

Enterprise Network Automation:

Emerging From the Dark Ages and Reaching Toward NetDevOps

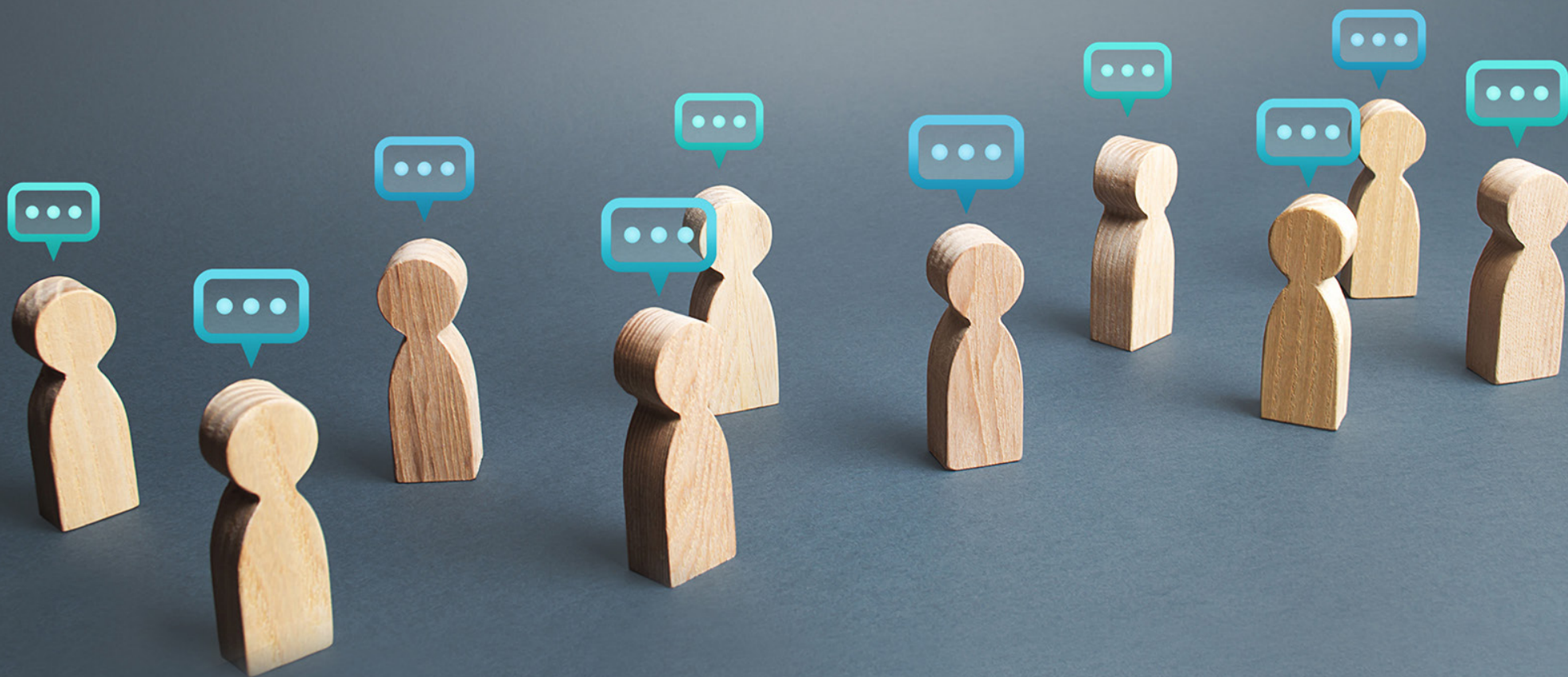
March 2024 EMA Research Report

By Shamus McGillicuddy, Vice President of Research
Network Infrastructure and Operations



Table of Contents

2	Introduction	27	Using AI/ML-Driven Network Automation
3	Methodology	28	Continuous Network Compliance Monitoring
4	Demographic Overview	29	Benefits of Continuous Compliance Monitoring
5	Key Findings	29	Integration Requirements
7	Drivers of Network Automation	30	Spotlight on Network Source of Truth
8	Technical Initiatives that Require Network Automation Investment	32	Effectiveness of Sources of Truth
9	Preventing or Solving Problems with Network Automation	33	Critical Features of a Source of Truth
10	Snapshot of Network Automation Strategies	34	Achieving a Source of Truth
11	Project Status	35	Where Do You Find the Truth?
11	Budgeting for Automation Projects	35	Source of Truth Data
12	Budgets are Growing	36	Gathering Source of Truth Data to Make a Change
13	Network Automation is a Multi-Tool Proposition	37	Consequences of Manual Data Gathering
13	Extent of Automation	38	Spotlight on Network Validation
14	Where are They Automating?	39	Pre-Change Validation
15	Self-Service Networking	40	Frequency of Pre-Change Validation
16	Build Versus Buy Network Automation	41	Post-Change Validation
17	DIY Network Automation	42	Frequency of Post-Change Validation
18	Drivers of DIY Network Automation	42	What is Validated?
19	Maintaining DIY Tools	43	Comparing Network Intent and State
20	Commercial Network Automation	44	Project Outcomes
21	Drivers of Commercial Network Automation	45	Project Success
22	Weighing Vendor Solutions Against DIY Solutions	46	Benefits of Network Automation Investments
23	Network Automation Solution Requirements	47	Current Support of Key Capabilities
24	General Feature Requirements	48	Business Challenges
25	General Platform Requirements	50	Technical Challenges
26	No-Code, Low-Code, High-Code?	52	What Needs Improvement in Automation Toolsets
27	Intelligent Automation with AI and Machine Learning	53	What Network Automation Vendors Need to Know
		54	Conclusion
		56	Appendix: Demographics



Executive Summary

This independent, multi-sponsor market research report explores the state of network automation initiatives in enterprise IT organizations. Based on a survey of 354 network automation stakeholders and in-depth one-on-one interviews with ten network automation professionals, the report explores the entire lifecycle of network automation strategies, including both homegrown and commercial solutions.



Introduction

Network automation remains an unsolved problem for enterprise IT organizations. For decades, vendors and IT professionals have developed and implemented tools aimed at reducing manual management of networks with mixed results. Commercial tools often lack multi-vendor support or have challenges with scalability or support of diverse network designs. Networking professionals write single-use scripts to automate individual tasks, but these scripts are difficult to maintain and orchestrate across processes.

“Once you have a script doing one little task for you, that’s automation,” a network automation engineer at \$3 billion SaaS provider recently told EMA analysts. “But that’s not necessarily doing well in the big picture. Network automation folks make mistakes when they write 100 different scripts unrelated to each other, which causes issues in the big picture of orchestrating everything together.”

Moreover, networks are inherently more complex than other aspects of IT infrastructure. Network equipment is highly proprietary, and many equipment features are best exposed via command line interface (CLI), even though many vendors have offered application programming interfaces (APIs) for years. Part of the problem is also cultural. Network engineers are simply accustomed to managing equipment manually, which leads to errors, compliance issues, and inefficient operations.

Enterprise Management Associates’ (EMA) Network Infrastructure and Operations practice has tracked this issue for years. We have consistently found that IT organizations cobble together a mix of homegrown, open source, and commercial tools to automate their networks. Clearly, IT organizations recognize that there isn’t one tool that can solve the entire problem. Instead, they need a portfolio of tools – but what makes a successful network automation tool portfolio? This report explores that question in depth. Through survey data and interviews with network automation experts, EMA will attempt to provide a roadmap toward network automation success by revealing what your peers are doing, where they run into problems, and where they are finding success.

Methodology

EMA surveyed 354 IT professionals in January 2024 about their organization’s approaches to network automation. All respondents had direct involvement with network automation as developers of homegrown tools, implementers of commercial tools, users of tools, or managers of teams responsible for network automation.

Also, EMA interviewed ten networking professionals, primarily from Fortune 500 enterprises, who either implement or use network automation tools. These interviews enriched EMA’s analysis of its survey data and interview subjects are quoted anonymously throughout this report. The interview subjects were a:

- Network tools engineer at a Fortune 500 retailer
- Network automation engineer at a large university
- Network automation engineer at a medical school and hospital chain
- IT tool architect at a Fortune 500 media company
- Network automation engineer at a \$3 billion SaaS provider
- NOC analyst at a very large private media company
- Network engineer at a Fortune 500 food and agriculture company
- Network engineer at a midmarket business services company
- Network automation engineer at a Fortune 500 manufacturer
- Network engineer at a private gaming company

Demographic Overview

Figure 1 details the demographics of the 354 people EMA surveyed for this research. It reveals a diverse mix of job roles and IT groups, industries, and sizes of enterprise. Also, it reveals a transatlantic view of network automation, with respondents from the Unites State, Canada, France, Germany, and the United Kingdom.

FIGURE 1. DEMOGRAPHIC OVERVIEW

Job Titles

- 22%** Network administrator/engineer/architect
- 5%** Network automation engineer/NetDevOps engineer
- 7%** Project manager
- 49%** IT middle management
- 18%** IT executives

IT Groups

- 17%** Network engineering
- 17%** Network operations/NOC
- 16%** CIO suite/executive management
- 14%** IT architecture
- 11%** Cloud engineering/operations
- 10%** Information security/cybersecurity
- 7%** IT tool engineering/development
- 7%** Security operatio

Top Industries

- 20%** Finance/Banking/Insurance
- 20%** Manufacturing
- 13%** Retail/Wholesales/Distribution
- 9%** Health Care
- 6%** Business Services – not related to IT
- 4%** Education/Research
- 4%** Consumer Services
- 4%** Oil/Gas/Mining

Company Size (Employees)

- 49%** 1,000 to 4,999
- 38%** 5,000 to 19,999
- 13%** 20,000 or more

Revenue

- 19%** \$100 million to less than \$500 million
- 25%** \$500 million to less than \$1 billion
- 39%** \$1 billion to less than \$5 billion
- 15%** \$5 billion or more
- 3%** Unknown/Not applicable

Region

- 63%** United States/Canada
- 37%** France/Germany/UK



Key Findings

- Only 18% of organizations have a completely successful network automation strategy
- The top technical issues with network automation are:
 - Integration issues
 - Lack of network standards
 - Legacy network issues (poor vendor APIs, inconsistent features)
- The top business issues with network automation are:
 - Poor IT leadership
 - Staffing issues
 - Budget issues
- Nearly 94% of organizations use both vendor solutions and do-it-yourself solutions for network automation
- 91% of network automation strategies are multi-tool
- Top drivers of vendor adoption are:
 - Security/Compliance requirements
 - Platform requirements (stability, scalability)
 - Breadth/Depth of functionality
- Top drivers of DIY adoption are:
 - Functionality aligned to specific network requirements
 - Security/compliance requirements
 - Cost savings
- Cloud migration and hybrid multi-cloud architectures are the primary drivers of network automation
- Network automation investments are primarily aimed at addressing network complexity and improving operational efficiency
- Security policy management, configuration compliance management, and network validation/assurance are the more important features organizations are seeking from their tools
- Most organizations (58%) are looking for low-code automation solutions, where minimal coding skills are required
- 80% of organizations have a network source of truth, but only 20% say those solutions are very effective
- 85% of network automation tools require users to manually gather at least some data before they implement a change
- This manual data gathering often leads to ineffective automation tools with increased security vulnerabilities, and network errors that create downtime or performance trouble
- 98% of organizations have tools and processes in place to validate an automated change before committing it
- 99% of organizations have tools and processes in place to validate an automated change after committing it
- These pre- and post-change validations typically check for potential network performance impacts and security policy compliance
- The top benefits of network automation investments are operational efficiency and reduced security risk



Drivers of Network Automation

Technical Initiatives that Require Network Automation Investment

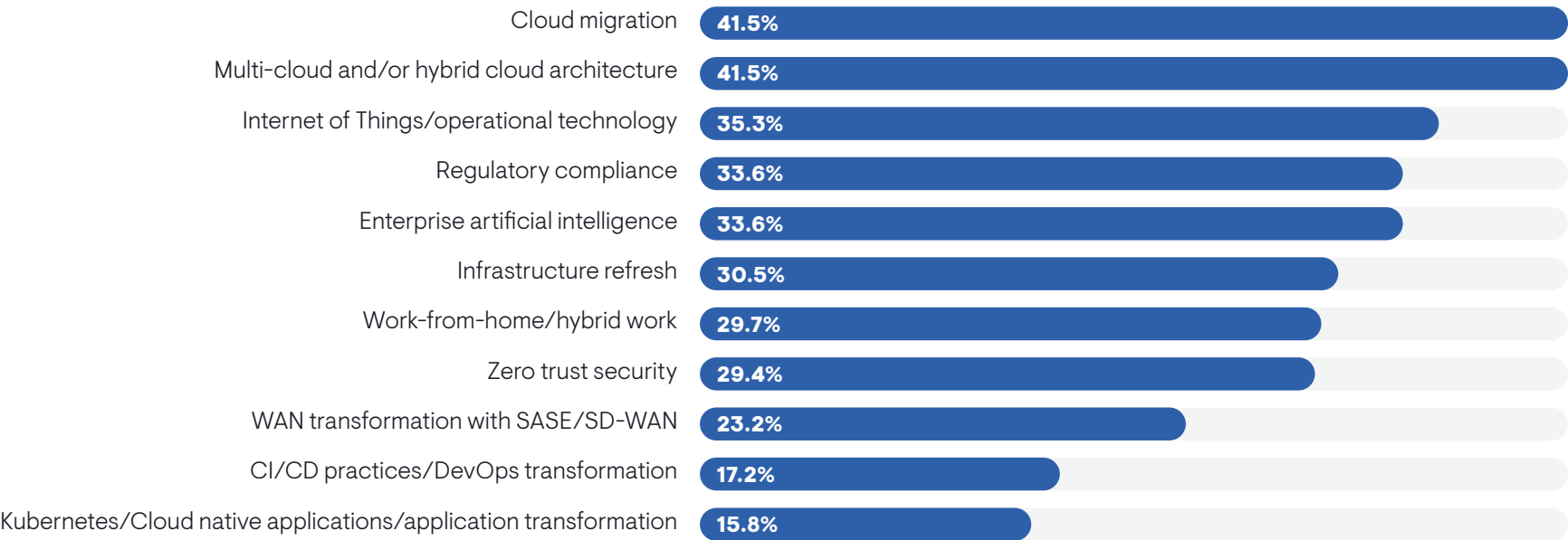
Figure 2 reveals initiatives and projects that motivate an IT organization to devote resources to network automation. The public cloud is a major factor, with cloud migration and hybrid multi-cloud architecture topping the list. Successful network automation strategies correlated more with hybrid multi-cloud, while less successful projects correlated with cloud migration. This suggests that automation delivers more value when organizations are trying to mitigate multi-cloud complexity.

Among secondary drivers, IoT and enterprise AI were more likely to affect mid-sized enterprises, while infrastructure refreshes were more likely to impact larger companies. Organizations that use proprietary tools from a network

infrastructure vendor were more likely to cite WAN transformation as a driver. This makes sense because many enterprises consider their software-defined WAN controller to be a network automation tool.

Kubernetes, CI/CD, and DevOps were insignificant drivers of network automation. EMA suspects that network teams are more focused on enabling automation of cloud networks. Any enablement of DevOps and Kubernetes is outside the scope of most projects. They may provide APIs and integrations with DevOps and Kubernetes platform teams to enable end-to-end orchestration, but they consider such projects above their pay grade.

FIGURE 2. WHICH OF THE FOLLOWING TECHNICAL INITIATIVES AND TRENDS ARE DRIVING YOUR ORGANIZATION’S NEED FOR NETWORK AUTOMATION TODAY?



Sample Size = 354

Preventing or Solving Problems with Network Automation

Aside from the technical initiatives that network automation can support, many organizations also invest in automation in response to technical or business issues connected to their networks. **Figure 3** reveals that organizations are typically trying to resolve network complexity and inefficient operations with network automation technology. Network operations and cloud teams were most likely to cite inefficient operations, and IT architecture and network operations teams were more likely to cite network complexity. Organizations that are trying to address inefficient operations are less likely to take a DIY approach to network automation. Instead, they use commercial tools.

“We as an organization are really good at processes and throwing people at problems,” said a network engineer at a Fortune 500 food and agriculture company. “If something comes up, we are good at finding bodies to throw at the problem instead of pausing and thinking about whether there is a way to do that process better or set it up for automation. Speed is not that important. It’s

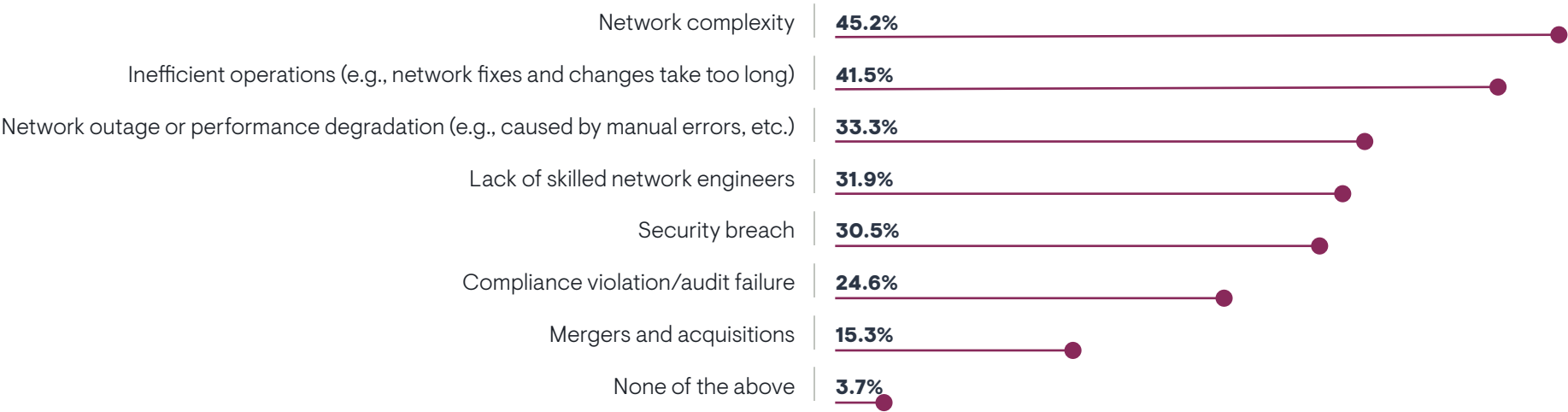
more about consistency and knowing whatever you set as a standard for the network is there and having a level of certainty that it’s being enforced.”

Secondarily, some organizations are responding to network outages or performance degradation, a lack of skilled network engineers, and security breaches. Engineering gaps and security breaches are more prevalent in midsize enterprises.

“The major goal is to not interact with devices directly,” said a network engineer at a midmarket business services company. “We want to eliminate human error as much as possible because most of the outages we have happen when we do changes. About 60% to 70% of our outages are bad changes.”

“We are automating to cut costs,” said a network automation engineer at a medical school and hospital network. “We’re also trying to stay up to date with what’s going on in the industry. Industry innovation requires automation.”

FIGURE 3. WHICH OF THE FOLLOWING BUSINESS ISSUES OR EVENTS PROMPTED YOUR ORGANIZATION TO DEVOTE RESOURCES TO NETWORK AUTOMATION?



Sample Size = 354

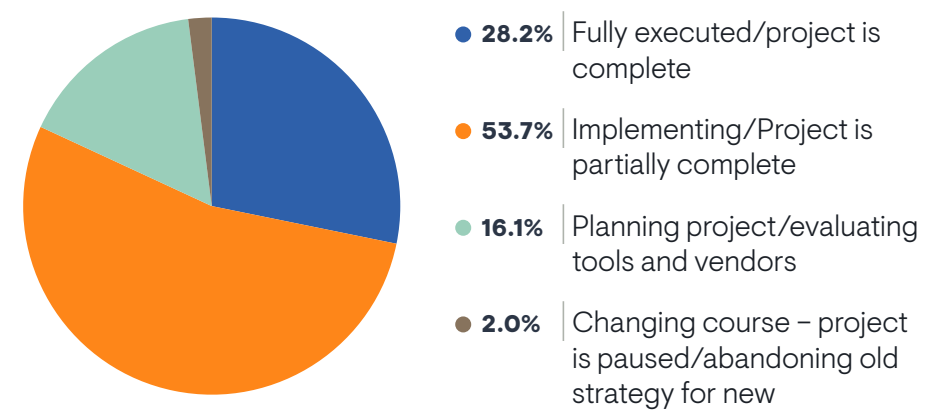


Snapshot of Network Automation Strategies

Project Status

Figure 4 reveals where survey respondents are in their network automation journeys. Only 28% believed that they had fully executed on their plans for automation. More than half had partially implemented their automation, but had father to go. The rest were still evaluating their options, with 2% admitting that previous unsuccessful automation efforts had forced them to start from scratch. EMA found that the largest enterprises in this survey (20,000 or more employees) were more advanced with their initiatives than smaller companies.

FIGURE 4. CURRENT STATE OF NETWORK AUTOMATION STRATEGY



“We’re in the early stages,” said a network engineer at a Fortune 500 food and agriculture company. “There is a budget to start a project with a system integrator to look at what automation means for all our infrastructure groups.”

Sample Size = 354

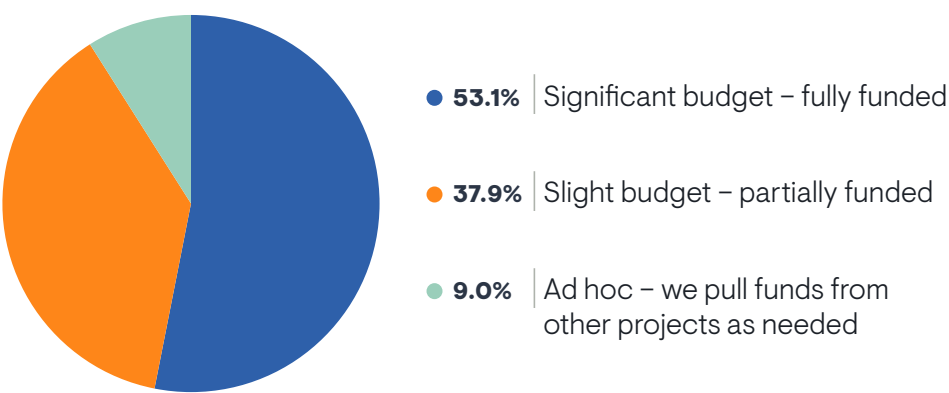
Budgeting for Automation Projects

Network automation strategies require budget allocations, whether those strategies focus on commercial solutions or DIY solutions. Commercial solutions involve subscription and product support fees. DIY homegrown and open source tools require the hiring of software developers to build, install, and support them.

“We have done some organizational changes where we have a network automation and reliability team,” said a tool architect at a Fortune 500 media company. “You need resources because a lot of it is development. You need people who understand enough about networking, then you need people who understand scripting. Depending on how advanced you want your automation, you may need developers.”

Figure 5 reveals that only 53% of EMA’s research participants believe that a budget fully funds their network automation strategies. Most others describe their projects as only partially funded, and 9% say they have no dedicated budgets at all.

FIGURE 5. TO WHAT EXTENT DOES YOUR ORGANIZATION ALLOCATE BUDGET SPECIFICALLY FOR NETWORK AUTOMATION TOOLS AND PROJECTS?



Sample Size = 354

“We allocate budget,” said a network tools engineer at a Fortune 500 retailer. “There is a huge team devoted to it and we’re increasing resources. We’ve requested a doubling of the automation budget for this year compared to last. That’s because we’re doing some changes globally with a network refresh and adopting zero trust. Deployment of that will require network automation.”

Network automation success correlates very strongly with significant budget allocations.

Unsurprisingly, network automation success correlates very strongly with significant budget allocations. While 80% of completely successful organizations reported a fully funded project, only 57% of partially successful organizations and 29% of partially failed organizations reported the same. Different silos of the IT organizations reported varying points of view on the issue. While security and cloud teams reported robust funding, network engineering, IT architecture, and IT tool engineering teams reported budget gaps. Also, EMA perceived a gap between IT executives and

middle managers (who generally believe projects are fully funded) and network administrators, engineers, and architects (who mostly believe these projects are only partially funded). Finally, among organizations that have DIY tools, those who write homegrown software tend to have more funding than those who adopt open source tools.

Budgets are Growing

EMA also found that 76% of organizations expect their network automation budgets to grow over the next two years, but only 21.2% described that growth as significant. Midsized enterprises (1,000 to 4,999 employees) expected more budget growth than larger companies. North Americans expected more budget increases than Europeans. Customers of proprietary network automation solutions expected more budget growth than customers of vendor-supported open source tools.

“We don’t have a specific budget for it,” said a network automation engineer at a large university. “We just have a networking budget. We’re in talks for our 2024 fiscal budget right now and trying to figure out what gets allocated to automation. But the funding that ultimately goes to automation is definitely increasing. Our team was growing. There were two of us, but now I’m managing five or six developers focused on network automation.”

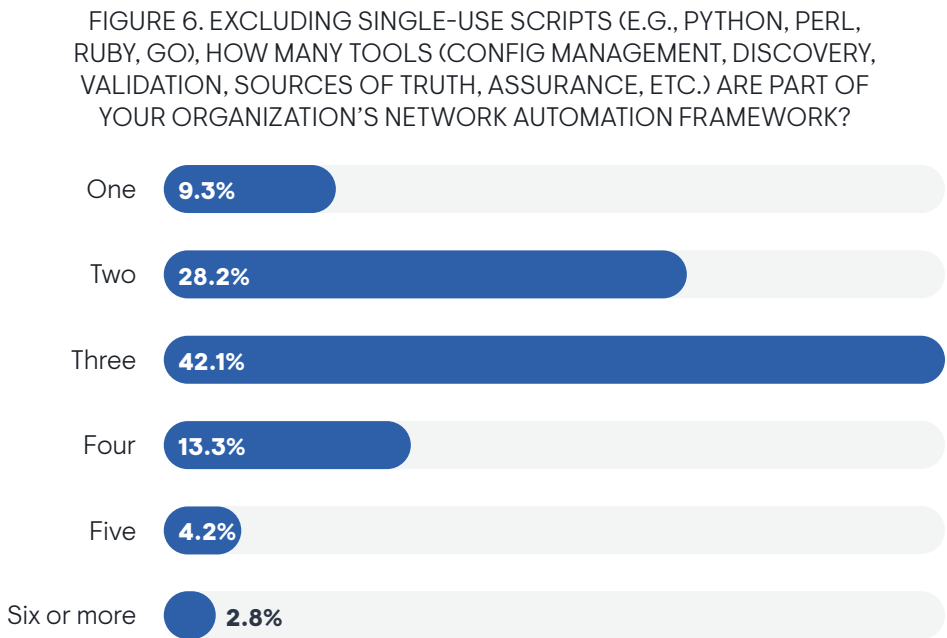
“We’re increasing our resources. I was brought in recently,” said a network automation engineer at a medical school and hospital network. “Before me, there was no one devoted to automation. It’s my sole purpose, and I assume the size of the team will increase in the future.”

“I think our resources are increasing as we see the benefits coming out of it,” said a network automation engineer at a \$3 billion SaaS provider. “As the organization sees positive outcomes coming out of the network automation team, they are more willing to grow the team.”

“We’re moving to the cloud, migrating from the data center, and that involves losing some control,” said a NOC analyst at a very large media company. “So the budget for network automation is way less than it used to be if we still had our own data center.”

Network Automation is a Multi-Tool Proposition

Figure 6 reveals that the typical IT organization has two or three network automation tools. Note that this number does not include the scores of single-use scripts that many network engineering teams use to automate individual tasks. EMA’s analysis found that organizations tend to be more successful with network automation when they use a larger toolset. Also, the larger a company is, the more tools it has.



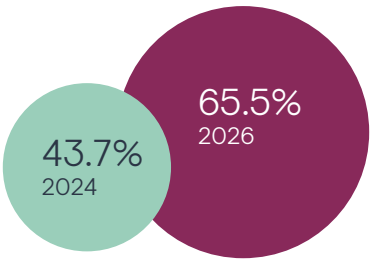
Sample Size = 354

EMA typically advocates that network teams consolidate their toolsets to unified, multifunction platforms. However, in the world of network automation, tool categories are emerging that solve very specific problems around network automation, such as task orchestration, configuration management, data management (e.g., network sources of truth), and network validation (network modeling and digital twins). Vendors that specialize in different areas are increasingly partnering to deliver comprehensive solutions. In fact, research participants who reported the most success with network automation told EMA that they were expecting to add more tools in the future, suggesting that they are identifying opportunities to add new tools to optimize their overall automation strategy.

Extent of Automation

Figure 7 reveals the mean response to a question that asked respondents to estimate the percentage of their organization’s overall network management tasks that are automated today versus where they expect to be in two years. It reveals that IT organizations expect to increase their overall level of network automation by nearly 50% by the end of 2025. Midmarket enterprises expected more progress than larger enterprises. Respondents who reported more success with network automation also reported higher rates of automation.

FIGURE 7. ESTIMATE TO WHAT EXTENT YOUR ORGANIZATION’S NETWORK MANAGEMENT TASKS ARE AUTOMATED TODAY AND TO WHAT EXTENT THEY WILL BE AUTOMATED BY THE BEGINNING OF 2026.



Sample Size = 354

This chart is best read as a measure of how much progress organizations expect to make with network automation over the next two years, rather than a true measure of how much automation they have implemented. EMA does not believe these percentages are particularly exact. When our analysts interviewed networking professionals one on one, we asked a similar question. Interviewees indicated that it was impossible for them to offer a good estimate because they don't have full visibility into the daily tasks of all their colleagues.

Furthermore, many survey respondents were executives or middle managers who have some distance from day-to-day operations. For instance, respondents with titles such as network administrator, network engineer, and network architect all reported a lower percentage of automation today (37%) and in the future (54%).

Where are They Automating?

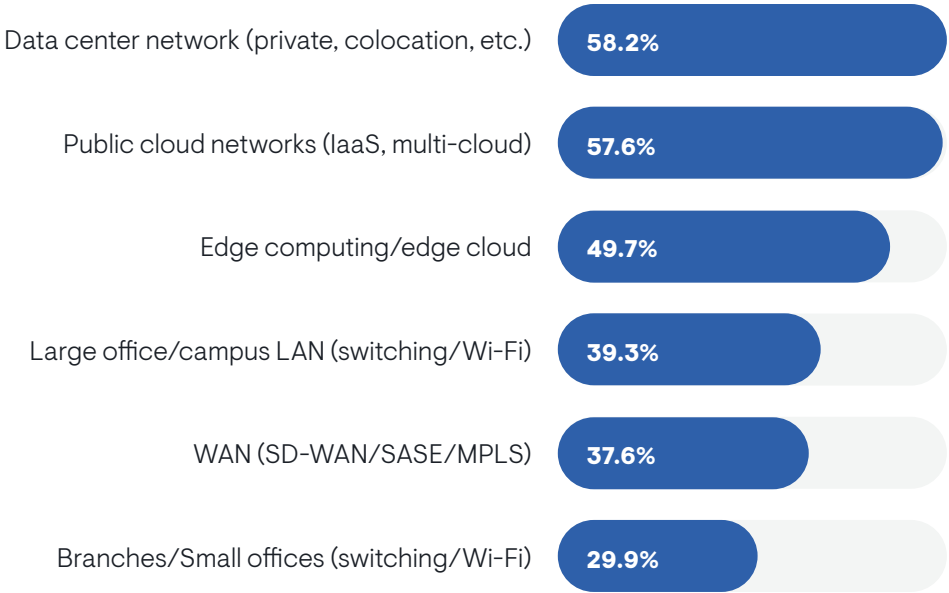
Most of the enterprises represented in this survey tended to focus their network automation strategies in data center networks and public cloud networks, as **Figure 8** reveals. Nearly half were also applying network automation to edge computing and cloud edge deployments. Organizations that focused on these three areas were more likely to be successful than unsuccessful with network automation in general.

"We are automating everything," said a network automation engineer at a Fortune 500 manufacturer. "There is nothing we won't automate."

The chart shows that large office LAN, branch office LAN, and WAN infrastructure were all secondary priorities for automation. Organizations that focus on automation of large office LANs were more likely to buy proprietary network automation software from a tool vendor and less likely to use a vendor-supported open source network automation tool.

"There are two things that are very important to automate," said a network engineer at private gaming company. "We are managing peering relationships, so insertions, deletions, and modifications of peering relationships with different internet exchanges. The other is our EVPN-VXLAN data center fabric, making it easier for server people to plug in servers and get new connectivity without delays or any EVPN weirdness. A third big focus for us over the last two years is deploying new remote points of presence."

FIGURE 8. WHICH DOMAINS OF YOUR ORGANIZATION'S NETWORK ARE THE FOCUS OF ITS NETWORK AUTOMATION STRATEGY?



Sample Size = 354, Valid Cases = 354, Total Mentions = 964

Self-Service Networking

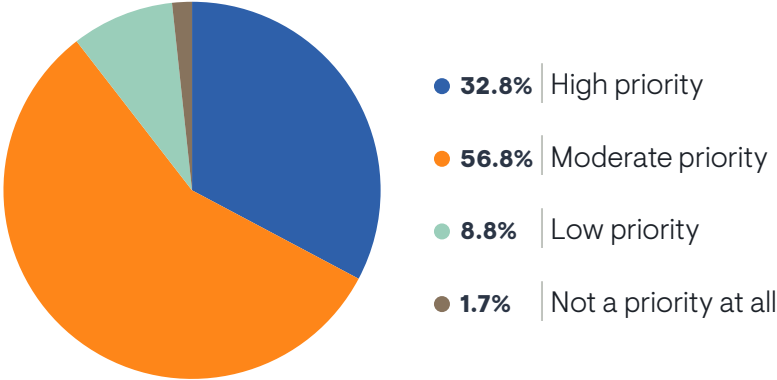
Figure 9 reveals that nearly 98% of organizations are interested in using network automation to enable self-service networking. Just 33% are making it a high priority. Success breeds aggression. Sixty-one percent of successful network automation strategies include a high priority for self-service networking, versus only 21% of failed projects.

Nearly 98% of organizations are interested in using network automation to enable self-service networking.

A network tools engineer at a Fortune 500 retailer said self-service would be helpful to his company because even with large-scale automation implemented, his network automation team still faces backlogs. “New requests for network automation capabilities take time. You have this huge platform, but you can’t let just anyone go in there and mess around. It would be nice to have some self-service in it for people who don’t want to wait three or four weeks for a new use case.”

Cloud and security teams are the most interested in enabling self-service. Network engineering teams are also enthusiastic. IT architecture, DevOps, IT tool engineering teams, and network operations teams are less engaged with it.

FIGURE 9. SELF-SERVICE NETWORKING IS THE CONCEPT OF ENABLING NON-NETWORKING PERSONNEL TO CONSUME NETWORK INFRASTRUCTURE SERVICES VIA ROLE-SPECIFIC UIS OR API CALLS TO NETWORK AUTOMATION TOOLS. TO WHAT EXTENT IS SELF-SERVICE NETWORKING A PRIORITY IN YOUR NETWORK?





Build Versus Buy Network Automation

One major area of discussion in the network automation world is the concept of build versus buy. Network teams often perceive this as a choice, where they either buy a network automation tool from a vendor or they craft a do-it-yourself (DIY) solution with developers writing homegrown software and/or using open source software. Anecdotally, EMA has often observed DIY network automation strategies that use open source software as foundational components for internally developed network automation software platforms.

Based on past research, EMA believes that build versus buy is a false choice. In reality, IT organizations usually do both. This research confirmed this hypothesis. We found that more than nine out of 10 organizations build AND buy network automation.

DIY Network Automation

Nearly 94% of respondents have some kind of DIY network automation tool.

Figure 10 reveals that nearly 94% of respondents have some kind of DIY network automation tool. Nearly 64% developed software in house, possibly leveraging open source components. Also, 57% are using open source software that has no associated vendor support.

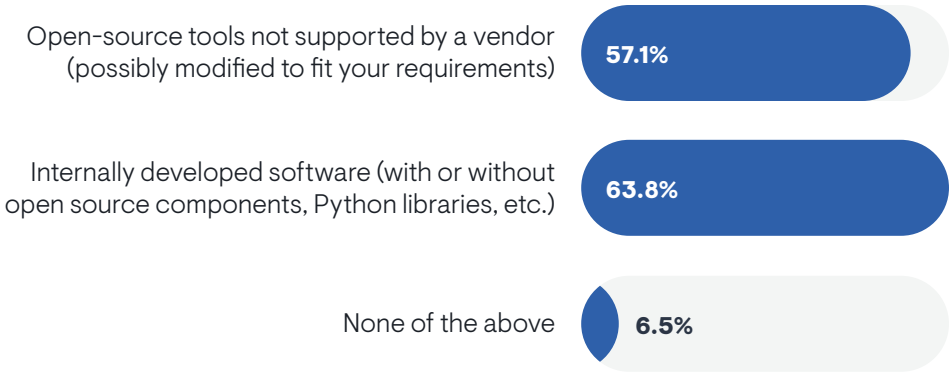
Cloud teams were more likely than IT tool engineering teams to report use of unsupported open source network automation. Open source was less common in very large enterprises (20,000 or more employees). Organizations that use unsupported open source tools were also more likely to use commercially supported open source. In other words, they use a mix of different open source tools, some of which have vendor support and some that don't. Meanwhile, organizations that use homegrown software are more likely to use proprietary network automation software, too. This suggests that organizations create homegrown software to close gaps in their proprietary solutions or vice versa.

“We started with some scripting,” said a tool architect at a Fortune 500 media company. “Now, we’re going into complex automation, and we’re building internal, homegrown tooling with a UI that users can work with.”

“We implement a lot of open source, like Ansible, Python, Go, Jenkins, Kibana, Elasticsearch,” said a network engineer at a midmarket business services company. “I wouldn’t call myself a software engineer. It’s more about scripting, but sometimes a bit more advanced. I try to integrate Ansible playbooks into our CI/CD process. Fifty percent of my time is spent writing those scripts.”

“We’re at the point where we build our own tools,” said a network automation engineer at a Fortune 500 manufacturer. “We rarely go off the shelf for anything. We even have multiple automation teams. Almost all of our in-house development uses open source.”

FIGURE 10. WHICH OF THE FOLLOWING TYPES OF DIY NETWORK AUTOMATION TOOLS DOES YOUR ORGANIZATION USE?



Sample Size = 354

Drivers of DIY Network Automation

Figure 11 explores why organizations adopt or build DIY network automation tools. First, many believe that a DIY project allows them to build tools with functionality and capabilities that are better aligned with their networks. Many also report that their security and compliance requirements require a DIY approach. Security and compliance were more prevalent among very large enterprises (20,000 or more employees). Secondly, one in three organizations see DIY as a way to save money. IT tool engineering and cloud teams were the most likely to cite cost savings.

“Some of the [commercial] tools we looked at buying are too damned expensive,” said a network engineer at a private gaming company. “The price is way more than the value when we compare it to writing the code ourselves. On other parts of our network there wasn’t anything that did what we wanted. So, we had to figure out how to glue things together.”

“I’m pro build-your-own because you get more flexibility,” said a network automation engineer at a \$3 billion SaaS provider. “You also get a lot of savings out of it, and you build your skills up by building your own product, rather than buying something and trying to make it fit your needs, which can often require more effort.”

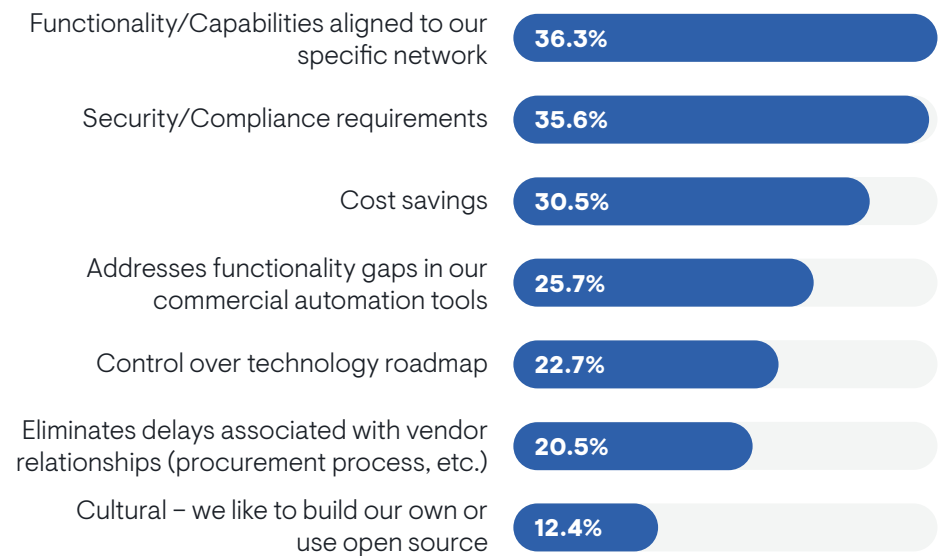
A network engineer at a midmarket business services company said cost savings isn’t what drives him to use DIY. It’s more about a lack of budget. “I request budget for network automation software, and I don’t get it. So, I use a lot of open source software.”

Control over technology roadmap is a minor driver, but networking personnel and IT project managers were more likely to cite it than IT middle managers. Cultural preferences for DIY were the biggest nonfactor, but network automation engineers and NetDevOps engineers named it a major driver. “We try to stay away from software vendors because we don’t want to get locked in,” said a network automation engineer at a large university. “Also, I don’t think a software vendor can come up with one orchestration tool that can fit everyone’s needs.”

“If you have enough people, going in the development direction makes sense because you can control everything,” said a tool architect at Fortune 500 media company. “But if you don’t have enough manpower, commercial tools make sense.”

“You can’t get all the features you want [from one vendor],” said a network automation engineer at a Fortune 500 manufacturer. “Usually, they do some subset of things. Vendors can’t do everything we need. Also, it’s about a level of customization. We can get exactly what we want when we need it.”

FIGURE 11. WHAT ARE THE PRIMARY REASONS WHY YOUR ORGANIZATION USES DIY TOOLS LIKE HOMEGROWN SOFTWARE OR UNSUPPORTED OPEN SOURCE TOOLS?



Sample Size = 354

Maintaining DIY Tools

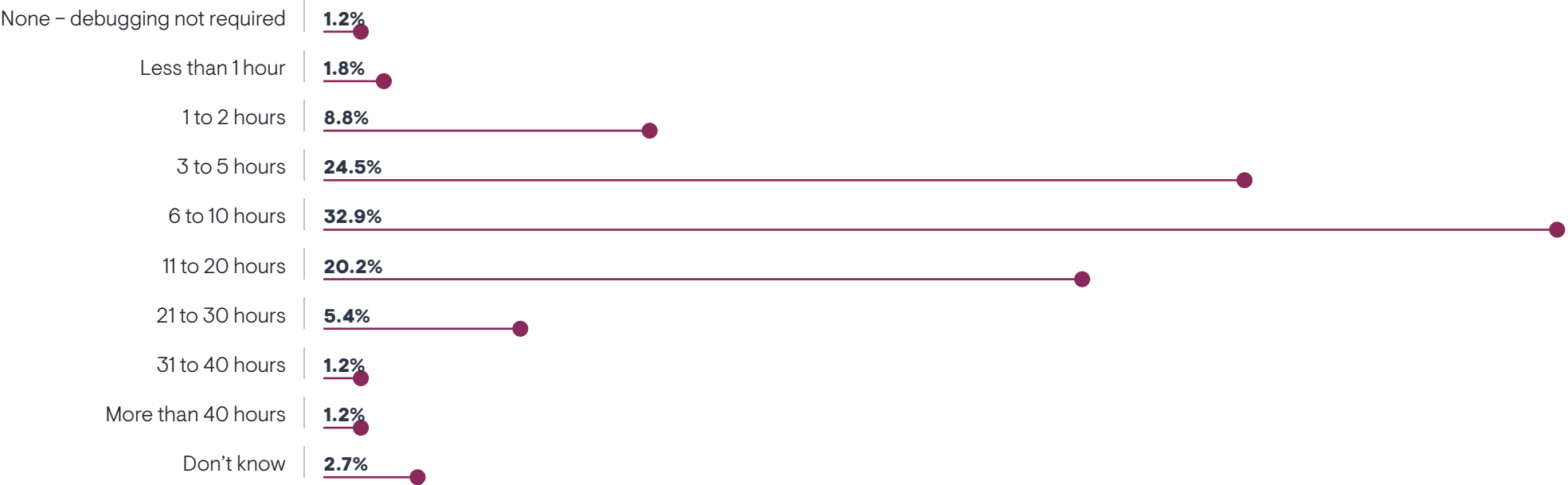
Obviously, DIY tools do not come with vendor support. If tools fail or bugs emerge, it's up to the internal network automation team to resolve them. **Figure 12** offers some insight into the support burden DIY tools present. The typical organization devotes anywhere from three to 20 hours a week supporting, maintaining, and debugging their DIY tools.

“In my last role, our philosophy was buy it, don’t build it, because as soon as you build it, you have to support it. It’s like having a kid,” said a network automation engineer at a Fortune 500 manufacturer. “My new company has an army of engineers, so we can build our own.”

The larger the company, the more hours they devote to it. For instance, 19% of very large enterprises (20,000 or more employees) spend more than 20 hours a week on DIY tool support, versus only 4% of midsize enterprises (1,000 to 4,999). EMA also found that failed network automation projects devote more time to coding support than successful ones. All organizations that rated their projects a complete failure devoted more than 20 hours a week to code support.

“In my last role, our philosophy was buy it, don’t build it, because as soon as you build it, you have to support it. It’s like having a kid,” said a network automation engineer at a Fortune 500 manufacturer.

FIGURE 12. HOW MUCH TIME PER WEEK DOES YOUR TEAM CURRENTLY SPEND SUPPORTING, MAINTAINING, AND DEBUGGING HOMEGROWN OR UNSUPPORTED OPEN SOURCE NETWORK AUTOMATION TOOLS?



Sample Size = 331

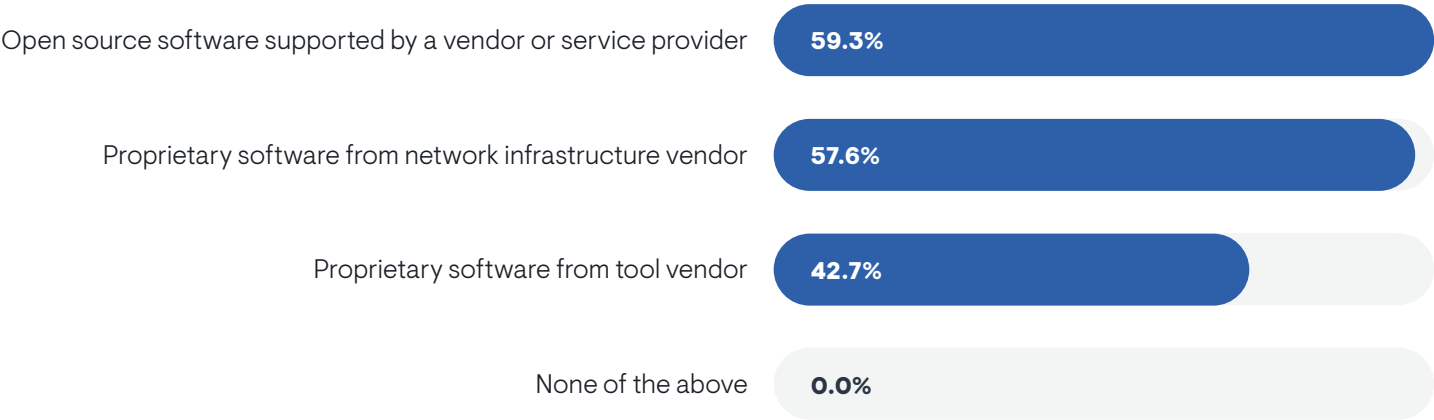
Commercial Network Automation

Figure 13 reveals that 100% of research respondents are using some kind of vendor-supported network automation solution. More than 59% use an open source tool that a vendor (or managed service provider) supports. Nearly the same number use a proprietary network automation tool offered by a network infrastructure vendor. This might include an element management tool from a switching vendor or a controller from an SD-WAN vendor. Nearly 43% use a proprietary solution from a network automation tool vendor. EMA also observed an affinity between proprietary solutions from tool vendors and

infrastructure vendors. If an organization was using one, they were likely to be using the other. Meanwhile, customers of vendor-supported open source solutions tended to avoid proprietary tools.

Respondents who use a proprietary solution from a tool vendor were more likely to report that their overall network automation strategy is successful rather than unsuccessful. EMA observed no statistically relevant relationship between success and failure and use of proprietary tools from an infrastructure vendor or vendor-supported open source tools.

FIGURE 13. WHICH OF THE FOLLOWING TYPES OF VENDOR-SUPPORTED NETWORK AUTOMATION TOOLS DOES YOUR ORGANIZATION USE?



Sample Size = 354

Drivers of Commercial Network Automation

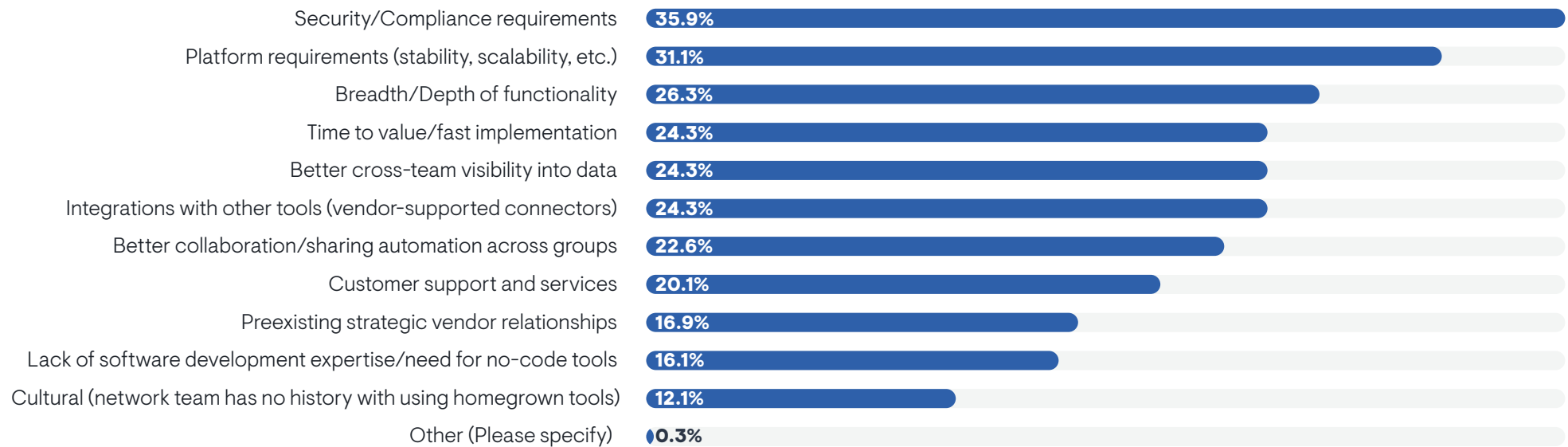
Figure 14 reveals why an organization might spend the money on commercial tools rather than stick with DIY tools. First, they have security and compliance requirements. Note, this is a top motivator for DIY, too. This suggests that network teams have complex network environments, where they trust commercial tools to fulfill certain requirements and they trust only DIY tools to fulfill others. The other driver is general platform requirements, where commercial tool vendors tend to outperform DIY tools, such as stability and scalability.

“There are some things you can’t really build on your own, especially if it touches multiple groups and systems,” said a network automation engineer at \$3 billion SaaS provider. “IPAM solutions, for instance. We did a lot of research comparing and looking at what was available on the market. It’s a company-wide tool that touches multiple teams and needs to be very customizable.”

Successful organizations found platform requirements less compelling. Instead, they were more likely to select secondary drivers like breadth and depth of functionality and cultural preferences. Networking personnel were more likely to cite cultural preferences than IT middle managers. Breadth and depth of functionality is also a bigger driver for larger enterprises (20,000 or more employees).

Organizations that use proprietary network automation tools from a third-party tool vendor were more likely to cite better collaboration and sharing of automation across groups as a driver, while users of commercially supported open source tools were less likely.

FIGURE 14. WHICH OF THE FOLLOWING ARE THE MOST COMPELLING REASONS TO ADOPT COMMERCIAL NETWORK AUTOMATION SOLUTIONS, AS OPPOSED TO DIY NETWORK AUTOMATION?



Sample Size = 354

Customer support and services was a tertiary motivator, but a network engineer at a Fortune 500 food and agriculture company identified it as a primary reason why his company might buy tools. “It would be the commercial support. That’s the biggest thing that comes up in discussion. The members of my team aren’t developers and don’t want to be developers. When something goes wrong, they want someone they can turn to, rather than build and maintain it themselves. We’ve done a lot of proofs of concept with homegrown automation and people often say, ‘We’re not going to be able to use this when you leave.’”

“We have a hybrid strategy,” said a tool architect at a Fortune 500 media company. “We can buy some commercial tools where it makes sense. But we are also developing tools internally where we can’t get the capabilities we need from vendors.”

Weighing Vendor Solutions Against DIY Solutions

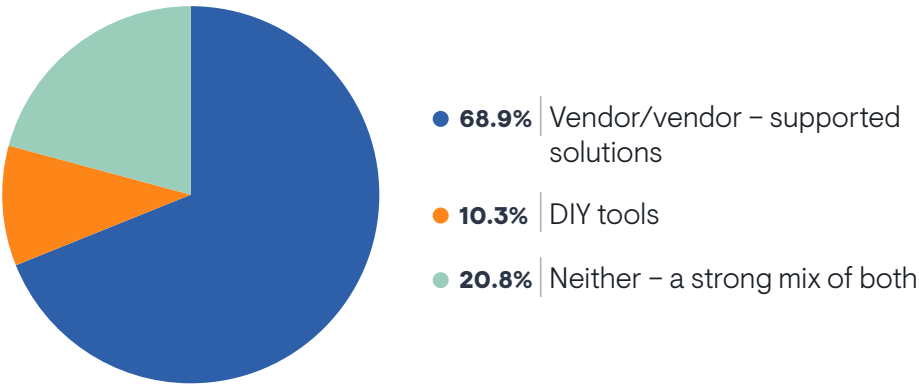
Of the 331 respondents who use both commercial and DIY network automation, 69% reported that commercial solutions, like proprietary tools and vendor-supported open source, dominate their overall network automation toolset, as **Figure 15** details. Only 10% are primarily a DIY shop. Another 21% said they use a roughly equal balance of both classes of tools.

“We have a hybrid strategy,” said a tool architect at a Fortune 500 media company. “We can buy some commercial tools where it makes sense. But we are also developing tools internally where we can’t get the capabilities we need from vendors. Commercial tools can meet about 80% of our needs.”

“We are trying to figure out if we’re going to use open source tools or buy a platform,” a said network engineer at a Fortune 500 food and agriculture company. “I think the outcome will be to do open source. If you buy something, then you’re accountable for the success of that investment. If it doesn’t work, you’re going to be blamed for the bad investment.”

Members of network engineering and security teams were the most likely to report a commercial-centric approach to network automation. DevOps teams were split between commercial and DIY, but rarely reported a balance of using both. IT tool engineering teams were more likely than others to embrace a balance of both.

FIGURE 15. YOU INDICATED THAT YOU USE BOTH COMMERCIAL OR COMMERCIALLY SUPPORTED NETWORK AUTOMATION AND DIY NETWORK AUTOMATION. WHICH CLASS OF SOLUTION IS MORE PREVALENT IN YOUR OVERALL NETWORK AUTOMATION STRATEGY?



Sample Size = 331



Network Automation Solution Requirements

General Feature Requirements

Figure 16 reveals which network automation tool features are most important to organizations. Security policy management topped the list. The CIO’s suite, network operations, security, and cloud teams all rated it high, but network engineering teams made it a low priority. Larger enterprises (20,000 or more employees) were more likely than midsize enterprises (1,000 to 4,999) to select it.

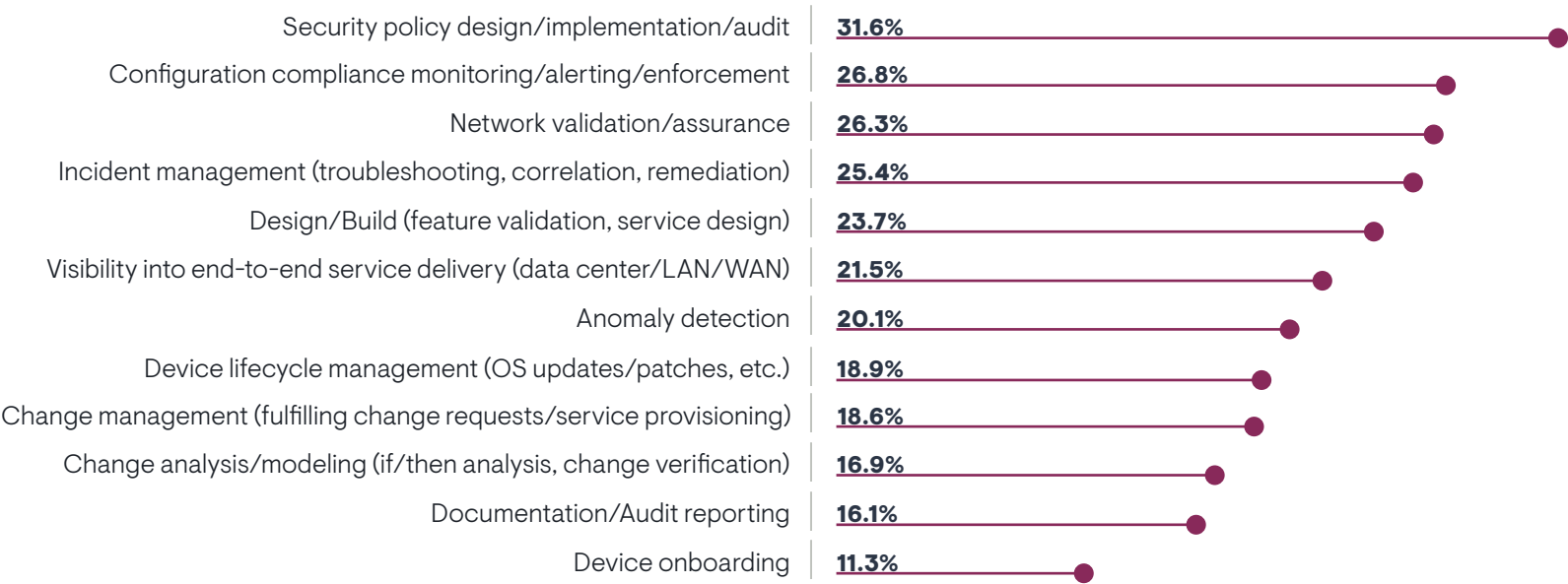
“One of the complex use cases we’re looking at is firewall automation and updating firewall policies or adding rules,” said a tool architect at a Fortune 500 media company. “These are very frequent requests, but it’s very difficult. We get hundreds of tickets a month on firewalls. Our firewall vendors all have their own configuration management tools that are supposed to push those changes out, but when you’re as big as us, you have multiple firewall vendors. We need to automate across them.”

Secondarily, configuration compliance, network validation and assurance, incident management, and design/build features were very important. Configuration compliance was especially important to organizations that use proprietary network automation tools that a network infrastructure vendor supplied.

“We try to automate any kind of new network deployments. We have a bunch of security projects we are deploying to new locations. Being able to do that fast is important,” said a network tools engineer at a Fortune 500 retailer.

Change analysis/modeling, documentation and auditing, and device onboarding were low priorities. Device onboarding was a high priority for midsize enterprises.

FIGURE 16. WHICH OF THE FOLLOWING NETWORK AUTOMATION FEATURES ARE MOST IMPORTANT TO YOUR ORGANIZATION?



Sample Size = 354

General Platform Requirements

Figure 17 reveals the general platform requirements that enterprises set for their network automation tools. The chart clearly shows that four characteristics are priorities. First, organizations are looking for tools that are stable and resilient. Next, they want tools that are easy to deploy and administer. Finally, these tools must have strong data management capabilities and platform scalability.

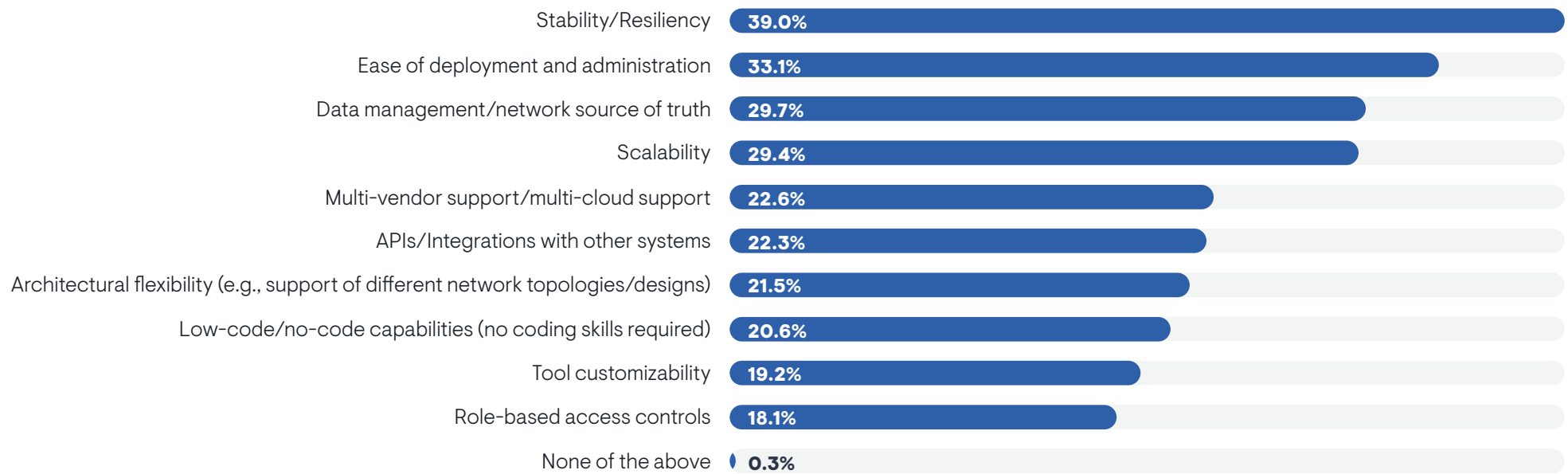
Successful organizations were less likely to select stability and resiliency. DevOps and network engineering teams also made stability and resiliency a

low priority, but security and IT tool engineering teams made it a high priority. Scalability was more important to organizations that avoid DIY tools.

Role-bases access control (RBAC) was the lowest priority, but networking staff (administrators, engineers, and architects) were more likely to select it than IT middle management.

Tool customizability was another low priority, but users of vendor-supported open source tools were more likely to demand this than customers of proprietary tools.

FIGURE 17. WHICH OF THE FOLLOWING PLATFORM CHARACTERISTICS OF A NETWORK AUTOMATION TOOL ARE MOST CRITICAL TO YOUR ORGANIZATION?



No-Code, Low-Code, High-Code?

Network engineers rarely describe themselves as software developers, but they tend to have some coding skills, given that so many of them have spent years leaning on scripts to implement ad hoc network automation. Unfortunately, many IT organizations struggle to hire expert network engineers with such skills.

“We want to enable self-service capabilities for normal network engineers who don’t have a lot of scripting skills. They work in the UI,” said a tool architect at a Fortune 500 media company.

Thus, network automation teams must think about the scripting and coding abilities of automation users when implementing solutions. Many network automation tools, both DIY and commercial, often require some coding skills of their users. **Figure 18** reveals how organizations are navigating this issue. Only

6% are aiming for “no-code” tools. More than 35% target “high-code” tools, where users must have strong coding skills. Most follow a middle path, a “low-code” tool, where users need some coding skills but are not expected to be experts.

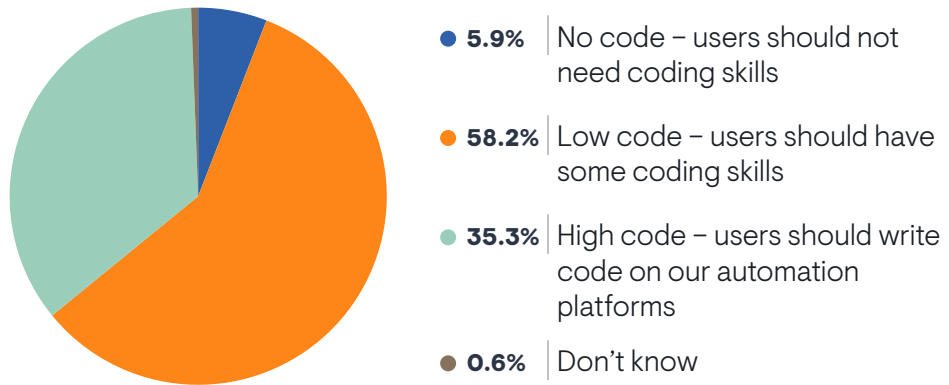
Network operations teams preferred low-code tools while network engineering and security teams preferred high-code tools. Smaller companies targeted low-code and larger companies targeted high-code. NetDevOps engineers and network automation engineers, who tend to be coding ninjas, were more likely to report a high-code strategy.

Network operations teams preferred low-code tools while network engineering and security teams preferred high-code tools.

“I’m building a low-code environment for our network engineers to get started with automation,” said a network automation engineer at a medical school and hospital network. “Presently, I’m doing automation by using Python scripting and open source Ansible, but we’re going to adopt a platform.”

“We have a team with different levels of understanding of networking,” said a network engineer at a Fortune 500 food and agriculture company. “Some want to work within a system, but others want to go deep and do custom automation. We want to be able to work within a platform at different levels because there are some guys who are low-code/no-code, but sometimes, we have people who want to do the code.”

FIGURE 18. WHAT ARE YOUR ORGANIZATION’S GOALS IN TERMS OF THE MINIMUM AMOUNT OF CODING SKILLS NETWORKING PERSONNEL NEED TO HAVE WHEN USING YOUR ORGANIZATION’S NETWORK AUTOMATION TOOLS?

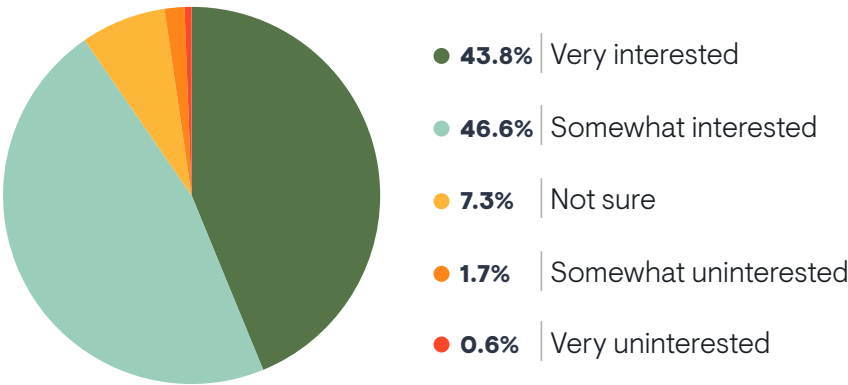


Sample Size = 354

Intelligent Automation with AI and Machine Learning

Artificial intelligence and machine learning (AI/ML) are everywhere today. Most IT vendors are building and training AI/ML algorithms to make their solutions more effective and useful. Network automation is no exception. **Figure 19** reveals that 98% of organizations have at least some interest in adopting network automation products that leverage AI/ML technology. Organizations that are the most successful with network automation are the most interested in AI/ML.

FIGURE 19. ARE YOU INTERESTED IN INCORPORATING SOLUTIONS THAT LEVERAGE AI/ML TECHNOLOGY INTO YOUR NETWORK AUTOMATION STRATEGY?



IT executives, IT middle managers, and networking professionals (administrators, engineers, architects) are the most likely to covet AI/ML features. IT project managers, NetDevOps engineers, and network automation engineers are the least interested. From an IT silo perspective, the CIO’s suite, cloud engineering/operations, and security are the most interested in AI/ML. DevOps and network engineering are least interested. Midsized enterprises (1,000 to 4,999 employees) were more interested than very large enterprises (20,000 or more).

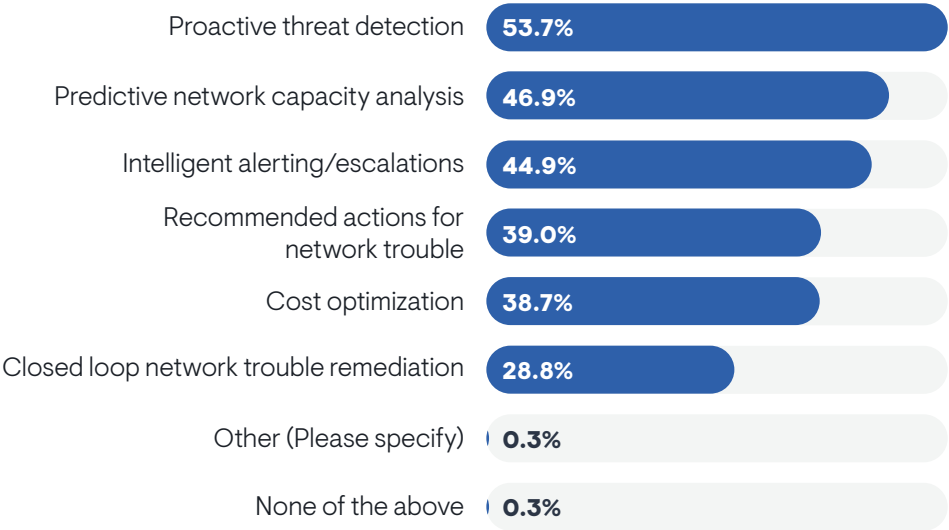
Sample Size = 354

Using AI/ML-Driven Network Automation

Figure 20 reveals how organizations want to use AI/ML capabilities in their network automation tools. The biggest focus is on security with proactive threat detection. Organizations want network automation tools that are capable of recognizing threats on the network and adjusting accordingly. Many are also interested in predictive capacity analysis and intelligent alerting and escalations. Predictive capacity analysis is especially interesting to very large enterprises (20,000 or more employees).

Recommended actions for network trouble, cost optimization, and closed loop network trouble remediation are lower priorities. Cloud and network operations teams were more interested in cost optimization.

FIGURE 20. WHICH OUTCOMES FOR AI/ML-DRIVEN NETWORK AUTOMATION ARE YOU MOST INTERESTED IN ADOPTING?



Continuous Network Compliance Monitoring

Network compliance is a key component of a network automation strategy. Network change is constant, and network automation only accelerates the rate of change. Network teams need ways to ensure that network standards are complied with, whether those are configuration and design standards or security standards. **Figure 21** reveals how many organizations are actually monitoring network compliance. Well over half are doing it today, and nearly 40% have plans to adopt this in the future. Successful organizations are more likely to do

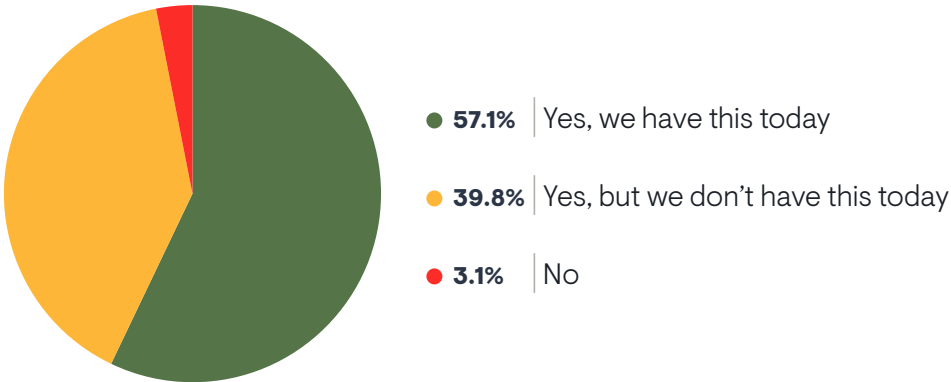
this today. Organizations that use proprietary network automation tools from a network tool vendor or homegrown, internally-developed software are the most likely to do this today. Organizations with an effective network source of truth are also more likely to continuously monitor network compliance. Fully funded network automation budgets also correlate with using this today.

“We are constantly doing validations between intended state and running state to make sure they are in sync. If it goes off, we generate a config drift alert to address it,” said a network automation engineer at a \$3 billion SaaS provider.

“We are constantly doing validations between intended state and running state to make sure they are in sync. If it goes off, we generate a config drift alert to address it,” said a network automation engineer at a \$3 billion SaaS provider.

Network automation strategies that are launched in response to a security incident are more likely to be doing continuous network compliance monitoring today. Network engineering and cloud teams perceive continuous monitoring more often than the CIO’s suite, IT tool engineering, and IT architecture groups.

FIGURE 21. ARE YOU CONSIDERING A TOOL THAT CAN CONTINUOUSLY ASSESS NETWORK COMPLIANCE (E.G., CONFIG COMPLIANCE, SECURITY POLICY COMPLIANCE, ETC.)?

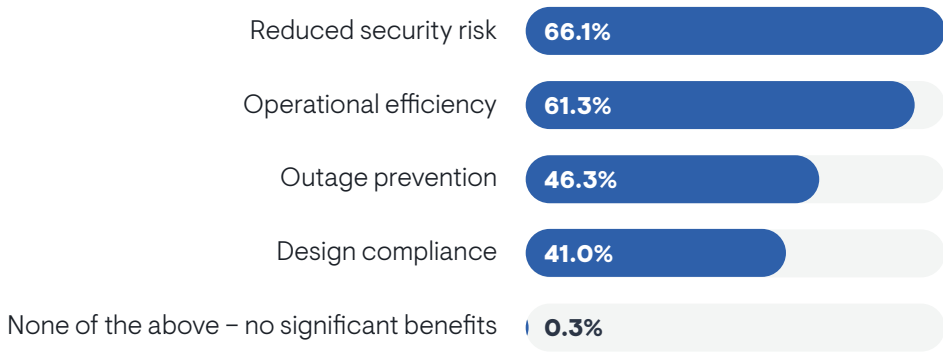


Benefits of Continuous Compliance Monitoring

Figure 22 reveals the top benefits of continuously monitoring network compliance. Respondents chose reduced security risk and operational efficiency as the big wins. But many are also seeing value in the form of outage prevention and design compliance. Organizations that are the most successful with network automation especially valued outage prevention.

Security risk reduction is more common among organizations that use proprietary network automation tools supplied by network infrastructure vendors and less by those that use vendor-supported open source network automation.

FIGURE 22. WHAT ARE THE MOST IMPORTANT BENEFITS OF CONTINUOUS NETWORK COMPLIANCE VALIDATION?



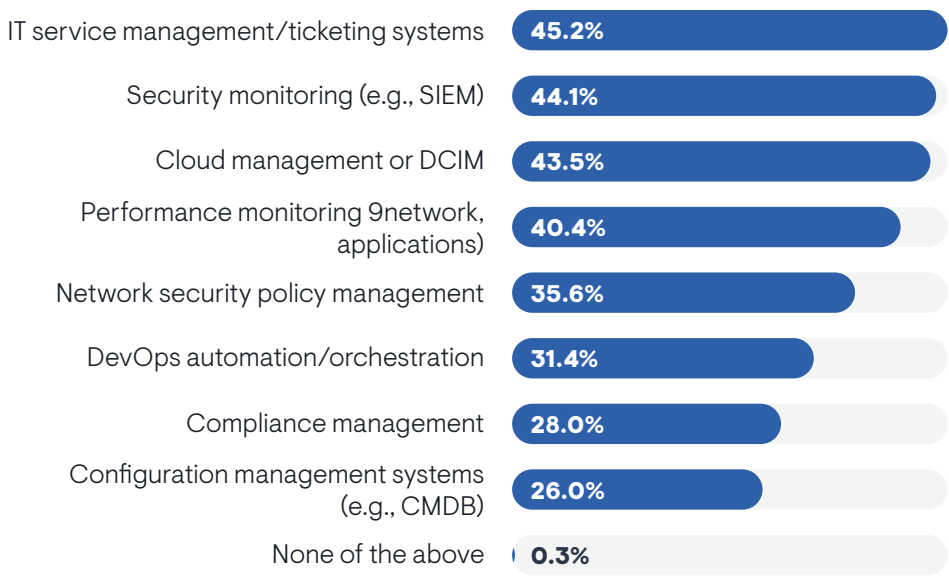
Integration Requirements

Like many IT management systems, network automation tools are part of an ecosystem of solutions. IT organizations integrate them with other systems for the exchange of data, to trigger changes, and other reasons. **Figure 23** reveals the top integration requirements that organizations set for their network automation tools.

Organizations are prioritizing three integrations: IT service management, security monitoring, and cloud or data center infrastructure management (DCIM). Many are also integrating with performance management and security policy management systems. Performance management integration was especially important to organizations that avoid DIY automation for 100% vendor-supported solutions.

Configuration management database (CMDB) is the lowest integration priority. In fact, organizations that reported the most success with network automation were the least likely to integrate with CMDBs. This finding suggests that most network teams are building network automation toolsets that have native configuration management systems, such as a network source of truth, rather than integrating with a third-party CMDB.

FIGURE 23. WHICH SYSTEMS, IF ANY, DOES YOUR ORGANIZATION WANT TO INTEGRATE WITH ITS NETWORK AUTOMATION TOOLS?





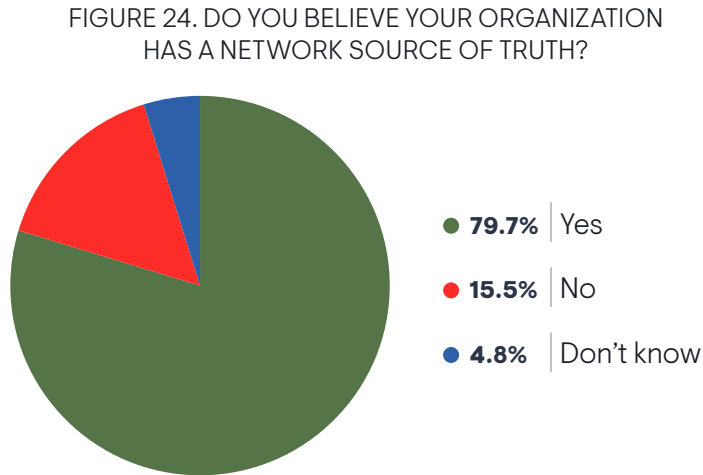
Spotlight on Network Source of Truth

This section explores an essential component of network automation toolsets. A network source of truth is a repository of critical data about a network. A network source of truth ensures that all network management tools (including network automation tools) have the same information about the intended state of a network and the actual state of a network. When an IT professional uses a network automation tool, they gather data from a source of truth to ensure that a network change will comply with design standards, configuration standards, security policies, IP address space, and much more. It will supply inventory data so that users know which devices they need to reconfigure, where they are, and whether the current software versions on those devices can accept a proposed change. In other words, a network source of truth should provide all the data and information a user could possibly need to make automated changes without breaking the network.

“I would say the source of truth is the production network,” said a network automation engineer at a Fortune 500 manufacturer. “But I think you need to be able to model intent and then match it to state.”

“I would say the source of truth is the production network,” said a network automation engineer at a Fortune 500 manufacturer. “But I think you need to be able to model intent and then match it to state. You have to have a very well-engineered solution to be able to say that [our intent repository] is correct 100% of the time. If you can just make your network super, super discoverable, then it’s almost self-documenting.”

Figure 24 reveals that nearly 80% of research participants believed that they have a network source of truth today. Network automation success correlates with having a source of truth. Network engineering, DevOps, and cloud teams were more likely to perceive a source of truth than the CIO suite and IT architecture and IT tool engineering teams. North Americans were much more likely to have one than Europeans.



“That’s been a source of debate for a while,” said a network automation engineer at a large university. “Our network architect wants a source of truth, but what is a source of truth? In our minds, it’s what is currently on the devices. If the network is set up the way it should be, the source of truth should be the network itself. We’re still working on the best way to rectify this problem.”

Users of proprietary network automation software from a tool vendor were more likely to have a source of truth today. However, users of DIY tools, including unsupported open source and homegrown tools, also reported high rates of source of truth adoption.

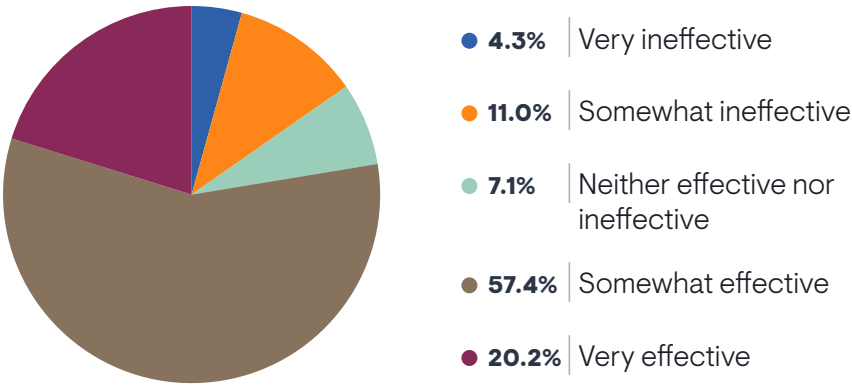
Effectiveness of Sources of Truth

Organizations that had an effective source of truth reported more success with their network automation strategies.

Among the 282 research participants who believed that they had a network source of truth, only 20% described this source of truth as very effective, as seen in **Figure 25**. Most respondents felt these repositories were only somewhat effective, suggesting that they saw room for improvement. More than 15% describe their solutions as somewhat or very ineffective. Organizations that have fully implemented their network automation strategy were more likely to believe their source of truth was effective. Users of proprietary network automation software from a tool vendor also tended to report effective sources of truth.

Unsurprisingly, organizations that had an effective source of truth reported more success with their network automation strategies.

FIGURE 25. HOW EFFECTIVE IS YOUR ORGANIZATION'S NETWORK SOURCE OF TRUTH?



Sample Size = 282

“We’re not 100% satisfied,” said a network automation engineer at a \$3 billion SaaS provider. “It was a quick and dirty solution to get something out the door. We’re planning to revise it. It takes too long to pull data from it, especially in our larger sites.”

“I’m pretty satisfied with it,” said a network tools engineer at a Fortune 500 retailer who uses multiple vendor-supported open source tools for his source of truth. “We considered ServiceNow, but it wasn’t maintained by the network team. It’s maintained by different groups that are not focused on data governance of the network. We lacked full control of it.”

“There is no perfect tool for a source of truth,” said a network automation engineer at a medical school and hospital network. “There is always something we’d like added to it. But it’s okay. I’d like easier reporting from it. It’s not a click and run tool. You have to know how to run queries and how to use Python.”

Security teams were the most enthusiastic about the quality of a network source of truth. Cloud teams were also quite bullish. The CIO’s suite and the IT architecture and network engineering teams were moderately enthusiastic. DevOps and IT tool engineering teams were pessimistic.

Organizations with a good source of truth reported that a higher percentage of network management tasks were automated. They also reported that they were more consistent with running pre-change and post-change validation when using network automation tools. These validations also tended to focus on configuration and design compliance. Organizations with an ineffective source of truth tended to report that their network automation tools suffered from slower returns on investment or time to value.

“We’re not happy with our source of truth right now,” said a network engineer at private gaming company. “There are various pieces to it. Historically, we did not always have a source of truth. Some of it is discoverable, but people do not always keep things up to date and it’s difficult to do that discovery. It’s an issue that goes across tooling, people, and processes.”

EMA observed the following tendencies among organizations with an effective source of truth:

- Fully funded network automation budgets
- Reported that it is easier to understand the difference between network intent and network state
- Gathering data before making an automated network change is more automated
- Automation tools focus on large office LANs and data center networks
- Strong multi-vendor support
- Automation toolset integrations with
 - IT service management
 - Security monitoring
 - DevOps automation/orchestration
- Strong automation tool support for
 - Maintaining intent repositories
 - Discovery and reporting on network state
 - Discovering and reporting on differences between network intent and network state
- Sources of truth contain security policies

Organizations that have an effective source of truth emphasized the importance of a data reconciliation feature.

Critical Features of a Source of Truth

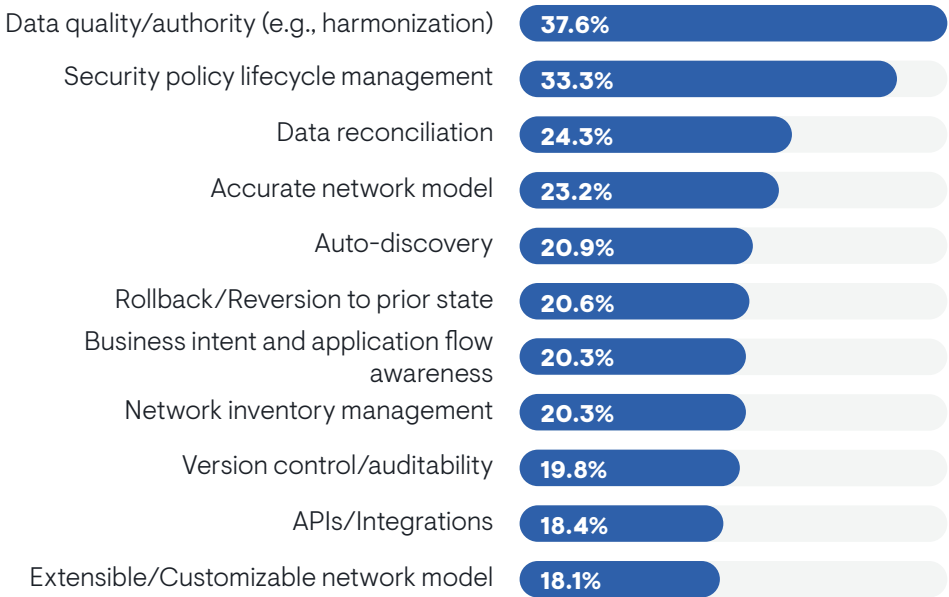
Figure 26 identifies what IT organizations are looking for in a network source of truth. The two primary requirements are data quality and security policy lifecycle management. Secondly, organizations want data reconciliation and an accurate data model.

Organizations that have an effective source of truth emphasized the importance of a data reconciliation feature.

“A network source of truth can be expanded [beyond device management] to alerting concepts,” said a tools architect with a Fortune 500 media company. “You can expand it to configuration alerts, performance alerts, fault alerts. So, we have an event management tool that provides that source of truth.”

Among tertiary priorities, version control was a higher priority to larger companies. Version control was also important to organizations that concentrate on vendor solutions rather than DIY network automation. Organizations with ineffective solutions singled out business intent and application flow awareness as important features. Cloud and security teams emphasized the importance of APIs and integrations.

FIGURE 26. WHAT ARE THE MOST IMPORTANT FEATURES TO HAVE IN A NETWORK SOURCE OF TRUTH?



Sample Size = 354

Achieving a Source of Truth

EMA asked all respondents, regardless of whether they reported having a source of truth, to tell us where they store all the information that might be found in one. **Figure 27** reveals that it's rare for an organization to have a single platform that holds all this data. Instead, most of them have federated multiple systems of record, either through direct integration or integration into a central platform. In other words, they have multiple sources of truth, but those systems are sharing and reconciling data to maintain an authoritative view of the network. Network automation engineers and NetDevOps engineers were more likely to perceive this federated source of truth. Among IT groups, this approach was also reported more often by network engineering, DevOps, and cloud teams.

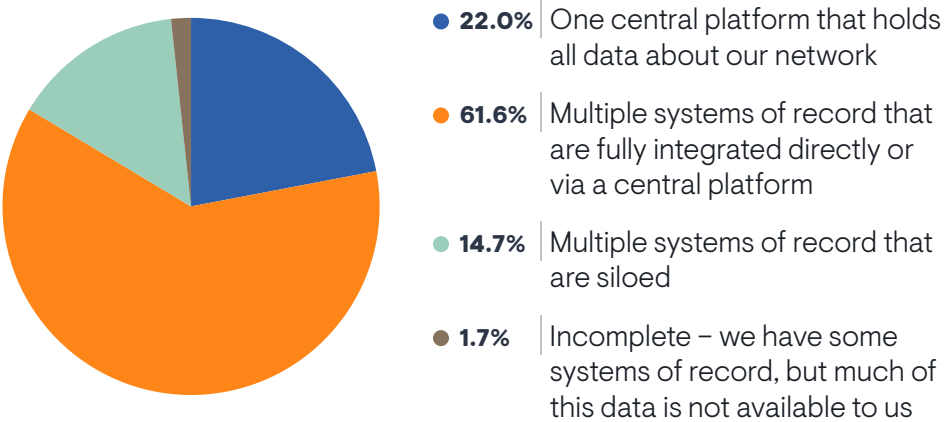
“No matter how hard you try, you’re not going to have one tool that has all this information,” said a tool architect at a Fortune 500 media company. “You have to get good at aggregating and integrating things from multiple places.”

“No matter how hard you try, you’re not going to have one tool that has all this information,” said a tool architect at a Fortune 500 media company. “You have to get good at aggregating and integrating things from multiple places. For automating devices, we have to pull data from ten different places. We don’t stop at devices. We have a source of truth for sites, so we have a data feed from our SD-WAN solution.”

Organizations that have one centralized platform reported that their sources of truth were more effective. Organizations that relied on multiple, siloed systems of record reported a poor source of truth. Europeans were also more likely to have siloed systems. Organizations that write their own network automation software were also more likely to report using a federated source of truth.

Organizations with siloed systems of record told EMA that their network automation toolsets had weak support for network intent repositories and reporting on configuration drift. Organizations that used one central platform had strong support for reporting configuration drift and provisioning and deploying network changes. Teams that used a federated source of truth reported strong support of intent repositories.

FIGURE 27. HOW WOULD YOU DESCRIBE YOUR ORGANIZATION’S CURRENT APPROACH TO COLLECTING, STORING, AND MAINTAINING ALL THE INFORMATION THAT MIGHT BE CONTAINED IN A NETWORK SOURCE OF TRUTH?

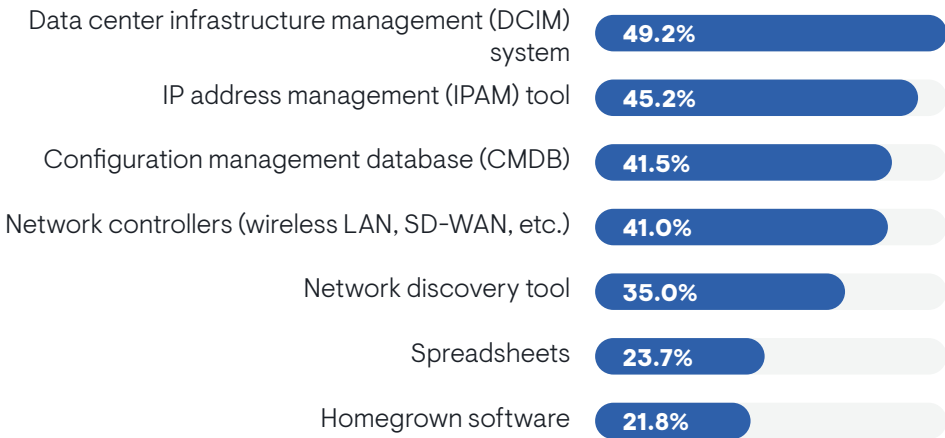


Sample Size = 354

Where Do You Find the Truth?

Given that so many organizations maintain a federated network source of truth, it’s important to understand which systems of record might be involved. **Figure 28** reveals which repositories respondents have that contain data that is important to a source of truth. It reveals that data center infrastructure management (DCIM) tops the list. DCIM tools typically maintain device inventory data. Some also maintain IP address space information and configuration data.

FIGURE 28. WHICH OF THE FOLLOWING TOOLS AND SOLUTIONS DOES YOUR ORGANIZATION CURRENTLY USE TO COLLECT AND STORE DATA THAT WOULD BE CONTAINED IN A NETWORK SOURCE OF TRUTH?



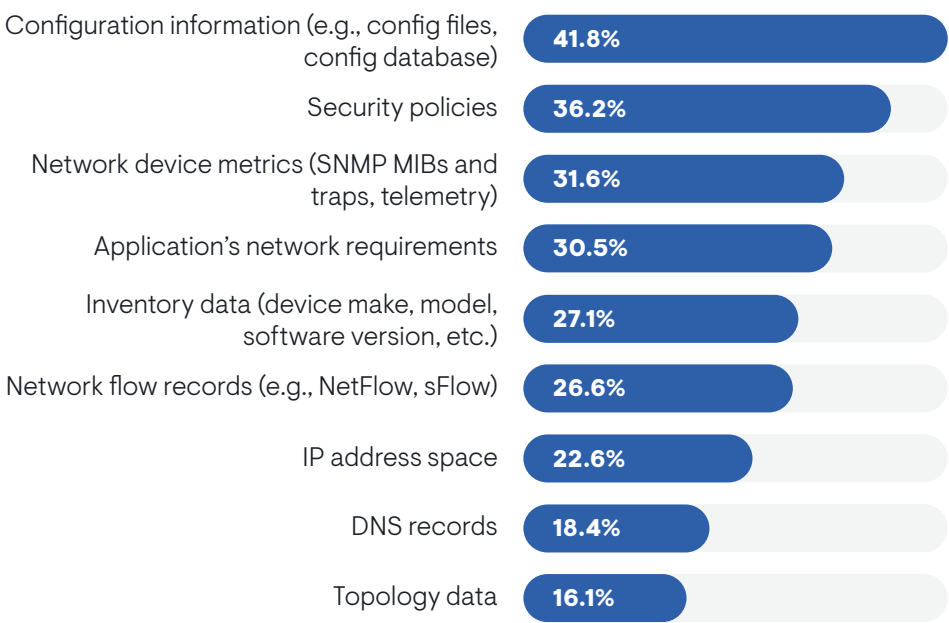
Secondarily, IP address management (IPAM), configuration management databases (CMDB), and network controllers (like wireless LAN controllers or SD-WAN controllers) are important. Successful network automation projects were more likely to involve CMDB. Organizations that avoid DIY network automation also cited CMDB as more prominent. IPAM was more common in North America, while homegrown software was more common in Europe.

Sample Size = 354

Source of Truth Data

In the context of network automation, a source of truth provides networking personnel with all the information they need to make an automated change correctly. So, what data do they need? **Figure 29** reveals that configuration information (e.g., golden configurations or configuration standards) is the top priority, followed by security policies. Network automation engineers and NetDevOps engineers placed a greater emphasis on security policies.

FIGURE 29. WHICH NETWORK DATA AND INFORMATION ARE MOST CRITICAL FOR IT PERSONNEL TO GATHER BEFORE THEY MAKE A CHANGE TO THE NETWORK WITH A NETWORK AUTOMATION TOOL?



“The config data is important, because then we know the steady state,” said a network automation engineer at a large university. “Security policies are also important. But now we’re talking firewalls, and things like that are harder to deal with because our firewalls change 15 or 20 times a day.”

Sample Size = 354

“We need devices, device types, and components of a config like IP addressing,” said a network engineer at a Fortune 500 food and agriculture company. “And for us, sites and locations are very important. Application requirements and security policies haven’t come up yet, but once you have true automation in place and are trying to automate services on top of the network, those would make sense.”

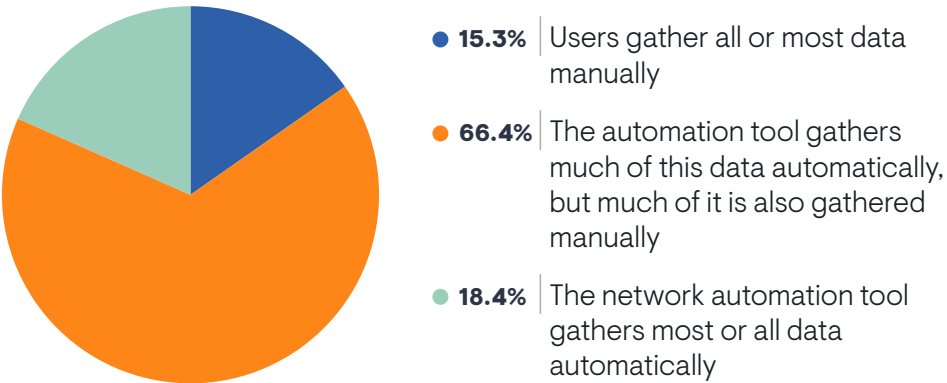
Network device metrics and applications’ networking requirements are secondary. Device metrics can reveal current network state, which helps users align intended change with network state. Application requirements will allow users to ensure that a change will improve or at least not harm the performance of an application. Device metrics were more important to less successful organizations.

DNS records were more important to network operations teams. Network flow data (another source of information on network state) was more important to DevOps, cloud, and security teams. Inventory data was more important to customers of vendor-supported open source tools.

Gathering Source of Truth Data to Make a Change

While many IT organizations do have a network source of truth, very few are able to automate the process of gathering data when making a network change. EMA asked all respondents to describe how IT personnel gather the data they need to make a change with a network automation tool. **Figure 30** reveals that only 18% have fully automated this data gathering process. More than 66% have a mix of automation and manual processes and the rest manually gather all data. IT administrators and engineers reported more manual data gathering than IT middle management and executives, revealing a potential awareness gap in just how automated this process is. Overall, the security team perceived the most data automation, while network engineering teams perceived the most manual processes. Very large enterprises (20,000 or more employees) reported the most data automation.

FIGURE 30. WHEN IT PERSONNEL MAKE A CHANGE VIA NETWORK AUTOMATION TOOLS, WHICH OF THE FOLLOWING BEST DESCRIBES HOW THEY GATHER THE DATA THEY NEED TO MAKE THAT CHANGE?



Automation of this data collection is more extensive when organizations avoid DIY network automation, regardless of whether they’re using proprietary tools or vendor-supported open source. Also, network automation projects that are fully funded have more automated data gathering.

EMA’s data analysis reveals that when organizations automate much of this process, they tend to:

- Be more successful with network automation in general
- Automate more network management tasks
- Reduce security risk and accelerate incident response via their network automation investments
- Be happier with customizability of their tools

Sample Size = 354

Consequences of Manual Data Gathering

Obviously, forcing users to manually collect data before making a change can impact the quality and efficiency of those changes. **Figure 31** examines what organizations have experienced as a consequence of having manual data gathering in their automation workflows. The biggest issue is the sense that the overall effectiveness of network automation is lower.

Increased security vulnerabilities and downtime or performance issues caused by errors are also frequent. Midsized enterprises (1,000 to 4,999 employees) reported a higher incidence of security vulnerabilities.

Increased policy violations are less frequent, but DevOps and security teams perceived them more often. A lack of change visibility and verification was another lesser issue, but DevOps, security, and IT architecture all reported it more often. Adoption failure was another rare issue, but it was reported more often by customers of open source vendors and network automation tools that network infrastructure vendors offer.

FIGURE 31. HOW DOES MANUAL DATA COLLECTION IMPACT THE EFFECTIVENESS OF YOUR NETWORK AUTOMATION TOOLSET?



Sample Size = 289



Spotlight on Network Validation

“The most challenging thing about network automation is testing to make sure that whatever you are doing will work,” said a network automation engineer at a medical school and hospital network.

In this section, we explore a critical and sometimes underrated stage of network automation. Network validation is the process of understanding how changes made through automation might impact the state of the network. Network validation should be performed before a change is made to ensure that the proposed change is good, but it should also be performed after the change is made to ensure the change was successful and had the expected outcome.

“The most challenging thing about network automation is testing to make sure that whatever you are doing will work,” said a network automation engineer at a medical school and hospital network. “Network automation is powerful, but it is also dangerous. You can make a change that can bring down the whole network.”

Pre-Change Validation

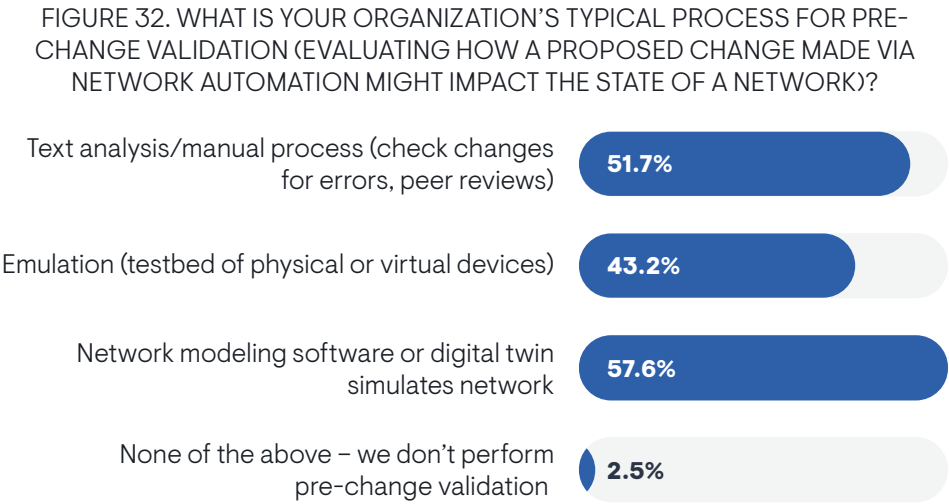
Figure 32 reveals how network automation strategies are currently accounting for pre-change network validation. First, at least 98% are doing at least some form of pre-change validation. Most are using network modeling software or digital twin software to simulate their networks, and they are relying on text analysis and manual processes to validate change. A smaller number are emulating a network using a virtual or physical lab or testbed. Successful network automation strategies are more likely to leverage network modeling or digital twin technology for pre-change validation.

“Some of our tooling is able to look at the entire network and create a digital twin, so we look at how traffic is supposed to flow from point A to point B,” said a tool architect at Fortune 500 media company. “But we’re a bit early on this.”

Network automation engineers and NetDevOps engineers perceived more use of network modeling and digital twin software than network administrators, network engineers, or network architects. Text analysis was more commonly used by organizations that write their own homegrown network automation software.

“We have a virtual lab environment of our network. We have replicated most of our network in it, but not at the scale that we have in production,” said a network tools engineer at a Fortune 500 retailer. “The team tests it in the lab first. Once everything is confirmed and running for a couple weeks, we decide it’s good to go. We then push it out as the new standard.”

“We have some containers we run in a lab environment to check changes, and also some custom scripts,” said a network engineer at a midmarket business services company. “It’s not a full topology of our network, just a reference model. We don’t have the resources to simulate our production environment.”

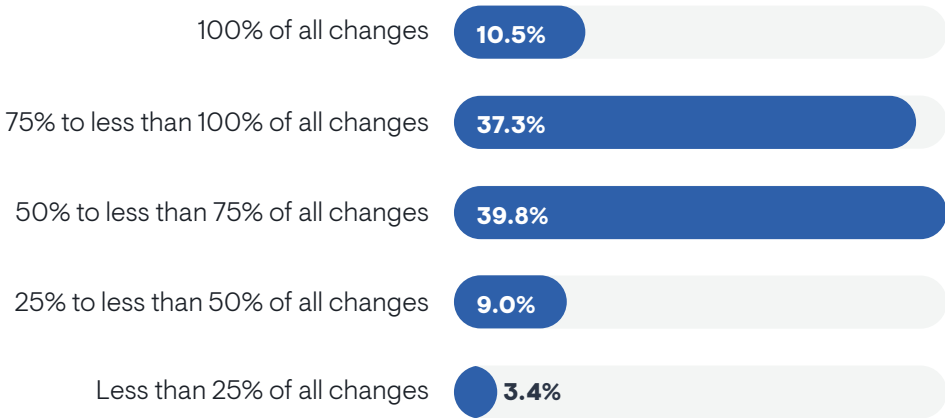


Sample Size = 354

Frequency of Pre-Change Validation

Pre-change validation isn’t an easy process, especially for organizations that rely on manual processes or labs. Thus, many network teams may skip it occasionally. **Figure 33** reveals that fewer than 11% of organizations validate 100% of network changes before implementing them. Most fall between 50% and fewer than 100% of changes.

FIGURE 33. HOW CONSISTENTLY DOES YOUR TEAM PERFORM A PRE-CHANGE VALIDATION PROCESS ON AN AUTOMATED NETWORK CHANGE?



Sample Size = 354

“We want to make sure that anything changed in code is validated before it is committed, and once it’s committed, we want to make sure it’s a valid code change that results in a valid configuration on a device,” said a network automation engineer at a \$3 billion SaaS provider.

Organizations that are the most successful with network automation reported a more consistent approach to pre-change validation. Larger enterprises (20,000 or more employees) and midsize enterprises (1,000 to 4,999) perform this task more often than enterprises with 5,000 to fewer than 20,000 employees. EMA also found that organizations that automate the process of gathering all the data required to implement network changes are more consistent with pre-change validation.

“We have some validation, but not enough,” said a network engineer at private gaming company. “That’s something we’re working on. It’s a concern, but not that big of one. I would love to know if this change will make my traffic move in a different direction. Also, when I upgrade this device, what will happen? No one can solve that in a container lab.”

Organizations that are the most successful with network automation reported a more consistent approach to pre-change validation.

Post-Change Validation

Once a change is implemented, there are more ways to perform a post-change validation, partly because the change now impacts the production network. A monitoring tool will detect many problems that occur because of a bad change. Of course, one might not want to rely on such a reactive approach to post-change validation, because it takes time for network engineers to connect the dots between a monitoring alert and a bad change.

Figure 34 reveals that as with pre-change validation, network modeling and digital twin software are the most popular approaches to post-change validation. Again, successful network automation strategies are more likely to use these tools. Also, they are perceived more by network operations, security, and cloud teams, and they are perceived less by IT tool engineering and IT architecture groups.

“This was a challenge in my last role,” said a network automation engineer at a Fortune 500 manufacturer. “If I had continued at that company, I would have put a lot of focus on trying to model the network. Validation is really tricky. It gets cumbersome to be able to say without any doubt that the intended change had the effect that I intended. Part of the problem is that the network vendors don’t provide good APIs.”

Many organizations also rely on manual configuration checks, proactive traffic monitoring and analysis, and alerts from a network source of truth. Source of truth alerts are more popular among very large enterprises (20,000 or more employees). It’s also more common among organizations that are using vendor-supported open source tools, rather than those that use proprietary software that a network infrastructure vendor offers.

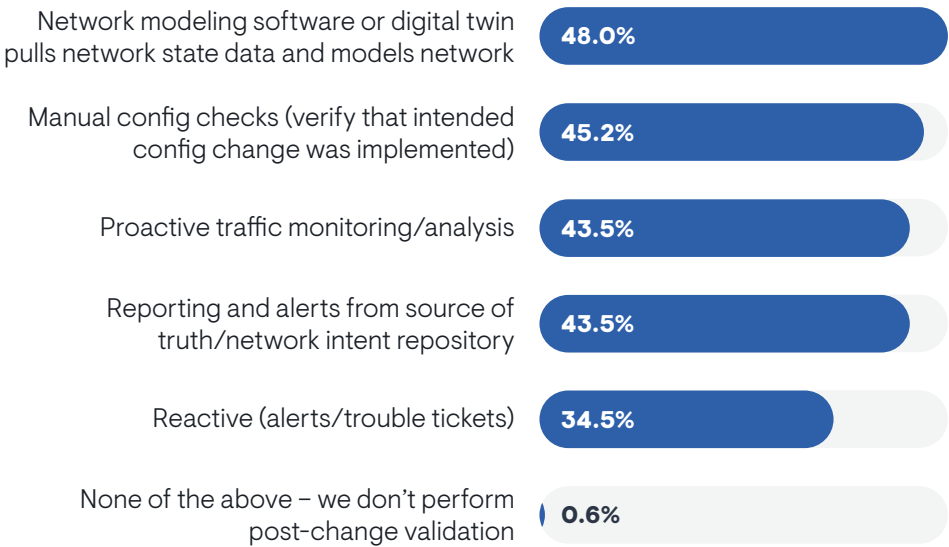
The least popular approach is the reactive strategy of waiting for alerts from tools and trouble tickets. EMA would like to see the number of organizations that rely upon this method to shrink over time.

“We will get alerts from our monitoring system that something is wrong,” said a network automation engineer at a medical school and hospital network. “If it

was not successful, we have to roll back the change and document what went wrong and analyze why it didn’t work.”

“Right now, we do show-version at the beginning and end of a change and hopefully the end state is what your target was,” said a network engineer at a Fortune 500 food and agriculture company. “We’re trying to bake things in, like what ports are up on devices, then look at it when you reload the device post-upgrade to answer the question, ‘Is the same set of interfaces up?’ But integrating that into our processes is so complex.”

FIGURE 34. WHAT IS YOUR ORGANIZATION’S TYPICAL PROCESS FOR POST-CHANGE VALIDATION (EVALUATING HOW A CHANGE MADE VIA NETWORK AUTOMATION IS IMPACTING THE STATE OF A NETWORK)?

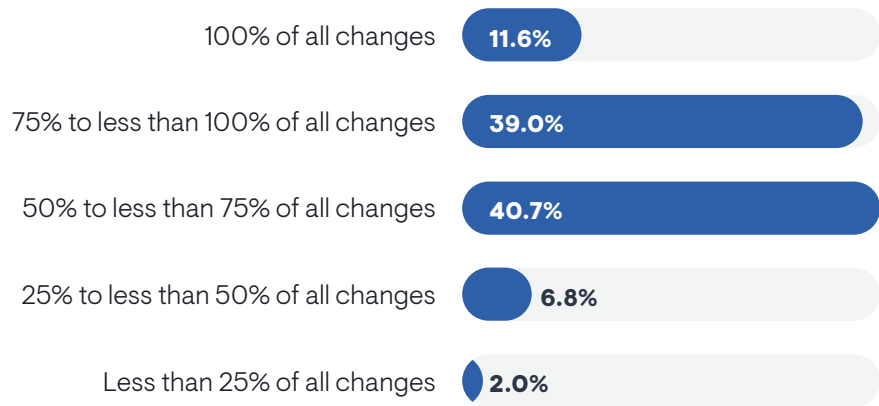


Sample Size = 354

Frequency of Post-Change Validation

Figure 35 reveals how often network teams validate an automated change after it's been committed. Fewer than 12% validate 100% of changes. As with pre-change checks, most organizations perform a post-change validation between 50% and less than 100% of the time. Successful organizations reported a higher frequency of post-change checks.

FIGURE 35. HOW CONSISTENTLY DOES YOUR TEAM PERFORM A POST-CHANGE VALIDATION PROCESS ON AN AUTOMATED NETWORK CHANGE?



“Before an upgrade, we run a pre-check and after the upgrade happens, we do post-checks. That is something we are starting to do,” said a tool architect at a Fortune 500 media company. “The problem is that we have a lot of different types of automation. If you do 100 different types of automations, then you have to build 100 different kinds of checks.”

Larger enterprises (20,000 or more employees) reported the highest rate of post-change checks. Organizations that automate data gathering for network automation reported more consistency, too. The CIO’s suite and the DevOps team reported more consistency than IT architecture. IT tool engineering teams reported the most inconsistent post-change checks.

Sample Size = 354

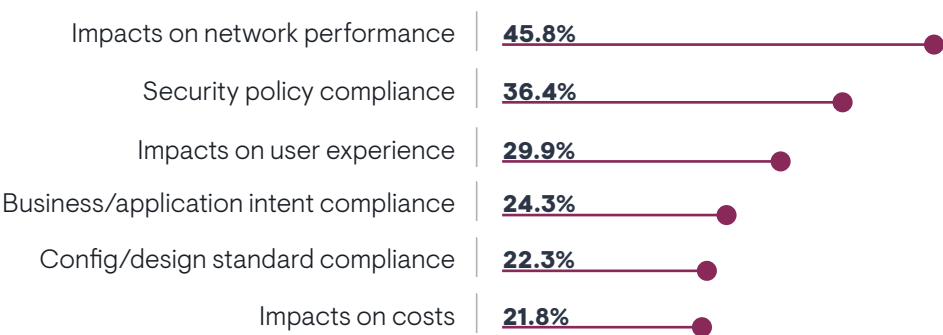
What is Validated?

There are multiple ways that a network change can impact a network. IT organizations will vary in what they want to validate when they perform pre- and post-change checks. **Figure 36** reveals that most network teams are focused on understanding overall network performance. Successful organizations are less likely to validate impacts on network performance. The second priority is understanding compliance with security policy, especially among IT executives and middle management.

Nearly 30% try to get a more abstract understanding than just network performance by trying to understand impacts on user experience.

The lowest priorities are business or application intent compliance, configuration or design standard compliance, and impacts on costs.

FIGURE 36. WHEN PERFORMING PRE- AND POST-CHANGE VALIDATION, WHAT IS YOUR NETWORK TEAM PRIMARILY TRYING TO VERIFY?



Sample Size = 354

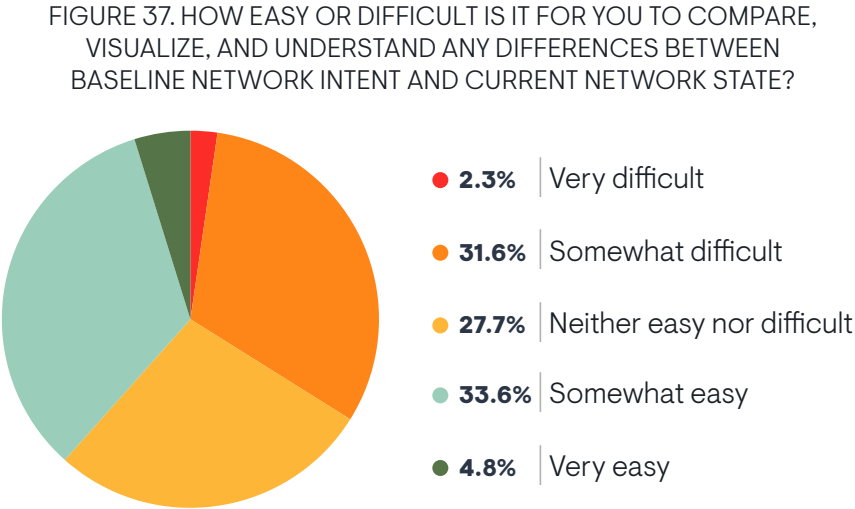
Comparing Network Intent and State

Less than 5% of organizations believe it is very easy to compare and understand the difference between intent and state.

The key question to answer when performing pre- and post-change network validation is whether network intent and network state are in synch. It is not a trivial question to answer. **Figure 37** reveals that less than 5% of organizations believe it is very easy to compare and understand the difference between intent and state. Nearly 34% report actual difficulty, while nearly another 34% believe it is only somewhat easy, meaning they see room for improvement. Organizations that have successful network automation strategies are more likely to have an easy time with this issue. Network engineering teams reported an easier time with comparing differences than most other groups, especially more so than DevOps, cloud, and IT tool engineering teams.

EMA found that differences between network intent and state are easier to find when organizations have the following:

- Larger network automation toolsets, possibly because that toolset includes a dedicated solution for reporting these differences
- Network modeling or digital twin software for network validation
- High-code network automation tool strategies
- Fully funded network automation budgets
- An effective network source of truth
- Tools that perform continuous configuration compliance monitoring



Sample Size = 354



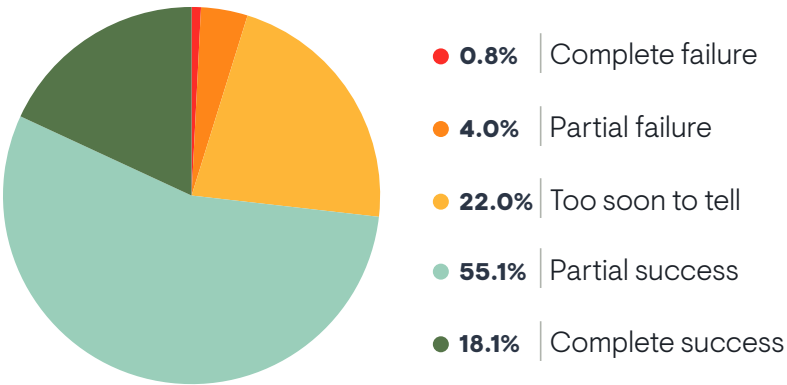
Project Outcomes

Project Success

Only 18% of research participants believe that their network automation strategy is a complete success. Another 55% described their efforts as a partial success. Only 5% admitted to failure, as **Figure 38** shows. North Americans were more confident than Europeans, and larger companies claimed to be doing better than smaller ones.

IT executives, middle managers, and networking personnel (administrators, engineers, and architects) were all more optimistic than project managers, network automation engineers, and NetDevOps engineers. In other words, the people who build network automation tools are feeling the most pessimistic. This conclusion is further solidified by the fact that members of IT tool engineering teams were pessimistic or uncertain about success.

FIGURE 38. HOW WOULD YOU RATE YOUR ORGANIZATION'S OVERALL NETWORK AUTOMATION STRATEGY TO THIS POINT?



Benefits of Network Automation Investments

Figure 39 identifies the benefits that IT organizations experience when they invest in and use network automation tools. There are two major opportunities: operational efficiency and reduced security risk. In other words, network automation boosts network team productivity and eliminates errors that might lead to security events.

“We often provide our vice presidents with metrics in terms of estimates of how many man hours we spend today doing it manually versus how many hours we can potentially save by having an automated workflow,” said a tools architect with a Fortune 500 media company. “If I’m spending 100 hours a month on firewall changes, I can show them that I can reduce it by half with automation. That’s how I demonstrate value.”

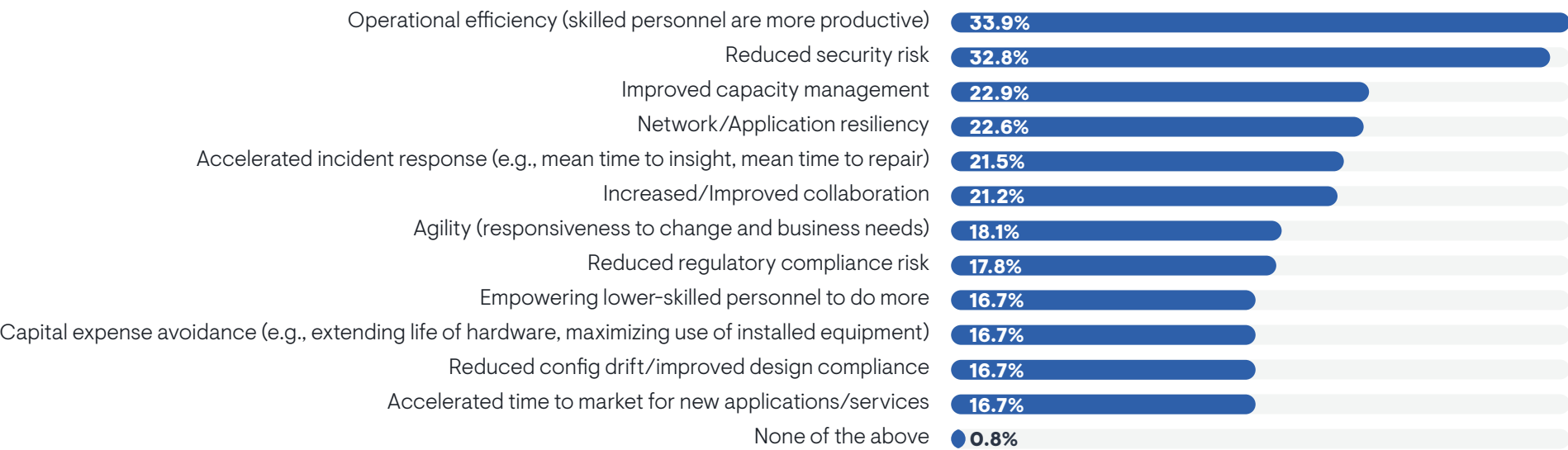
“Automation takes human error out of the network. We’ve decreased outages by a significant amount,” said a network automation engineer at a large university. “When people hit a button to automate something, we have scripts running so

many checks before a change is done. Also, we’ve empowered technicians who lack the skillsets to make changes and write configs. Field teams can be made up of people with lower skillsets, who can go out and hit a button to troubleshoot things.”

Secondarily, organizations told EMA that they improved capacity management, improved the resiliency of networks and applications, accelerated incident management processes, and boosted collaboration. Resiliency and operational efficiency were more common benefits for users of proprietary network automation software. Network operations teams were more likely to perceive reduced configuration drift, increased collaboration, and improved capacity management.

“I want to find ways to work together and see what’s going on and get more collaboration out there,” said a network engineer at a Fortune 500 food and agriculture company.

FIGURE 39. WHAT ARE THE MOST VALUABLE BENEFITS THAT YOUR ORGANIZATION HAS EXPERIENCED FROM ITS INVESTMENTS IN NETWORK AUTOMATION?



Current Support of Key Capabilities

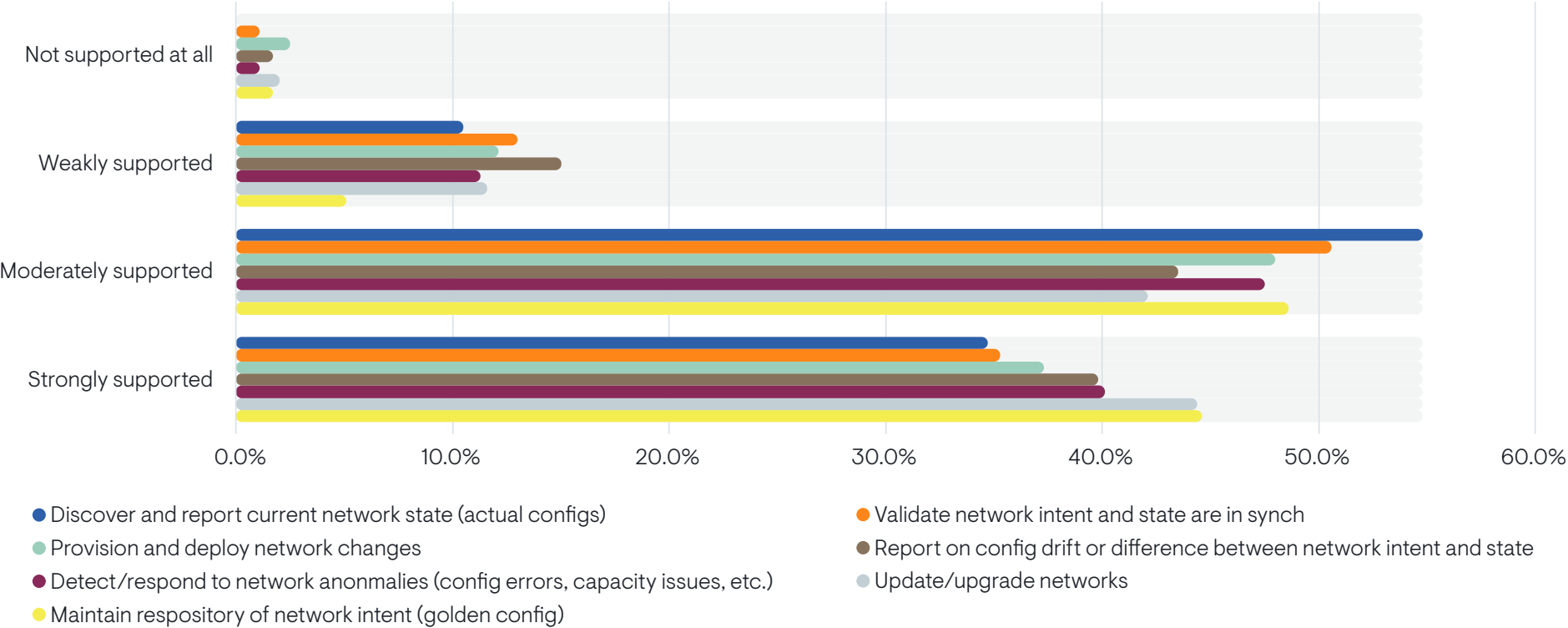
Figure 40 explores how well network automation tools are supporting seven key areas of network automation. Research participants told EMA that their tools are most effective at maintaining a repository of network intent and supporting workflows around updating and upgrading networks (e.g., patches and software updates).

Network automation toolsets are slightly less effective at enabling detection and response to network anomalies and reporting and responding to network configuration drift.

Respondents reported weaker support for provisioning and deploying network changes, validating that network intent and network state are in synch, and discovering and reporting on current network state.

Overall, respondents who reported the most success with network automation indicated stronger support of all seven aspects of network operations. Members of network engineering teams felt better about how their network automation tools supported intent repositories and reporting on configuration drift.

FIGURE 40. TO WHAT EXTENT DOES YOUR NETWORK AUTOMATION TOOLSET SUPPORT EACH OF THE FOLLOWING ASPECTS OF OPERATIONS?



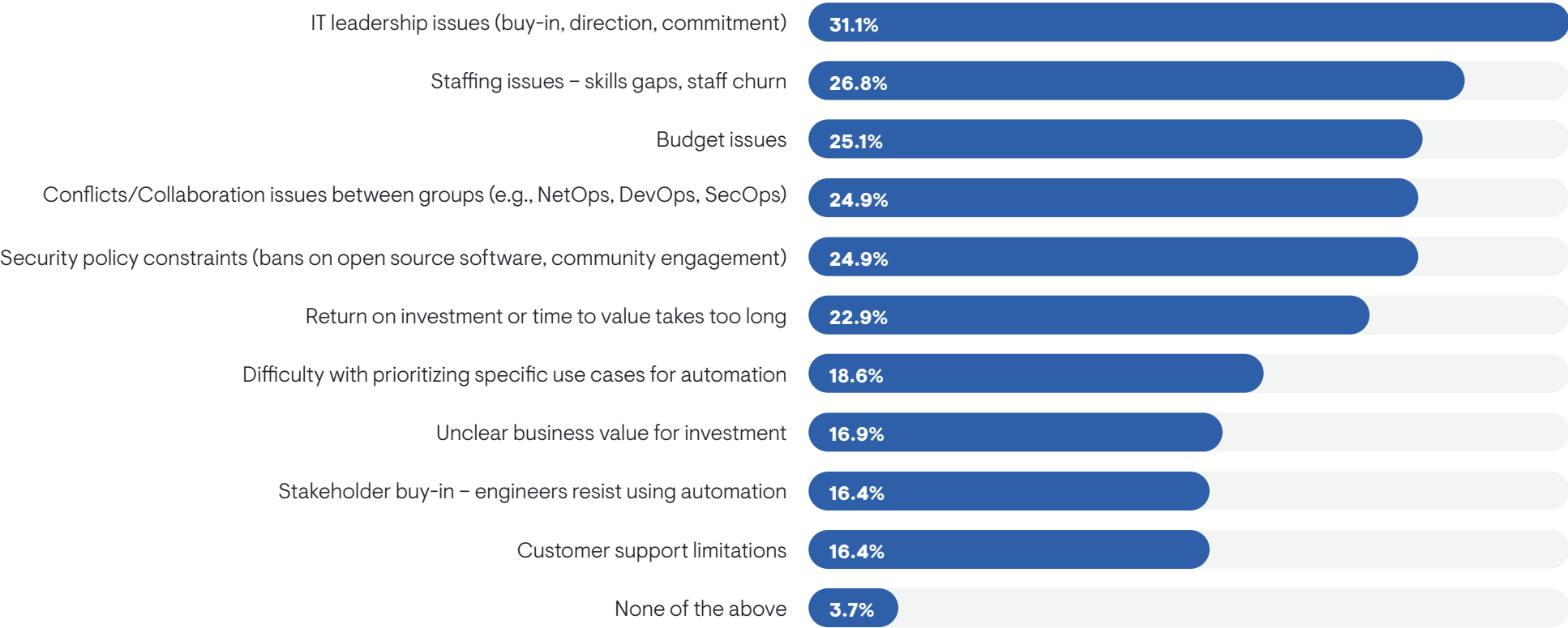
Sample Size = 354

Business Challenges

Figure 41 reveals the business challenges that IT organizations struggle against when trying to implement a network automation strategy. IT leadership topped the list. Executives aren’t aligned with the people trying to execute on automation, or they’re failing to set an agenda for technology strategy and adoption.

Staffing issues are the chief secondary problem. Both midsized (1,000 to 4,999 employees) and very large enterprises (20,000 or more) struggled with this issue, while all other companies were less likely to have a budget problem.

FIGURE 41. WHICH OF THE FOLLOWING BUSINESS ISSUES ARE MOST CHALLENGING TO YOUR NETWORK AUTOMATION STRATEGY?



Sample Size = 354

“It’s hard to convince a developer to work with networking because they don’t understand it or want to work with it,” said a tools architect with a Fortune 500 media company.

“Even though we have expanded to a six-person team, the amount of automation that’s required is overwhelming,” said a tools architect with a Fortune 500 media company. “We need more scripts and developers. It’s easy to find people who can automate and to find people who are network engineers. But it’s hard to find people who understand both of these worlds very well. It’s hard to convince a developer to work with networking because they don’t understand it or want to work with it.”

“The most challenging thing for me is the lack of network engineers who can contribute to automation,” said a network engineer at a midmarket business services company. “The community is small, and it’s hard to find people who can help you solve a problem.”

“One big thing is training, because the cognitive lift for the team is going to be a huge thing,” said a network engineer at a Fortune 500 food and agriculture company.

“You have to have wide and deep knowledge,” said a network automation engineer at a Fortune 500 manufacturer. “That’s the biggest barrier to entry. It’s become clear to me now that I’m a software engineer with a network engineering background. I can’t know everything about BGP anymore. It all changes so fast. There’s lots of learning to do.”

Budget, conflicts, and collaboration issues between groups, security policy constraints, and slow returns on investment are also prominent problems. Successful organizations were less likely to complain about budget or slow returns on investment. Very large enterprises were also more likely to run into budget shortfalls. Organizations that use internally developed software perceived slow returns on investment as a bigger issue.

“One thing that needs to improve is collaboration,” said a network automation engineer at a medical school and hospital network. “Departments work in silos. Sometimes you might have a challenging use case that you are trying to figure out, but you might not realize that someone else is already doing it. They’ve figured out a way to solve it.”

“It’s not easy to automate a task, because you don’t know all the variables that might be affected by it,” said an NOC analyst at a very large media company. “It’s not just the data, but also authorization by a change review board. Sometimes the process is above your paygrade, so you have to leave it to a supervisor to make the decision. It’s hard to control that authorization process.”

Resistance to automation (stakeholder buy-in) emerged as a very minor issue. That wasn’t always the case.

“Right now, network teams are more on board with it. Three or five years ago, all our teams were anti-automation,” said a network automation engineer at a large university. “They worried that they would be automated out of a job. That has shifted because they are seeing how beneficial it is. Automation can take things off their plates.”

“Bypassing automation is an issue,” said a network engineer at a private gaming company. “In areas where automation tools exist, people might have a good reason for doing things manually. But doing things manually stops you from fixing the tooling problems you are working around and it increases the likelihood that you implemented something incorrectly. We need to remove that temptation.”

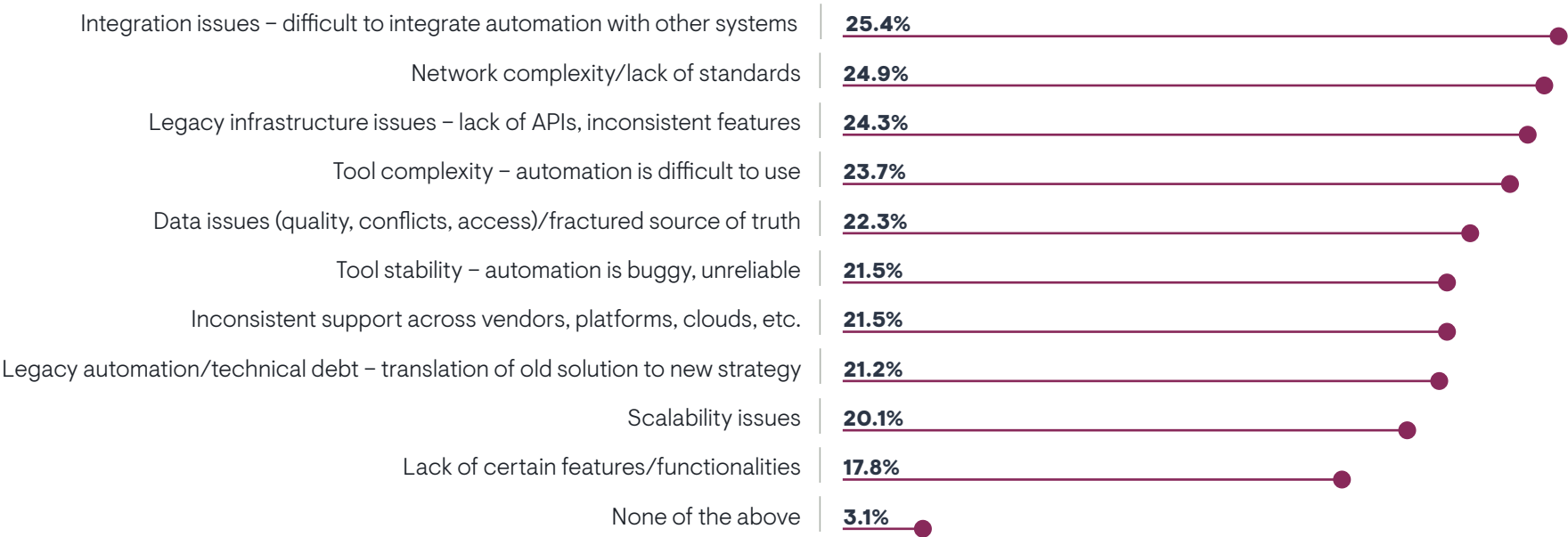
Technical Challenges

Figure 42 identifies the technical challenges that organizations encounter with network automation. There isn’t much distance separating the top four issues. Integration problems and network complexity edge out legacy infrastructure issues and tool complexity.

Nearly everyone that EMA interviewed one on one had some issue with standard compliance.

“Standardization is the biggest obstacle,” said a network tools engineer at a Fortune 500 retailer. “When the network is not standardized and the data is not standardized and you don’t have a standard way of generating inventories and a source of truth, it’s a big problem. You can’t automate at scale because you’re forced to automate one device at a time without standardization.”

FIGURE 42. WHICH OF THE FOLLOWING TECHNICAL ISSUES ARE MOST CHALLENGING TO YOUR NETWORK AUTOMATION STRATEGY?



“If you don’t have standards, what are you going to base your automation on?” asked a tool architect at a Fortune 500 media company. “You can’t just tell automation to do something. It has to have some inventory to go on.”

“If you don’t have standards, what are you going to base your automation on?” asked a tool architect at a Fortune 500 media company. “You can’t just tell automation to do something. It has to have some inventory to go on.”

“The biggest challenge is the standards,” said a tools architect with a Fortune 500 media company. “No matter how much we try, we still find devices not adhering to standards. Everything greenfield has a good standard, but the challenge is retrofitting brownfield to standards.”

“We have 160 sites that have all been deployed at different times by different people,” said a network engineer at a Fortune 500 food and agriculture company. “When we go over that to make sure we meet some kind of golden standard and compliance, we find that none of them are compliant right now. They are all ‘artisanally’ configured.”

Legacy infrastructure issues were cited more often by organizations that use proprietary network automation software from a network infrastructure vendor. This suggests that their networking vendor is offering automation that doesn’t fully support their older products.

DevOps, IT tool engineering, network operations, and cloud teams all complained of integration issues more often than network engineering and IT architecture teams.

Inconsistent support across multiple vendors is a tertiary problem, but organizations with failing network automation strategies selected it at a very high rate, suggesting it can make or break many projects.

Scalability was a minor challenge, but organizations that use proprietary automation software from a tool vendor encountered it more often. Network complexity also challenged these tools.

A network engineer at a midmarket business services company said API issues with his network infrastructure vendors are causing technical issues everywhere in his automation strategy, and it’s not limited to legacy network equipment with old APIs. “API documentation is poor and it often has bad information. Open source APIs don’t have this problem because they’re not trying to hide commercial secrets. Network vendors have this mindset that they should not share too much information.”

What Needs Improvement in Automation Toolsets

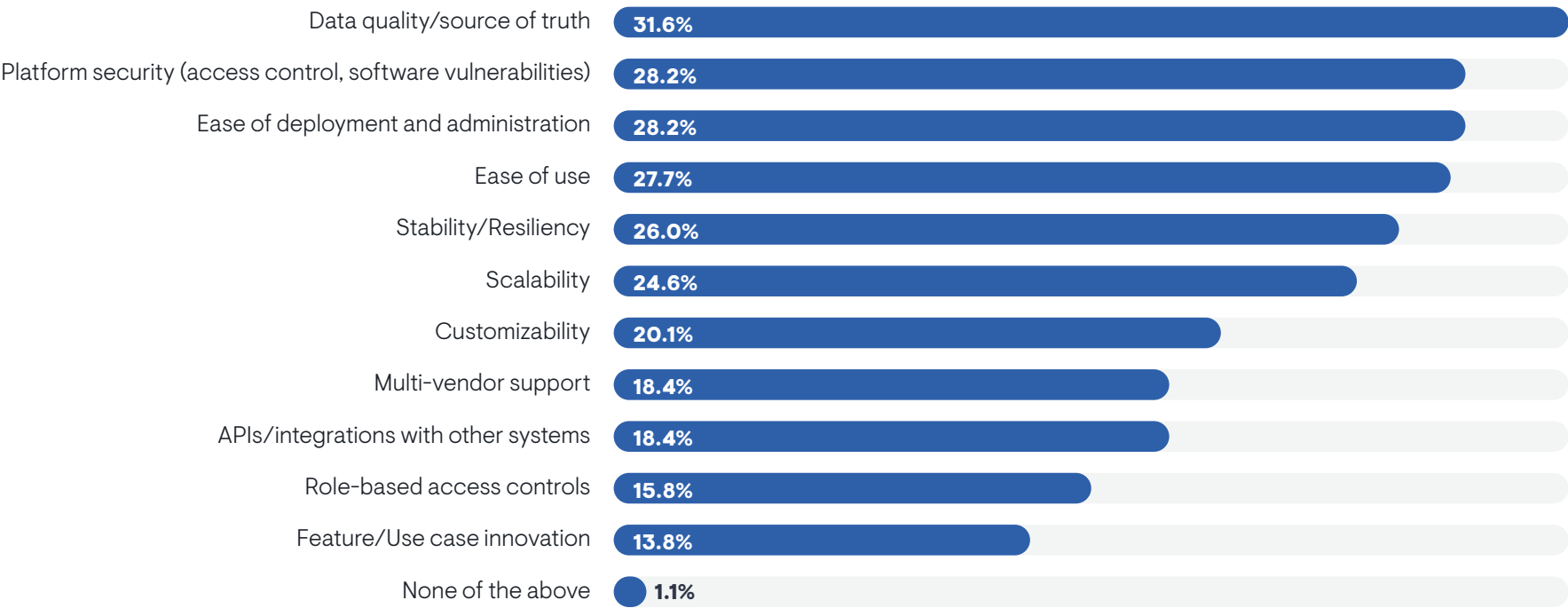
Figure 43 reveals the aspects of current network automation toolsets that respondents think they need to improve. Data quality is the biggest target for improvement.

Secondarily, organizations need better platform security, ease of deployment and administration, ease of use, stability, and scalability from their tools. Organizations that are failing with network automation were more likely to say they need better ease of deployment and administration, suggesting that this an issue that can make or break a project.

Feature and use case innovation was the least likely to be an issue for respondents; however, organizations that use homegrown, internally-developed network automation software were more likely to struggle with this innovation issue, suggesting that IT organizations that build their own tools are more likely to struggle to keep pace with feature requirements.

IT organizations that build their own tools are more likely to struggle to keep pace with feature requirements.

FIGURE 43. WHICH OF THE FOLLOWING ASPECTS OF YOUR NETWORK AUTOMATION TOOLSETS NEED THE MOST IMPROVEMENT?



Sample Size = 354

What Network Automation Vendors Need to Know

We asked research interviewees to tell us one thing that network automation engineers fail to understand about their requirements. Here are some of their answers.



Network automation engineer at a medical school and hospital network:

Vendors need to understand that a production network is different from a test environment. A lot of times, I have an issue and a vendor will tell me I need to test it in my lab. A lab has five or six users, but I'm dealing with 50,000 users. Vendors don't think about how things work under the load of a production environment. They test things in a lab and tell you it works in the real world, and that's not always the case.



Network automation engineer at a large university:

I think it's hard for vendors to make something that we can use off the shelf, especially in a university setting. We're governed by all these different colleges and all their needs are so vastly different that it's hard to find one product that can do all of it.



Network tools engineer at a Fortune 500 retailer:

I see a lot of vendors talking about no-code and low-code. I hate that technology because they try to make everything dumbed down so it can be done on a dashboard with a couple of buttons. When you go from one version of a network vendor's software to another, suddenly something changes in the config and it's no longer supported. Then it's all about going back and forth with the vendors to resolve the issue.



Tools architect with a Fortune 500 media company:

All vendors claim they can do everything. I often ask them to tell me about their core competencies. Don't sell me on everything. Just tell me what you're best at and we can work from there. It's difficult for me to see what they're good at so that we can position their product in our toolset.



Network automation engineer at a \$3 billion SaaS provider:

Some of the off-the-shelf products don't foresee the production complexity, such as the different vendors we have and how a production setup can be more complicated than what they have in their product. Most of the time, I find myself trying to explain that challenge to a vendor.



Network automation engineer at a Fortune 500 manufacturer:

I want to turn my network into an API. My biggest gripe is not with network automation vendors, but network vendors. Their APIs are terrible. This is not an option to just bolt on a toy API. Make an actual API, not just a marketing checkbox thing. A bolt-on API is one that is not very well documented, not very well designed, and doesn't conform to best practices. You just get the sense that it's an afterthought. And APIs should be officially supported. I should be able to open a TAC case on it. The reason I am well-paid is because I know how to get what I need from the network without an API, by scraping SSH and things like that.



Conclusion

For network automation, clearly, there is not one tool that addresses every requirement an IT organization has. Instead, network automation is a multi-tool endeavor. It's also going to be a mix of commercial and DIY solutions. Most organizations work with vendors, but they also build their own tools. There are myriad reasons for this state of affairs. Partly, it appears that no one vendor does everything that an IT organization needs. Moreover, no internal development team can build tools that can cover every requirement an organization has.

The future of network automation is an ecosystem of tools and products that must integrate to provide a fully effective solution.

EMA believes that the future of network automation is an ecosystem of tools and products that must integrate to provide a fully effective solution. For instance, there have long been multiple vendors that automate network design, provisioning, configuration, and change. Now, there are multiple providers of network validation and assurance software, too. Furthermore, there are multiple vendors that specialize in providing a network source of truth. In many cases, these vendors complement each other, but also, they complement many of the open source tools that network teams adopt on their own without vendor support.

In other words, there are multiple paths toward success with network automation, and each path appears to involve a constellation of components. Anecdotally, EMA finds that even the largest IT organizations with healthy budgets and large teams of talented engineers have vastly different approaches to network automation. Some of them focus on developing large libraries of single-use scripts. Others are working with multiple vendors of proprietary and/or open source software. Still others are writing full-featured homegrown automation tools. Yet somehow, all of them are finding success.

There may be no one path to network automation success, but there are a few things an organization can do to ensure success. First, network data is essential. Organizations must maintain an authoritative repository of network intent and network state data to ensure compliance with design standards and security policies. They should also monitor this compliance continuously to avoid security branches and outages. Moreover, organizations need tools to validate changes to protect against unintended consequences. It's not just about automating the provisioning and implementation of a change. It's about knowing the impact of that change and making sure the change is successful.

Organizations must maintain an authoritative repository of network intent and network state data to ensure compliance with design standards and security policies.

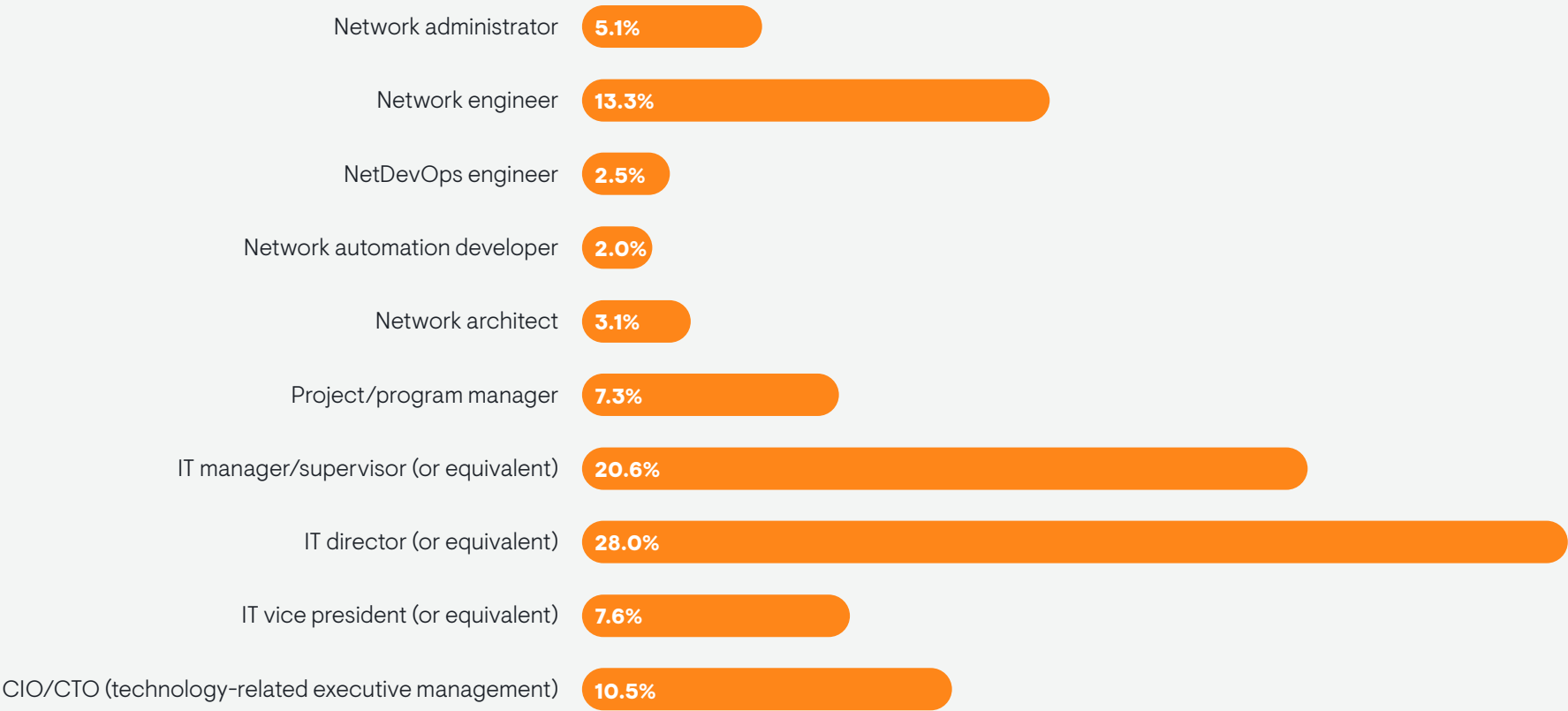
This will take commitment. IT executives must be prepared to lead and to provide the budget and resources needed to do network automation right. It will also require network teams to make sure their networks are ready to be automated. They must clean up their networks, establish standards, deal with legacy infrastructure that have limitations (such as a lack of APIs), and ensure that they have good data management. Excel spreadsheets and wikis won't cut it. Network teams need to build modern repositories of golden configurations, IP address space, device inventories, and more. The potential payoff of an effective network automation strategy is immense. Get to work.

"At the scale we do things with thousands of locations, even doing a little thing like running a simple change or command on a network device is just a huge job," said a network tools engineer at a Fortune 500 retailer. "Automation just makes life so much easier for people in terms of compliance, gathering config files from devices, running reports, and deployment."



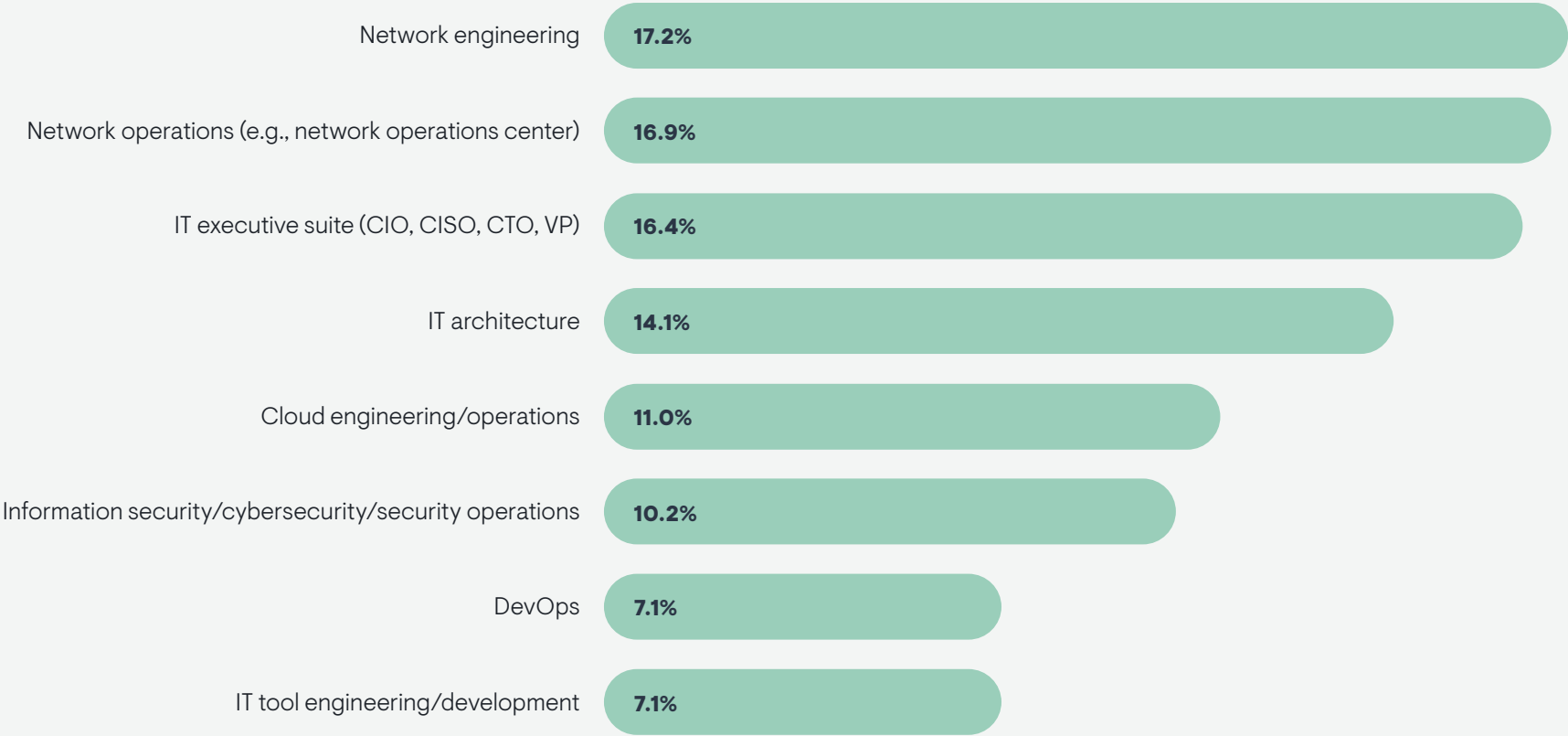
Appendix: Demographics

FIGURE 44. JOB TITLES



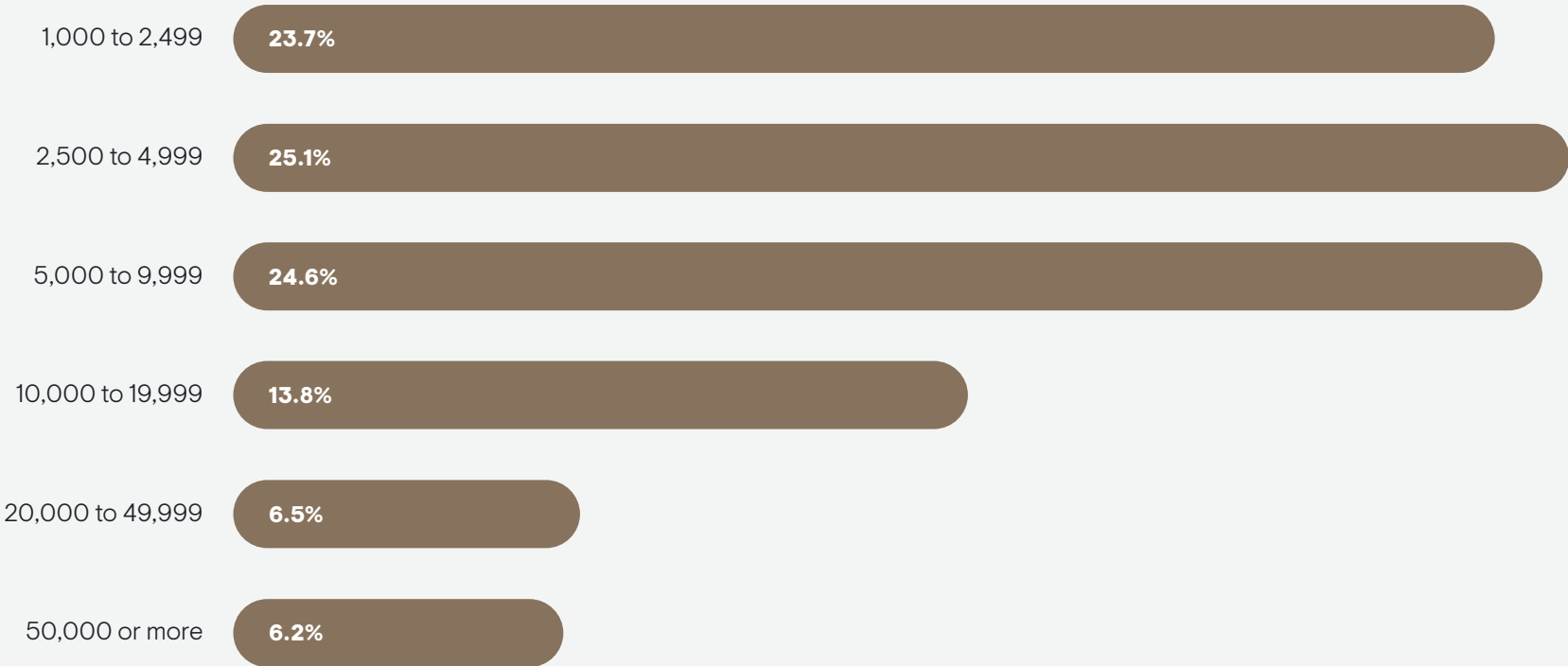
Sample Size = 354

FIGURE 45. IT GROUPS



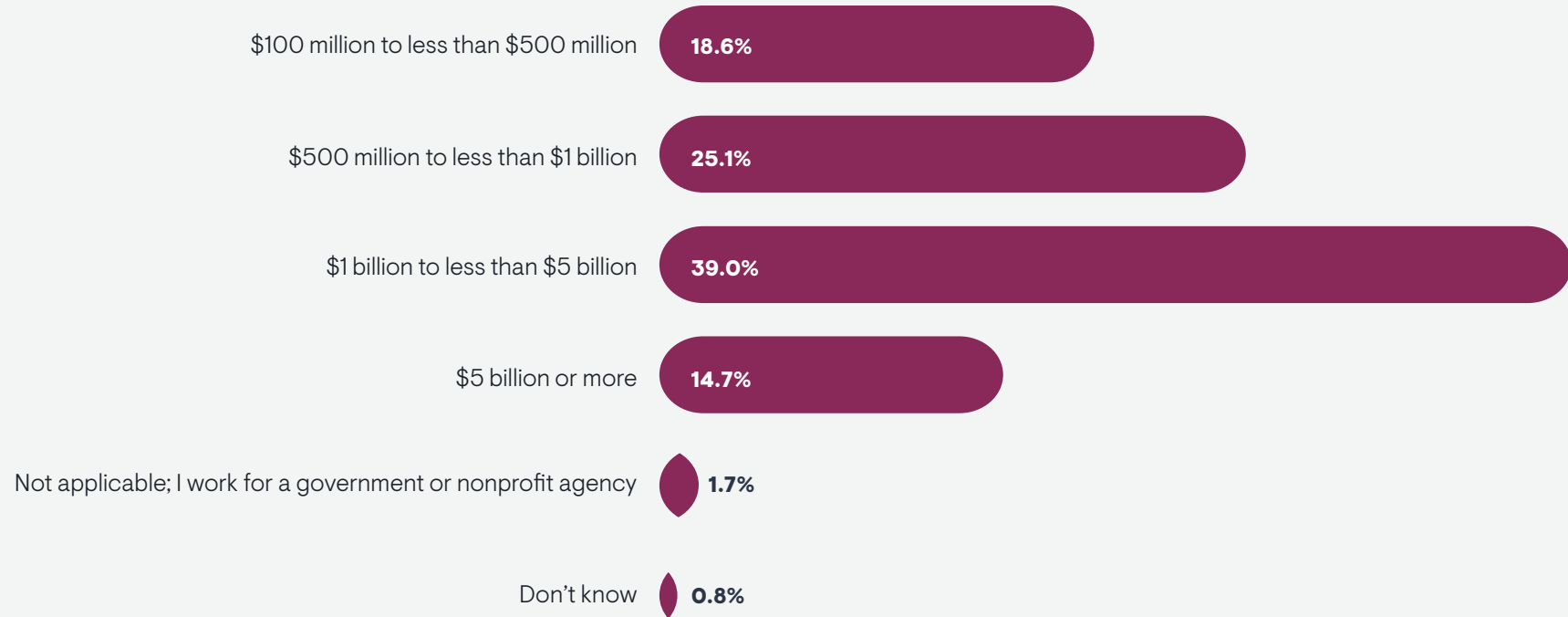
Sample Size = 354

FIGURE 46. COMPANY SIZE (TOTAL EMPLOYEES)



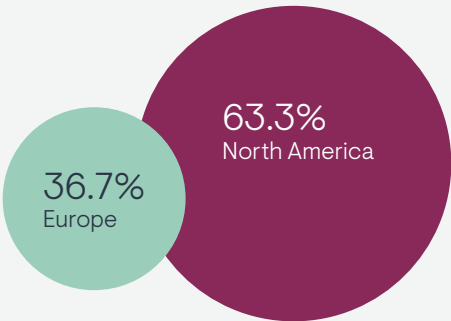
Sample Size = 354

FIGURE 47. ANNUAL SALES REVENUE



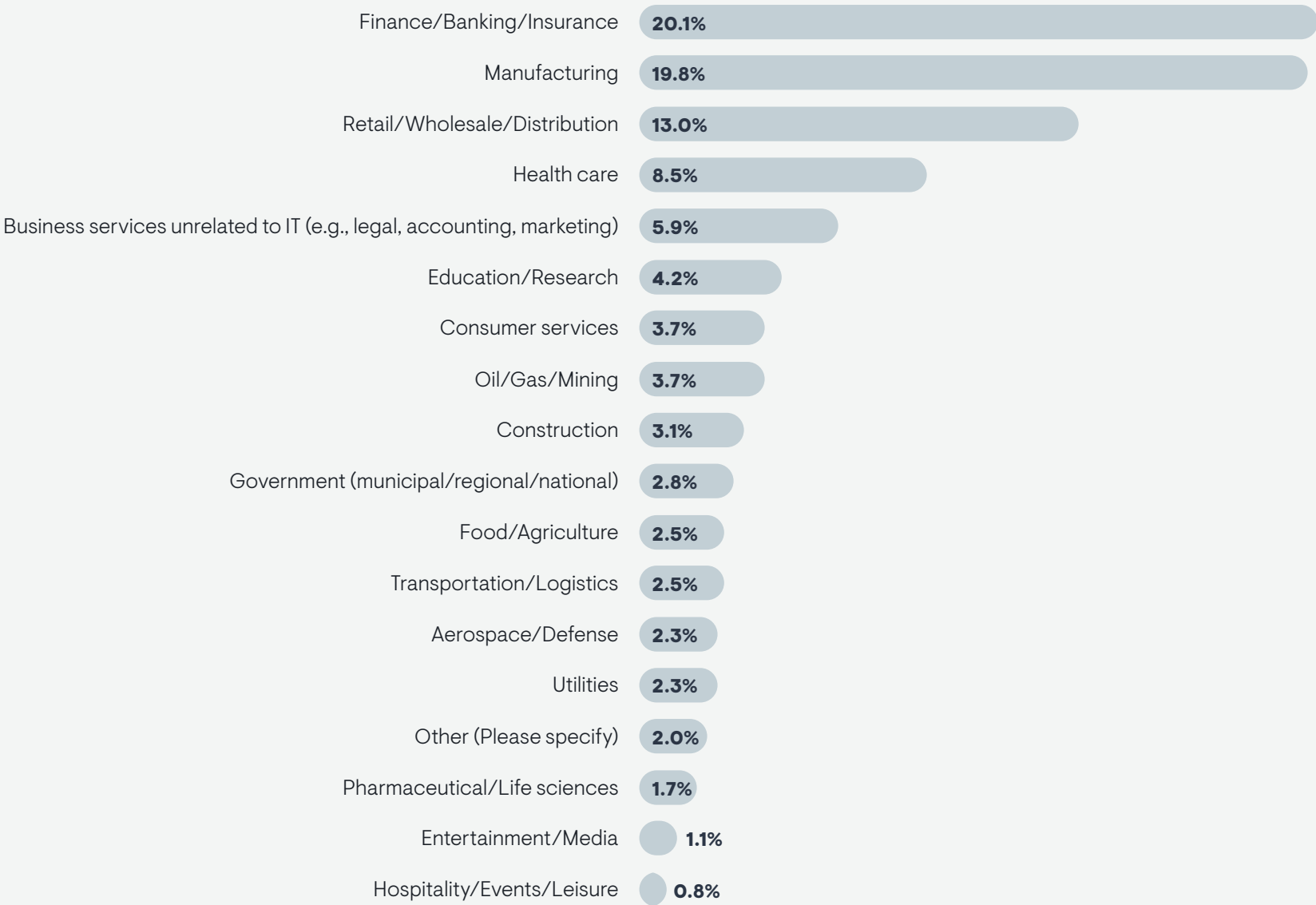
Sample Size = 354

FIGURE 48. REGION



Sample Size = 354

FIGURE 49. INDUSTRIES



Sample Size = 354





About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT 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 its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at www.enterprisemanagement.com or follow EMA on [X](#) or [LinkedIn](#).

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2024 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.