codilime

# Network automation for business leaders

## How to drive business growth and boost efficiency

- Pros and cons of introducing network automation
- Case studies and real-world examples
- Tools for network automation

# Table of Contents

## Executive summary

Having a reliable, efficient network is more important than ever before. Whether you're running a tech-focused company or simply relying on your network to keep operations smooth, network automation is no longer a luxury but an essential.

This ebook explores why network automation is worth considering for businesses of all sizes. It explains how automation can help companies reduce costs, speed service delivery, and maintain reliable, secure systems.

Automation is critical for staying competitive in industries like telecom and ISPs, where the network is the business. But even for businesses in finance, healthcare, retail, or other sectors, network automation helps ensure stability and scalability without stretching resources thin.

You'll learn about the benefits and practical concerns of automating networks, from initial setup challenges to overcoming the fear of losing control over systems. We'll walk you through the tools and steps needed to start your automation journey and introduce concepts like Digital Twins, configuration as code, and automated pre- and post-checks. And we don't overlook real-world case studies and practical examples.

By reading this guide, you'll have a clear understanding of how network automation can transform your business and be able to make better-informed decisions during your automation journey.

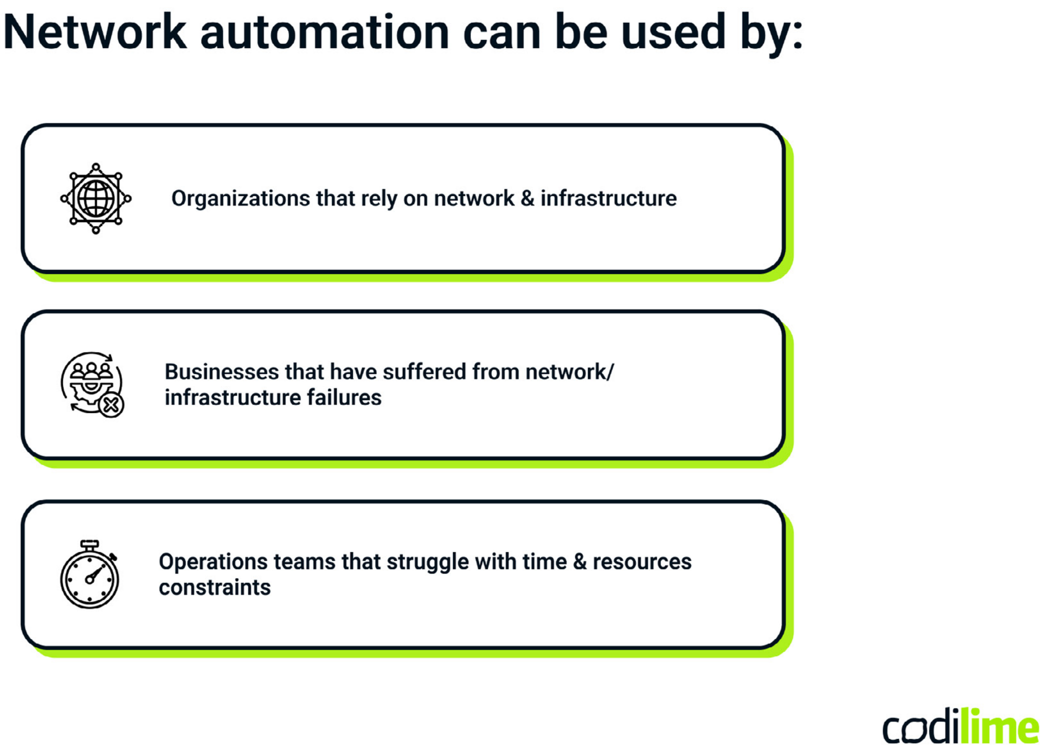
# Introduction to network automation for business leaders

In today's businesses, whether tech-focused or not, a reliable network is key to success. Network automation is now essential, helping companies keep systems reliable, cut costs, and speed up service delivery.

For companies like ISPs or telecom providers, where the network is the core of their service, automation is crucial. It enables faster service launches, ensures regulatory compliance, and keeps systems running smoothly, while controlling costs.

For other businesses that use networks to support their operations, like those in finance, healthcare, or retail, the expectations are more simple: the network needs to work reliably and affordably.

In both cases, network automation offers big benefits, helping companies stay competitive, reliable, and ready to grow as their needs change.



Network automation can be used by:

- Organizations that rely on network & infrastructure
- Businesses that have suffered from network/ infrastructure failures
- Operations teams that struggle with time & resources constraints

## Why is network automation worth considering?

Businesses need network automation to stay competitive and secure – as networks grow more complicated, traditional management methods simply don't cut it anymore.

Here's why implementing network automation is a smart choice:

- Manually maintaining configuration consistency across a complex network can be a

Herculean task. Differences in configurations can lead to outdated security measures, unmonitored services, and inefficiencies. I**mplementing automation helps maintain uniformity, reduce the risk of security gaps, and simplify the troubleshooting process.**

- The expense and effort of manually updating configurations across a network can be significant. Automation simplifies these tasks, whether it’s updating the IP address for a syslog server on hundreds of devices or rolling out new services. **Automation cuts down on time and labor**, allowing teams to focus on more strategic initiatives.
- **Manual network management is prone to human error**, which can lead to costly outages and challenging troubleshooting sessions. Automated scripts, tested thoroughly in controlled environments, ensure that updates are applied accurately, reducing the chances of mistakes that could disrupt network operations.
- **Teams can use automated tools to monitor the network continuously**, identifying weak spots. Whether using custom scripts or comprehensive solutions, this proactive approach keeps the network secure and resilient.
- **Automation can streamline the process of keeping network documentation up-to-date** by automatically updating records and tracking assets, ensuring that all information is accurate and current.

Network automation is a strategic decision that can lead to a more efficient, secure, and scalable network infrastructure. While there may be challenges, such as the initial time investment and the need for specialized skills, the long-term benefits – consistency, reliability, and security – are well worth the effort.

## Why do you need network automation?

Many traditional methods of managing networks are no longer sufficient. Below, we have listed the key points highlighting how an automated approach can enhance current network management.

### Automation is a logical choice

Network automation stands out as a logical choice for handling the complexities of modern network environments. With increasing demands on network infrastructure, automation helps streamline operations, making managing and maintaining large-scale networks easier.

### Increased efficiency and productivity

Automated systems allow operation teams to focus on more strategic initiatives. This shift accelerates task completion and frees up valuable resources, enabling businesses to allocate their workforce to areas that drive innovation and growth.

### Improved compliance and security

Network automation facilitates compliance and being in line with security standards by providing comprehensive monitoring and auditing capabilities.

### Cost savings

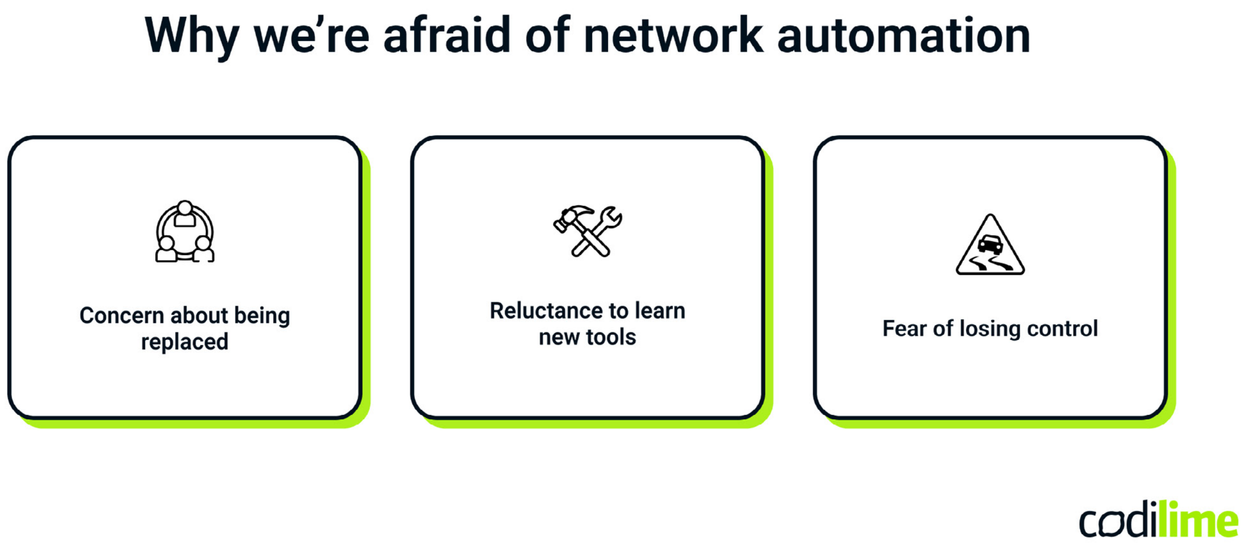
By reducing the need for manual intervention, automation lowers labor costs and minimizes the likelihood of costly outages caused by human errors. Moreover, automation can reduce downtime costs, further driving down operational expenses.

### Enhanced network insight and control

With automated monitoring and reporting, businesses can gain real-time insights into network performance and health.

Network automation offers a wide range of business benefits, from increasing efficiency and reducing errors to improving security and cutting costs. By adopting automation, organizations can achieve greater control over their networks, optimize their resources, and focus on delivering innovative services to their customers.

# The concerns of automating networks



Why we're afraid of network automation

Concern about being replaced

Reluctance to learn new tools

Fear of losing control

Embarking on network automation can be both exciting and daunting. Automating complex tasks is challenging, especially as it involves change. These concerns are common to any major technological advancement.

One of the most typical fears is the **potential for job displacement**. The idea that automation could render network engineers obsolete is a daunting one. However, this perspective overlooks the value of human expertise in guiding and overseeing automated processes. Rather than replacing engineers, automation empowers them to apply their skills more effectively, tackling the kind of work that demands creativity and deep technical knowledge.

Another common hurdle is the **hesitation to adopt new tools**. Automation often requires learning to use platforms like Ansible, Terraform, and Python, which can be daunting for those used to traditional methods.

However, the learning curve associated with these tools is not impossible. Many of them are designed to be user-friendly, with intuitive interfaces and straightforward scripting languages. Just as learning to configure a new vendor's equipment is a necessary skill, so too is mastering these new tools. The investment in learning pays off in increased efficiency and productivity.

A very human aspect of the resistance to automation is the **fear of losing control**. However, this concern can be mitigated through proper oversight and robust observability tools. Engineers still play a crucial role in supervising these automated processes, ensuring they align with the intended outcomes. Moreover, advanced observability solutions, often integrated with AI-based tools, provide comprehensive visibility into the network's operational state. This means that engineers maintain a clear view of what's happening within the infrastructure even in scenarios involving closed-loop automation.

The notion of losing control extends to concerns about the impact of automation on network performance. There’s a fear that **automated changes could introduce or exacerbate new issues**. Automation can enhance data consistency and network visibility with a well-implemented Single Source of Truth or Single Source of Intent, such as through GitOps. These frameworks ensure that all configurations are aligned with the desired state of the network, reducing the likelihood of performance issues.

Finally, it’s natural to resist change, especially when it means moving away from familiar ways of working. Change can be uncomfortable, mainly when it involves adopting new technologies and workflows. Yet, this resistance often stems from a lack of familiarity rather than a fundamental flaw in the technology itself. As organizations grow more accustomed to automation, they often find that the benefits far outweigh the initial discomfort.

# How to start the automation journey?

The journey towards network automation doesn't have to be overwhelming. By adopting a gradual, step-by-step approach, businesses can seamlessly integrate automation into their operations, ensuring a smooth transition from manual processes to automated systems.

The path to network automation can be mapped out in five basic steps:

1. **Source of Truth/ Source of Intent**
   Establishing a reliable and centralized repository for all network data, like configurations, but not only, is the foundational step to ensure consistency and accuracy, providing a clear reference point for all automated processes.
2. **Script-based automation**
   Implementing automation scripts for repetitive tasks can save time and reduce errors. Tools like Ansible, Terraform, and Python are commonly used in this phase, enabling precise and efficient network management.
3. **Digital Twins**
   Creating a digital replica of your network environment allows for safe testing and validation of changes before they are applied to the live network.
4. **Automated pre- and post-checks**
   Automated checks before and after network changes can detect potential issues and confirm that changes have been successfully implemented.
5. **Platform-based automation**
   The final step involves integrating comprehensive automation platforms that can manage and orchestrate complex network operations to provide a unified interface for monitoring and controlling automated processes, enhancing overall visibility and control.

It's important to note that not all steps are mandatory. The process can be tailored to fit each organization's unique needs and existing infrastructure. This flexibility allows businesses to prioritize and implement the most relevant aspects of automation at their own pace.

Such gradual implementation helps avoid overwhelming existing systems and personnel, framing the transition as a natural evolution rather than a disruptive revolution.

In the following sections, we will delve deeper into each of these steps, providing detailed insights to help you navigate your network automation journey.

## Source of Truth vs. Source of Intent

Source of Truth (SoT) / Source of Intent (SoI) comes into play when we talk about maintaining accurate data – the backbone of effective network automation.

Every network starts with a design. Initially, managing this design is straightforward. However, as networks grow, different teams handle different parts, leading to fragmented data and inconsistencies. A SoT or SoI serves as a reliable repository, ensuring all data is centralized and consistent. This is essential for maintaining a clear, unified view of the entire network.

SoT / SoI aim to represent the same goal – managing the network's data effectively ensuring alignment between the current and intended states. This is crucial for ensuring that network changes align with the intended architecture, rather than just reflecting the current, possibly flawed, configuration.

Centralizing data with SoT / SoI ensures all teams can easily access and update information consistently. Tools like GitHub, Nautobot, and NetBox can serve this purpose, offering structured environments for managing network configurations and intentions.

## Script-based automation

Script-based automation has become a staple in modern network management – engineers frequently utilize scripts to automate routine tasks, leveraging tools such as Ansible playbooks, Python scripts, or Bash scripts. These scripts significantly reduce the need for manual intervention, streamlining processes and enhancing efficiency.

To maximize the benefits of script-based automation, it is essential to establish a centralized repository where all engineers within the organization can share and access scripts. This repository serves as a collective resource, enabling engineers to collaborate on developing and refining scripts. By standardizing scripts, organizations can achieve greater consistency in network configurations and operations.

A unified script repository fosters a culture of collaboration and continuous improvement. Engineers can build upon each other's work, ensuring that best practices are disseminated and adopted throughout the organization. Moreover, having a shared repository means that scripts can be thoroughly reviewed and tested before deployment.

## Digital Twins

Traditionally, network operators have relied on physical labs that mimic the production environment to test new equipment, software, or services. These labs typically consist of physical hardware, and network simulators like IXIA or Spirent, which are used to evaluate performance, scalability, and reliability. However, physical labs come with significant limitations, including high costs, limited scalability, and restricted concurrent usage.

Digital Twins offer a compelling solution to these challenges in the form of virtualized network models. These models replicate the control and management planes of the physical network, allowing operators to test and observe the interactions between network elements in a safe, controlled environment.

When implementing automation scripts, particularly those designed to perform tasks at scale, testing these scripts in a Digital Twin environment ensures they function correctly before deployment in the live network. This virtual environment allows for comprehensive validation of variables and the order of operations, minimizing the risk of service disruptions.

For instance, automation scripts often need to apply changes across multiple devices simultaneously. Using a Digital Twin, operators can verify that these scripts pass the correct values to variables and execute changes in the proper sequence, ensuring network stability and continuity. This is particularly valuable for large-scale networks where physical replication is impractical.

Moreover, Digital Twins facilitate continuous integration (CI) practices in network management. Network changes can be tested automatically by integrating Digital Twins with techniques like GitOps.

### Configuration as Code (CaC)

The concept of Digital Twins is closely related to CaC. By using a Digital Twin, organizations can safely experiment with and refine their CaC strategies, ensuring that changes will perform as expected in the live network.

Configuration as code is changing the way companies manage their infrastructure. By treating configuration settings like software, CaC ensures everything stays consistent, easy to track, and simple to update. This approach helps integrate configuration management directly into the development process, making things run more smoothly and reducing the amount of mistakes.

## Safe network and infrastructure changes with pre- and post-checks

A production environment is like a living organism, and evolves over time. Changes can be planned, such as configuration updates or new service deployments, or unplanned (as a result of error), often resulting from failures or unexpected interactions. Automated pre- and post-checks are essential to mitigate these risks.

Pre- and post-checks ensure that network changes do not introduce issues. Before any change is implemented, pre-checks verify the network's current health and readiness. For example, if a network is already experiencing issues, adding new configurations might worsen the situation.

Pre-checks help operators detect such risks early, allowing them to pause or adjust the change process if necessary.

After implementing the change, post-checks are conducted to assess its impact. These checks compare the network's state before and after the modification, identifying any discrepancies or issues caused by the change. This process ensures that the change was applied correctly and that the network remains stable and functional.

Various tools and methods can be used for automation, such as Ansible playbooks or API calls in Python scripts. These tools gather comprehensive information about the network's state, including device configurations, protocol statuses, and traffic patterns. By standardizing the output format (e.g. JSON or XML), automated systems can efficiently compare pre- and post-change data to identify any unexpected differences.

A Digital Twin can be invaluable for testing and validating pre- and post-checks. By simulating the production environment, Digital Twins allow operators to safely experiment with changes and refine their verification processes. Digital Twins also enable parallel testing, crucial for large-scale networks. Simultaneously executing checks across multiple devices ensures consistency and reduces the time needed for validation.

The short list of techniques below will help you ensure the high reliability of your network:

- **Redundant network/infrastructure design** allows for retention of operability even in a degraded state, with zero or minimal impact on customers and services.

- **Prior deployment service/feature tests** means that every new service and feature is thoroughly tested in a lab environment before it is deployed to production. The testing can be using physical hardware or with the help of a Digital Twin.

- **Configuration unification** is an approach to configuring a device (or its software-based representation) to make sure that the same feature or service is configured exactly the same way everywhere.

- **Making changes during maintenance windows** is a process that is rigorously followed in all large organizations and it means that all impacting (or potentially impacting) change operations are performed only during hours of least infrastructure usage.

- The **pre-check** aims at two things: firstly, to verify if a network/infrastructure is healthy and ready for a change; i.e. there are no issues ongoing that can impact the change, so the process can be stopped before it is even started. The second goal is to have benchmark data to compare with the results gathered during **post-check** tasks after the modification is introduced.

- **Change history tracking** is needed to be sure of what has happened and when, and for documentation purposes. We can look at the state of the network before the change and after the change and everything may look okay, but if someone reports that something is not right then we have access to data showing exactly what the status was before the change was implemented.

- **AI-based anomaly detection** helps with revealing events or patterns that should not be there. The process is similar in its goal to pre- and post-checks - to make sure all works as expected - but it uses different tools and methodologies, and is continuous; contrary to pre- and post-implementation checks which are done on request.
- **AI-based root cause analysis (RCA)** is used in situations when an issue in the network/ infrastructure has already occurred. When using AI-based RCA, an operator is assisted by the software to search for changes introduced prior to the issue, known issues that may have surfaced with the existing configuration in place, and checks that take place automatically.

## Platform-based automation

The next step in the network automation journey is the integration of a network automation platform. These platforms serve as comprehensive solutions that centralize and streamline the management of network automation processes. With numerous options available on the market, it’s essential to carefully evaluate each platform’s capabilities and compatibility with your organization’s needs.

When considering a network automation platform, it’s essential first to understand what each solution offers - different platforms come with varying levels of built-in functionality, from monitoring and reporting to advanced automation and orchestration features. A thorough evaluation should include an assessment of how well the platform integrates with your existing tools and systems, such as your chosen Source of Truth / Source of Intent.

Another consideration is whether the platform operates as a read-only solution or if it has the capability to interact directly with your network infrastructure. Read-only platforms provide visibility into the current state of the network but do not make changes. On the other hand, more advanced platforms can execute configuration changes and automate workflows, offering greater control and flexibility.

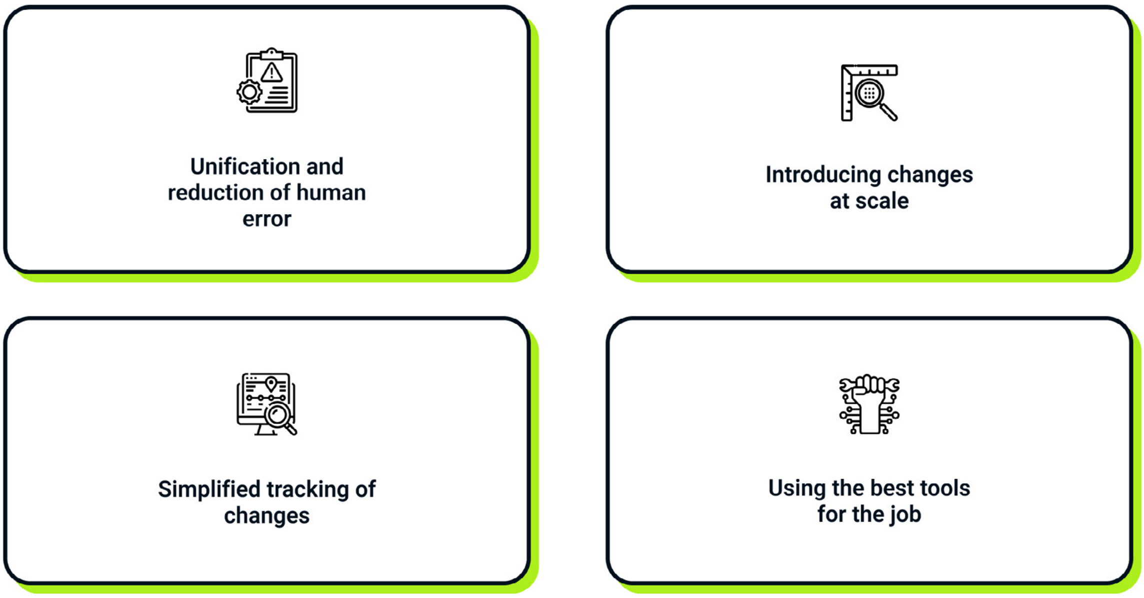
Additionally, it’s essential to define how the platform supports creating and managing automation pipelines. These pipelines are sequences of automated actions that can be triggered by specific events or scheduled at particular times.

As a result, organizations can achieve a higher level of automation maturity by incorporating a network automation platform.

## Pros and cons of introducing network automation

Understanding both the benefits and the hurdles of network automation can help organizations make informed decisions about integrating automation into their network management practices. So, let’s dive deeper into the main advantages and possible challenges of this approach:

### The benefits of network automation


Unification and reduction of human error

Introducing changes at scale

Simplified tracking of changes

Using the best tools for the job

#### Enhanced network management

Implementing a Single Source of Truth / Single Source of Intent is transformative, especially in large and complex networks. For small networks, it centralizes data, making management easier. In larger infrastructures, it provides a comprehensive view that can bridge gaps between different network segments managed by various teams, facilitating end-to-end service delivery.

#### Scalability and efficiency in changes

Automation allows for changes to be made at scale, significantly reducing the time and effort required compared to manual processes. Tasks that once took multiple maintenance windows can now be executed in parallel, thanks to automation. This scalability is particularly beneficial in large networks, where manual changes would be impractical and time-consuming.

### Reduction of human error

Automation minimizes human error by ensuring tasks are executed consistently and accurately. Scripts and automation platforms provide a reliable way to implement changes, reducing the likelihood of mistakes. Additionally, automated rollbacks make it easier to reverse changes if something goes wrong.

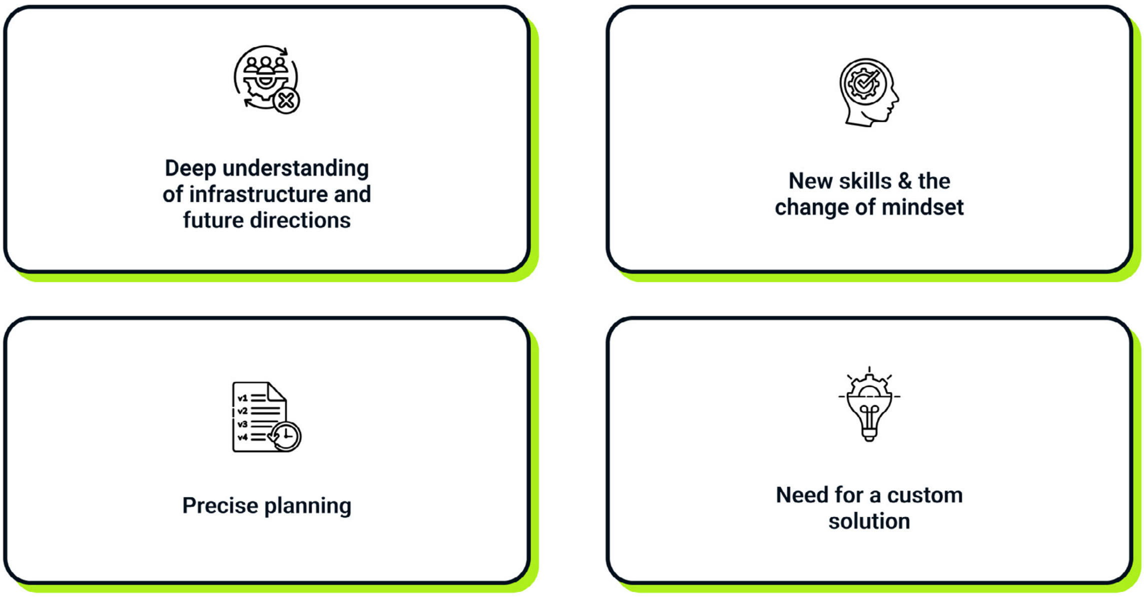
### Consistency and standardization

Standardization simplifies troubleshooting and ensures that best practices are consistently applied across the network, leading to more reliable operations.

### Improved change tracking and analysis

Detailed records of changes and their outcomes are invaluable for post-mortem analysis, helping to identify root causes and prevent future issues.

## The challenges of network automation



Deep understanding of infrastructure and future directions

New skills & the change of mindset

Precise planning

Need for a custom solution

### Demanding learning curve

Transitioning to network automation requires teams to learn new tools and technologies. While many engineers may already use these tools to some extent, full-scale automation demands a deeper understanding and proficiency.

### The shift in operational mindset

Automation changes how engineers interact with the network, moving from direct, hands-on configuration to script-based management. This shift introduces a layer of abstraction that can be challenging to adapt to.

### Need for precise planning and execution

With automation we can quickly implement changes across the entire network. However, this power also means that any errors can have widespread effects. Therefore, careful planning is essential. Engineers need to plan the order of changes, select the right devices, and choose appropriate testing methods.

Network automation offers numerous benefits, including enhanced understanding and management, scalability, error reduction, consistency, and improved change tracking. However, it also presents challenges, such as the need for new skills, a shift in operational mindset, and the necessity for precise planning.

## Case studies and real-world examples

This section highlights real-world applications of network automation, showcasing how organizations have tackled diverse challenges, from streamlining large-scale operations to reducing risks through automated validation processes.

Each case study demonstrates the benefits of automation, such as faster deployment times, enhanced reliability, and reduced human error.

### Case study #1 Automated VNF deployment in public clouds

automated provisioning | automated testing

A cybersecurity provider sought to streamline and scale virtual network function (VNF) deployments across multiple public cloud platforms. This case study demonstrates how automation can empower hardware vendors, multi-site enterprises, and cloud infrastructure providers aiming to optimize provisioning and testing processes.

**Challenge**:

The client's manual deployment processes were slow and error-prone, making it difficult to scale their operations effectively. They needed an automated solution to enhance accuracy and efficiency.

**Benefits:**

- Deployment time and effort were significantly reduced, allowing engineers to focus on strategic tasks.
- Automated testing minimized the risk of deployment failures, improving efficiency and lowering operational costs.

**Solution**:

We addressed this challenge by developing custom Terraform modules and fully automating the client's cloud infrastructure deployment process, including VNF bootstrapping.

Key features included:

- Integration with continuous integration and continuous deployment (CI/CD) pipelines across AWS, GCP and Azure to ensure a seamless and efficient deployment process.
- Extensive knowledge transfer and ongoing support to empower the client's engineering team to fully leverage the solution and adapt it to their specific operational needs.

**Technologies we used:** Terraform, GCP, AWS, Azure, GitHub Actions

## Case study #2 Large-scale network operations automation

network automation | operations automation

A healthcare enterprise faced challenges in managing software updates for a vast network of firewalls. This case study illustrates how automation can transform operations for hardware vendors, independent software vendors (ISVs), and large, multi-site organizations looking to enhance reliability and minimize downtime.

**Challenge**:

The client needed to update a large number of firewalls while ensuring minimal downtime and a high success rate due to the critical nature of healthcare services. With such restrictions it was challenging to keep the software up to date across all firewalls.

**Benefits:**

- Upgraded 500+ firewalls within three months, including 100 in a single maintenance window.
- Reduced downtime risk, ensuring healthcare service continuity and operational resilience.
- Automated backups and manual rollbacks in case of issues.

**Solution**:

We implemented a custom automation solution for safe, large-scale firewall upgrades. Key elements included:

- Automated upgrades for standalone firewalls and firewall clusters across physical and virtual environments, ensuring failover with no downtime.
- Readiness checks, comparison tests, and automated backups to ensure robust recovery in case of issues.
- Parallel workflows enabled more changes per maintenance window.

**Technologies we used:** Python, Ansible, AWX

## Case study #3 Automated pre- and post-checks for network operations

operations automation | network automation

Telecom operators and cloud providers often face challenges in validating large-scale network changes. This case study highlights the impact of automation in validating large-scale network changes, ensuring consistency and reducing human error.

**Challenge:**

The manual validation processes were not thorough enough, occasionally resulting in missed issues that caused post-cutover service disruptions. They needed a fully automated workflow with pre- and post-checks to validate all network changes.

**Benefits**:

- Increased network change reliability with comprehensive automated pre- and post-checks.
- Eliminated manual work, saving time and resources while reducing errors.
- Parallel workflows enabled more changes per maintenance window.

**Solution:**

We designed an automated workflow with pre- and post-checks to validate network changes. Key components included:

- Capturing snapshots of the network's operational state before and after changes for programmatic comparison.
- Running multiple pre- and post-check playbooks in parallel to increase operational efficiency.
- Testing and optimizing the process with a Digital Twin to simulate the production environment.

**Technologies we used:** Python, Ansible, AWX, Red Hat Ansible Tower

## Case study #4 Automated NFV telco cloud upgrade

network automation SDN telco cloud NFV

A hardware vendor and ISV sought to enhance their telco cloud operations by automating critical upgrade processes. This study showcases how data centers, cloud providers, telecoms, and ISPs can use automation to streamline SDN and ensure service continuity.

**Challenge**:

The client needed to ensure that their software-defined networking (SDN) deployment continued to perform optimally after a critical upgrade. They needed to validate that the upgrade did not impair real-time service functionality and continuity.

**Benefits**:

- Reduced risk and improved efficiency by enabling informed decisions based on an in-depth study of the SDN controller upgrade.

- Freed the client’s internal team from testing, saving time while ensuring network performance and functionality.

**Solution**:

We developed a detailed upgrade process for telco cloud components, focusing on:

- Analyzing the working state of the SDN controller and OpenStack environment and enhancing monitoring where necessary.
- Designing an upgrade procedure in manageable steps  with success/fail indicators, pre/post-checks, and DB backup/restore mechanisms.
- Automating upgrade steps using Ansible and Python scripts, integrated into CI pipelines with defined outputs..

**Technologies we used**: Openstack, KVM, Tungsten Fabric, Ansible, GitLab CI

As these success stories wouldn’t have been achievable without network automation tools, now is the perfect time to give them the spotlight.

# Tools for network automation

In this section, you'll find an overview of some of the most widely used network automation tools, focusing on their capabilities and business benefits.

## Ansible

Ansible is an open-source automation tool designed to simplify configuration management and task automation. It is agentless, meaning it does not require any software to be installed on the managed devices. Ansible uses YAML (Yet Another Markup Language) to define tasks in playbooks, which are easy to read and write.

Ansible excels in environments where consistency and repeatability are crucial. It allows for the rapid deployment of configurations across numerous devices, significantly reducing the time and effort required for manual configuration.

**Benefits of Ansible:**

- **Ease of use:** its straightforward syntax and declarative language make it accessible even for those new to automation.
- **Flexibility:** Ansible can manage a wide range of devices and applications, making it versatile for various network environments.
- **Scalability:** capable of handling large-scale deployments efficiently, Ansible ensures that configurations are consistently applied across all devices.

## Terraform

Terraform is a powerful infrastructure as code (IaC) tool that excels in provisioning and managing infrastructure across cloud providers and on-premises environments. It uses a declarative language called HCL (HashiCorp Configuration Language) to define the desired state of an infrastructure.

**Terraform benefits:**

- **State management:** Terraform tracks the current state of infrastructure, ensuring precise and reliable deployments.
- **Community and support:** a large community and extensive documentation provide robust support and resources for users.
- **Integration:** supports numerous providers, enabling seamless management of diverse infrastructure components.

### Python SDK

Python is a versatile programming language widely used for network automation due to its simplicity and extensive library support. While not an automation tool in itself, Python's flexibility allows for highly customized automation scripts tailored to specific network requirements.

Using SDKs (software development kits) network engineers can interact directly with network devices, creating detailed and complex automation solutions.

**Business benefits of Python SDK:**

- **Flexibility:** it offers unparalleled customization, allowing for tailored automation solutions.
- **Integration**: easily integrates with other tools and systems, enhancing overall automation capabilities.
- **Extensibility**: the wide range of available libraries and SDKs supports diverse automation needs.

### Which tool is the best choice?

Selecting the appropriate network automation tool depends on various factors, including the complexity of the network environment, the specific requirements of the automation tasks, and the expertise of the team. Each tool offers unique advantages:

- Ansible is ideal for quick, consistent configuration management across large numbers of devices.
- Terraform is best suited for comprehensive infrastructure management.
- Python SDK provides the highest degree of customization for complex and specific automation needs.

Ultimately, many organizations find that a combination of these tools offers the best results.

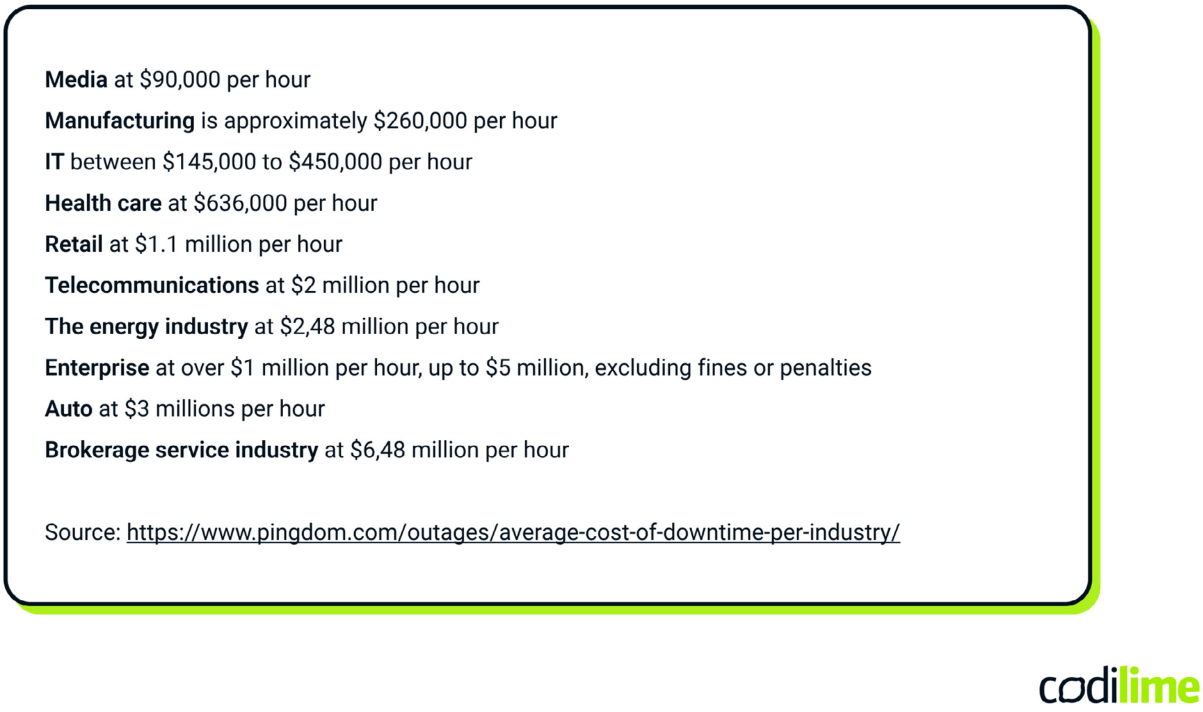
## ROI and cost of downtime

When discussing ROI (return on investment) and justifying investments in network automation, it's essential to highlight three key factors: cost reduction, enhanced reliability, and increased operational efficiency.

Downtime is inevitable, and the speed of recovery is crucial. Automated systems can recover faster from failures, reducing downtime significantly. Moreover, downtime can be extremely costly. For 98% of organizations, one hour of downtime costs over $100,000. Below, you can find more detailed information about potential downtime cost by industry:

**Up to $9,000 per minute**

For 98% of organizations one hour of downtime costs over $ 100,000.



**Media** at $90,000 per hour

**Manufacturing** is approximately $260,000 per hour

**IT** between $145,000 to $450,000 per hour

**Health care** at $636,000 per hour

**Retail** at $1.1 million per hour

**Telecommunications** at $2 million per hour

**The energy industry** at $2,48 million per hour

**Enterprise** at over $1 million per hour, up to $5 million, excluding fines or penalties

**Auto** at $3 millions per hour

**Brokerage service industry** at $6,48 million per hour

Source: https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/

However, losing money isn't the only critical reason to minimize downtime. Downtime can also severely damage a company's reputation, leading to loss of customer trust and potential long-term revenue loss. Having automation onboard allows for quicker post-mortem analyses and faster recovery, ensuring that systems can return to normal operations with minimal disruption.

Last, but not least, frequent downtime increases stress on employees and diverts their focus from productive tasks to emergency fixes, leading to overall reduced productivity.

## The future of network automation

The future of network automation will transform how businesses work. As networks become increasingly automated, engineers will have more time to develop new services and integrate cutting-edge technologies.

With automation, scalability is no longer a hurdle. Automated networks can effortlessly handle growth, allowing businesses to expand their operations globally without compromising performance or reliability.

Engineers freed from repetitive tasks can dedicate their expertise to driving technological advancements and optimizing network performance. Integrating AI with network automation promises even more significant improvements, providing deeper insights and proactive management capabilities.

## Summary

Network automation is increasingly essential for businesses that want to stay competitive. As networks continue to grow in complexity, managing them manually is no longer practical. By automating repetitive tasks, businesses can reduce the risk of human error, increase efficiency, and maintain a high level of security and compliance.

But beyond the immediate technical benefits, network automation frees up your teams to focus on what really matters: innovation and strategic growth. Rather than spending time on tedious, manual processes, your engineers can work on developing new services, enhancing customer experience, and driving your business forward. Automation also makes it easier to scale operations, meaning you can grow without worrying about whether your network infrastructure can keep up.

At the end of the day, network automation isn't just about making things easier; it's about making your business future-proof – the ability to quickly adapt to changes, minimize downtime, give space for innovation and business growth, and stay ahead of security risks. By creating this ebook, we wanted to give you the tools and insights to start (or continue) your automation journey, ensuring your network is ready for the future.

## About CodiLime

Since 2011, CodiLime has been the engineering partner of choice for semiconductor companies, networking vendors, telecom services, and software solution providers.

We're home to 250 top-notch software developers, network engineers, DevOps experts, and solution architects. We appreciate long-term collaborations above all, as well as our partners. Below are some of the names that have already trusted us:

cisco
paloalto NETWORKS
EQUINIX
JUNIPER NETWORKS
NUTANIX
altera An Intel Company
bigleaf networks
SELECTOR
NTT Security Holdings
FluxNinja
FREEDOMFI
CLOUDIFY
AT&T
NVIDIA
Captor Therapeutics
GIGASPACES innovate with confidence
MESH7
neptune.ai
swift NAVIGATION
Procyon

CodiLime aims to link network engineering talent with business domain expertise – we  focus on five N.E.E.D.S. - Networks, Equipment, Environment, Data and Security.