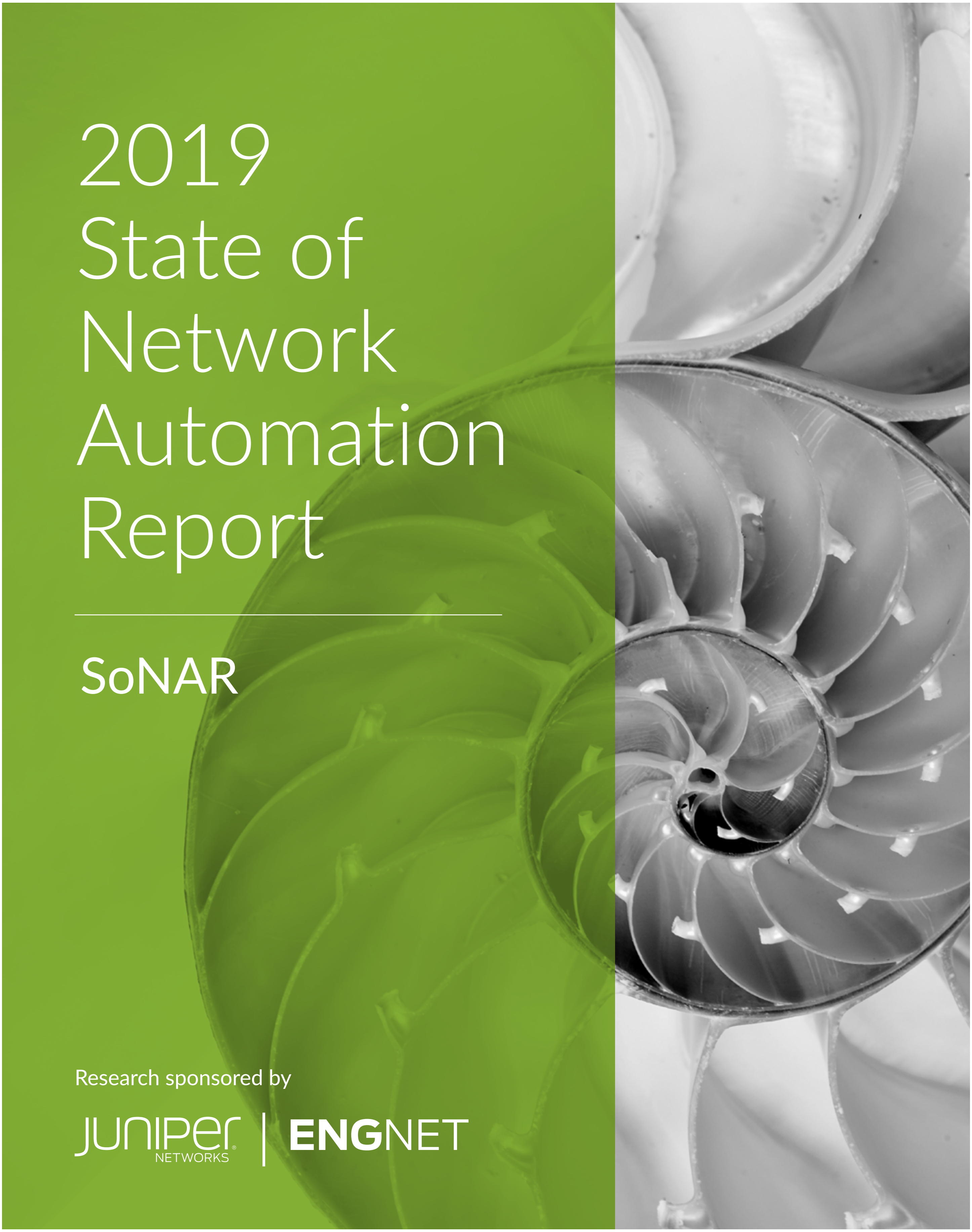


2019 State of Network Automation Report

SoNAR

Research sponsored by

JUNIPER NETWORKS | ENGNET

Contents

Join the Juniper community of engineers automating their way from simply building better networks to now making networking better.

Download and participate in future SoNAR research on Juniper Networks EngNet juniper.net/sonar

Share it on social #SoNAR

Executive Summary

Juniper Networks is a leader in network automation and network reliability engineering, bringing simplicity to networking with products, solutions, and services that connect the world. In May 2019, Juniper conducted inaugural research for the annual State of Network Automation Report (SoNAR), surveying 400 networking and security professionals from a diverse set of industries.

The SoNAR results provide insight into how network automation tools and behavior affect network operations (NetOps), both generating and correlating them with business performance, IT outcomes, and success factors for team and individual work.

This year we examined automation maturity, adoption, motivations, benefits, cultural behaviors, NetOps practices, and tooling. The 2019 SoNAR included many key findings:

96% of respondents are on an automation journey:

- 57% have 2-4 years of experience automating, while 8% have more than four years of experience
- 31% have started their automation journey within the past two years
- Mature automators from large enterprises outnumber those from small-to-medium enterprises 2:1
- Beginner or immature automators from small to medium enterprises outnumber those from large enterprises 2:1

Data center networks are the most automated:

- 43% of respondents are automating their data center networks
- Campus network automation is close behind at 39%
- NetOps time and weekly touch points are dominated by the campus and data center, at 74% and 68% respectively
- 76% of immature automators are touching their data center in NetOps weekly work—more than anywhere else. This represents both the biggest opportunity to benefit from data center automation and the most progress in this area.
- Mature automators are automating more than 50% of their data center NetOps work
- Three-quarters of respondents are automating at least 30% of their data center network

Security is the top driver for network automation:

- 67% of respondents ranked security as a *technology* driver for automation
- 60% of respondents ranked *business* agility as the top business driver for automation
- 33% of respondents ranked business agility as most improved factor due to automation
- Scaling staff or IT headcount efficiencies was the lowest motivator to automate

Those further along their automation journey are more often exceeding their business goals:

- Three quarters of respondents that are on average 40% or more automated are exceeding their business goals and score approximately 25% higher on goal performance
- 96% of respondents who have automated 50% or more of their network are exceeding their goals for network product or service quality to their stakeholders
- Of those respondents who are automating 40% or more of their work:
  - 83% exceeded their goals for network product or service quality
  - 75% exceeded their goals for security product or service quality
  - 77% exceeded their goals for operating efficiency
  - 71% exceeded their goals for customer or stakeholder satisfaction

Employee job satisfaction and performance are strongly correlated with automation:

- Of those respondents who are automating 40% or more of their work, over 90% agree or strongly agree that:
  - They are satisfied with the work they do
  - They regularly reach high productivity
  - They have the tools and resources to do their jobs well
  - Their job makes good use of their skills
- Of those respondents who are automating 40% or more of their work, they're about 30% more likely to report high job satisfaction and performance

High-performing organizations have healthy cultural behaviors to foster automation:

- 92% have good visibility into errors, outages, and issues
- 85% have a culture of continuous improvement where opportunities for improvement are valued and acted upon
- 79% have service levels that are measured and reported with transparency to stakeholders
- 78% have service-level objectives

Keeping up is difficult for IT organizations and individuals, but helped with automation:

- Immature automators are twice as likely to be encumbered by budget or financial restraints
- 52% of respondents report the overwhelming number of technology choices as an impediment to adopting automation
- 48% of respondents suffer from lack of time on the job to learn automationThree-quarters of respondents are automating at least 30% of their data center network

Automators make changes faster, more frequently, and more reliably:

- Mature automators complete more than 50% of changes in under a day, while immature automators complete only 22%
- Beginners make changes most infrequently—weekly to monthly
- Only 8% of respondents make daily changes to their networks
- More than half the respondents reported that approximately 10% of the changes they made resulted in an outage or degraded service
- Respondents automating for more than three years outnumbered those with less automation history 3:1 in reporting fully successful changes

Mature automators suffer fewer service degradations and remediate faster:

- Half of mature automators report that it takes less than a day to restore service
- More than half of immature automators report most outages take more than a week to remediate
- Those who automate find themselves in a virtuous cycle that gives them more time to spend on strategic or transformative endeavors, while those who fail to automate are pulled further into the vicious cycle of firefighting to simply keep the lights on

Most organizations advance their automation endeavors in multiple ways:

- More than half of respondents' organizations will:
  - Hire new talent
  - Invest in training staff
  - Dedicate part of the team to automation
  - Use professional services
  - Build custom and NetOps contextual automation
  - Buy turnkey vendor products
- Beginners were the least likely to have a dedicated team focused on automation and were less likely to build customer NetOps contextual automation, which requires inhouse engineering expertise
- Beginners were less likely to invest in upleveling the existing talent pool, opting instead to hire new people or bring in outside resources such as professional services; while this strategy is a useful bootstrap, it shouldn't preclude training existing staffThey are satisfied with the work they do

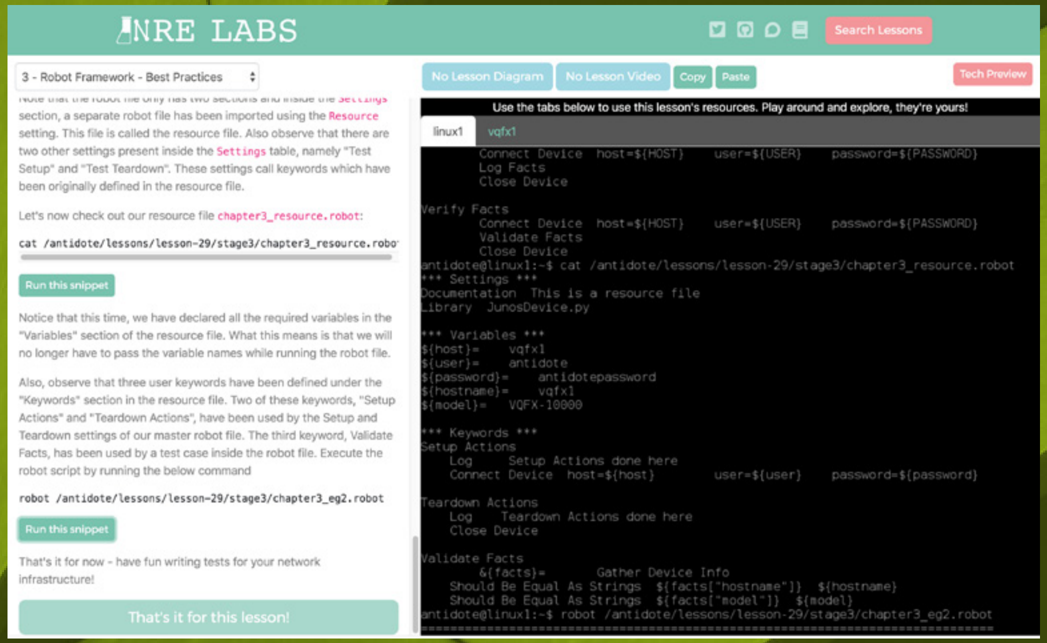
Paradoxically, configuration management tooling has the highest adoption rate for automation, while network provisioning, deployment, and configuration consume the least NetOps activity:

- Network monitoring is where most NetOps time is spent
- 53% of respondents are using configuration management tooling
- 50% are using event-driven frameworks
- 38% are using custom monitoring tools and telemetry collection
- 37% are using source-code management and infrastructure as code tools
- 36% are using container tooling
- 35% are using software-defined networking (SDN) tools

NRE LABS

An automation dojo in your browser. Learning to automate is now free, open, easy, and fun.

Learn more



Note that the robot file only has two sections and inside the Settings section, a separate robot file has been imported using the Resource setting. This file is called the resource file. Also observe that there are two other settings present inside the Settings table, namely "Test Setup" and "Test Teardown". These settings call keywords which have been originally defined in the resource file.

Let's now check out our resource file chapter3_resource.robot:

```
cat /antidote/lessons/lesson-29/stage3/chapter3_resource.robo
```

Notice that this time, we have declared all the required variables in the "Variables" section of the resource file. What this means is that we will no longer have to pass the variable names while running the robot file.

Also, observe that three user keywords have been defined under the "Keywords" section in the resource file. Two of these keywords, "Setup Actions" and "Teardown Actions", have been used by the Setup and Teardown settings of our master robot file. The third keyword, Validate Facts, has been used by a test case inside the robot file. Execute the robot script by running the below command

```
robot /antidote/lessons/lesson-29/stage3/chapter3_eg2.robot
```

That's it for now - have fun writing tests for your network infrastructure!

Use the tabs below to use this lesson's resources. Play around and explore, they're yours!

```
        Connect Device  host=${HOST}    user=${USER}    password=${PASSWORD}
        Log Facts
        Close Device

Verify Facts
        Connect Device  host=${HOST}    user=${USER}    password=${PASSWORD}
        Validate Facts
        Close Device
antidote@linux1:~$ cat /antidote/lessons/lesson-29/stage3/chapter3_resource.robot
*** Settings ***
Documentation  This is a resource file
Library  JunosDevice.py

*** Variables ***
${host}=    vqfx1
${user}=    antidote
${password}=    antidotepassword
${hostname}=    vqfx1
${model}=   VQFX-10000

*** Keywords ***
Setup Actions
    Log     Setup Actions done here
    Connect Device  host=${host}        user=${user}    password=${password}

Teardown Actions
    Log    Teardown Actions done here
    Close Device

Validate Facts
        &{facts}=       Gather Device Info
    Should Be Equal As Strings  ${facts["hostname"]}  ${hostname}
    Should Be Equal As Strings  ${facts["model"]}  ${model}
antidote@linux1:~$ robot /antidote/lessons/lesson-29/stage3/chapter3_eg2.robot
==============================================================================
```

Respondent Demographics

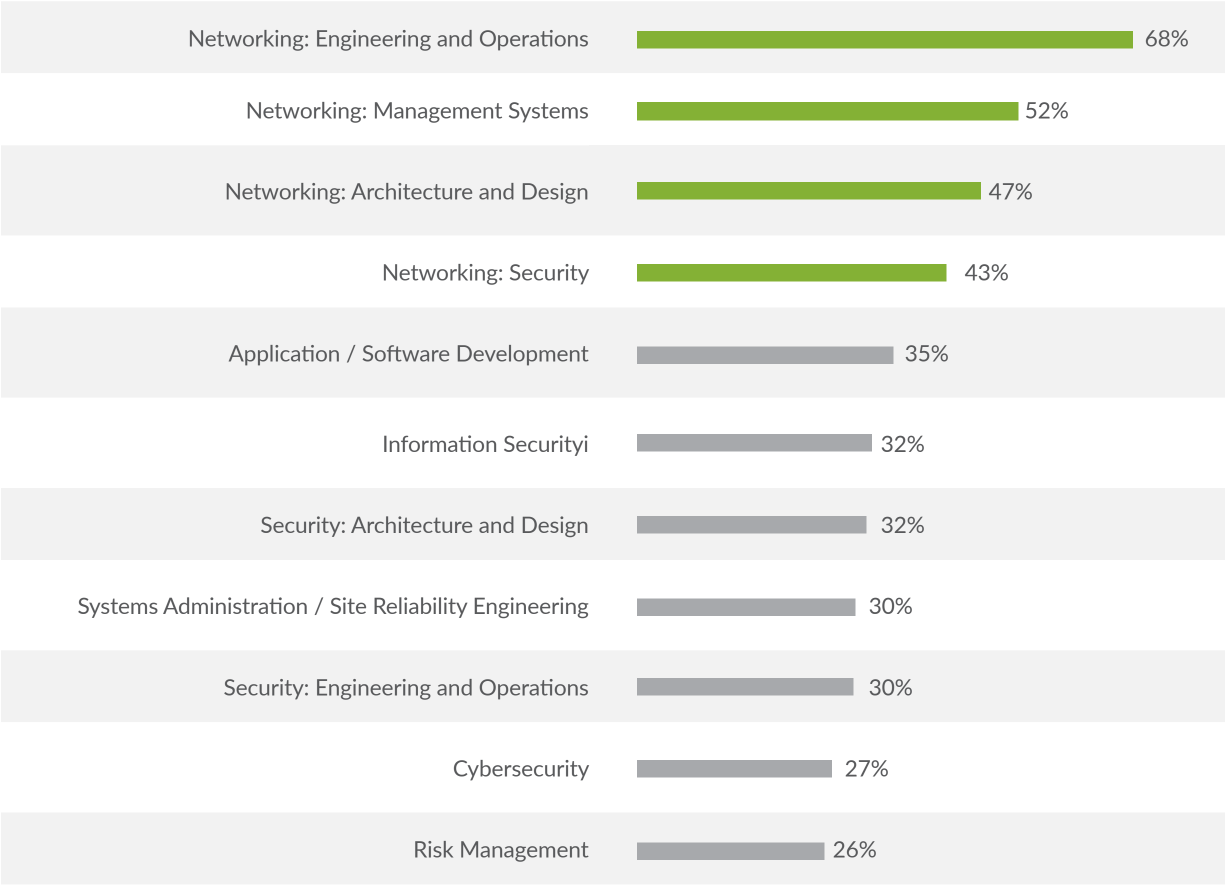
The research behind the 2019 State of Network Automation Report (SoNAR) included interviews with 400 respondents from across the USA. In future reports, we aim to extend the survey globally, but for this inaugural report, we elected to concentrate on one large geography.

All respondents were networking professionals that identified their typical weekly job functions as at least one of the following:

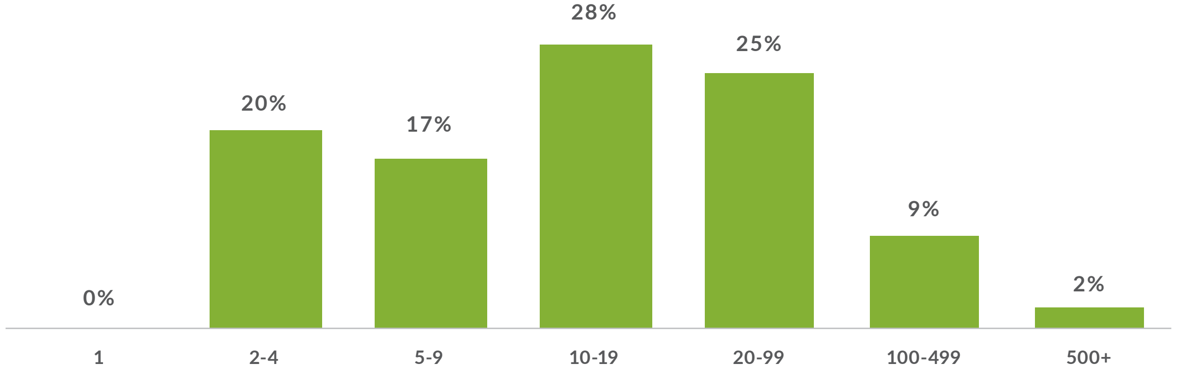
- Networking: Engineering and Operations
- Networking: Management Systems
- Networking: Architecture and Design
- Networking: Security

Demographics

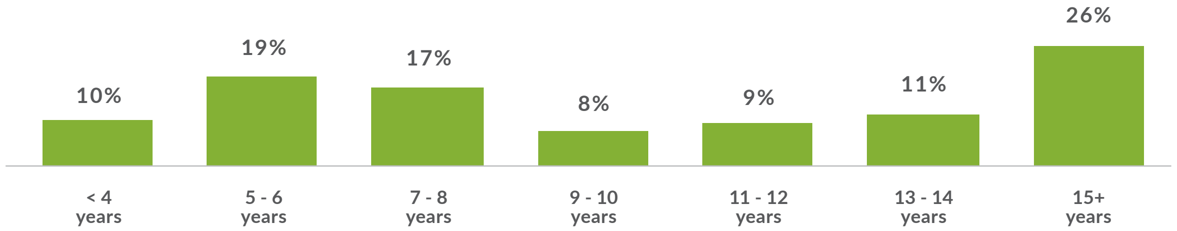
Department



Number of Employees in Networking Team

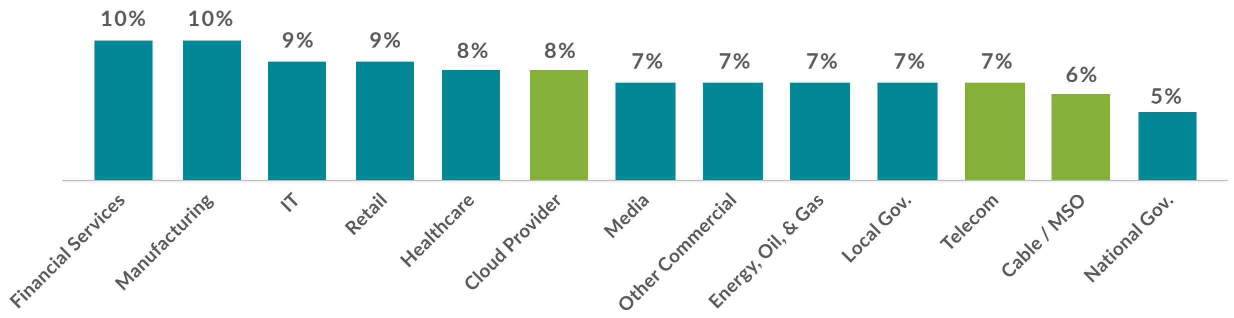


Tenure

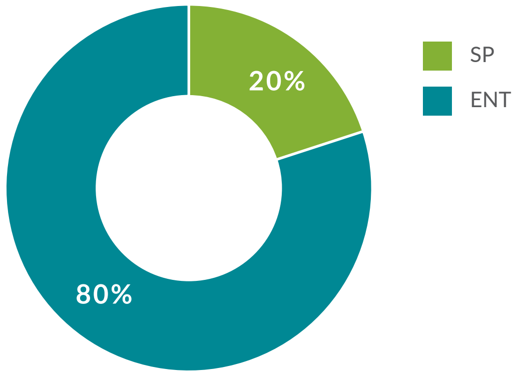


Firmographics

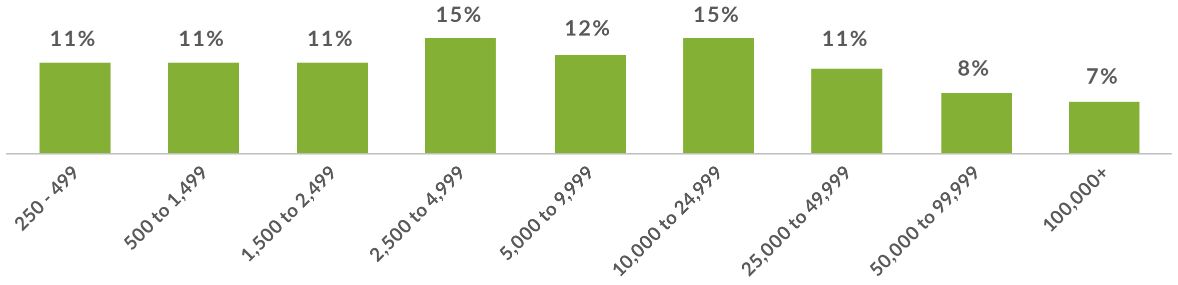
Industry



Service Provider vs. Enterprise



Number of Employees in Organization



Automation Maturity and Adoption

The Evolution of Network Operations

The desire to automate and program networks is as old as networks themselves. Early attempts at automation saw little success, but with the emergence of widespread IP networking and the growth of the internet, the demand for network engineering exploded. To deal with the demand for networking and the lack of processes for automating networks, responsibility for network operations was simplified from technologist to technician, mainly because of the move to network device command-line interfaces (CLIs). Network security specialists at the network infrastructure level followed suit.

Fast forward to today. The network CLI is still a staple, but it's increasingly being replaced by higher-order tools such as graphical user interfaces (GUIs), application programming interfaces (APIs), and various other tools that abstract control and management above the level of the individual device and its commands. To varying degrees, these solutions may be considered automation tools that allow engineers to refocus their energies on building systems that support business service levels rather than device-level operations.

Looking back, a decade of network innovation like new protocols, new architectural paradigms, and new APIs stemmed from industry discussions around programmability. That desire for programmability led to the development of software-defined networking (SDN) and more recent trends like intent-based or intent-driven networking.

In the same timeframe, server systems administration has similarly been driven—even forcibly pulled—away from manual operations by the evolution to DevOps and site reliability engineering (SRE). These trends brought together the worlds of software development and operations with a focus on automation to improve velocity, agility, scale, security, and reliability.

The modern-day impact and influence of these movements on networking automation are undeniable. SDN and intent-driven networking adoption was reported by 35% of SoNAR respondents, and over the past few years we have seen new networking job titles like Network Reliability Engineer (NRE), inspired by DevOps and SRE.

While only 8% of respondents have four or more years of experience automating network operations, the journey is well underway; 57% of SoNAR respondents started their transition to automation between two and four years ago.

Automation Maturity Assessment

In this report, we look at several findings through the lens of respondent self-assessed automation maturity and experience. We denote respondents at these four levels from least to greatest experience:

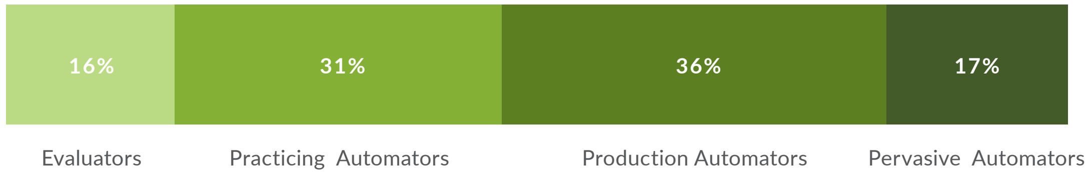
Evaluators reported no experience operating above GUIs or CLIs (only 4%), or are just beginning (12%) to automate beyond those with other tools and scripting.

Practicing Automators reported automating in a test, development, or lab environment, but not yet in production networks.

Production Automators reported automating production network environments, but not in all places. For example, they may have automated some data center networks, but not all. They may also be automating in some areas such as the WAN and in data centers, but not in places like campus and branch networks.

Pervasive Automators reported automating in production across all places in their networks.

Automation Maturity of Respondents



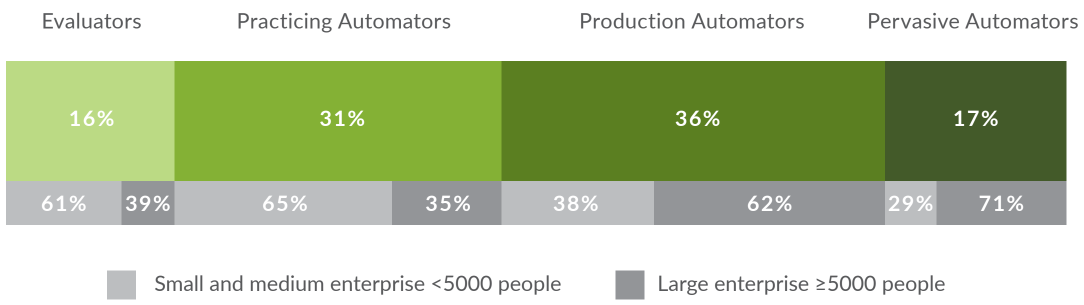
This chart does not indicate how automation is defined in the eyes of each respondent, nor does it indicate to what extent their operations are automated. Some people may consider the deployment of a single SDN system as automation, while others may be using event-driven infrastructure and still others may be pushing configurations with Ansible. In later SoNAR sections, we present respondent choices in technology, practices, behaviors, and culture—all things that shed light on how automation is defined. Later in this section, we also explore to what degree respondents feel they are automated in each domain.

The relationship of organization size to automation maturity

While the SoNAR survey results were roughly split between large enterprises (companies with more than 5000 employees) and small and medium enterprises, the maturity results show that 65% of the Production and Pervasive Automators belong to large enterprises, whereas 62% of the Practicing Automators and Evaluators work in small and medium enterprises.

This shows the propensity for larger organizations to be further ahead in their automation journey, which we hypothesize is due to the fact that larger, more demanding network architectures need to be automated sooner. Larger enterprises are also more likely to have in-house development teams whose DevOps practices may cross-pollinate into network teams. Notably, three times as many Pervasive Automators were from large enterprises vs. small and medium enterprises, whereas the Production Automators were more evenly balanced.

Automation Maturity by Organization Size



Automation Adoption

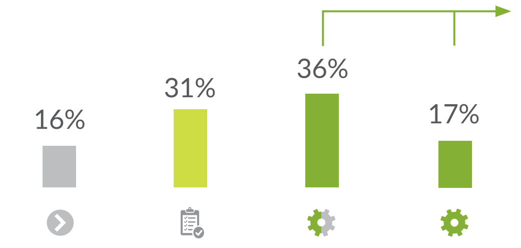
How far into the timeline are we when it comes to network automation?

While more than half of respondents are automating in production, only about a third of them are automating pervasively across all network places. Not surprisingly, among Pervasive Automators, three times as many respondents—18%—said they had been on their automation journey for more than four years. This confirms that a higher assessed maturity level goes hand-in-hand with more experience, if we assume that pervasive automation takes more time to accomplish.

Of the two groups still evaluating and learning to automate, not surprisingly, more than half are less than two years into their journey.

> 88% of all organizations have been automating for less than 4 years.

Time Automating by Respondent Maturity



- 53% are automating in production
- The majority state that their automation journey has lasted less than 4 years
- One-third are already testing in select areas, while very few are in the beginning stages of automation

	Total	Evaluators	Practicing	Production	Pervasive
Not automating	4%				
Less than 2 years	31%	**55%**	53%	13%	19%
2 - 3 years	31%	22%	25%	**45%**	26%
3 - 4 years	26%	16%	16%	36%	**37%**
4+ years	8%	6%	5%	6%	**18%**

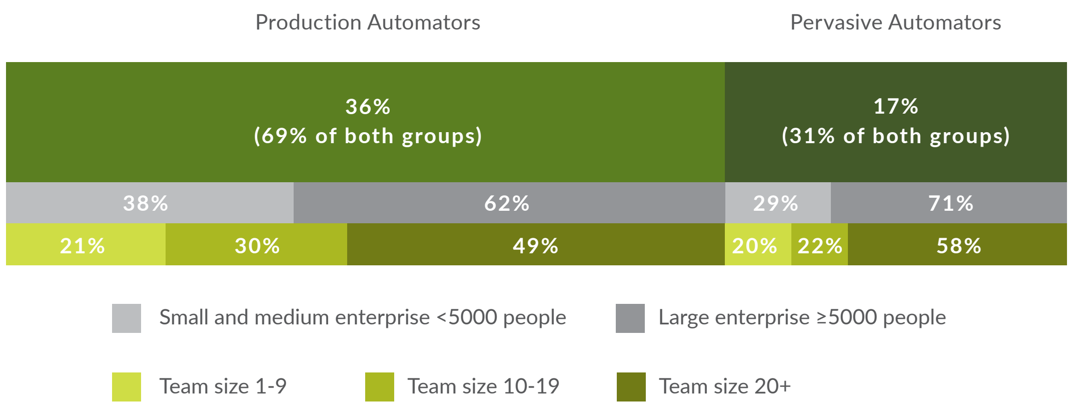
One might expect the more experienced, mature Pervasive Automator group would outperform the Production Automators. However, as you will see, in many metrics throughout the report, the exact opposite is true. In fact, it is the Production Automator group that most often reports the positive outcomes we'll cover in the next major section.

This curious finding will result in some interesting research questions in our next version of SoNAR. Until then, we can only speculate on the reasons for this based on some correlations:

Team Size Respondents in the Pervasive Automators with a team size of more than 20 people outnumber the teams with less than 20 people by 3:1. In the Production Automators group, this ratio is closer to 1:1.

Organization Size While both Production and Pervasive Automators tend to come from large enterprises, respondents in the Pervasive Automators group are far more biased toward large enterprises.

Mature Automator Groups by Organization and Team Size



This conundrum raises some questions for future research, including:

- Are enterprises better off focusing on solving for automation culture, processes, and tools within one domain, or fewer domains at a time?
- Are the more experienced Pervasive Automators slower to adapt to the latest processes and tools because they come from larger teams or because they are trying to solve for a common toolchain that needs to be applied across more network domains? If so, which factors slowing them down are leading to slightly lower performance?

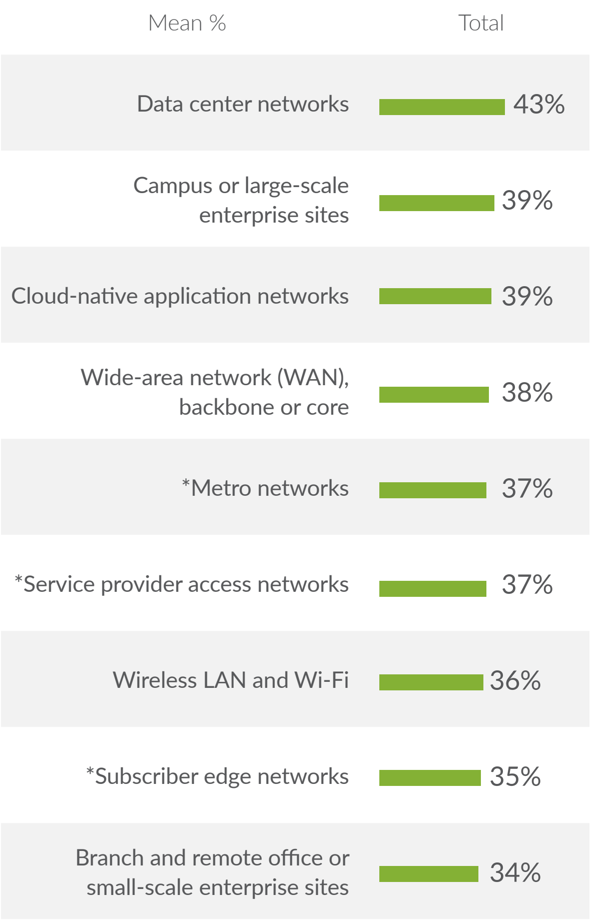
Another possibility to consider is how respondents define automation and decide whether a domain is automated. Perhaps Pervasive Automators are sprinkling a little automation everywhere, while the Production Automators focusing their hardcore automation efforts in a few select domains. For those Production Automators, it's not that there is no automation in their other network domains; it's possible they just consider the automation there too rudimentary to count.

To counterbalance this strange result in some areas, we also look at results grouped by other maturity indicators like experience automating in years and the average degree to which their networks are automated.

In which domains is adoption most advanced?

We asked SoNAR respondents to rate their various network domains for the degree to which they are automated on a percentage scale.

Average Automation by Network Domain



*Data is representative of SP audience only

Averaging the results per domain, we see that respondents indicate that data center networks are the most automated, followed by campus sites and cloud-native application networks.

Given the push for enterprises to evolve data centers into private clouds and operational factors which make data centers more readily automated, these results are not surprising. Furthermore, as a close second to campus sites, data centers are where respondents indicated they spent the most amount of time. As we will see later in the NetOps Practices section, the data center is also the area where, by far, most Evaluators spend their time. Thus, the data center domain shows both the most operational opportunity for automation and the most focus and progress.

When we break out the average results per domain across maturities, the data center scores even higher as an area of automation adoption with the mature Production and Pervasive Automators. The data center was also the area where the fewest respondents—only 2%—reported no automation at all.

Average Automation by Network Domain and Maturity

Mean %	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Data center networks	43%	14%	35%	52%	**59%**
Campus or large-scale enterprise sites	39%	14%	29%	48%	**56%**
Cloud-native application networks	39%	9%	32%	47%	**54%**
Wide-area network (WAN), backbone or core	38%	15%	29%	48%	**51%**
*Metro networks	37%	7%**	27%**	42%	**52%****
*Service provider access networks	37%	8%**	29%**	35%	**58%****
Wireless LAN and Wi-Fi	36%	16%	26%	45%	**48%**
*Subscriber edge networks	35%	13%**	21%**	38%	**52%****
Branch and remote office or small-scale enterprise sites	34%	7%	27%	40%	**52%**

*Data is representative of SP audience only **Low base size, use data directionally only

In every network domain, the Pervasive Automators rated their automation deployment stronger than the other groups, and most groups rated data center networks as their most automation-forward domain. The sole exception were the Evaluators, where Wireless took the top spot. Interestingly, wireless took the bottom spot among the Pervasive Automators, though all domains were rated within a tight range.

For the degree of automation adoption, we grouped the individual percentage ratings in each network domain into ranges and measured the number of responses. Here again, the data center stood out as the domain where automation deployment is the greatest, but it is generally encouraging to see many domains where a large number of respondents reported 50% or greater automation of their processes.

Degree of Automation by Network Domain

	No Automation	1-29% Automated	30-49% Automated	50% or Greater	70% or Greater
Data center networks	2%	25%	24%	**44%**	12%
Campus or large-scale enterprise sites	6%	25%	**35%**	31%	11%
Cloud-native application networks	7%	24%	28%	**38%**	9%
Wide-area network (WAN), backbone or core	2%	29%	32%	**33%**	11%
Wireless LAN and Wi-Fi	5%	31%	**33%**	27%	9%
*Metro networks	6%	28%	**34%**	32%	12%
*Service provider access networks	9%	27%	29%	**35%**	7%
Branch and remote office or small-scale enterprise sites	12%	26%	28%	**30%**	7%
*Subscriber edge networks	4%	**35%**	30%	30%	9%

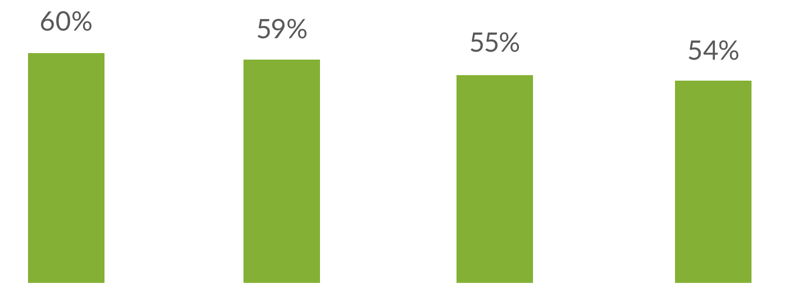
*Data is representative of SP audience only

Automation Motivations and Benefits

The Drivers of Automation

In researching factors within the SoNAR respondents' organizations that drive automation, we separated the business factors from technology factors.

Business Factors Driving Automation



	Business Agility	Cost Savings	IT Service Reliability	IT Service Delivery Efficiency
Evaluators	55%	**64%**	52%	61%
Practicing Automators	**58%**	53%	53%	41%
Production Automators	**65%**	62%	63%	57%
Pervasive Automators	56%	57%	46%	**62%**

The business drivers

While none of the main motivating factors were a runaway leader, business agility did emerge as the primary driver.

Looking more closely at the maturity groups, none of them ranked these four factors in the same order. We believe this is because motivations change as performance in some areas improves.

It's also worth noting that while the net ranking listed agility, costs, reliability, and efficiency as the primary drivers in that order, agility and reliability are the most closely related, while costs and efficiency are also closely related. DevOps professionals, SREs and NREs are well aware that achieving reliability is critical before pursuing speed and agility, since speed without reliability will often result in failure. Even in endeavors that symbolize speed, like racing or rocket science, there is no result without reliability first.

While agility and reliability embody effectiveness, cost savings and effective IT service delivery are obviously related to efficiency. Surprisingly, both ends of the maturity scale—the Evaluators and Pervasive Automators—rated these efficiency factors as more important than the other two factors of effectiveness. As for the groups in the middle of the maturity spectrum—the Practicing and Production Automators—both rated the effectiveness factors of agility and reliability as more important than the efficiency drivers.

With so much of the automation IT narrative focused on agility and reliability, this raises questions about those focused on efficiencies, like:

- Are the more experienced Pervasive Automators past the point of doing the right (effective) things and more keenly focused on functional efficiency?
- Are costs and efficiencies simply a greater imperative in large enterprises, which represent three quarters of the Pervasive Automators group?
- Do Evaluators realize that learning automation is an additional cost, and thus costs will probably rise before they fall?
- Are Evaluators just naïve in their approach of pursuing automation tasks in shorter, more efficient, periods of time regardless of whether a given method is the most effective? If so, they may end up working harder and longer to make up for their method's lack of effectiveness, or learn later that entirely different, more effective strategies exist.

We won't attempt to answer these questions in this report, but it is instructive to see the performance differences in the rest of this section. Of course in business, effectiveness and efficiency must be balanced and exercised at different times to maximize growth and profitability, respectively.

Technology Factors Driving Automation

	Total	Evaluators	Practicing Automators	Production Automators	Pervasive Automators
Security	67%	58%	56%	**78%**	71%
Improving mean time between failure	55%	50%	49%	**62%**	56%
Reducing hard and repetitive work	54%	47%	48%	**63%**	53%
Improving incident response and time to resolution	53%	58%	42%	**65%**	46%
Keeping current on network technologies	51%	44%	50%	52%	**54%**
Sustaining innovation	51%	42%	47%	**56%**	54%
Service uptime levels	50%	42%	46%	53%	**59%**
Compliance	49%	44%	36%	**62%**	50%
Improving time to change	47%	33%	51%	**52%**	44%
Service experience levels	46%	39%	42%	**53%**	46%
Scaling efficiency of network footprint relative to staff headcount	42%	30%	37%	45%	**53%**

The technology drivers

Among the technology drivers for automation, security is clearly a huge step above other factors within all organizations. This is true overall and within each maturity group, as well as in other groupings not shown, like small and medium vs. large enterprises. With such a standout difference, we have devoted a separate section to security automation to explore this in more depth.

> Security tops the list of drivers for automation.

Another notable result is how low respondents ranked scaling staff efficiency. One of the popular misconceptions about network and security automation is that it eliminates jobs; however, these results clearly show that across all maturity groups, automation either creates (sometimes different) jobs or at the very least changes them. This result starkly contrasts with the top technology drivers, which are mostly about automating to achieve greater reliability, which—in descending order of rank—encompasses security, MTBF, MTTR, uptime, compliance, and experience levels. Other innovation and especially agility-related factors, like time to change, come in lower on this list.

The Business Impact of Automation

After we asked respondents which business drivers motivated their organizations to pursue network automation, we inquired about the one factor that has shown the biggest improvement so far: business agility.

Business Factor with The Greatest Improvement due to Automation

Drivers with biggest improvement	Total	Evaluators	Practicing Automators	Production Automators	Pervasive Automators
Business Agility	34%	30%	26%	**40%**	37%
Cost Savings	26%	27%	**34%**	19%	24%
IT Service Reliability	18%	17%	**25%**	15%	13%
IT Service Delivery Efficiency	23%	**26%**	15%	**26%**	**26%**

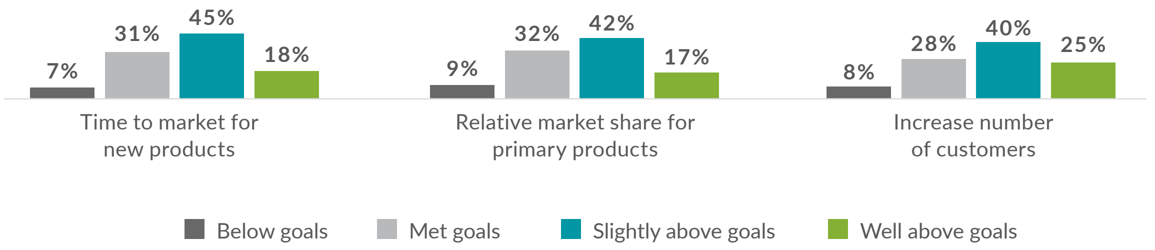
Business agility took the top spot for all but the Practicing Automators group, which ranked it second. Few respondents in the Production and Pervasive Automator groups ranked cost savings as the primary area improved, but the Practicing Automators ranked cost savings as their primary area improved over the others. The variance between the groups suggests that different factors come to the fore at different phases of automation adoption.

Automating IT service-level reliability ranked last. This is interesting because as described above, reliability should precede speed and agility. Perhaps because reliability is so foundational to network engineering, it's the least changed. Indeed, improving agility while holding reliability constant are wins on both fronts, even though agility is more noticeable in such a case. Or possibly, because network engineers are so close to the pain of reliability hick-ups, improvements may be less remarkable when reliability continues to be managed instead of maximized.

Additional survey questions reported stronger indicators, with organizational performance generally improving with automation.

We asked respondents to rate their organization's performance over the past year based on their goals using a scale of below, meeting, above, and well above meeting their goals. We did this based on these indicators: time to market for new products, relative market share for primary products, and increased number of customers.

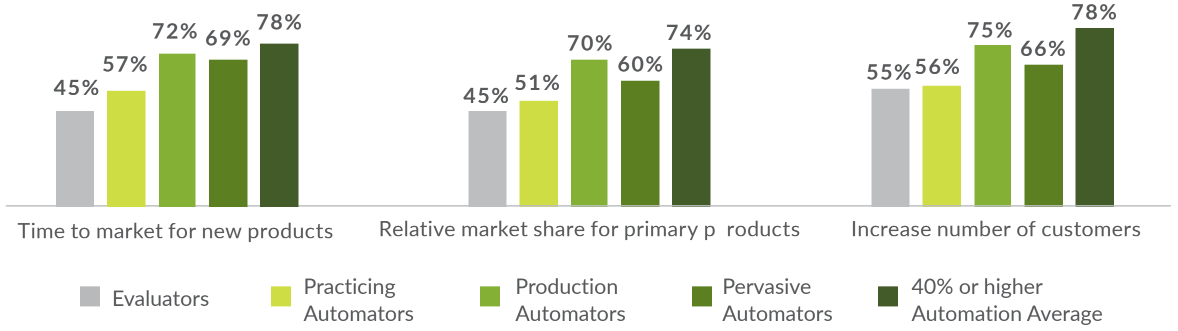
Organization Performance in the Past Year



Most SoNAR respondents scored their organizations par for the course or better, with 63%, 59% and 65% of respondents saying they exceeded their goals for the three measures, respectively. This also meant we had a good sample of respondents exceeding their goals, allowing us to meaningfully see where they are by automation maturity.

Organization Performance in the Last Year by Automation Maturity

Slightly above/well above goals



Across the board we see higher organizational performance for the Automators, but curiously the Pervasive Automators are slightly lower performing than the more narrowly focused Production Automators.

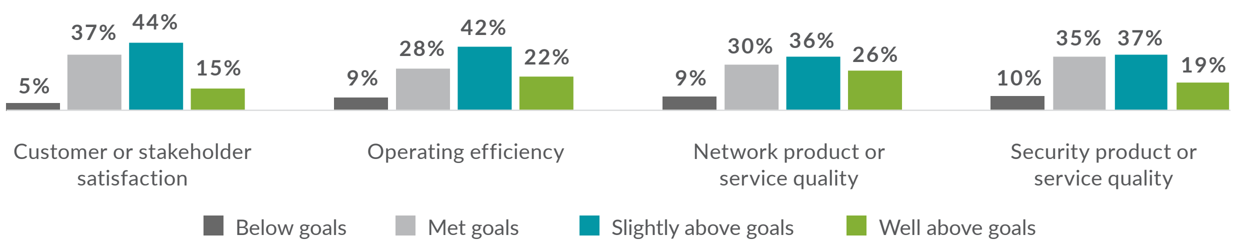
We also measured performance based on the degree to which respondents were automated. Recall we saw the results to which respondents were automated by network domain earlier in the report. When averaging out the scores across all network domains, roughly one third of the respondents were 30% or less automated, one third were 30-39% automated, and one third 40% or more automated. With that division, no group is too small to be statistically irrelevant for comparison, and those that are 40% or more automated showed far better performance as a group, topping all others by maturity. This 40%+ group also scored 23-27% higher in goal performance than those that were 30% or less automated on average (not shown).

In summary, organizations that are further ahead in their effort to automate their networks and security, are more often exceeding their business goals.

The Team Impact of Automation

Similar to the survey on organizational performance, we asked SoNAR respondents to rate their team's performance over the past year using a scale of well below, below, meeting, above, and well above meeting their goals. We did this based on the following team performance indicators: customer or stakeholder satisfaction; operating efficiency; network product or service quality; and security product or service quality. The product or service quality scores were an aggregation of perceived quality, one can assume that those scores include reliability factors such as MTBF, MTTR, and security threat effects and containment; user and application experience factors in latency, jitter, and throughput.

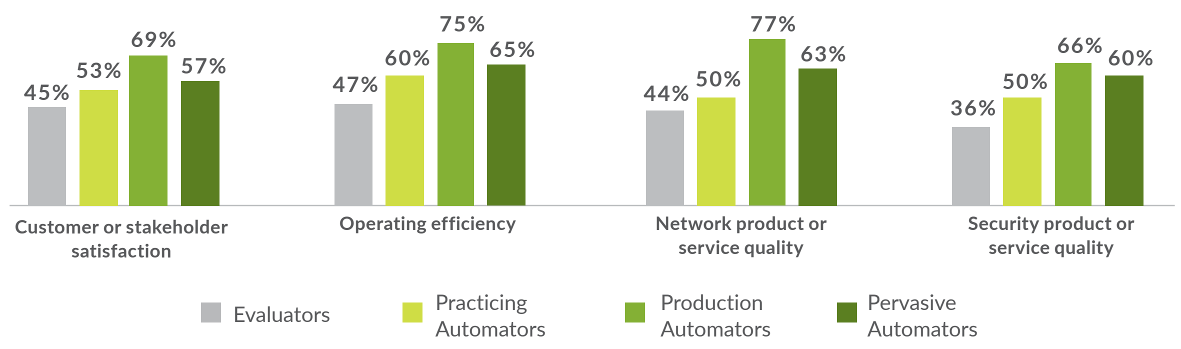
Team Performance in the Past Year



Again, most respondents scored their organizations meeting their goals or better, giving us a meaningful sample of respondents exceeding their goals to correlate with other aspects.

Team Performance in Past Year by Automation Maturity

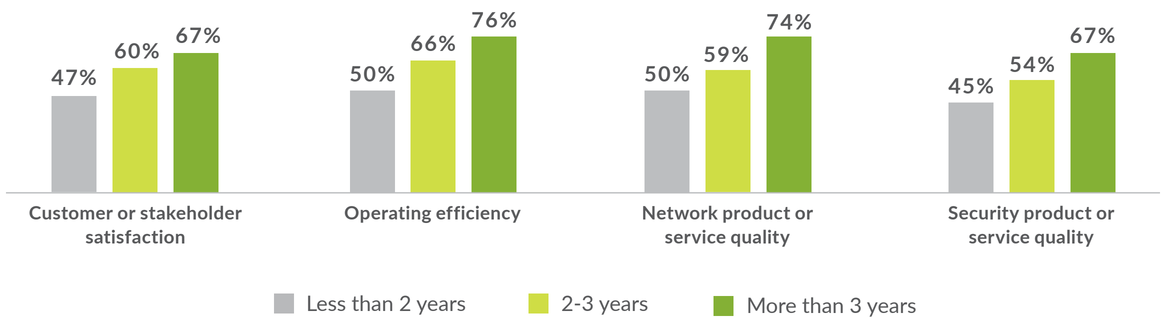
Slightly above/well above goals



Curiously, when looking at team performance indicators by self-assessed automation maturity groups, here again we see Production Automators out-performing the Pervasive Automators. As mentioned above, one factor contributing to this outcome is that the Pervasive group is biased toward large enterprises. With other organizational performance indicators, we didn't observe much discrepancy between small and medium vs. large enterprises, but for these team performance indicators, in fact, the respondents in small and medium enterprise organizations did rank slightly higher. For more consistency and clarity, look at the other groupings reported below.

Team Performance in the Past Year by Time Automating

Slightly above/well above goals

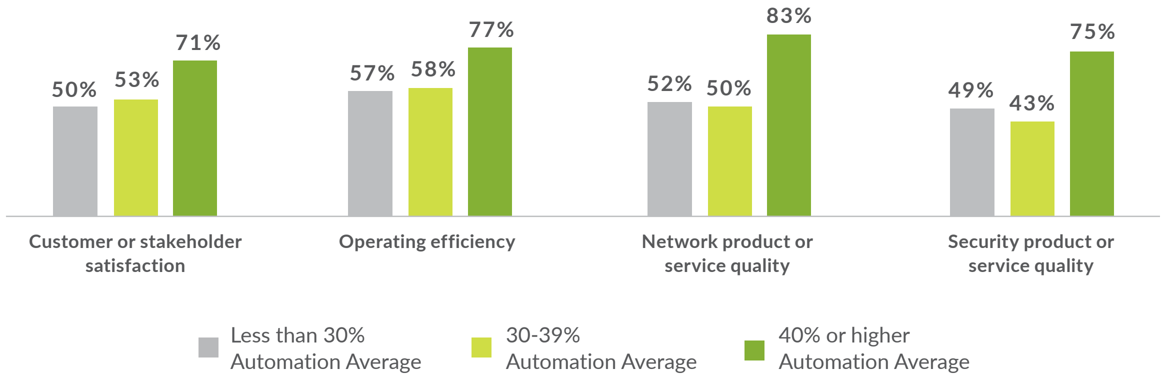


When we group by the time automating, we can segment our respondents into approximate thirds by groups automating less than two years, two-to-three years, and more than three years.

When we look at the same performance indicators, those with longer histories and more experience with automation clearly correlate with superior performance.

Team Performance in the Past Year by Automation Deployment

Slightly above/well above goals



Again, we also measured performance by the degree to which respondents were automated. Recall that we saw statistics that indicated how respondents deployed automation by network domain earlier in the report. When we averaged out scores across all network domains, respondents were roughly one third 30% or less automated, one third 30-39% automated, and one third 40% or more automated. With that breakdown, all groups are statistically relevant.

Those 40%+ automated showed far better performance as a group. Not only do they tower above those with less automation deployed on average, but this group also stands higher than those with three or more years of automation experience and any automator maturity group.

Among the group averaging 40% or higher automation deployment across all network domains, it's impressive that 83% of them—150 respondents out of 180—are exceeding their goals for network product or service quality. However, if we drill down into this group to look at those averaging 50% or higher automation deployment across all network domains, an astounding 96%—107 respondents out of 112—report exceeding this goal!

> Of those automating 50% or more of their NetOps, 96% exceed their performance goals for network product or service quality.

The Individual Impact of Automation

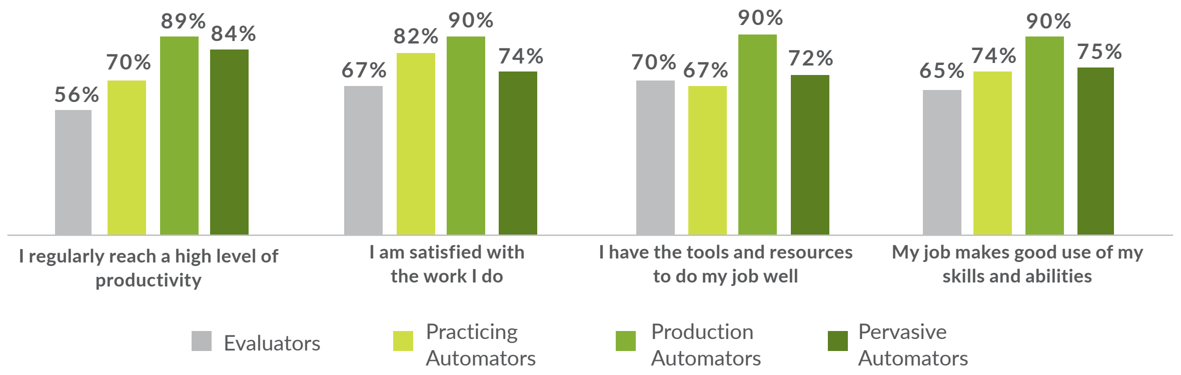
The SoNAR research survey also asked respondents to rate their own individual performance and satisfaction indicators as follows:

- I regularly reach a high level of productivity
- I am satisfied with the work I do
- I have the tools and resources to do my job well
- My job makes good use of my skills and abilities

These statements were presented with a Likert scale for respondents to strongly disagree, somewhat disagree, remain neutral, somewhat agree, or strongly agree. To all statements, 77-81% of respondents somewhat or strongly agreed. Looking at the grouping by self-assessed maturity, once again we see the Production Automators out-performing the Pervasive Automators.

Personal Workflow and Satisfaction by Automation Maturity

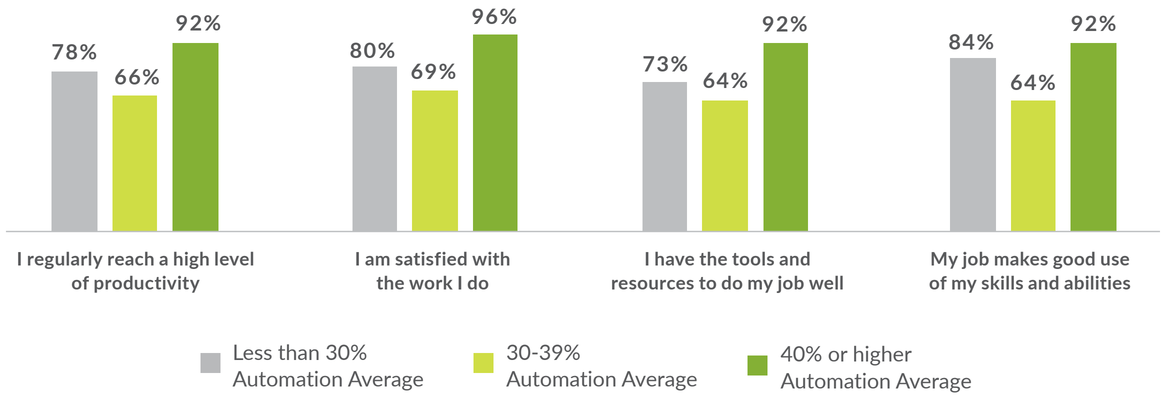
Somewhat/strongly agree



Unlike team performance indicators, looking at respondent grouping by their automation history is less helpful here as the ratings are all fairly close. In general, we observe the Production Automator group above any other, but the remaining results are fairly lumpy.

Personal Workflow and Satisfaction by Automation Deployment

Somewhat/strongly agree

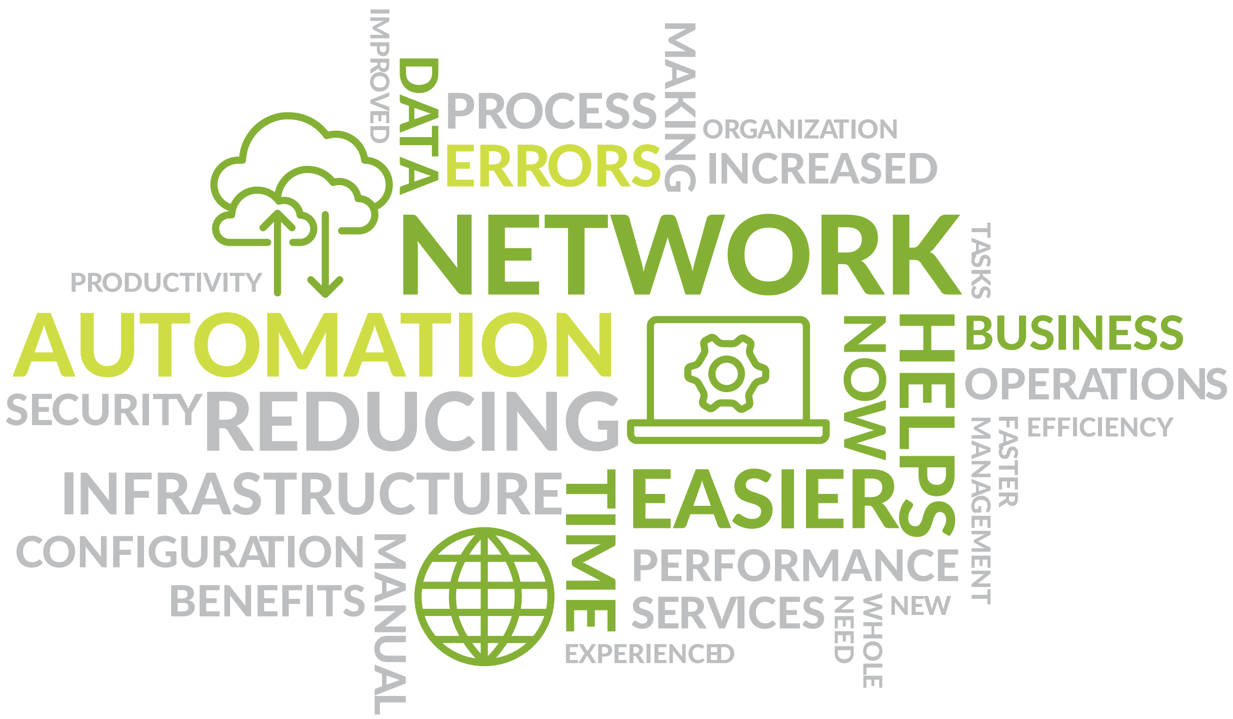


If we regroup by automation deployment as we did for team performance, once again we get a consistent result pattern. This time, however, the group of respondents that fell in the 30-39% range, oddly enough, seem to fare worse than those automating even less. This result may be difficult to explain intellectually, but easy to understand emotionally if this is due to growing pains experienced during the journey to improve one's automation. At the very least, by all accounts of this view of the data, we can say that the journey appears to be well worth the pain experienced along the way.

Summary

We asked SoNAR respondents for one written-in answer. Rather than provide all the answers or pick favorites, we will provide the top themes that emerged from the responses.

What benefits have you or your organization experienced from network automation?



Security Automation

The numbers tell the tale of just how important security is to businesses adopting automation. A full 67% of respondents identified security as a key driver of automation, resulting in a significant gap between security and the next closest driver—improving mean time between failure—which was mentioned by only 55% of respondents.

Technology Factors Driving Automation

	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Security	67%	58%	56%	**78%**	71%
Improving mean time between failure	55%	50%	49%	**62%**	56%
Reducing hard and repetitive work	54%	47%	48%	**63%**	53%
Improving incident response and time to resolution	53%	58%	42%	**65%**	46%
Keeping current on network technologies	51%	44%	50%	52%	**54%**
Sustaining innovation	51%	42%	47%	**56%**	54%
Service uptime levels	50%	42%	46%	53%	**59%**
Compliance	49%	44%	36%	**62%**	50%
Improving time to change	47%	33%	51%	**52%**	44%
Service experience levels	46%	39%	42%	**53%**	46%
Scaling efficiency of network footprint relative to staff headcount	42%	30%	37%	45%	**53%**

All tracked key drivers other than security ranged from 41% to 55%, with the majority between 50% and 55%. The percentage of respondents reporting security and incident response as key drivers for automation remain consistent, regardless of the size of their organization.

Security is clearly the stand-out reason for automation adoption, and it only becomes more important as organizations become increasingly comfortable with automation. A deeper dive into the numbers reveals important, even if largely expected, insights.

Between 56% and 58% of Evaluators and Practicing Automators view security as a key driver for their automation efforts. Between 71% and 78% of Production Automators and Pervasive Automators feel the same. The gap between the two is important.

Improving incident response and time to resolution varies from 42% to 65% as a key driver for automation between groups of respondents. This indicates that, for those considering or implementing automation, how to cope with the inevitability of compromise events is an important area of focus.

Even more interesting is that the range of responses regarding the importance of incident response, while lower than interest in general security benefits, is on par with “reducing hard and repetitive work” as a driver for automation. Incident response between 42%-65% is very close to reduction of repetitive work, which is at 47%-63%.

Security is a Consequence of Automation

Organizations looking to secure their networks rely on some combination of two basic approaches to security: white/black listing and baselining. These are admittedly broad generalizations, but the overwhelming majority of information security approaches fit within one of these two boxes.

Where workloads are well documented and understood, security is usually as "simple" as preventing anything unknown or unexpected from reaching the workload. If you know every valid command that will ever be exchanged with a given workload or device, then you can block all but those commands and raise a flag if anything tries to issue an invalid request. Similarly, you can block all communication to a given workload or device for all except pre-vetted systems. This is whitelisting. Blacklisting is the opposite; it blocks "known bad."

Baselining, the other broad category of security approaches, involves characterizing a workload in some fashion and then responding to deviations in predicted behaviour. This can be done by examining a workload or device's behaviour, or by examining data flows in flight. Detonating malware in sandboxed environments to see what happens would also fall into this category.

Regardless of one's approach, information security relies on understanding what "should" happen, and then comparing that to what is actually happening. For this reason, security is a consequence of properly implemented automation.

Automation enables reliability. Reliability leads to predictability, and predictability is an important part of modern information security. It should come as no surprise that the more comfortable organizations become with automation, the more important security becomes as a motivator for further automation.

Beyond the Perimeter

The network perimeter is evolving. IPv6 has made every device and workload publicly addressable. Hybrid cloud, multicloud, and edge computing are requiring that organizations learn how to implement security across a diverse number of infrastructures.

At the same time, the rise of lateral movement during compromise events and the increasing use of encryption in flight are reinforcing the need for deep network visibility into data flows, as well as multiple points of enforcement throughout the network. Any workload, device, or endpoint can be compromised. Any point of compromise is a platform from which to launch attacks against the rest of the network. East-west monitoring and security enforcement is now just as important as north-south efforts.

Organizations must be able to inspect data flows—and act upon what is discovered—as close to the workload, device, or endpoint as possible. Network Functions Virtualization (NFV) plays an important role in providing this ability, as does interconnectivity between multiple security and networking products throughout the network.

But this requirement to move security visibility and enforcement deeper into the network comes with a cost: it dramatically increases the scale and scope of information security efforts when compared to traditional (and ineffective) perimeter-only security. Increased scale without automation quickly leads to unmanageable complexity, making automation absolutely vital to securing today's organizations.

Effective information security is both enabled by, and is a consequence of, the predictability and simplicity made possible by IT automation. This reality is reflected in the survey results, as it has been in multiple industry surveys over the past decade.

Network Operations Culture

Organizational Goals

The SoNAR research survey asked respondents to rate statements about their behaviors and culture. These statements were presented with a Likert scale to strongly disagree, somewhat disagree, remain neutral, somewhat agree, or strongly agree. More than 70% of respondents somewhat or strongly agreed to all statements.

Cultural Statement Ratings by Automation Maturity

Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
We have a culture of continuous improvement where opportunities for improvement are valued and acted upon 40% 37% (77%)	67%	75%	**85%**	74%
We have good visibility into errors, outages and issues 39% 42% (81%)	64%	83%	**88%**	78%
We have service-levels that are measured and reported with transparency to our stakeholders 31% 41% (72%)	58%	72%	**77%**	72%
We have service-level objectives 23% 48% (71%)	62%	**75%**	**75%**	65%

🟩 Strongly agree 🟦 Somewhat agree

Many respondents indicated that a culture of continuous improvement was key, especially those in the sweet spot of the Production Automator group. This suggests that these respondents are being careful to establish a beachhead for automation and learn how to do it well before moving on.

Less likely for most respondents, though more likely for experienced automators, was the practice of maintaining and communicating service-level objectives to stakeholders. This underscores a problem that has existed in infrastructure disciplines for a long time, which is that it's very difficult to translate technical metrics like throughput, latency, and infrastructure element uptime to service-oriented metrics that business stakeholders can consume.

Cultural Statements Ratings by Goal* Attainment

Somewhat/strongly agree

	Above goals	Met goals	Below goals
We have a culture of continuous improvement…	**85%**	73%	66%
We have good visibility into errors…	**92%**	78%	63%
We have service-levels that are measured…	**79%**	65%	64%
We have service-level objectives	**78%**	63%	68%

*Goals are listed in the aforementioned result for "Organization Performance in the Past Year"

When looking at the cultural statement ratings through the lens of organization performance in the past year, which was reported in the section on Automation Motivations and Benefits, we see a strong correlation between these positive cultural traits and high performers.

We believe that organizations seeking to enjoy the benefits of automation should not spend five years developing an automation roll-out plan, but should rather start small and instill a culture of continuous improvement in which engineers are free to experiment and learn by trial and error.

Automation Challenges

Respondents were asked for the top challenges facing organizations when it comes to adopting automation, from a set of ten potential options. The results were pretty telling, as the front-runner was selected 10% more than the runner-up.'

The top challenge for adopting automation—especially for those Evaluators that are barely getting started—is the overwhelming number of technology choices. As the pace of technology innovation increases and the number of responsibilities placed on enterprise IT continues to rise, creating a comprehensive automation solution from the plethora of approaches will become more difficult, requiring more cross-functional skill-sets.

We believe these findings show the rising need to balance "build" vs. "buy" because it's unlikely that a single product will automate everything across the board. At the same time, building everything in-house would be far beyond the capabilities of most IT teams, to say nothing of opportunity costs. Rather, those that find success with automation often do so by relying on specialists and vendors to do the heavy lifting of automating within a single technology domain—for example, the virtualization stack or wireless infrastructure. This allows the user organizations—often by focusing on a few key workflows at a time—to spend time creating operations contextual automation and tooling and architecture contextual automation between domains that ties everything together.

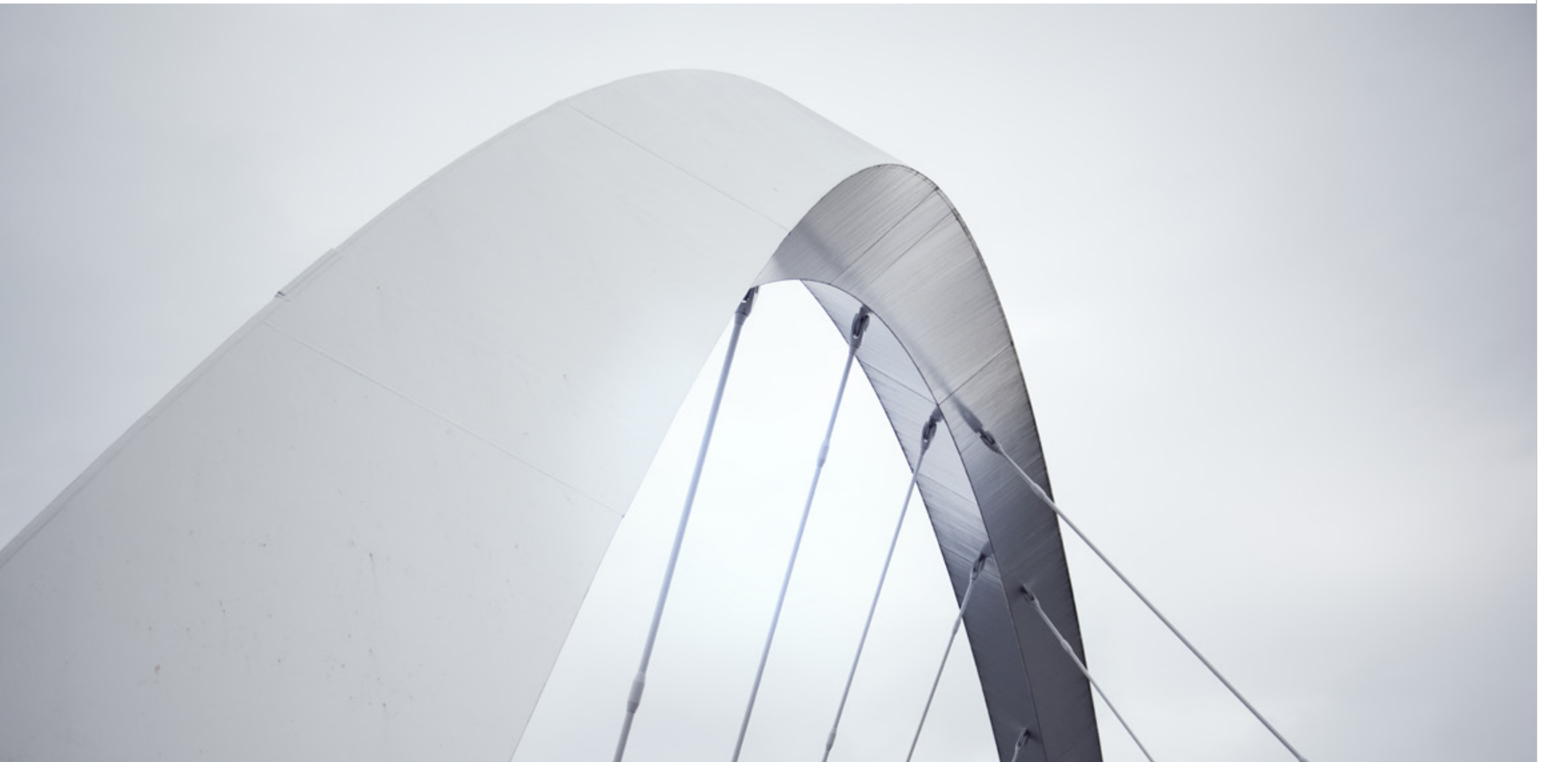
Challenges Faced by Organizations Developing an Automation Practice

	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Overwhelming number of technology choices	52%	**59%**	47%	53%	50%
Older networking equipment that is hard to automate	42%	**58%**	48%	28%	46%
Lack of budget or financial barriers	39%	**55%**	52%	20%	41%
Not enough motivating factors to warrant deployment of automation	37%	**55%**	43%	20%	44%
Organizational culture doesn't value automation	36%	**50%**	44%	19%	46%
Lack of a lab or safe place to test or practice	36%	**52%**	39%	24%	41%
Lack of knowledge necessary to access training	21%	**29%**	27%	12%	24%
Lack of training resources	21%	**38%**	21%	13%	19%
Fear of making a mistake in production	21%	**26%**	23%	19%	15%
Lack of time to learn on the job	16%	17%	**19%**	14%	15%
None of the above	10%	0%	3%	**18%**	13%

The other nine factors, while secondary to the overwhelming number of technology choices, are still quite significant. Among them are factors like legacy infrastructure that doesn't have modern programmability options; lack of budget; lack of perceived value in automation; and an inability to safely test automation without breaking production.

While these seem to be fairly distinct hurdles, they're all tied together by the core reality that automation is an operational model—one that can and should be woven into every aspect of daily operations, starting as early as procurement. Automation can start small, and progress should be expected to be incremental, but shouldn't be artificially limited to a technical discipline. The emphasis should be on weaving continuous improvement and experimentation into the culture of the organization.

Respondents were also asked about their top personal challenges in adopting automation. While there were certainly similarities to the responses from an organizational level, a consistent theme emerged: individuals do not feel like they have the opportunity to develop automation skills.



Challenges Faced by Individuals Developing an Automation Practice

	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Lack of time to learn on the job	48%	**59%**	48%	40%	54%
Overwhelming number of technology choices	46%	**48%**	47%	47%	41%
Lack of knowledge necessary to access training	41%	**52%**	46%	28%	47%
Fear of making a mistake in production	40%	**50%**	**50%**	25%	46%
Lack of training resources	37%	**56%**	41%	26%	35%
Lack of budget or financial barriers	20%	24%	**25%**	15%	16%
Lack of a lab or safe place to test or practice	13%	**20%**	14%	7%	19%
Not enough motivating factors to warrant deployment of automation	13%	**26%**	16%	8%	7%
Older networking equipment that is hard to automate	10%	**14%**	12%	8%	9%
Organizational culture doesn't value automation	5%	**9%**	8%	1%	3%
None of the above	9%	0%	3%	**17%**	13%

Perception of Automation

The IT industry prolifically generates buzzwords to describe changes in operational practices or technology innovations. Respondents were asked for insight into the kinds of terms that inspired self-improvement. The results were very telling, in two distinct ways:

Trends Inspring Automation Self-Improvement

	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
DevOps	38%	23%	39%	**45%**	38%
NetOps 2.0	22%	**27%**	25%	19%	16%
DevNetOps	22%	23%	16%	21%	**31%**
Network Reliability Engineering	13%	**20%**	15%	11%	9%
Network software developers	5%	8%	5%	3%	**6%**

The leader, by a large margin, was “DevOps.” The appeal of DevOps is strong across the board, but in particular, it resonates with those who have introduced automation in production. This seems to indicate that while this term has general currency, it rings true with those who have managed to get automation into production, because they’re actually living it.

Another interesting point from the results was the term “Network Reliability Engineering,” whose appeal was strongest with those who have barely begun automation. This is likely because it provides a familiar on-ramp that simultaneously moves an individual into thinking about automated network operations as a byproduct of a focus on reliability, while also respecting existing network engineering skill sets. Rather than forcing network engineers to consider themselves developers, or telling them that they need to learn programming, it’s more motivating to start small and redirect existing skill sets into the new way of doing things.

Network Operations Practices

For the purposes of this section, we define network operations (NetOps) practices as the methodologies, philosophies, and tools that govern the design, deployment, and operation of networks.

NetOps Network and Technology Areas

We asked SoNAR respondents which technology areas they spend significant time with during a typical week.

Significant Technologies Touched in a Typical NetOps Week

Networking vs. Security	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Campus / Branch Networking	74%	68%	71%	**79%**	71%
Data Center Networking	68%	**76%**	65%	70%	65%
Managed Services	63%	**70%**	61%	64%	56%
Wide-Area Networking (WAN and SD-WAN)	59%	45%	55%	**70%**	53%
Network Management Systems	57%	41%	52%	**68%**	59%
Software Defined Networking (SDN)	52%	38%	43%	**67%**	50%
Edge Compute Networking	52%	32%	43%	**65%**	56%
Network Functions Virtualization (NFV)	51%	41%	43%	**60%**	54%
Carrier Network Infrastructure	48%	**56%**	52%	40%	51%
Wireless Systems	41%	32%	40%	**50%**	34%
Public Cloud Networking	41%	24%	39%	**51%**	38%
Security Operations	41%	**52%**	49%	30%	40%
Cloud Security	40%	**52%**	48%	30%	37%
Information Security Products / Solutions	39%	**48%**	45%	30%	35%
Cybersecurity Products / Solutions	38%	**47%**	43%	24%	**47%**
Mobile Infrastructure	19%	15%	**24%**	15%	22%

Similar to the top two areas that are most automated on average, covered in the Automation Maturity and Adoption section, campus/branch and data center networking are where most respondents are spending their weekly time.

While it may be interesting for readers to compare this overall result to their own reality, we did not expect to see such high numbers for relatively new technology areas like edge-compute networking and modern tools like NFV and SDN. Almost as many respondents are using SDNs as network management systems: 52% vs. 57%. We suspect most of these SDN systems are commercial products, not homegrown. Furthermore, 52% may be slightly exaggerated, depending on how one defines SDN because in the subsequent section on tooling adoption only 35% of respondents reported automating using SDNs and intent-driven networking products that include a centralized controller (a stricter definition).

Management systems and software-defined networks (SDNs) reduce NetOps complexity. Indeed, SDNs attempt to abstract and automate complexity to simplify operations and deliver reliability. SDNs typically accept intent-based configurations that are both more abstract—working across a group or whole domain of devices at a time—and declarative—dealing in the desired end state of the network and not imperative steps of how to render that state in the network. SDNs generally offer automated change workflows, as described above, that guide processes to provide the desired intent. In doing so, they typically provide higher-order GUIs or CLIs working across a network domain.

Such SDN automation is most often engineered and delivered by vendors rather than created by network operators. Vendor-supplied SDNs focus on automating the common dynamics, integrations, and workflows within a network domain deployed by many users; they are generally deployed as blackbox tools from an operations standpoint.

It often makes sense for operators to buy rather than build because few, if any, can achieve the same level of engineering productivity and focus of vendors, especially as SDN systems mature. But by buying productized SDN solutions, operators risk changing the operations management plane without changing the management paradigm. In other words, though many SDNs provide APIs, it's still entirely possible—and easy—for operators to manually change, observe, and troubleshoot SDNs. On top of an SDN's elevated management plane, there are still operator-contextual processes and service-level indicators that need to be automated and engineered.

NetOps Changes, Failures, and Fixes

In the age of DevOps, it is assumed that the frequency of manual network changes will shrink as trust in automated changes increases. Given that only 8% of respondents make daily changes to their networks, we assume most of these changes are manual. With the bulk of respondents reporting they make changes once per week, it's likely that these changes are taking place with traditional weekend maintenance windows, which is a known DevOps antipattern.

Operational Changes by Frequency

		Evaluator	Practicing Automator	Production Automator	Pervasive Automator
More than once per day	2%	2%	5%	0%	3%
Once per day	6%	2%	7%	6%	9%
Multiple times per week	19%	14%	16%	27%	10%
Once per week	34%	23%	**34%**	**40%**	**32%**
Once per month	24%	**44%**	22%	15%	24%
Once every 3 months or longer	16%	17%	16%	12%	22%

It isn't clear whether change control authorities within an organization slow down the rate of change, or if the types of changes themselves are the reason they are less frequent. However, among automator groups, changes are noticeably more frequent.

A habit among automators is to use infrastructure as code processes and continuous testing and pipelining tools and processes. While such behaviors and tooling are still nascent in networking operations, they do help to make smaller, less risky changes that are easy to remediate if they cause problems. We may speculate that automators are at least starting to embrace this, given they are clearly outpacing the Evaluators group in change frequency.

Operational Changes by Implementation Time

		Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Less than 1 hour	7%	11%	2%	5%	15%
Less than 1 day	33%	11%	20%	**51%**	**35%**
Between 1 day – 1 week	29%	**33%**	**39%**	25%	16%
Between 1 week – 1 month	14%	18%	15%	12%	12%
Between 1-3 months	12%	20%	16%	3%	13%
More than 3 months	6%	8%	7%	3%	9%

When looking at the results for how long changes take to execute, the automator groups are, once again, outperforming the Evaluators. Among the Evaluators and Practicing Automator groups, only 22% of changes could be implemented in a day or less, compared to the two more mature automator groups that were completing more than 50% of changes in under a day.

It's also interesting to note that the Evaluators are still implementing a good portion changes quickly: 11% are implemented in under an hour. It's important to understand that faster changes can be a sign of both maturity and immaturity because immature automators can still move quickly by making changes without proper safety measures and testing in place. In fact, a common pain point for operators beginning to automate is how much longer it takes to build the automation and run the automated processes compared to simply manually executing a change in production. Of course, these old habits of short-term gain are hard but useful to break for the long-term payoffs of reliability and the speed that will enable managing multiple changes quickly and more frequently.

Percentage of Operational Changes Resulting in Degraded Service

		Evaluator	Practicing Automator	Production Automator	Pervasive Automator
None	8%	0%	2%	13%	15%
1-10%	37%	27%	29%	**49%**	**35%**
11-20%	27%	**29%**	**36%**	24%	15%
21-30%	13%	23%	12%	8%	12%
31-40%	6%	5%	8%	2%	9%
Over 40%	11%	17%	13%	5%	15%

Of the 8% of respondents who reported fully successful changes—those that never resulted in degraded service—there is a strong correlation to automation maturity shown in the results. In addition to the table by maturity group, respondents automating for more than three years outnumbered those with less automation history 3:1 in reporting fully successful changes.

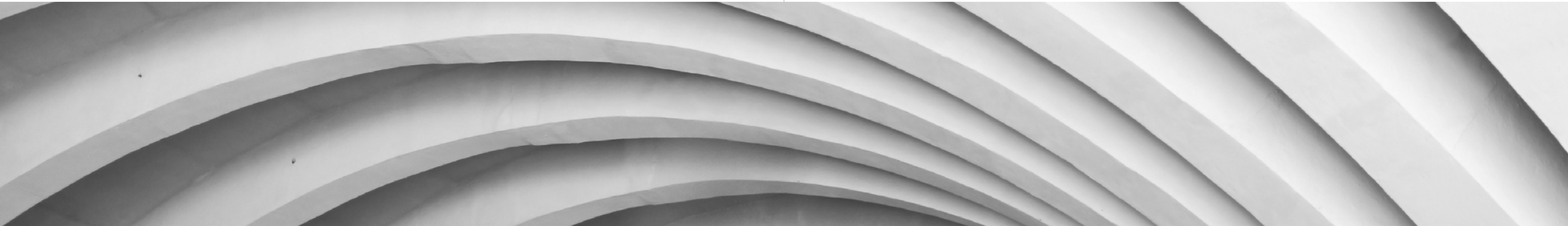
Also, respondents deploying automation 40% or more on average across their network domains outnumbered those with lesser deployed automation 7:1 in reporting fully successful changes. (Recall that we saw the results to which respondents were automated by network domain earlier in the report in the Automation Maturity section; when averaging out the scores across all network domains, approximately one-third of respondents averaged more than 40%).

More than half the respondents felt that approximately 10% of the changes they made resulted in an outage or degraded service. The results below show that almost half of respondents experience degraded service once per week.

The SoNAR survey did not directly ask respondents what caused outages or degraded service beyond network changes. Nonetheless, it's fascinating that the chart for the frequency of changes loosely tracks the chart below showing the frequency of service degradation reports. User-affecting service degradation can occur for many reasons; the interpretation here is that changes applied to the network often cause outages as shown in the chart for changes resulting in degraded service. This is no surprise, since a commonly held stigma in the industry is that many failures are caused by human error. As organizations adopt network reliability engineering practices, we expect to see this relationship break and the frequency of service degradation reports to track external events like fiber outages, hardware failures, and pre-existing bugs in software tools. As reliability engineering matures, even these failures can be mitigated.

Frequency of Operational Outages or Service Degradation

		Evaluator	Practicing Automator	Production Automator	Pervasive Automator
More than once per day	4%	5%	4%	3%	3%
Once per day	8%	12%	11%	3%	6%
Multiple times per week	23%	**38%**	33%	11%	15%
Once per week	46%	33%	**42%**	**55%**	**49%**
Once per month	16%	5%	8%	26%	18%
Once every 3 months or longer	4%	8%	2%	2%	10%



Operational Changes by Implementation Time

		Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Less than 1 hour	6%	3%	3%	6%	16%
Less than 1 day	30%	12%	14%	**52%**	**31%**
Between 1 day – 1 week	20%	20%	27%	19%	9%
Between 1 week – 1 month	22%	**36%**	**28%**	8%	25%
Between 1-3 months	15%	15%	20%	12%	12%
More than 3 months	8%	14%	8%	4%	7%

The results for so-called NetOps "firefighting" are rather distressing for novice or non-automators in the Evaluators groups. They generally experience service degrations multiple times per week, and such plights take far longer for them to remedy than they do for the Automator groups. Notably, about half of the Production and Pervasive Automators report that it takes less than a day to restore service. The contrast of immature vs. mature automators paints a familiar picture of IT reality of how people spend their time: those who automate find themselves in a virtuous cycle that gives them more time to automate and spend on strategic or transformative endeavors, while those who fail to automate are pulled further into the vicious cycle of firefighting to simply keep the lights on.

> Those who automate find themselves in a virtuous cycle that give them more time to automate and spend on strategic or transformative endeavors, while those who fail to automate are pulled further into the vicious cycle of firefighting to simply keep the lights on.

Strategies to Improve Automated NetOps

Using a Likert scale as described above, we asked SoNAR respondents to rate their agreement with strategies they see implemented in their organization to create more automated network operational processes and technology.

Organizational Strategies to Further Automation

	Strongly Agree	Somewhat Agree	Neutral	Disagree / Strongly Disagree	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Hiring new talent	18%	46%	29%	7%	64%	65%	60%	**67%**	60%
Investing in training existing staff	30%	33%	30%	8%	63%	52%	52%	**74%**	66%
We have a part of the team dedicated to automation	25%	36%	30%	9%	61%	47%	52%	**72%**	66%
We rely on professional services	32%	28%	31%	9%	60%	**64%**	**64%**	60%	50%
We rely on custom and contextual automation	29%	25%	37%	10%	54%	44%	40%	**66%**	60%
We rely on vendor products that require no customization	13%	40%	32%	14%	53%	45%	53%	54%	**59%**

🟩 Strongly Agree 🟩 Somewhat Agree 🟦 Neutral ⬛ Disagree / Strongly Disagree

The results show that large combinations of these methods are used to expand automation. A few of the top and bottom numbers do stand out and confirm some of our assumptions.

Naturally, the immature automator groups were the least likely to have a dedicated team focused on automation and were less likely to build customer NetOps contextual automation, which requires inhouse engineering expertise. Somewhat surprisingly, they were also less likely to invest in upleveling the existing talent pool, opting instead to pull in outside resources such as professional services or hire new people. While this strategy is a useful bootstrap, it shouldn't preclude training existing staff.

Looking at the more mature automator groups, they're much more often dedicating parts of the team to focus on automation, and their organizations more frequently invest in existing staff. These two strategies are practiced by more than 70% of respondents with teams of over 20 people, who are above their organization performance goals, who have been automating more than three years, and who have deployed automation in 40% or more of their network domains.

The reports show that 77% of respondents who have deployed automation in 40% or more of their network domains on average also indicated they were relying on custom and contextual automation in their network operations. Generally speaking, custom and contextual automation adoption is far more prevalent in the mature automator groups compared to the immature groups, but it's interesting to note that these mature groups are also adopting turnkey vendor products to automate. Perhaps this is the wisdom of not reinventing the wheel for things like SDN systems when vendors can best solve the problems common between all NetOps practices.

Network Operations Day-to-Day Responsibilities

No automation process discussion would be complete without looking at the responsibilities and brain context switching for the human bystanders involved in the automation revolution. By automating processes, we expect to see harder tasks bubbling to the surface, with well-understood and toil-based tasks being automated out of the slow, human-based path.

We asked respondents which of the following responsibilities are part of their day-to-day jobs.

Network Operations Day-to-Day Responsibilities

	Total	Evaluator	Practicing Automator	Production Automator	Pervasive Automator
Network monitoring	71%	64%	63%	**83%**	66%
People management	62%	59%	57%	**67%**	63%
Documentation	59%	**65%**	61%	60%	49%
Network automation software engineering	53%	44%	46%	**63%**	56%
Requirements analysis	51%	**55%**	47%	**55%**	44%
Project or product management	50%	50%	40%	**62%**	41%
On-call / incident response	48%	44%	42%	49%	**57%**
Testing	46%	44%	**54%**	45%	37%
Network automation architecture, frameworks, and tools integration	46%	36%	39%	**55%**	47%
Network architecture	38%	38%	34%	38%	**44%**
Information or network security	35%	**53%**	39%	24%	35%
Network provisioning	32%	30%	34%	27%	**38%**

Network monitoring, even without the spike from the Production Automators, rose to the top of the list. We expect that monitoring is one of the activities that changes just a little with added automation. After all, SRE and NRE practices advocate for a culture of measurement, both with toil and error budgets, but also manage and measure the metrics that matter to stakeholders using service-level indicators (SLIs). So in all likelihood, more immature automators are monitoring low-level signals and traditional dashboards such as alerts, alarms, and network metrics measured by such things as SNMP, whereas SREs and NREs are monitoring things like SLIs and periodic stakeholder reports. With the rise of AI applied to IT, hopefully we'll see a reduction in alert false-positives and monitoring fatigue.

It's fascinating to see 83% of Production Automators spend time on network monitoring, with a significant drop for the Pervasive Automator group to closely track the Evaluators and Practicing Automators. This could be interpreted as, once network monitoring has been understood and the data required for automation can be extracted, the focus shifts from intense monitoring to maintenance. Furthermore, the time spent documenting decreases significantly for the Pervasive Automator group compared to other groups. We cannot tell for sure why this is, but it could be perceived that documentation is automatically generated, or a part of automated workflows (e.g. documentation) is mixed with Python in Jupyter notebooks.

It's natural that Production Automators spend a lot of time on network automation software engineering while experience builds, followed by a slight drop in time engineering for Pervasive Automators as their toolchains change less frequently. The same is true for requirements analysis; time must be invested into what deployed services require so they may be automated.

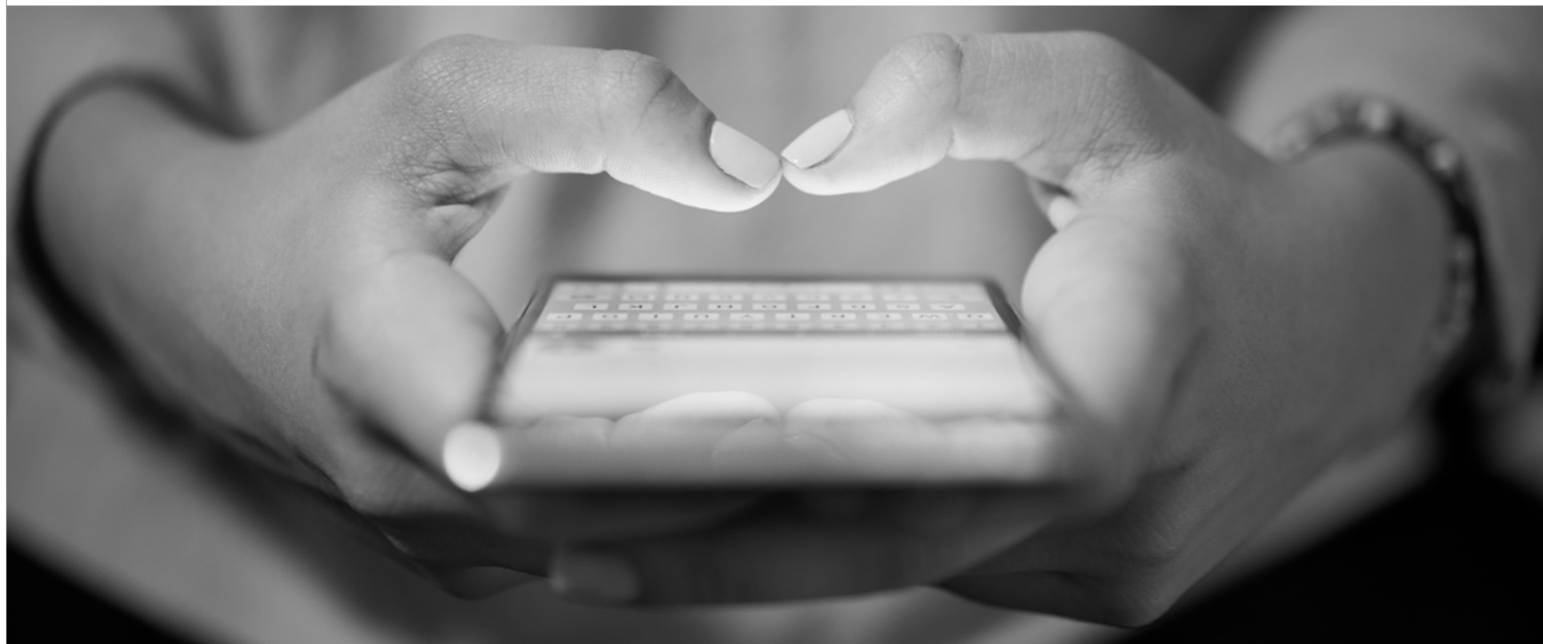
Security, the top technology factor motivating automation seen in earlier sections, is actually seen as one of the least frequent job areas. This could be because SoNAR naturally targeted network engineers, and security operators are often still siloed within their own discipline. Nonetheless, security as discussed in the Security Automation section is increasingly integral to networking and other IT work.

As a daily responsibility, security drops linearly and dramatically from Evaluators to Production Automators. As network configurations are standardized and tested, security requirements can be embedded and the security posture can be tested automatically. Furthermore, a large part of a strong security posture relies on automating protection and enforcement as new threats emerge and as compromised hosts attempt to spread attacks. We might conclude that more mature automator groups are ahead and better at this than the Evaluators, hence they spend less time on it. While there is an uptick for Pervasive Automators in the amount of time they spend on security, we cannot tell what this means without more research. One possibility is a deeper and broader outlook on what it means to be secure.

Finally, network provisioning, including deployments and configuration, fell to the bottom of this list of daily work tasks. This is interesting because a common network automation pretense is that provisioning ought to be automated first. Indeed, many configuration management tools (examples such as Ansible and Chef are covered in the next section) have risen to popularity and lent credence to a configuration-first approach to learning and deploying automation. However, there are many indications that diving into automation with only configuration management in mind is rash and ill-advised because:

- Read-only workflows are safer for novice automators to learn.
- Emerging automators often don't have testing or staging labs, and automating configuration changes at scale in production can be disastrous if an error is made.
- DevOps professionals have put down configuration management tools for direct production deployment and provisioning in favor of continuous integration, delivery, and deployment, using configuration as code and immutable infrastructure.
- As shown in this SoNAR finding, provisioning is not where most network operators are spending their time, so the return on investment comes mostly in terms of a reduction of errors, not toil.

Of course, configuration management tooling can still be part of a continuous pipeline toolchain, and learning about them is generally better than venturing into network automation. However, this SoNAR finding about daily NetOps work confirms the belief that those pursuing automation should look beyond configuration management and probably set that aside initially to focus on troubleshooting and monitoring workflows. In spite of this, in the next section on tooling, we will see that configuration management tools take the lead in terms of adoption.



Tooling Adoption

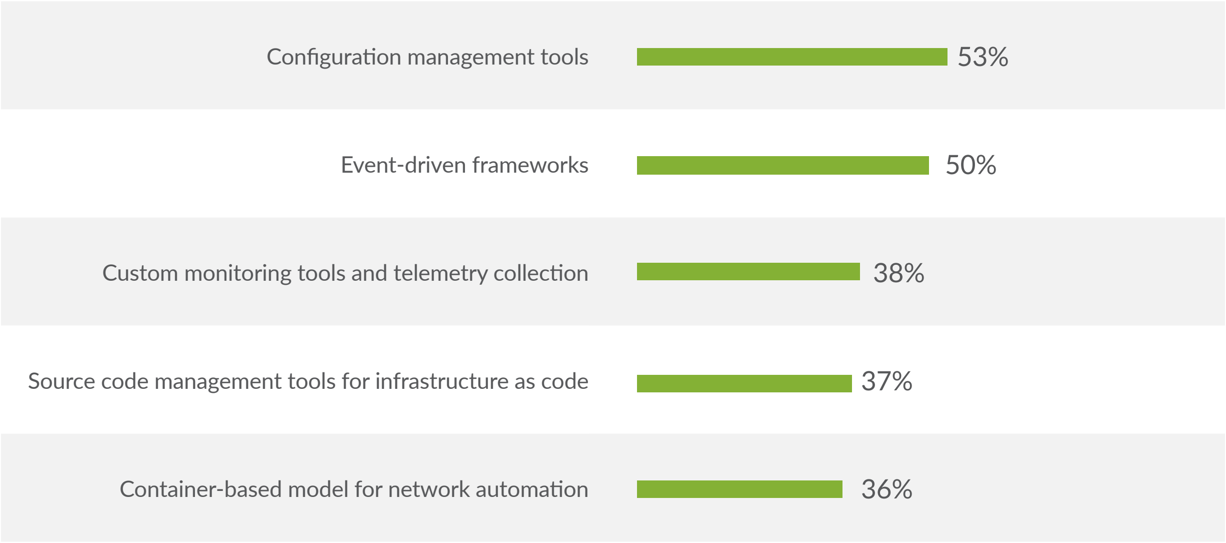
The SoNAR survey asked respondents about many possible types of tools used in their organizations. Because there are so many technology functions, in the survey and results, we grouped automation tooling into two categories:

- Tooling used to automate network deployments, changes, and management
- Tooling used to automate network testing for making changes

Some tools can span both categories, and configuration management tools and event-driven frameworks-- indeed the top two tools adopted overall and at the top of each category-- are perfect examples of this. Configuration management tools such as Ansible and Chef can be used for deployments and equally used in testing frameworks, as can event-driven frameworks like Salt or Stackstorm. Additionally, some tools may fall into several technology categories; for example, Salt can be used for configuration management as well as for event-driven framework.

Looking at the technology function tooling—regardless of the category and individual tools—may be the most fair approach because testing and deploying changes in pre-production and then monitoring and managing dynamic state in production is a continuum. The top five tools adopted overall by the SoNAR respondents are probably familiar to anyone following DevOps technology trends because many network and security automation tools started their life in software development and sysadmin operations.

Top 5 Tooling Functions Adopted for Network Automation



Tools for Deployment, Changes, and Management

Automation Tooling Adopted for Deployment, Changes and Management

	Total	Evaluators	Practicing Automators	Production Automators	Pervasive Automators
Configuration management tools	53%	29%	50%	**69%**	50%
Custom monitoring tools and telemetry collection	38%	29%	39%	40%	**43%**
Container-based deployment model for our network automation	36%	33%	**43%**	33%	32%
Software-defined / intent-driven networking products that include a centralized controller	35%	30%	**39%**	34%	32%
Cloud-based network management	33%	24%	32%	31%	**46%**
APIs at the virtual or physical device level	31%	29%	31%	27%	**43%**
Infrastructure as code templating and modeling tools	26%	27%	26%	24%	**31%**
Databases and repositories for inventory and artifacts	26%	**35%**	25%	22%	29%
APIs at the controller or management plane level	24%	20%	**30%**	22%	22%
On-device automation with on-box scripting	19%	**23%**	20%	15%	22%

One standout result is the very high rate of adoption of configuration management tools by Production Automators: 69%. They lead by a significant margin in this category; overall, this category had a very high response rate, with half of Practicing and Pervasive Automators responding they use such tools.

As described in the previous section, this is not surprising. Configuration management tools are some of the most mature off-the-shelf automation tools available, with many having existed for a decade or more with both open source and commercial offerings. Production Automators, or those automating in only some places of their network, did not lead any other categories here. They had the least diverse adoption of these types of tools among the three automator groups. The second highest category for this group was the use of customized telemetry. Recall that this group is the highest performing in many categories, topping even the Pervasive Automators much of the time. It could be that their higher reported performance is the result of focusing on fewer tools and fewer places in their network, with greater emphasis on workflow integration.

Pervasive Automators report higher rates of adoption across most categories, and indeed the highest aggregate adoption of tooling as well. This is likely a natural consequence of having adopted more tools over time, as this group has been automating the longest.

What is peculiar about the Pervasive Automators is that while they reported a high percentage of adoption across all categories, as seen in previous sections, they also reported that their biggest individual challenge was a lack of time for learning new technologies, while their biggest organizational challenge was an overwhelming number of tools.

The challenge, both individually and for organizations, of sifting through an overwhelming number of tools was highly reported, but the higher performing Production Automators seem to be doing the best job of managing this challenge because they had lower aggregate tool adoption than both the Practicing and Pervasive Automators. As described above, we can only speculate as to why the Production Automators outperform the others, but recall they are automating only some parts of their networks, not all places. Correlation is not causation, but if one was to model them, the more focused toolkit and approach is noteworthy.

Tools for Automating Network Testing

Automation Tooling Adopted for Testing and Making Changes

	Total	Evaluators	Practicing Automators	Production Automators	Pervasive Automators
Event-driven frameworks	50%	33%	43%	58%	**62%**
Source code management tools in our network or security operations for infrastructure as code	37%	27%	31%	**48%**	35%
Reviewing tools as part of change management	32%	26%	32%	33%	**37%**
Tools for test simulation	32%	35%	34%	26%	**40%**
Pipelining tools for continuous integration and deployment	32%	24%	28%	31%	**49%**
Frameworks or tools for testing	28%	30%	28%	23%	**34%**
Automated hooks and testing on code commits	26%	23%	24%	**29%**	26%

Validation of the versatility of event-driven frameworks

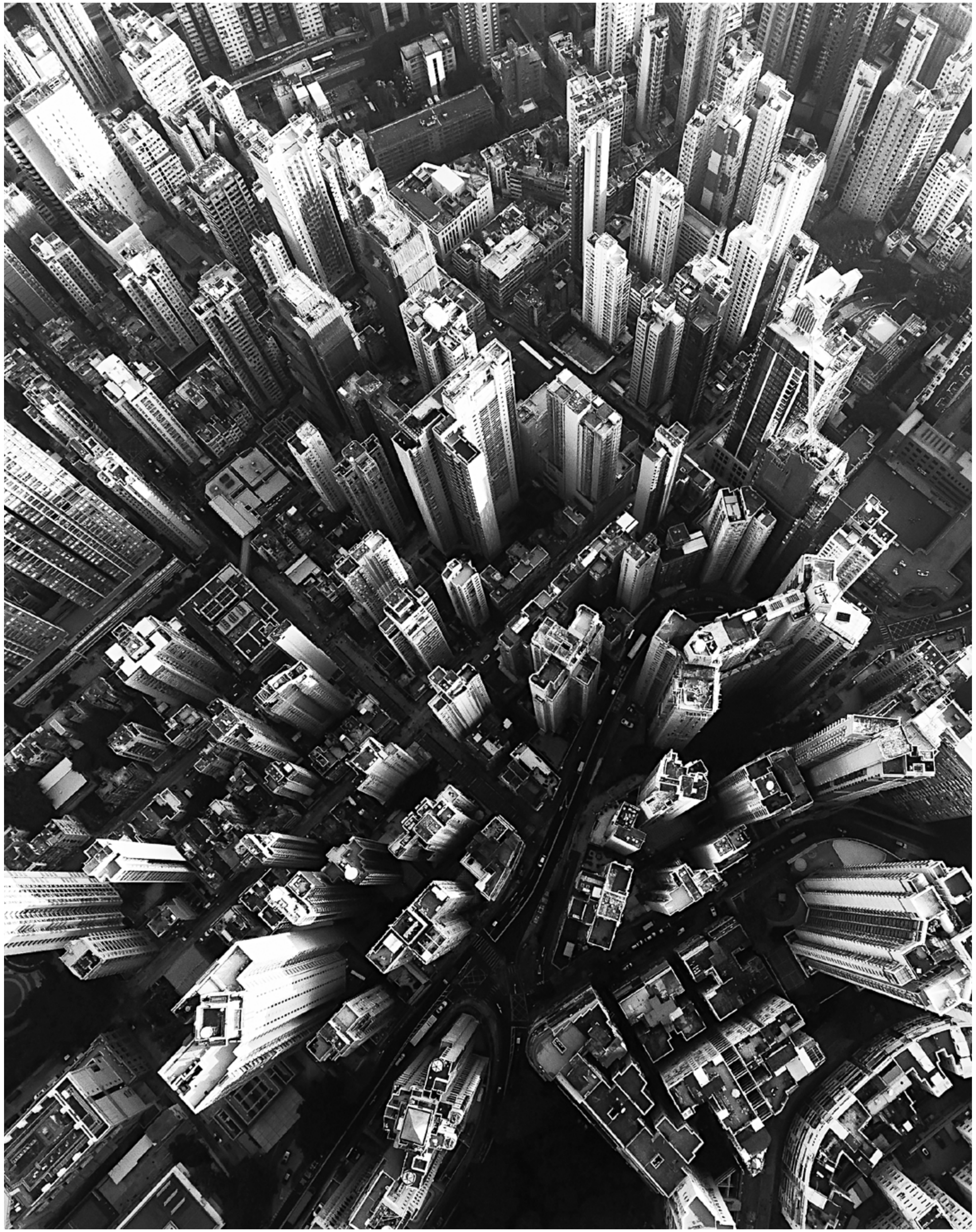
One can construct almost anything with an event handling system, and event loops are at the heart of many software programs. Event-driven network automation has, not surprisingly, clearly established its viability in solving a variety of network automation problems, with both Production and Pervasive Automators leading the pack with a roughly 60% adoption rate.

These are more elaborate "if-this-then-that" tools, such as Stackstorm and Salt or Saltstack. They provide intuitive interfaces for defining event triggers and associated workflows. Much of what network engineers do revolves around collecting information, processing it, and subsequently disseminating it, and these tools fit the bill perfectly.

Source code management (SCM) tools like git and repositories like GitLab and GitHub are also popular. These are often called the "source of truth" because they manage and contain automation software code and, increasingly, network configuration "as code" too. Employing codebases are not only useful for versioning and facilitating engineering collaboration on development and reviewing, but these systems are also the headend of pre-production continuous (CICD) pipelines for building, integrating, and delivering software and infrastructure artifacts and configuration. Testing is integral throughout the process, and some pipelines automate deployment into staging and production as well.

The Production Automator group leads the adoption of SCM tooling, with almost half of those respondents indicating they use it. An inexplicable finding, however, is that half of the Pervasive Automators reported using continuous pipeline tooling, but only 35% of them reported using SCM tools, which are generally a prerequisite for CICD tooling.

The key takeaway from this part of the data is that automated testing becomes important the more you automate in production. Pervasive Automators led in most categories here, and Production Automators were second in the diversity of testing tools adopted.



Methodology

SoNAR research objectives include:

- Providing insight into network automation adoption today, including business and technology drivers.
- Identifying perceived benefits and challenges of automation deployment.
- Understanding the impact of automation on both organizational and individual performance.
- Determining the state of network operations and automation within networking systems and their operation.

The 2019 State of Network Automation Report (SoNAR) is the inaugural annual research sponsored by Juniper Networks EngNet. It is designed to provide value to the industry through objective measurement and unbiased reporting in the hopes of helping networking teams and network engineers successfully automate network operations through improved understanding.

☎ Phone-to-web based survey

Data collection May 7 - May 31, 2019

400 Interviews

The 2019 SoNAR survey was conducted "phone to web" between May 7 and May 31, 2019. All 400 respondents that completed the survey were based in the USA. In future reports, we hope to broaden our geographic reach.

All respondents were IT decision makers in organizations with 250 or more employees. Survey respondents were required to be involved in at least one of the following networking functions: Architecture and Design, Engineering and Operations, Management Systems, or Security.

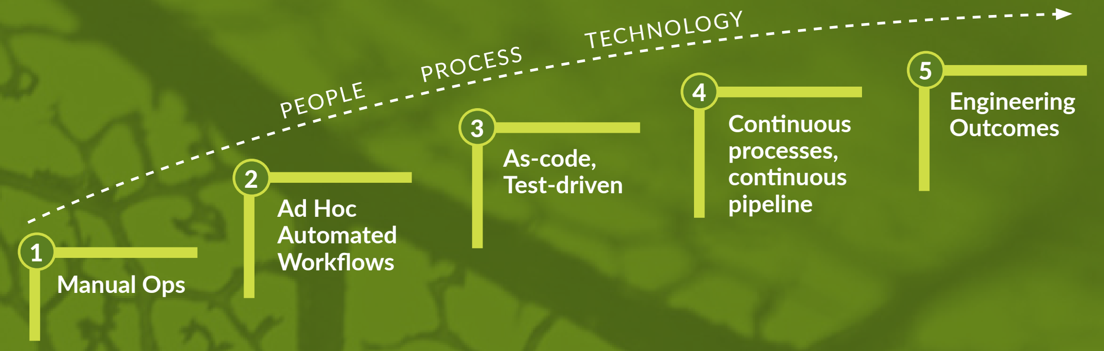
THE AUTOMATION JOURNEY

The challenge lies not only in knowing where to go, but how to get there.

Automation has become imperative to modern network operations. You need it within the products you use to build your network to make it more autonomous. It's also critical to enabling reliability in your network operations processes. But not everyone knows how to get started with automation, how to set long- and short-term goals for achieving it, and how to measure success.

Getting there certainly raises technical challenges that organizations must address. Equally important, however, are changes in processes, skill sets, and culture. All three areas—people, process and technology—must evolve in parallel to accomplish the ultimate automation goal, a more reliable network infrastructure, and such secondary goals as speed, efficiency, and agility.

The approach to automation as a network reliability engineering journey can be summarized in five steps:



Use the many resources on this page to learn how Juniper can help you successfully follow this path to achieving more reliable network operations.

Watch video

JUNIPER NETWORKS | ENGNET

Download and participate in future SoNAR research on Juniper Networks EngNet juniper.net/sonar

Share it on social
#SoNAR

Engineering
Simplicity

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

7400113-001-EN SEP 2019