IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Research Summary: Enterprise Network Automation for 2020 and Beyond

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) RESEARCH SUMMARY REPORT
BY SHAMUS MCGILLICUDDY
SEPTEMBER 2019

SPONSORED BY:

Red Hat

Table of Contents

Executive Summary

This summary of new EMA end-user research examines how enterprises are formalizing their approach to network automation. Based on a survey of 250 subject matter experts and one-on-one interviews with six network automation practitioners, this report identifies the tools enterprises are using, the processes they are automating, the infrastructure involved, and the challenges they encounter.

Introduction

Over the last several years, Enterprise Management Associates (EMA) research has found that enterprises are actively expanding their use of network automation. In the spring of 2018, 92% of network managers claimed that they have a formal initiative to expand their use of network automation, and 70% called that initiative a high priority. They were looking to leverage automation to improve how they optimize networks, respond to security incidents, and manage capacity.[1]

Thus, EMA decided to launch a new research project that explores advanced approaches to enterprise network automation. This report is the result of that study.

1 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.

Overview of Research Participants and Their Networks

This research is based on an online survey of 250 enterprise IT professionals who are directly engaged with a formal initiative to expand their organization's use of network automation technology. Seventy percent of respondents were located in North America, and 30% were based in Europe (France, Germany, and the United Kingdom).

Screening for Network Automation Subject Matter Experts

EMA asked respondents several screening questions to ensure that these individuals not only had an automation initiative in place, but that they were directly engaged with the initiative. **Figure 1** details the nature of this engagement.

The importance of network automation

- 77% "Network automation is a high priority"
- 23% "Network automation is a low priority"

Individuals' engagement with network automation

- 20% Research/evaluate/procure solutions
- 26% Implement/support/maintain solutions
- 30% Manage/operate network with solutions
- 24% Leadership: Set strategy and budget

General state of network automation adoption

- 42% "We are evaluating/developing/testing solutions"
- 32% "We are implementing approved solutions"
- 26% "Our solutions have been deployed on our production network"

Figure 1. Involvement with network automation

Demographics Overview

IT Job Titles

- 29% Middle management (IT manager/director/supervisor)
- 18% Network subject matter experts (engineer, architect, operations pro)
- 14% Software engineer/developer
- 13% Business analyst
- 9% Project manager

IT Group

- 20% IT executive management
- 16% Network engineering
- 14% AppDev /DevOps
- 14% IT management tool architecture/engineering
- 12% Application management/support

Figure 2. Highlighted job titles and IT groups of survey respondents

Company size by number of employees

- 38% Medium enterprise (500 to 2,499)
- 35% Large enterprise (2,500 to 9,999)
- 27% Very large enterprise (10,000 or more)

Annual revenue

- 23% $20 million to less than $100 million
- 48% $100 million to less than $1 billion
- 27% $1 billion or more

Vertical industries (Top 6)

- 19% Finance/Insurance/Banking
- 18% Manufacturing
- 11% Healthcare/Medical/Pharmaceutical
- 10% Retail/Wholesale/Distribution
- 6% Education
- 6% Government

Figure 3. Corporate profiles of survey respondents

Focal Interviews

In addition to the survey, an EMA analyst conducted one-on-one interviews with six network engineers and developers who have hands-on involvement with a network automation initiative. To encourage candor, EMA granted these interviewees anonymity. They included:

- A network reliability engineer with a midsized global media and entertainment enterprise
- A network automation engineer with a large North American research university
- A network automation engineer with a large North American entertainment enterprise
- A network engineer with a very large global pharmaceutical company
- A network automation specialist with a very large North American software enterprise
- A network engineer with a very large North American healthcare enterprise

The Network Automation Mission

EMA asked respondents to identify their most important goals for network automation. They were allowed to select up to three from a list, and the results are detailed in **Figure 4**. Security and compliance risk reduction was the top network automation goal. Automation removes the chance of errors or poor decisions from introducing vulnerabilities. It can also take quick, remedial action when a possible breach or policy violation is detected.

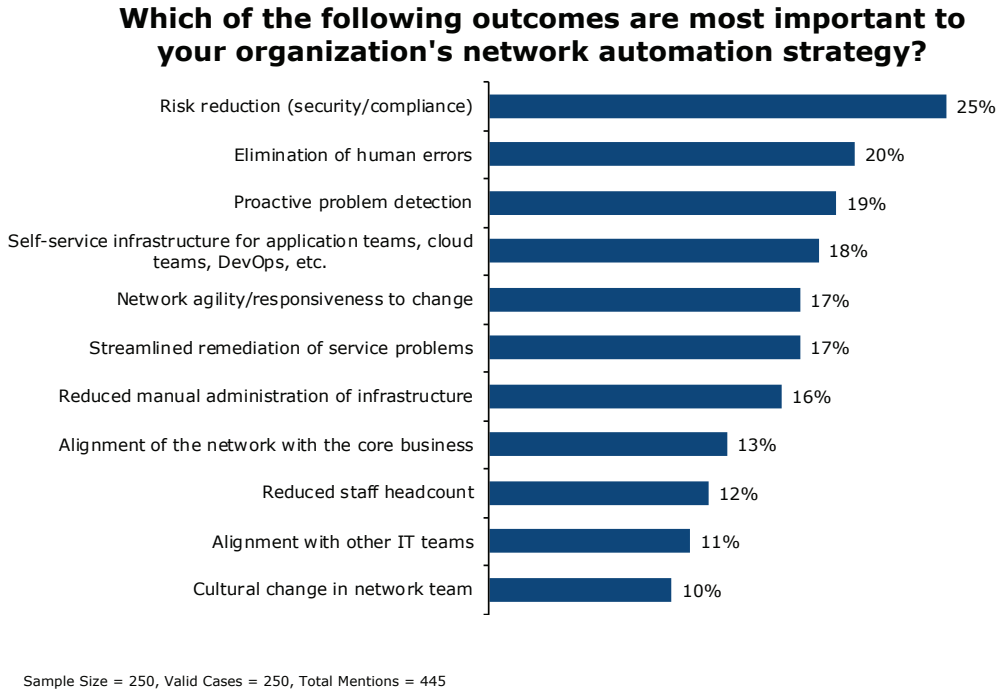


Figure 4. Most important goals of network automation initiatives

Survey respondents had a variety of secondary goals in mind after risk reduction, elimination of human error and proactive problem prevention especially.

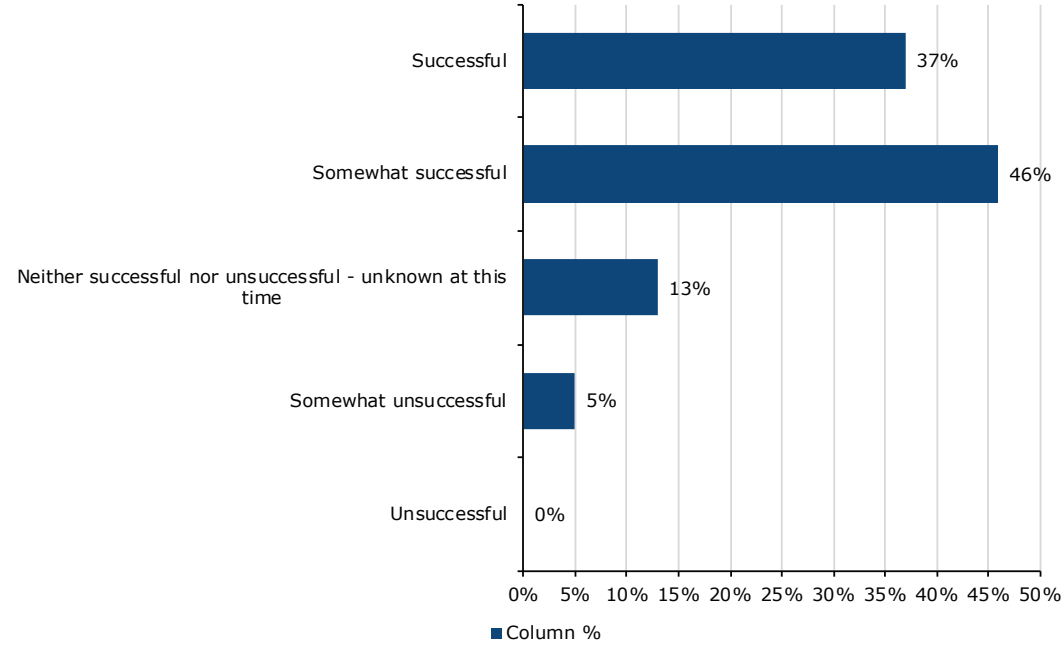
"We wanted to take a template and be sure the template for some device config is being used accurately. We were dealing with a lot of human mistakes," said a network automation specialist with a very large North American software enterprise.

Security and compliance risk reduction was the top network automation goal.

Self-service network infrastructure was a lofty secondary goal. Such a setup allows application teams and others to programmatically request network connectivity and services. Another related secondary goal was network agility. "A major driver was that it was taking too long for multiple teams to push a single request from customer inception out to production," said a network reliability engineer with a midsized global media and entertainment company.

Succeeding with and Trusting Automation

Figure 5 reveals how survey participants feel about their automation efforts. A majority see room for improvement. Nearly half (46%) say they are only somewhat successful and 5% feel somewhat unsuccessful. Only 37% feel successful.



Sample Size = 250

Figure 5. How you do you feel about your team's overall level of success with network automation?

"I would say we were fairly successful, considering what was being thrown at us. But we weren't getting to a product we wanted or that would work. It didn't meet our vision," said a network automation specialist with a very large global software company. This specialist recently left the software company because of this disconnect between implementation and vision. He was trying to write an in-house network automation solution using a variety of open-source solutions and outside professional services, but he felt leadership wasn't aligned with the technical realities of the project.

Survey participants who primarily engage with network automation as users of the technology were more likely to say their automation initiatives were successful. Meanwhile, individuals who provide high-level leadership on network automation were less likely to say they were successful.

Success and Trust are not the Same

Network automation requires a bit of faith. Network operators must be willing to trust that the technology will do what it is meant to do. Not everyone takes that leap of faith, as **Figure 6** reveals. Only 44% fully trust their network automation. Exactly half partially trust it, acknowledging that the technology occasionally introduces errors or network failures. Only a small number completely distrust their automation.

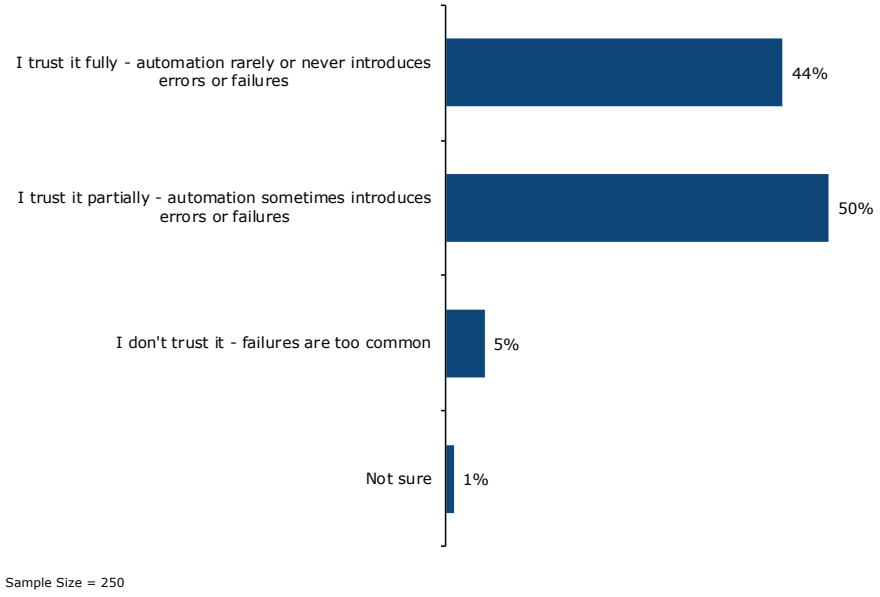


Figure 6. How much do you trust your organization's network automation?

EMA found a strong correlation between success and trust. Individuals who described their network automation initiatives as successful were more likely to fully trust automation. However, focal interviews reveal some significant, well-reasoned exceptions to this correlation.

A network reliability engineer at a midsized global media and entertainment enterprise said that he doesn't fully trust the network automation solution he built, even though he thinks the project has been a great success. "Since we are generating and overwriting 100% of the configurations every time we make a change, most of that configuration information is coming from our [database]. We are exposed to someone making a change in that database that could break the network because we don't have tight controls over those changes. We trust the tools, but we don't trust the data we are using."

Network Automation Challenges

EMA asked research participants to identify the top challenges, if any, that they perceive with the network automation solutions their organizations have chosen to implement. As **Figure 7** illustrates, 96% admitted to having at least one significant challenge. Price was the top response, suggesting that many enterprises are buying commercial products that are difficult to budget for.

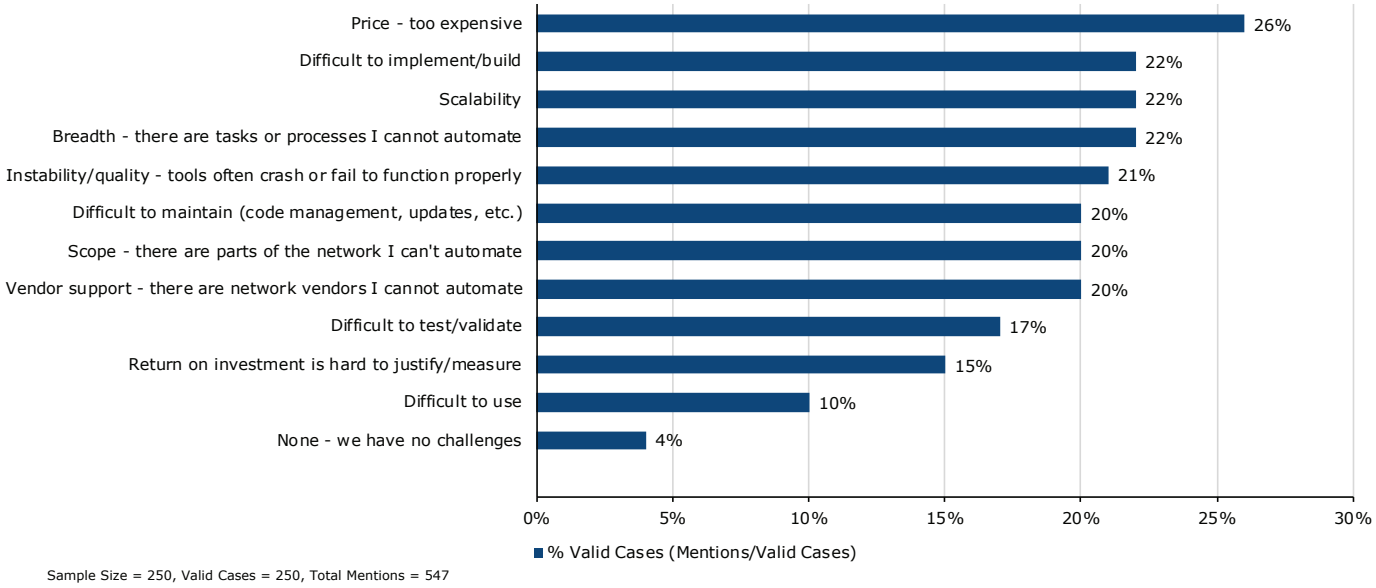


Figure 7. Top challenges encountered with network automation technologies

Seven other challenges emerged in a virtual tie for second, starting with implementation difficulty, scalability, and breadth in terms of tasks/processes automated. A nearly equal number complained of technology instability, maintenance overhead, scope in terms of places in the network that can't be automated, and support of specific network vendors.

Figure 8 looks at automation challenges from another angle: business and cultural barriers. EMA asked respondents to identify their biggest barriers to automating their networks. Security risk is the top response, an interesting finding since risk reduction is also the top goal of automation. Still, EMA noted earlier that many enterprises don't fully trust their automation, even when they feel successful with it. Fear of an automation platform introducing a security vulnerability appears high.

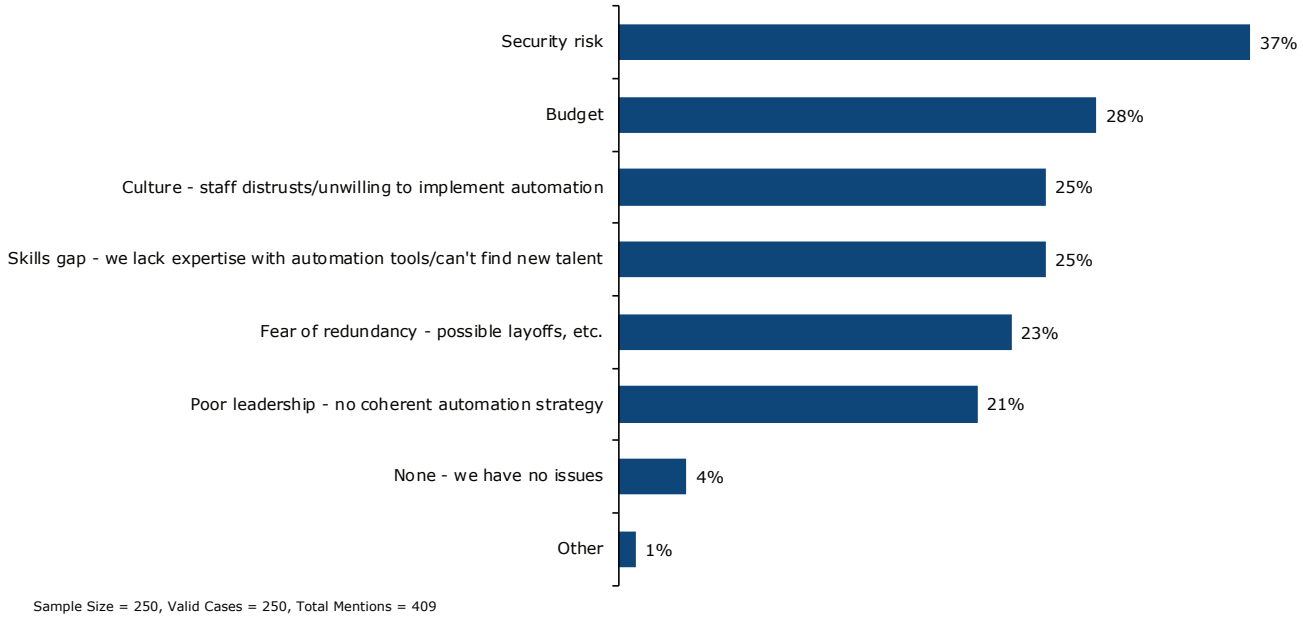


Figure 8. Business and cultural barriers to network automation

Budget is the top secondary issue here, which is unsurprising given that so many people were complaining about the prices of network automation products in Figure 7.

Next on the list of concerns is culture. Network staff simply distrusts or is unwilling to implement automation.

> *"The problem is the pushback from the old guard, who are used to doing things a certain way. This automation scares them a little bit," said a network automation engineer with a large North American research university.*
>
> *"I think their fear is legitimate. The future is software."*

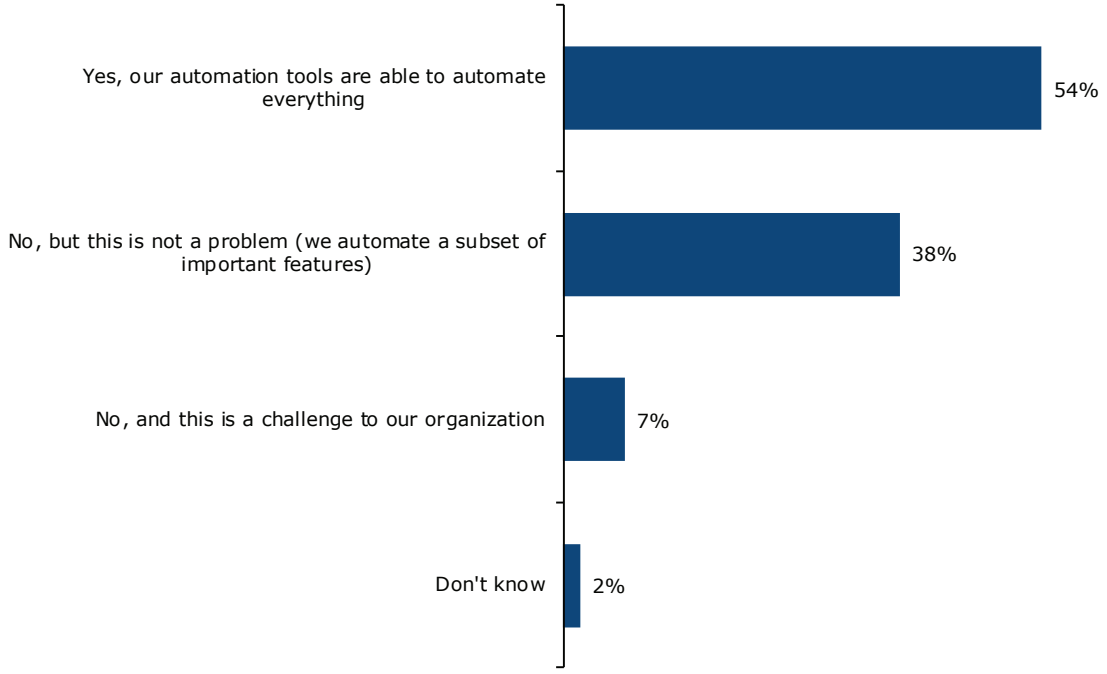
A network reliability engineer with a midsized global media and entertainment enterprise noted that his company's network engineers believe their manual processes are simply more effective, if also more time-consuming, than the automation solutions provided to them. "Even the people who are enthused about automation struggled to get on the right page with it. People loved the config capabilities, but they spent so much time manually collecting information from the network for troubleshooting. They struggled to identify how automation could affect them in that space. They couldn't visualize how solutions could help them."

Fear of redundancy is another issue here. Network engineers are worried that automation is going to put them out of work. Some automation experts say that fear is justified. “The problem is the pushback from the old guard, who are used to doing things a certain way. This automation scares them a little bit,” said a network automation engineer with a large North American research university. “Our NOC has handled most of the hands-on config for things. The most recent project our team developed was zero-touch provisioning. Since we’re taking over that whole process, they were scared. And they feel left out of the process. ‘You’re taking things away from us that are part of our job.’ I think their fear is legitimate. When I was a network engineer, I saw the writing on the wall. The future is software, just like the Industrial Revolution and automation in factories.”

Network Infrastructure: Difficult to Automate

Networking is a prickly technology. Generally speaking, network devices are complex and have broad feature sets, and they make myriad individual decisions within a larger system of other complex, independent network devices. Automation tools have a lot of variables to consider each time they take action, from the standpoint of an individual device and from the view of the overall network. For that reason, EMA has found that network automation solutions tend to tackle the most pressing problems first, automating certain tasks, features, and protocols for which customers are demanding solutions.

Figure 9 illustrates this issue. Forty-five percent of survey respondents noted that their automation solutions are unable to automate 100% of the features and functions on their complex network devices. Fortunately, many of them (38%) say this isn’t a problem, because they are automating a subset of important features. Respondents who are successful with their automation and fully trust the automation were more likely to say their tools can automate everything on their network devices.



Sample Size = 250

Figure 9. Generally, are you able to automate 100% of features and functions on your complex network devices?

Achieving this depth of automation appears to require investment in more tools. For instance, enterprises that use four or more network automation tools were most likely to be able to automate all network features, but enterprises that use one or two tools said they were able to automate only the important features on their devices.

One focal interviewee implied that vendor diversity is a factor here. A network engineer with a very large global pharmaceutical company said he uses multiple vendors and multiple platforms throughout his network. "We are a brownfield environment. We have multiple site types because of acquisitions. There is nothing in the world that would allow us to automate 100%. But if we were deploying [our solution] in a greenfield, you could automate everything,"

EMA asked research participants whether their network automation projects have led them to adopt products from new network vendors. Figure 10 shows that 89% of enterprises have been influenced in this way. Forty-five percent say automation has been a primary driver of new vendor adoption, while 44% say automation was just a contributing factor.

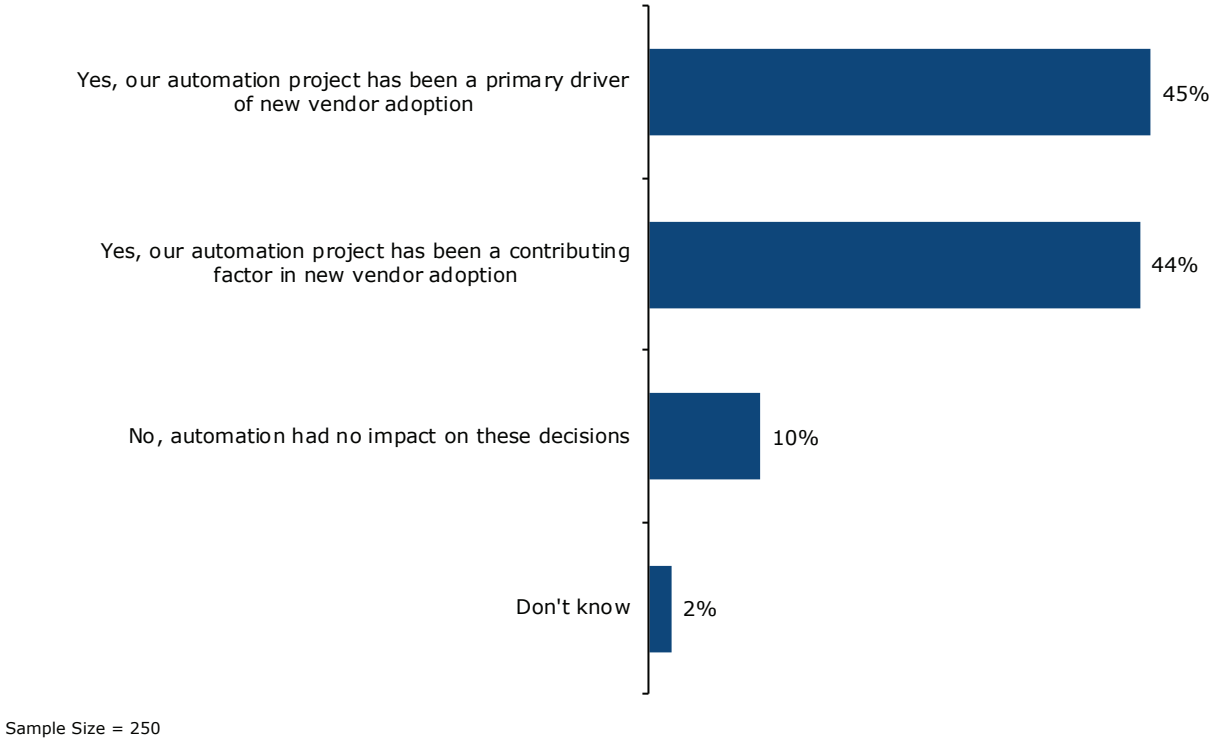


Figure 10. Has your network automation initiative led you to buy products from a new network infrastructure vendor?

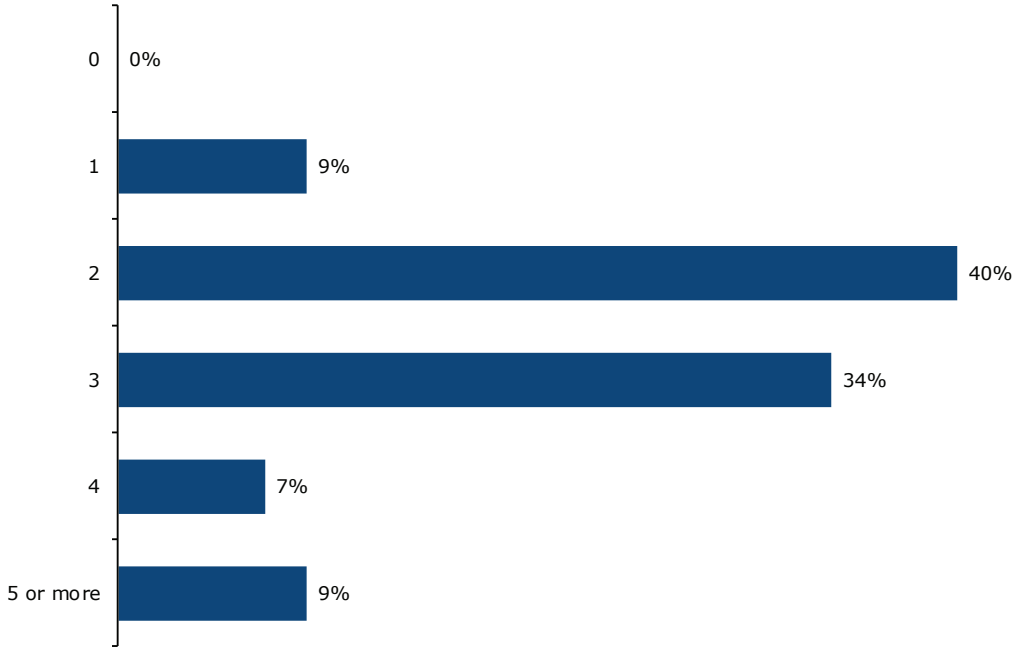
52%

of enterprises consider network device APIs to be critical to their network automation strategy, and another 44% consider APIs to be helpful.

EMA's survey found that 52% of enterprises consider network device APIs to be critical to their network automation strategy, and another 44% consider APIs to be helpful, but not required. APIs correlate strongly with network automation success. Seventy-six percent of successful enterprises describe these APIs as critical, versus only 41% of somewhat successful and 25% of somewhat unsuccessful organizations. EMA observed similar correlations with enterprises that fully trust their automation.

Automation Technology Strategy

For most enterprises, network automation is not a single product that one buys off the shelf. Instead, it's a collection of technologies, some commercial, some open-source, some homegrown. In fact, the typical enterprise in this research has two or three network automation tools, excluding one-off scripts, as revealed by **Figure 11.** Nearly 10% of these enterprises have five or more automation tools.



Sample Size = 250

Figure 11. Number of network automation tools in use, excluding one-off scripts

Given the fact that enterprises are using multiple network automation solutions, EMA asked respondents to characterize the nature of their automation efforts in a number of ways. First, the survey asked them to describe the high-level state of their network automation. **Figure 12** shows the results. In some respects, this chart represents a progression from primitive to advanced automation.

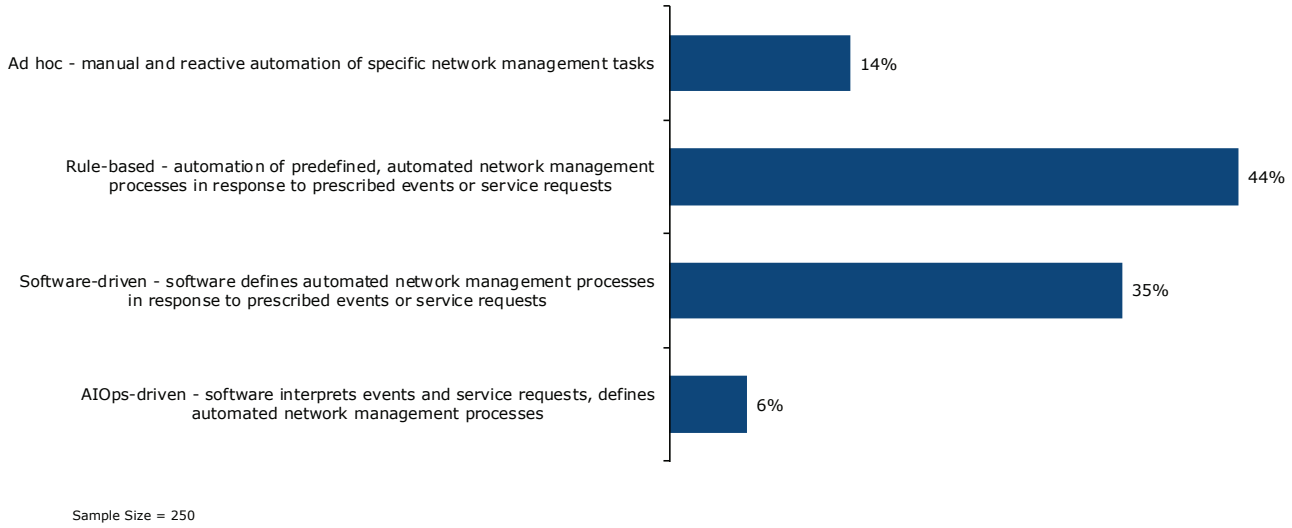
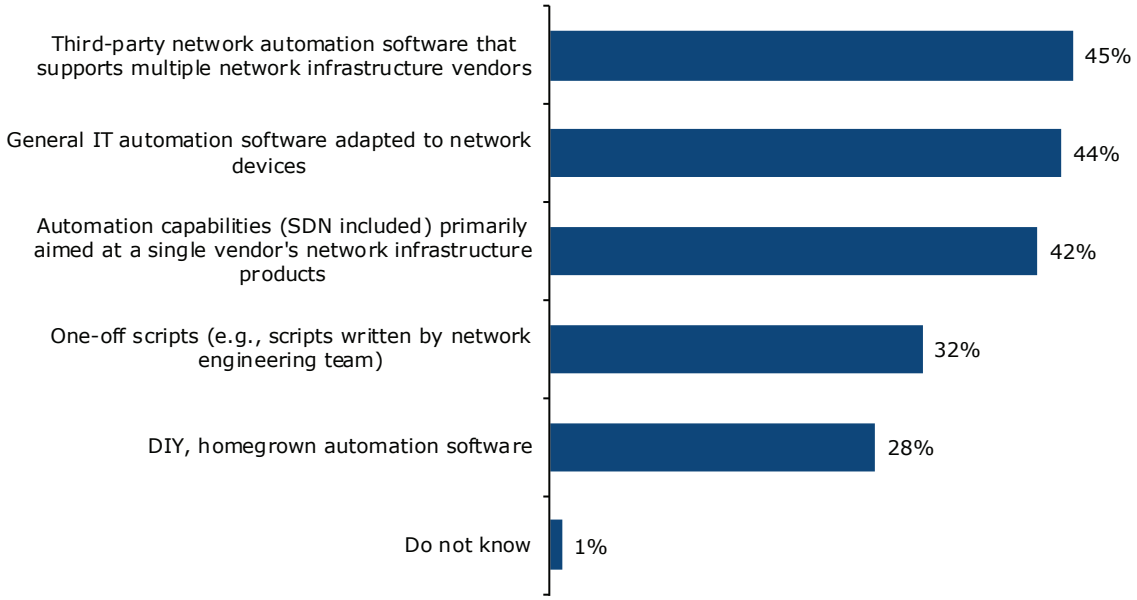


Figure 12. High-level overview of the state of automation

- **Ad hoc**: Fourteen percent of these enterprisers describe the current state of their automation as ad hoc, where engineers are using tools that allow them to automate tasks, rather than business processes. These enterprises are likely relying heavily on a collection of one-off scripts that engineers are writing to automate specific tasks. Most of the enterprises in this survey have moved beyond this approach. Ad hoc automation is more common with aerospace, finance, and government organizations.
- **Rule-based**: The largest cohort in this research describes their automation as "rule-based," in which tools automate a set of predefined network management processes in response to prescribed events or service requests. In this situation, a network automation team might have tools in place that allow them to "push a button" in response to a change request, for instance, kicking off templated series of tasks that completely implement a change and close the ticket.
- **Software-driven**: A more advanced approach, also fairly common, is software-driven automation. This automation still responds to a set of predefined events or service requests, but tools can define an automated network management process in response to these events. Software-driven automation is more common with legal, oil & gas, and retail enterprises. It is less popular with enterprises that have 10,000 or more network devices.
- **AIOps-driven**: AIOps-driven automation is least common. Some engineers might characterize this as a future-state goal; others might call it science fiction. In these rare environments, software interprets network events or service requests and then defines automated processes in response. Enterprises that use AIOps-driven automation were more likely to be successful with their automation initiatives.

Next, EMA asked respondents to identify the classes of technology they use or plan to use for network automation. EMA identified five general categories, as revealed in **Figure 13.** Three types of solutions are most common: third-party network automation software that supports multiple infrastructure vendors, general IT automation software adapted to networking, and automation capabilities primarily aimed at a single vendor's networking products.



Sample Size = 250, Valid Cases = 250, Total Mentions = 482

Figure 13. Classes of network automation technology in use or planned for use

General IT automation software adapted to networking was more popular among large enterprises. Single vendor automation capabilities were more popular among Europeans. More significantly, third-party, multi-vendor network automation software was more popular with individuals who fully trust their automation solutions.

One-off scripts and homegrown automation software were the least popular classes of technology. Homegrown automation appears to be risky. It was more popular among somewhat unsuccessful and somewhat successful network automation initiatives, and less popular among successful ones.

"Source of Truth" for Network Automation

Authoritative data is essential to network automation. Automation tools need a complete understanding of the network before they attempt to make changes to it. Many industry leaders have begun referring to this authoritative data repository as a network "source of truth." A source of truth might contain data on device inventories, monitoring metrics, configuration files, network policies, and much more.

"Our [network automation] is driven by a central database that we call a source of truth, where we put in network intent. Then, all our automation tools are integrated around that database, and our tools generate configs based on that information and deploy it. We have all our monitoring and alerting tools hooked into that database to compare every alert coming in and understand what was worth alerting on," said a network reliability engineer with a midsized global media and entertainment enterprise.

41%

described their sources of truth as "essential" to their network automation initiatives.

Some network automation tools will have a source of truth integrated directly into the platform. As a network engineer with a very large global pharmaceutical enterprise noted, "Our automation solution is the most comprehensive source of truth that we have. It has a Yang model built into the platform."

Other enterprises will maintain one or more separate sources of truth that are integrated with their automation tools. EMA asked survey respondents whether they have a source of truth for their networks. Ninety-eight percent said yes, and 41% described their sources of truth as "essential" to their network automation initiatives. Half called their sources of truth "helpful."

Figure 14 reveals how enterprises are approaching these sources of truth. Only 26% have a single, authoritative repository, which underscores exactly how hard it is to build such a thing. There is such a diversity of data that it's hard to normalize all of it into a single database, as one interviewee caustically noted.

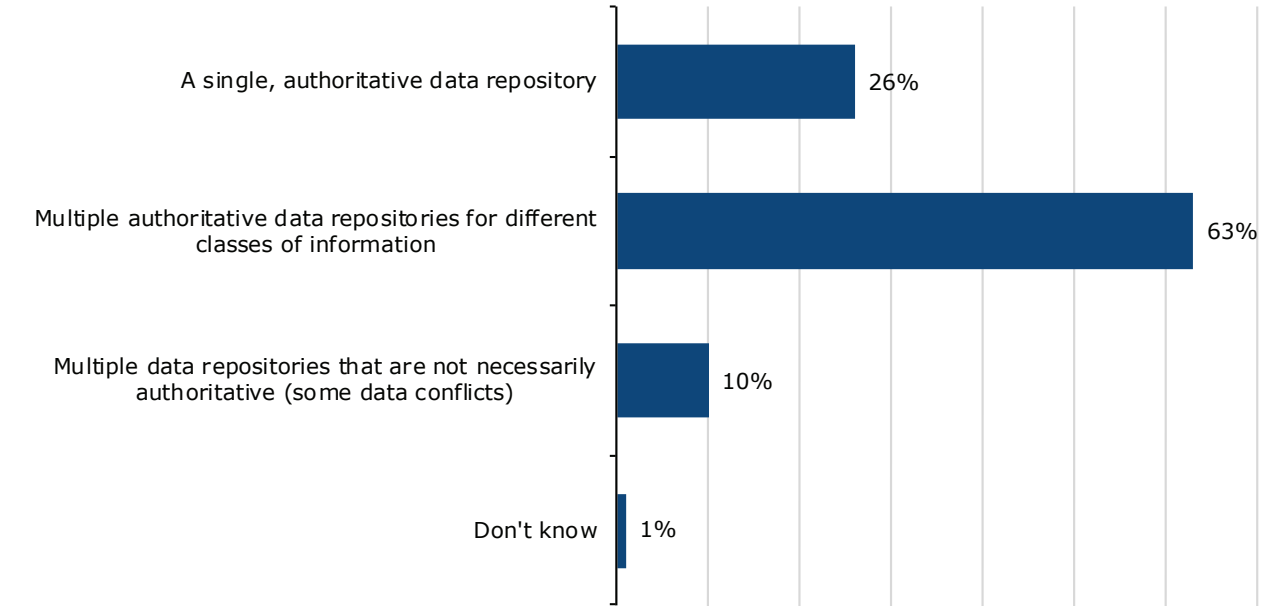


Figure 14. Enterprises characterize their network automation "source of truth"

"[Authoritative source of truth] is a BS term. There isn't a single source of truth. There are systems of record, like IPAM for IP addresses and DCIM software that has a record of all devices on the network, and another that tracks cabling. All of them can be combined to create a system of record, but it's always ephemeral," said a network automation engineer with a large North American entertainment company.

"We ended up with multiple repositories for our source of truth. We used Netbox as the primary database, but there were a lot of things we couldn't store in it. So, we built an additional source of truth in Git and merged information from different places," said a network reliability engineering with a midsized global media and entertainment enterprise.

85%

of respondents said they use advanced analytics in their network automation strategy, and 34% described analytics as essential.

Network Automation and Advanced Analytics

EMA asked survey participants whether advanced analytics technology, such as AIOps and machine learning, were a part of their network automation strategy. Eighty-five percent of respondents said they use advanced analytics in their network automation strategy, and 34% described analytics as essential. More than half called it helpful. Another 11% said they haven't integrated analytics into their automation, but they hope to do so in the future.

Figure 15 reveals how enterprises primarily apply analytics to their network automation solutions. The most common approach is the integration of a third-party analytics tool into one or more network automation tools (39%). A smaller number have network automation tools with built-in native analytics capabilities. The least common approach is to maintain a separate analytics tool through direct integration. In other words, personnel manually apply insights from the analytics solution to their network automation tools. This latter, manual approach to analytics correlated to enterprises that were unsuccessful with automation.

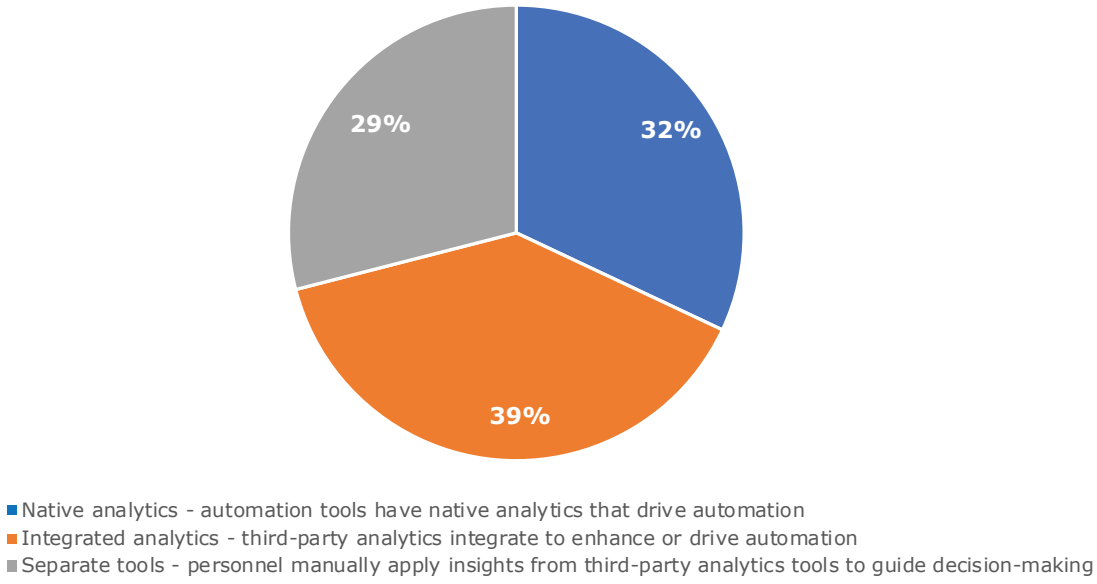


Figure 15. How enterprises primarily apply advanced analytics to network automation

Native Zero-Touch Provisioning on Network Devices

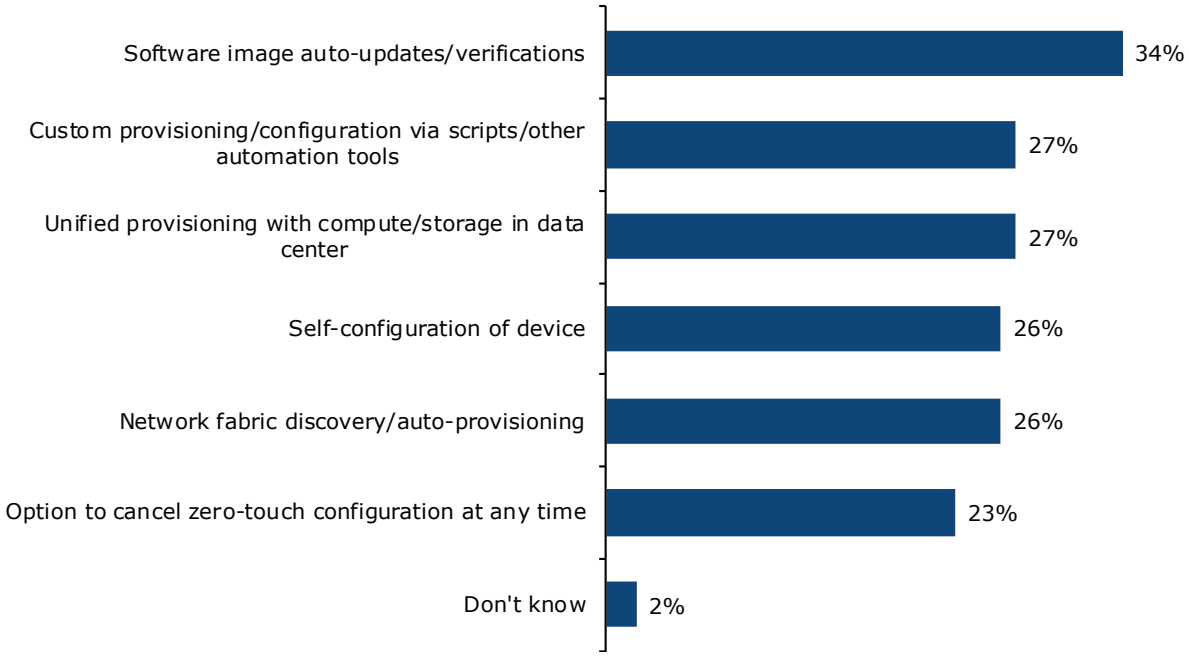
Zero-touch provisioning (ZTP) is a capability that can be enabled via third-party network automation software, but embedded ZTP capabilities are another option. Some vendors are shipping network platforms with ZTP native to device firmware. Ninety-one percent of survey participants expressed interest in network devices with ZTP features, and 39% called such embedded features "critical."

91%

of survey participants expressed interest in network devices with ZTP features, and 39% called such embedded features "critical."

Successful enterprises were much more likely to consider these ZTP features critical (58%), as were enterprises that fully trust their network automation (58%).

Figure 16 reveals the aspects of embedded ZTP features that enterprises find most valuable. The highest priority is the ability to auto-update and verify software images at initial activation of the device. Nearly every other ZTP feature EMA investigated in the survey was of equal secondary interest, such as custom provisioning and configuration via scripts, unified provisioning with other layers of data center infrastructure, self-configuration of devices, and network fabric discovery and auto-provisioning. North Americans were more interested in unified provisioning than Europeans.



Sample Size = 250, Valid Cases = 250, Total Mentions = 409

Figure 16. Most valuable aspects of embedded zero-touch provisioning features on network hardware

What are Enterprises Automating?

EMA asked research participants to identify the tasks they want to automate, the infrastructure domains they are targeting, and the classes of devices they are automating.

Network Management Task Automation

Figure 17 reveals the general network management tasks in the data center network that enterprises are targeting for full automation. It also reveals the automation plans of a subgroup of enterprises that fully trust their automation technology.

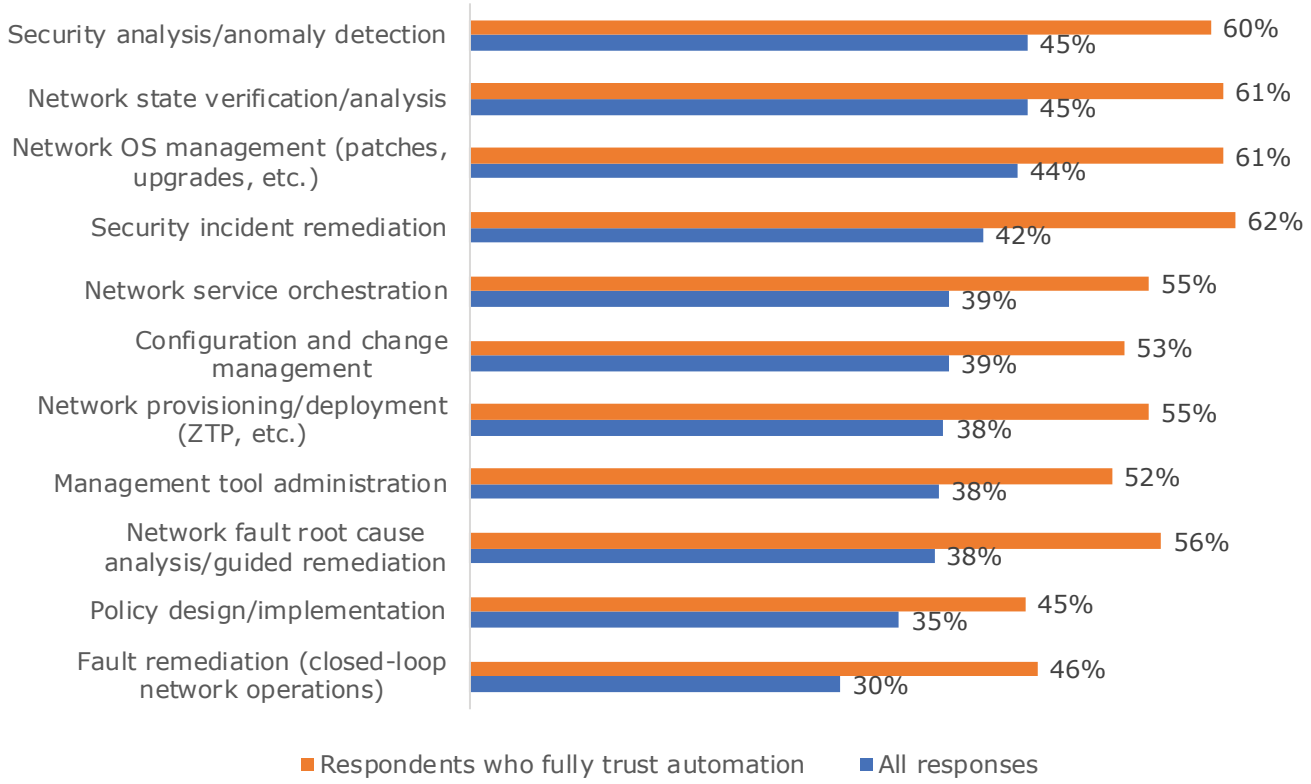


Figure 17. Network management tasks targeted for full automation in the data center network

EMA found that enterprises are most interested in fully automating the following management tasks in the data center network:

- Security analysis
- Network state verification and analysis
- Network operating system management
- Security incident remediation

They are least interested in automating policy design and fault remediation (e.g., closed-loop network operations).

As Figure 12 also reveals, those who fully trust their automation are more interested in fully automating every task. EMA observed a similar pattern with those who consider their automation to be successful.

The enterprise network, such as campus networking and the WAN, presents slightly different requirements than the data center network. For one, the sheer volume of network devices outside the data center can create a different set of priorities, as will the features and functionality of Wi-Fi and user access switches. Some enterprises focus a tremendous amount of their automation efforts on the enterprise network.

Figure 18 looks at interest in fully automating network management tasks on the enterprise network. Security analysis is still a top priority, but the rest are different from data center networking priorities. Here, management tool administration and security incident remediation have risen to the top of the list, while network state verification has slid down a few spots.

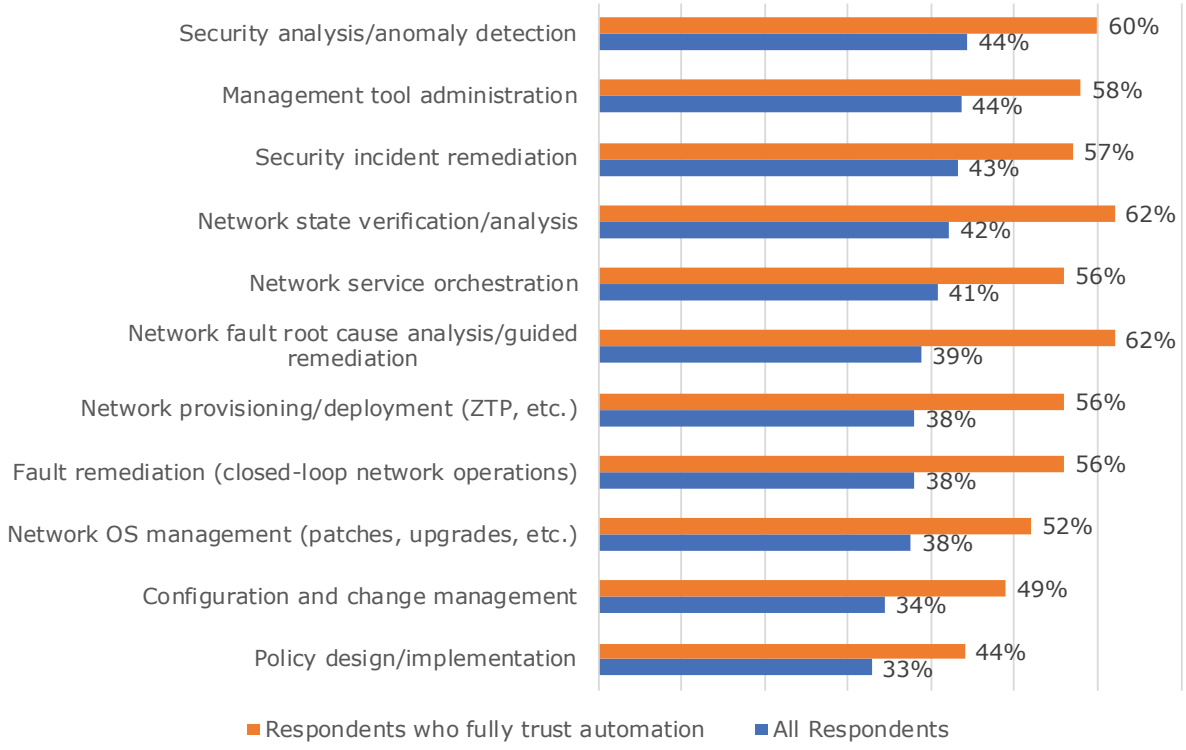
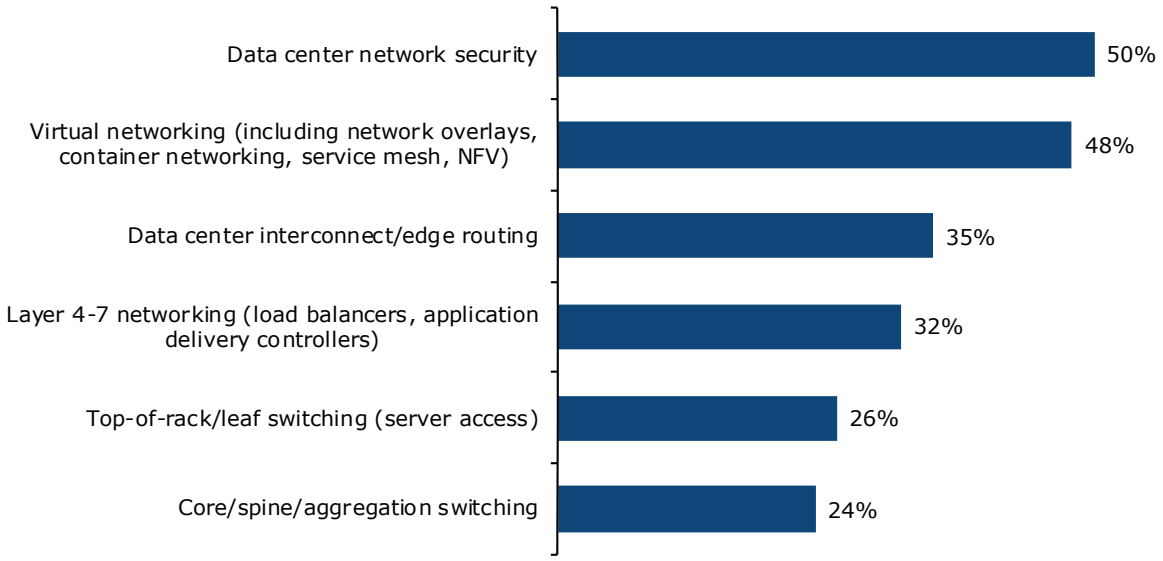


Figure 18. Network management tasks targeted for full automation in the enterprise network (LAN, WAN, etc.)

Figure 18 also shows that interest in full automation of all these tasks is higher among enterprises that fully trust their automation. Again, EMA observed a similar pattern among enterprises that are successful with automation.

Automating Places in the Network

Figure 19 identifies the places in data center networks that enterprises are trying to automate with their initiatives. Clearly, network security and virtual networking (such as overlays, containers, virtual network functions) are the two major foci.

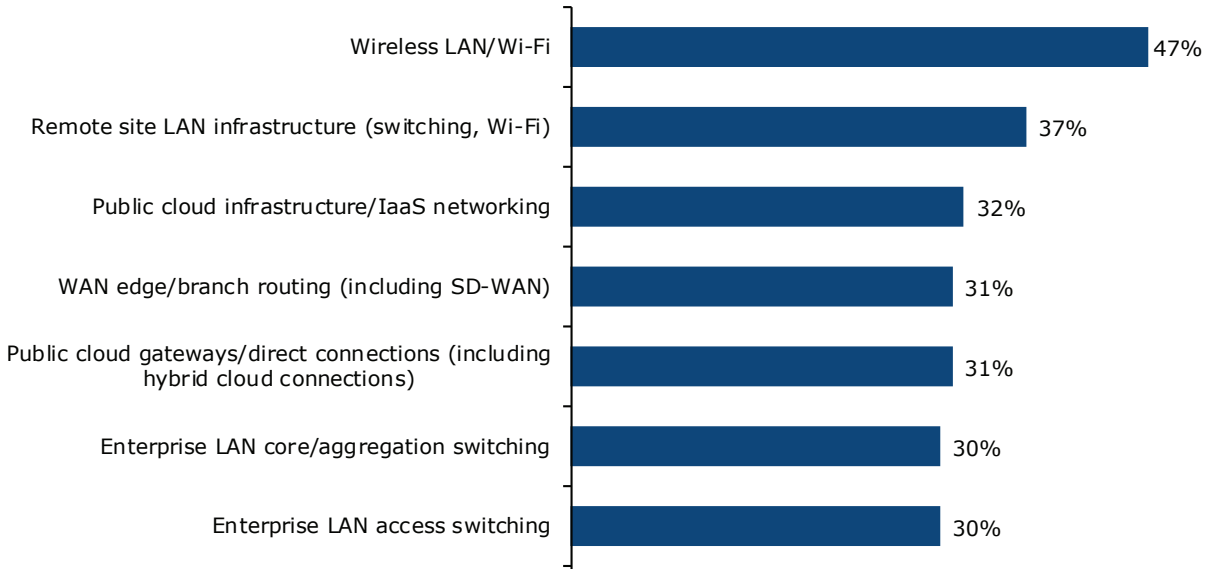


Sample Size = 250, Valid Cases = 250, Total Mentions = 543

Figure 19. Places in the data center network targeted for automation

Data center interconnect, edge routing, and Layer 4-7 networking (such as application delivery controllers and load balancers) were the secondary targets.

Figure 20 looks beyond the data center and identifies places in the enterprise network that these organizations are automating. There is less of a hierarchy in overall priorities. Wireless LAN is clearly the most popular target, followed by remote site LAN infrastructure, such as branch office switching and Wi-Fi. This reveals that enterprises are focused on automating the access layer of the enterprise network, except for enterprise LAN access switching, which is becoming less relevant as Wi-Fi becomes a de facto access layer for most networks.



Sample Size = 250, Valid Cases = 250, Total Mentions = 596

Figure 20. Places in the enterprise network targeted for automation

Assembling the Automation Team

Addressing Network Automation Skills Gaps

Network automation tends to expose skills gaps in the IT organization. As **Figure 21** reveals, only 3% claim their current skillset is sufficient. Forty-six percent are primarily addressing the skill issue by moderately training up existing staff, and 37% are devoting very significant resources to training. Enterprises that use four or more network automation tools are more likely to devote very significant resources to training existing personnel.

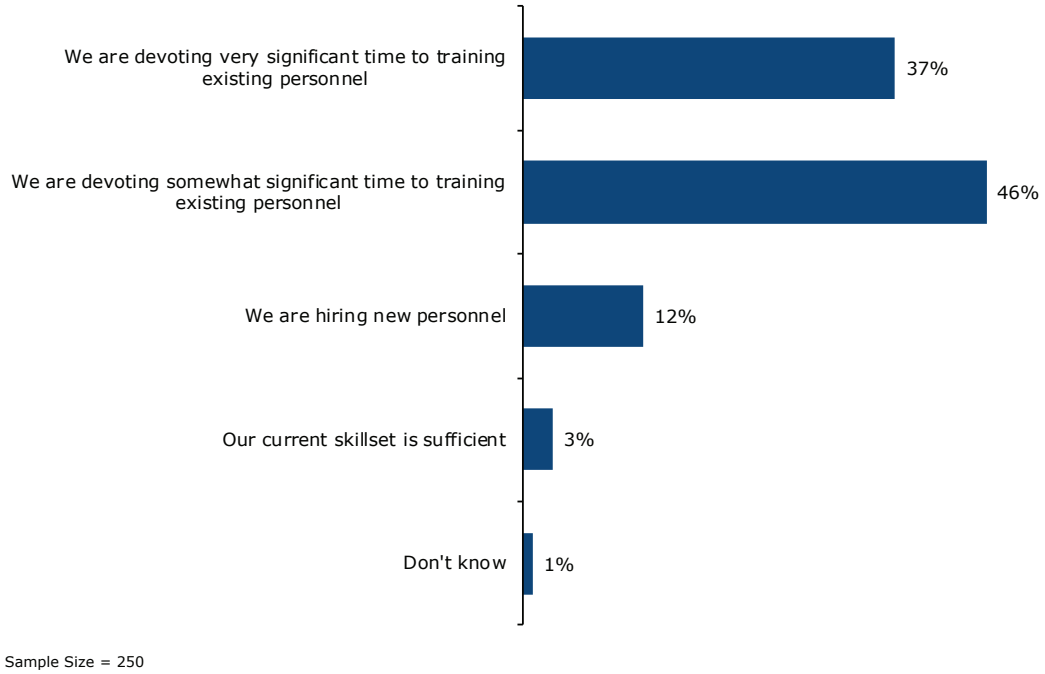
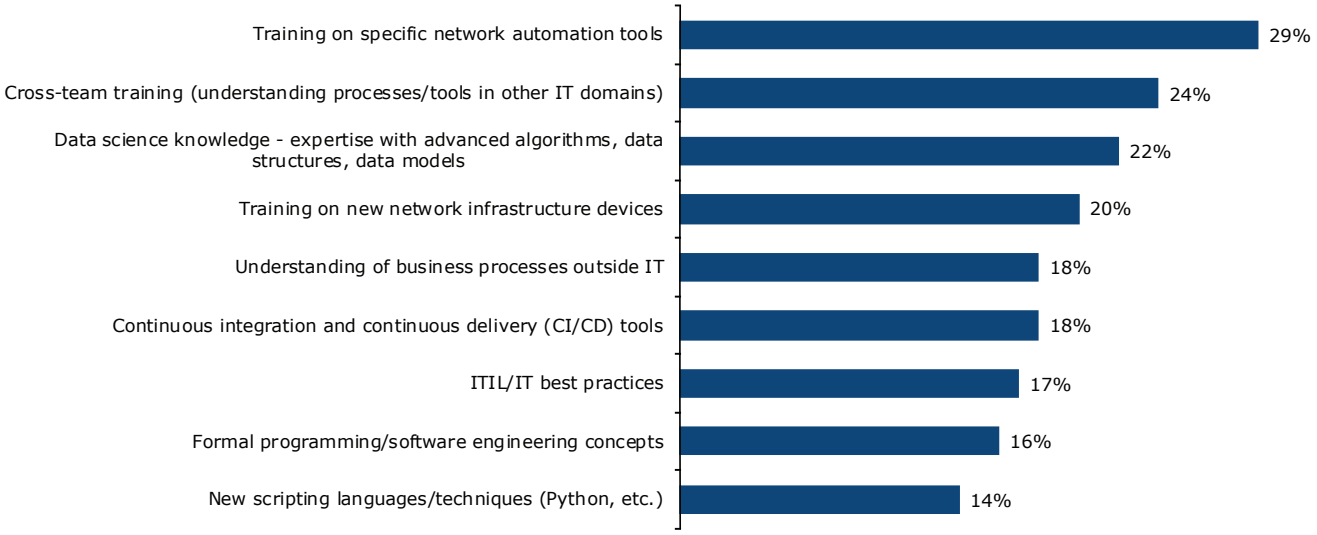


Figure 21. How enterprises are dealing with network automation skills gaps

"Companies need to set aside time to let network engineers develop skills over time, so they're not in this constant panic of firefighting," said a network automation engineer with a large North American entertainment company. "With [network automation] programming, you can't send a person to a one-week bootcamp and turn them into a software developer. The whole concept of writing code and testing it is completely akimbo from what a network engineer does every day."

"Companies need to set aside time to let network engineers develop skills over time," said a network automation engineer with a large North American entertainment company. "You can't send a person to a one-week bootcamp and turn them into a software developer."

Figure 22 identifies the skills and knowledge that enterprises most need to add for their network automation initiatives. The priority is training on a specific tool. In other words, enterprises have adopted network automation tools and now they need to train their network team to use them. This is typical for any new network management product. This type of training is a higher priority for enterprises successful with automation.



Sample Size = 239, Valid Cases = 239, Total Mentions = 427

Figure 22. Skills and knowledge network teams most need to acquire in support of network automation

The next priority is cross-team training. Automation apparently requires network teams to understand the processes and tools other IT teams use. This requirement is more common with enterprises that use four or more network automation tools, suggesting that as automation toolsets grow, some of those tools are shared with or borrowed from other parts of the IT organization.

The prominence of data science expertise reflects the strong interest enterprises have in applying advanced analytics technology, such as machine learning, to network automation. Also, data science expertise is in more demand among organizations that are successful with network automation.

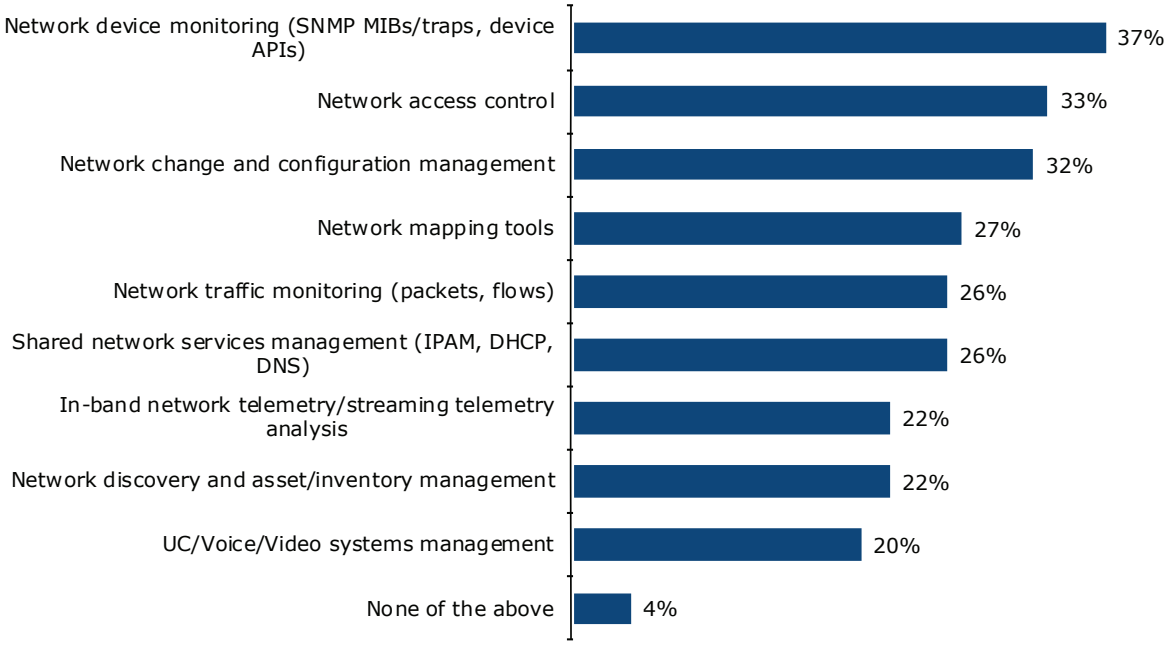
The lowest training priorities are formal programming, software engineering expertise, and scripting skills. These latter findings are surprising given the dominant conversation in the industry about network engineers learning how to be programmers. In fact, Cisco recently launched a new series of career certifications aimed precisely at this skillset.

Several focal interviewees emphasized the need for formal software engineering skills:

- Depth of programming skills is an issue for a network engineer with a very large North American healthcare enterprise. “We have a very highly skilled team, but I’m the Python expert and my counterpart knows very little of it. She handles most of Ansible, and I’m not well-versed in that. I have a hard time finding peer review [for my scripts], and I can’t peer review her stuff.”
- A network automation engineer with a large North American entertainment company said network automation software developers especially need code management and project management skills. “They need a discipline around source control hygiene. Do you use GitHub to check in your code? Do you use version control and peer review? Another core skill is, are they using a tool that allows them to break down [software development] tasks into stories and allows them to put time estimation around it? And are those systems being used to keep a software development process on track?”

Integrating Network Automation with IT Systems

EMA explored the network management tools that enterprises are integrating with their network automation. **Figure 23** reveals three top priorities: network device monitoring, network access control (NAC), and network change and configuration management (NCCM). Device monitoring will be valuable for insight into the network state, and this research already found that device metric data is valuable both to network sources of truth and to advanced analytics for driving automation. NAC and NCCM both offer some orchestration capabilities, and they can also serve as repositories for authoritative truth for the network, such as for access policies and for gold-standard configurations. In fact, many enterprises consider NCCM tools to be a part of their network automation toolset. Successful organizations were more likely to integrate automation with NAC systems.

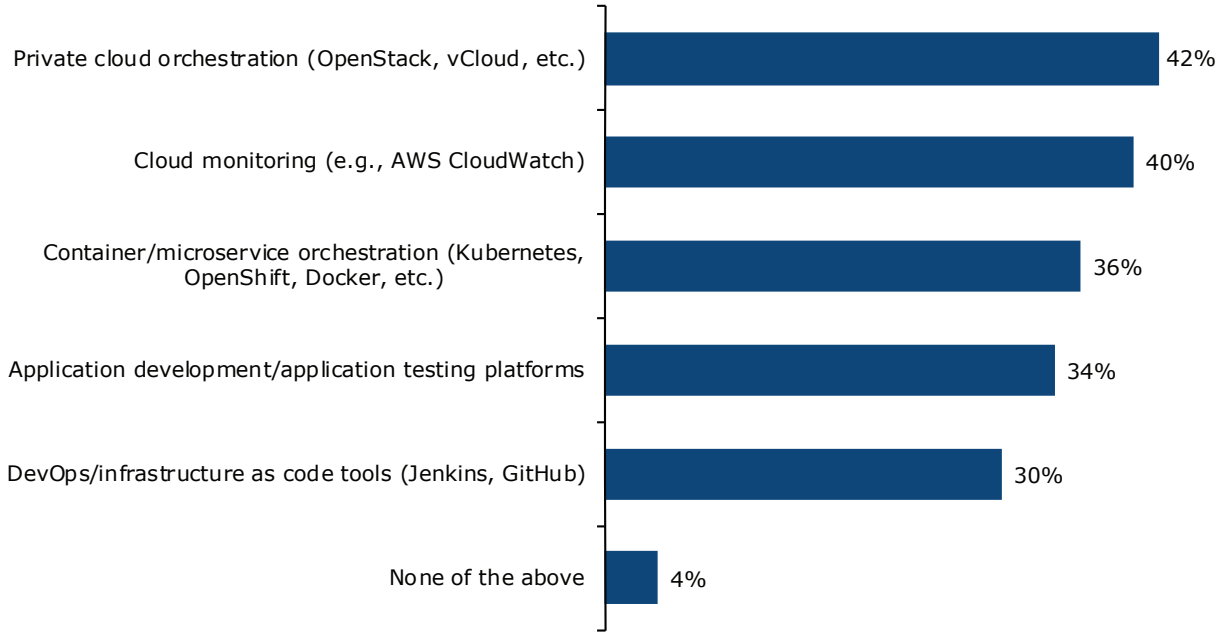


Sample Size = 250, Valid Cases = 250, Total Mentions = 624

Figure 23. Network management tools integrated with network automation solutions

Network mapping tools, traffic monitoring tools, and shared network services management are secondary integration priorities. Shared services in integration was more popular among enterprises that use three or more network automation tools.

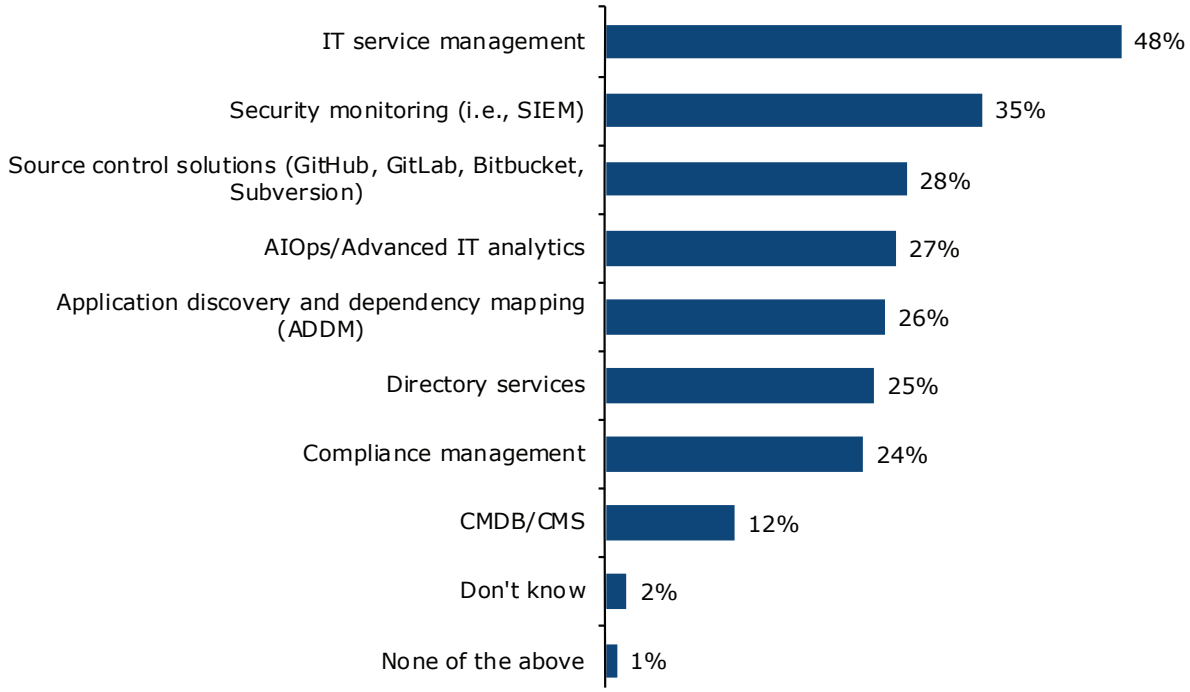
Figure 24 explores the cloud operations and DevOps tools that enterprises are integrating with network automation. Private cloud orchestration and cloud monitoring are the hottest targets. Container/ microservices orchestration and application development and testing platforms are secondary priorities.



Sample Size = 250, Valid Cases = 250, Total Mentions = 463

Figure 24. CloudOps/DevOps tools integrated with network automation solutions

Finally, **Figure 25** reviews the general IT systems that enterprises integrate with network automation. IT service management (ITSM) is the major priority, which is unsurprising given how much of automation is driven by ticketing. Successful enterprises were more likely to integrate with ITSM.



Sample Size = 250, Valid Cases = 250, Total Mentions = 571

Figure 25. IT management systems integrated with network automation solutions

Security monitoring is the chief secondary priority. Everything else is a tertiary integration target, with the exception of CMDB/CMS, which is mostly an afterthought. In fact, CMDB/CMS integration was a priority for organizations that don't trust their automation, which is a red flag. Previous research found that network operators have struggled to integrate their tools with CMDBs because this integration sometimes adds more manual administrative overhead into the CMDB tool.

Conclusion

This research found that network automation is about more than buying an off-the-shelf product. In fact, very few enterprises install a single tool to solve the problem of automation. Instead, enterprises are adopting a variety of solutions, including commercial software, embedded capabilities in network hardware, homegrown software, and tried-and-true on-off scripts.

Automation initiatives typically leverage some kind of advanced analytics technology, like AIOps. They also have an authoritative source of truth, so that network automation tools understand the intended configuration of the network and the network's true state. However, enterprises rarely have a single data repository for this source of truth. It requires a federation of non-conflicting repositories.

The majority of enterprises see room for improvement in their overall network automation efforts, and most enterprise also don't fully trust their automation—even some of those that feel successful. Success does have its benefits. Enterprises are primarily focused on reducing security and compliance risk, eliminating human errors, proactively preventing problems, and establishing self-service infrastructure to the business.

This research revealed what enterprise peers are doing today with network automation and offers a roadmap for potential best practices. EMA will continue to monitor this space closely in the context of future research projects on other topics, such as performance management and cloud networking.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3869.08272019