Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING WHITE PAPER

Network Automation for Tier 2/3 Service Providers:

Heavy Reading Survey Analysis

A Heavy Reading white paper produced for Juniper Networks

JUNIPER NETWORKS

AUTHOR: STERLING PERRIN, SENIOR PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

Network automation holds tremendous promise to help communications service providers (CSPs) build and operate networks more efficiently and reliably at lower cost and with greater innovation than ever before. The advent of artificial intelligence (AI) and machine learning (ML) technologies makes the promise greater and the mission to automate to survive more urgent.

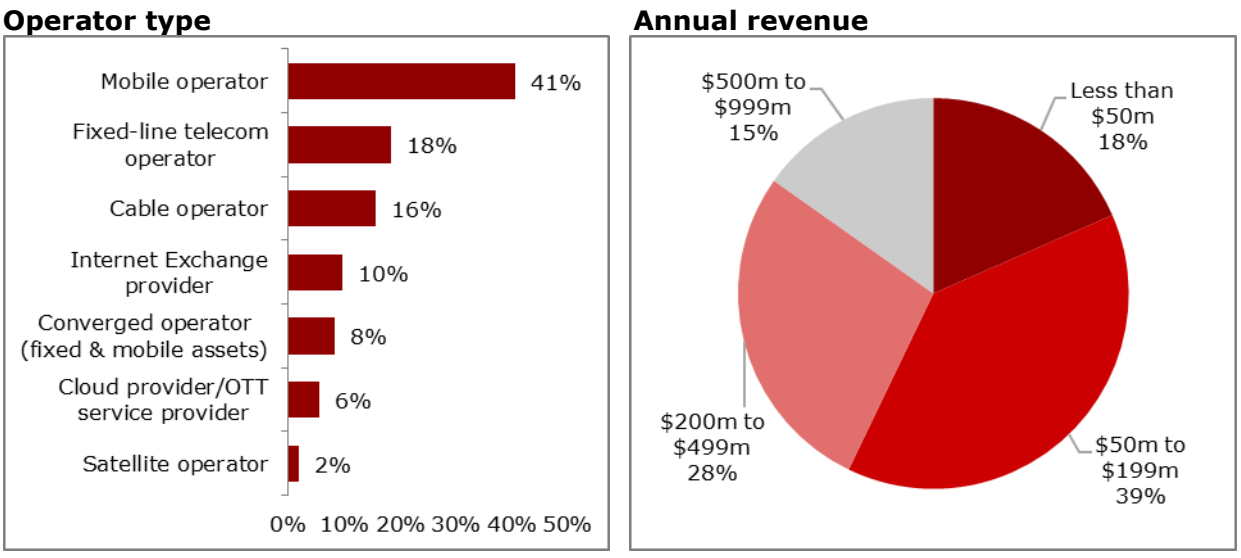
Yet, the technologies involved are highly complex, and the cost of building wide-scale automation can be prohibitive. Hyperscalers have benefitted the most from automation to date, and large Tier 1 CSPs with big budgets and sufficient staffing are beginning to invest. But what about the smaller CSPs—Tier 2 and Tier 3 operators—that also have much to gain from network automation yet face unique challenges getting started? The Tier 2/3 segment is a virtual unknown.

To better understand the needs of this important CSP segment, in May 2023, Heavy Reading surveyed 217 Tier 2 and Tier 3 CSPs globally in what Heavy Reading believes is the industry's first in-depth network automation survey to focus specifically on Tier 2 and Tier 3 network operators.

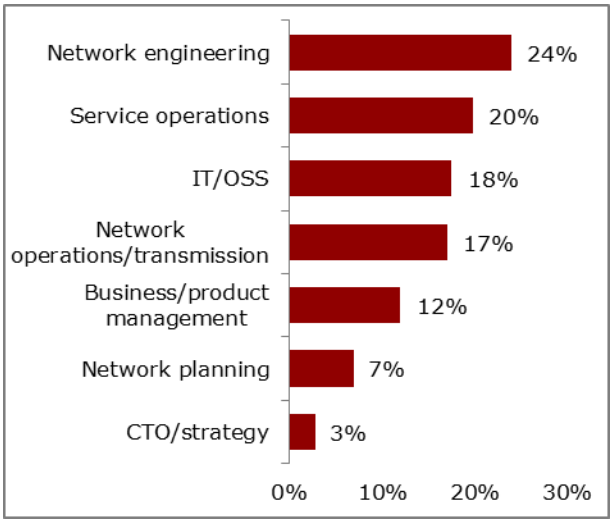
For the study, Heavy Reading defined Tier 2/3 by revenue and included only service providers generating less than $1bn annually. To further refine the focus on *network* automation, all respondents are involved in deploying, managing, purchasing, or using network automation, engineering, management, operations, or assurance solutions for IP, MPLS, or IP-integrated optical transport networks. In the end, the survey fielded 217 qualified respondents across all major geographic regions.

Figure 1 shows the full demographics.

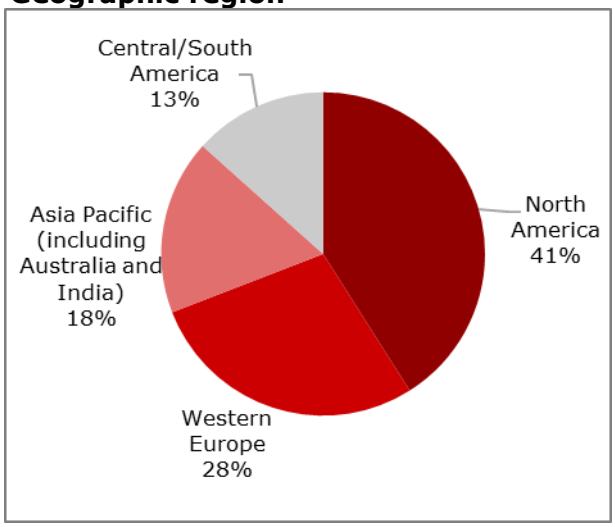
Figure 1: Survey response demographics



Job function



Geographic region

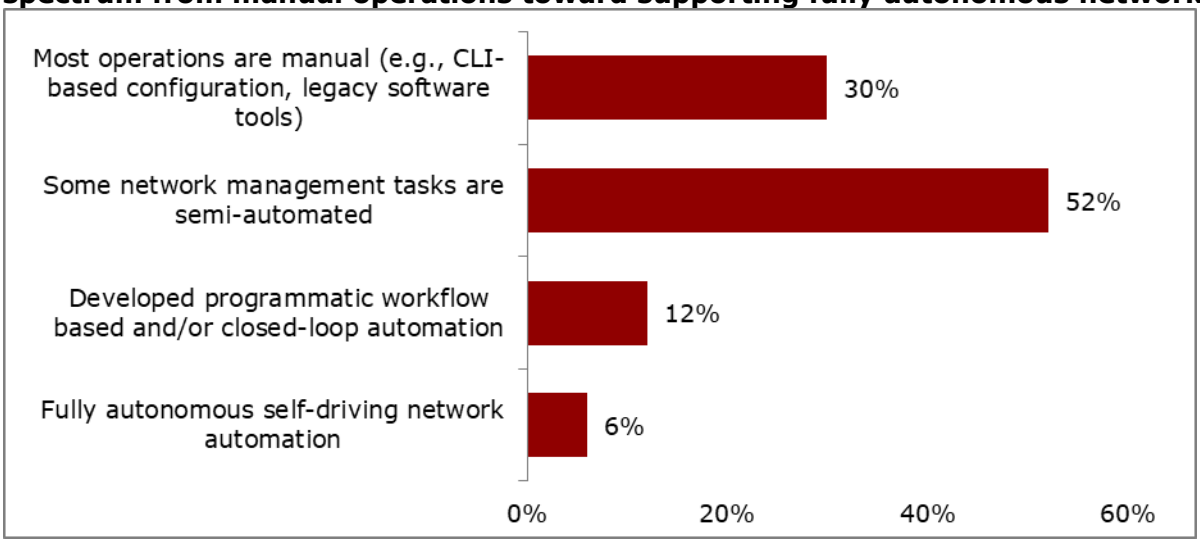


Note: Numbers in figures throughout this report may not total 100 due to rounding.
n=217
Source: Heavy Reading, 2023

TRENDS IN NETWORK AUTOMATION

Most Tier 2/3 operators surveyed are at an early stage of network automation, which is to be expected. The network automation trend is new, and smaller operators typically let Tier 1 take the lead on new technology adoption. 52% of Tier 2/3 operators report that some network management tasks are semi-automated. But for 30% of the group, most operations are still manual using command-line interface (CLI) and other legacy software. Closed-loop and higher levels of automation remain very rare—regardless of operator size (see **Figure 2**).

Figure 2: In terms of automated activities, where is most of your time spent in a spectrum from manual operations toward supporting fully autonomous networks?

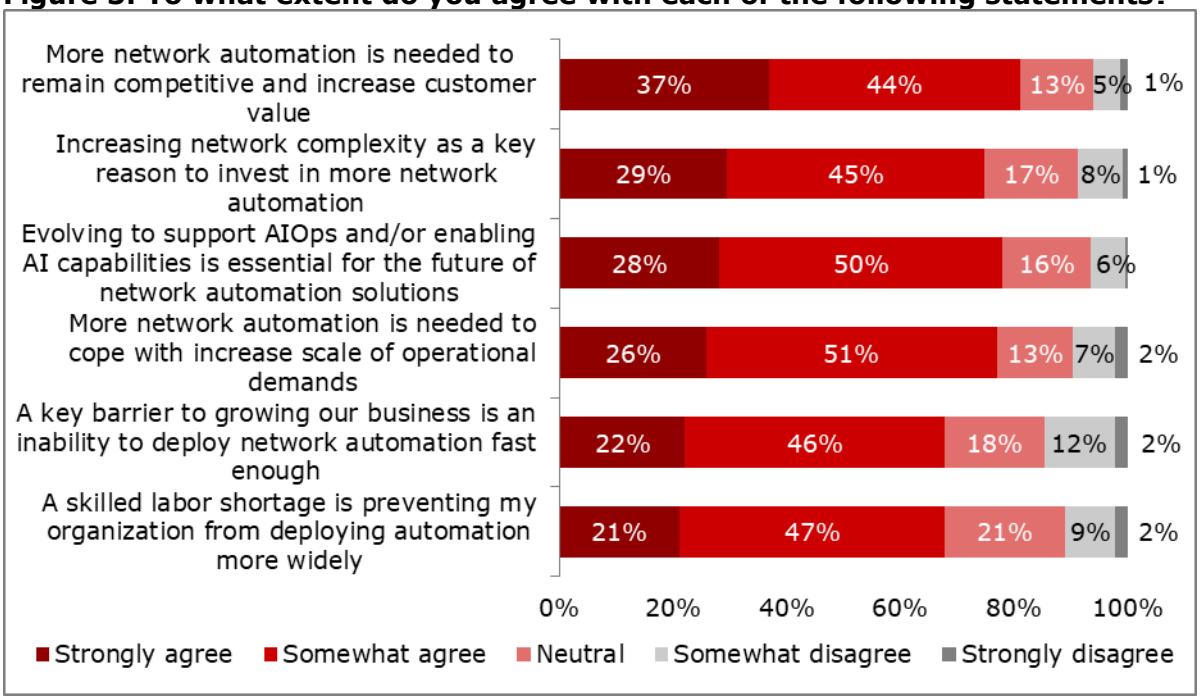


n=217
Source: Heavy Reading, 2023

Although they are in an early stage of adoption, Tier 2/3 CSPs see automation as an important strategic initiative. They understand the value and potential of automation to address some major challenges. 81% of survey respondents agree with the statement that more network automation is needed to remain competitive and increase customer value (37% strongly agree), while 74% agree that network complexity is a key reason to invest in more network automation (29% strongly agree).

These top results indicate automation has a broad role to play, including addressing both customer-facing (external) and network-centric (internal) challenges. Tier 2/3 CSPs are also tuning into the potential for AI automation. 78% agree that support for AIOps/AI capabilities is essential for the future of network automation (28% strongly agree). AI could be utilized to help Tier 2/3 CSPs achieve the interrelated goals of remaining competitive, contending with increasing complexity, and scaling to be able to achieve more, given that 77% agreed that more network automation is needed to cope with the increasing scale of operations (see **Figure 3**).

Figure 3: To what extent do you agree with each of the following statements?



n=217
Source: Heavy Reading, 2023

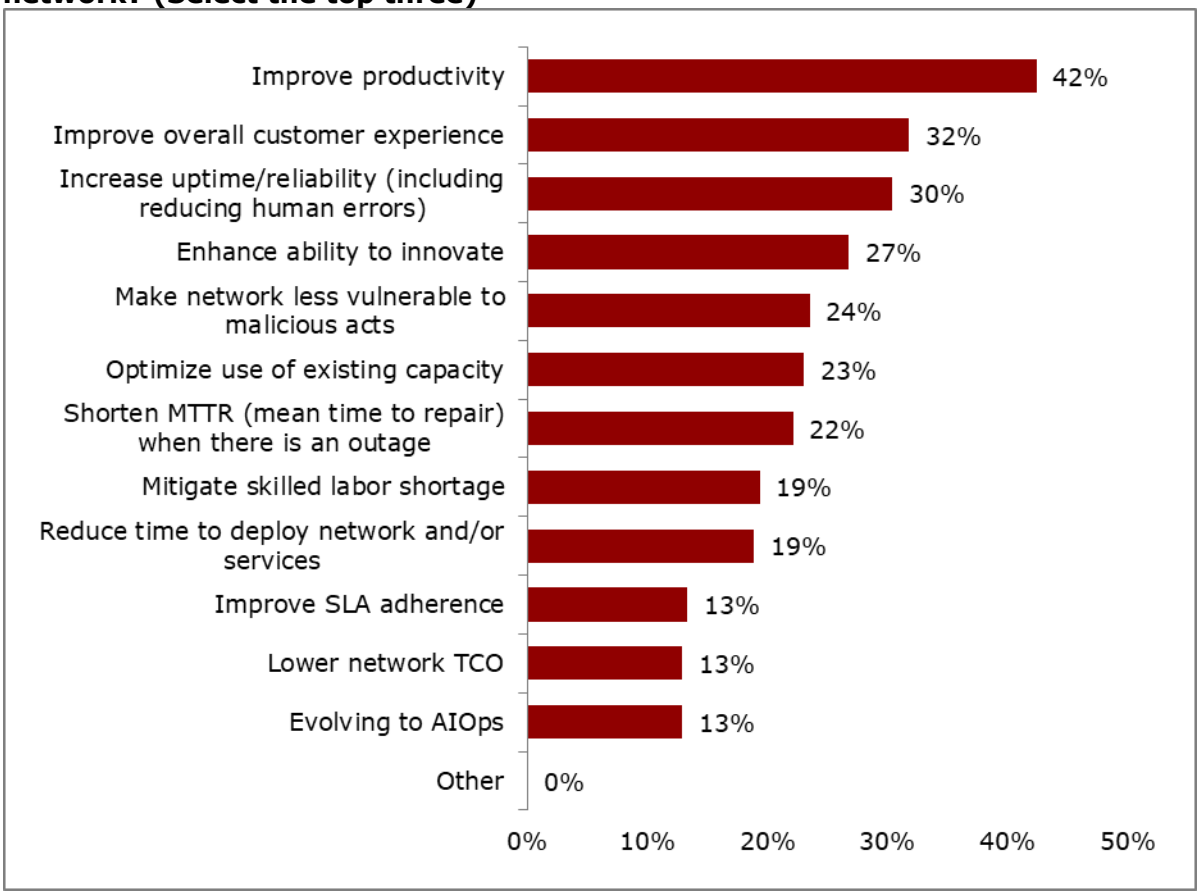
Asked specifically about drivers for automation in their own networks, 42% of respondents cite improving productivity, 32% pick improving overall customer experience, 30% name increasing uptime/reliability, and 27% choose enhancing ability to innovate—making these the top four drivers. Again, drivers point to both network-focused benefits (e.g., improving operational productivity and network reliability) as well as customer-facing external benefits (e.g., improving customer experience and innovating services).

Automation aids productivity in multiple ways, including allowing CSPs to do more tasks with the same staff or allowing lower-skilled staff to do jobs they otherwise would not be able to do. As networks get more dynamic and complex, automation will increasingly be

required to do tasks that humans simply cannot perform quickly enough, regardless of the number of workers and their levels of skill.

Multiple Heavy Ready surveys have pointed to the rising importance of network reliability as a competitive differentiator. Results here show CSPs expect that automation will aid significantly in those efforts (see **Figure 4**).

Figure 4: What are the primary drivers for implementing automation in your network? (Select the top three)



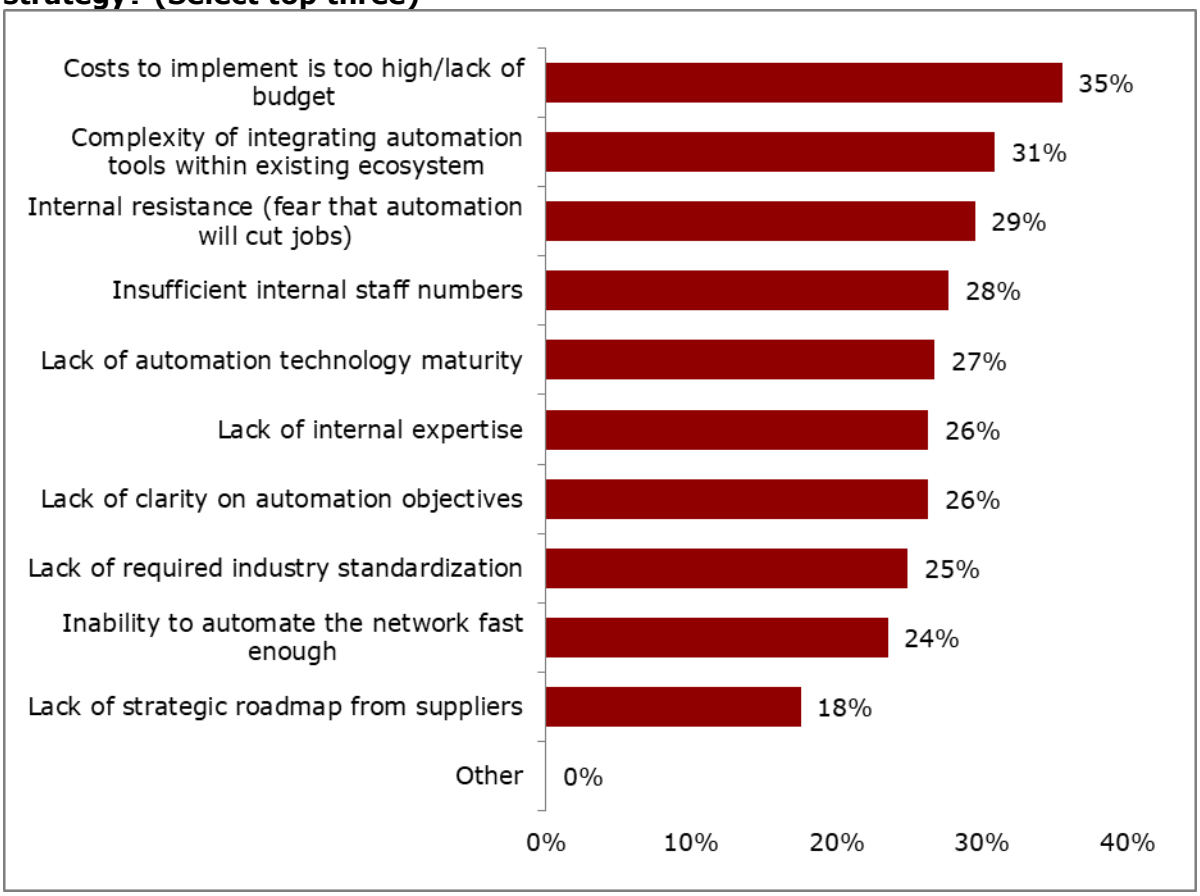
n=217

Source: Heavy Reading, 2023

High costs/lack of budget and complexity of integrating automation tools within the existing ecosystem are the top challenges to network automation, according to the Tier 2/3 CSPs surveyed. These challenges are not unique to Tier 2/3 CSPs, as they are the same top two automation inhibitors identified by larger operators in other Heavy Reading research studies. Beyond these more universal challenges, significant factors for Tier 2/3 operators include staffing constraints, such as internal staff resistance to automation (#3), insufficient number of staff (#4), and lack of internal expertise for automation (#5).

Staffing challenges are not unique to Tier 2/3 operators, but they are felt more acutely by this segment. Tier 2 and Tier 3 operators have smaller operational budgets compared to Tier 1 operators, fewer workers, and (generally speaking, though not always) less opportunity to dedicate money to emerging technologies (see **Figure 5**).

Figure 5: What are the biggest challenges to achieving your network automation strategy? (Select top three)



n=217

Source: Heavy Reading, 2023

The Heavy Reading survey data supports this assessment. When the data is segmented by smaller Tier 2 and Tier 3 operators only (defined as annual revenue less than $200m), "insufficient staff" rises to the #2 challenge, surpassed only by high costs/lack of budget.

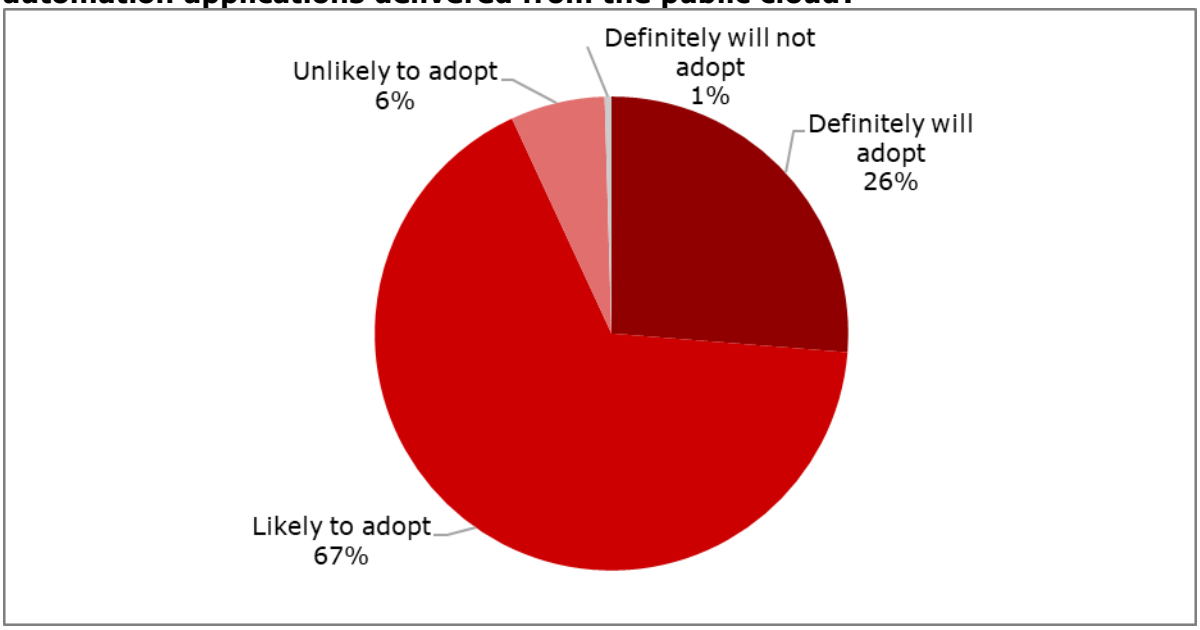
CLOUD-DELIVERED AUTOMATION

Public cloud delivery of software, or software as a service (SaaS), is well understood by organizations and is used in some form by 95% of Tier 2/3 CSPs in the survey. But what about applying cloud delivery to network automation applications and specifically using a public cloud in which resources are shared and applications are delivered over the internet?

The survey found that several key concerns must be addressed before CSPs will adopt SaaS-based network automation. These include concerns around customer data housed in a public cloud or private cloud, data traversing the internet without full encryption, meeting data sovereignty requirements (i.e., data travel out of the country or region not managed), and ensuring specific customer service-level agreement (SLA) thresholds.

However, despite cloud concerns, an overwhelming 93% of Tier 2/3 CSPs report that they are at least "likely to adopt" automation applications delivered using the public cloud. And over a quarter (26%) "definitely will adopt" public cloud-delivered automation (**Figure 6**). This strong endorsement of the public cloud model for automation is one of the biggest surprises of the study. The takeaway from the data is that SaaS concerns for network automation are manageable, with public Tier 1 cloud providers showing the way in scale, availability, reliability, and security.

Figure 6: How interested is your organization in adopting at least some automation applications delivered from the public cloud?



n=217
Source: Heavy Reading, 2023

Value of cloud-delivered automation for Tier 2/3 operators

The result is surprising given the newness of the technology, but perhaps less so given its potential to address the major pain points and requirements identified by Tier 2/3 operators throughout this study.

Automation integration complexity

CSPs large and small consistently report "complexity of integrating automation tools" as either the #1 or #2 challenge in automation. Therefore, addressing integration complexity is crucial for the future of network automation. The complexity of release alignment across various systems is a prevalent issue for integration. Innovation is often reduced to the lowest common denominator when on-premises systems are not updated to a release that supports the latest features and capabilities and complies with current standards.

SaaS-based automation simplifies integration complexity with an API-first approach. This means that the SaaS application architecture and codebase are designed to enable fast, easy, and secure API calls from other applications. With modern API documentation templates such as Swagger specs and automation tools for integrating APIs, application integrations are now made possible in hours, not weeks. In the SaaS model, another benefit

is that the release velocity is very fast. However, weekly updates or minor releases rarely affect APIs, instead offering API-level backward compatibility.

Staffing challenges

Staffing challenges factor highly as barriers to wider network automation adoption among Tier 2/3 CSPs, including internal resistance, lack of staffing, and lack of staff expertise. Among operators with less than $200m annually, insufficient staff is the #2 challenge. The SaaS model provides access to sophisticated applications without requiring internal expertise to maintain them.

Cloud-delivered automation is instantly accessible and does not require any staff to manage the infrastructure. SaaS applications are typically designed with modern web-based graphical user interfaces (GUIs) that are easier to use and require less training. In addition, cloud-delivered automation enables a single and shared source of key information. The centralization of network automation data and workflows that reduce required expertise also allows better collaboration among network operators, engineers, field technicians, and other specialists. Cloud-delivered automation also enables operators to share insights across different job functions to keep the ball rolling toward achieving desired outcomes such as increased productivity and reduced human errors, both of which will increase uptime and reliability.

Release agility

The survey results show that two-thirds of operators update their automation software frequently. The cloud model moves that burden from the operator to the software vendor. A monthly update cycle, for example, means 12 times less work for the CSP per year, reducing total cost of ownership (TCO). For those who do not update frequently due to lack of time and staff, automation as a service offers the benefit of much more frequent updating (again, with the update burden falling on the software vendor), which enhances the ability to innovate with new features faster.

One example of release agility is Juniper Networks, a pioneer in cloud-delivered automation software as part of its Cloud Metro solution. The vendor's automation cloud instance for Juniper Paragon Automation updates weekly so that customers can access the latest capabilities and enhancements to existing features based on a tight feedback loop. This means that users gain immediate access to the new release of the automation capabilities every week without having to deploy new software, such as in the on-premises model of operations. Faster access to the most updated software through a cloud-delivered model allows providers to rapidly differentiate their services with new features.

Implementation speed

Automation projects take many months to complete, the CSPs surveyed say. CSPs without in-house expertise rely on third-party vendors to do this work, but third-party automation projects take even longer. A successful cloud-delivered automation strategy will reduce—and potentially dramatically reduce—the time to implement automation and TCO.

Juniper data gathered from its own experience in SaaS trials indicates that it takes hours to days to fully set up an automation solution connected to network devices, as compared with do-it-yourself (DIY) projects that run into months. That is a significant improvement because 92% of CSPs surveyed by Heavy Reading indicate they currently complete their DIY automation in more than three months (with 51% of third-party automation projects taking more than six months).

Juniper's own data also concludes that deploying a new use case is even faster with SaaS, taking on average days instead of the months spent on DIY network automation projects.

Higher availability guarantees

Public Tier 1 cloud suppliers such as Google Cloud, Amazon Web Services (AWS), and Microsoft Azure often tout how their cloud platforms deliver more scalability and higher availability with resilience through geographic redundancy. It is common for public cloud-delivered solutions based on these suppliers to offer guarantees of 99.9% availability. Cloud-delivered network automation is also designed with the expectation that managed devices will continue to function without interruption to operations in the data or management planes.

A more secure environment

Public Tier 1 cloud suppliers also promote that their cloud platforms deliver better security, built-in by design. For example, data centers are ISO 27001 certified and follow industry standards for physical security. Role-based access mechanisms and logging capabilities are typically more robust, with a high degree of automation and damage control in case of breaches. Vulnerability and patch management are more proactive than in on-premises deployments.

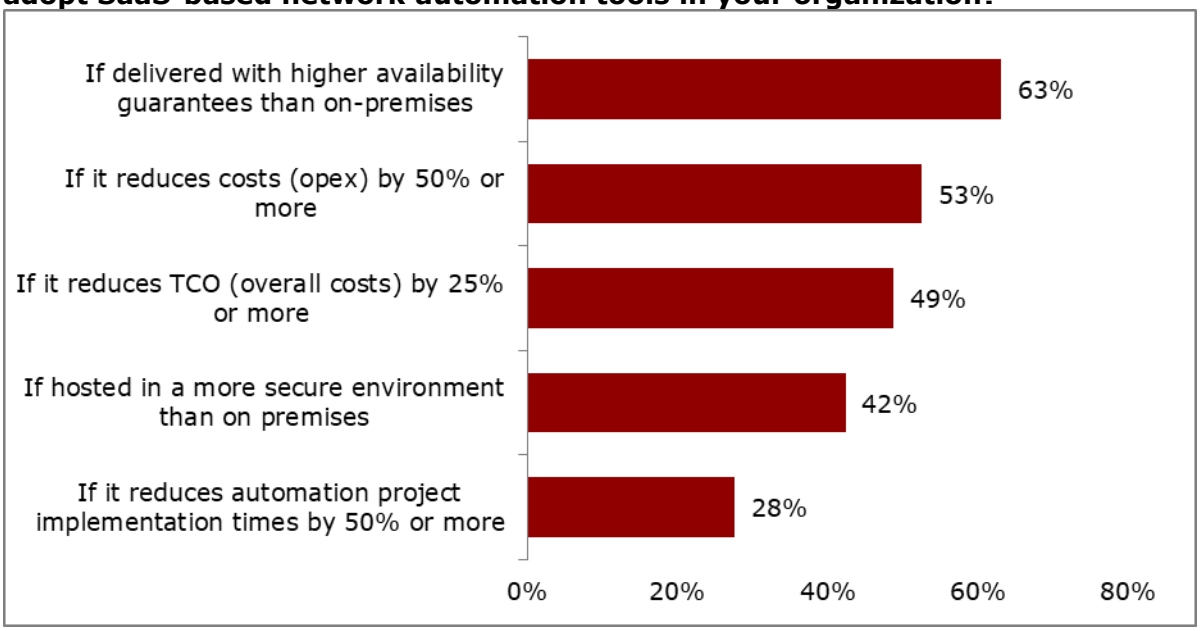
Vendors also play a crucial role. In terms of vendor design, it is important for cloud-delivered network automation solutions to consider security best practices by using industry-standard encryption for data in flight and data at rest. It is also important for them to put in place the needed administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of device data and network administrative data. In addition, cloud-delivered solutions enable frequent updates to keep the cloud secure and up to date with new features.

The business case for cloud-delivered automation

Cloud-delivered automation is not without its challenges, and operators have strict requirements for making the migration from traditional software to SaaS. In all instances, CSPs will weigh the pros and cons of SaaS against the status quo. Higher availability guarantees compared to on-premises (selected by 63% of respondents) top the list of factors that would support the business case for migration. Note that earlier in the survey, respondents cited increasing reliability as one of the main drivers to adopt automation. These results indicate that they will look to the cloud to help them achieve that goal (see **Figure 7**).

As expected, large reductions in opex and TCO are also crucial in making the business case for the cloud model. Interestingly, greater security compared to on-premises is important but is not a top three factor, based on the survey results.

Figure 7: Which of the following would support a business case or decision to adopt SaaS-based network automation tools in your organization?



n=217

Source: Heavy Reading, 2023

Role of AI

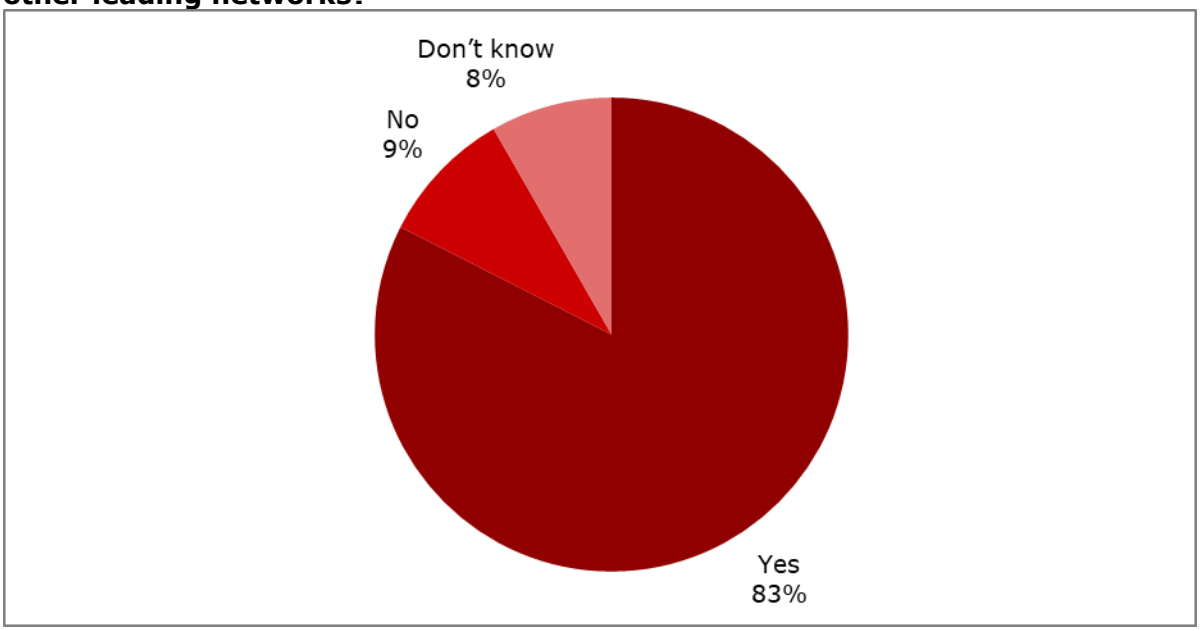
ChatGPT, Google's Bard, and similar AI applications based on advanced ML algorithms have rocketed AI to the top of C-suite discussions across nearly every industry—including communications. Executives have an urgent need to understand how their organizations will benefit from AI and ML to remain competitive and survive.

At this very early stage, Heavy Reading wanted to gauge the potential for advanced AI as an enabling technology in network automation. Thus, Heavy Reading asked Tier 2/3 CSPs if they would consider an AI-enabled SaaS solution that is also trained on other networks.

The pros of advanced AI trained on other networks are clear. Pooling aggregate and anonymized data across an entire industry greatly accelerates ML, leading to greater accuracy and quicker iterations of applications. Inhibitors include a required level of trust in AI and potential resistance to exposing anonymized traffic data and insights to AI systems.

In another major surprise, an overwhelming 83% of CSPs said that they would consider an AI-enabled SaaS solution which is also trained on other leading networks, showing a very high degree of interest in AI for their own use as well as that they would opt to share data for leveraging an even more advanced trained AI (**Figure 8**). With only 9% against AI-enabled SaaS, the pros clearly outweigh the cons and the potential fears of AI are overblown, at least for Tier 2/3 CSPs. The result is a major endorsement of the role of budding AI in cloud-delivered automation. Operators want to benefit from this emerging technology.

Figure 8: Would you consider an AI-enabled SaaS solution which is also trained on other leading networks?



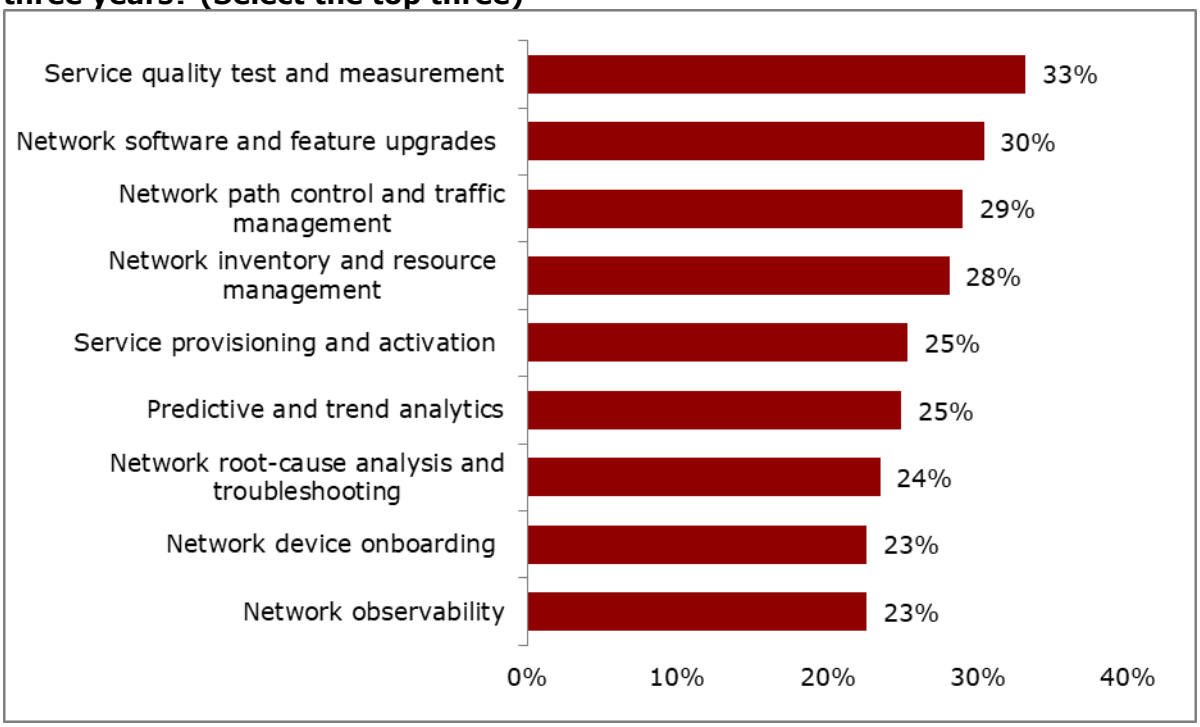
n=217
Source: Heavy Reading, 2023

Notably, the survey found that the top assurance capabilities of importance to CSPs were faster detection of service quality and network performance issues and faster root-cause analysis and problem diagnosis. When asked about selecting an assurance solution, 29% of the 217 CSPs surveyed said that their top desired outcome is an increased number of problems that can *only* be detected due to AI/ML. This may point to a desire to use AI/ML for network observability and troubleshooting to reduce mean time to know (MTTK) and mean time to repair (MTTR) using common AI/ML-based capabilities such as trend and predictive analysis, event noise reduction, and anomaly detection.

Automation use cases

Tier 2 and Tier 3 network operators have several use case priorities in mind for network automation. Their priorities are not the same as those of larger operators, based on Heavy Reading's research. Service quality test and measurement topped the list of priorities over the next three years, followed by network software/feature upgrades, network path control/traffic management, network inventory/resource management, and finally, service provisioning/activation and predictive/trend analysis (these last two tied for fifth place; **Figure 9**).

Figure 9: What are the primary use cases for network automation over the next three years? (Select the top three)



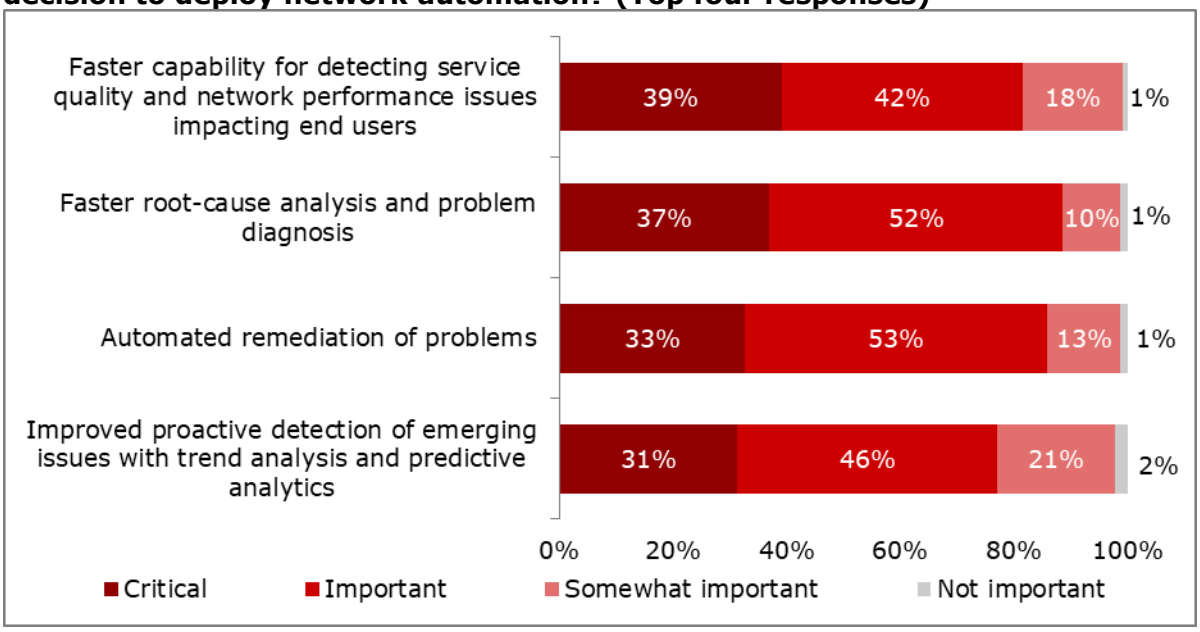
n=217

Source: Heavy Reading, 2023

The survey also examined a few use cases outside of this list in more detail to identify additional Tier 2/3 CSP priorities. Among the findings:

- Monitoring network trustworthiness and configuration compliance and capabilities to assess integrity to understand security vulnerabilities are highly important. 89% of Tier 2/3 CSPs reported these capabilities as at least "very useful," with 35% rating them as "extremely useful."
- Among service assurance capabilities, faster detection of service quality issues is "critical" for 39% of respondents, followed closely by faster root-case analysis ("critical" for 37%), automated remediation of problem ("critical" for 33%), and improved proactive detection of emerging issues with trend analysis/predictive analytics ("critical" for 31%; see **Figure 10**).

Figure 10: How important are each of the following assurance capabilities in your decision to deploy network automation? (Top four responses)



n=217

Source: Heavy Reading, 2023

CONCLUSION

Most Tier 2/3 operators have limited use of automation in their networks today, but they clearly see the value of expanding. 81% of CSPs surveyed by Heavy Reading believe that more network automation is needed to remain competitive and improve customer experience. These operators expect a broad role for network automation to address both customer-facing (external) and network-centric (internal) challenges.

Newer still is automation delivered via the cloud in the SaaS model. Significantly, 93% of Tier 2/3 CSPs report that they are at least *likely* to adopt public cloud-delivered automation in some form. For these Tier 2/3 operators, cloud-delivered automation promises the following key benefits:

- Reducing cloud automation integration complexity by moving the burden to the cloud software vendor, which would coordinate all releases, updates, and deployments and do so quickly.
- Addressing staff issues felt keenly by Tier 2 and Tier 3 operators, including insufficient staff count as well as insufficient in-house expertise.
- Increasing innovation velocity, with much faster release agility and automatic weekly updates that provide new features and functions that help them to innovate service offerings and stay competitive.

- Reducing DIY and third-party implementation times from many months to potentially weeks (or less).
- Delivering guarantees of higher availability and resiliency through the built-in redundancy of the cloud.
- Providing a more secure environment when implemented by using best practices refined by the hyperscalers.

Challenges exist for both network automation and the cloud delivery of automation, but this Heavy Reading survey shows that Tier 2/3 operators are confident that challenges are being addressed; they will look to automation software suppliers to help them adopt these technologies. Leading edge vendors, including Juniper Networks, are innovating to meet CSPs' network automation needs, most recently in network automation delivered via the cloud model.