IP FABRIC

Regain Trust in Your Network with 8 Automation Dos and Don'ts

Control change, compliance, and security outcomes with confidence.

ipfabric.io ↗

Why The Automation Buzz?

As network demands grow, so too does the complexity surrounding management and operations. Drivers such as operational efficiency, stability, security, and compliance outpace individual and team manual capabilities, resulting in the need for new approaches and solutions.

The benefits of network automation are manifold but not without certain caveats. Automation itself can bring a set of challenges and risks that depend on the operating environment, available expertise, and alignment with business goals.

Once basic operational efficiencies are realized, network automation and assurance can further enhance security, compliance, and scalability. Teams are empowered to reduce manual work, and with their time and talent freed up, missed opportunities can be reassessed, allowing innovation to thrive.

In this whitepaper, we will explain some foundational elements and quick wins for effective and efficient automation-based outcomes. With these tactics and strategies, the force multiplier of network automation and assurance can be used to deliver more than just cost savings at the individual, group, and organizational levels.

The Automation Status Quo

In any growing modern enterprise, there are complex business and functionality requirements a network must meet, and this evolves and morphs into inevitable network diversity and complexity over time. Connectivity, performance, and security requirements compound. To meet these business needs, the network must be:

- Stable, efficient, and resilient on a day-to-day operational basis
- Cost-optimized and strategic around orchestration and resource allocation
- Proactively secure, observable, and compliant with regulatory demands
- Ready as the bedrock and foundation for ongoing change to futureproof for a range of strategic technology projects

But this requires exacting control of your environment, and many organizations don't have the broad, deep, and consistent understanding of their network to claim this control. Most CIOs admit to accepting a level of risk that wouldn't be acceptable elsewhere in the business, with 90% of surveyed CIOs saying they have no single network architecture model, and rely on a patchwork of incoherent knowledge to understand their environment.

Organizations rarely prioritize giving network teams the necessary tools, and technology-specific or vendor-specific tooling doesn't provide holistic network intelligence; thus, network teams don't know the whole truth about their networks. At IP Fabric, we've learned through experience with 150 of the world's most complex networks that without the right visibility tooling in place, up to 10% of a network estate (in device count) remains unmanaged, unmonitored, and vulnerable to exploitation In the traditional approach to network management, devices are understood and managed according to a singular function. Their interactions are recorded in static documentation, as are any changes to devices. Knowledge of network domains relies on subject matter experts alone.

**Device health is measured,
but overall network health is not.**

Legacy tools – such as traditional real-time monitoring or static documentation tools - fall short of providing operators with an end-to-end understanding of and insight into the current network architecture. This fragmented understanding begets a fragmented approach to managing and operating the network leading to inefficiencies, errors, heightened risk, and unplanned outages.

The natural result is a range of functional and security-related network vulnerabilities slipping through the cracks. frustrated teams become trapped in a constant state of firefighting, with no time to consider, plan, and implement more effective management strategies.

Network Automation has emerged as not just an optional strategy but a necessary one to maintain the continuous connectivity, security, and performance requirements of complex modern networks. The promised outcomes of network automation include:

Ensuring Business Continuity:

- Establishing operationally stable automation workflows and continuously measuring network behavior to validate and maintain stability and performance
- De-risking change management through eliminating manual errors, ensuring consistent configurations, and proactively understanding and modeling change outcomes
- Empowering proactive maintenance and rapid scalability in the face of variable demand
- Becoming an exception to the reality that most enterprises experience nine brownouts or outages every month, often lasting 12 hours (each) and costing $13M annually. (Source: Network World, reporting on SolarWinds study.)

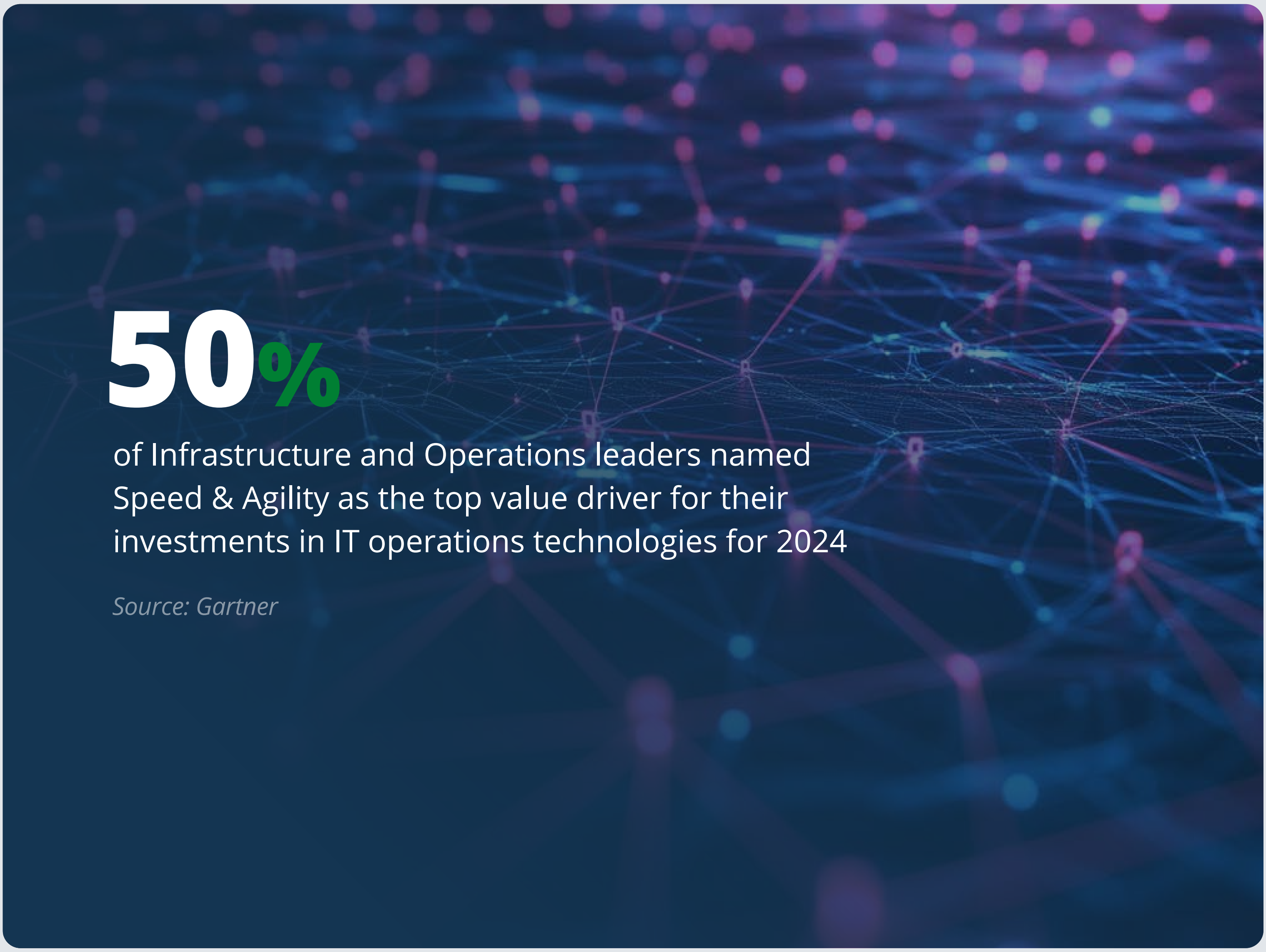
Proactively Mitigating Risk:

- Speeding up troubleshooting through automation-based error identification and isolation, and lower MTTR (Mean Time to Resolution) due to automated remediation. Gartner agrees that automating IT service management not only brings capacity gains, but improves speed, service quality, and mitigates risks by reducing the risk of human error (Source)
- Improved security due to better observability, orchestration, and detection engineering. Real-time intelligent responses are made possible based on a complete view of attack vectors, better network intelligence, and API integrations across platforms.

Accelerating Business Growth and Innovation:

- Eliminating repetitive, tedious manual work involved in documenting, diagramming, analyzing, and modeling the network which frees up time and talent for higher-impact projects and initiatives
- Expediting new network service provisioning by eliminating bottlenecks through self-service and automation-enriched workflows

In a Gartner survey, 50% of Infrastructure and Operations leaders named Speed & Agility as the top value driver for their investments in IT operations technologies for 2024 (Source: Gartner), with Resilience and Reliability following as second.
As described above, network automation is proven to impact both of these value drivers directly.



50%

of Infrastructure and Operations leaders named Speed & Agility as the top value driver for their investments in IT operations technologies for 2024

Source: Gartner

So, what's stopping you?

While it's clear to everyone running and operating networks day-to-day that automation is necessary, the reality is that most organizations do not have a mature, closed-loop automation practice. According to Gartner, 65% of enterprise network activity is still manual, but it's assumed that by 2026, 30% of enterprises will automate more than half of their network activities. In an EMA (Enterprise Management Associates) sample of over 300 enterprise IT professionals, only 18% believe they have a successful network automation strategy. Serious technical and cultural barriers complicate the path to automated network operations, most notably organizational consensus and risk aversion.

> "
> *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.*

Organizational Consensus

Many automation efforts are driven by individuals who suffer a lack of organizational support and alignment and, therefore, a lack of resources. Engineers on the ground, dealing with repetitive manual processes, are motivated to improve their workflows and streamline operational processes. They begin to lean on automation to do so, however, these self-built projects usually don't gather the necessary support or scale to make a wider organizational impact.

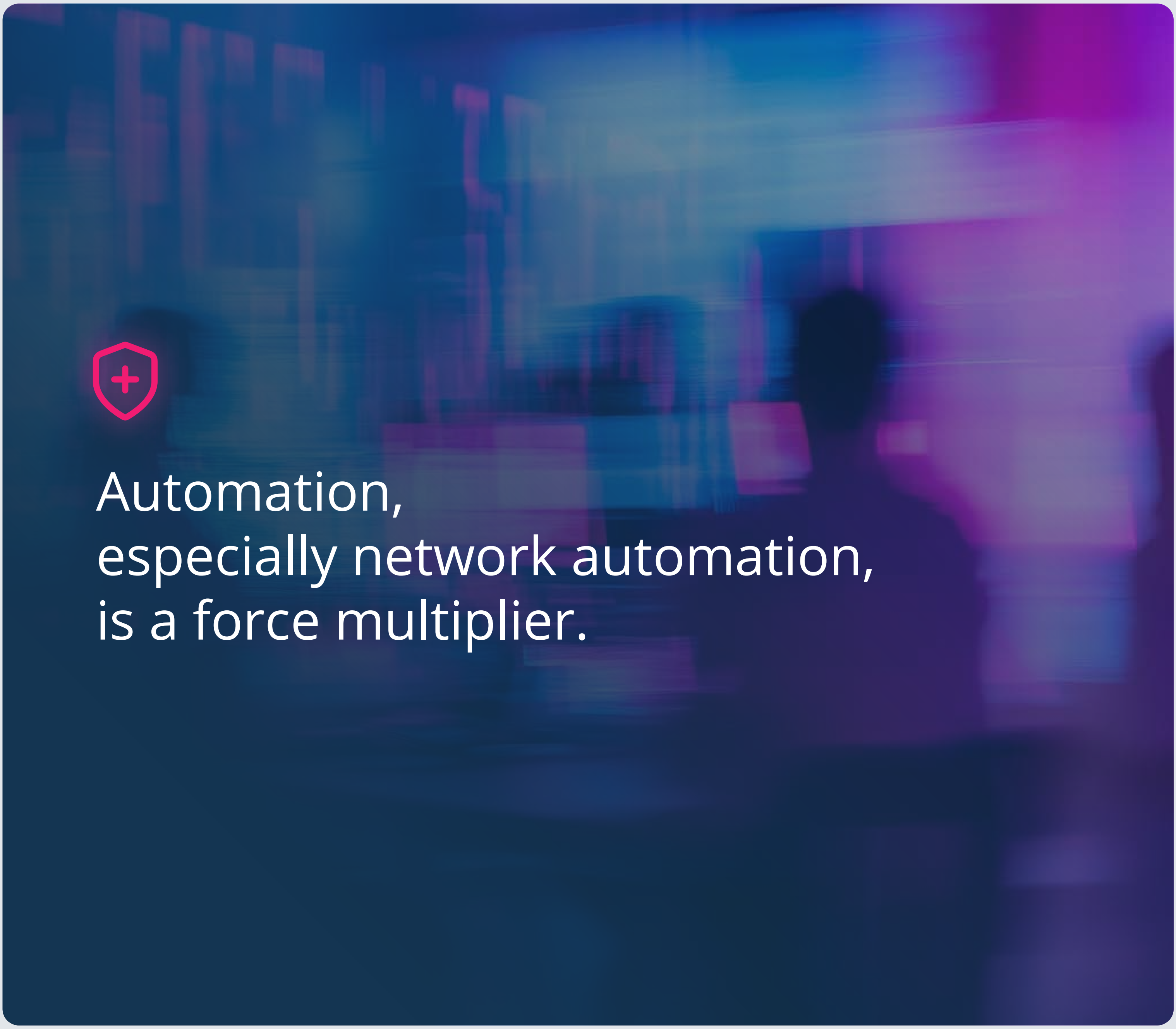
Without the relevant strategic Objectives and Key Results (OKRs), to align leadership and technical teams, these efforts flail along without the required buy-in and mandate. Individual initiatives tend to lack useful documentation and have little impact on established processes. Additionally, these projects risk abandonment without their original champions as individuals move on.

EMA found that IT leadership emerged as the top business challenge that IT organizations struggle with when trying to implement a network automation strategy: "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." (Source: EMA 2024). Enterprise business leaders must prioritize network automation as a strategic business initiative that deserves the necessary resources and attention to ensure wider success.

Risk Aversion

Automation, especially network automation, is a force multiplier. When done well, it can create positive generative effects throughout an organization. However, if a flawed process is automated, or certain outputs are not handled correctly, the fan-out risk can adversely affect large numbers of services and even propagate to other networks. Testing and simulating the impacts and outcomes of network automation becomes crucial, but many organizations have no means to do this and either blindly accept the risk or do not engage in automation efforts at all.

Infrastructure and Operations leaders appear to agree that the risk of stagnating is far greater, as according to Gartner, even though automation technologies like automated incident response.



Automation,
especially network automation,
is a force multiplier.

Where To Begin?

There may be a desire to automate and an acceptance of certain levels of risk, but there is frequently a lack of clarity on how and where to take the first step. Your first goal may be to improve day-to-day operational stability or efficiency; you may have a mandate to cut costs; you may be transforming your network to support new digitally delivered revenue-generating activities, but the best place to start is normally with low-risk “read-only” initiatives that increase the visibility, consistency, and augment the quality of frequently undertaken manual activities. But how do you even begin to collect, analyze, and clean the data you need to get started?

Automate With Precision, Clarity, And Confidence

IP Fabric proposes a three-pronged reference architecture for network automation. It offers a structured and safeguarded approach to network operations.

The first component is a network intent repository, often referred to as a Network Source of Truth. It expresses the intended state of the network in terms of inventory, topology, configuration, desired state, and application delivery behavior. These indicators are derived from the strategic business objectives and are used by the fulfillment component.

The second component, fulfillment, automates the configuration and policy changes across network devices to achieve the desired network behavior. This automation ensures:

→ Consistency across network sites, segments, and domains

→ Accurate delivery, verified by post-change network behavior testing

→ Scalable operations across the entire network in minimal time

Fulfillment may also respond to triggers from the assurance component.

The third component, assurance, models and measures the observed end-to-end network behavior, comparing it to the intended state. It gathers data on inventory, topology, configuration, state, and forwarding behavior to create a comprehensive model of the network’s actual performance.

It is essential to recognize that the assurance component assesses the collective network behavior, not just that of individual devices. Let’s look at 8 approaches to use as your springboard to an automated network environment, including some first-stop tactical actions you can take to ensure network assurance and automation become achievable and sustainable at the strategic level.

8 Ways To Break Ground On Network Automation

→ Today's Tactical Actions

1 Unify Network Visibility

2 Accelerate Troubleshooting & Root Cause Identification

3 Validate Change and Configuration

4 Fill Gaps in Your Tooling Ecosystem

→ Tomorrow's Strategic Outcomes

5 Secure a Growing Attack Surface

6 Build a Trusted Regulatory Compliance Programme

7 Retire Technical Debt

8 Enable Self-Service Network Provisioning

Today's Tactical Actions

1 Unify Network Visibility

Stop relying on stale states, manual checks, and static diagrams created in tools like Visio to understand, plan, or execute changes. You may trust your teammates, but human fallibility and out-of-date documents only give a partial and point-in-time view that cannot replace true situational awareness. Better observability is required to deliver better outcomes.

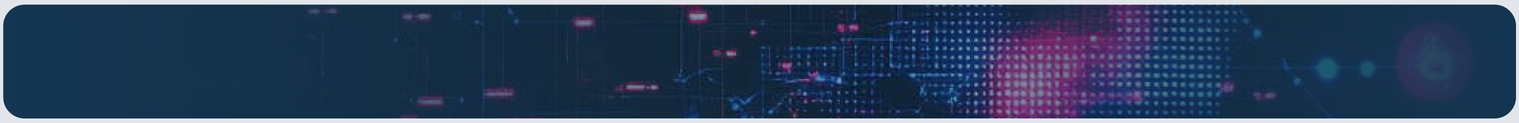
Enterprises and teams need the technical guardrails, speed, precision, and validation that automated visibility offers, especially for pre- and post-change validation. Automating network discovery, modeling, and visualization is an ideal first or early step on an automation journey. Doing this manually is inefficient and leads to fragmented, inaccurate network understanding, breeding false confidence and leaving critical vulnerabilities unchecked.

Take Action with Automated Network Assurance

Replace static spreadsheets and diagrams with a vendor-neutral, end-to-end automated discovery and modeling mechanism to validate and prove the state across all your network infrastructure continuously. This will reveal the key truths, risks, and opportunities in your networks.

To be effective, an automated visibility approach must:

- Provide a holistic view of the entire heterogeneous network through vendor-neutrality and end-to-end discovery
- Analyze and standardize diverse network data to compare like-for-like no matter which vendor, technology, or domain
- Be reliably accurate using specific discovery mechanisms that provide sufficient detail about network state and configuration (as using SNMP *(Simple Network Management Protocol)* is not complete enough).



Ideally, the data collected from the network would be presented in flexible ways for easy consumption and sharing by human or machine agents. Spending hundreds of thousands of dollars and multiple months on consultants to collect and prepare this data before transformation projects is not just inefficient but a waste of resources. Automated visibility and assurance is not just smarter but safer and becomes an ongoing nexus for automation and operational efficiency gains throughout a lifetime of change.

Take note:
Visibility is the foundation and precursor to success with wider automation initiatives, as it forms the basis for the scoping and execution of all further etwork automation projects.

2 Accelerate Troubleshooting & Root Cause Identification

Cease being wholly reactive, manually looking for deltas, and being unable to see a holistic view of network state. Problems and incidents are predicated on configuration or state changes either upstream, downstream, or on-box, but when and where did they occur?

Incidents can have single or multiple aggregate root causes, and converging on answers can be a stressful and anxious endeavor, especially during high-priority outages. Operational teams are constantly under pressure to improve incident metrics which leaves little time for proactive automation and associated tooling Automation reduces MTTR (Mean Time to Resolution), but ongoing workloads often hamper teams' aspirations of implementing it strategically. A light-touch and frictionless way to start automating is required.

Take Action with Automated Network Assurance

Auto-generate and enrich IT Service Management (ITSM) tickets with key information to help diagnose issues quickly, consistently, and repeatedly, irrespective of who is on call. Network history can be used to isolate the root cause of application or reachability issues

Set up intent checks (rules to assess the delta between network reality and intent) that reflect your desired network state. For example:

→ When an intent check fails, use an established integration, webhook, or API call to trigger ticket creation in your ITSM (IT Service Management) platform.

→ Enrich these tickets with key network intelligence from your network assurance platform, such as relevant device or interface details, diagrams, or end-to-end network path lookups, including IP and transport layer reachability.

→ Catch MTU mismatches, non-redundant layer 3 paths, missing VLANs, and blocked ACL or firewall policies.

With network intelligence available programmatically through discovery, dynamic documentation, and modeling, a degree of automatic triage is possible; root cause information can be inserted directly, and automatically into tickets. Using webhooks, API calls, or pre-built integrations, ensure that your ITSM system can access and use key network data as needed. The need to hunt down specific root cause information is eliminated, and this dramatically speeds up time to resolution. Compounded over 10s, or 100s, or 1000s, of tickets, the ROI (Return On Investment) for automating this data collection is quantifiable and, therefore, easily justified.

3 Validate Change & Network Configuration

Don't overlook steps, impact functionality, or waste time attempting to manually validate changes when intended reachability (including path lookups/policy violations), and application outcomes can be automatically validated **before** actual configuration or state changes in production.

When one device's configuration is another device's state, small changes can ripple through forwarding tables and across networks, adversely affecting endpoints and services. With a multitude of changes to enterprise networks every year, each and every change opens up the risk of outages and incidents... If your only option post-change is to wait for something to go wrong, then you need to take steps toward proactively protecting your

Take Action with Automated Network Assurance

Automatically validate the entire network state pre- and post-change to de-risk change management and regain trust in the process.

→ Take an automated point-in-time snapshot of your network to establish and preserve the last "known-good" state, or a network baseline, pre-change.

→ Establish network intent rules, so that unwanted impacts of change will trigger a violation and alert you to problems.

→ Run a post-change network discovery to validate that your network is still able to pass traffic as intended.

Adding unplanned changes to the mix makes it even more complicated to quickly identify what went wrong without some form of automation that can be quickly accessed by operational teams.

Detect unplanned change with daily automated audits.

Create or select pre-built intent checks to configure a set of rules that your network must meet.

→ Set network discovery and snapshot creation to run on a daily schedule.

→ Every morning, review relevant dashboards to understand if and where any violations were found.

Bonus (for more advanced automation):

→ Have any violation trigger an automation workflow for remediation.

→ Learn more: Itential & IP Fabric

4 Fill Critical Gaps In Your Tooling Ecosystem

Refrain from having portions of your footprint running dark, stale, or out of compliance. Leverage assurance to amplify the efficacy of existing tooling.

Even with a huge list of tools to manage your network, there are still a multitude of gaps and inconsistencies that you can't control - not for lack of will or trying, but due to the limiting scope or focus of existing platforms. To manually populate and update these tools is a time-intensive task requiring full-time attention and precision. You can use automation to maximize the value of your tooling ecosystem and make existing investments more reliable, precise, and up-to-date.

Take Action with Automated Network Assurance

Automatically ensure the accuracy of your real-time monitoring tools. Realize true network effects by integrating platforms and workflows. Run a daily scheduled network discovery to get a full and accurate network inventory:

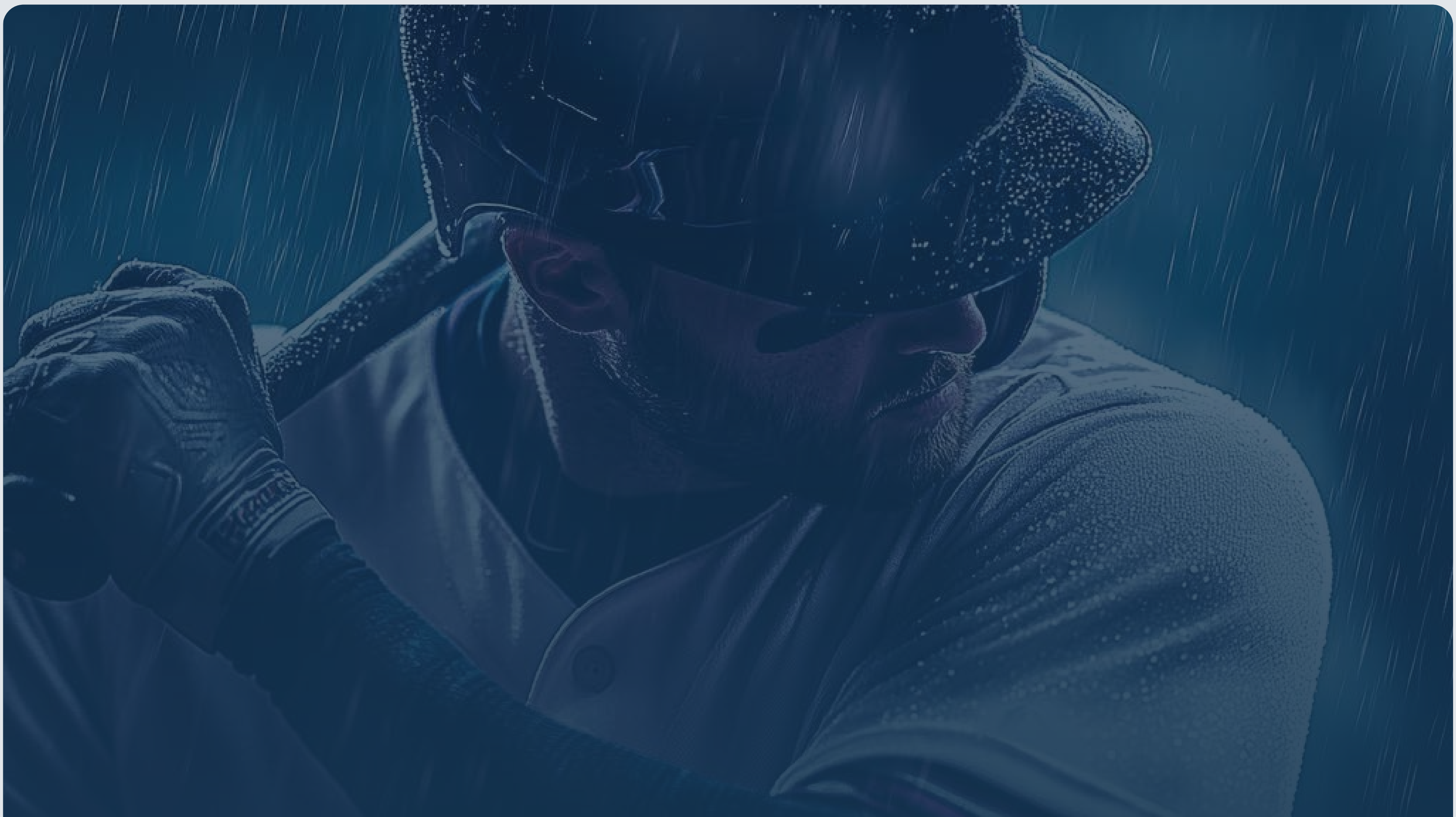
- Give your monitoring platform direct access to this freshly validated inventory via API
- If new devices are discovered, trigger an alert or workflow to initiate or enact updates
- Next, run automatic configuration checks to ensure that new devices have the correct credentials for monitoring and that desired access is allowed via any ACLs (Access Control Lists) or policy enforcement points.

Examples: PRTG & IP Fabric, Centreon & IP Fabric
You might use tools like spreadsheets, purpose-built software, or a CMDB to manage your network's desired state, known as the Network Source of Truth (NSoT), but it can quickly fall out of sync with the actual network due to inevitable changes.

Automatically populate and regularly update your NSoT (Network Source of Truth) tooling. Run a plugin, script, or API calls to populate a fresh deployment of your NSoT tool with accurate network inventory information obtained via detailed network discovery:

- Validate accuracy on a regular basis (e.g. weekly) by comparing your NSoT data to your latest network snapshot. Isolate differences to understand what changed.
- Synchronize this data so any changes or additions are reflected in the NSoT platform.

Examples: IP Fabric & NetBox or IP Fabric & Nautobot



SPOTLIGHT

Major League Baseball pioneers automation tech for digitally delivered sports entertainment and broadcasting

MLB's unique network environment is propelled forward safely and securely in the hands of Jeremy Schulman, Senior Director of Solution Engineering and Infrastructure.

He describes IP Fabric as a "force multiplier" in his automation tool stack. It not only provides the basic foundational elements of automation ("network automation requires discovery") but also paves the way for more sophisticated initiatives (democratizing access to important network intelligence via self-service ChatBot or automatically providing essential network diagrams to security teams).

Jeremy discussed his approach to automation at the Network Automation Forum Design Driven Network Assurance.

→ Tomorrow’s Strategic Outcomes

5 Secure a Growing Attack Surface

Don’t waste time trying to figure out if you’re vulnerable to current, aging, or blended threats due to vulnerabilities. Why give attackers any chance of getting a foothold or pivoting off your assets to penetrate deeper into your network?

As your network inevitably grows, so too does the landscape of vulnerabilities waiting to be exploited. Security observability is predicated on visibility, discovery, and asset management. The network sees everything and is the best vantage point to identify what is connected, where, and how. You may have confidence in your network security posture, but change is constant so your approach to security must be equally dynamic.

Proactively detect when any network devices are affected by published vulnerabilities i.e. Common Vulnerability and Exposures (CVEs). rather than waiting to be exploited and breached at great cost.

Take Action with Automated Network Assurance

Automatically validate your observed network infrastructure against CVE vulnerabilities to proactively harden your security posture.

- Perform automated discovery to create an up-to-date snapshot of your network
- When a vulnerability is published, compare network inventory to CVE data; take advantage of tools like PyNetCheck to identify at-risk devices.
- Use this information to begin remediation or kick off automated remediation

Example:
Were you affected by CVE-2400-3400? (CVSS Base Score: 10 Critical)

6 Build a Trusted Regulatory Compliance Program

Compliance is a subset of security but mandated for operating in certain domains and markets. This mandate can be useful and is a catalyst for action.

Consistent compliance with industry-specific or regional regulations, laws, and frameworks is simply part of working within certain markets or when providing specific services. You can, however, turn your compliance burden into an opportunity, by automating the associated tasks and processes.

In a digitally-delivered business, achieving ISO-27001 certification or readying for the EU's DORA (Digital Operational Resilience Act) or NIS2 (Network and Information Security Directive 2) touches a wide array of teams. Whether you are in financial services or part of the supply chain for any critical or important services, the network team can become a blocker if key intelligence about critical business functions and dependent services aren't readily accessible and consumable to those who need it.

Take Action with Automated Network Assurance

Use intent checks to verify compliance continuously.

- Build best practice intent checks that reflect a compliant network state. A strategic combination of checks can cover the requirements of multiple regulations.
- Perform daily, weekly (or on whatever schedule you choose) discoveries and modeling of your whole, or partial network, as it relates to supporting critical business functions.
- Be alerted to non-compliance with every network snapshot taken.
- Take remediation action or have alerts trigger automated remediation workflows.

Export automatically generated network analysis reports for inclusion in audits. Automatically update low-level network design documentation and network analysis reports on a schedule you choose (e.g. weekly, daily, twice daily).

- Export canned or custom reports for anyone who needs an understanding of the network OR
- Funnel this data into observability platforms or dashboards OR
- Add a self-service ChatBot on top of your structured network data so non-network teams can query the network and get quick answers.

7 Retire Technical Debt

Stop accruing technical debt with out-of-date processes and procedures. Begin to pay it down with confidence when removing or retiring configuration or infrastructure. Free teams from their historical shackles.

Improving performance while lowering costs is a constant business pressure applied to every area of an organization. Legacy builds, and historical decision-making becomes an expensive ghost in your network, making it difficult to spend on new strategic initiatives that would help you deliver a secure, stable, high-performance network at scale.

Continuing with manual processes — documenting, optimizing, and consolidating unknown elements — only adds to your technical debt. Automation is the key to gaining clarity, especially at scale or in complex environments.

Take Action with Automated Network Assurance

Automatically map the network to understand, plan, and take action on vestigial network architecture.

- Run regular, comprehensive network discovery to collect network state and behavior information and normalize it for consumption
- Identify unmanaged and unmonitored devices
- Model the network through flexible network diagrams to understand relationships, behavior, and interdependencies
- Execute change with automatic pre- and post-change validation in place to assure success or quick roll-back where needed.

Export automatically generated network analysis reports for inclusion in audits. Automatically update low-level network design documentation and network analysis reports on a schedule you choose (e.g. weekly, daily, twice daily).

- An accurate and complete Network Bill of Materials (BoM)
- A contextualized map and model of your network environment
- Confidence throughout your change process
- The runway to let go of vendor lock-in, outdated technology, and over-priced support and maintenance

8 Enable Self-Service Network Provisioning

Stop wasting experienced engineers' time with low-level tasks and checks that can be performed automatically with intelligent automation, which delivers faster results. Don't let already overworked engineers become the bottleneck for customer satisfaction.

With the introduction of structured network data and APIs instead of fragmented manual documentation, it's possible to build integrations and interfaces to give users direct access to the network data and services they need without having to raise information requests - using natural language ChatOps, email, ticketing, or any other method familiar to them.

Self-service can go further by placing automation workflows behind a UI which allows users to directly requisition or modify (within set guard rails of course) their network environment without having to use valuable engineering time or resources.

Take Action with Automated Network Assurance

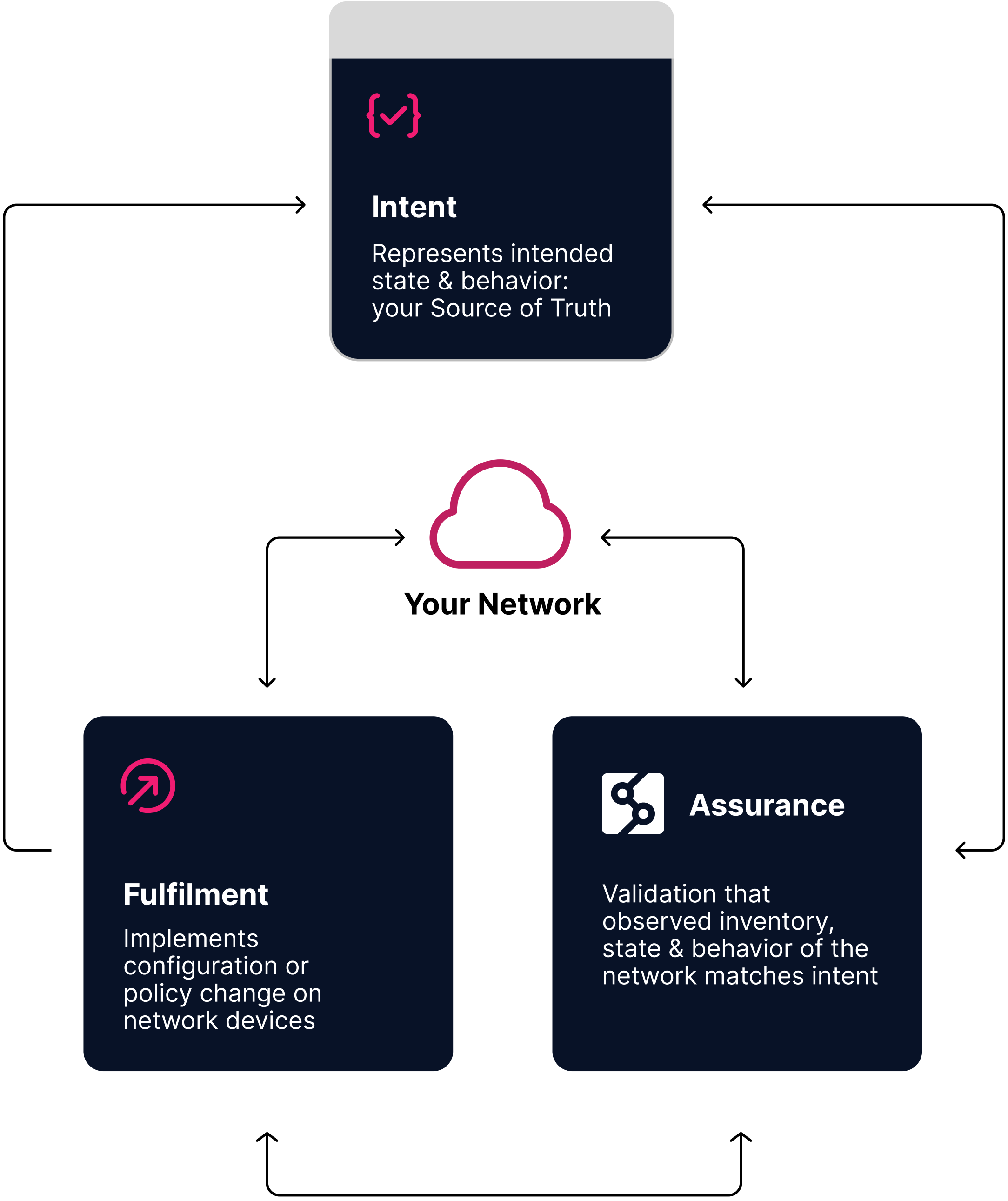
Query structured network data without needing subject matter experts to collect, interpret, analyze, and transform it into fit-for-purpose responses or network intelligence.

- Produce structured, normalized, and complete network data across technologies, domains, and vendors
- Take advantage of an open API or plugins to funnel whatever data you need to the right people, and let them ask questions about the network in plain natural language
- Integrate with automation fulfillment platforms to kick off actual change when needed
- Let users or internal customers request network services, e.g. firewall updates, deployment of new virtual assets, or propagation of configuration changes
- Validate the network post-change and report any change to relevant monitoring or observability platforms
- Update documentation to reflect the new network state

IP Fabric as your Network Assurance Solution

IP Fabric is the industry-leading automated network assurance that will help you execute these automation scenarios to achieve stable day-to-day network operations, cut costs, enhance your security and compliance projects, and set the stage for long-term strategic innovation.

As the Assurance element of a three-pronged approach to automation, it closes the necessary feedback loop required to automate safely, ensuring accuracy across your Source of Truth and Intent tooling while validating the effect of Fulfillment tools.



Intent

Represents intended state & behavior: your Source of Truth

Your Network

Fulfilment

Implements configuration or policy change on network devices

Assurance

Validation that observed inventory, state & behavior of the network matches intent

Without Assurance providing regularly updated insight into holistic network behavior, you might as well be automating in the dark.
IP Fabric is vendor-neutral and includes public cloud, producing the most complete network discovery output in a flexible and dynamic network model.

It's detailed, accurate, and complete in its discovery method, using the command line just like a network engineer would and discovering the network hop by hop. It's easy to use and quick to deliver value. Users take about 30 minutes to install and deploy IP Fabric and start their first discovery.

It's light on network resources. IP Fabric requires read-only access to the network and runs on a single virtual machine.

It's the ideal first step toward automation. For any automation efforts, you're going to need to gather the data that IP Fabric provides upon first network discovery anyway. Eliminating this time and effort (and the inaccuracies) while proving the value of automation to the business with an automated network assurance platform is the best possible use of resources for the modern enterprise requiring a stable and highly performant network environment.

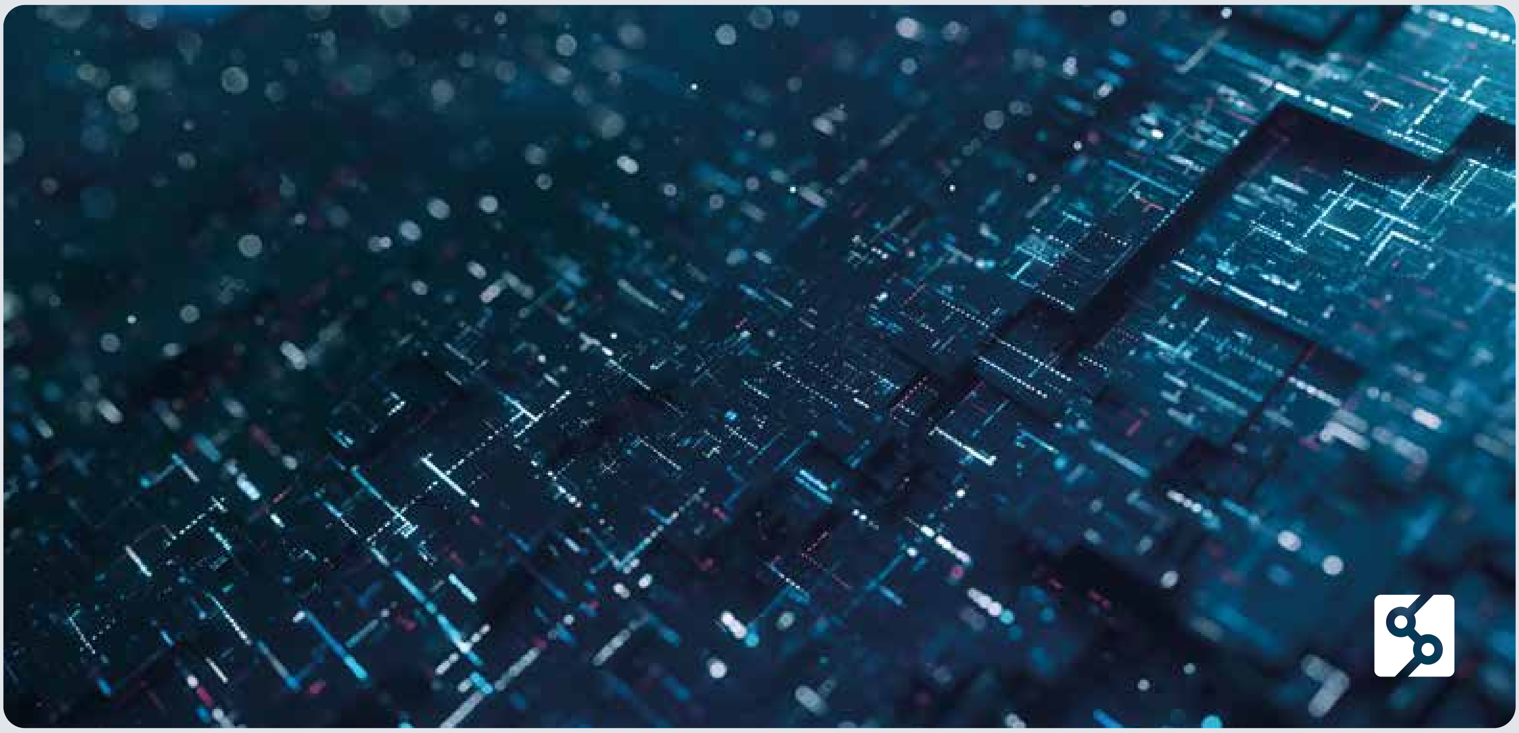
Learn from pioneers in automation
Airbus brings its "Automation Manifesto" to life with network assurance

The Airbus Connectivity Team was managing a large, distributed, constantly evolving network infrastructure, and needed a global, unified view to proactively manage stability, security, and outage prevention.

Leaders at Airbus knew automation was necessary for the technology to support the goals of the business.

Julien Manteau, at the time the Network Solutions Architect Lead, tasked himself with creating the Airbus action plan for automation. He proposed an ecosystem of open source tooling and one commercial non-negotiable; IP Fabric's network assurance platform:

"IP Fabric is a cornerstone of our automation strategy and a "must have" software for network management. We saw benefits from day one. It enabled us to consolidate internal tools into a single source, with a proper diagramming feature and extensive network data collection. Furthermore, the embedded network experience included in our predefined reports allows the operation teams to be more efficient in their day-to-day activities."



About IP Fabric

IP Fabric is a vendor-neutral network assurance platform that automates the holistic discovery, verification, visualization, and documentation of large-scale enterprise networks, reducing the associated costs and required resources whilst improving security and efficiency.

It supports your engineering and operations teams, underpinning migration and transformation projects. IP Fabric will revolutionize how you approach network visibility and assurance, security assurance, automation, multi-cloud networking, and trouble resolution.

Don’t take our word for it

See how assurance can transform your approach to network management.

Access the demo

IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+420 720 022 997

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io