NetBrain

Reduce Network Downtime by Half Every Year

The Promise of AI-based Automation for Modern Network Operations

Executive Summary

Modern enterprise networks have grown dramatically more complex—spanning physical infrastructure, SDN, SD-WAN, and cloud—yet network operations remain largely manual and human-centric. This mismatch drives prolonged outages, high mean time to resolution (MTTR), and recurring incidents caused by configuration drift and human error. Industry data consistently indicates that up to 80% of network outages stem from human error, while critical incidents often take 5–7 hours or longer to resolve with traditional, people-dependent troubleshooting methods.

NetBrain proposes a fundamentally different, automation-first, AI-driven operating model for network operations. The objective is not merely productivity gains, but a measurable and sustained reduction in network downtime—up to 50% year over year—through systematic application of no-code intent-based automation and agentic AI.

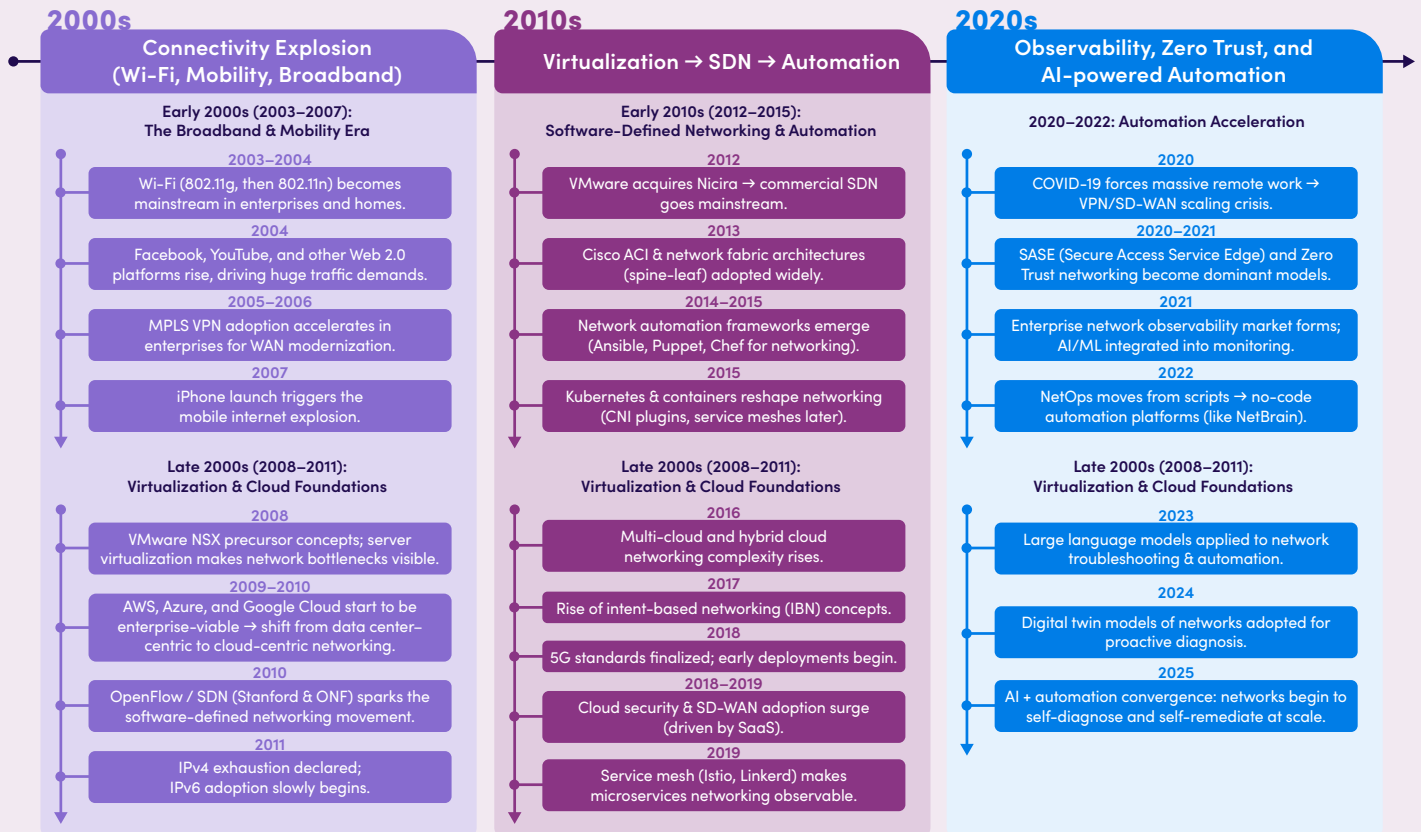# Contents

Unsolved Challenges in Network Operations

Over the past 20 years, networks have become far more complex. Physical infrastructure now coexists with virtual networks such as SDN, SD-WAN, and cloud. While networks have evolved, management technologies and operating methods have not kept pace.

The biggest unsolved challenges in today's network operations—change, diagnosis, and proactive assessment—are still centered on people and manual processes.

- Human error is inevitable when changes are executed without strong automation. About 80% of network issues stem from human-error-driven drift: fault-tolerant designs break down; QoS settings are applied inconsistently; security protections are only partially implemented; and more.
- People-driven diagnosis is a major source of prolonged MTTR. In the real world, 5–7 hours of MTTR for critical network incidents is common—often an unacceptable business impact. At the same time, the required skill set is extremely broad, and few people truly master end-to-end production networking.
- Every enterprise with a critical network is looking for ways to stay proactive—but the state of the art for assessing risk, vulnerability, and hidden issues is still ad hoc. It often takes the form of human-centric peer review, sometimes supported by in-house scripts or inventory tools.

The following picture shows the efforts in both areas, although one is well ahead of the other.

20 YEARS OF NETWORKING

2000s
Connectivity Explosion (Wi-Fi, Mobility, Broadband)

Early 2000s (2003–2007): The Broadband & Mobility Era

2003–2004
Wi-Fi (802.11g, then 802.11n) becomes mainstream in enterprises and homes.

2004
Facebook, YouTube, and other Web 2.0 platforms rise, driving huge traffic demands.

2005–2006
MPLS VPN adoption accelerates in enterprises for WAN modernization.

2007
iPhone launch triggers the mobile internet explosion.

Late 2000s (2008–2011): Virtualization & Cloud Foundations

2008
VMware NSX precursor concepts; server virtualization makes network bottlenecks visible.

2009–2010
AWS, Azure, and Google Cloud start to be enterprise-viable → shift from data center–centric to cloud-centric networking.

2010
OpenFlow / SDN (Stanford & ONF) sparks the software-defined networking movement.

2011
IPv4 exhaustion declared; IPv6 adoption slowly begins.

2010s
Virtualization → SDN → Automation

Early 2010s (2012–2015): Software-Defined Networking & Automation

2012
VMware acquires Nicira → commercial SDN goes mainstream.

2013
Cisco ACI & network fabric architectures (spine-leaf) adopted widely.

2014–2015
Network automation frameworks emerge (Ansible, Puppet, Chef for networking).

2015
Kubernetes & containers reshape networking (CNI plugins, service meshes later).

Late 2000s (2008–2011): Virtualization & Cloud Foundations

2016
Multi-cloud and hybrid cloud networking complexity rises.

2017
Rise of intent-based networking (IBN) concepts.

2018
5G standards finalized; early deployments begin.

2018–2019
Cloud security & SD-WAN adoption surge (driven by SaaS).

2019
Service mesh (Istio, Linkerd) makes microservices networking observable.

2020s
Observability, Zero Trust, and AI-powered Automation

2020–2022: Automation Acceleration

2020
COVID-19 forces massive remote work → VPN/SD-WAN scaling crisis.

2020–2021
SASE (Secure Access Service Edge) and Zero Trust networking become dominant models.

2021
Enterprise network observability market forms; AI/ML integrated into monitoring.

2022
NetOps moves from scripts → no-code automation platforms (like NetBrain).

Late 2000s (2008–2011): Virtualization & Cloud Foundations

2023
Large language models applied to network troubleshooting & automation.

2024
Digital twin models of networks adopted for proactive diagnosis.

2025
AI + automation convergence: networks begin to self-diagnose and self-remediate at scale.

# NetBrain's Approach to Reducing Network Downtime

NetBrain pioneered no-code intent-based automation for network operations. Across five generations of automation, the focus has not been to save human time, but to reduce downtime—because many outages, in one form or another, trace back to human error during day-to-day operating tasks.

- Automating diagnosis can significantly reduce troubleshooting time, shortening the duration of an IT outage.
- Automating network assessment can discover hidden issues before they create real-world negative impact.
- Automating change can systematically prevent new changes from violating existing network design and intent, consistently reducing the number of incidents.

Together, automation can reduce both the length of outages and the number of outages, resulting in a systematically more reliable network.

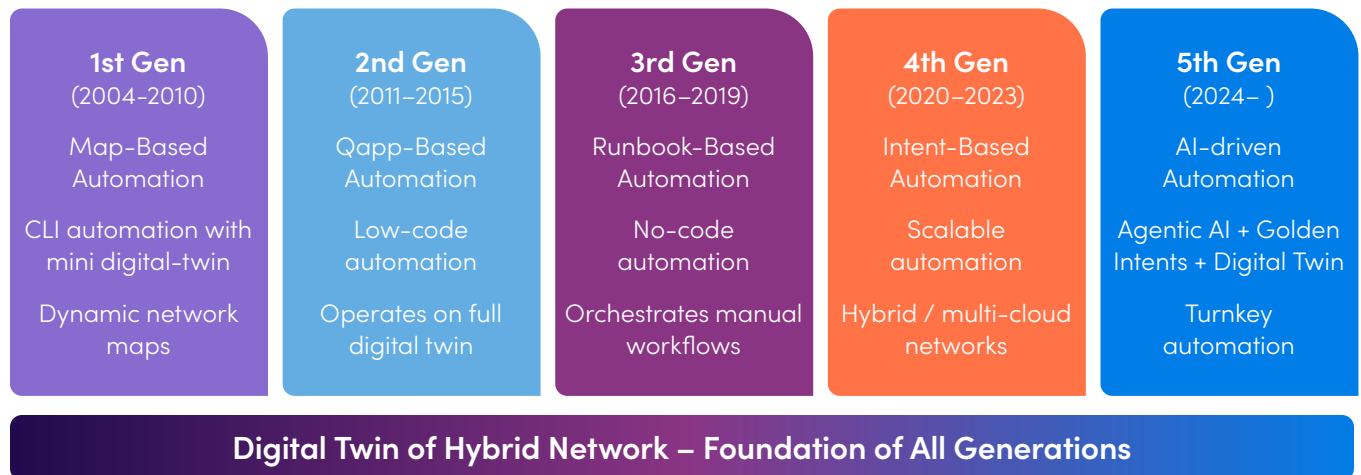| Operational Task	Goal	Apply Automation to
Diagnosis	Reduce MTTR; Reduce dependence on individual experts	Shift work left—from senior engineers to junior staff to the machine
Assessment	Discover hidden issues; Automated continuously	Run post-mortem and golden assessments
Change	Guard against configuration drift; Enforce policies and standards	Standardize changes and automate validation
Docs	Complete and accurate	Self-document via the digital twin

This highlights a simple truth: as networks advance, network management must advance as well. The most important remaining challenge is to reduce network downtime so the business can depend on a functional network with confidence.
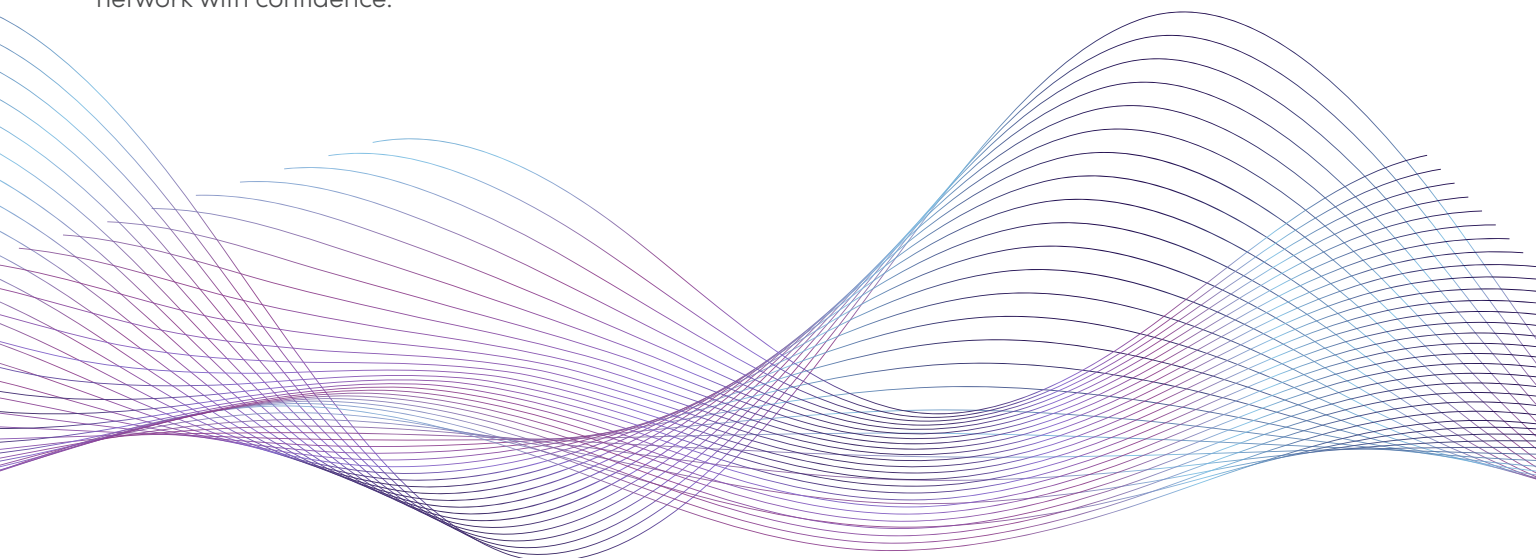
AI-Driven Automation Is a Game Changer

Over 21 years, NetBrain has advanced through five generations of automation to address the operational challenges above with the same goal: reduce network downtime by accelerating diagnosis and preventing outages. (See diagram below.)

20+ YEARS OF NETBRAIN AUTOMATION (2004–2026)

1st Gen (2004–2010)	2nd Gen (2011–2015)	3rd Gen (2016–2019)	4th Gen (2020–2023)	5th Gen (2024–)
Map-Based Automation	Qapp-Based Automation	Runbook-Based Automation	Intent-Based Automation	AI-driven Automation
CLI automation with mini digital-twin	Low-code automation	No-code automation	Scalable automation	Agentic AI + Golden Intents + Digital Twin
Dynamic network maps	Operates on full digital twin	Orchestrates manual workflows	Hybrid / multi-cloud networks	Turnkey automation

Digital Twin of Hybrid Network – Foundation of All Generations

Each generation has built on the last, but the 5th generation—powered by state-of-the-art agentic AI—is a step change. With the ability to learn, reason, and operate across tools provided by the underlying platform, agentic AI effectively pairs a PhD-level network engineer with NetBrain's automation and digital-twin capabilities to (1) diagnose issues, (2) assess vulnerabilities, and (3) propose and execute network changes. Its ability to orchestrate tens of thousands of automations, evaluate complex outcomes, and iterate on reasoning makes the following results possible:

From 2025, a Large and complex network can expect **50% reduction** of network down time **every year** after systematic application of automation and AI.
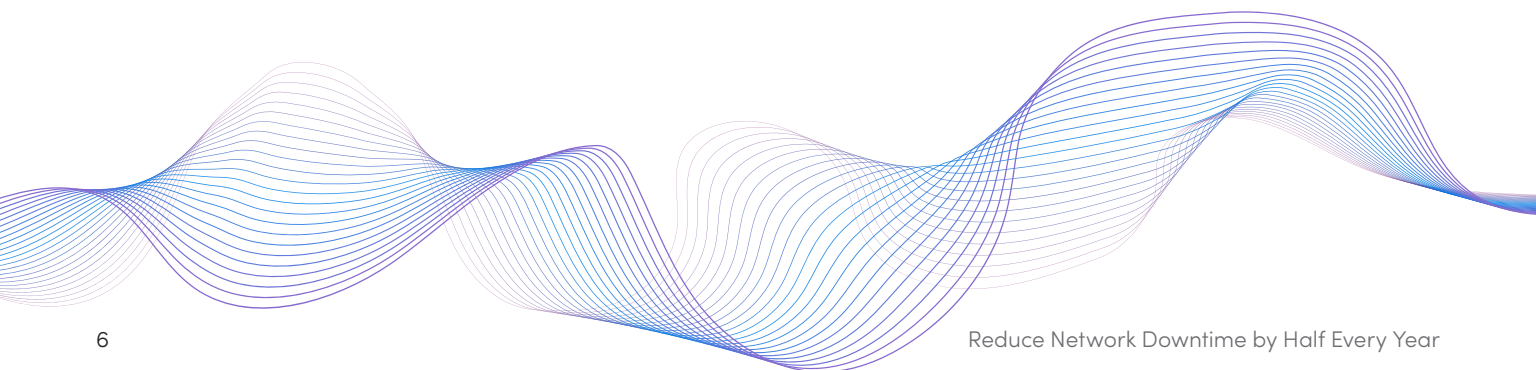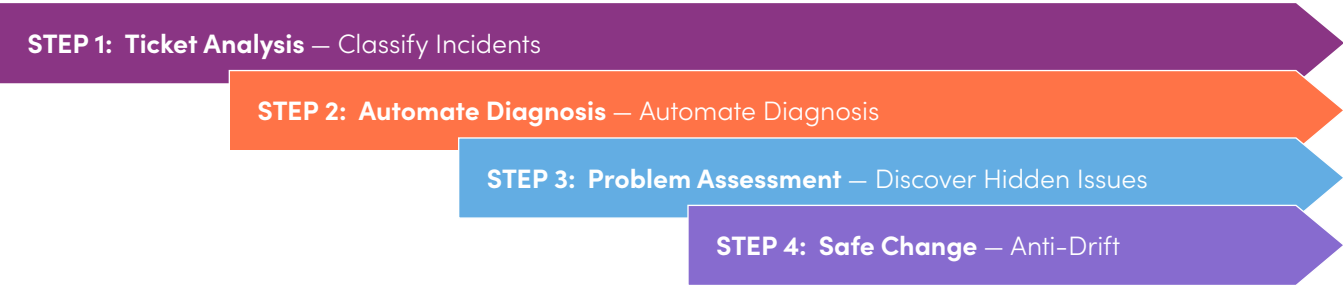
The 4-Step Methodology to Halve Network Downtime Every Year

The goal of cutting network downtime is achieved by reducing the average time to resolve each issue and reducing the total number of tickets. The stakes are high, as the per-hour and per-incident costs in modern enterprises are substantial.

Year	MTTR	Number of Tickets	Total Down Time
2025	7 hrs	XXXX	· · · · · · · · · · · ·
2026	5 hrs	XXX	· · · · · ·
2027	3 hrs	XX	· · ·
2028	1.5 hr	X	· ·
2029	30 min	Y	·

Enabled by modern automation and AI, a four-step methodology can reduce network downtime by half every year.

STEP 1: Ticket Analysis — Classify Incidents

STEP 2: Automate Diagnosis — Automate Diagnosis

STEP 3: Problem Assessment — Discover Hidden Issues

STEP 4: Safe Change — Anti-Drift

STEP 1: Ticket Analysis — Analyze Past Tickets

To apply automation and AI effectively to network operations, start with historical ticket analysis. Just as patient records help clinicians diagnose, treat, and prevent disease, tickets provide the data needed to improve operations. By feeding past years of tickets into NetBrain's AI-based ticket analysis, organizations can classify incident types, identify common diagnostic steps, and quantify frequency. Most importantly, the analysis provides a foundation for grouping future incidents and driving continuous improvement.

Even tickets not caused by the network are valuable to classify. In practice, nearly every IT incident raises a network-related question: "Is it the network?" Associating automated diagnosis with each incident type—network or non-network—is a recommended best practice.

TOP TICKET TYPE: NETWORK & NON-NETWORK ISSUES

	Wi-Fi Connectivity	VPN Access	Host Unreachability	BGP Neighbor	Interface Down
■ MTTR(hrs)	2	2	1	4	1
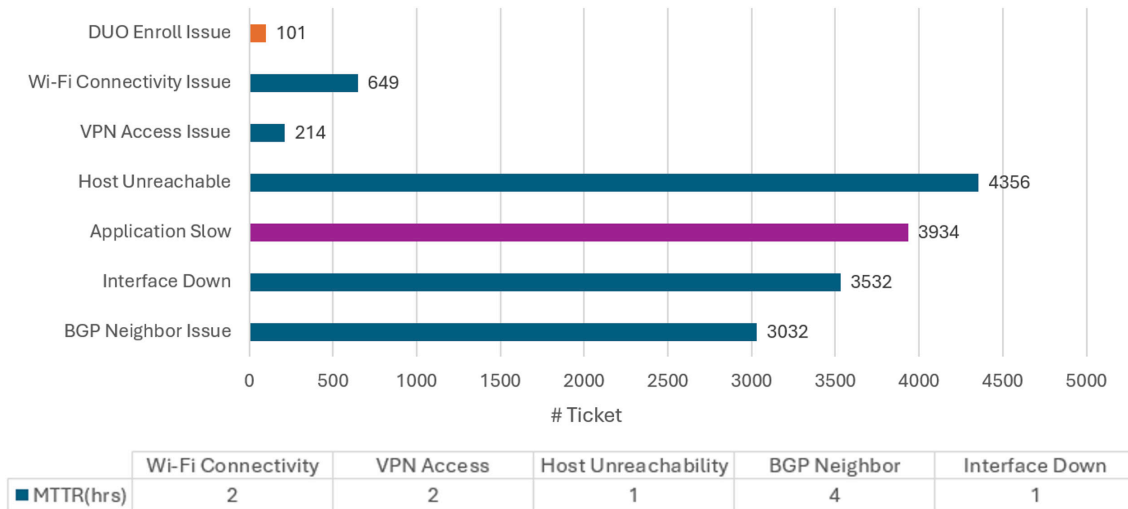
STEP 2: Automate Diagnosis — Runbook for Each Type of Ticket

Automated diagnosis in the age of AI-based automation requires a systematic approach to shift work left—from senior engineers to junior engineers and ultimately to the machine. This is made possible by (1) discovering the network into a digital twin, (2) using automation to capture diagnostic and validation know-how, and (3) using AI to orchestrate automation, reason through outputs, and provide root-cause analysis.

To scale automated diagnosis to cover most problems, a disciplined approach is required—often by following the incident categories identified in Step 1. For each incident type, capture the manual steps used to diagnose the issue across possible root causes (one incident type may have multiple root causes). Then create an executable runbook and continuously improve it as workflows are transformed. A runbook may include multiple node types, such as:

- **CLI Node** – Runbook automation that executes CLI commands for humans or AI to consume
- **Config Node** – Configlets or golden configuration elements related to a specific diagnostic goal
- **Quick Assessment Node** – An intent-based automation node that runs impact analysis or advanced intent-based diagnosis
- **Document Node** – An automated documentation node that summarizes runbook data with the help of AI

Each runbook uses AI to interpret results collected by automation and may also recommend additional automations to improve diagnosis. This creates a white-box AI solution where human expertise, machine automation, and AI reasoning are combined to solve a problem—often delivering an order-of-magnitude faster diagnosis and much broader coverage. For a well-managed network, 99% problem coverage is now achievable.

It is also feasible for black-box AI—where automation and AI interaction are invisible to users—to address a similar share of issues after tuning. For example, NetBrain's deep-diagnosis capability, built on AI and intent-based automation, can leverage the same white-box automation assets and achieve comparable accuracy without a human in the loop.

Reaching 99% coverage for automated diagnosis is a journey, not a silver bullet. Done properly, coverage can converge quickly across much of the network. The key is to insist on problem assessment after each outage—and to include past outages identified through the ticket analysis in Step 1.

Post-Mortem Assessment

Post-mortem assessment extends the familiar post-mortem analysis most organizations already perform after business-impacting network outages. Using NetBrain's no-code intent-based automation, teams first model the diagnosis for a known root cause, then use a Quick Assessment runbook node to apply that intent across the network and answer a critical question: Do similar issues exist elsewhere? As an equally important outcome, the assessment produces automation that enables future occurrences of the same issue to be diagnosed automatically, as described in Step 2.

Golden Assessment

Can an organization benefit from the know-how of the broader industry—not just its own outage history—when it comes to assessment? That is the purpose of Golden Assessment, where seed intents and rules are created by NetBrain based on industry best practices and issue reports. The golden assessment then adapts to a specific network so only relevant automations are created, improving efficiency.

Organizations can further customize the golden assessment library for their environment to speed up automation coverage and AI-based diagnosis.

In summary, post-mortem assessment and golden assessment help uncover hidden issues before they create negative business impact—a powerful mechanism for reducing network downtime.

Up to 80% of outages are associated with network change—in the form of drift from the original design. With millions of lines of configuration and countless parameters to review, preventing drift is a major challenge. NetBrain offers a new approach: Golden Config. Using intent-based automation and AI, enterprises can "discover" the golden configurations that represent the network's true design, then continuously monitor them before, during, and after change—triple defense. Before change, every proposed design is checked against the golden-config library to ensure no drift is introduced. During change, the change and its impact are validated immediately so negative effects can be caught early. After change, golden-config rules are updated so future changes remain aligned with the current design.

After drift is effectively controlled, enterprises can further improve change success rates by standardizing frequent changes using runbook-based templates with parameterized inputs. In many environments, standardized changes represent the majority of changes, and this can materially improve network reliability.

A Hypothetical Example

Enterprise ACME completed a major M&A and struggled with chronic issues in addition to new challenges. Business leaders often heard the following complaints:

- There have been several business-impacting network outages, and resolution has taken hours and involved dozens of people over the past six months.
- The IT team went through a reorganization, creating significant knowledge gaps in parts of the network, including AWS cloud and SDN.
- There is little proactive protection against future outages—operations have been largely reactive, and resources are tight.
- Change success rates have been poor, and the business has coined a term: "Monday morning syndrome."

An Automation-Centric Solution

After adopting NetBrain's automation and AI product suite, the ACME team moved through three phases of transformation to tackle these challenges:

Phase I: Automated Network Discovery and Benchmark
To address knowledge silos, ACME used NetBrain's discovery and benchmarking capabilities to build a dynamic digital twin and enable self-documentation of the network.

As a result, a dynamic network map of the entire network can be built on demand; and site and data center maps are created automatically, annotated with additional context.

With additional training, the team began using the dynamic map to:

- Perform ad hoc checks of network health whenever there was suspicion of an issue
- Communicate diagnosis progress with non-network teams
- Learn new network technologies such as SDN and cloud

Phase II: Incident-based Manual Workflow Transformation
ACME leadership embraced an automation-first approach to IT operations. After discovery, they immediately began the four-step workflow transformation:

- Ticket analysis is performed quarterly, and incident-based diagnosis and root-cause analysis are continuously captured in runbook templates.
- Each troubleshooting effort now starts with a dedicated runbook template built by ACME's domain experts for specific problem areas.
- Post-mortem assessment is carried out after every outage using the intent-based Quick Assessment feature.
- Change processes are converted with runbook-based automation, with triple defense implemented through a CLI-centric approach.

After Phase II, the NOC, SOC, engineering, and architecture teams can all benefit from automation-centric troubleshooting, assessment, and change, in addition to dynamic documentation.

With key workflows transformed, leadership also created observability dashboards to continuously monitor critical network assets, including:

- Network fault-tolerance dashboard – Monitor all major network failover points
- Critical application network dependency dashboard – Monitor critical business applications
- CVE dashboard – Monitor common vulnerabilities and exposures affecting network assets
- Past outage dashboard – Monitor similar instances of past outages across the network

Is NetBrain for You?

Reducing network downtime is a continuous journey. No one should expect a perfect network without issues, but with modern automation and AI technology, the network can become more reliable each year. In fact, the pace to minimal outages could be even faster than "half every year" described above—the key is to take a people-centric approach and have AI and automation learn aggressively from human expertise. In other words, using automation and AI to take humans out of day-to-day data gathering and validation loops is key to success.

So is this for you and your organization?

A short checklist may help you decide:

- Are you ready to adopt automated network documentation?
- Is troubleshooting taking too long and requiring too many people each time?
- Is proactive discovery of hidden network issues a high priority?
- Are you ready to reduce human error in everyday network changes and upgrades?
- Is a shortage of network-operations staff an ongoing issue?
- Is leveraging AI for productivity high on your to-do list?

About NetBrain

NetBrain empowers enterprises to cut MTTR in half every 12 months and prevent network outages using AI-driven, no-code automation. Trusted by more than 2,500 enterprises, our intent-based platform turns reactive, manual workflows into proactive, automated, and self-healing network operations that ensure consistency, scale, and security.

NetBrain Technologies
15 Blue Sky Drive
Burlington MA 01803

SCHEDULE A DEMO

NetBrain