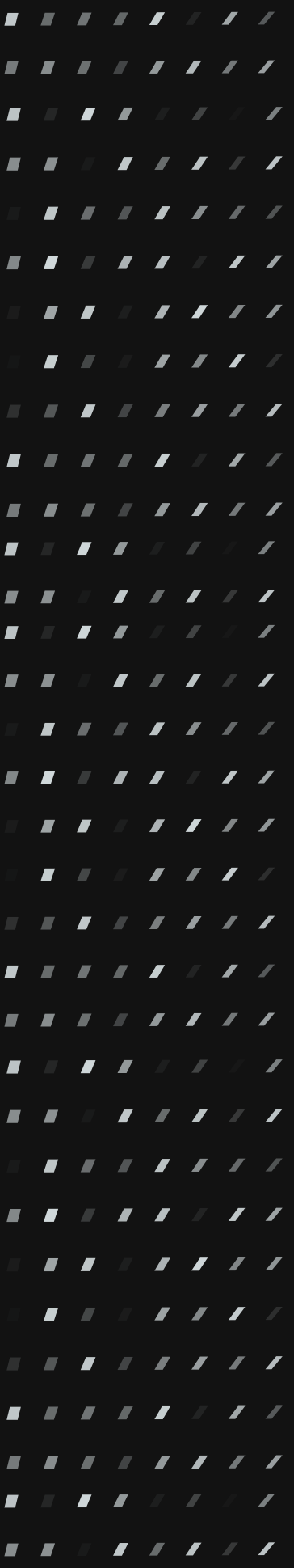
BACKBOX

WHITE PAPER

Network Engineer Buyer's Guide for Automation Solutions



Introduction

The network automation buyer's journey is not for the faint of heart. While automation solutions for network teams can deliver rapid value to network operations in the form of enhanced security and time-savings, the marketplace is filled with options... from roll-your-own scripting to complex automation orchestration. Making the correct choice requires assembling the right expertise within the enterprise – a buying team with the technical and operational knowledge to evaluate each solution for its suitability in meeting an organization's specific needs and business objectives.

Network engineers play a critical role in this process of fact finding – knowing the benefits and limitations of each option, what features to look for, what questions to ask, and what pitfalls to avoid. This guide will help the technical buyer navigate all these considerations, with real-world examples to illustrate how network automation should ideally work within the enterprise. Our goal is to support decision-making and empower the buyer to confidently choose the network automation solution that best suits the needs of the organization.

> **While there is no single formula for choosing the right automation platform for network teams, it is possible to isolate key criteria to ensure maximum efficiency, security, and value for the organization.**

Five Questions Network Administrators Should Ask When Assessing Current Systems

Making the right choices in network automation requires asking the right questions up-front about your current systems. These five questions can help baseline existing capabilities – and clarify how to best evolve them with network automation.

1 What network automation tools do you currently have in place?

Do you have legacy tools that were bought to automate network changes but that have instead fallen out of use? Do you have homegrown scripting that could be updated to handle new requirements, but find that there's never enough time to work on improving the tools? Do your cloud teams leverage a cloud automation tool that could be connected to your network automation strategy? Taking an inventory of the tools you have is a great place to get started.

2 What other tools are in your network operations stack?

Do you need to integrate your network automation capabilities with the rest of your NetOps tech stack? Will you need to integrate with a service desk tool? Are there NetOps-oriented automation use cases within the scope of this automation project?

3 How ready is your team?

Are you understaffed? Is there someone on the team with deep python skills whose role includes time allocated for scripting? Or do you need a turn-key solution that doesn't require scripting skills? Do you have time to create scripts, or do you need an out-of-the-box solution that works quickly? Has someone been specifically selected and trained to become the network automation expert or to act as an automation team lead?

4 Have you defined and assessed the management scope?

Which parts of the network will this automation project touch? Are all those parts routable from a single location? What kinds of devices are present? Which versions of TCP/IP are in use? Do you have a current inventory of all your network devices? How standard are device configurations today? Questions like these can help define and narrow the scope, an important step in any successful network automation project.

5 Do you leverage any of the vendor-provided configuration management tools?

In some cases, working with the tools provided by your hardware vendors can offer significant value. If your team highly leverages these types of tools, then understanding how they can be integrated with your overall network automation strategy is a key part of building requirements for a successful project.

> **Look for a solution that enables automated backups, and that automatically validates each backup to ensure the integrity of the restore process. The restore should be simple, as easy as 1-click.**

Kicking the Tires: Key Criteria for Evaluating Network Automation Options

Because the network automation marketplace offers many choices, buyers must do their homework on capabilities, performance, and solution strategy. Each organization will have their own requirements, especially when it comes to scope and scale of the implementation.

While there is no single formula for choosing the right network automation solution, it is possible to isolate key criteria – some must-haves in your network automation to ensure maximum efficiency, security, and value for the organization. Here are four core capabilities to assess, including industry relevant examples, when evaluating the merits of a network automation solution.

Industry Example: Global Manufacturing

Automated reliable backups with single-click restore

Network automation solutions should provide simple, automated reliable backup that makes it easy to restore in the event of an emergency. Each backup should be tested to ensure it's a valid backup that's in a restorable state. Before restoring, the backup should again be validated to make sure the restore file hasn't been corrupted. The restore process should be simple to initiate and should be complete – meaning the restore should work even if restoring to bare metal.

This reliability and simplicity should remain the case regardless of how many multi-tenant sites and service providers are involved. Look for solutions that enable automated backups of all the devices on the network, can schedule and store any number of configuration backups for as long as needed wherever you want to keep your backup files, can automatically verify backup processes, and provide a single-click restore.

Your goal is to eliminate the need for manual or scripted backup procedures while pulling all the configuration files required for recovery and storing them in a central and secure location.

Challenge:
A large, global manufacturing company needed a platform that provided consistent, scheduled backups that could be reliably used to recover devices when they failed or when unwanted configurations were made to devices.

What they did:
The company set up a list of requirements and found several vendors that matched their requirements.

Outcome:
The company was able to run through a proof-of-concept in their lab environment, develop a test plan of their scenarios, and work with a proven vendor that showed them the value of an open platform that integrates securely in their environment.

Industry Example: Regional Banking

Task Automation

Robust and flexible task automation is a must-have for any Network Automation solution. This requirement becomes especially critical at scale. A task may be as simple as adding or removing an administrator from devices, or as elaborate as performing complex automated upgrades or hotfixes to multiple devices with the single click of a mouse. Look for solutions that offer a set of pre-configured tasks that can alter configuration settings on multiple devices.

Tasks quickly become unmanageable in scenarios where you need to push a configuration to a large number of multi-vendor devices. Your solution should be able to adjust operating system level parameters, access lists, policy changes, routing, and many other common configurations seamlessly, across numerous devices at one time. Also seek out options that can build custom chains of automation to complete either routine or complex tasks – for example, upgrading IOS while including post and pre checks – to simplify and make the process much more effective.

> **Tasks quickly become unmanageable in scenarios where you need to push a configuration to a large number of multi-vendor devices.**

Challenge:
A regional bank was faced with constant, unapproved changes to device configurations that were causing service impacts to their customers and users.

What they did:
The bank implemented a platform that can take snapshots of configurations from a central, virtual machine – allowing visual display comparisons of configuration files, by device and by file, to identify specific daily changes to configuration files.

Outcome:
The tool was able to save valuable time-to-recovery by providing a daily report of only the devices on which configuration changes were made in a specified time frame. The configuration could be quickly and confidently reverted and applied to restore the device to its prior working state.

35%

According to Gartner as of 2022 less than 35% of network activities are automated

Industry Example: Telecommunications

Network Inventory

Network inventory is much more than a snapshot of assets that make up your network. Your network automation solution should allow a deep inventory of assets that allows you to gain practical, actionable insights. For example, can you tell which devices are at their end-of-life (and no longer getting security updates) so they can be aged out of operations? Can you tell which CVEs apply to your devices so that you get an accurate assessment on the vulnerability state of your network?

Choose a solution that can automatically grab network information that allows you to build a rich inventory that helps you administer your network devices. The inventory collection should be highly performant and scale to even the largest networks.

Challenge:
A global telecommunications service provider needed a solution that could help position the organization to win services business in competitive bids across unknown network environments.

What they did:
They evaluated vendors that could do the basics of administration, like backing up devices simply and reliably, and also that had a rich set of flexible inventory collection features.

Outcome:
They selected a vendor that had out-of-the box inventory reporting and allowed them to customize data collection to suit their specific needs. The reports were generated at the same time as nightly backups were completed, and as such didn't add any performance overhead to the network. As a result they were able to move with certainty when exploring new business opportunities, price engagements more accurately, and quickly win new business.

Industry Example: Global Services Company

Operational and Security Audits

The right network automation solution can support pre-emptive health checks on network devices to prevent problems and verify proper operations before an issue affects the network. It's important that any measurable data collected during these checks can be reported on and viewed over time to streamline ongoing device administration such as upgrades, replacements, and routine configuration changes.

The best solutions come with a predefined automation library that can make it easier to check the health of your systems. Operational checks can help company with company or industry policy standards, such as HIPAA, STIGs, or CIS Benchmarks, as well as automate remediation.

Challenge:
A large global services company needed out-of-the-box functionality to satisfy requirements for replacing a legacy solution and building a set of network health check automations for one of their large customers running a variety of network devices.

What they did:
They went through their current vendor list, identified shortcomings, and put together an RFP with a checklist of devices they needed to be supported.

Outcome:
They selected a vendor that was able to demonstrate a prebuilt automation library that satisfied most of their needs, and had a service offering that enabled them to partner on building more without any extra cost.

> 300,000
>
> According to Gartner, IT system downtime causes an average loss of $300,000 per hour.

Additional Considerations

This is just a partial list of some key capabilities that define a superior solution. Generally speaking, your network automation solution should be easy to implement, and you should get to value quickly from the platform.

It's important to vet each network automation solution for how well it solves the challenge organizations face in minimizing the human element in infrastructure management. The right solution can save time, facilitate scalability, and free up time to focus on more strategic tasks. With automation, network engineers can devote more time to strategic activities like R&D or growth-related initiatives, instead of administrative work like updating configurations with manual, error-prone scripts.

Inventory management remains critical. Your solution should be able to regularly pull necessary asset information for a dynamic list of devices associated with the network – generating custom workflows and reports that are automatically populated and updated with each backup. Related to this is the need to standardize procedures and streamline knowledge transfer to avoid "homegrown scripts" and other bottlenecks from excessively manual processes.

The networking automation solution itself should stand up to the scrutiny of industry standards and methodologies for security and compliance. This will ensure that, as your solution goes to work in your IT environment, the integrity of your information assets is maintained, your business risks are reduced, and data remains protected.

Navigate the Network Automation Space with these **10 Vendor Questions**

1 What types of vendors do you support?

Be sure to steer clear of solutions that only work with a narrow slice of potential vendors. The best network automation solutions will be vendor agnostic and support a best-of-breed approach comprised of devices from hundreds of vendors.

2 What are the types of automation you support?

Avoid being limited by solutions that still require scripting, as there is a lot of overhead in managing the scripting code infrastructure and those skills are hard to find in network engineers. Instead choose a solution that delivers no-code automations and has a pre-populated automation library that allows you to get to value quickly.

3 Does the solution have verification steps to confirm an automation has been successful?

Select a solution provider that verifies the successful completion of automations and enables you to easily troubleshoot and report when automations fail to run, or run completely.

4 What is the process for adding or customizing automations?

Do you have to work with the vendor to add new automations or customize existing ones? Will the vendor help you write automations as part of your support contract, or does creating automations require a costly professional services arrangement?

5 What level of customer support do you offer?

Is your vendor knowledgeable about all the different products you might automate? Will they help to create new automations to save you time and effort? Do they offer flexility to add new supported devices should you need them?

6 What about automated OS Updates?

Does the solution support multi-step updates? Can updates be automated in a way that eliminates the need for after-hours work? Can backups be integrated into the update flow so that you ensure the integrity of your network, and can easily roll-back in the event of a failed update?

7 How simple is your licensing model?

Look for a vendor that can easily explain their licensing model and has no hidden suprises based on the number-of or types-of devices you need supported. Look for a vendor that's not dependent on heavy professional services fees to get your project up and running.

8 Which environments and third-party integrations can your solution support?

Make sure you're not falling for a network automation solution that boxes you in to a limited or closed ecosystem. Your solutions should work in multi-cloud environments and on-premises with any type of VM, VMware, Hyper-V, Virtual Box, or other platform. And it should offer REST API code examples to incorporate with third-party solutions and ticketing systems.

9 Can your system support centralized device management?

Look for solutions that can push configuration to multiple devices, onboard devices to the network, and keep them up to date. Capabilities should include real-time dynamic inventory information and reports for all devices. Look for a solution that avoids polling, and has scalable distributed automation execution across the network for the best possible performance?

10 How does your platform enforce security and compliance policies?

Your network automation solution should help simplify compliance with industry, vendor, or regulatory policies. It should have some out of the box support for common standards like HIPAA, STIGs, or CIS Benchmarks. It should rapidly identify issues before they impact network and data integrity. And it should generate multiple types of reports including user reports, schedules configured, backup job configured, backup status, device inventory and more.

About BackBox

Backbox is a Network and Security Device Automation Platform that supports over 180 vendors, with thousands of pre-built automations and a scripting-free way to build new ones. Enterprises and service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance, BackBox gives you confidence that your automations will deliver the expected outcome every time.

Find out more at www.backbox.com