謀
RESEARCH
社交媒体影响与洞察

2016年10月

助力企业获取竞争优势

高性能网络边界

白皮书

编写：
Zeus Kerravala

ZK Research
Kerravala Consulting
旗下部门

作者介绍

Zeus Kerravala 是 ZK Research 的创始人兼首席分析师。Kerravala 通过提供战略建议与指导帮助客户适应当前与长期商业环境。他为以下客户提供研究与洞察：最终用户、IT 与网络经理、IT 硬件、软件与服务供应商以及计划对他所覆盖的公司进行投资的金融界成员。.

导言：当今企业均以网络为中心

数字化转型正在以前所未有的速度改变商业格局。已快速接纳数字化转型的企业成为了各自市场的领导者，相反，没有转型的企业则被进一步拉开差距。ZK Research 的研究表明，数字化企业的利润比未进行这一转变的公司高出 64%，因此数字化转型成为 IT 与企业领导者的首要工作。

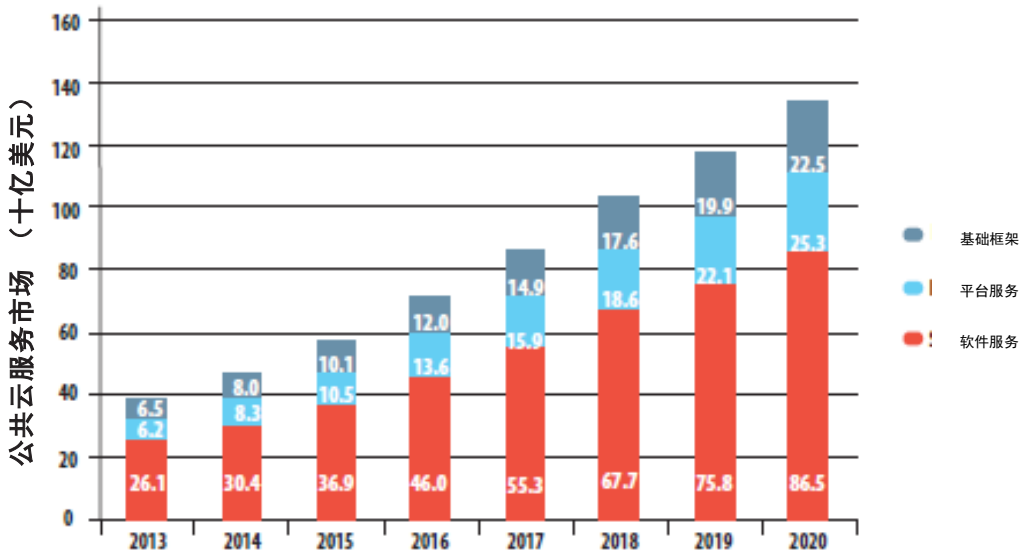
与之前的其他重大转型一样，数字化技术的发展需要新技术的支撑。互联网时代作为最近的一次商业转型，是由低成本个人电脑、Windows 操作系统、浏览器的出现和家庭宽带的发展所共同推动的。

数字化时代将由一系列新兴技术所领导，包括云计算、移动服务、物联网（IoT）、大数据和协作等。所有这些技术看似毫不相关，但却有一个共同点 —— 它们都以网络为核心，也就是说网络在成功部署上扮演了关键角色。比如云服务正在爆炸性增长（附录 1），但用户需要优质的网络服务获得良好的云体验。

多年来，许多专家已预测网络将成为一种商品。在此背景下，购买最低成本的产品将成为最佳选择，因为各供应商之间的差别微乎其微。这一趋势也发生在 IT 的其他领域，比如个人电脑等，因此有人推测网络行业也将朝着这个方向发展。

的确，通用型交换机的成本低于增强型交换机，但交换机成本之间的比较不应只限于价格上的比较。

附录1：云服务正在快速增长



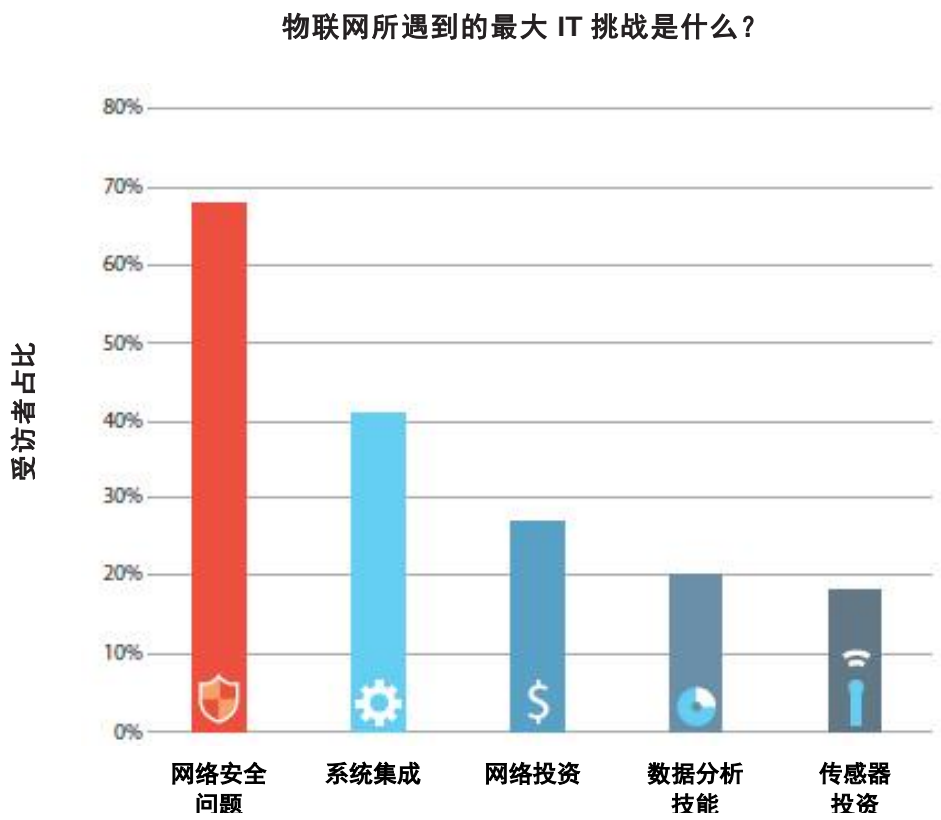
ZK Research 2016 年全球云服务预测

实际上，ZK Research认为通用型交换机最终将给企业产生更高的成本，原因如下：

网络安全风险： 企业所有有价值的数据都能通过网络访问。因此，如果没有采取合理的预防措施，就很容易遭到黑客的攻击。如今，每一台连接网络的设备都能被渗透。网络安全团队曾经将代理放在公司的个人电脑上来保护终端。现在，IT需要应对个人移动设备与物联网终端的涌入，因此已经很难通过代理提供安全保护。由于大部分物联网终端不具备运行代理的能力，因此物联网设备面临着重大挑战。此外，ZK Research 2016年物联网调查发现，在受访的IT人员中，有78%表示自己无法确定物联网设备是否已经与网络连接。这就是网络安全性是物联网部署的首要问题（附录2）的原因所在。

停机时间成本：通用型：交换机的价格一般比增强型交换机低并且不具备相同的数据恢复能力。在当今的数字化世界，所有设备都连接在一起，因此停机会给公司造成经济

附录 2： 物联网部署问题



ZK Research 2016 年网络购买意向研究

IT领导者必须将网络边缘视为一项战略资产而非商品，并且选择一家鼓励创新而非鼓励降低成本的供应商。

损失。ZK Research计算了各个行业的平均停机成本，结果为每小时170万美元。即便是正常运行期间发生的一次小规模异常事件，也能立刻抵消通用型交换机所节省的所有成本。

不良用户体验成本：企业花费几十亿元开发新的技术，目的是提高用户的效率。根据ZK Research的计算，用户因应用性能不佳会平均损失14%的效率。通用型交换机在高负荷下也无法正常运行，并且将对用户的效率造成直接影响。

机会错失成本：数字化转型是一个长期的过程。企业必须不断收集数据并且通过分析数据来完善自身的竞争策略。网络边际能够提供大量有关用户、设备、应用和其他上下文信息的数据。通用型网络设备不具备能够为企业提供相关洞察的衡量与监测能力。

此外，网络的商品化会逐渐阻碍创新。网络产品的制造商将使用成本最低的现成组件并且削减工程成本。理论上，如果所有产品都没有区别，那么唯一的竞争优势将是价格，这会进一步延缓创新。

但这一理论已被证明是错误的，并且网络选择的重要性更甚于以往，尤其是在边界——因为这是用户、应用与设备的连接点。IT领导者必须将网络边界视为一项战略资产而非商品，并且选择一家鼓励创新而非鼓励降低成本的供应商。

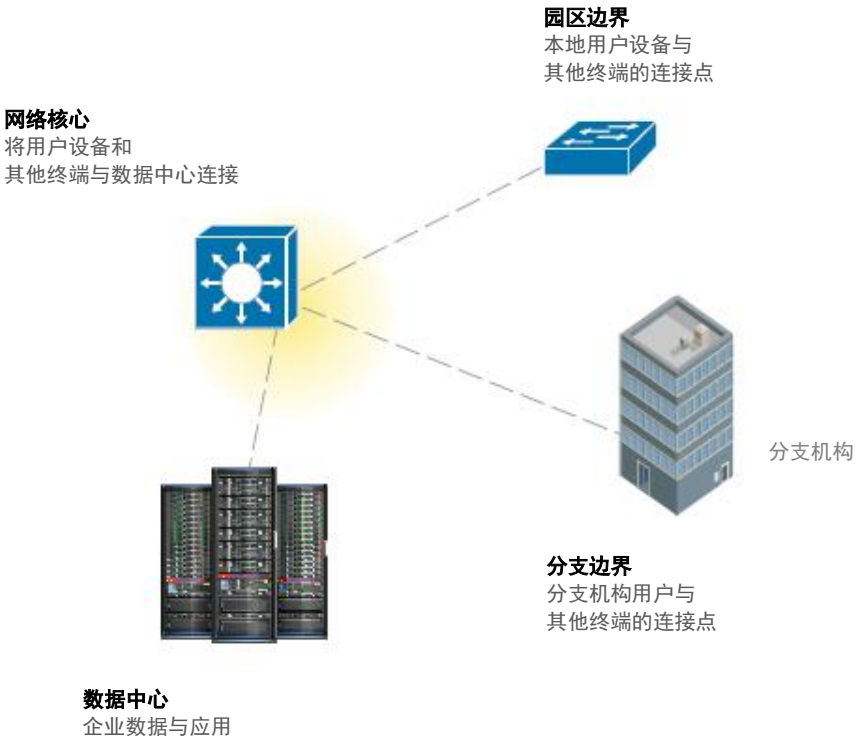
第二章：了解网络边界的角色

非网络工程师常常想方设法地了解网络的运行方式。网络看起来像是一个整体，但实际上是由多个具备特定功能的层级组成（附录3）。

数据中心与网络核心至关重要，并且主要是为了以最快速度将数据流从一个地点移动到另一个地点而建立的。十年前，网络边际主要将个人电脑和打印机连接到公司网络。但数字化转型已经使由园区边界与分支边界组成的网络边界比以往更加重要。以下是如今网络边界的功能：

首个网络安全强化点：根据ZK Research 2016年网络安全研究，80%的网络安全漏洞出现在网络边界内。这对网络安全策略产生了深远的影响，因为企业的防火墙无法抵御网络安全威胁。网络边界是实施和验证策略的最佳地点，这是因为它不会限制企业获取用户必须与之连接的资源。

附表 3：网络层的角色



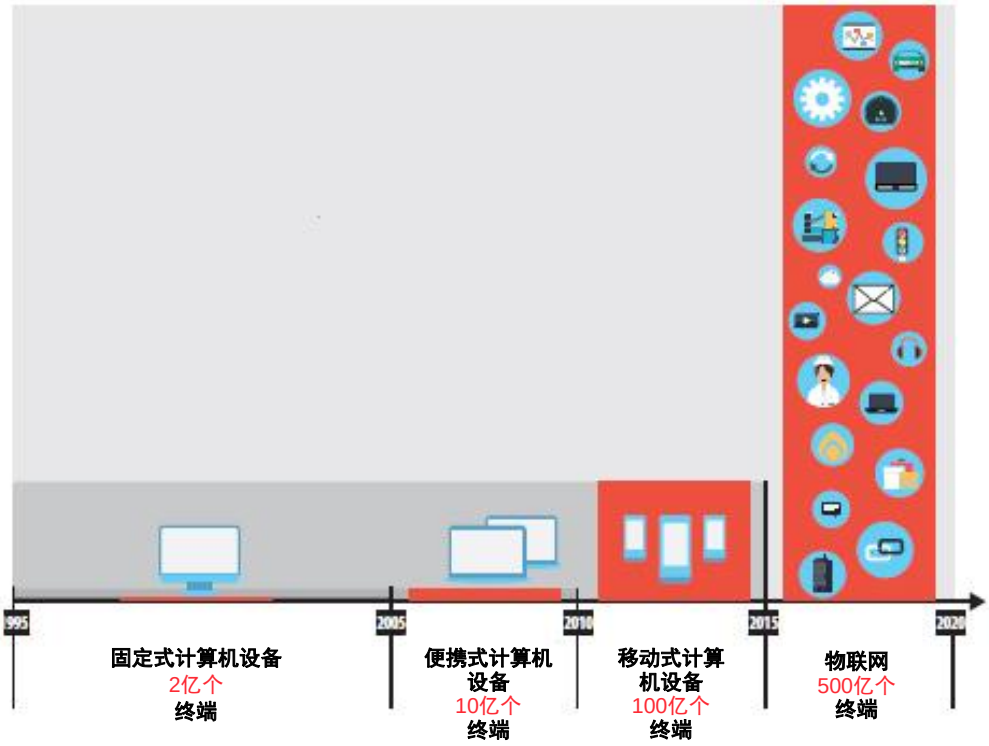
ZK Research，2016 年

因为这不会对用户需要连接的资源的访问加以限制。设置在边际的网络安全策略可以阻止大部分内部威胁，并且在出现漏洞时防止威胁横向扩散。

物联网的基础：ZK Research预测，从现在到2020年期间，联网终端的数量将呈爆炸性增长（附录4）。随着物联网连接在IP周围集聚，网络边际成为医疗系统和LED照明系统等设备的连接处。除了连接之外，许多此类设备还将通过以太网供电（PoE）通过网络获得电能。如果网络边界没有合适的功能，那么企业可能无法实现物联网投资回报的最大化。

应用性能的优化：无论位于公司数据中心还是位于云端，所有企业应用都必须通过网络边界。应用在网络边界可以进行优先级排序，从而防止实时或关键任务型应用运行缓慢。

附录4：物联网创建了数百亿个网络边际连接



ZK Research，2016年

改善客户体验：企业的首要数字化任务之一创造差异化客户体验。数字技术可以改变客户的购物方式、学生的学习方式和医生的诊疗方式等。但性能不佳的边际会对面向客户的服务产生严重的影响，从而影响客户的忠诚度。ZK Research的一次近期调查发现，三分之二的“千禧一代”在过去12个月内因不良的体验而更换供应商。

商业附加值：网络边界是获得业务新洞察的最佳平台。所有数据流都会通过网络边界，因此企业可以轻易地获取和分析数据流。通过有关用户、设备、应用与威胁的信息，企业可以比竞争对手作出更快更好的决策，并且长期处于领先地位。

第三章：启用高性能网络边界时需要考虑的问题

在选择网络供应商时，既有低成本的通用型产品，也有价格高、功能齐全的增强型产品。

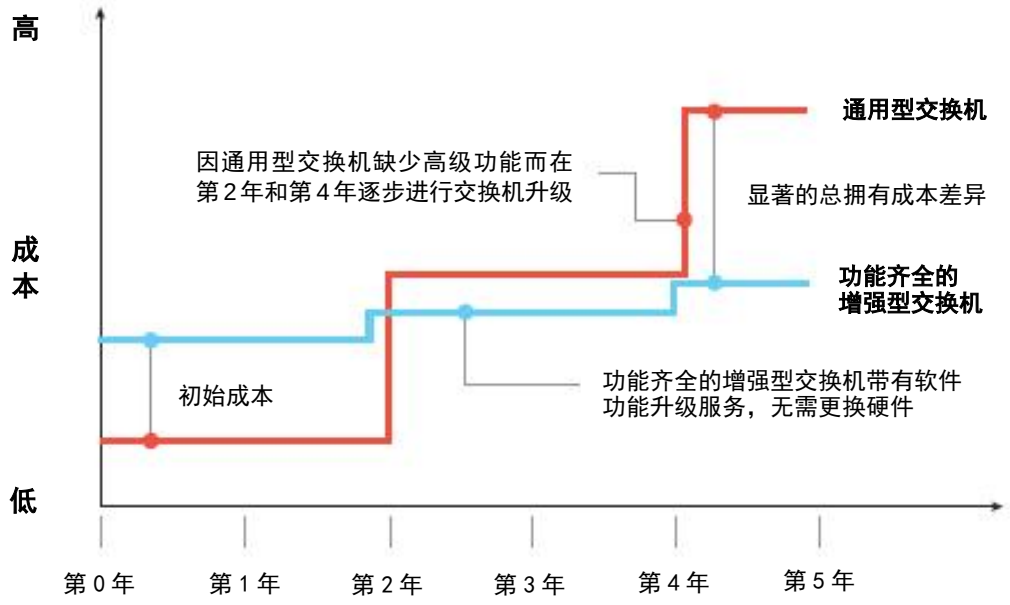
由于价格、功能范围、可管理性以及网络安全性的巨大差异，很难对这些产品进行评估。以下是企业在启用高性能网络边际时应该考虑的几个关键问题。

五年中的总体拥有成本（TCO）是多少？

由于企业会继续部署数字技术，因此企业应该转变对网络的看法，并且将网络视为数字化的基础。正确部署的网络可以为网络边界提供丰富的服务。但要实现这一点，就必须能够在不中断业务的情况下轻松适应不断变化的商业环境并且支持高级集成功能，这将产生巨大的长期总体拥有成本优势。

在评估网络边界上的产品时，企业应着眼于五年后的总体拥有成本，这段时间相对于一轮更换周期。正如附录5所示，商品级产品生命周期初期的总体拥有成本看似较低，但由于企业需要新的服务并且逐步进行升级，因此需要更加频繁的更换通用型交换机，这会使总体拥有成本大幅增加。另外，如果选择的长期产品不当，则可能导致不必要的停机时间、失去商机和设备管理的不一致。某首席技术官将功能齐全的交换机比喻成一把瑞士军刀：虽然自己不知道什么时候需要其他功能，但可以肯定的是，自己在需要时就能获得这些功能。

附录5：相比通用型交换机产品，功能齐全的网络交换机能够带来显著的总体拥有成本优势



ZK Research，2016年

数字化转型需要不断的变革，因此了解网络在创新过程中的角色十分重要。

数字化转型需要不断的变革，因此，了解网络在创新过程中的角色十分重要，无论是部署在未开发领域还是现有网络的更新都不例外。该问题可以分为三个主要类别：创新、安全与灵活性。

网络如何促进创新？

网络不仅要提供连接，还需要实现数字化活动，这引发了以下与创新相关的问题：

1. **该解决方案能否保证可用性以及服务的一致性？**

灾难性的网络故障已不复存在。保证网络的正常运行相对容易，难的是在网络组件发生故障时保证最终用户的体验不受影响。如今的网络需要能够根据这些故障自动调整并且确保性能不受影响。IT还需要能够了解网络异常情况和趋势，从而确定其潜在影响。可通过遥测数据快速发现和解决应用问题。

ZK Research 2016年WiFi运营调查发现，近50%的受访者至少花费25%的时间解决WiFi问题。企业需要审视该如何大幅缩短这一时间。

2. **该解决方案能否快速适应不可预测的新需求？**

网络需求的变化速度非常快。因此，企业需要不断部署能够自动根据客户快速扩展与信号质量变化调整WiFi网络的解决方案。

3. **该解决方案能否改进设备性能和电池寿命？**

移动设备是用户访问信息的主要方式，而网络必须具备能够理解所连接的设备并且通过调节在新移动世界提供最佳体验的内置智能。漫游的优化将减少电池的耗电量并且保证用户与移动网络的连接。

4. **网络能否提供准确的内部与外部元素洞察？**

得数据者得天下。网络是宝贵的数据来源，能够提供关于用户、设备、应用、甚至是威胁的见解。但该数据只有在准确的前提下才有价值，而准确性则来源于细致化。相比带有定期数据点的五米级视图，数据点更多的一米级视图更能反映实际发生的情况。目前，正在通过360°客户、网络或应用三角剖析等高级网络服务创建新的客户使用实例和体验。正是这种视图通过提供可执行的业务数据帮助IT部门占据一席之地。

数字化企业需要通过灵活的IT基础比其他竞争对手更快应对市场变化。

5. 该解决方案是否已经能够支持用户不常连接的新物联网设备？

该网络边界可以提高终端的可用性。许多连接该网络的设备，比如物联网所使用的设备等，通过一个以太网供电（PoE）连接实现这一点，这使其成为交换机故障时的单一故障点。这些设备所连接的交换机需要具备能够最大程度减少停机时间的数据恢复功能。此外，通过交换机为设备供电的需求正在增加，并且交换机需要提供足够的功率才能满足这一需求。

该网络能提供数字化时代所需的灵活性吗？

数字化企业需要通过灵活的IT基础比其他竞争对手更快应对市场变化。但IT的灵活程度取决于最不灵活的组成部分，通常就是网络。网络边缘必须与IT的其他组成部分一样灵活，并且不能增加成本和复杂性。为了了解是否如此，企业必须提出以下问题：

1. 该解决方案能否一致地确定从云到最终用户的应用优先顺序？

通过“孤岛式”方案确定应用服务的质量会导致回报的减少。企业发现通过一致的方式对待来自从云、私人或公共网络到最终用户等的应用对于保持统一、优质的用户体验至关重要。

2. 该解决方案能否帮助几乎无法获得本地支持的新分支机构或部门建立网络？

为偏远地区提供网络搭建“上门服务”既费钱又费时。数字化企业的运营节奏很快，快到等不及让工程师前往现场为新的分支机构、业务部门或职能部门进行接线和配置。因此，即插即用功能与当天配置成为了加快部署和降低成本的关键。

3. 能否在不进行“叉车式”升级的情况下添加新功能与标准？

无需频繁使用新设备代替旧基础设施就能添加功能可以最大程度地减少业务中断并且显著节约成本此外，网络经理需要在不干扰用户的前提下进行软件升级，从而避免影响工作效率。为了满足新的业务需求，必须投资于能够快速、轻松扩展功能的解决方案。

4. 能否轻松地转让许可证？

企业需要能够在不购买新的软件许可证，从而产生附加成本的前提下更新硬件。避免软件许可证与硬件挂钩十分关键，其原因是企业因快速增长的需求而需要频繁地更新其网络基础架构。

威胁检测仍是企业面临的一大挑战。

能否通过该网络提高安全性和最大程度地降低风险？

该网络可以成为一个巨大的优势，不仅能够为用户提供访问权限，而且还能根据深层次的背景验证用户的行为。威胁探测仍是企业面临的一大挑战。ZK Research 2016年网络安全调查发现，确定漏洞的平均时间超过100天。企业需要找到能够在几小时内而非几天内探测到威胁的方法。为此，可以提出以下问题：

1. **该解决方案能否通过基于软件的方案根据逻辑对数据流进行分割并且在确认新风险时自动调整规模？**

由于客户希望能够在安全区域隔离用户与应用流量，因此网络分割正处于上升趋势。在处理小型部署中的访问控制列表与半径时，最直接的方法时保证员工、访客、承包商和物联网只能访问他们所需要的内容。但随着用户与设备数量的增加，管理此类列表已不再有效。新的数字化企业正在寻找基于用户类型与角色对数据流进行逻辑分割的方法，从而能够快速调整访问政策并且根据风险等级进行自动调整。

2. **该解决方案能够在网络基础架构中加入网络安全功能，从而探测访问点、内核、WAN与分支上的内部与外部威胁？**

ZK Research 2016年网络采购意向研究发现，78%的受访者不确定IT企业是否完全知晓所有与网络连接的物联网设备。网络是自动探索物联网终端的宝贵资产，而且网络可以通过数据流分析监控用户与物联网的活动。任何正常行为上的变化都有恶意行为或存在漏洞的嫌疑。

3. **该解决方案能否通过分析数据流修复威胁所产生的影响？**

每家企业都会遇到威胁，但这些威胁所产生的瞬间影响可能会使一家企业陷入瘫痪。企业需要放眼于传统的威胁检测与分析技术之外。企业可通过网络数据确认攻击的根源和所在位置，从而快速进行修复。网络边缘可以在出现漏洞时，快速映射数据流，以便进行进一步的检查。

4. **该解决方案能否在网络出现新的威胁前统一更新有关新威胁的信息？**

实施降低风险的应对措施意味着在恶意活动出现在网络前没有任何事先的通知。企业可以通过不断从企业外部了解新的威胁并且自动更新系统以预防出现漏洞来占得先机。网络与安全专业人员需要将被动的网络安全策略思维转变为主动减少出现漏洞的风险。如果出现漏洞，采集数据和进行分析的工具可以快速找到恶意软件并且自动进行网络变更，从而最大程度地缩小受影响的范围。

硬件只占网络总运行成本的约20%，而运营成本则占到50%。

应该如何管理网络？

这个问题往往被许多企业所忽视，但它确实最重要的问题之一。人们对于网络设备的成本十分关注，但硬件只占网络总运行成本的约20%，而运营成本则占到50%以上。

以前，我们通过命令行界面对设备进行逐一管理。当时，整个网络的变更过程费时费力。ZK Research 研究指出，进行全网络变更的平均时间达到四个月，这对于数字化企业而言实在是太慢了。此外，人为失误占网络停机时间的35%，是造成中断的最大原因。数字时代的网络管理必须改变。网络管理者应寻求 具备以下能力的解决方案：

统一的有线与无线管理

全网络与集中设备配置

丰富的图形界面，使低级别的工程师能够进行基本的配置变更

能够在需要时恢复配置变更

同时具备企业内部与云端管理能力，让客户能够选择管理模式

第四章：总结与建议

数字化趋势已提高了网络的价值。人们不再认为网络是低价值的资源或“商品”。相反，网络边际是用户与应用和内容进行连接的地方，因此具有高度的战略意义并且成为了一项竞争优势。IT和企业领导者必须考虑发生在网络边缘的所有活动，并且对商品级基础架构与思科等供应商的高级网络进行考量。

低成本网络设备在一开始可能看起来极具吸引力，但随着时间的推移，它们会带来较大的网络安全风险，削弱企业监控和优化应用性能的能力，并且几乎无法实现流程的自动化。这些对于数字时代的成功与否至关重要，因此企业必须就网络边缘作出正确的选择并且将其作为数字化转型的基础。鉴于此，ZK Research提出以下建议：

在购买网络设备时，考虑总体拥有成本而非购买成本。

ZK Research 的数据显示，网络硬件只占网络总运行成本的约20%，而运营成本则占到50%。在硬件上所节约的几个百分点可能会显著增加运营问题，从而提高总体拥有成本。

分析网络对您的企业的影响。

为了正确了解网络边缘的影响，需要清晰地了解企业计划中与计划外的停机时间。任何停机或性能问题都会降低工作人员的工作效率并且“赶跑”客户。安全漏洞可能会对品牌造成巨大损坏，甚至导致法律诉讼。

制定面向未来的网络边界决策。

了解企业目前所使用以及未来将要使用的应用与通信服务（视频、IP语言、消息收发、移动服务、物联网等），并且选择能够为您提供最佳整体解决方案的供应商，为未来将要建立的数字服务与应用打下基础。

联系方式
zeus@zkresearch.com
手机：301-775-7447
座机：978-252-5314