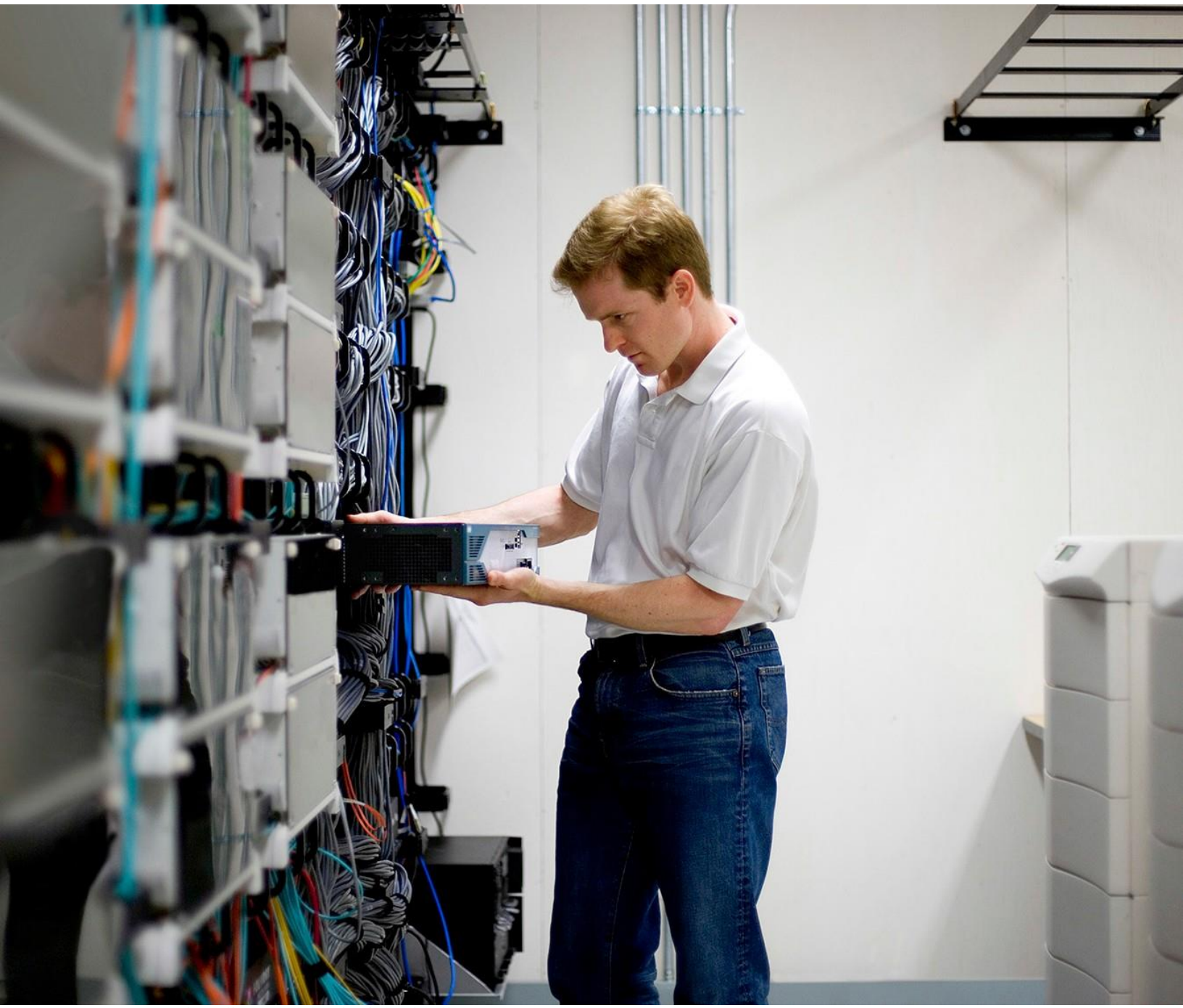
让您的网络边缘变得智能，现在即满足未来需求



© 2016思科和/或其附属公司版权所有。保留所有权利。

摘要

在新型数字化企业中，网络边缘从未像现在这样重要。常常被人们忽视的网络边缘是决定数字化转型是否成功的基石。请考虑以下网络边缘处所发生的一切：

- 它是阻挡不可信或恶意设备侵入的第一道防线。
- 它是向目标受众交付（通常是巨资投入的）应用及服务的管道。
- 它是互连分布广泛的各个企业的战略性网关。
- 它是贵企业与客户之间的一座桥梁。
- 它是全新物联网（IoT）设备实现互联和得到管理的地方。
- 它是您真正了解贵公司情况的最佳场所。

人们有时在部署网络边缘时认为，所有网络解决方案基本上都是相同的。这种认识是错误的，因为新型数字化企业需要高智能的网络边缘。思科提供取得商业成功所需的解决方案和战略功能。我们提供一个全新的网络架构，它始于最终用户，并延伸至托管应用的地方，而且关注：

- 借助更好的体验以及与用户、设备、应用和威胁有关的细粒度洞见**提升创新速度**。
- **降低成本和复杂性**，使企业能够轻松制定策略和大规模管理变更，同时降低有线/无线网络和 WAN 上的软硬件流失率。
- 借助全面的威胁可见性以及防范有线/无线网络和 WAN 上的内外风险来**降低风险**。

当前，对于踏上数字化转型旅程的所有企业而言，网络在促进此项变革方面扮演着不可或缺的角色。这段旅程将帮助企业以更快的速度创新，并降低成本和复杂性，从而让他们能够提升敏捷性和员工生产力，与客户更好地互动，并保护重要的知识产权和资产。

网络边缘在促进这一转型方面发挥着关键作用，与网络核心和数据中心网络相比，肩负着最为广泛的责任。如图 1 所示，通过对比各个网络层，网络边缘在园区中肩负着广泛的责任，并且在分支机构亦是如此。

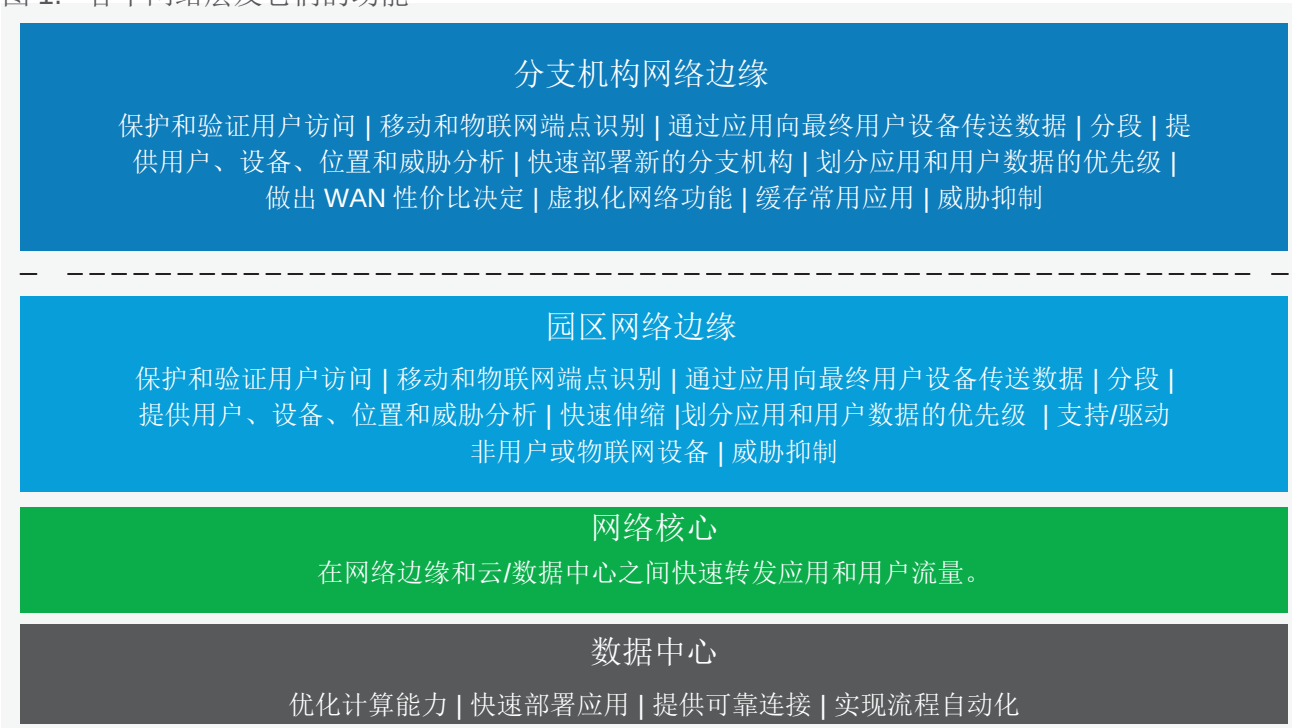
网络边缘的角色

数字化转型让网络边缘变得比以往任何时候都重要。请考虑以下网络边缘处所发生的一切：

- **它是第一道防线。**您在网络边缘处应用策略，而且还能不受限制地访问所需的一切。如果访问未得到良好管理，您的企业就有可能遭受入侵或威胁扩散，而且随着威胁的加剧，情况会越来越严重。设备、固件甚至操作系统都会遭到破坏。

© 2016思科和/或其附属公司版权所有。保留所有权利。

图 1. 各个网络层及它们的功能



- **它是交付巨资投入的应用的管道。**优先级划分在网络边缘发生。网络边缘处糟糕的体验将减缓应用的普及速度，从而降低投资回报率。
- **它是互连分布广泛的各个企业的战略性网关。**为您的员工、合作伙伴和客户－无论他们身在何处－提供无缝体验至关重要。二流网络只会给这些关键受众提供偏离标准的服务。
- **它是贵企业与客户之间的一座桥梁。**如果您身处零售或酒店行业，低于标准的访问将削弱您在个人层面上与客户交流的能力，从而影响您的品牌形象。
- **它旨在满足市场对物联网设备日益增长的需求。**通过将几乎所有行业过渡到数字时代，并优化运营和成本，网络边缘改变了物理环境。如果网络边缘处没有所需功能，企业在缩减成本和提高运营效率方面将落后他人。
- **它是您了解贵公司情况的最佳场所。**在一个分布式网络中，只有网络边缘能够通过数据采集和分析看到所有数据流量。

借助与用户、应用、设备和威胁有关的数据，企业能够获得洞见，从而真正帮助它们做出更好的决策，以支持员工，降低风险和成本，并向目标受众传送信息。如果没有合理水平的粒度，这些数据会变得扭曲和不可信。

网络边缘的商品化是好事吗？

很多企业肩负着实现数字化，然后以更快的速度进行创新、提升体验和安全性的任务。但是，通过改造网络来满足这些需求是一项异常艰巨的任务，因为现在建立的网络基础需要在未来几年为企业提供支持。选择一个网络厂商是一个重大决策，将决定您是持续创新，满足业务需求，还是趋于迟钝，在低下的能力下苦苦挣扎。

对于数字化转型而言，没人真正知道未来将会怎样，但有一点可以肯定：您网络上的需求将迅猛增长。无论是物联网、云、复杂的安全威胁或增强现实，数字化转型都会改变您运营和服务企业的方式。

© 2016思科和/或其附属公司版权所有。保留所有权利。

现在还足够好的东西在不远的将来将变得不可接受，而且所有这一切都始于网络。您必须以更快的速度创新，降低风险和复杂性，并控制风险。那些真正为数字化做好准备的企业知道，在通向这些变革的道路上，它们不能在重大问题上做出妥协。

有何风险？

为“数字化第一”世界做好准备，并不是为了应对网络中某一处的问题，而是为了从网络接入边缘开始，借助一种数字化就绪架构方法，使用通用网络核心和 WAN 中的通用功能。这种方法为何重要？因为当今的“数字化第一”世界移动和运动地更快，意味着您的网络需要做好准备。那些已为数字化世界做好准备的企业不需要因为在重大问题上做出妥协而承担不必要的风险。它们知道：

1. **让您的创新变得毫无用处只需一项糟糕的体验。**

   在企业内部，一切都是为了创新。但在您的应用与外部世界相交、全新物联网设备推动业务转型的网络边缘，不可靠的连接和低性能有可能永远赶走您的用户。
   这将影响设备性能，让您无法获得保持竞争力所需的洞见。思科将洞见植入到您的数字网络架构（DNA）中：不仅包括有助于提升性能的网络洞见，而且还包括有助于打造更好的个性化体验的实时消费者洞见。

2. **毁掉您的声誉只需一个“no”。**

   世界正在快速发展，如果您跟不上它的步伐，您将会被抛弃。更有甚者，资源和预算都很紧张。一个分支机构一个分支机构、一个设备一个设备地配置和重配置您的网络可将一次简单的“更新”变成一个总体拥有成本（TCO）深坑。思科将自动化植入到您的 DNA 中，让您能够在一个地方将您的整个网络（园区、WAN 和分支机构中的有线和无线网络）视为单一实体，实现其自动化，并对其进行管理。

3. **成为所有人的问题只需一次事故。**

   我们不需要告诉您网络宕机的成本有多高，也不需要强调网络安全对于确保网络正常运行、防范那些威胁您的网络服务的恶意软件有多重要。

   因此，您为何要去购买不能控制访问、抵御攻击、检测和抑制漏洞的网络基础设施？您怎能委托一家不能确保网络完全的公司建设您的基础网络？在思科的帮助下，您可以在分支机构和总部将您的有线和无线网络转变成一个威胁传感器和安全策略执行器。切勿将安全交到他人手中。

思科在网络边缘实现智能化

数字化就绪企业的基础是思科数字网络架构（Cisco® Digital Network Architecture（DNA）），它能够在网络各处实现创新和智能。为什么？很简单，Cisco DNA 专注于全程保护、简化和实现业务。只有思科能够做到这一点，因为 Cisco DNA 是唯一能让您做到以下几点的解决方案：

1. **提供更好的体验，**并获得与用户、设备、应用和威胁有关的**细粒度洞见**。数字化就绪意味着提供正确的体验，以赋予员工能力，与客户互动，提供用于优化用户体验的宝贵洞见，开辟新的收入来源，并控制成本。高可用性基础设施可发现变化，并自动适应，以支持更大的容量。作为苹果公司唯一的网络战略合作伙伴，思科可帮助企业将音频质量提升 20%，将 web 浏览器故障数量减少 90%，并将处于漫游状态的 iOS 设备的网络消息负荷降低 86%。业内领先的 1 米定位精度以及可使用实时 NetFlow 数据的能力可让您简要了解用户互动和威胁影响，从而真实地描绘出您的环境中正在发生的情况。

2. **轻松制定策略和大规模管理变更，**同时降低有线/无线网络和 WAN 上的软硬件流失率。可集中管理所有网络域的能力，加快企业调整网络和优化用户体验的速度，并让它们将部署成本降低 79%。
   一个开放、可编程、可通过 LAN、WLAN、WAN 和其它战略数据仓提供 API 的基础设施可让您采集、开发和部署新应用及控制机制。

© 2016思科和/或其附属公司版权所有。保留所有权利。

存在一个庞大的开发者社区，您可以在其中学习和开展合作，从而受益于最佳实践和思科应用能指南。

竞品解决方案能够管理一或两个网络域，如有线和无线，但却不具备端到端集中管理能力。只使用 API 的竞品解决方案不具备思科提供的紧密社区和专业知识。

3. **全面的威胁可见性以及防范**有线/无线网络和 WAN 上的**内外风险**。网络扮演传感器和执行器的角色，依据策略在每个网络跳验证流量。这种能力让网络能够快速发现和消除潜在威胁，降低风险，并坚持合规。企业也能避免 99.2%的威胁，并以快于传统方法 98%的速度调整网络以应对新的威胁。此外，它们还能实现 140%的投资回报率。

   其它解决方案只在接入层寻找威胁，并使用已知恶意软件的信息。这意味着现代恶意软件能够通过伪装成正常流量侵入网络，然后在网络内部开展恶意活动。企业不得不从各种抽样数据中提取信息，试图找出问题所在，以便消除它。

数字化企业还在消除孤岛，因为它们知道生产性网络和数据需要齐心协力才能提供更好的用户、设备和应用体验。Cisco DNA 专注于从头至尾（从用户开始到应用终结）分析、简化、自动化和保护业务。

提供更好的体验和细粒度洞见

在网络边缘，赋予员工能力，与客户互动，并提供物联网设备。它是宝贵洞见的来源。

- **为企业网中的 iPhone 和 iPad 提供最佳用户体验**。借助 iOS 10 中的新特性以及思科最新的网络软硬件，任何地方的企业都能充分利用它们的基础设施，提供卓越的应用、呼叫和协作体验。思科和苹果公司联手为您的移动员工开发最佳无线连接，而且当 IT 部门在思科的网络上使用 iOS 设备时，让他们能够轻松地为那些重要的应用分配较高的优先级。业内其它厂商不提供这种互操作性。
- **获得网络、接入和最终设备一级的永远在线、永远就绪可靠性，将对用户的影响减至零。**思科的解决方案提供具备多层弹性的网络，为您树立信心：网络在需要时总是可用，而且您和您的物联网设备正在为贵企业效力。
- **需要时自动调整 Wi-Fi 网络。**借助超越无线标准的创新技术提供稳定的高质量体验。思科的网络可提升新旧移动设备的能力，消除干扰，并通过调整容量满足不断变化的需求。
- **借助故障保护功能更好地支持物联网设备，以确保可靠性，提升性能。** 思科的网络在物联网设备连接的交换机中内置故障保护功能和雾计算，后者能够自行决定处理物联网设备数据的最佳地点。思科的网络已为全新的互联世界做好准备。

与业务相关和只是另一个设施之间的区别在于用户体验的好坏和数据精度。

企业可以期待实时应用具备更高的可靠性，将 WiFi 呼叫的音频质量提升 20%，通过减少服务集标识符（SSID）将网络管理开销降低 50%，将来自 iOS 设备的网络消息负荷降低 86%。与此同时，当漫游最终用户在思科的网络上使用 iOS 设备时，他们将能受益于更长的电池寿命。

© 2016思科和/或其附属公司版权所有。保留所有权利。

- **借助 1 米定位精度真实地了解用户、设备、应用和威胁 。**思科提供业内领先的位置数据粒度，可让您更好地了解用户如何与环境互动，从而做出更好的业务决策。

借助 Wi-Fi 外加低功耗蓝牙（BLE），零售、酒店、教育等企业对消费者（B2C）性质的企业已能实现低于 1 米的定位精度和直接的收入增长。例如，凯悦酒店的非客房收入增长了 20%；

Starry Bowar 商场的顾客停留时间增长了三倍，用户体验提升了 80% – 同时提供个性化移动体验。

轻松制定策略和大规模管理变更

为满足企业不断增长的业务需求，按设备逐一不断地重配置和调整网络，是一件成本高昂并且耗时的活动，但企业很难摆脱这种活动。思科提供一种轻松管理网络的方法，无论是一个或多个站点。

数字化企业需要网络才能提升敏捷性，这意味着网络需要借助“零日”和“首日”能力实现流程和新服务自动化，并消除人工干预。这种能力可让数字化企业部署和维护一个适合当今快速变化行业格局的网络。

- 管理一个服务质量（QoS）策略，并根据网络性能进行调整。思科的解决方案在 LAN、WLAN 和 WAN 上使用相同的 QoS 策略，以便提供更好的端到端应用处理。它们能够根据使用情况和服务评级，并考虑环境中的变化和 QoS 定义，向时延敏感型语音和协作等关键应用自动分配高优先级，从而确保业务关键型应用能够获得高优先级。
- 采用零接触部署方式更快地开通新网段和分支机构。Cisco Application Policy Infrastructure Controller Enterprise Module（APIC-EM））（思科应用策略基础架构控制器企业模块）的即插即用应用可采用针对 Cisco Enterprise Network 路由器、交换机和无线控制器的零接触部署方式，减少配置、部署和开通新网段和分支机构所需的资源和时间。
- 在无需更换设备的情况下添加新的软硬件。思科的网络可让企业利用现有接入点、控制器和交换机添加新功能，同时不影响其性能。
- 实现简单的许可证管理和基础设施升级的可移植性。您可以利用重要的新功能，同时不需要耗时的许可证管理。升级基础设施时，可以将软件许可证发送到新硬件上。
- 利用现有无线接入点扩展功能。您可以通过模块向现有接入点添加新的行业标准功能或来自第三方生态系统合作伙伴的功能。

通过将软件与硬件分离，并虚拟化 WAN 边缘，思科能够加快部署速度，并将部署成本降低 79%。

全面的威胁可见性以及防范内外风险

网络边缘是非法和恶意访问最多的地方，这是因为用户和设备从那里进入园区和分支机构。为了发现和控制网络访问，它必须值得信赖。它还需要与网络核心和分支机构中的安全解决方案进行配合，以抵御最新的恶意软件攻击。

© 2016思科和/或其附属公司版权所有。保留所有权利。

借助 Cisco Identity Services Engine、Cisco TrustSec®和 Cisco StealthWatch，您可以将您的网络转变成一个传感器和执行器，以优化防护和响应时间。这意味着当威胁进入网络，或者通过初始接入，在网络中扩散时，您能够避免、发现和消除威胁。Cisco DNA 可让您：

- **利用软件分段管理用户和设备接入，**消除大量的静态 VPN 和 SSID。确保用户、访客、承包商、临时工和客户能够访问所需信息，不能访问他们不能访问的信息。这种基于软件的用户和设备分组方式提供更大的规模，而且可让您减少配置错误，更快地添加设备，比传统人工方法更加合理地分类用户和设备，从而能够以快于传统方法 98%的速度执行变更。
- **将安全性植入到各处，以便在接入层和网络内部检测和抑制威胁。**在接入、内核和分支机构层中的每个网络出入口验证流量。即使恶意软件通过某个用户设备或物联网设备被引入网络，或某人蓄意盗窃数据，思科网络基础设施也能发现威胁存在于何处，并采取措施消除或减少影响。
- **利用实时 NetFlow 数据快速分析和减少威胁影响。**利用 NetFlow 超越传统威胁检测方法。它可以为您提供网络可见性、分析和防护高级功能。您可以看到网络中发生的一切，也可以发现那些绕过防线、侵入到您的内部环境的攻击行为。
- **利用全球生态系统了解整个网络中的最新威胁。**了解最新威胁，以避免和快速消除网络中的威胁。利用来自全球各地的共享数据制止攻击，即使您看不见他们，并关闭大门，防止它们进入数据仓库或网络中的其它设备。

防护网络边缘处的重要资产。通过将网络用作传感器和执行器，企业可以避免几乎 100%的网络漏洞。这是可以做到的，同时还提供有助于改进防护和提升响应速度的洞见。

Forrester 新近发布的一份研究报告显示，Cisco TrustSec 可让 IT 部门将执行变更的速度提高 98%，将成本降低 80%，并实现 140%的投资回报率。

网络边缘的持续创新

随着连接的爆炸式增长带来重大机遇，企业开始意识到，这一转型要求它们的网络基础设施以及管理和分析数据的能力发生彻底改变。通过促进网络基础设施创新，管理基础设施，并分析数据以获得行之有效的洞见，我们正在引领这一转型。

思科旨在将被动排障转变为主动排障，并将排障时间从数天缩短至数分钟。为了实现这个目标，我们将把网络中的每个设备视为一个传感器和一个分布式数据处理网元。通过从网络边缘设备采集数据，并将处理设备靠近数据源，我们能够以线速进行性能分析，从而通过机器学习获得行之有效的洞见。

凭借业内最大的装机量和定制 ASIC 解决方案，思科具备独特优势，能够设计出专为分析而优化的软硬件。融合有线和无线的单一网络意味着网络边缘处的智能可帮助您在几秒内解决问题（无论它们是否发生在网络边缘），而且随着时间的推移，能够在潜在问题发生前消除这些问题。这将帮助 IT 部门履行未来所需的网络和应用性能 SLA（服务等级协议）。

© 2016思科和/或其附属公司版权所有。保留所有权利。

结束语

由于如此之多的因素依赖于网络边缘，无线和有线 LAN 和 WAN 的商品化将带来风险，从而有可能产生安全漏洞、降低效率和收入、丧失机遇、降低可见性。思科的网络边缘可让企业超越基于标准的现成方法，为他们提供智能，从而帮助他们以更快的速度创新、降低风险和复杂性，并控制风险。该方法可让企业实现以下目标：

- 借助固若金汤的第一道防线保护企业业务。
- 充满信心地向目标受众交付应用。
- 为身处任何地方的员工提供无缝体验。
- 与客户互动，开辟新的收入来源。
- 更好地管理物联网设备，并优化物理环境。
- 最佳地了解企业现状。

更多信息

详情请访问 Cisco Unified Access™ Technology 网页：
http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

© 2016 思科和/或其附属公司版权所有。保留所有权利。思科和思科徽标是思科和/或其附属公司在美国以及其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL:www.cisco.com/go/trademarks。文中提及的第三方商标均归属各所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合作伙伴关系。(1110R)

C11-737691-01 11/16