BLACK & WHITE PAPER

451 Research | Advisory

MANRS项目研究报告

2017年8月

委托人

Internet Society

©COPYRIGHT 2017 451 RESEARCH. ALL RIGHTS RESERVED.

关于本文

黑白白皮书是一项基于基础研究调查数据的研究，它通过实际从业人员的“现场”经验和观点来评估关键企业技术领域的市场动态。在做。

关于451研究

451 Research是一家杰出的信息技术研究与咨询公司。我们以技术创新和市场破坏为核心，为数字经济领导者提供重要见解。超过100位分析师和顾问通过联合研究，咨询服务和现场活动向北美，欧洲和全球1000多个客户组织提供了这一见解。 451 Research成立于2000年，总部位于纽约，是451集团的子公司。

©2017 451 Research，LLC和/或其关联公司。保留所有权利。未经事先书面许可，严禁以任何形式全部或部分复制和分发本出版物。内部和外部分配使用条款应受您与451 Research和/或其关联公司的服务协议中规定的条款约束。本文包含的信息均来自认为可靠的来源。 451 Research不保证此类信息的准确性，完整性或充分性。尽管451 Research可能会讨论与信息技术业务有关的法律问题，但451 Research并不提供法律咨询或服务，也不应以此为由解释或使用其研究。

451 Research对本文中所包含信息的错误，遗漏或不足之处不承担任何责任。读者对选择这些材料以达到预期效果负全部责任。本文所表达的观点如有更改，恕不另行通知。

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 207 426 1050

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

执行摘要

建立相互同意的路由安全规范（MANRS）项目的目标是提高全球互联网的安全性和可靠性。在MANRS成立三周年之际，已经开展了一项研究，以更好地理解互联网服务提供商和项目周边更广泛的企业社区的态度和看法。本报告记录了这项研究的结果，并对MANRS项目的状态和未来提供了建议和观点。它包括概述MANRS参与收益的服务提供商和企业用例。

对研究的解释产生了一些有趣的结果，与项目参与者和项目委员会相关。这项研究的关键点是：

- 尽管MANRS本身在企业中并不为人所知，但其属性却受到高度重视。
- 企业对MANRS的工作寄予厚望。
- 企业对MANRS的理解可以转化为服务提供商收入的增长。
- 现有的MANRS动作包含一组合理的控件。
- 有一些选项可以扩展某些提供商的MANRS操作。

研究表明，MANRS项目具有巨大的未实现潜力，企业利益应是促使更多服务提供商参与的强烈动力。市场教育在克服许多供应商面临的运营惯性方面可能特别有效。

项目说明

开展该研究项目是为了更深入地了解MANRS取得的进展，包括在企业和服务提供商社区中的知名度和感知，并探索可采取的行动来提高参与度和认识。对参与互联网服务合同的服务提供商和企业IT人员分别进行了离散研究。这些研究确定了他们对MANRS的意识，并深入研究了实施的各个方面以及MANRS行动的感知价值。分析研究回应，评估两组之间的相关性和差异。本报告详细介绍了发现和结论。

除本报告外，还创建了两个用例，一个针对企业，一个针对服务提供商。每个研究对象都研究了特定人群更多参与MANRS的好处，并依赖于研究中收集的数据。

研究方法论

深入了解信息和路由安全等领域的理解可能很复杂。为该项目进行的研究试图比较两个离散但相互联系的社区的结果。期望服务提供商可能会接触到MANRS，理解水平很重要。对于企业而言，人们期望的是风险敞口会更有限，更重要的方面是围绕MANRS特征调整价值观。因此，尽管研究是在一个共同的基础上进行的，但对于每个目标群体而言，所使用的问题集具有不同的重点。最终研究由一个独立的组织进行。

服务提供者研究的范围比企业研究的范围更窄，深度更深。在最初由10个已知对MANRS项目有所了解的提供商中，对问题集进行了测试。通过不限成员名额电话采访进行。最初小组访谈的结果未包括在研究中，但用于形成每个后续小组的最终问题集。最初的小组地域不同，代表来自亚洲，欧洲和北美。正式研究的重点是对25名随机选择的服务提供商员工进行电话采访，对这些员工进行筛选，以确保他们参与路由基础设施运营的决策并在其组织内担任管理职位。这个群体几乎完全来自北美，组织规模平均分布，员工人数中位数为2500至4999。

企业用户研究是通过网络表格进行的，从250名受访者中随机选择一组，对这些受访者进行筛选，以确保他们是参与互联网服务采购和承包的IT管理人员。公司规模不得超过1,000名员工，以针对对互联网服务有更重要要求的人员。受访者主要来自北美，广泛分布于各个行业。制造和专业服务组织的代表最强，每个垂直领域占小组总数的14%。医疗保健，电信和零售紧随其后，其他行业则以个位数百分比增长。组织规模中位数也为2,500-4,999。

研究数据可提供研究受访者的完整受众特征。

结果概述

这些研究证实了我们的期望，即MANRS能见度对于企业和服务提供商都有改善的空间。他们还透露，服务提供商低估了客户在其广泛的安全定位中所享有的价值。一个出乎意料的发现是企业在多大程度上将安全视为自身的核心价值。这可能是由于媒体对安全事件的覆盖范围扩大导致意识增强的结果，但也可能反映了企业间IT定位的日益成熟。

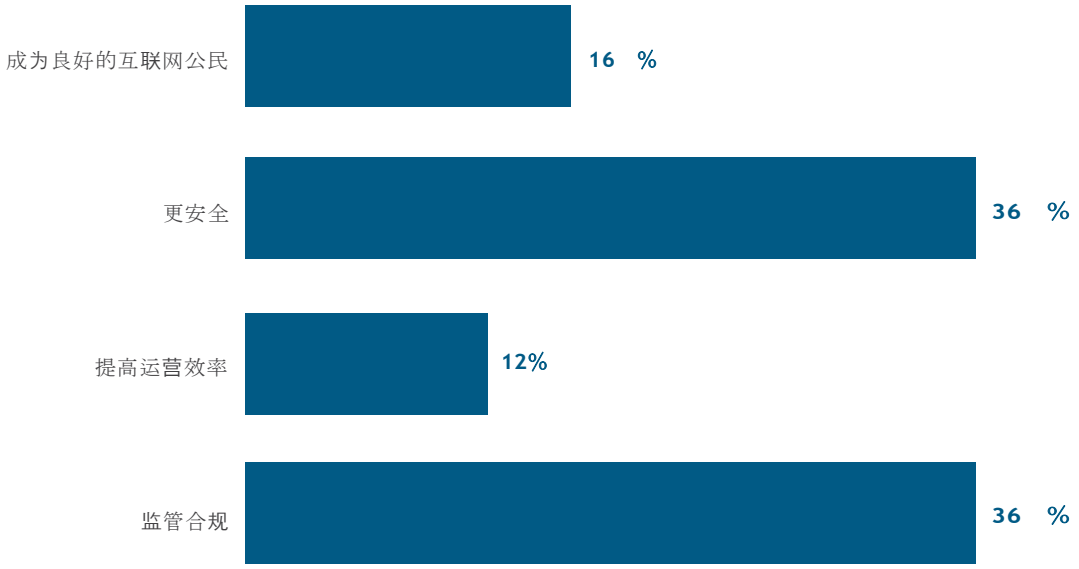
服务提供商研究详情

服务提供商的研究证实了初始评估中已经表达的许多担忧。这些担忧可能并不完全合格，因为只有一个受访者表示他们已经实施了MANRS的大部分行动，因此，接受调查的服务提供商在MANRS实施方面没有直接经验。这就是说，调查基础的看法可以合理地代表MANRS项目希望达到的服务提供商社区，即尚未参与的社区。

几乎三分之一的受访者从未听说过MANRS，而略微更多的受访者充分了解了该项目。这意味着对实施工作的估计是推测性的。有趣的是，没有一个受访者担心MANRS会增加运营力度或复杂性，而超过三分之二（68%）的受访者认为可以减少运营或复杂性。人们常常认为，新的，未尝试的技术需要付出更多的努力，因此，这对服务提供商的期望是一个积极的信号。就是说，超过一半（52%）的受访者中度关注MANRS实施造成的中断——24%的受访者不关注，而同样数量的受访者则非常关注，表明运营可能会中断。

采用MANRS后，对罪责的影响中等，为60%，但28%的受访者表示完全没有担忧。这很可能是由于与不同服务提供商的客户互动方式不同。那些已经证明自己具有担保权益的人的关注点较低。

图1：实施原因



资料来源：451研究报告：MANRS感知与行动，2017年7月

MANRS的决策流程毫不奇怪。虽然有64%的受访者表示，技术管理将推动采用，但只有4%的团队有权实施技术管理；相反，有80%的服务提供商需要中高层管理人员的批准（每人40%）。如果组织中的实施命令没有明确传达，这将给企业带来挑战。

实施动机也与企业成果不符。尽管有97%的企业考虑在RFP中纳入MANRS法规遵从性，而13%的企业将其视为锁定要求，但服务提供商调查结果反映出人们缺乏这种重要性的理解。如果MANRS要求作为RFP的一部分，则只有12%的服务提供商会计划实施。它将刺激对价的72%，对16%没有影响。这些响应可视为推测性的，因为在提供商选择中几乎没有使用MANRS合规性。我们的估计是，如果在RFP和招标过程中有MANRS遵从经验，应对措施将更倾向于实施。

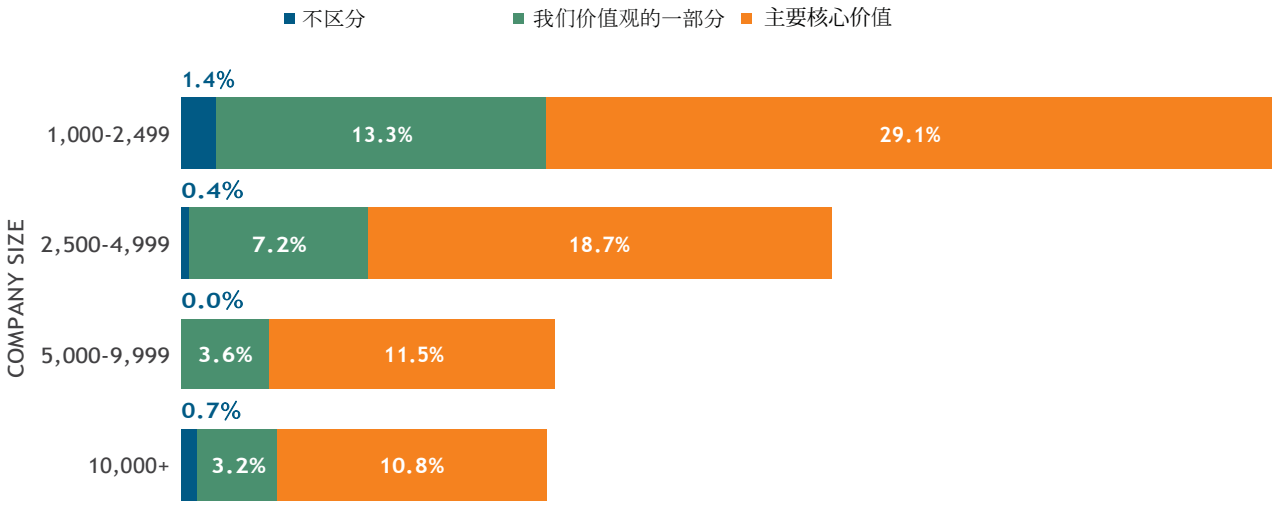
服务提供商研究影响

MANRS在服务提供商社区中持谨慎的热情。面对客户可能不重视MANRS的期望，这令人振奋。但是，要增加实施的动力，就需要与教育之间弥合知识差距，而且双方都必须有扎实的故事。MANRS可以使企业在服务提供商上花费更多，这是高层管理人员希望听到的信息，企业重视技术团队渴望推广的安全细节。企业对将MANRS纳入RFP和招标流程的兴趣应该只会增加这种潜力。

企业研究详细信息

研究的企业部分检查了安全隐患，并探讨了与MANRS价值观的一致性。数量惊人的企业受访者（71%）表示，安全是其组织的核心价值。对按公司规模划分的细目分类评估表明，小企业对安全作为其主要价值的一部分有过分关注。在企业研究的许多响应中，这种关注水平仍然存在。

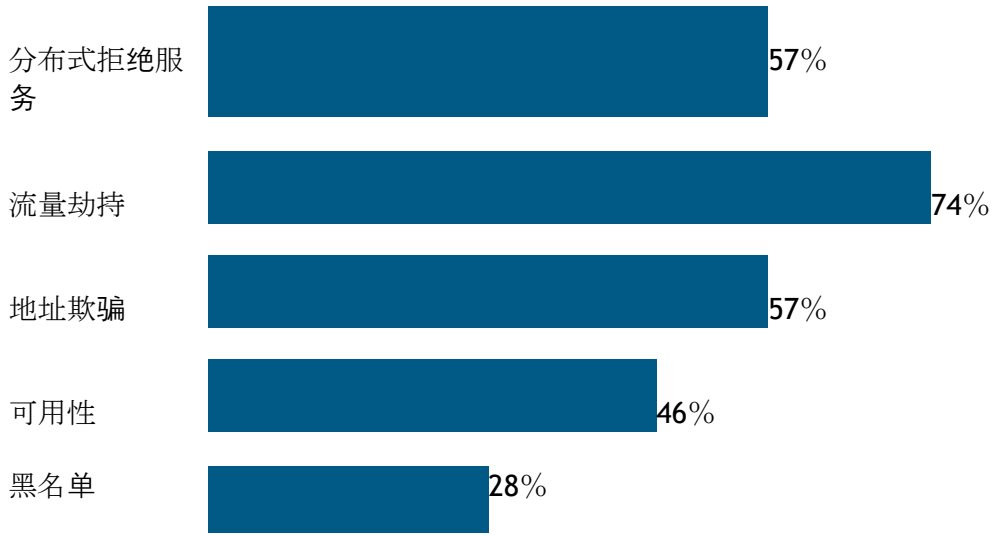
图2：总体安全态势的重要性



资料来源：451研究报告：MANRS感知与行动，2017年7月

当检查安全隐患类型时，流量劫持名列前茅。这可以看作是另一项确认，即受访者对互联网服务的关注可能会增强人们对MANRS希望解决的问题类型的认识。这对他们的期望是个好兆头。

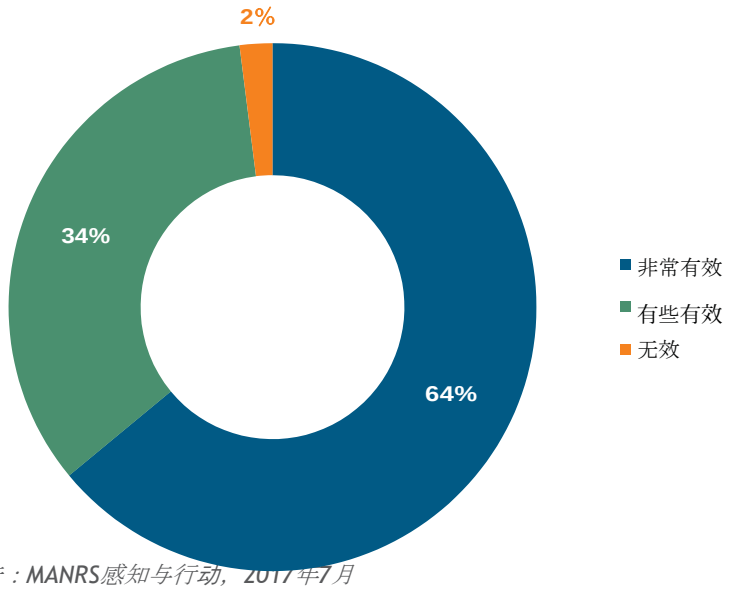
图3：互联网安全问题



资料来源：451研究报告：MANRS感知与行动，2017年7月

除了这些担忧之外，人们有信心MANRS行动可以有效解决这些问题。这对MANRS价值观和叙事条目中表达的期望做出了一系列积极回应。

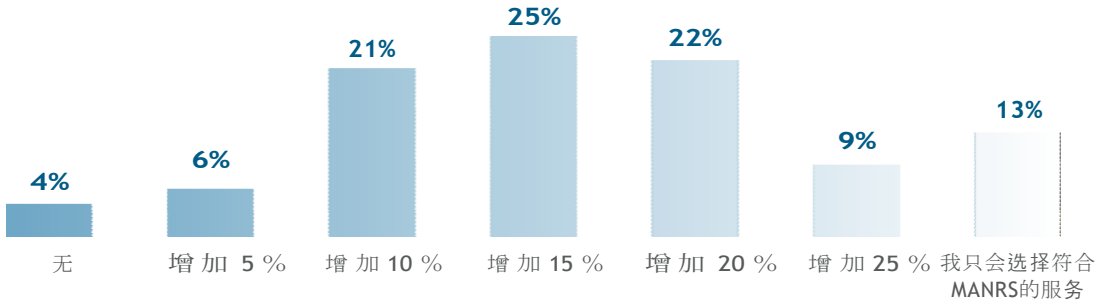
图4：MANRS有效性



资料来源：451研究报告：MANRS感知与行动，2017年7月

最重要的是，企业表现出愿意为自己认为有价值的东西付款。在确定将支持MANRS合规的价格上涨时，中位数为15%，比通常视为商品服务的溢价高得多。

图5：MANRS的企业定价溢价



资料来源：451研究报告：MANRS感知与行动，2017年7月

此外，有13%的受访者表示，如果有竞争优势，他们只会选择符合MANRS规定的供应商。

企业研究影响

企业结果表明，参与MANRS的服务提供商有很大的机会。企业决策者正在寻找MANRS赋予参与者的各种价值观念。存在切实有效的增加收入和竞争改善的机会。安全是企业关注的重点领域，而在越来越难以区分提供商时，MANRS可以成为其IT基础设施关键部分的信任标志。

用例

该研究项目的两个用例解决了MANRS参与对服务提供商和企业组织的好处。它们作为单独的文件提供，此处包含以供参考。

建议

研究发现，MANRS项目目前有更多的采用潜力，以及为服务提供商社区某些部门扩展该计划的选项。这项研究的主要发现可以归纳如下：

- MANRS在企业中的意识可以推动服务提供商的参与。
- 围绕企业价值观的服务提供商教育可以推动参与。
- 可能需要某种程度的监管参与。

通过与参与服务的供应商建立伙伴关系，可以提高MANRS对企业的认识。企业报告称，他们将服务提供商视为技术权威的来源，并且，作为促销的一部分，提供商在竞争地位中获得直接利益。通过对等组织可以为企业提供其他途径，例如用户组和在线社区。这些也是可以与服务提供商合作探索的途径。以安全为中心的论坛最具潜力，例如：

- ISACA -提供安全和监管认证以及社区的非营利组织。
- RSA会议-可以提议MANRS会议的安全性会议。
- （ISC）2 -安全认证非营利组织，也举行安全会议。
- InfraGard -由联邦调查局赞助的美国协调组织，致力于基础设施保护。

进一步教育服务提供商企业在MANRS中看到的价值水平非常重要。这里显然存在偏差，而MANRS在企业决策者眼中提供的差异对提供商有利。鉴于社区规模较小，直接推广以及针对性活动都可以有效。运营商团体和特定于提供商的会议可以包括：

- NANOG，RIPE，AfNOG，APRICOT和其他运营商集团
- HostingCon -专注于服务提供商的年度会议

服务提供商和企业都认识到一定程度的监管参与将成为MANRS采用的强大驱动力。在这方面，我们建议您谨慎行事，因为政府互动中响应的性质和方向可能难以管理。一种有效的途径是与审计师和行业组织合作，促进符合政府要求的活动。美国国家标准研究院（NIST）和欧盟网络和信息安全局（ENISA）的努力为改善企业安全提出了建议。解释和实施这些建议的任务通常由审计师和安全服务公司负责。努力将MANRS纳入其实践中可能是在不承担政府直接行动风险的情况下利用监管任务优先级的一种实际方法。 ISACA COBIT框架是另一种可能性。也许还会有与支付卡行业安全标准委员会这样的组织合作的途径，但与MANRS目标受众的联系不太直接。

MANRS的未来可以包括许多扩展其任务的选择。现有的MANRS活动非常适合互联网服务提供商的职责范围。随着越来越多的提供商开始提供增强的安全服务，MANRS可以在这些领域提供指导。服务提供商希望在托管安全服务中满足企业客户不断增长的需求。表示，安全信息和事件管理（SIEM）项目首次与企业端点“安全”，*The 451 Research Voice of the Enterprise (VotE)Information Security study from Q1 2017*

仅略微落后于安全意识计划。这充分表明了企业对运营安全管理的重视。服务提供商可以提供咨询咨询和托管服务，以满足这些需求。

在这项研究中，企业将对流量完整性的关注确定为高度优先事项。据报告，流量路由，拦截和劫持是主要的安全隐患（占74%，其中分布式拒绝服务和地址欺骗分别占57%），而路由验证则是单独问题中的领先MANRS值（32%）。 。这种担忧可能会扩展到基础设施完整性的其他领域。 MANRS可以识别名称空间安全之类的技术，这将由DNSSEC解决。服务提供商虽然依靠域名注册服务商（DNSSEC）来实施域名服务，但它们通常有着紧密的合作关系，可以为希望实施域名服务的企业提供实施服务。这可以增强服务提供商已经开始承担的受信任安全顾问角色。

MANRS还可以帮助定义服务提供商的另一种收入机会框架。许多企业正在将情报源纳入其运营。企业正在寻求提高态势感知能力，并对可以馈送到SIEM系统的运营信息感兴趣。 MANRS动作可能产生的信息和事件流对企业具有价值。反欺骗和路由验证控件通常会生成日志消息，可以将其作为情报源传递。 MANRS项目可以为这些智能馈送定义标准格式，以帮助服务提供商将其与企业客户集成。这可能是与其他组织创建安全信息交换格式的努力。 STIX，Cybox和TAXII在当今许多企业中得到应用，将是有用的起点。作为MANRS的一部分，创建可货币化服务可能是参与的另一个原因。

虽然要大幅提高MANRS的采用率面临挑战，但研究表明，服务提供商的动机与企业的抱负之间存在着牢固的一致性。付出更多努力，将两者结合起来可以为MANRS创造光明的未来。

关于作者

埃里克·汉塞尔曼（Eric Hanselman）是451 Research的首席分析师。他对广泛的IT主题领域有广泛的动手理解，在网络，虚拟化，安全和半导体领域有着直接的经验。他负责协调451个研究学科广泛领域的行业分析。跨技术领域的力量融合正在引发行业的构造转变，包括SDN / NFV，超融合和物联网（IoT）。埃里克（Eric）协助451 Research的客户导航这些湍急的水域，确定其影响以及如何最佳利用其资本。

埃里克（Eric）在20多年来一直与多个领域的部门领导者合作，最近担任虚拟化管理提供商Leostream Corporation的首席技术官。在此之前，Eric为IBM和互联网安全系统提供了安全解决方案。在Wellfleet / Bay网络公司，Sitara网络公司和NEC公司，他参与了许多新技术的引入，从高性能图像分析到IPv6推出。 Eric拥有图像压缩系统专利。他还是电气和电子工程师协会（IEEE）的成员，信息系统安全认证专家（CISSP）和VMware认证专家（VCP），并且经常在领先的行业会议上演讲。他在里德学院主修化学。

附录一：服务提供商-安全带来更好的业务

概述

对于互联网服务提供商而言，要在当今市场中脱颖而出可能会面临挑战。客户通常对提供商之间的功能和性能差异感到困惑，并且可能很难明确表达提供商所提供的价值。在安全领域可能有具体的区分，对企业具有确定的价值，并可能对客户采购和决策流程产生重大影响。路由安全互认规范（MANRS）项目可以为那些能够参与的提供商提供安全熟练程度和社区参与的标志。这种差异可以为提供商增加竞争价值，也可以提高运营效率。 451 Research的一项新研究详细说明了价值所在以及服务提供商如何实现价值。

企业价值

当企业希望选择基础设施合作伙伴时，他们会处理一系列可能难以管理的需求。如果无法确定各种提供商产品竞争方面的价值，那么他们通常会将重点放在定价上。为了使决策点不仅仅是价格，服务提供商需要具备易于识别和区分的质量。451 Research研究表明，服务提供商的安全状况对企业至关重要，MANRS的参与具有价值。尽管MANRS在企业中并不为人所知，但该项目所代表的理念却受到高度重视，对企业买家具有真正的价值。

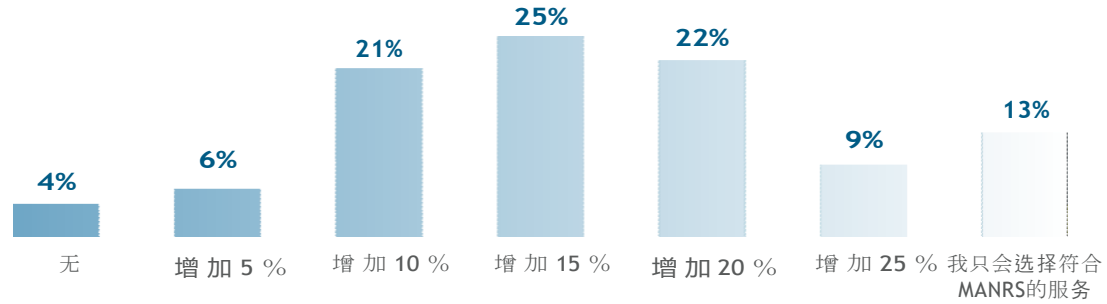
这项研究包括对该项目的简要介绍，然后询问受访者如何看待MANRS参与项目的价值，以及哪些项目指令和成果对他们最有价值。这些估值中的第一个是评估他们愿意为MANRS参与方的提供商的服务花费（如有）的多少。溢价的中值为15%，对于许多买家来说，这是一笔相当可观的商品服务估值。此外，有33%的受访者表示，如果有MANRS参与，他们将使用MANRS作为排他性选择标准。共有97%的受访者有兴趣让MANRS参与RFP和招标要求。

这种估值意味着MANRS的参与可以为服务提供商带来一系列好处：

- 改善RFP和招标过程中的竞争地位
- 增加客户保留率并降低流失率
- 增值服务的机会

所有这些都是服务提供商使用MANRS可以实现的内部收益的补充。服务提供商可以通过与对等方建立更好的通信路径来提高运营效率。它们还具有通过尽早发现客户端和对等端问题来改善安全操作的潜力，并且为互联网社区的整体安全做出贡献具有附加价值。

图1：MANRS企业定价溢价



资料来源：451研究报告：MANRS感知与行动，2017年7月

货币管理

服务提供商可以通过多种方式利用MANRS参与的价值为他们服务：

- 在建议中包括MANRS
- 向客户宣传MANRS价值观
- 提供增值服务

直接利用MANRS的价值和上涨的价格是有问题的。大多数市场的现实情况是，无论购买决策的其他方面如何，都将进行价格比较。参与MANRS可能会有用的是降低赢得合同所需的折扣水平。参与MANRS可用于增加竞争过程中选择的可能性。可以用作淘汰不合格竞争者的手段。研究结果表明，企业热衷于将MANRS作为选择标准。进一步的分析表明，提高竞争地位和减少必要折扣可以使长期收入增加7%。

客户重视MANRS的参与度，服务提供商可以通过宣传其参与度加以利用。通过在向客户和更广阔的市场进行营销和传播时纳入信息和品牌，服务提供商可以在客户认为有价值的领域中留下深刻的印象。宣传MANRS可以使了解的客户了解其提供商具有宝贵的能力，并可以减少考虑更换供应商的可能性。通过以安全为重点的通信和社区建设，可以加强客户联系。451 Research的研究还表明，MANRS的另一个重要组成部分是对客户而言至关重要，而这个更大的社区致力于提高互联网的安全性。

服务提供商可以通过在其产品组合中添加MANRS衍生服务来获得额外收入。反欺骗控制日志活动可用于为客户生成定期报告。这些报告可以作为智能源的一部分，向客户提醒配置错误或潜在攻击。如果适当地自动化，这种类型的服务运营成本低廉，除了可以带来收益外，还可以提供更多的客户绑定。

结论

对于服务提供商来说，参与MANRS项目会带来很多好处。它可以增加客户价值，并有可能增加收入。 MANRS指令是提高运营效率同时有助于改善互联网社区安全的有用指南。客户影响力和内部收益的结合应该足以使提供商成为这个不断发展的社区的一部分。

附录二：企业–加入社区以提高安全性

概述

企业在运行其IT基础设施方面面临许多挑战，最重要的挑战之一就是服务提供商的选择。评估提供商的能力和绩效可能是一个复杂的过程。可以帮助做出此决定的一个因素是提供商参与路由协议相互同意规范（MANRS）项目。 MANRS是一个协作项目，重点在于采取具体步骤增强参与者的安全状况，从而为互联网社区的整体安全做出贡献。通过与属于MANRS项目的服务提供商合作，企业可以跻身于具有安全转发职责的人员的先锋阵地，并加入致力于改善安全性和可靠性的大型互联网社区。

MANRS项目目标

MANRS项目旨在通过标准化网络运营商使用的控制和操作原则，提高全球互联网的安全性和可靠性。它列出了参与者采取的四项行动，作为行动和与他人互动的一部分。总体而言，这些努力旨在遏制可能损害互联网可靠性的意外或故意活动。四个操作是：

- 路由过滤-防止传播错误的路由信息。
- 防欺骗-阻止源IP地址欺骗的流量。
- 协调-促进网络运营商之间的全球运营通信和协调。
- 全局验证-促进在全球范围内验证路由信息。

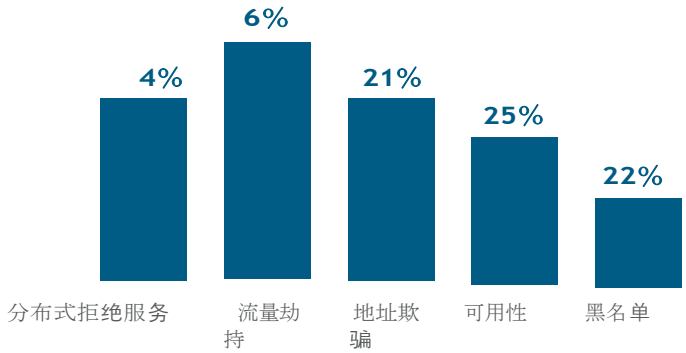
这些动作一起可以帮助防止问题并在问题发生时快速解决。参与MANRS的服务提供商已承诺参与这项工作。互联网结构面临的挑战之一是，要想有效运作，就需要社区做出更大的努力。这项工作可以帮助减少长期存在的问题，例如流量重路由（绕行），拒绝服务攻击（DDoS）和流量劫持。

芒斯研究

为评估和评估MANRS项目及其对企业和服务提供商的影响，451 Research进行了广泛的研究，研究结果提供了有用的同等基准数据，该项目对企业的重要性和影响。超过70%的研究受访者认为，信息安全状况是其组织的首要核心价值。在企业安全环境中，很大一部分是与互联网的连接以及与之选择的合作伙伴的连接，这使MANRS成为了一个重要的限定条件。

该研究还探讨了企业对互联网安全的担忧，并试图量化企业期望如何解决这些担忧。最令人担忧的是流量劫持，这个问题经常在新闻中报道，而客户满意度问题超出了安全问题。

图1：互联网安全问题

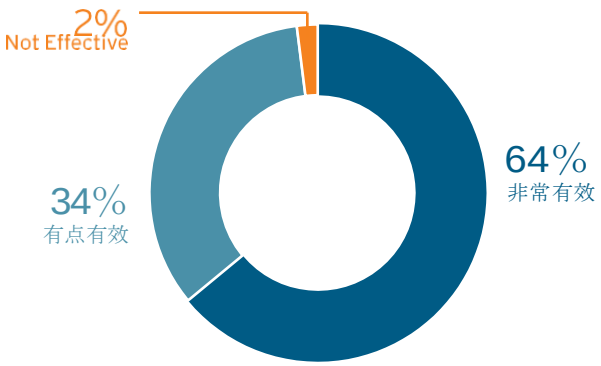


资料来源：451研究报告：MANRS感知与行动，2017年7月

接下来的两个最重要的问题具有内在联系。尽管拒绝服务攻击是一个令人担忧的问题，但研究受访者对地址欺骗（一种可用于掩盖分布式拒绝服务攻击源的技术）的关注程度与此相同。 MANRS项目旨在通过其四项措施解决这些担忧的根源。

这项研究还评估了做出回应的组织对MANRS项目在解决与他们相关的问题方面的有效性的想法。几乎所有受访者报告称，随着时间的推移，该项目将有助于解决互联网安全问题。近三分之二的人认为这将非常有效。

图2：MANRS有效性



资料来源：451研究报告：MANRS感知与行动，2017年7月

发挥企业杠杆作用

MANRS项目对企业的主要好处之一是，它表明服务提供商围绕操作安全性采取的态度和主动性。典型的企业在选择IT基础设施合作伙伴时会花费大量精力，但很难制定有效的选择标准。参与MANRS的服务提供商已在努力改善其安全状况，并与更大的社区合作以减少对互联网安全和稳定的威胁。 MANRS的参与可能是一个合理的选择指标，可以包含在RFP，招标和采购流程中，以增进对提供商能力的理解。在“ 451研究”中，有97%的受访者表示，他们将考虑将MANRS纳入其选择过程。

MANRS项目还为组织提供了一种加入与安全相关的更大社区的途径。这可以帮助希望合作解决问题的组织。这可能是一种识别生态系统合作伙伴的方法，企业可以与之合作，为安全创造更坚实的基础。在受监管的行业中，MANRS链接可能是审核员评估组织总体安全状况时要考虑的其他因素。

MANRS还可以增强企业的底线。正如451 Research研究表明的那样，大多数组织都担心安全问题，加入MANRS社区可以增强企业安全证书。它可以将企业的安全投资传达给客户。 MANRS的参与可以包括在营销资料中，也可以作为较大品牌声明的一部分。

尽管MANRS项目是针对服务提供商的，但任何具有涉及BGP的对等安排的组织也可以成为社区的一部分。将MANRS行为纳入IT运营可以增加成熟度并提高运营效率。

结论

MANRS项目为直接可实现的企业带来许多好处。对于MANRS的参与，应该仔细考虑，不仅是企业的服务提供商，还可能是企业本身。项目提供的更高的安全意识可以使更广泛的互联网社区受益，而企业在这里发挥着重要作用。加入MANRS社区的企业可以改善安全状况和业务。

附录三

RFP语言，用于Manrs选择

以下是示例语言，可供有兴趣在选择互联网服务提供商时将MANRS合规性纳入提案申请流程一部分的企业使用。这仅是示例，并非法律建议。准备任何RFP文件时，应始终咨询适当的法律顾问。

推荐组织的资格要求

1.提议组织遵守MANRS

XXXX支持更广泛的互联网社区为提高弹性和安全性所做的努力。所有提案组织至少应在提案提交前30天内参加并遵守“路由安全互认准则”项目（）。提议组织将在整个合同期限内保持合规性，并在任何时候失效合规性时通知XXXX。通知必须通过合同中指定的联系人进行，并且必须采用书面交流的形式。遵守情况将由MANRS项目定义的至少一组最低预期行动的执行情况决定。违反法规将被视为严重违反任何有效合同。*https:// www.manrs.org*