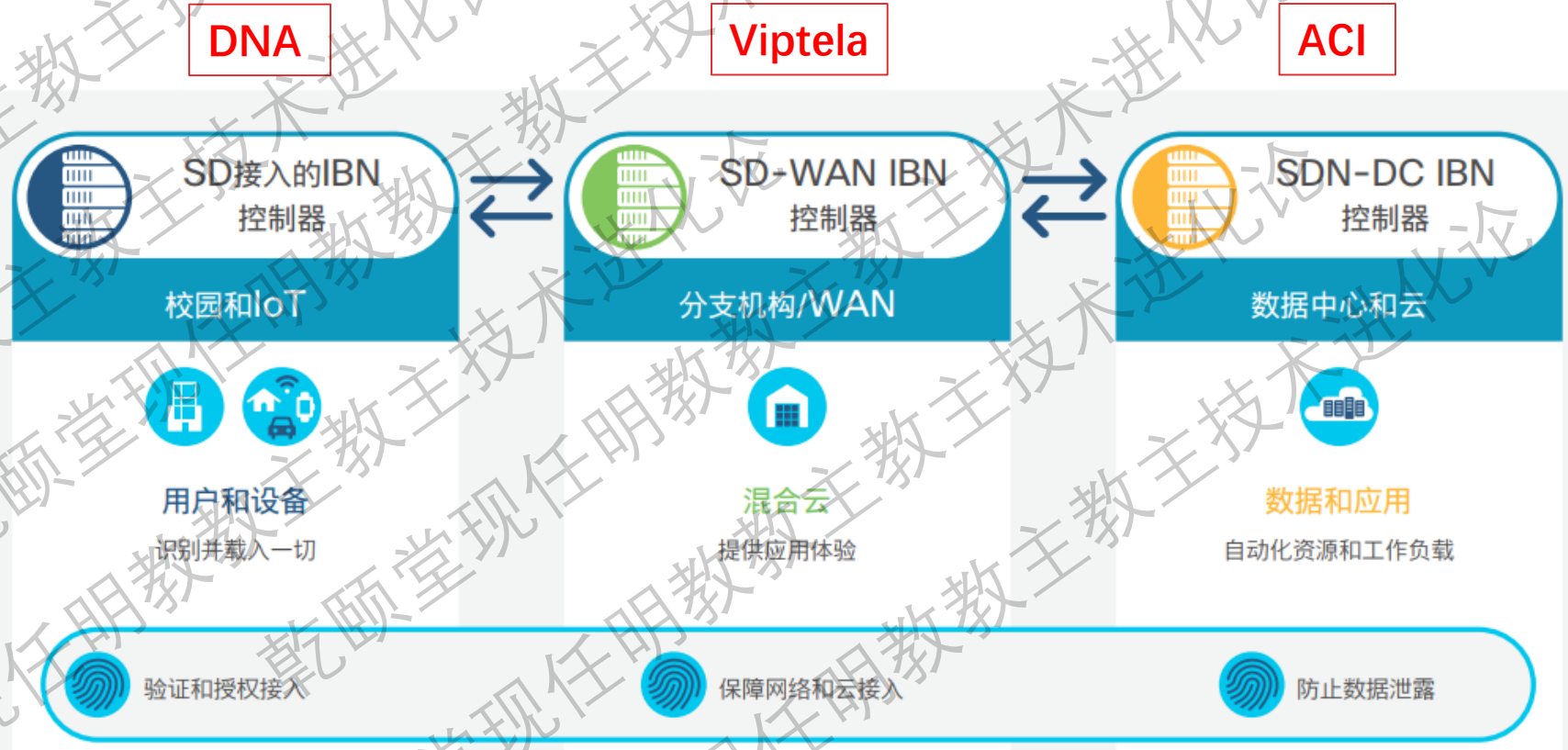
IETF标准模型（像YANG)提供了一套完整的北向编程接口，打造易于使用、性能一致的可持续运营模型。

该控制器上的应用程序编程接口(API)可使控制器将相邻网络及IT服务、其他IT域、业务应用程序和异构基础设施整合在一起并与之交换智能。

这将网络转变为开放的平台，该平台可接受来自应用程序和设备的策略规范，利用集中的跨域策略自动化，并确认系统是否满足业务需要。通过简化跨网络域工作流程、IT系统，以及用于独立管理的行业流程，改善了IT服务交付。

IBN的整合

现状分析: 要使企业成功地实施基于意图的网络,它需要在数据中心、园区、广域网和分支机构中完全实现自动化。[20]



第三部分

五大新型技术二:AI驱动保障

AI驱动保障摘要

要点

- 人工智能 (AI) 的使用对运营、服务交付和网络保障日趋重要。将AI能力与运营结合在一起的AIOps (智能运营) 正日渐完善。
- 流量、连接的移动和IoT设备、互联的应用程序和微服务，以及日益增加的安全威胁都呈爆炸性增长，这些让网络团队不堪重负。
- 由网络支持的数量激增的设备和服务所产生的海量数据、遥测和事件超出了人类操作员应对的能力。
- AI是基于意图的网络(IBN)模型的基础，它使用大量的网络源数据探索环境的复杂性，并动态地提出网络调整的建议。
- 机器学习和机器推理相互补充，应对复杂的事件处理，提供关联洞察和指导性补救。

AIOps

网络的剧烈变化与安全挑战让人类不堪重负

IBN,机器学习和机器推理也许是解药

关键调查结果

AI的趋势

- 超过50%的网络策略师将AI视为网络投资优先项。
- 仅17%的网络策略师认为AI技术的不成熟阻碍了网络现代化。
- 目前，仅22%的网络团队将AI用于网络保障，这可能是因为真正的AI驱动的工具的可用性仍为新概念所致。
- 72%的网络策略师计划在今后两年内采用AI驱动的预测性洞察或规范性补救。

重要指南

- 利用基于云的AI学习：在某些情况下，企业数据策略的变化需要利用云驱动的AI工具带来的益处。
- 人和AI联锁：渐进式定义AI在决策或采取行动方面走多远后需要人类操作员介入监控、批准或更改。
- AI知识：网络专业知识将成为确认AI是否按意图实现IT和业务目标所必需的重要技能。

拥有网络专业知识的人才,用于监控,审批和确认AI的操作

高层前瞻

高层前瞻

“到2025年，AI驱动的网络保障工具将使若干定义明确的特定任务很好地完全实现自动化。然而，大多数要求更灵活和更情境化决策的运营任务仍需要人类操作员的专业知识和介入。”

依然需要高端网络专业人才

– 思科研究员JP Vasseur

AI,ML和MR

简而言之，AI是一个研究领域，在执行任务时，它能赋予计算机如人类般的智能。**机器学习(ML)**和**机器推理(MR)**是AI最重要的两个门类。机器学习可描述为无需显式编程便可从数据中进行“统计学习"的能力，而机器推理则是使用已获得的知识浏览一系列可能的选项，直至找到最佳结果。

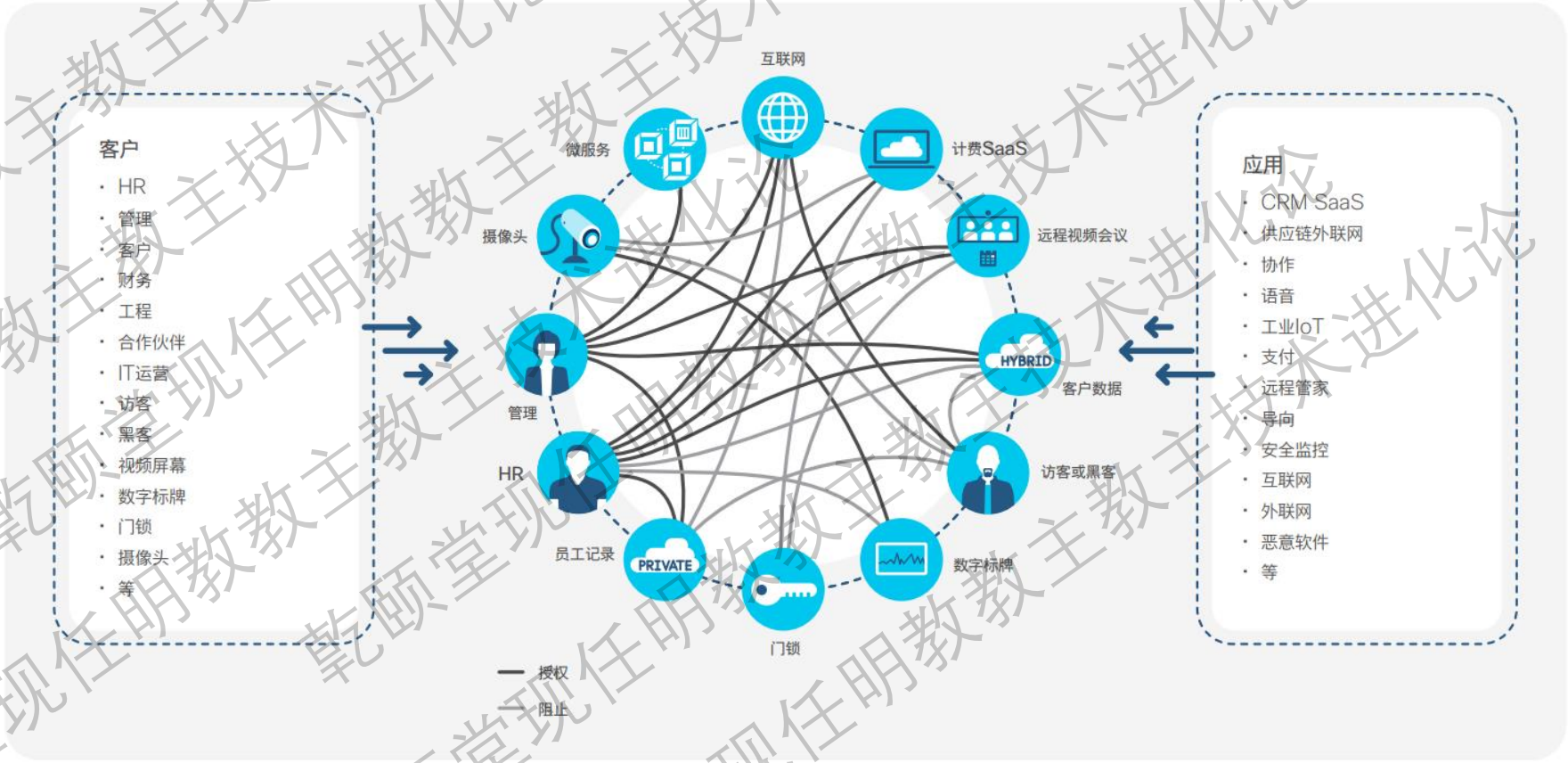
因此，ML能使系统审查数据并推断知识。它不再只是简单地学习或提取知识，而是随着时间的推移和经验的积累来利用和改进知识。从本质上说，ML的目标是**识别和利用那些隐藏在“训练"数据中的模式**。

MR很适于解决需要深厚专业知识的问题。为**让推理机能够对新数据进行操作**，人类需事先明确获取所有知识。**MR是对ML的完美补充**，这是因为它能根据ML得出的结论分析可能的原因和潜在的改进选择。

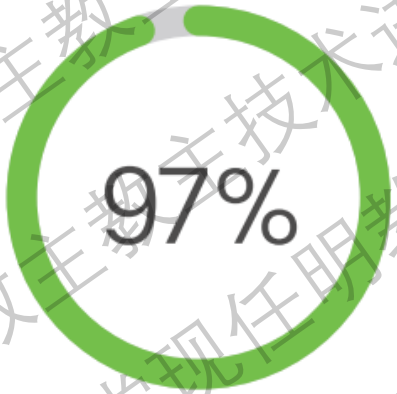
复杂的网络需要AIOps

有很多因素推动着AI驱动的网络的发展。由于网络复杂性和规模的空前增加，AI在帮助IT团队交付水平一致的网络和服务方面越来越必要。

网络正支撑着流量、连接的移动和IoT设备、及互联的应用程序和微服务的爆炸性增长。同时，**当今网络所产生的海量数据超出了只由人类操作员管理的能力，更不用说理解了**。



网络故障造成的损失



网络故障造成的损失

在被调查的全球IT领导者中，有97%的人说，他们在过去6个月遇到过与关键业务应用程序相关的性能问题。每次网络故障的平均损失有多少呢？美国是402,542美元，英国是212,254美元。[21]

由AI驱动的基于意图的网络

AI及IBN这样的先进网络技术显然正在颠覆着事情执行的方式，对网络运营尤其如此。对新的应用程序的测试可分分钟完成，无需数周。**保障引擎会找出问题的根本原因，并给出解决建议**，这使网络问题排查变得容易不少。实际上，如果给未来的网络操作员配备上提供可执行洞察的强大面板，则其可能只需查看几个地方，而无需对众多可能的故障原因一一排查。

ML和MR三个主要保障领域

复杂事件处理：将ML用于网络遥测时，可建立对某个给定意图构成正常运营条件的**动态基准**。

了解动态基准

关联洞察：ML可提供对网络运营更深刻的洞察和可见性，甚至能帮助**预测未来何时可能出现异常情况**。通过应用从排查类似问题的工作流程中获得的预加载专业知识，MR提升了ML的能力。

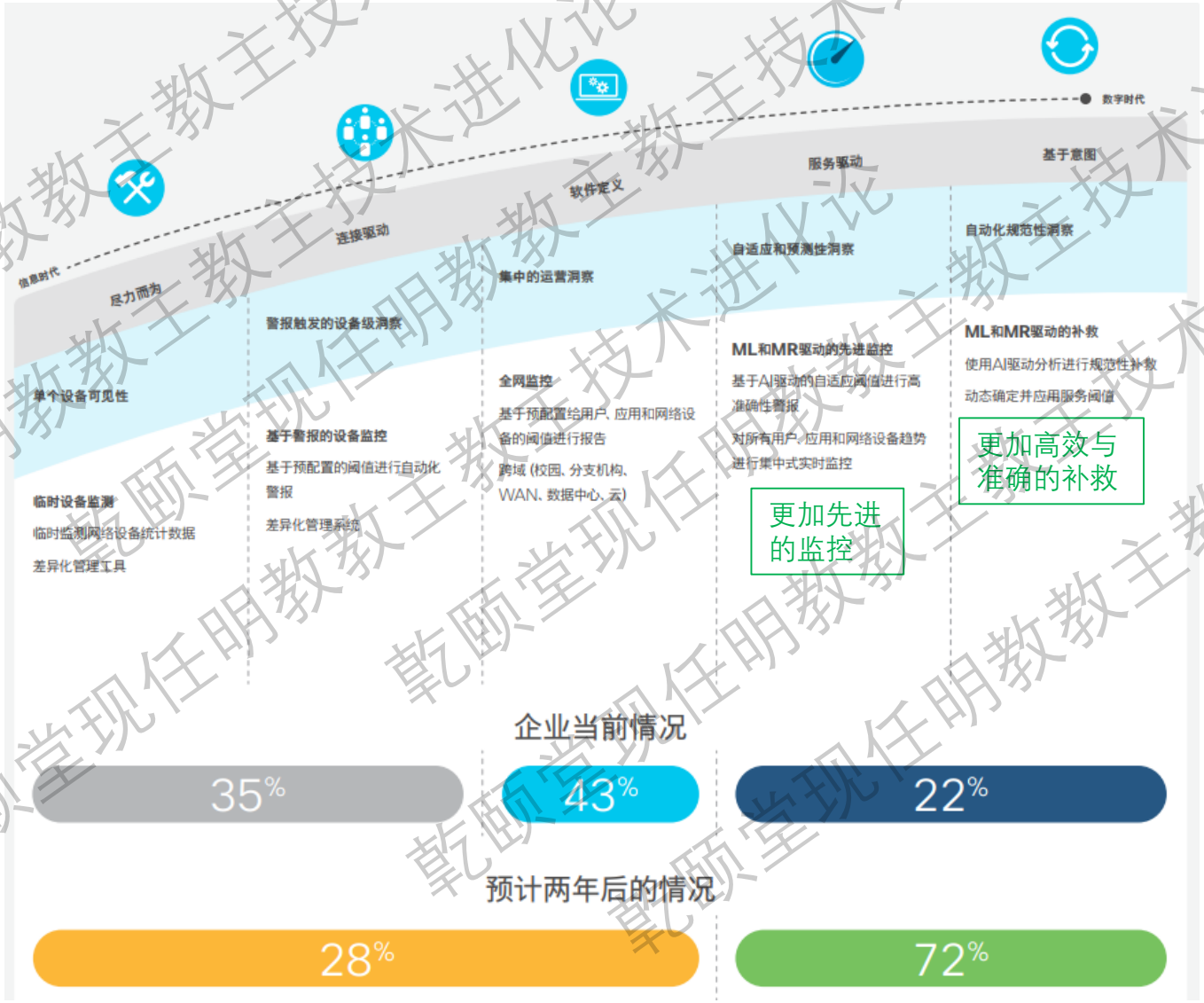
预测未来故障

补救：通过使用由MR等提供的知识库**找出最恰当的纠正措施**，可使补救始终符合意图。

恰当的补救措施

	机器学习	机器推理
技术途径	源于大数据集的数学模型	掌握人类知识、符号逻辑
适用性	预测性分析、异常检测、分类、回归	机器化可决策流程
网络保障功能	• 动态基线和问题识别 • 洞察和可见性 • 预测性分析	• 自动排查问题 • 自动补救

AI驱动的保障就绪度



第四部分

五大新型技术三:多云环境

多云环境下的数据和应用程序网络

总有重要的数据存在的公司内部

容器,私有云,公有云,边缘计算

多云环境改变了网络连接需求

云技术驱动SDN/NFV的快速增长

要点

- 所有公司都需要基于云的服务，但始终有必要将一些数据和工作负载保留在内部。
- 在很多情况下，整体式应用程序正分解为相互连接的微服务，并通过位于容器内、企业内部、云中和企业网络边缘的一系列虚拟和物理工作负载交付。
- 分布式数据中心与传统数据中心的运行方式不同，因此IT企业需适应并满足这种新型架构增加的应用程序和网络连接需求。
- SD-WAN、云直接访问、主机托管设施、云交换，以及更经济的高带宽宽带和5G服务，正逐渐成为重要的新构架元素，以确保云服务可按业务要求有效而实惠地交付。

关键调查结果

- SDN/NFV已在企业数据中心内传输了23%的流量，到2021年，有望增加到44%。
- 29%的IT领导者和网络策略师认为，两年内他们将在企业内部、混合云和多云环境中部署基于意图的网络能力。
- 对云的日益依赖驱动WAN流量上升，到2022年，全球商用IP WAN流量预计将增长2倍，达到每月5.3艾字节。
- 全球超过58%的企业已经以某种形式部署了SD-WAN，且超过94%的受访者相信，他们会在未来两年内部署基本或更高级的基于意图的SD-WAN。

SD-WAN的大量使用

重要指南

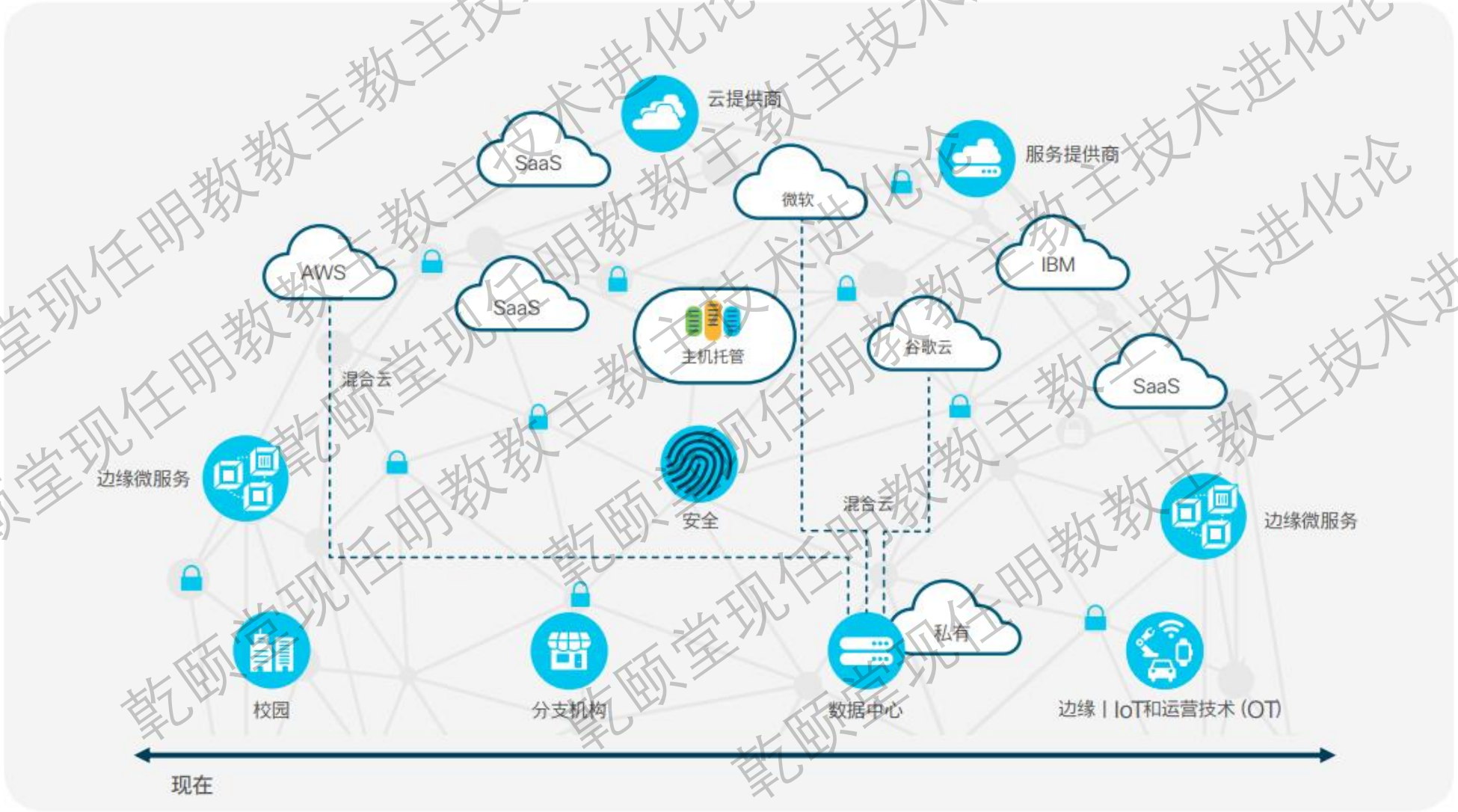
- 确定最关键的基于云的应用程序和服务，并优先考虑任何SD-WAN计划，以首先访问并保护这些应用程序。
- 跨混合云和多云扩展一致的、基于策略的自动化，仔细考虑跨任何位置和任何工作负载的任何平台、任何管理程序或任何容器框架（云原生、裸机、管理程序、容器和无服务器）。

多云环境一致的，自动化的策略

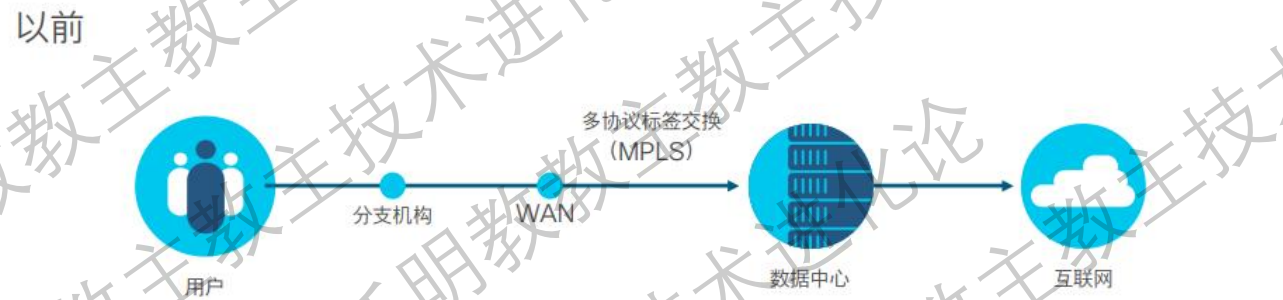
以前:客户与服务和工作负载间的通信

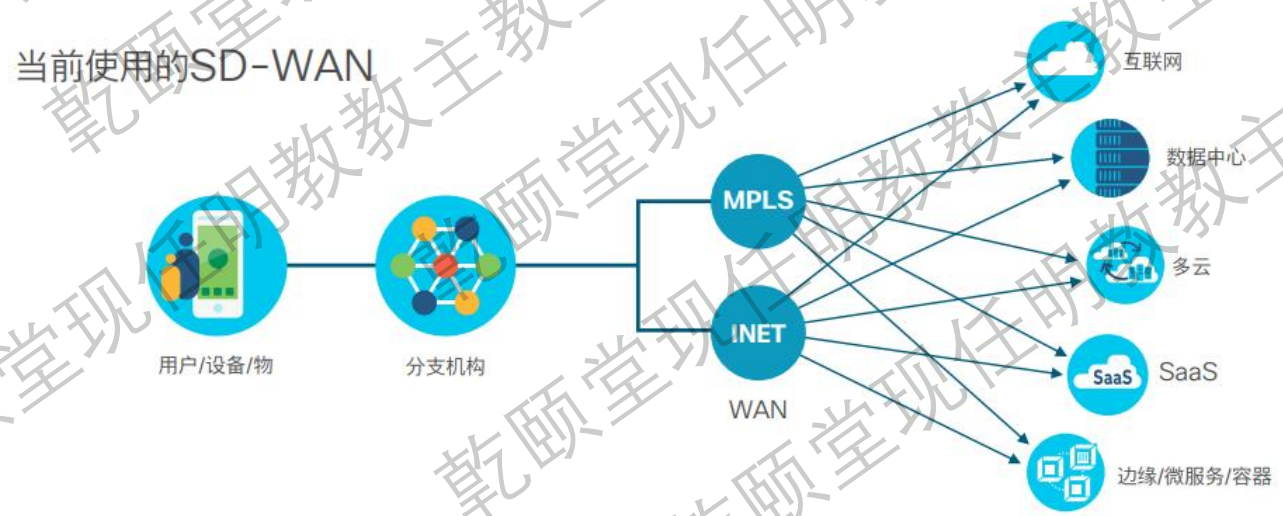
但这种方式已无法满足需求，因为应用程序团队不断采用更为灵活的应用程序模式，这些模式不再是单一的，而是由多个并非总是在一起的、更倾向于分散的、在数据中心和内部环境之外的工作负载或服务组件构成。

以后:客户与服务和工作负载间的通信



不断变化的WAN领域





SD-WAN

↑2X 对云的日益依赖也使WAN的流量上升，到2022年，全球商用IP WAN流量预计将增长2倍，达到每月5.3艾字节。[12]

IT团队需要在多云环境中的控制与自己网络中的相同，这样他们可以继续交付业务所期望的服务。

SD-WAN

SD-WAN是以软件定义的方式去管理WAN，这种方式可使集中控制器优化多云应用体验，大大简化WAN运营。

近来对SD-WAN的迅速采用表明，它为云日益增长的需求提供了很多解决方案。其实，云是采用SD-WAN最大的驱动器。在IDC对SD-WAN的调查中，近75%的受访者认为，SaaS/云服务对当前WAN的技术选择来说是重要的（或非常重要的）。[26]

云是SD-WAN最大驱动器

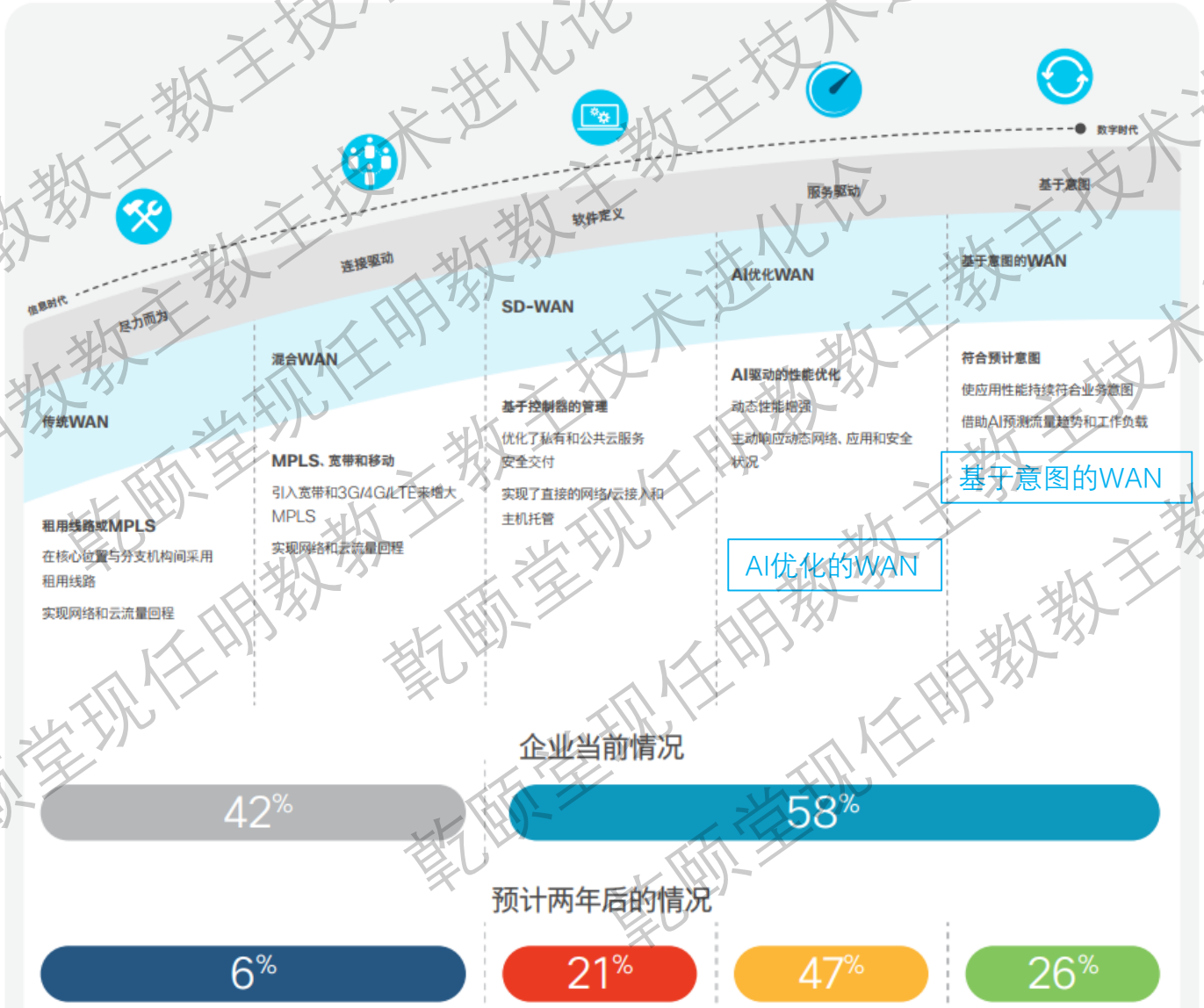
这并不令人意外，因为用于连接由云服务提供商提供的虚拟私有云的传统选项和服务让企业网络团队在多云情境中控制受限。

据我们的《*2019全球网络趋势调查*》，全球超过58%的企业已经以某种形式部署了SD-WAN，且超过94%的受访者认为，他们会在未来两年内部署基本或更高级的SD-WAN。[14]

需要更加高级的SD-WAN技术,并且需要无缝的集成5G移动技术

同时，随着5G服务的应用越来越广泛，SD-WAN会将它们无缝集成到一个与传输无关的框架中，以实现最大的灵活性和最佳性能，改进始终在线支持，并减少成本。

多云就绪WAN

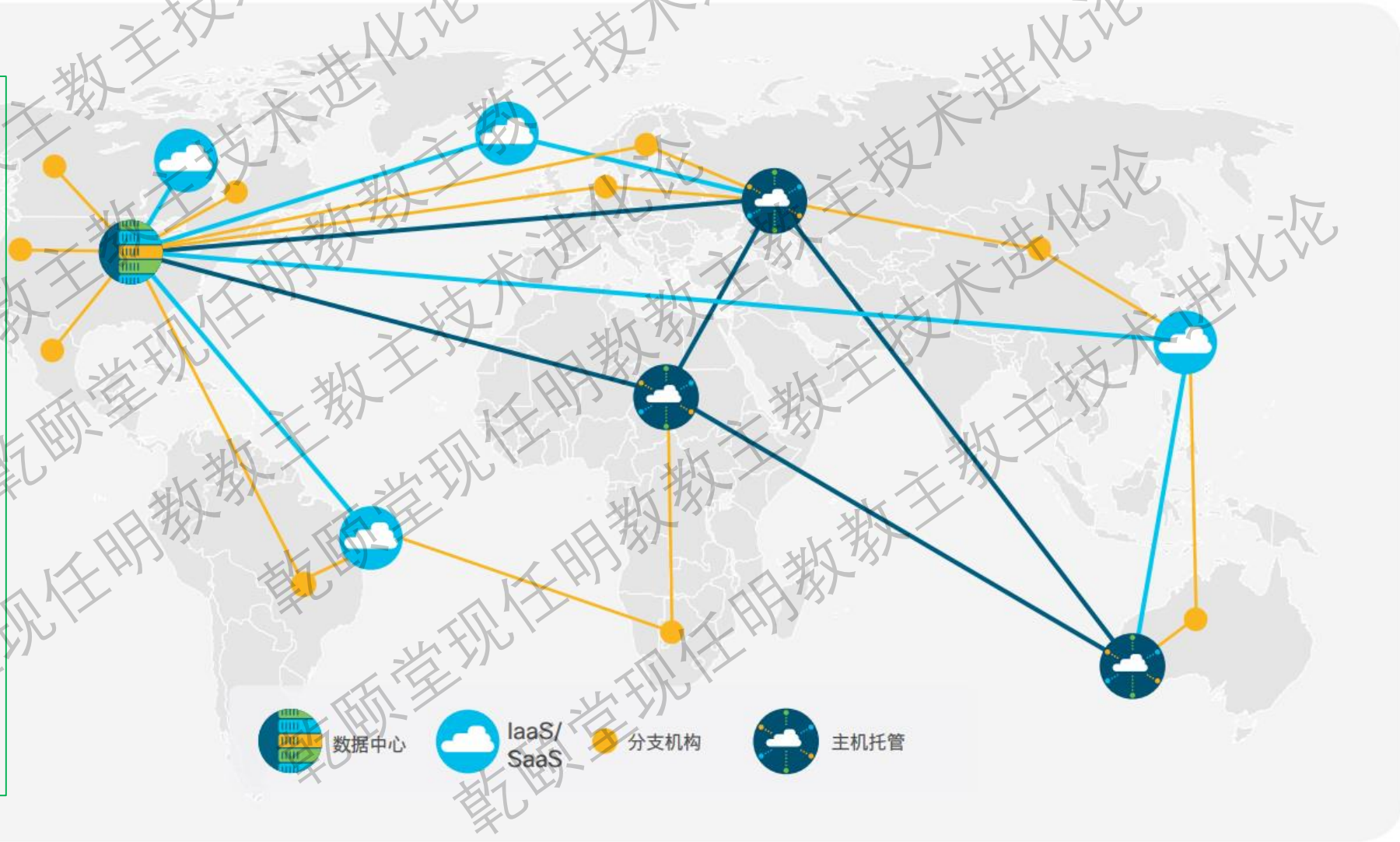


云直接访问

将分支机构流量通过昂贵的WAN电路回传至数据中心或通过中心辐射型架构回传至集中式互联网网关的传统方式可能阻碍向云服务的转变，同时还将增加费用并产生降低用户体验的延迟。

直到现在，网络架构师由于替代方法的成本和复杂性仍囿于这种方式，替代方案需要在每个分支机构路由器部署和管理分布式安全功能，如防火墙、URL过滤和DNS保护。

但“云直接访问”或“互联网直接访问”功能现在可将用户直接从分支机构安全连接到云服务。这简化了跨远程站点的策略管理，并在数分钟内自动提供新的网络服务，同时实施了多层次安全防护，包括加密、认证、分段、防火墙和DNS保护。



IBN

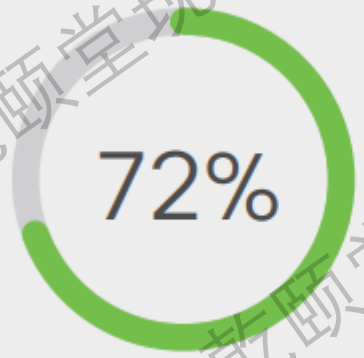
“基于意图的网络是网络界最大胆、最包罗万象的成果，其创建了一个系统范围的网络模型，可让敏捷企业应对所有最新技术趋势和瞬息万变的需求。”

– 思科数据中心CTO兼名誉顾问Tom Edsall

流量的变化

3倍

未来五年，全球数据中心IP流量将增长3倍。[23]



到2021年，数据中心内的流量将占数据中心总流量的72%。[23]

网络基础设施需要灵活性和容量，以支持高性能的客户到应用程序流量（南北流量）和日益增长的服务器到服务器或VM到VM流量（东西流量）。目前，这一般是使用由一个或多个控制层覆盖协议支持的扁平"脊叶"架构完成的。

据《思科全球云指数》，到2021年，**数据中心内的流量将占数据中心总流量的72%**，将远远超过数据中心到用户（15%）和数据中心到数据中心（14%）的流量。对以太网交换性能的要求将不断提高，以支持计算流量及基于文件，甚至基于块的存储流量增长的需求。

第五部分

五大新型技术四:网络接入与无线

网络接入与无线

Seamlessly roam across Wi-Fi 6 and 5G networks

OpenRoaming, currently in beta, enables mobile users to automatically and seamlessly roam across Wi-Fi and cellular networks, including Wi-Fi 6 (802.11ax) and 5G. This is achieved through a collective of industry partners and collaborators, whose goal is to provide a better bridge between mobile and Wi-Fi networks.

WIFI6和5G的无缝的全局漫游

使用AI进行无线规划,健康监控,问题排错和补救

统一,一致的安全管理

更好的支持IoT和AR/VR

大量的IoT与M2M设备

章节摘要

要点

- 开放漫游（OpenRoaming）等新兴功能将在不同的Wi-Fi 6网络和5G公共网络之间提供无缝、始终在线且安全的全球漫游。
- 网络团队需要增强的分析和AI功能，用于无线规划、健康监控、问题排查和补救。
- IT团队需要跨不同的接入网络自动管理、实施并传播一致的访问策略，以更好地保护应用程序、数据、用户和设备。
- 无线网络需要识别并动态支持新型沉浸式媒体应用程序和IoT设备的需求。

关键调查结果

- 在全球范围内，到2022年，无线设备将占到所有联网设备的43%。
- 到2022年，IoT M2M设备将占到全部联网设备的51%，其中大多数是无线连接。
- 35%的网络策略师认为，排查网络问题是当今网络运营中最耗资源和时间的活动。
- 34%的企业仍在使用人工方式管理有线和无线网络的访问。
- 40%的企业提供策略自动化和细分以减少威胁，而另外15%则使用AI驱动的访问解决方案。
- 27%的企业计划在两年内建立基于意图的网络访问模型。

重要指南

- 考虑Wi-Fi 6和5G将如何影响你所在企业的未来业务需求，并据此制定您的无线策略。
- 制定使所有移动和IoT设备的安全载入和细分实现自动化的路线图。
- 探索自动化设备分类的使用，实现各型IoT设备的大规模载入。
- 评估基于位置的服务和网络分析如何能为你的企业带来业务利益。

网络排查最有技术含量,也最耗资源与时间

高层前瞻

高层前瞻

“到2025年，像开放漫游（OpenRoaming）这样的无线联合会将无处不在，IT企业和服务提供商由此可使用零信任访问系统，安全共享身份凭证，终端用户可安全无缝地在任何私人或公共无线接入网络上漫游。用户体验将是无摩擦和策略执行式的，不管用户在哪里访问都能为其提供最佳体验。”

– 思科无线技术CTO Matt MacPherson

“到2025年，基于IEEE 802.11ax标准的Wi-Fi 6网络将与计划中的Wi-Fi 6扩展网络一起成为无所不在的Wi-Fi的主要形式。大概在2024年，基于制定中的IEEE 802.11be标准的下一代Wi-Fi（可能作为Wi-Fi 7推出）才会开始上市。”

– 思科董事、Wi-Fi联盟前主席和技术领导
Andrew Myles

OpenRoaming

802.11be (WIFI7)

移动卸载流量增加

Wi-Fi被广泛用作一种移动卸载机制，在5G时代甚至更为必要。据预测，5G将卸载其流量的70%以上，相比于4G网络的59%有明显提升。[27]

WIFI对5G的卸载越来越重要

OpenRoaming

“有了OpenRoaming，移动用户再也无需猜测哪个Wi-Fi网络可用、忍受弹出式强制门户，或再次使用不安全的用户名和密码。无论他们身处何处都可以接入网络，下载、串流、视频聊天、玩游戏，甚至随心所欲地工作。”

– 思科无线技术CTO Matt MacPherson

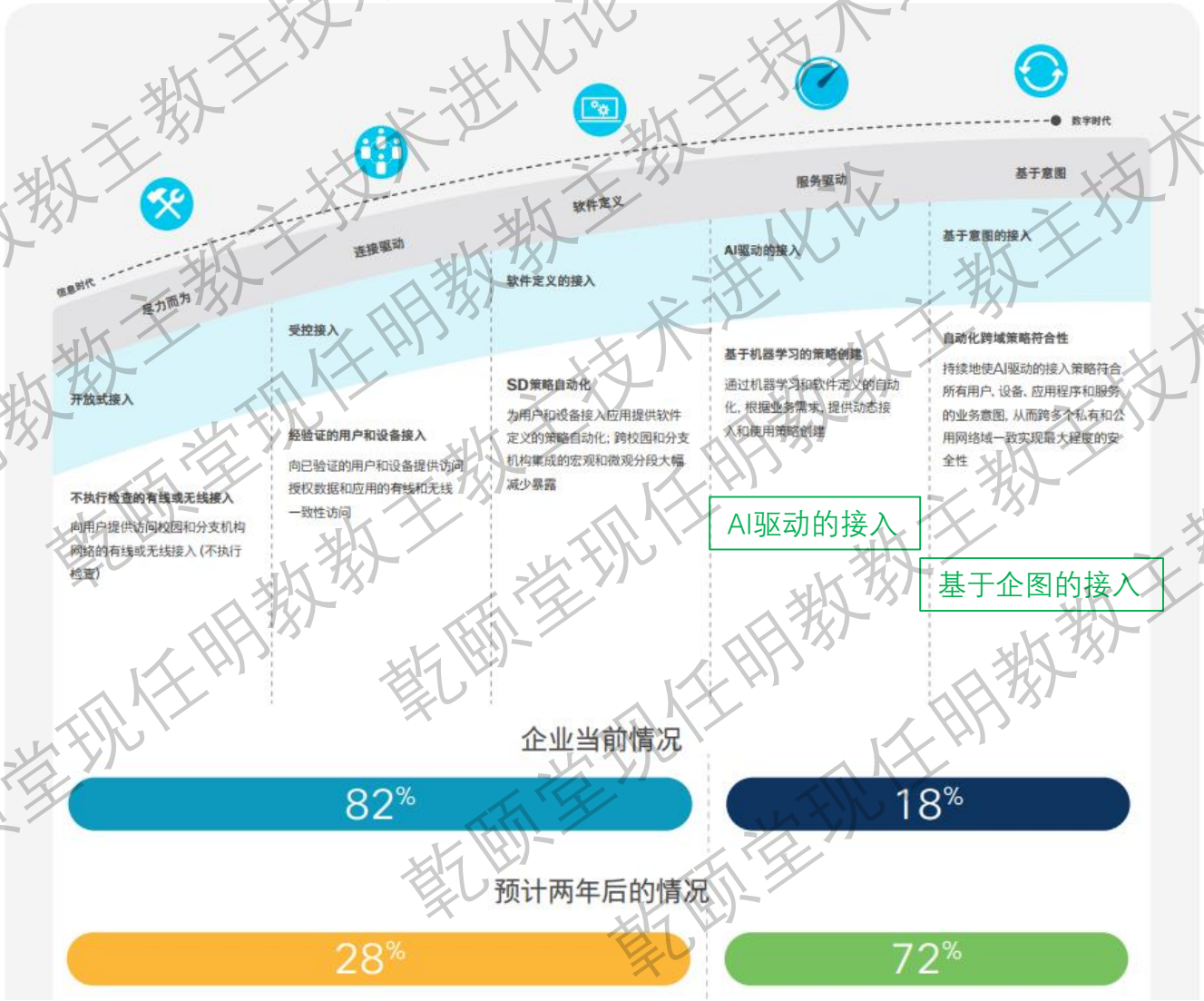
维护与排错的难度

由于部署和维护无线网络所用的传统方式不可持续，因此网络运营要走在这些新兴业务需求的前面。**特别是无线网路的问题排查，对大多数网络团队而言，这是一项被动、复杂且耗资源的工作(无线网络排查是网络问题排查中最难的事情)。**难怪网络领导者目前将排查网络问题视为网络运营中最耗时的作业。

更为复杂的是，除了新兴的**Wi-Fi6**和**5G**网络外，IoT设备还可通过包括**BLE**、**Zigbee**和**Thread**(https://en.wikipedia.org/wiki/Thread_(network_protocol))在内的多个利基无线协议通信。IT面临的挑战将是确保网络管理工作不会在这些不同的网络上分崩离析。

尽管许多IoT用例集中在主流Wi—Fi6和5G网络上，但IT团队应考虑如何通过公共管理层来管理独特或高要求用例所需的更专业的无线技术。若想先人一步，NetOps团队需要一种更主动的方法来进行无线规划、监控、问题排查和补救。这要求使用分析及AI驱动的监控更好地了解无线性能及其健康状况。

安全接入就绪度



第六部分

五大新型技术五:不断改变的网络安全角色

不断改变的网络安全角色

传统的基于边界的安全已经落后

可见性和控制的缺失

安全与IBN强大的结合

补救时机是重要的PKI

要点

- 随着应用程序、数据和身份向云端和网络边缘的迁移，仅基于边界的安全无法有效防御当前的威胁。
- 许多不同类型的设备，以及从各处接入网络应用的移动客户，混杂的状态带来新的挑战，如可见性和控制的缺失。
- 将安全性与基于意图的网络功能集成在一起，可产生强大的组合，从而跨网络实现有效的策略执行、保护和修复。

关键调查结果

- 网络策略师将安全视为仅次于AI的重要投资领域。
- 43%的网络团队将提高嵌入式网络安全能力作为优先事项。
- 2019年，48%的首席信息安全官（CISO）将“补救时机”看作主要的关键性能指标（KPI），比2018年的30%有所上升。
- 近75%的网络领导者有信心在两年内拥有AI驱动的适应性或自动化的策略定义和实施。

急需AI驱动的安全

重要指南

- 在五个关键领域开发网络安全能力：可见性与威胁检测、零信任接入、持续保护、可信网络基础设施、安全运营（SecOps）和网络运营（NetOps）一体化工作流程。
- 确保将零信任安全策略包括在任何网络自动化和保障计划中，以有效管理安全威胁，不管它们存在于分布式网络的何处。
- 在升级基础设施和流程时，网络团队应考虑可信要求，确保网络本身可防篡改。
- SecOps和NetOps团队需要考虑如何分享数据，并应整合工具，以简化威胁防御、检测和响应工作流程。

SecOps与NetOps需要更好的协作

高层前瞻

基于AI的SecOps

量子计算的威胁

高层前瞻

“到2025年，一些领先的IT企业会部署一系列有限的完全自动化的网络驱动安全工作流程，帮助提高补救速度，减少SecOps团队的工作负荷。随着IBN平台、AI/ML技术、及安全和网络工具间的集成日趋成熟，将使一些定义明确、不会给企业的安全态势或网络带来风险的用例实现自动化。”

– 思科CISO顾问团队负责人Wendy Nather

“虽然量子计算到2025年仍将处于早期阶段，但人们已经在努力应对量子计算被用于破坏当前加密方法的新危险。”

– 思科研究员David McGrew

规模和复杂性增加

面对更大、更复杂及快速变化的移动优先和云优先环境，以及防御难度日益增加的安全威胁，IT必须保护企业及其数据。

工作负载：随看应用程序、数据和身份向云端和网络的迁IT模型继续拓展并超越传统的企业边界。混合云计算和多云计算以及边缘托管的服务的兴起，要求我们改变保护工作负载的方式。仅基于边界的安全无法有效防御当前的威胁。

客户：此外，许多不同类型的设备（用户设备和互联IoT设备）与从各处接入网络应用的各种不同用户（员工、承包商、第三方）的混合也使情况更为复杂.

基础设施：最后，随看威胁复杂性的发展，攻击者越来越多地试图颠覆底层交换和路由基础设施，以便窃听、窃取或操纵数据，并对网络的其他部分发起攻击。

思科面临的安全挑战

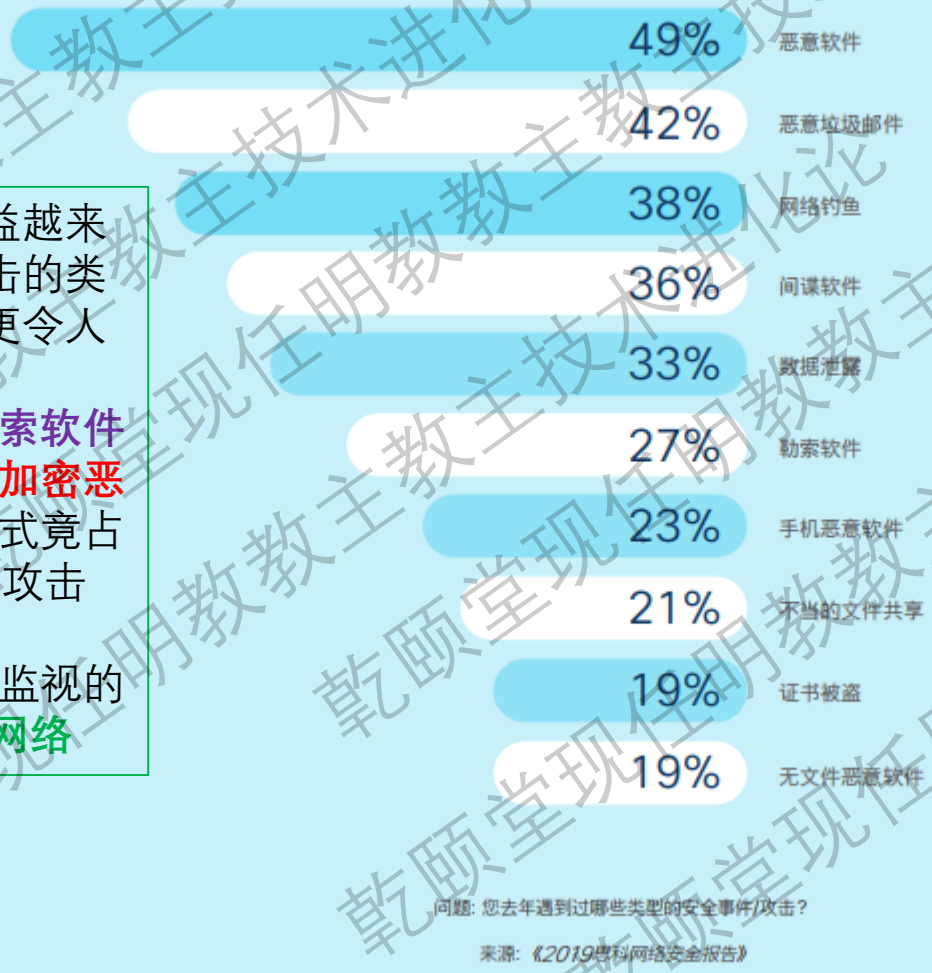
“我们和任何其他大型企业一样，需要应对日益增加的复杂性。我们每天要检查47太字节的互联网流量，分析280亿次流动，记录1.2万亿个安全事件。”

– 思科基础设施安全总监Marisa Chancellor

当前网络安全威胁

由于网络攻击的潜在收益越来越具有诱惑力，因此攻击的类型也越来越复杂。一些更令人担忧的攻击趋势包括：

- 基于网络的**自传播勒索软件**
- 隐藏在**加密流量内的加密恶意攻击**，这种攻击方式竟占到了2017年所有恶意攻击的70%
- 部署在有漏洞和不受监视的IoT设备上的**IoT僵尸网络**



IoT设备的激增扩大了受攻击面

联网IoT设备在没有充分安全保护的情况下继续迅速增加，这主要是因为它们经常不被IT所知或未受IT检测。对企业来说，每联网一台设备都会增大受攻击面。针对IoT设备的网络级攻击可能包括分布式阻断服务(DDoS)攻击、射频识别(RFID)电子欺骗、以密码为目标的软件威胁和恶意软件威胁。

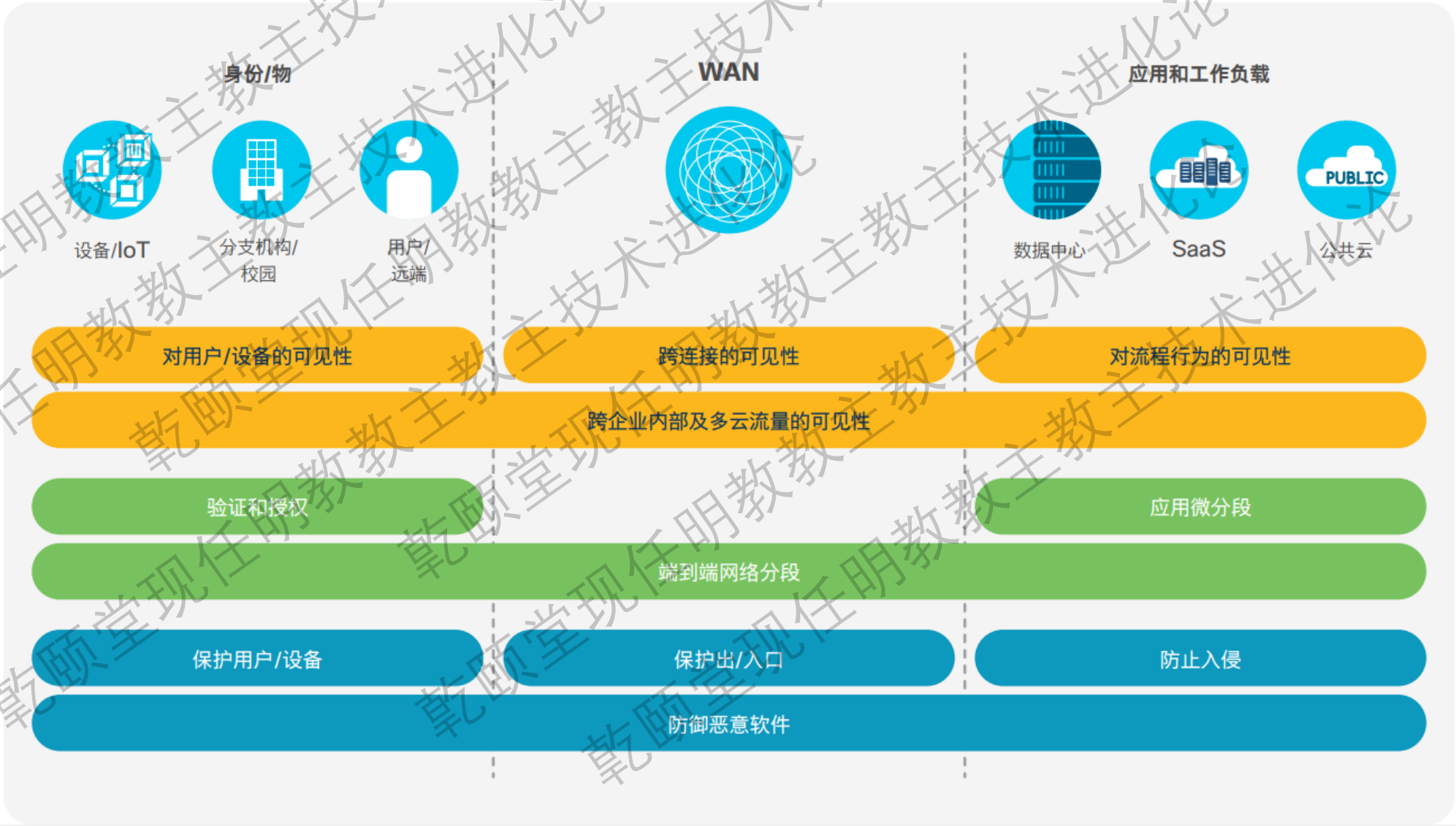
> “许多IoT设备本身的安全防护很有限，很少使用数字证书或凭证，所以易受到攻击。因此，设备识别、分类和网络接入策略激活的自动化成为了防止或遏制安全漏洞的重中之重。”
>
> – 思科IoT首席工程师Tim Szigeti

可见性的缺失

“我们正面临向SaaS的大规模迁移，并正在失去我们过去曾经拥有的传统的可见性和控制。”

– 思科基础设施安全总监Marisa Chancellor

集成的网络安全模型



零信任接入

保障网络接入安全：在零信任接入模型中，IT对有线和无线网络上的用户和IoT终端可在**何时、何地，如何做什么实行精确控制**。同时，还能借助基于群组的策略控制和端到端．客户到应用程序分段来应用零信任方式，从而限制对您网络上资源的访问。

主动遏制应用程序漏洞：IT工作人员可**减缓数据中心内外工作负载间未经授权的横向运动**，这有助于在攻击者已经进入时减少攻击面。

降低未经授权访问应用程序的风险：不管是什么用户（员工、承包商、第三方等），当他们登录到任何内部或外部应用程序时，**需使用双因素验证**确认其身份及其设备的安全性，降低因密码被盗或密码弱而导致的未经授权访问应用程序和数据的风险。

基于意图的网络安全就绪度