

The NetBrain logo is positioned in the upper right corner of the page. It features the word "NetBrain" in a white, sans-serif font. The background of the entire page is a dark blue gradient with intricate, glowing white and orange/pink wavy lines that create a sense of motion and depth.

NetBrain

# Buying Guide for Network Automation

Network automation remains the largest unsolved IT challenge today. Network Operations have remained stagnant for decades, relying on labor-intensive, engineer-led tasks that struggle to keep up with modern, complex infrastructures. As networks grow, these outdated processes become the Achilles heel of IT service delivery.

However, a new generation of network automation platforms is changing the operations landscape.

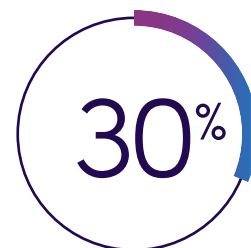
This guide outlines the key drivers for network automation, along with examples of how to automate in today's modern infrastructures to realize immediate operational excellence and scale. It also covers a structured approach to realizing network automation, including the use of no-code technology to democratize automation, the innovation of Intent-based management, and the structure and role of observability.

While production networks have grown in both scale and complexity over the past 25 years, the means to maintain these networks have largely remained tactical in approach and highly labor-intensive. Additionally, most large enterprises struggle to manage thousands of network service tickets per month to keep their production networks up and running at the level needed by the business. Putting these two facts together, the critical need for an entirely different approach is apparent.

A little-known fact is that while a huge volume of service tickets is generated each month, there are relatively few types of actual problems. If you take the concept of similar – it introduces an innovative approach that you could apply to solving many network problems of the same kind at scale.

And this fact is not lost on the industry analysts. According to the Gartner Market Guide for Network Automation Platforms report “By 2026, 30% of enterprises will automate more than half of their network activities, an increase from under 10% in mid-2023.”<sup>1</sup>

Scalable problem diagnosis automation remains the largest unsolved IT challenge today. And the tactical approach to NetOps is not just a philosophical issue, it prevents the business from growing. Truly supporting the business means changing this all-too-common brute-force NetOps paradigm to take a results-oriented and scalable view. While there are many tools that manage individual devices, those still suffer from the same traditional and code-based inefficient approach we have seen for decades.



**According to Gartner®,  
“By 2026, 30% of  
enterprises will automate  
more than half of their  
network activities, an  
increase from under 10%  
in mid-2023”<sup>1</sup>**

## TRADITIONAL “CODE-BASED” APPROACH

- Applies to primarily fixed environments which can be specified precisely at the time of project commence—devices, connectivity, and application requirements identified
- Focuses on device health and connectivity, not aware of any details of applications or service delivery required to support them
- Rigid programming projects, with detailed functional specifications
- Limited device-level abstraction; every vendor, model, and version must be treated separately and uniquely and code revised as device configurations are changed
- Requires DevOps, SECops, WANops and DCOps engineers, and NetOps engineers to work together, long and costly development cycles, excessive costs, rigid deliverables
- Challenges to scale since every situation, no matter how similar, must be programmed individually
- Focuses on interactive usage, rather than responding to external events or prevention
- Considered for only the biggest and most well-defined tasks that rarely changed

Instead, current buyers should be looking for automation platforms that focus on the delivery of network results. By taking a tops-down view of the network, you can verify conditions, diagnosis abnormalities and proactively enforce the production services it delivers. A no-code automation solution can streamline a variety of operational workflows including network performance and outage prevention, change management and problem diagnosis.

EMA research found that 64% of network automation leaders prefer low-code or no-code solutions to empower all personnel to interact with their automation solutions.<sup>2</sup>

Exploiting the management of many individual problems is done by treating them similarly with proper abstraction, network intelligence, and a means to re-use subject matter expertise. A solution like this would provide a concise understanding of how the network delivers 'intents' which are closely aligned with the needs of the business and its applications.

The best way to evaluate a network operation's platform is to qualify and quantify what you have today. Look at your Service Desk and see how the network operation's function is represented along with the volumes of tickets and the kinds of problems being seen. Above all, you need to understand your operational baseline and expectations when evaluating how network automation can help.

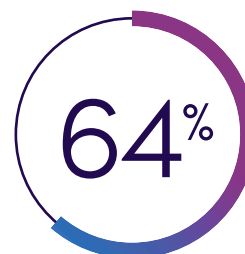
## Automation Drivers

Today's digital businesses are highly distributed and typically include hundreds or thousands of applications which span vast distances and organizational boundaries. The effectiveness and efficiency in the way an infrastructure is managed directly affects the overall success of the business itself. From the top down, the scalability of Network Operations is one of the single most critical factors in determining if the business is being supported properly.

Traditional help desks create service tickets for every issue, regardless of complexity. These tickets are then escalated through various engineer levels, with highly skilled engineers tackling the most critical problems. This approach becomes inefficient and costly as technology scales:

- **Manual and labor-intensive:** Thousands of tickets per month burden engineers, increasing costs.
- **Escalation burden:** Escalations to senior engineers add time and expense, especially for critical issues.
- **Slow response times:** Mean time to repair of almost two days hinders business operations.

This highlights the need for a more efficient and automated solution to network management. The current manual approach to network management is outdated and inefficient.



EMA research found that 64% of network automation leaders prefer low-code or no-code solutions to empower all personnel to interact with their automation solutions.<sup>2</sup>



## Key capabilities to look for in a network automation solution:

- The ability to scale to any infrastructure size, including the edge and public cloud and everything in between. Support for major public cloud providers, traditional network infrastructures and software defined LAN and WAN. Support for all major vendor components.
- Provides operational scalability by solving for similar problems across the entire infrastructure.
- Captures and shares SME knowledge across the organization without coding and programmers.
- Allows your experts in each scenario to capture their best practices and make them re-usable without coding.
- Auto-discovers details of the entire hybrid network infrastructure and knows the parameters for every device. This is in stark contrast to many of the early automation approaches that were unaware of their surroundings.
- Builds a live digital twin that includes not only the devices and topology, but also the network logic for all traffic flows and critical IT logic translated from business needs.
- Includes a pre-built automation library that can immediately solve your most common network issues out of the box and is extensible without the need for coding.
- Takes a proactive approach to automation and continuously assures preservation of network intentions and verifies the infrastructure can support your applications.
- The ability to interactively apply stored automation units for remedial purposes when operators and engineers are addressing network issues.
- The ability to execute automation in response to external events from third-party applications, including threat detection from SIEM systems, ITSM workflow managers and network monitoring consoles.
- Full-stack observability for the processes, problems and workflows across the infrastructure.

## GETTING STARTED:

# Determine your most commonly occurring problems

The ability for your chosen network automation solution to quickly address your problems in your environment is the key to demonstrating value and gaining support throughout the organization. So, the best place to identify your needs is to start with the most valuable information available: Your top use case(s) and a dedicated automation engineer(s) to build automation.

## CREATING SUCCESS:

# Scaling NetOps and Applying No-Code Network Automation

Automation projects over the last couple of decades have become mired in mis-set expectations, budget overruns, and unclear ROI. As network operations scales in scope and complexity, IT has learned some valuable lessons regarding how to select and implement network automation that can be deployed immediately, increases in value over time, and quantifies ROI.

### Identifying Key Use Cases

1. Outage Prevention via Continuous Assessment
2. Collaborative Troubleshooting
3. Protective Network Change Management
4. Full-Stack Observability



## INTENT BASED NO-CODE APPROACH

- Applies to any hybrid multi-cloud, multi-vendor network
- Based on full stack Digital Twin, including devices, connectivity, real-time traffic flows and network intents
- Captures subject matter expertise through no-code to create desired network behaviors, replicate behaviors across the network, and then leverage that knowledge before, during, and after issues are detected
- Tackles all repetitive tasks throughout the lifespan of the infrastructure, from the smallest of tasks to the largest
- Scales expertise to provide solution consistency and reduced overhead and escalations
- Provides a robust change management platform to assure business services are preserved prior to making changes and after changes are complete, with roll-back as needed
- Provides a comprehensive collaboration platform where resources can resolve an operational issue that spans organizational responsibility
- Conserves engineering resources and reduces the staffing/skills needed for scale

## Avoiding Common Mistakes

Here are common mistakes to avoid and mitigate for a successful network automation experience.

### 1. Trying to scale network operations by adding staff to match business growth

As infrastructure scope and complexity expand, it is becoming impractical to simply hire more operational staff and train each of them in every network technology. While adding more service personnel is a common and tactical solution to this growing problem, it fails to achieve the desired results of lower operational costs, shorter task duration, and more consistent ticket resolutions. The varying skill levels of operators and engineers negatively impacts the ability to solve problems effectively and rapidly. The most successful IT leaders realize that their operational plan must not continue the labor-intensive model that has been in place for decades, but instead become smarter and transform knowledge into a re-usable asset.

### 2. Adding Another Tool or Point Solution

We all understand the value of documenting and mapping your network. You can identify where the root cause of the problem is faster, maintain compliance more easily and prepare for audits quickly. And the promise of a fancy new auto-discovery and mapping tool can be exciting. But if you stop there, you're overlooking the big picture. Tools are tactical. What you are really looking to do is change the approach. You are looking to change the workflows associated with network operations to re-use knowledge and automate the portions that are similar from ticket to ticket. Buying just another tool does nothing to change the trajectory of the problem.

### 3. Waiting for AIOps and ML tools

All AIOps and ML solutions take a black-box approach leveraging machine learning or traditional statistics-based AI functions to discover root causes from large amounts of machine data. But for most IT problems, a set of clean data is very hard to come by, on top of many other challenges including a PH. D to operate such a tool. Customers routinely state that AI and ML tools rarely meet the bar for success. These approaches are unaware of the infrastructure details and intents, so the observations they make are more theoretical or academic in nature. As such, they rarely produce results that have a material impact on the biggest challenge, which is solving a small number of similar problems at scale, using re-usable knowledge.



The average network management team spends

**3/4**

of its time fixing problems, according to Enterprise Management Associates (EMA) research

And, since it's a really small number of similar problems, gaining the requisite knowledge is not really the NetOps scale issue. It automatically captures and applying automation to solve this set of problems again and again. When selecting a strategic network automation platform, look for solutions that add playbooks or runbooks that emulate engineer steps to troubleshoot common events such as BGP/OSPF/interface down. These workflows will do the login, uptime checks, status checks, and update the incident ticket, or even close it or de-escalate the priority automatically.

#### 4. Taking a reactive approach to network operations

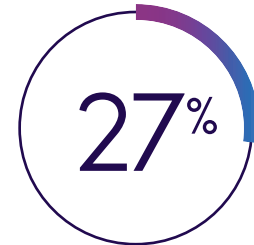
Troubleshooting is the singular focus of most enterprise network managers today, and it is a fundamental problem. The average network management team spends three-quarters of its time fixing problems, according to Enterprise Management Associates (EMA) research.

Look for a solution that focuses on applying knowledge and experience-based best practices proactively to prevent potential problems from impacting production. This empowers teams to instead focus on making the infrastructure more robust, defensible, and reducing service outage risk. The best results-oriented Network Automation solutions will continuously look for the existence of the normal or expected "good" operating conditions (as defined by your business apps). A solution like this understands the intents of each component and how business applications are designed, and the characteristics of the network services each application requires.

#### 5. Focusing only on Day 0 and Day 1 network operations

According to EMA, most enterprises focus their automation efforts on Day 0 and Day 1 network operations, such as zero-touch provisioning and change and configuration management. However, addressing Day-0 and Day-1 is just a tiny part of the total operational lifecycle. Addressing Day-0 and Day-1 alone neglects the much larger and longer-term opportunity to automate Day 2 network operations in a defensible fashion. Remember, the solutions needed to manage Day-2 will be used thousands of times per month in a larger organization, so making the right choice of network automation that addresses this Day-2 part of the lifecycle will have a much greater impact on the bottom line.

Omitting the Day-2 requirement from your selection process will perpetuate the longstanding struggle for scalable network operations, leaving engineers struggling with operational inefficiency, each having to craft a random portfolio of generic tools, a lack of reliable network documentation, and a litany of on-going design compliance issues. According to EMA research, "27% of network operations leaders say design and configuration compliance assessment is critical."<sup>3</sup>



**According to EMA research, 27% of network operations leaders say design and configuration compliance assessment is critical.<sup>3</sup>**



## 6. Personal libraries of generic scripts are not automation

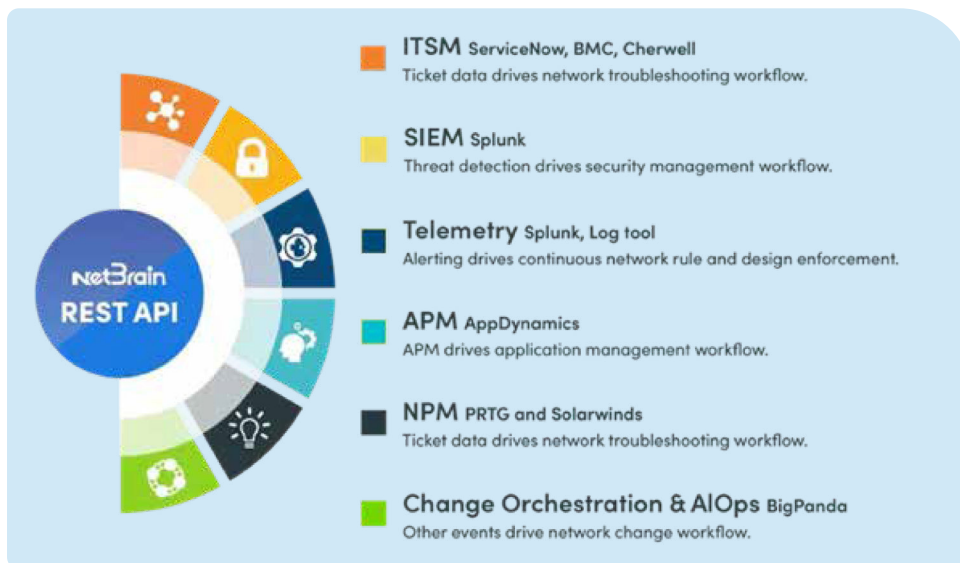
According to EMA, many early types of automation are with network engineers teaching themselves new scripting and coding languages and building themselves folders of single-use scripts, which may never be reused. These folders of scripts may amount to hundreds or thousands of scripts without any structure for re-use. So, while it may be theoretically possible to capture their expertise in these very rigid one-off scripts, there is also no system to leverage these efforts to be applicable to similar problems, nor make their knowledge accessible by a broader group of users with varying skills. The result is the same problem being addressed by two different network engineers will be handled independently, and inconsistently, with varying results.

When selecting a strategic network automation platform, look for solutions that leverage the wealth of existing subject matter expertise your engineers have about your unique network. Harness and store this knowledge for re-use through automation and by L1 operators to create maximum efficiency.

## Integrations

Seamless integration with a variety of external systems and enhances their value. Pre-built API connectors provide a single platform for the network when integrating data and events from your existing IT monitoring systems.

Integrating with different types of external systems and enhance their value by leveraging triggered event-driven no-code automation – northbound or southbound – with your ITSM or other tools. Pre-built API connectors provide a single source of truth integrating data and events from your existing IT monitoring systems. REST APIs and webhook capabilities make it easy to create and include brand new custom integrations: northbound, southbound, or east/west.



1. **ITSM systems** – ticket data drives network troubleshooting workflow
2. **Telemetry system** – alerting drives continuous network rule and design enforcement
3. **Application Performance Monitoring (APM) systems** – drives application management workflow
4. **Security information and event management (SIEM) systems** – threat detection drives security management workflow
5. **Change Orchestration, AIOps, etc.** – other events drive network change workflow

## Centralized Automation Library

Human knowledge can be captured via no-code and stored in a global library readily accessible to all users to automatically execute network troubleshooting and assessment. Automation network engineers could easily customize and let the platform, or anyone reuse the automation across the entire hybrid network at scale. The result is an extensible storage library for automation replication created with no-code for broad reusability.

# Examples of Automation:

## Network Design Assessment

- Network Design Assessment (152)
  - Overlay and Underlay Design (18)
    - Best Practice (2)
      - Check VLAN EVPN Infra Vlan
      - VLAN EVPN Infra Vlan Check
    - Design Error (4)
      - Check IPsec VPN Healthy
      - Check NHRP Neighbor
      - Check VLAN EVPN Neighbor
      - Check VLAN VPC Consistency
      - Check VLAN VTEP Peer
      - IPsec VPN Healthy Check
      - NHRP ADT Base
      - NHRP Neighbor Check
      - VLAN ADT Base
      - VLAN EVPN Neighbor Check
      - VLAN VPC Consistency Check
      - VLAN VTEP Peer Check
  - Routing Design (93)
    - Switching Design (49)
      - ADT NIT (1)
        - Best Practice (3)
        - Design Error (13)
      - Operational Status Assessment (5)

**Assessment Library:**  
300+ out-of-the-box assessments

## Fault Tolerance Assessment

- Fault Tolerance Assessment (24)
  - Device Fail Over (4)
    - ASA Failover Pair Both Active Check
    - ASA Failover Pair Both Active Check - Followup
    - HA Configuration Synchronization Check
    - HA Status Check
  - First-Hop Failover (14)
    - GLBP (4)
      - GLBP Base Group
      - GLBP Pair Device and State Check
      - GLBP Stability Check
      - GLBP Track and Preemption Configuration Check
    - HSRP (5)
      - HSRP Base Group
      - HSRP Pair Device and State Check
      - HSRP Pair Device Consistency Check
      - HSRP Pair Device Consistency Check - Followup
      - HSRP Stability Check
      - HSRP Track and Preemption Configuration Check
    - VRRP (5)
      - VRRP Base Group
      - VRRP Pair Device and State Check
      - VRRP Stability Check
      - VRRP Track and Preemption Configuration Check
  - Stack Topology Failover (5)
    - Design Error (5)
      - Mode of Port Channel Pair Check
      - Mode of Port Channel Pair Follow Up Check
      - Port Channel without Member Port Check
      - VPC Peer Link Port Status Check
      - VPC Port Status Check
    - Operational Status Assessment (1)
      - Check Port Channel Member Status

## Network Compliance Assessment

- Network Compliance Assessment (54)
  - Best Practice (20)
    - Config Drift (14)
      - Baseline Compare (11)
      - Golden Template Check (3)
    - Design Error (12)
      - Check for unused ports but no shutdown
      - Check the device that allows telnet
      - Cisco Coverage Summary
      - Cisco Hardware - End of Routine Failure Analysis Date
      - Cisco Hardware - End of Sales Data
      - Cisco Hardware - End of Security Vulnerability Support Date
      - Cisco Hardware - End of Service Attach Date
      - Cisco Hardware - End of Service Contract Renewal
      - Cisco Hardware - End of SW Maintenance Release
      - Cisco Hardware - End of External Announcement Date
      - Device access mode configuration check
      - Device unused ports configuration check

## SDN Assessment

- Cisco ACI Assessment Reference Library (44)
  - ACI Change Assessment (5)
    - Border Leaf BGP Routing Protocol Check
    - Border Leaf OSPF Routing Protocol Check
    - Border Leaf OSPF Routing Protocol Check
    - Check Neighb. Status Change
    - Monitor Switch Interface Stability
  - ACI Configuration (Self-Assessment) (14)
    - Authn/Contexts without any EPG to Provider
    - Build Fabric, mode device status
    - Check all interfaces status
    - Check Max Contracts number by an EPG
    - Check Overlapping Contracts between 2 EPGs
    - Check Shared State Ports and EPG Binding
    - Duplicated Filters Check
    - EPG Being Used Check
    - Get EPGs and Contracts
    - Monitor Switch Interface Status and Locate Problem Source
    - Software Version Check
    - Unread AP Checking
    - Unread EPG Checking
    - Unread Tenant Checking

## Network Performance Assessment

- Device and Interface Performance (4)
  - CPU and Memory (DNMP)
  - Device CPU
  - Device Memory
  - Monitor Interface Traffic Usage and Error
- IP Accounting (2)
  - Accounting ACL Configuration Check
  - Accounting ADT
- Network Monitor Tool (4)
  - IP SLA Base
  - IP SLA MOS for Voice Check
  - IP SLA Operation State Check
  - IP SLA Overall MOS Check
- QoS Design and Health (8)
  - QoS Conflict for Nexus Check
  - MLS QoS for IP Phone Check
  - MLS QoS Overall Traffic Check
  - MLS Trust State Check
  - MQoS QoS Best Practice Check
  - MQoS QoS Multimedia Conferencing Traffic Check
  - MQoS QoS Overall Traffic Check
  - MQoS QoS Voice Traffic Check
  - Netflow Tool-Lab

## App and Network Dependency Assessment

- Assessment Reference Library (167)
  - Application and Network Dependency Assessment (5)
    - Design Error-Path Failover Check
    - Operational Status-Path Delay Stability Check
    - Operational Status-Path Devices CPU Memory Stability Check
    - Operational Status-Path Next Hop Stability Check
    - Operational Status-Path QoS Stability Check

## Cloud Assessment

- Cloud Assessment Reference Library (20)
  - AWS (2)
    - 1- Foundation (13)
    - 2- Connectivity (7)
    - 3- Design (1)
    - 5- Security (5)
  - Azure (4)
    - 1- Foundation (12)
    - 2- Connectivity (6)
    - 3- Design (7)
    - 4- Application (5)
    - 5- Security (3)
    - 6- Public Service (3)
    - 7- Performance (2)
    - 8- Cost (7)
  - CCP (3)
    - 1- Foundation (3)

## DESIGN-LEVEL ENFORCEMENT

### Design / Feature / Technology / Security

- Must-have or forbidden routes
- QoS, ACL, or multicast rules
- HA/failover/redundancy rules

### Incident & Feature Agnostic

- Sufficient CPU, Memory, Power
- Link utilization, Latency, Interface status
- Device and service reachability

### Key Applications and Paths

- Voice, Internet, VPN path availability and performance
- DCI Paths performance and quality
- Validating key application path availability and quality

## EVENT & TICKET REMEDIATION

### Network

- Access errors
- Configuration errors and drift
- BGP or OSPF errors

### Device

- Host or Service Unreachable
- Printer/Database Device unavailable
- Permission restrictions

### Application

- Data unavailable
- Voice Choppy
- Slow App Response Times



These automation units would address the most common scenarios seen in most enterprises for event-driven responses, (such as those reported via a network helpdesk service ticket), as well as for proactive design-level compliance, security, and application performance support verifications.

Use this automation continuously to assess everything in the network to uncover unidentified network problems before they wreak havoc on business services and negatively impact the user experience. Continuous network assessments can give teams a 360-degree understanding to aid in maintaining network health for:

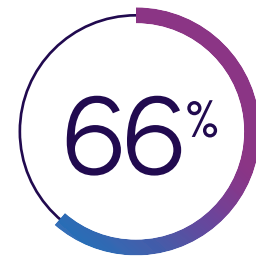
1. **Post-Mortem** - After a network outage, assess how many similar problems you might have across the network.
2. **Security and Compliance** - From security compliance to vendor recommendations, you can assess any vulnerability and fix them before problems occur.
3. **Network Design and Resilience** - Assess network performance, network design, and stability.
4. **Application Health** - better support critical applications.

## What the Experts Say

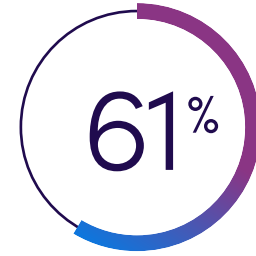
According to Enterprise Management Associates, there are three key benefits of a continuous, automated network compliance assessment. First, 66% of organizations reported reduced security risk and 61% reported improved operational efficiency. Nearly half (46%) reported that such a solution helps with network outage prevention.<sup>4</sup>

## The Platform Age is Upon Us

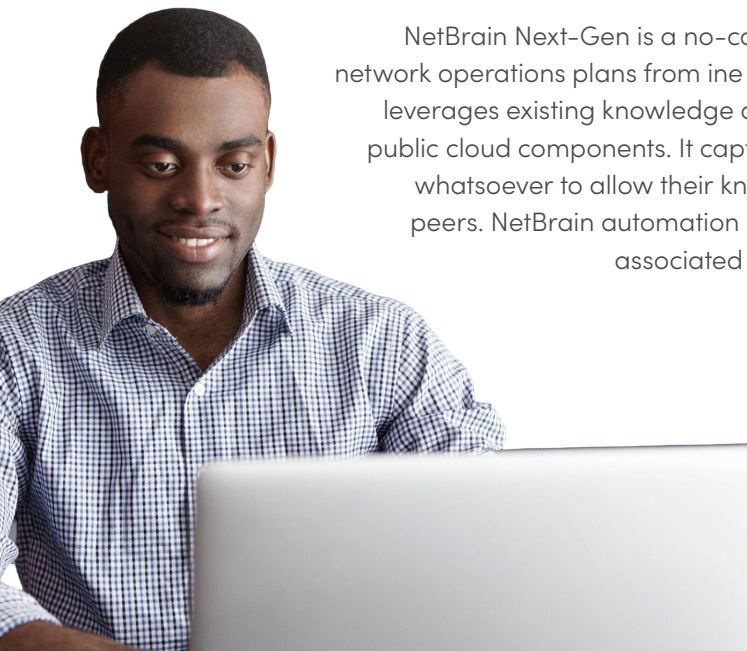
The days of maintaining individual siloed tools for individual tasks are over. Network operations teams must look for ways to combine automation tasks which span data centers, LANs, WANs, and the cloud. They should adopt automation platforms with visibility into the intent and the state of the network to minimize manual data gathering. Look for automation solutions that are focused on the net-result of delivering the IT services needed by the business, rather than maintaining device-level health. The selected automation platform should capture the knowledge of the network team's experts without software development or programming, to make it available to the entire network team.



of organizations  
reported reduced  
security risk and



reported improved  
operational efficiency



NetBrain Next-Gen is a no-code network operations and observability platform that transforms network operations plans from inefficient and reactive to proactive using a streamlined approach that leverages existing knowledge and expertise. NetBrain supports all multi-vendor on-premises and public cloud components. It captures the expertise of your subject matter experts without any code whatsoever to allow their knowledge to be replicated across the network and shared with their peers. NetBrain automation scales network operations more efficiently, at a level previously only associated with additional headcount, higher costs and increase business risk.

## Get Started Today

Assistance from our NetBrain Automation Center of Excellence (CoE) will help you select, adapt, and implement the latest in NetBrain automation tailored to your use cases while teaching you how to use the platform.

Through no-code mechanisms built, your engineers will be able to create additional situation and site-specific automation routines to be used by anyone, at any level to solve problems quickly and accurately when they re-occur. In effect, subject matter expertise becomes available when the subject matter experts are not!

[Get started today](#)

## About NetBrain

A pioneer since 2004, NetBrain is democratizing network automation through GenAI. With its intuitive no-code automation platform, NetBrain empowers network architects, operators and engineers to harness the power of AI and automation, transforming complex operational processes into efficient workflows. By automating network troubleshooting, change, and assessment workflows, NetBrain helps organizations boost operational efficiency, reduce MTTR and mitigate risk. Unifying GenAI and human intelligence, NetBrain provides comprehensive hybrid network observability through continuous network assessment automation and visualization technology, enabling IT organizations to be proactive, make informed decisions and drive innovation.