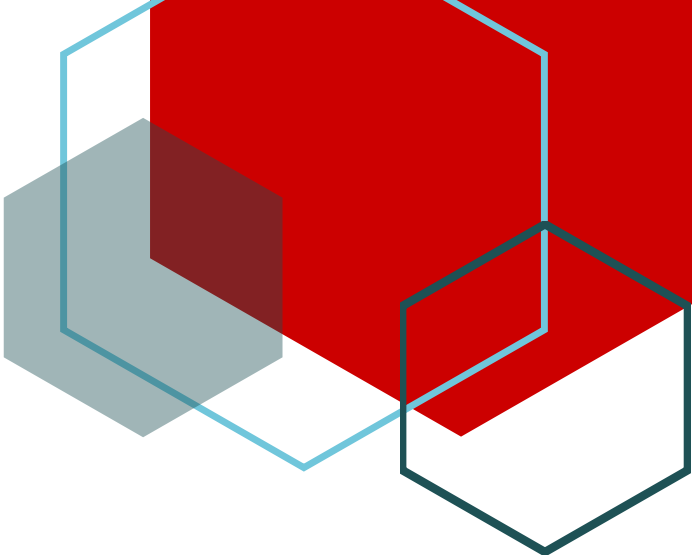


CSPs: Service Assurance Key to Automation Plans

A PRODUCTION OF HEAVY READING'S THOUGHT LEADERSHIP COUNCIL IN CONJUNCTION WITH:

NETSCOUT

SevOne

Spirent Promise. Assured.

HEAVY READING THOUGHT LEADERSHIP COUNCIL

CONTENTS

Almost 70 percent of communications service providers (CSPs) in this special NFV Carrier SDN 2018 show report say their companies are doing an excellent or good job with their current service assurance approach. But as operators continue down the path of virtualization toward automation, they acknowledge that service assurance becomes more difficult.

Members of Heavy Reading's Thought Leadership Council (TLC) answered a 10-question survey and provided detailed thoughts about how virtualization and automation are impacting service assurance, and how their companies are coping.

Key Takeaways

• • •

The majority of CSPs say that their companies are doing a good or excellent job with their current service assurance approach

Nevertheless, half of CSPs say that they will need to supplement their current service assurance tools as they virtualize networks

Meanwhile, 79 percent of CSPs say that analytics and closed-loop automation will be critical to their service assurance strategy over the next three to five years

Additionally, 46 percent of CSPs say they are evaluating their options for automation deployment and haven't yet settled on a firm plan

Yet 67 percent of CSPs say that they are already running network services as VNFs

And 75 percent of CSPs say the growth of virtualized networks will increase the need for proactive, automated testing of newly activated services

NFV is seen as the greatest challenge to current service assurance approaches by 58 percent of CSPs

ABOUT THE THOUGHT LEADERSHIP COUNCIL

The Thought Leadership Council (TLC) is a unique Heavy Reading initiative founded in August 2017, in which a panel of highly targeted CSPs participate in strategic research on topics such as automation, 5G and IoT. TLC members receive private invitations to take part in anonymous surveys, which enables them to provide insights that might otherwise go undisclosed.

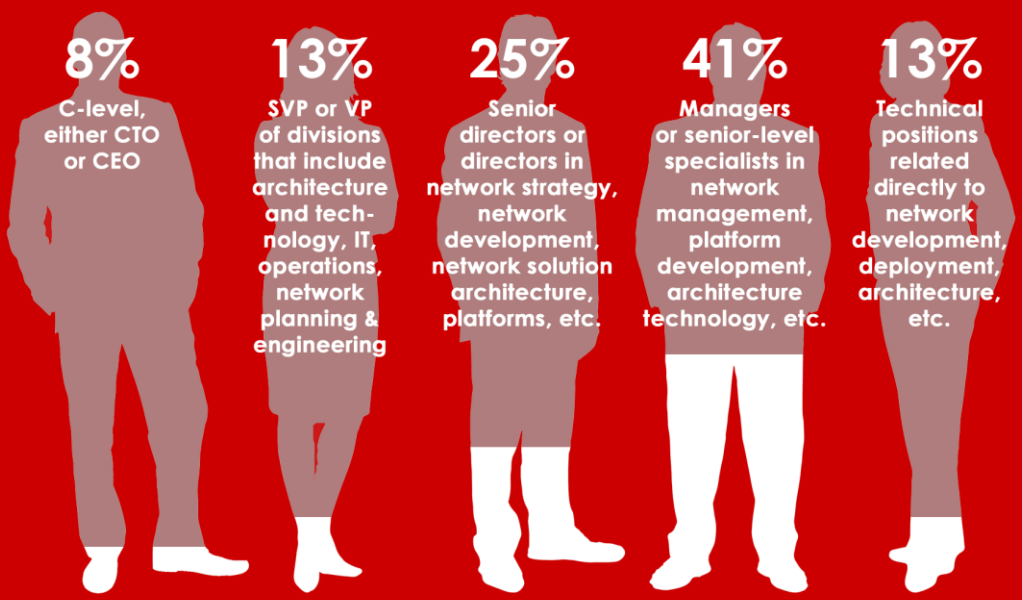
Additionally, vendors sponsor surveys in which TLC members provide valuable insights on topics of critical importance. These surveys are used to develop reports, white papers, webinars and other deliverables.

The TLC is under the exclusive purview of Denise Culver, Online Research Director with Heavy Reading. Individual TLC members develop long-term relationships with Culver, who personally chooses each member for the Council, developing a high level of trust and a sense of partnership.

The TLC currently boasts 100+ members, and new members are added monthly to ensure strong participation and representation. For more information about the Thought Leadership Council, contact Denise Culver at culver@heavyreading.com.

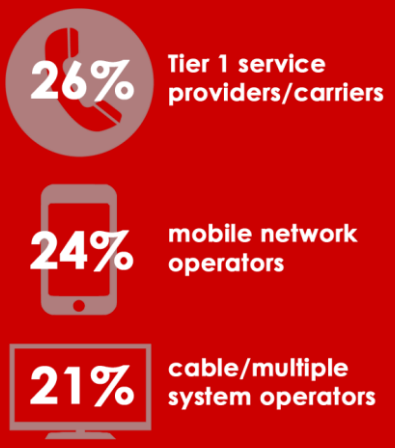
Breakdown of TLC Members in This Report

Job Responsibilities

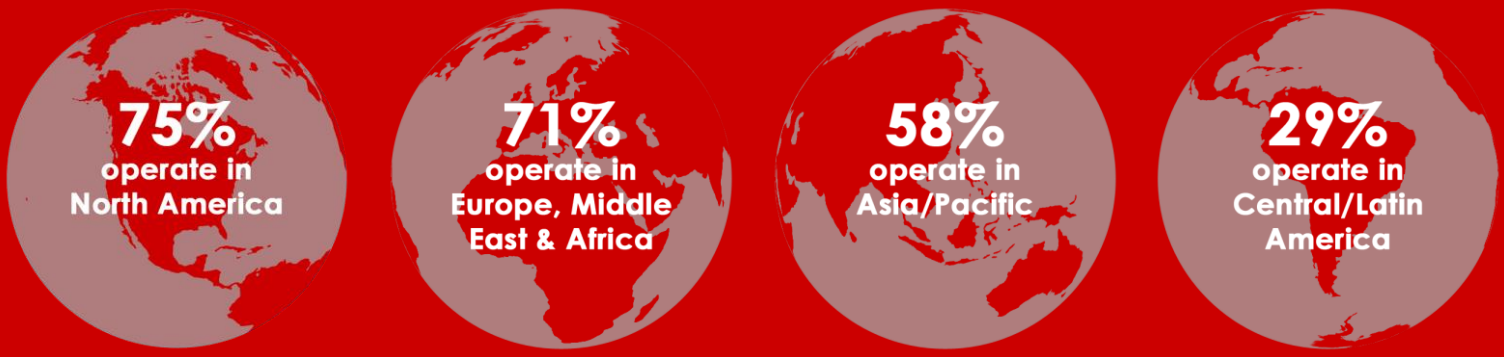


CSP Types

Companies represented have a mix of wireline, mobile, cloud, fiber, data and broadband networks; many have converged networks (wireline, wireless, cloud), many of which overlap.



Geographic Representation



SUSSING SERVICE ASSURANCE

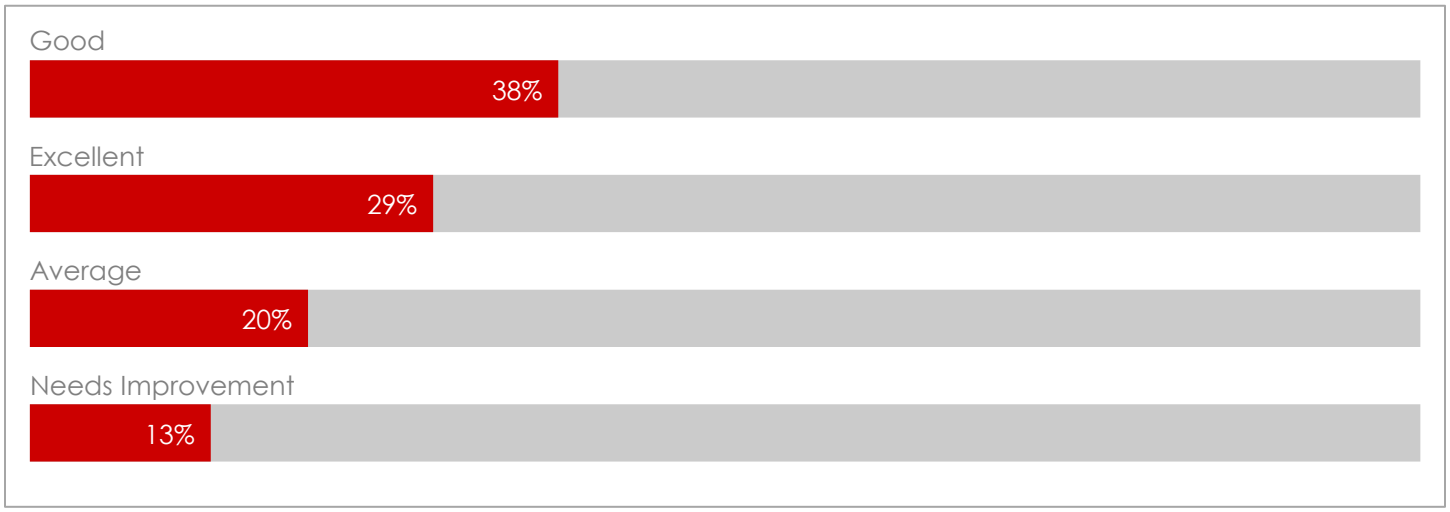
Rate your company's current service assurance approach

The majority of Thought Leadership Council (TLC) members say their companies are doing either a good or an excellent job with service assurance.

More panelists rated their companies as "good" (38 percent) than as "excellent" (29 percent). One CSP quipped about giving the company a "good" rating: "There is always room for improvement. Claiming excellent would leave little urgency for doing it even better."

Twenty percent of CSPs ranked their company's service assurance approach as "average," with one person commenting, "We're a typical telco with legacy OSS that we are migrating."

Meanwhile, 13 percent of those surveyed admitted their companies have room for improvement. "We have room for a lot of improvement," one CSP said. "We're not quite failing, though, since we have improved quite a bit in the past year or so."



SUSSING SERVICE ASSURANCE

What will create the greatest challenges with your current service assurance approach?

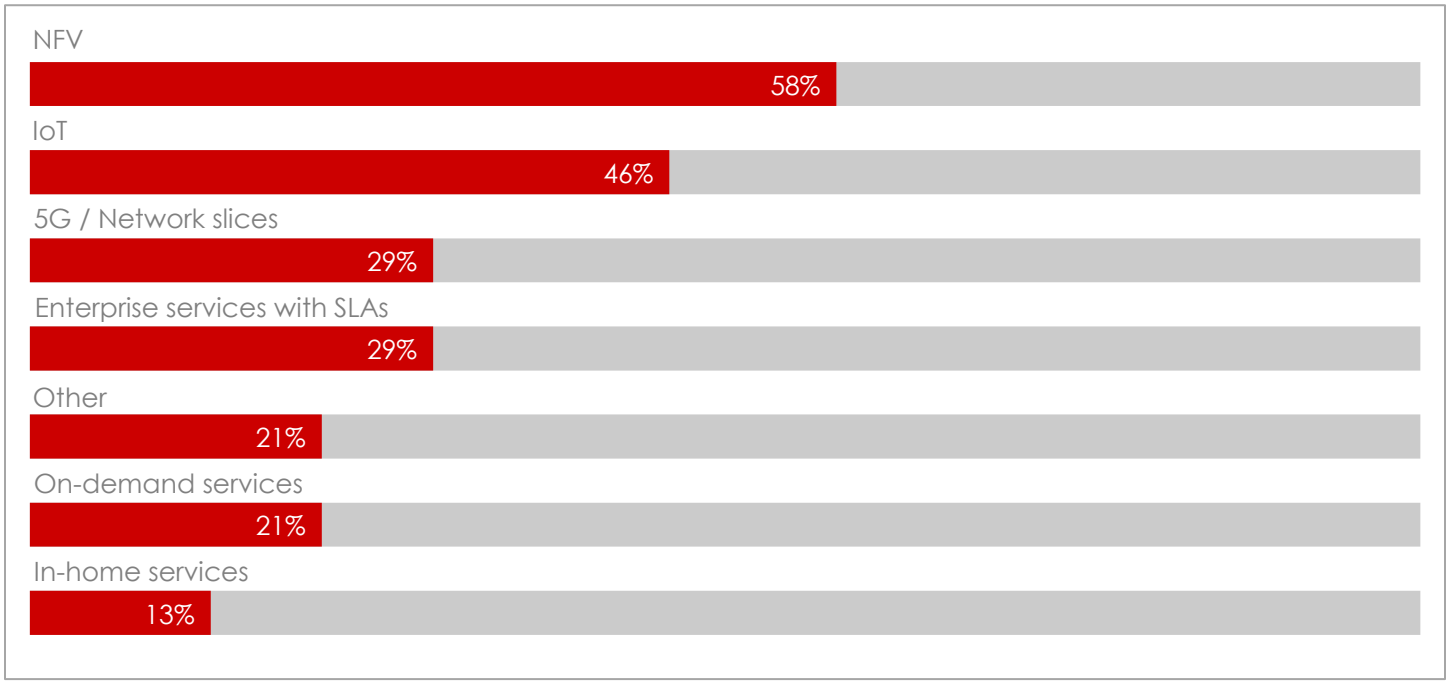
NFV is seen as the greatest challenge that TLC members currently face in their approach to service assurance, with 58 percent identifying it as a concern. One CSP specifically identified virtual network functions (VNFs) for enterprise customers as a specific concern in this space.

Twenty-nine percent of TLC members identified 5G/ network slices as a challenge, specifying: ultra-reliable and low-latency communications (URLLC); autonomous vehicles; primary connectivity services; and services for enterprise customers.

A number of CSPs, 21 percent, identified unique challenges they face related to service assurance:

- In general, all changes within a software-defined network (SDN) framework affect many areas. This increases the need for changes within many systems and processes. The needed speed due to market changes and related costs are significant. Additionally, we have the problem of standardization. We have many players in the game that aren't necessarily working together, nor are they following standards due to the flux in this area. This creates compatibility issues for products and networks.
- It's not so much an individual service as much as the prescriptive and machine-learning needs and investments required for the next generation of assurance.
- Increased managed services requires an integrated enterprise unified communications (UC) environment that utilizes multiple providers and technologies.
- Converged slices, such as fixed-wireless access (FWA), mobile edge cloud (MEC) and full-stack IoT applications, will create challenges for us.

Twenty-one percent of TLC members identified on-demand services as a challenge to their current service assurance approach, specifying: bandwidth on demand, video on demand (VoD), Ethernet on demand, software as a service (SaaS) and SD-WAN.



SUSSING SERVICE ASSURANCE

Thinking about your current service assurance tools and your company's roadmap to virtualization, which statement best applies?

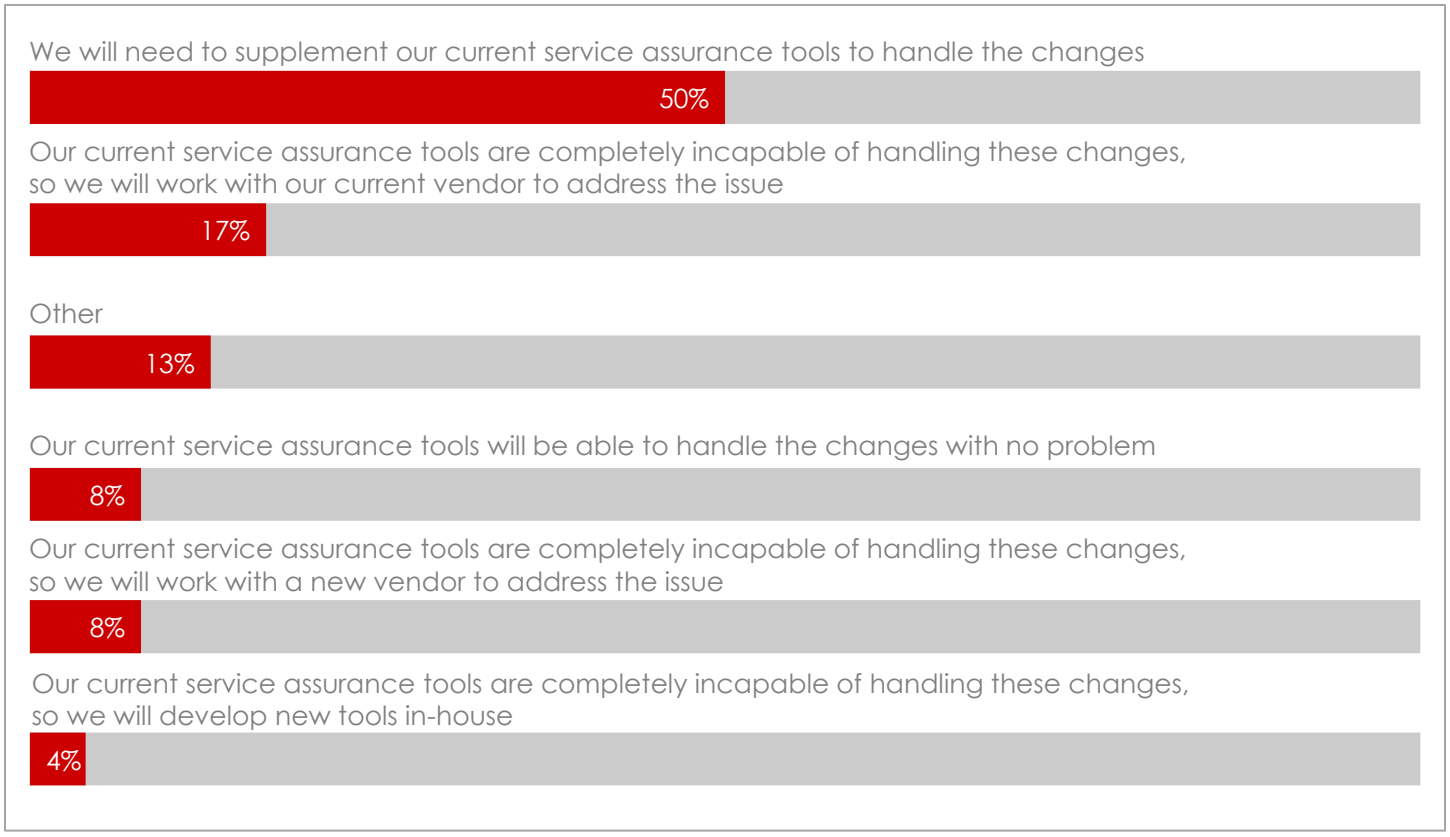
Fifty percent of TLC respondents said they will need to supplement their current service assurance tools to handle the changes that virtualization will create in their networks.

Several TLC members commented specifically about those changes:

- Since we will always support brownfield environments, we will continue to evolve and innovate on service assurance by leveraging our internal investments and, where appropriate, integrate best-of-breed and disruptors to support future requirements.
- We have almost completed the process of implementing new tools because our old tools did not enable us to make the journey.
- We will do this by evaluating and augmenting our current platforms and solutions with new vendor tooling abstracted under enterprise API facades.

Seventeen percent of CSPs said their current service assurance tools are completely incapable of handling virtualization, so they plan to work with their current vendor to address the issue. Meanwhile, 13 percent of respondents said their companies are choosing other options, including:

- The scale at which we operate is globally massive. As such, we must continue to push toward more efficient solutions for our own internal network and that of our customers.
- We'll develop tools in-house, explore solutions from existing vendors and seek tools from new vendors.



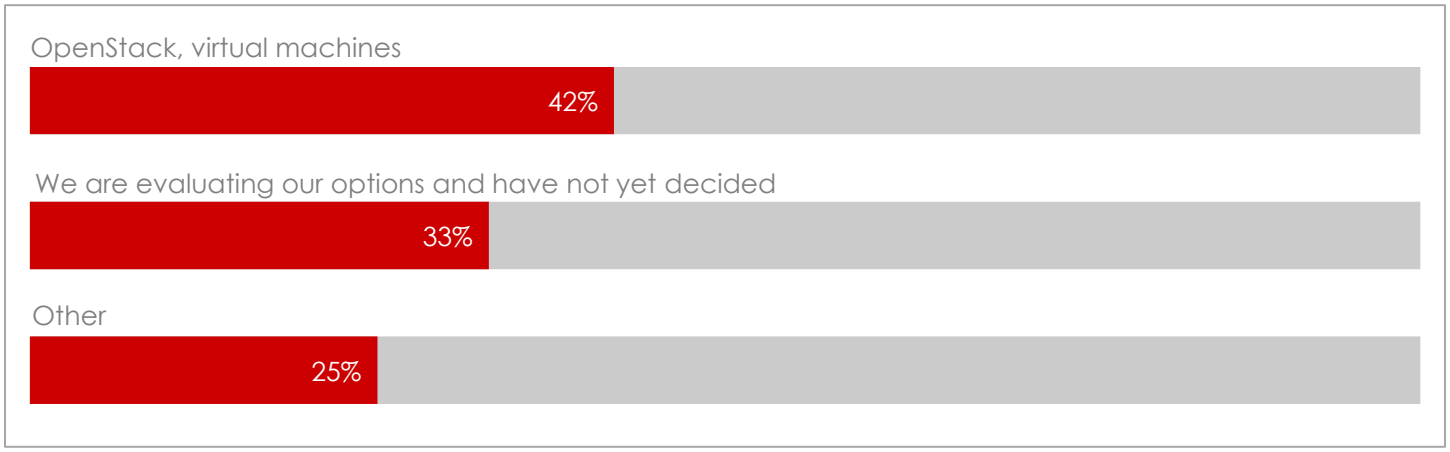
VETTING VIRTUALIZATION

What virtual implementation will you use?

CSPs were divided into three primary mindsets concerning the types of virtual implementations they plan to use. Forty-two percent plan to use OpenStack and virtual machines (VMs), while 33 percent continue to evaluate their options and haven't settled on a final implementation choice.

The remaining 25 percent of panelists have a variety of different plans, including:

- We will use VMs and containers, primarily in Red Hat and VMware.
- OpenStack is our current implementation, with a future roadmap that includes containers.
- We will use OpenStack, VMs, Kubernetes, containers and VMware.
- We will use OpenStack, VMs, Kubernetes and containers.
- Depending on the VNF, we will use OpenStack with VMs and Kubernetes.
- A combination of OpenStack, VMs, Kubernetes and containers, VMware and a virtual data center will be used.



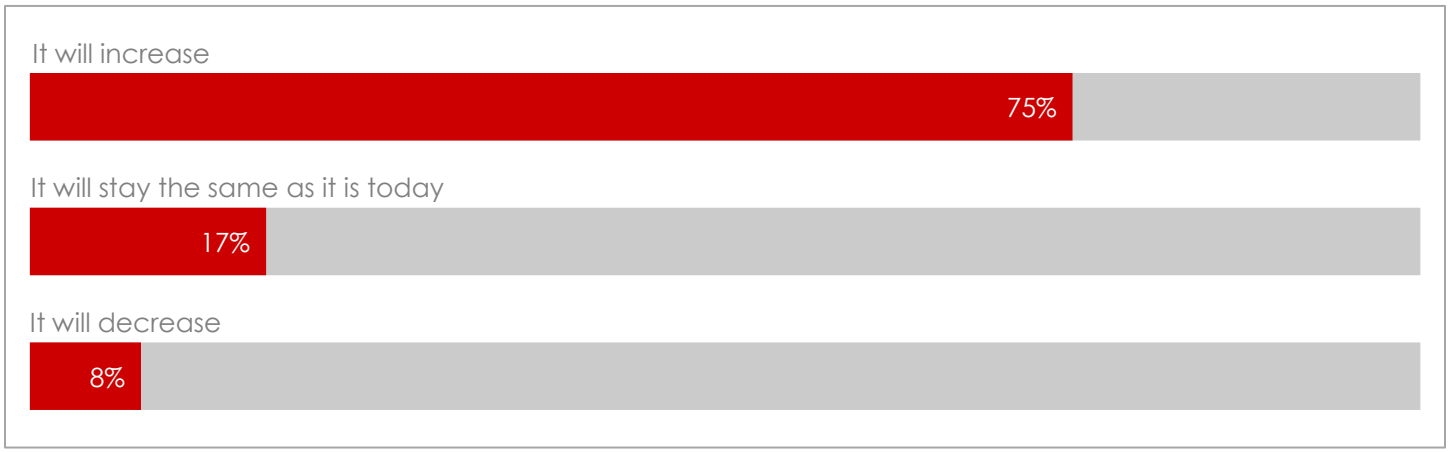
VETTING VIRTUALIZATION

How will the growth of dynamic, virtualized networks impact the need for proactive, automated testing of newly activated services?

The overwhelming majority of CSPs – 75 percent – said the growth of virtualized networks will increase the need for proactive, automated testing of newly activated services in a number of ways, including 5G, IoT, wireless core elements, network slice instance deployment, VPN clients and VNF equipment. Several TLC members explained in more detail:

- The disaggregation of network elements increases the testing load on service providers dramatically. This really will be for all virtualized services. The ability to do a real-time test with a feedback loop upon activation is critical to the automation efficiencies we hope to gain.
- It will increase, particularly for services such as fully integrated service chains and dynamic service chaining, in which every enumeration of application interaction, overlay and underlay will have to be automated to keep with the pace of the customer demand. Furthermore, as we move away from proprietary dedicated appliances to white boxes, it requires proactive and automated monitoring to ensure features and functions, performance and compliance adherence.
- Many of the new dynamic and new NFV-based services will introduce customer choice and self-service. So the permutations of a given customer's "stack" could become unwieldy. When you throw in DevOps, NetOps and the promise of live update, constant change within those stack components and assurance becomes a huge piece of customer experience.
- It will increase because of the complexity of operating, administering and managing (OAM) a combined hybrid traditional physical network and NFV-enabled infrastructure (NFVI), in addition to providing carrier-grade services to enterprise customers running on top of both.

Eight percent of respondents said the growth of virtualization will decrease the need for automated testing of newly activated services. One CSP said that this will occur as application-specific functions are replaced by VNFs, while another said it will be accomplished through automation.



VETTING VIRTUALIZATION

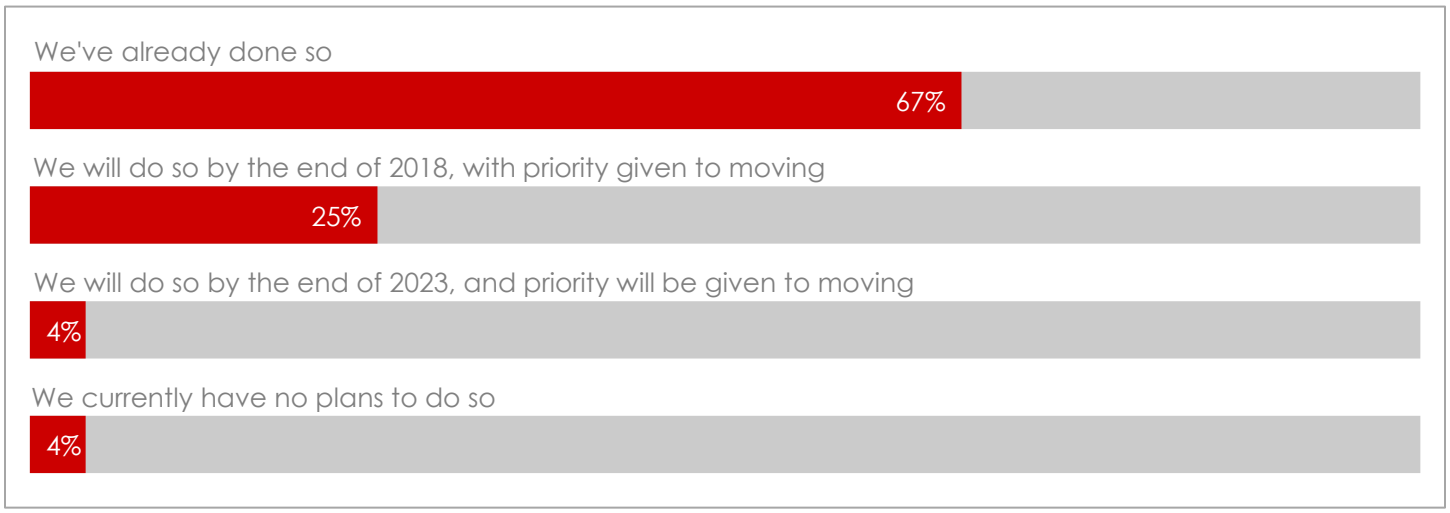
When will your company begin running network services as VNFs?

Sixty-seven percent of CSPs said they have already begun running network services as VNFs, with many specifying particular areas of focus, including:

- Five respondents specified IP Multimedia Subsystems (IMS), firewalls, routers and voice
- Three respondents specified Evolved Packet Core (EPC) and SD-WAN
- Two cited security, data centers and DNS services
- Others indicated the following are being run as VNFs: virtual PBX, WAN optimization, SDN controls, SDN-controlled access, content delivery networks (CDNs) and LAN controllers for end customers
- One TLC member said, "Our internal network is already more than 55 percent virtualized and will reach 75 percent by 2020." Another said, "We're running VNFs in our existing data centers for most applications, and plans are in progress to migrate the core network to VNFs."

Twenty-five percent of respondents say they will be running network services as VNFs by the end of 2018, with priority given to the following:

- Moving enterprise VNFs, such as SD-WAN and virtual firewalls
- Core and enterprise service components
- Enabling next-generation SDN services underpinned by an orchestrated SDN/NFV platform
- Moving packet core gateways onto VNFs



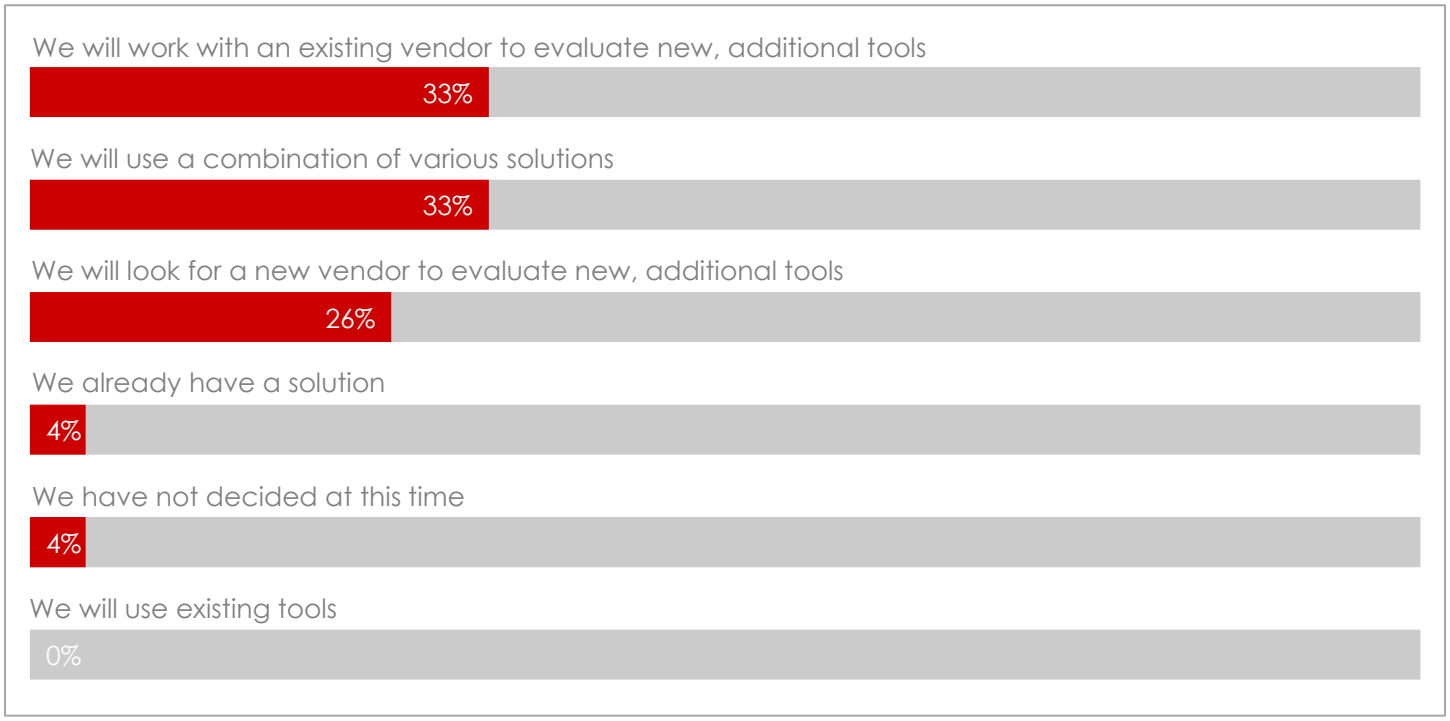
VETTING VIRTUALIZATION

What does your company plan to use for visibility into multi-access edge computing (MEC)?

TLC respondents don't have a tried-and-true method of gaining visibility into MEC. Thirty-three percent of respondents said they will work with existing vendors to evaluate new, additional tools to gain such insight, while the same number said they will use a combination of various solutions, including existing and internal tools, as well as working with existing and new vendors, to do so. Some CSPs explained those plans in detail:

- We leverage existing tools where possible and adapt them through application programming interfaces (APIs) to other existing systems and new systems that are part of our digital transformation. We also have many tools that are home-grown, based on open source, as well as those that are customized by us.
- We are leveraging all solutions to build and innovate on the demands of MEC.
- We will have a combination of developing tools internally, as well as evaluating new tools from new vendors.

Meanwhile, 26 percent of respondents said they will look for new vendors. One CSP's company already has a solution that was built internally.



ANALYZING AUTOMATION

When will your company implement a plan for closed-loop orchestration?

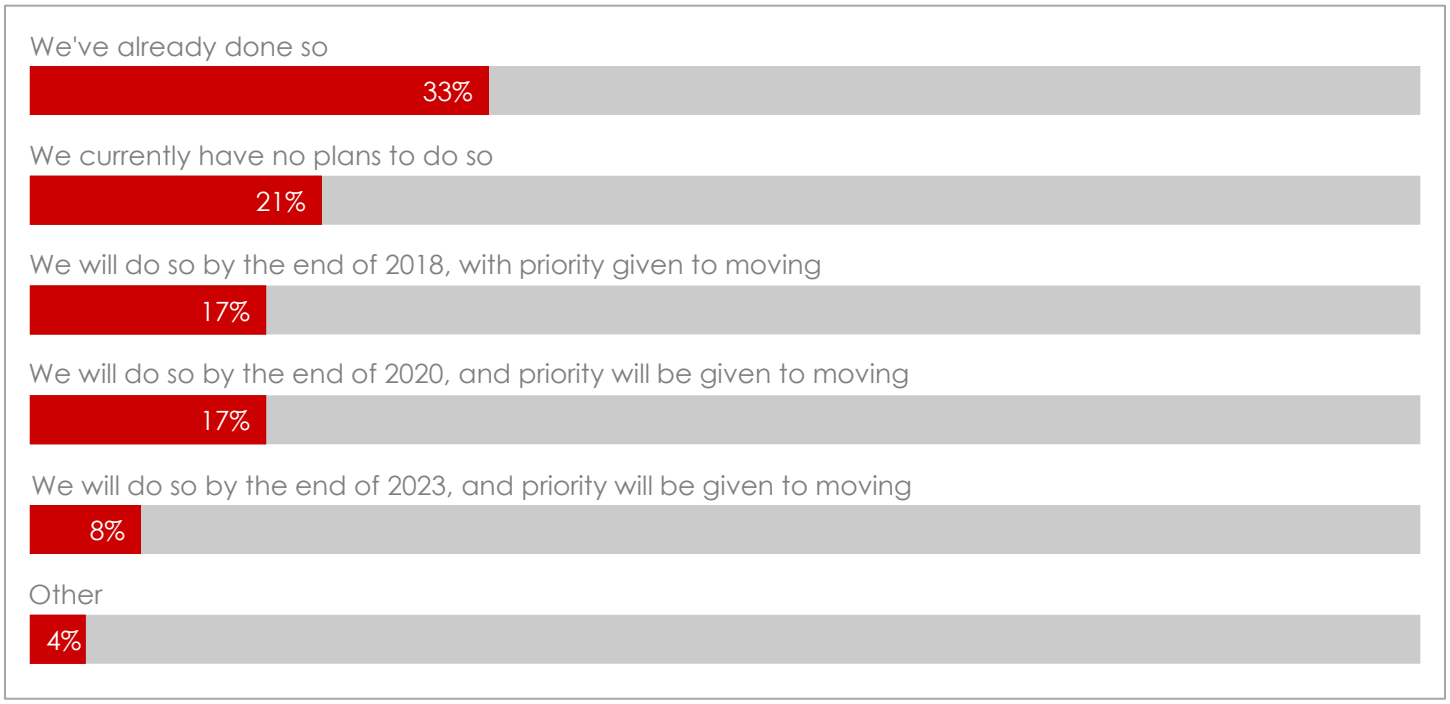
Thirty-three percent of CSPs have implemented a plan for closed-loop orchestration, including:

- Data center, NFV, VNF lifecycle and some product offerings in the traditional network are very mature and operational. Other traditional network services have been implemented on a cost/value basis. Growth markets and services are the first targets for commitment.
- We only apply closed-loop orchestration for virtually produced resources, including resource and service orchestration.
- Closed-loop assurance with orchestration and centralized policies for service behavior spanning the various deployment models.
- Network, security and remote-access services
- Automated customer-service provisioning

Interestingly, 21 percent of panelists said their companies have no plans to implement closed-loop orchestration. However, one of those panelists said, "Discussions have taken place within our company that this will eventually be a requirement that has to take place within our network."

Seventeen percent of CSPs said they will do so by the end of 2018, with one panelist specifying support for an SDN/NFV platform that supports SD-WAN and managed virtual security services, while another panelist specified moving telco network services but with limited functions. One panelist said, "We are currently running several proofs of concept around network health, call center and security."

Another 17 percent of CSPs said they will implement such a plan by the end of 2020, with some specifying priority given to moving enterprise VNFs, such as SD-WAN and virtual firewalls, core, MEC and enterprise applications, and customer automation services. Another 8 percent will implement a plan by 2023, with priority given to the core network, while 4 percent don't have a date for completion.



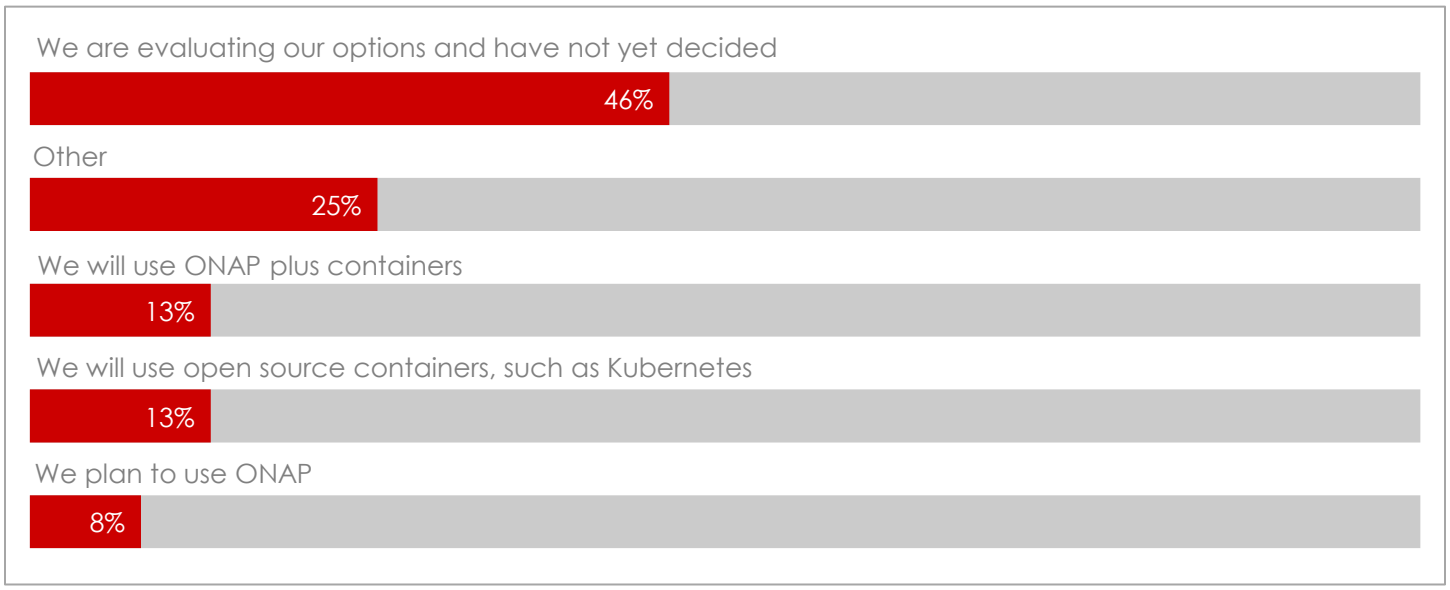
ANALYZING AUTOMATION

What are your deployment plans for automation?

Almost half – 46 percent – of CSPs said they are still evaluating their options and have not yet decided on deployment plans for automation. Another quarter of panelists are in the process of developing deployment plans that are a unique mix of solutions options, including:

- We are developing our own business orchestrator platform to drive end-to-end automation.
- We have already deployed orchestration with closed-loop assurance at scale globally and will continue to evaluate new features/functions to evolve the use cases, such as open source, containers and more.
- We have a custom-built SDN solution with a mix of vendor tools, such as a Tail-f Apigee.
- We are going to use OSM and containers.
- We are starting with OSM with ETSI MANO as a reference and will closely watch the evolution of ONAP, OPNFV, MEF LSO and others.
- Automation in a telco goes way beyond container orchestration and just automating network configurations. So we will use Kubernetes to some extent, but we have many other automation tools, some commercial and some self-developed.

Thirteen percent of panelists said they will use open-source containers, such as Kubernetes, with one panelist commenting, "We use OpenStack, VMware, Kubernetes, Docker, Cloud Foundry and many other virtualization technologies. We are all automated in some fashion as a technology domain, and all are part of larger automation frameworks to execute business functions, which serves as a micro-orchestrator."



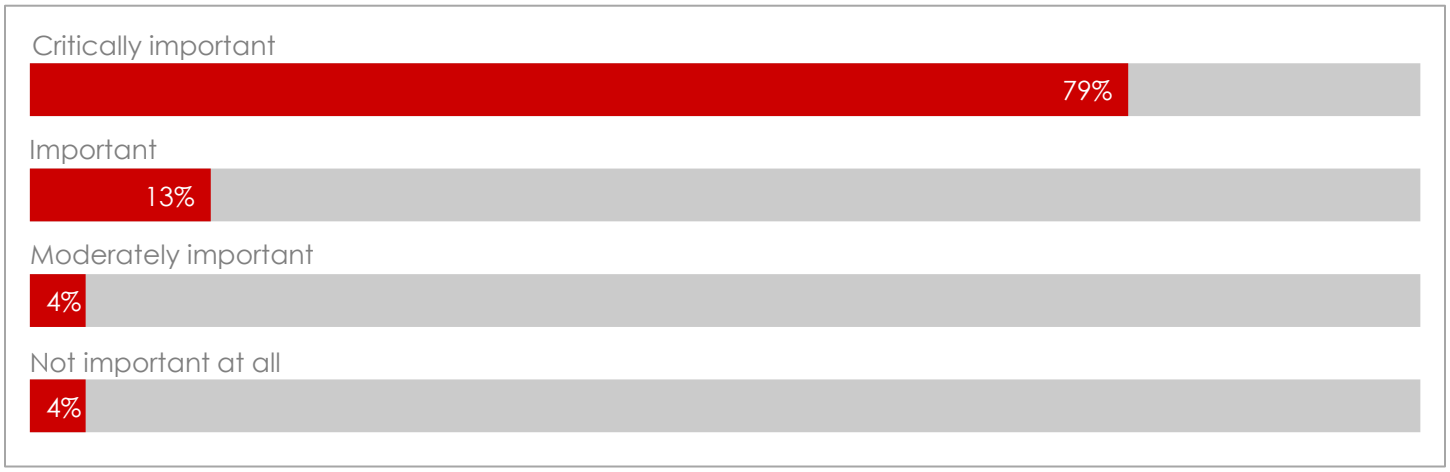
ANALYZING AUTOMATION

How important will analytics and closed-loop automation be to your service assurance strategy over the next three to five years?

The majority of CSPs – 79 percent – said analytics and closed-loop orchestration will be critically important to their service assurance strategies over the next three to five years, specifying the following as drivers:

- Multi-vendor software-based VNFs, the disaggregation of network elements and the burden of open-source elements on service providers.
- The ability to automatically respond to problems before, or very quickly after, they occur is critical to being able to provide low-cost customer services with a low-opex support model.
- It's the closed-loop behavior that adapts the service dynamically based on the demands of the consumer. What virtualization brought to applications in the data center is the expectation for software-defined and virtualized services in next-generation networks.
- Customers are demanding self-service, on-demand activation and provisioning and accountability on quality of service. We can't afford to staff millions of bodies to implement on-demand and real-time actions or real-time network and service validation.
- Analytics will be the backbone for dynamic on-demand virtualized services. Current manual service-assurance approaches deployed by most providers will be insufficient to provide early enough detection of quality, scaling, performance and network issues fast enough within dynamic NFV environments.
- Ensuring the system works as necessary before deploying and lab testing can never fully duplicate production. Utilizing closed-loop automation will ensure that the network performs as intended.
- Without data-driven automation, we can never be as efficient as needed. Self-healing is the only way to actually realize the resource savings.
- Networks and services will become way too complex to be assured without closed-loop. Customers expect full transparency and instant fulfillment already. If you want to fix problems before customers are detecting the impact, you have to build on closed-loop assurance and continuous testing.
- As networks become more complex and service offerings and product types become more numerous, our staff will become unable to keep up without analytics and closed-loop automation.

Thirteen percent of CSPs said analytics and closed-loop automation will be important but limited to areas such as critical services requiring enhanced SLAs and what can be achieved within the business constraints of budget, already available resources and cooperation from other departments.



ABOUT OUR SPONSORS

About NETSCOUT Systems Inc.

NETSCOUT's virtualization service assurance solution can assist service providers at any stage in their hybrid journey to NFV with complete visibility of applications and services deployed in either private or public clouds. vSCOUT and vSTREAM are scalable software instrumentation products optimized for NFV/SDN/cloud infrastructure to provide visibility down to the VNF layer with packet forwarding and smart data creation for service assurance, business analytics and security assurance. They are combined with vGeniusONE service assurance application to provide a proactive monitoring and service triage solution.

The solutions help CSPs meet the challenges of migrating infrastructure and services to the cloud by: delivery of end-to-end visibility and intelligence into cloud-based applications and services and interconnected legacy networks in a single view; managing the complexity of NFV, including new vendor implementations, standards, SDN, service chaining, microservices, automation and orchestration, and hybrid environments; end-to-end service orchestration, including real-time monitoring of orchestration, as well as orchestration of the solution with the orchestration layer in a closed loop; a low cost of ownership with virtual instrumentation that is optimized for the cloud and provides outstanding scalability and visibility with low consumption of cloud compute resources. The NFV software portfolio helps operators deliver service agility in 5G, IoT, NFV and hybrid networks with service assurance that is cloud-based and automated, includes analytics and monitors in real time on open platforms, regardless of the NFV adoption stage. Additionally, smart data empowers CSPs with scalable, easily consumable and affordable data with visibility for service assurance, business insights and security assurance. To learn more about improving service, network and application performance in physical or virtual data centers or in the cloud and NETSCOUT's performance and security solutions, powered by service intelligence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook or LinkedIn.

About SevOne Inc.

SevOne provides the comprehensive, flexible, and scalable network and infrastructure management capabilities that large organizations need to make smooth transitions from physical to virtual networking environments. Its cloud-based SevOne Data Platform simplifies the extraction, enrichment and analysis of network and machine data from across multi-vendor environments to deliver valuable insights and enable new efficiencies through automation. SevOne offers several pre-built solutions based on the SevOne Data Platform, including offerings specifically designed to solve SD-WAN, SDN, NFV and enterprise Wi-Fi challenges. SevOne is privately held and is headquartered in Boston, Mass. For more information visit www.sevone.com.

About Spirent

Spirent Communications Plc. (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers and enterprise networks. It helps bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

To realize the potential of NFV, 5G, and IoT, providers need to automate and accelerate the service lifecycle. To address this challenge, Spirent is pioneering a new approach to testing and assurance based on DevOps principles, called Lifecycle Service Assurance (LSA). LSA helps providers leverage automation to rapidly launch new services, reduce costs and enable differentiated quality. Spirent VisionWorks consists of a suite of active test, assurance and analytics components for delivering automated LSA solutions in both legacy and new NFV, 5G and IoT networks. Deployed by tier-1 providers around the world, VisionWorks accelerates service activation and issue resolution and reduces operations and customer care costs. To learn more about LSA and VisionWorks, visit www.spirent.com/Solutions/Service-Assurance.

TERMS OF USE

License Agreement

This report and the information therein are the property of or licensed to Heavy Reading, and permission to use the same is granted to purchasers under the terms of this License Agreement ("Agreement"), which may be amended from time to time without notice. The purchaser acknowledges that it is bound by the terms and conditions of this Agreement and any amendments thereto.

Ownership Rights

All Reports are owned by Heavy Reading and protected by United States Copyright and international copyright/intellectual property laws under applicable treaties and/or conventions. The purchaser agrees not to export this report into a country that does not have copyright/intellectual property laws that will protect Heavy Reading's rights therein.

Grant of License Rights

Heavy Reading hereby grants the purchaser a non-exclusive, non-refundable, non-transferable license to use the report for research purposes only pursuant to the terms and conditions of this Agreement. Heavy Reading retains exclusive and sole ownership of all reports disseminated under this Agreement. The purchaser agrees not to permit any unauthorized use, reproduction, distribution, publication or electronic transmission of this report or the information/forecasts therein without the express written permission of Heavy Reading.

Disclaimer of Warranty and Liability

Heavy Reading has used its best efforts in collecting and preparing this report. Heavy Reading, its employees, affiliates, agents and licensors do not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this Agreement. Heavy Reading, its employees, affiliates, agents or licensors shall not be liable to the purchaser or any third party for losses or injury caused in whole or part by Heavy Reading's negligence or by contingencies beyond Heavy Reading's control in compiling, preparing or disseminating this report, or for any decision made or action taken by the purchaser or any third party in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if Heavy Reading was advised of the possibility of the same. The purchaser agrees that the liability of Heavy Reading, its employees, affiliates, agents and licensors, if any, arising out of any kind of legal claim (whether in contract, tort or otherwise) in connection with its goods/services under this Agreement shall not exceed the amount the purchaser paid to Heavy Reading for use of this report.

Dispute Resolution

This License will be governed by the laws of the State of New York. In case of a dispute arising under or related to this License, the parties agree to binding arbitration before a single arbitrator in the New York City office of the American Arbitration Association. The prevailing party will be entitled to recover its reasonable attorney fees and costs.

Heavy Reading
P.O. Box 1953
New York, NY 10156