Using Network Automation to Power Modern Applications

How Network Automation Helps Meet Growing Networking Needs in the Era of Hybrid Cloud Applications and Digital Transformation

Pathfinder

October 2021

Commissioned by

Red Hat

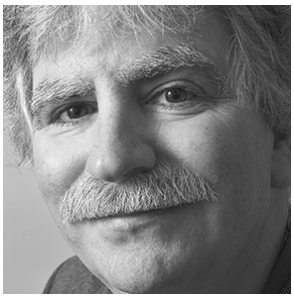
451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author



Mike Fratto

Senior Research Analyst, Applied Infrastructure & DevOps

Mike Fratto is a Senior Research Analyst on the Applied Infrastructure & DevOps team at 451 Research, a part of S&P Global Market Intelligence. He covers enterprise networking, including campus and datacenter networking, SDN, SD-WAN, SD-Branch, cloud networking, container networking, networking as a service, network performance monitoring, and network automation and orchestration. He has extensive experience reviewing and writing about enterprise remote access, security and network infrastructure products, as well as consulting with enterprise IT, equipment and software vendors, and service providers.

Prior to joining 451 Research, he was with GlobalData as Research Director with the Global IT Technology & Software team covering the enterprise networking and datacenter technology markets. Mike was with TechWeb for more than 15 years, most recently as Editor of Network Computing. He was Lead Analyst with InformationWeek Analytics, Senior Technology Editor with Network Computing and Executive Editor for Secure Enterprise. He has spoken at several conferences including Interop, SD-WAN Summit, MPLS + SDN + NFV World Congress and SDN NFV World Congress, as well as to local groups, and he served as the chair for Interop's Datacenter and Storage tracks. Prior to Network Computing, Mike was an independent consultant.

Mike teaches a graduate course in network security for Syracuse University's Information Science and Technology program. The course presents a technical and theoretical overview of network security strategies and technologies and how network security can fit into an organization's overall IT architecture.

Mike graduated from Syracuse University with a bachelor's degree in Information Science and Technology.

Executive Summary

To keep pace with modern application strategies, the growing number of network technologies and the distributed nature of hybrid IT architecture, networking teams need to automate and streamline the processes and tasks necessary for networking provisioning and management. The path to network automation should be well thought out; starting with simple automation tasks and maturing to more complex ones is a common approach that will give IT and network teams time to gain experience with network automation and ensure the least disruption. Early gains in efficiency – such as less time spent on provisioning tasks and less downtime from configuration errors – will quickly add up. And as networking teams gradually become more efficient with management and maintenance tasks, they will be able to spend more time on value-added work and less time manually configuring networks.

Network automation emphasizes skills carried by application architects and senior developers for project planning, achieving interim goals and taking a systems approach to automation, but they can't do it alone. Domain experts in networking must bring their skill sets to the project and be an integral part of the process. The collaboration that is fostered through a network automation project will have a number of benefits, including making DevOps teams more efficient and effective.

Key Findings

- Enterprise IT is only as agile as its least automated process. Measures of IT agility are how responsive the network is to configuration changes, how quickly a change request can be executed and how fast changes are deployed across the network.
- DevOps teams expect network teams to take responsibility for a growing number of on-premises, cloud and WAN network functions that span security, performance and monitoring and to provide those capabilities as a service that developers can include as a component of the continuous integration/continuous deployment pipeline.
- Manual management via the command line is error-prone and is proving to be unable to keep up with the pace of change demanded by modern application deployment strategies. While they are simple mistakes, typos and syntax errors can cause significant and costly downtime.
- Nearly all enterprises operate in a hybrid multicloud environment using cloud services and on-premises or colocated datacenters, and they will continue to do so for the foreseeable future. Enterprises increasingly expect that self-service infrastructure will be available wherever workloads reside. The network can be self-service while still abiding by regulatory requirements.
- The growing number of items under management and the need for faster change is driving IT departments to automate their networking process end to end, as well as in all environments where applications reside.
- A majority of enterprises that have become fully cloud native have said their networks are as responsive to change as they need to be, while a smaller minority noted that they had improved but could still do better. This suggests early successes in using automation to create more responsive network environments.
- Organizations should set realistic measures of success. For example, they may choose to reduce the time it takes to execute multi-stage workflows or measure the change in how much time they spend on daily operations and how much time they spend on higher-value architecture and design.

Introduction

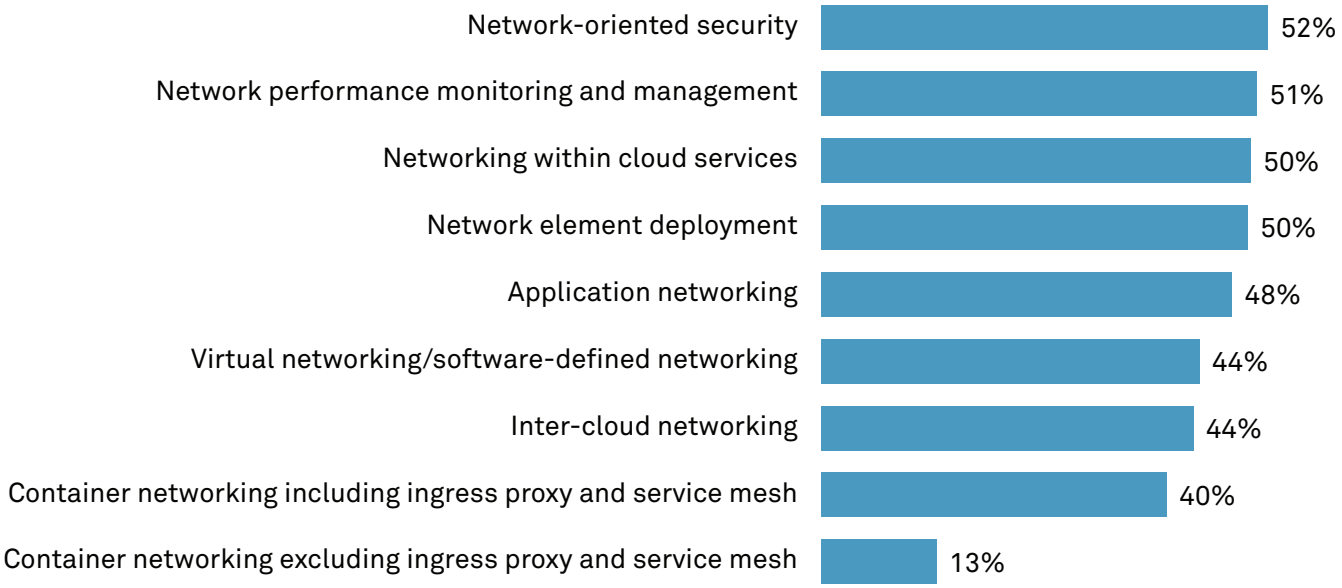
When most of us think of a traditional network, we think of routing and switching – the fundamental components that interconnect users, services, applications and resources. But the network has become much more, going beyond physical devices to now include software-defined, wide-area and cloud networks. These modern networks employ technology such as application delivery controllers, web application and network firewalls, transport layer security gateways, identity managers, caching controllers, network storage, virtual private network (VPN) gateways, container networks and service meshes. The expansion of network functions is a direct result of new demands from the growing use of multicloud and hybrid cloud computing with each type of cloud and on-premises environment offering its own set of networking services and capabilities.

Applications used to be largely contained in a single location, but designing and deploying applications to multiple cloud services, on-premises and the distributed edge is driving new demands from the network because of the increasing number of connections (including intermittent connections) from remote locations, and endpoints such as Internet of Things (IoT) sensors, application components and remote apps on mobile devices. All of these have varying demands, such as high throughput or low latency, depending on the application. The networking team must ensure reliable, secure and performant connectivity in this diverse and dynamic environment.

New application strategies are impacting IT organizations in new ways. The reconfiguration of IT into DevOps teams has been a boon for IT departments. Closer collaboration has enabled faster application deployment, improved IT efficiency and more consistent deployment strategies, but it doesn't do away with silos of responsibility. 451 Research has found that network teams and administrators are expected to own and manage a wide variety of network services and deliver them to the DevOps teams in a timely manner (see Figure 1).

...network teams and administrators are expected to own and manage a wide variety of network services and deliver them to the DevOps teams in a timely manner.

Figure 1: Network IT Ends Up Taking Responsibility for Every Aspect of Connectivity and Network Service, Led by Network Security



Q: Which functions should network administrators/teams own and manage? Please select all that apply.
Base: All respondents (n=549)
Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2021

The growth of responsibilities is one factor driving network automation. Manual workflows that worked well when applications were largely static and predictable won't work in a cloud-native world with distributed applications that scale on demand and can move locations when required. Supporting modern applications means IT will have to adopt network automation to play its part.

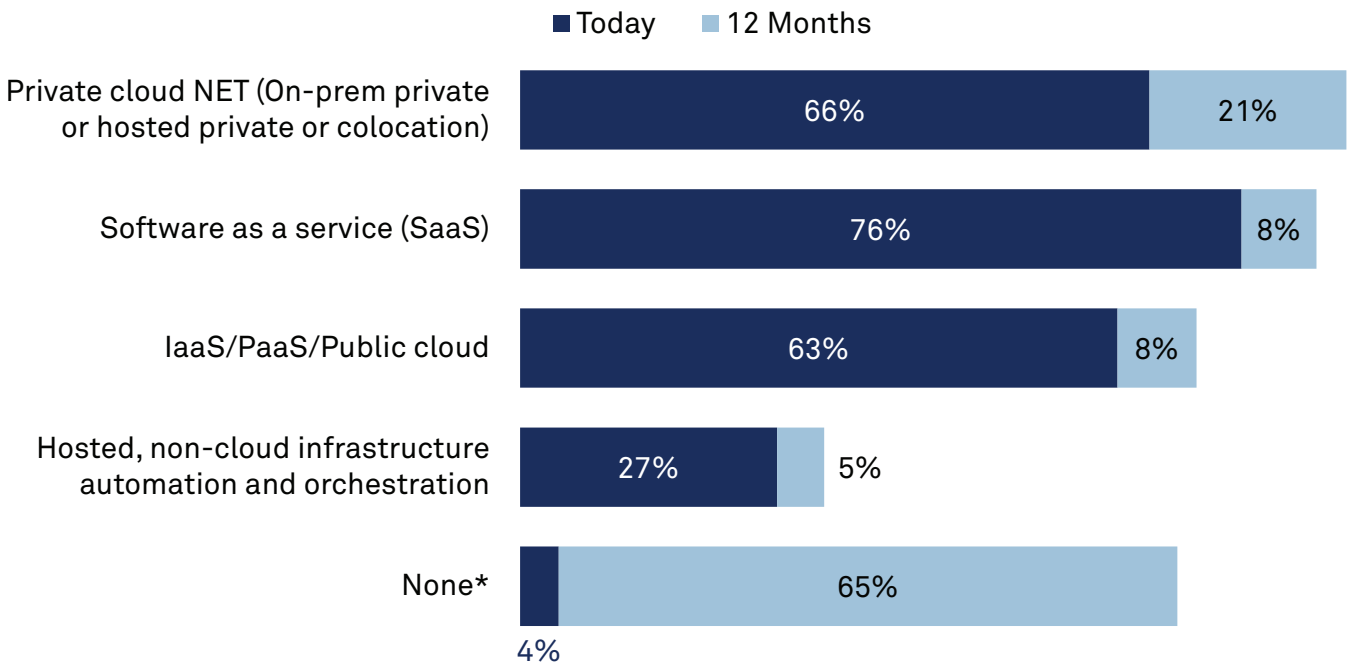
There are subtle but important distinctions between automated network management and network automation. Automated network management is what IT has been doing for years – writing scripts or using software to carry out bulk actions such as updating firmware, performing configuration management functions, and even deploying VLANs and networks across the datacenter and campus. Network automation is different because it is a holistic strategy across all network functions and is responsive to change. Network automation is workflow-driven, and it provides automation solutions or 'infrastructure as code' to handle the heavy lifting of configuring network elements end to end.

It's important to emphasize that in both the automated network management and the network automation models, IT is *always in control* of defining how changes are made and in setting any required policies that must always be in place.

Network Automation Drivers

Enterprises use a variety of on-premises and colocated datacenters along with cloud services (see Figure 2). They are gaining experience regarding which application environments are best suited for which workloads and applications. The use of hybrid cloud, which we define as an IT environment that leverages both on-premises systems and off-premises cloud/hosted resources in an integrated fashion, benefits the organization because it can select the best environment to run specific applications. However, such flexibility complicates network architectures because applications are distributed across multiple environments.

Figure 2: Hybrid Cloud and Multicloud Will Be with Companies for the Foreseeable Future



* The 'None' category is high because the majority of those respondents indicated no change in their cloud use in 12 months.

Q: Which of the following types of cloud or hosted services, if any, does your organization currently use? Which does it expect to use in 12 months? Please select all that apply.

Base: All respondents (n=444)

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets & Outlook 2021

For example, each cloud service has its management portals to allocate networks, provide services such as addressing and address management, interconnect to other instances the enterprise owns, and to use advanced networking services like load balancing and high-reliability services. In addition, enterprises can use virtual instances of products acquired from their networking vendor as a VM or acquired through a cloud service storefront and deployed within that cloud service. None of these tasks is complex (by design), but when taken as a set of actions that need to be executed to define a network in two or more services, it becomes a time-consuming and error-prone task.

The reorganization of IT around functional DevOps teams fosters collaboration among IT disciplines and is smoothing the way for network automation and integration. Developers are accustomed to using infrastructure like servers and storage as foundational elements for their applications and can often create them on demand once the underlying infrastructure is configured for automation. The goal is for the network to become a service to the application teams so that it's ready to be configured and provisioned based on the demands of the application. The network becomes a component of the continuous integration/continuous deployment pipeline that moves from development, through test and finally to production.

The reorganization of IT around functional DevOps teams fosters collaboration among IT disciplines and is smoothing the way for network automation and integration.

Edge and IoT are also driving IT to network automation. As the number of IoT devices grows from the hundreds to the thousands and tens of thousands, network connectivity, provisioning, monitoring and management will have to be automated to keep up with the scale of devices. This is an area where network IT has some experience with en masse offerings like laptops and mobile devices and business tools such as printers and IP phones. Network automation streamlines the onboarding and device lifecycle for IoT while being governed by IT policy, but without the need for constant staff time to manage all of it.

The outcome of the variety of application environments in use by enterprises shown in Figure 2 is that the network connectivity in the datacenter, the cloud and across the WAN is complex and getting more so with each new service that is used. At the same time, it is an essential underlying technology to hybrid cloud computing. With a thorough understanding of the networking capabilities available in different cloud environments, IT can create automated, reactive workflows that will select the proper components in each environment for a fully provisioned network.

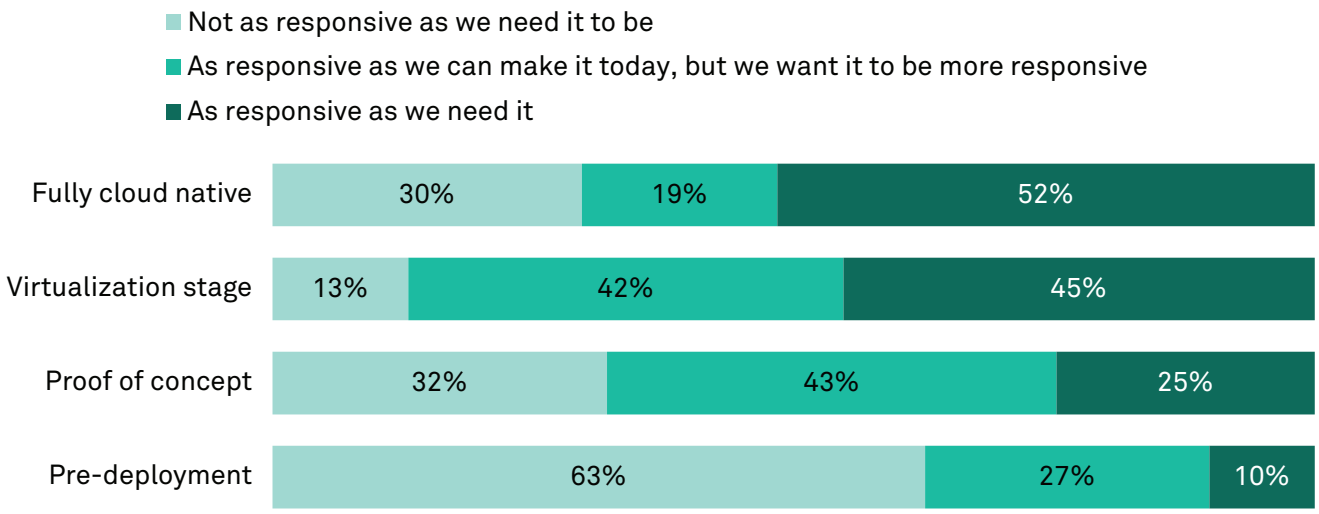
Network Automation Is Critical for Success

A chain is only as strong as its weakest link. Enterprise IT is only as agile as its least automated process. Measures of IT agility are how responsive the network is to configuration changes, how quickly a change request can be executed, and how fast changes are deployed across the network. Foundational elements, like networking, can hold up an application deployment. Naturally, there are provisioning tasks that simply take days or weeks to complete, such as provisioning a new WAN circuit or adding more network hardware to an on-premises or colocated datacenter. However, in a well-run IT organization, teams can anticipate those types of changes and plan for them so that the circuits are ready when they are needed. The types of changes we are talking about here are the provisioning and configuration of existing hardware and software.

Enterprise IT is only as agile as its least automated process.

It should be no surprise that the closer enterprise IT is to being fully cloud native – meaning the DevOps teams are collaborating well and working efficiently, and every stage of an application lifecycle is automated – the more responsive the network is to change (see Figure 3). In a recent 451 Research study commissioned by IBM, 52% of respondents said their cloud and virtual network technologies are fully cloud native, and they indicated that their networks are as responsive to change as they need them to be. In other words, the speed of change in the network is meeting or exceeding expectations for about half of respondents whose IT departments are fully cloud native. The work those organizations undertook resulted in quicker deployments and more workflows optimized for efficiency than before they started.

Figure 3: The More Fully Cloud Native the IT Department, the More Responsive the Network Is to Change, But There is Room for Improvement



Q: How dynamic and responsive is your network to change?

Q: How would you characterize your organization's progress in its effort to deploy cloud and virtual networking technologies as part of an overall network architecture?

Base: All respondents (n=387)

Source: 451 Research custom study commissioned by IBM

On the other end of the spectrum, for those in the pre-deployment phase of cloud-native and virtual networking, only 10% said their networks are as responsive to change as they need them to be. The reason for this, we believe, is that they are likely still using many manual processes for management. Manual processes are a holdover from the days when datacenters were generally static environments and the requirements needed by applications didn't change often, if at all.

The days of managing from the command line interface (CLI) are coming to an end. The workflows that result in CLI changes are inherently error-prone because administrators must enter complex commands without mistakes or typos. Any misstep along the way, such as using the wrong command syntax or missing a critical configuration step, can break the network and delay deployment. Enterprises have developed change management processes – such as performing peer reviews and approvals for all changes, creating pre-defined plans to back out of changes, and developing workflows to fully restore configurations if a change is catastrophic – in an attempt to reduce the chance of errors and recover more quickly, but all of those manual processes add time, so making changes themselves increases the chance of introducing errors.

The days of managing from the command line interface (CLI) are coming to an end. The workflows that result in CLI changes are inherently error-prone because administrators must enter complex commands without mistakes or typos.

All of this work and experience on manual change management is not wasted, however, because it becomes the foundation upon which network automation becomes possible. Note that in Figure 3, the group that identified as 'fully cloud native' and indicated the network 'is as responsive as they can make it today but want it more responsive' dropped by more than half to 19% compared to the proof-of-concept stage and the virtualization stages. This means the fully-cloud-native group crossed the chasm to networks that are responsive to change. Responsive to change doesn't mean immediate change; it means fast enough. Fast enough is efficient, and that's the goal.

One of the benefits of cloud computing is self-service, where developers can deploy infrastructure in clouds with a few clicks of a button. With the proper governance, the network can be just as responsive via self-service. Network IT and developers collaborate on automation, which defines the guardrails users have when requesting a resource. As with other IT resources, the network can be allocated to groups and monitored for performance, and proper security controls can be put in place so that developers and application managers can deploy and test in a live environment. Reaching a level of self-service enables other teams to be efficient and is a significant contributor to IT's success.

Enterprises don't want rapid change that is also error-prone. With network automation, network administrators, along with developers, spend their time building automated workflows with logic that will determine the state of the network, figure out what changes need to be made and then make them. Error handling can include everything from stopping the process and raising an alert to backing out of changes that have already been made, thus returning the network to its prior state. These are all steps network teams formally or informally perform today. If things go wrong, network automation enables IT to perform root cause analysis faster because time-consuming tasks like data collection and analysis can be performed automatically, saving hours in an investigation.

One of the benefits of cloud computing is self-service, where developers can deploy infrastructure in clouds with a few clicks of a button. With the proper governance, the network can be just as responsive via self-service.

What to Look for in a Platform

There is an array of platforms to choose from, but there are a few key points to consider when automating the network. It's important to understand both the capabilities of the product today and the product roadmap to ensure that it will match your plans. The following are some things to look for in a platform:

A model as a single source of truth: A network model is critical for network automation and mapping out network topologies and network functions so that the automation platform can expose the capabilities of the managed networking products and services and run pre- and post-automation validation. For a consistent view of the network, ideally, there is only one network model that is used by multiple network management functions. The model must be self-updating so that it captures changes from within the automation platform and from external process and doesn't drift away from what is expected to be deployed. The model should integrate with existing IT systems like configuration management data bases, SDN platforms, clouds and other software that can either add to the model or have their own models.

API creation and integration: Automation platforms leverage northbound and southbound APIs to communicate with network devices and services. East/west APIs facilitate integration with IT orchestration systems, service desks, network monitoring systems and other IT support systems. A critical integration feature of network automation is the ability to create and manage custom APIs that call workflow automations built with the automation platform. These API-enabled workflows are used by broader IT systems such as self-service provisioning, CI/CD pipelines, etc. Enterprise IT or developers can share their automated workflows with others through the API to enable smoother integration. The automation platform must support security features for these APIs, such as authentication, access control and encryption, to protect the automation system from misuse, and they must have auditing capabilities to trace API usage.

Integration with a broad set of products: The more products the automation platform has integrated out of the box, the more likely enterprises will find alignment between the networking products and services they currently own or will own. The ability to integrate missing products is also critical because there may come a time when the organization has a networking product that needs to be included.

Integrate islands of automation: Many networking products and services have their own automation systems within their products. Look for offerings that can automate your applications and devices directly, deliver automation across a full process so you don't have silos of automation, or can orchestrate changes across those other automation systems in cases where it is more efficient and effective to allow the vendor's own automation system to carry out its commands rather than recreating those capabilities.

Monitoring and tracing tools: With an automation system, being able to understand the automation steps and results is critical both when developing new automated workflows and when they are in operation. Much like a developer will use debugging and visualization tools to understand program flow, the network automation system needs similar tools so that issues can be identified, understood and resolved quickly. Having overall system monitoring capabilities, such as for health status, the number of jobs running and current scheduling status, helps in maintaining a reliable network automation platform.

Conclusions

Network automation offers a number of benefits to enterprise IT and to the staff that builds and uses it. Automation is necessary for any organization that wants to complete its cloud-native journey. The time savings for both network staff and those that depend on the network can accumulate into the thousands of hours per year as organizations get closer to a fully realized network automation platform. Network automation should be deployed in a controlled fashion. For example, in a 451 Research study, an engineering manager at a financial services firm said, "There's been a general initiative around automation for probably at least the last two years… We have [several] things that we've done through other tools that automation is fully progressing and working."[1]

Network automation offers a number of benefits to enterprise IT and to the staff that builds and uses it. Automation is necessary for any organization that wants to complete its cloud-native journey.

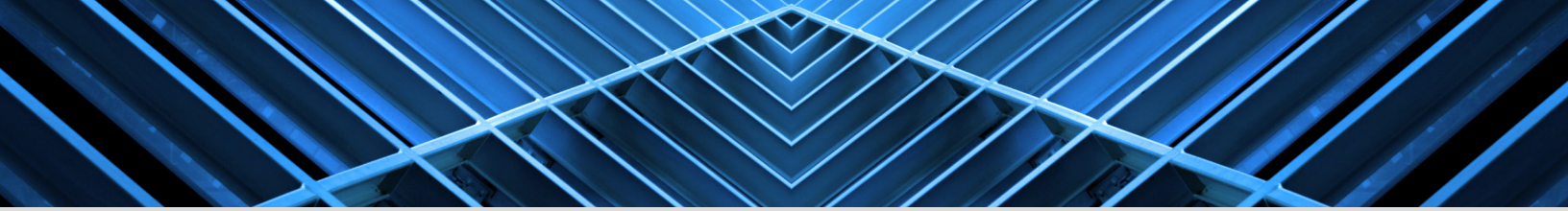
Starting with small, well-defined and well-understood projects – perhaps a workflow that is a simple but often-repeated task – gives IT teams the experience and confidence to think about automation and all the details that make it work well. Think of a network engineer being freed from repeatedly having to perform the same boring task. By picking a simple but often-repeated task, the benefits of automation become clear.

Application architects and senior developers who have experience in long-term project planning and delivering product roadmaps can help by creating a well-thought-out plan for success by managing the growth and complexity of network automation over a three-to-five-year timeline. For each workflow that is automated, more time is saved that can then be allocated to automating other workflows.

To be successful, network automation must eventually integrate with the rest of IT. From that same Digital Pulse survey, a senior manager from a financial services firm commented, "A lot of [projects delayed with the pandemic] were automation projects, things that are trying to replace manual procedures with more of a computer-digitized approach to doing those particular tasks… We were beginning to think about the digital processes across the firm as a whole." IT automation reaps more benefits when entire processes are automated, and that means integration across a variety of technology stacks. Enterprise IT must ensure there are existing integrations or a roadmap for adding integrations when they are needed.

Set realistic measures for success. For example, significantly reducing the time it takes to execute multi-stage workflows is achievable. Start by estimating how long it takes to execute multi-stage tasks, such as provisioning network services and connectivity for cloud-based applications. Set a goal to reduce that time by 80% via automation. Then measure the cost estimated in hours recovered to show the benefit of automation. Similar metrics can be tied to reducing downtime due to errors, time to recovery on network issues and so forth. Set reasonable goals from the start and work toward them.

1. 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey October 2020



content provided by: Red Hat

Red Hat Ansible Automation Platform is the foundation for building and operating automation services at scale, providing enterprises with a composable, collaborative and trusted execution environment for a broad variety of network and even full cross-domain IT processes. Ansible Automation Platform brings extreme flexibility in automating a wide variety of IT needs especially across operational "silos," as well as analytics, discoverability and governance to make automation faster to deliver and easier to govern and manage. A robust set of certified, reusable automation content can help create new network automation and other projects more quickly and in line with compliance needs. When these automation projects are combined, organizations can automate end-to-end processes, transform the way they work, and realize benefits such as great speed, agility and faster delivery of innovations.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence