



2023 Global Network Automation Report

# Accelerating Value Creation, Operational Efficiency, and Cost Reduction

## Why DDI Is an Obvious Starting Point

June 2023

Authors:

Bruno Teyton, Associate Vice President, Telecommunications and Networking, IDC  
Romain Fouchereau, Research Manager, European Security, IDC

An IDC InfoBrief, Sponsored by



# Content

Executive Summary	3
Navigating the Storms of Disruption: Network Automation Takes Center Stage	4
Where Enterprises Stand in Network Automation Maturity	5
Organizational and Technical Challenges to Network Automation	6
Overcoming Organizational and Technical Barriers with Training, C-Level Sponsorship, New Processes and Technologies	7
Significant Multifaceted Benefits Aligned with Business Drivers	8
All Verticals and Company Sizes Benefit From Network Automation with Specific Strategies, Inhibitors, and Benefits	9
Road Map for a Successful Network Automation Journey	11
Organizations Focus on Network Automation Implementations in Datacenter, Campus, and Wide Area Networks	12
Leveraging Network Security Automation for NetSecOps	13
Get Started with Essential Network Automation Tools	14
NSoT and Open API Adoption Is Foundational to Network Automation	15
DDI Is Key to Accelerating Network Automation and Maximizing Benefits	16
Essential Guidance	17
About EfficientIP	18
Methodology	19



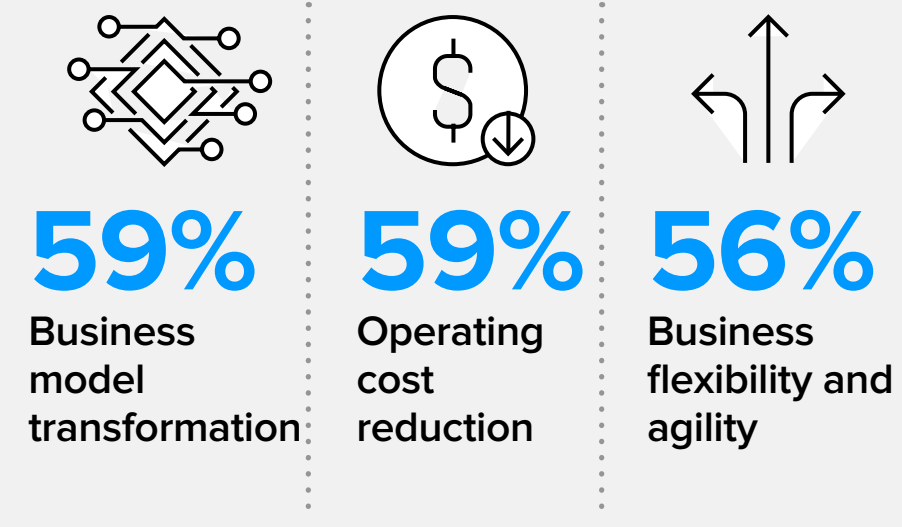
# Executive Summary

Driven by the uncertain economic outlook, enterprises are adopting new strategies to achieve greater cost savings, improve efficiency, and create value. Network automation is at the forefront of this, enabling IT teams to gain the required flexibility and agility.

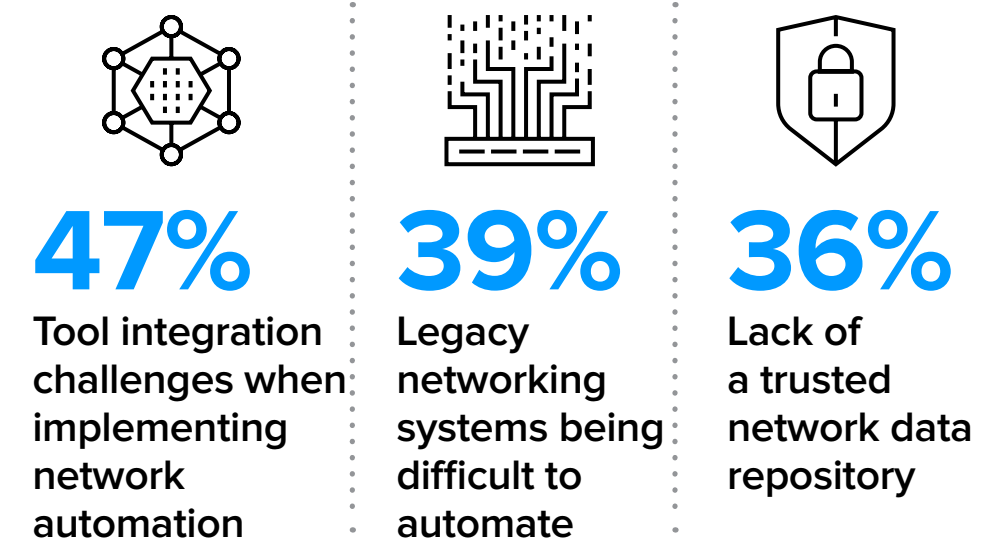
Nevertheless, full automation of network processes across the board will not happen overnight. Enterprises need to implement network automation now, starting small then iterating with first quick wins that do not impact production processes and organizations, such as network maintenance, observability and monitoring, or troubleshooting. Initial low-hanging fruit can have a significant impact and build the foundation for new initiatives across network domains, such as network security, compliance, provisioning, and deployment. Adopting a stepped approach and road map will enable enterprises to grow their maturity. Fostering cross-team collaboration and agile practices will also enable network automation.

## Network Automation key highlights:

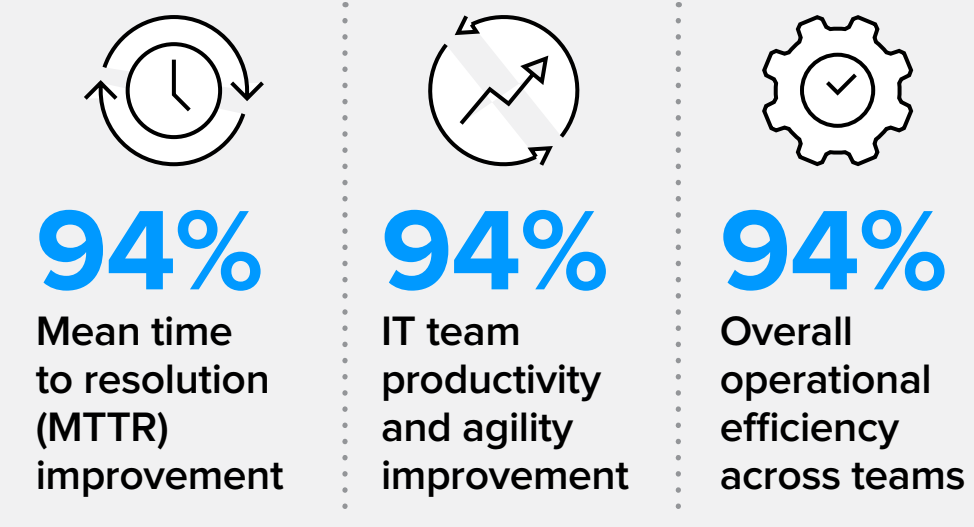
### Top 3 business drivers:



### Top 3 technical inhibitors:



### Top 3 achieved benefits:



More than 80% of enterprises acknowledge the importance of DNS DHCP and IP address management (DDI) and Network Source of Truth (NSoT) in their automation strategy. Organizations are realizing that DDI and NSoT are key success factors to overcome challenges such as a lack of consistency in network automation initiatives and siloed data. Using open APIs, DDI enables smooth integration with the IT ecosystem, removing the complexity to automate. Organizations using DDI realize greater benefits, especially in operational efficiency, cost reduction, security and compliance, network resilience, and IT team productivity and agility. Network automation without DDI makes no sense.



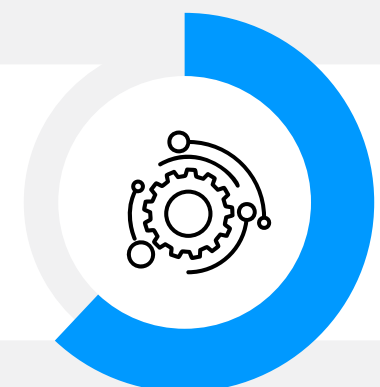
**Network automation is now a no-brainer and is being embraced by a growing number of enterprises as an enabler of their business transformation. So, the question is no longer why but how to make it happen. It's where DDI with built-in NSoT and open APIs capability brings a significant advantage as a true network automation hub to use efficiently at every stage of network automation tasks and activities.**

Jean-Yves Bisiaux CTO, EfficientIP

**74%** of organizations already use or will use DDI over the next two years.



Thanks to DDI, benefits of network automation are amplified up to **62%**



# Navigating the Storms of Disruption: Network Automation Takes Center Stage

Networking teams are under growing pressure to keep pace with technologies and ever-changing business needs. Understanding the state of the network and automating networking life-cycle tasks are key success factors to adapt to digital business transformation.

Network automation is future-proof: it enables business model transformation and is a key anchor for business growth. Given the economic headwinds — inflation, higher energy costs, interest rate increases, the risk of recession — “doing more with less” is truer than ever. Network automation reduces IT operating costs and improves business productivity by reducing outages and faults. At the same time, network automation improves business efficiency by enabling flexibility while improving the user experience with resilient infrastructure.



After infrastructure cost and lack of executive alignment of digital infrastructure, insufficient automation to optimize workloads and infrastructure **(with 34%\*)** is the third main barrier for organizations to achieve business priorities.

## Key Network Automation Business and Organizational Drivers



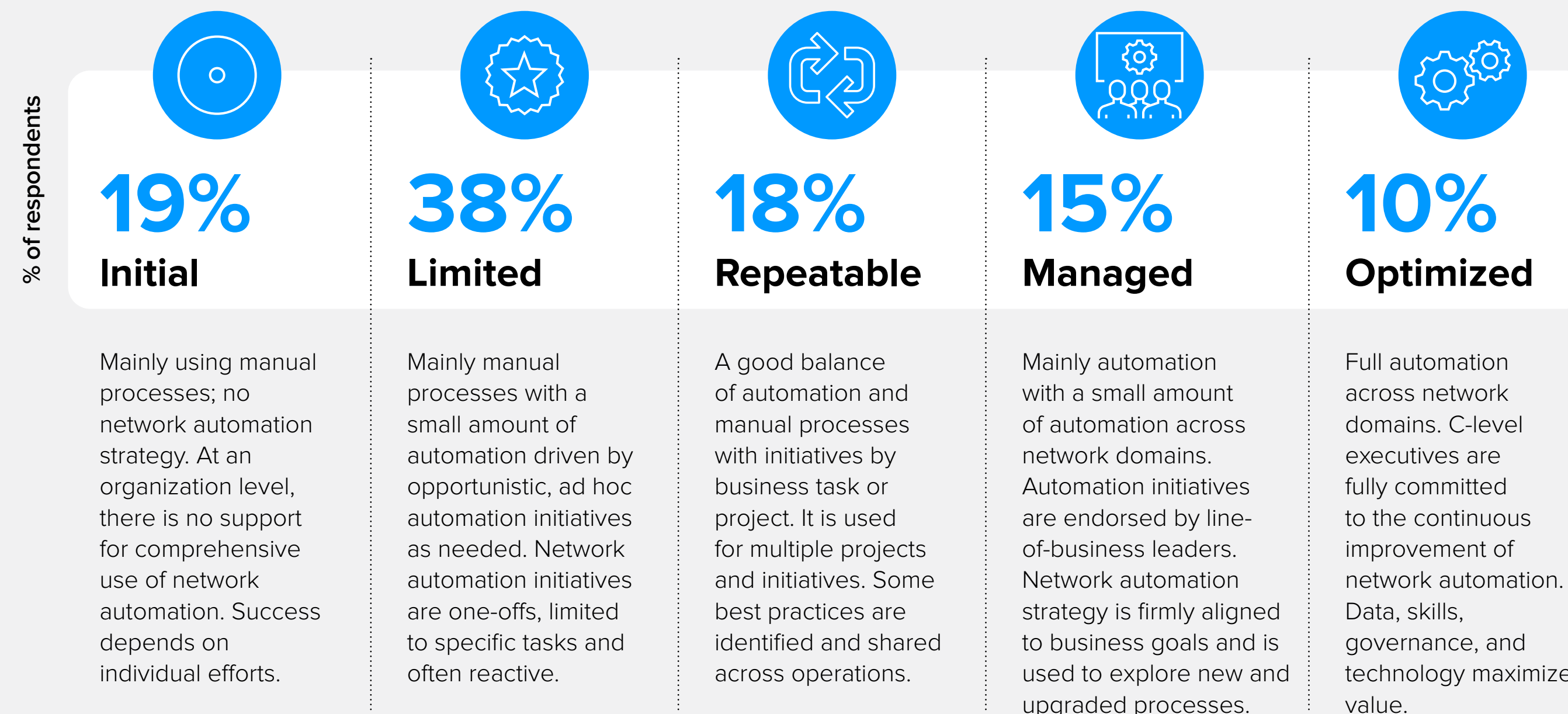
Network automation is critical to deliver business goals. Align your network automation strategy with your own “create, control, and improve” drivers.



# Where Enterprises Stand in Network Automation Maturity

Organizations are at various stages of their network automation journey. IDC's Network Automation Maturity Index helps to determine maturity level across the datacenter network, wide area network, campus network, public cloud network, and network security. There are five stages of maturity, and each maturity level builds on the capabilities of the previous one, with the most mature leveraging automation-first initiatives organizationwide.

## Network Automation maturity index



## A stepped approach toward Network Automation

- Not every enterprise starts network automation with a strategy.
- Midsize enterprises are less advanced strategywise.
- Organizations can start small with ad hoc, limited initiatives not associated with change, production processes, and organization.
- After a ramp-up phase shaping a nascent culture of network automation, organizations will progress on the maturity Index, define strategy and road map, then iterate with broader initiatives.
- It's an iterative process until organizations reach the most mature stage of maturity, paving the way to agility and innovation.

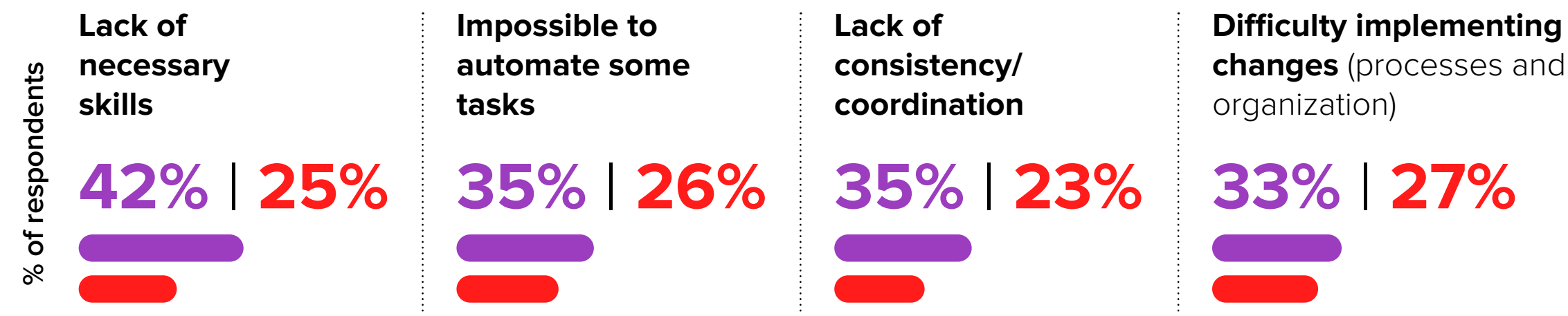
Beyond the network automation strategy, organizations should assess where they are on the network automation maturity index to effectively prioritize automation projects tied to business drivers and build out a road map that will speed up their progress on the path to transformation. Organizations need to define their network automation governance accordingly.



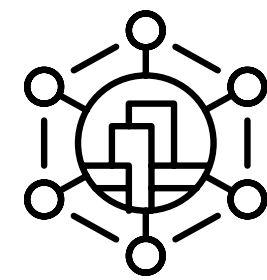
# Organizational and Technical Challenges to Network Automation

Network automation is complex, and enterprises face multiple technical and organizational difficulties and pain points. These challenges become less of an issue, however, as organizations move up the learning curve and become more mature.

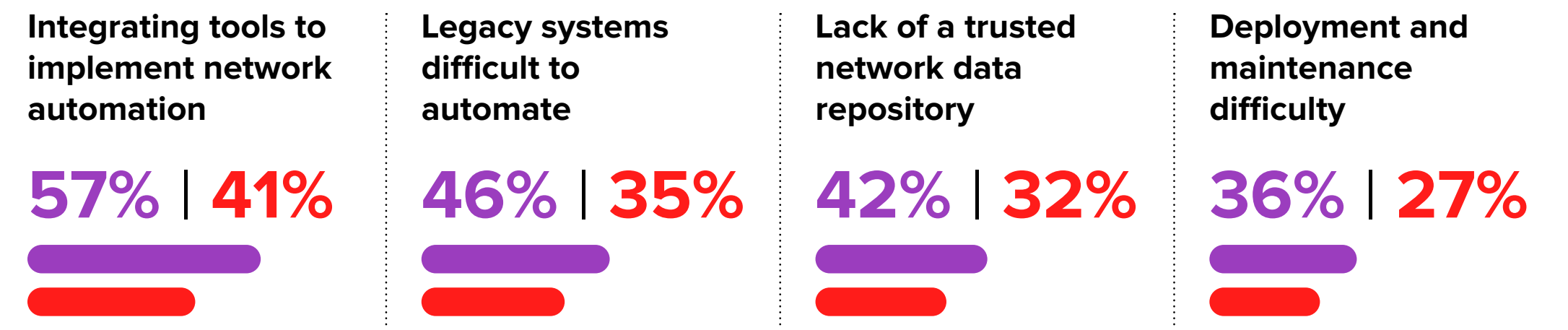
## Organizational challenges: plan to use automation versus already use automation



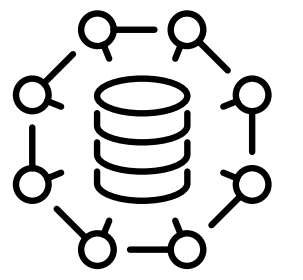
Organizations struggle with the fast pace of change brought by digital technology adoption and business model innovation. They need to accelerate organizational transformation and develop a culture of change.



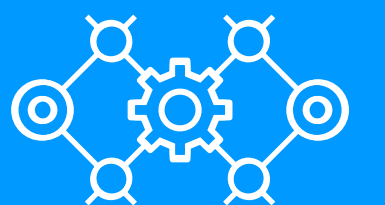
## Technical challenges: plan to use automation versus already use automation



The lack of a trusted network data repository is one of the top challenges. Without a network source of truth, network data remains siloed and fragmented across the organization and prevents organizations from managing the life cycle of network objects and devices easily and efficiently.



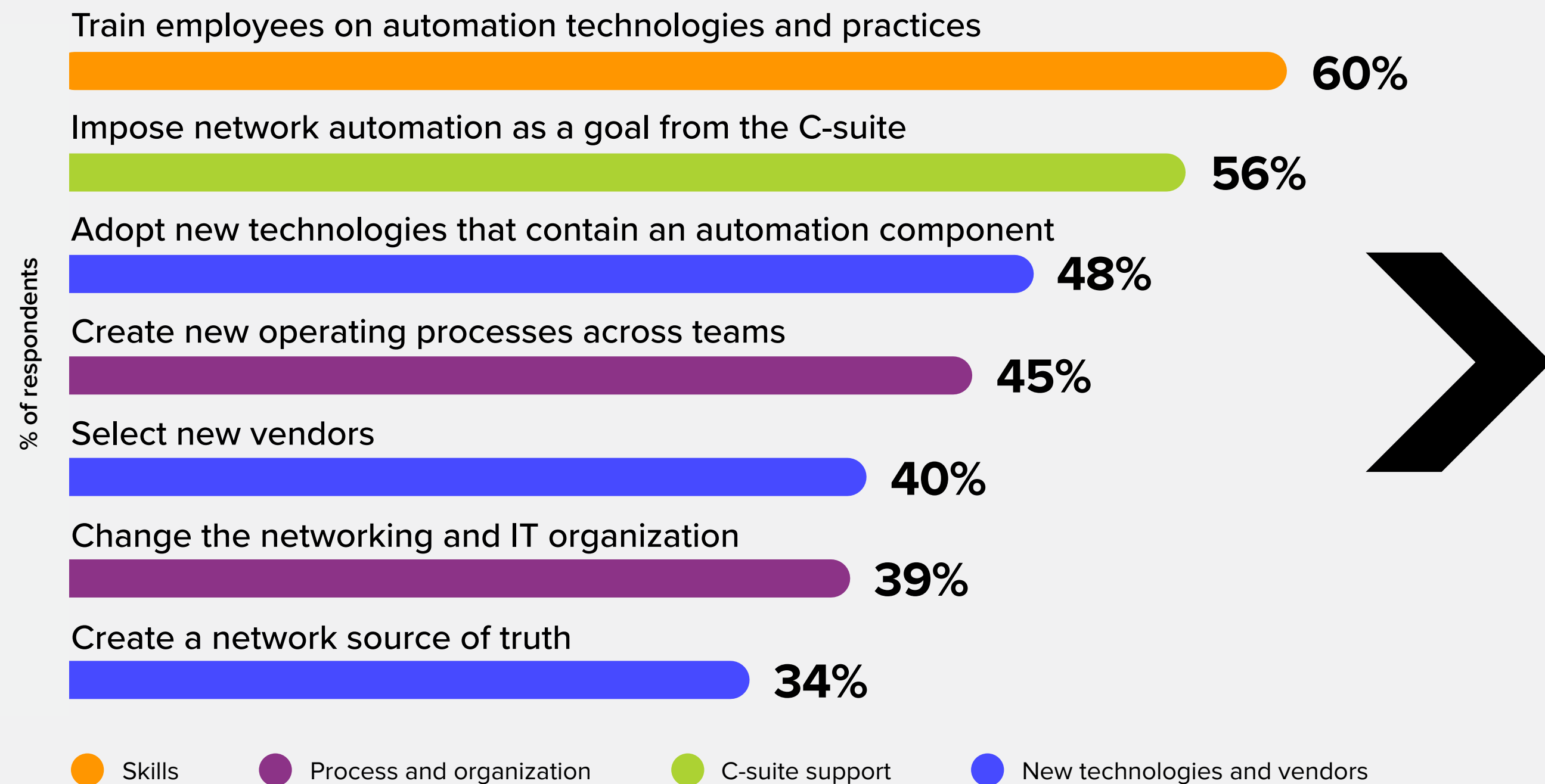
Organizations that are now planning to automate have greater concerns and challenges than those organizations that have already started their automation journey. Starting with network automation is key to overcoming the perceived technical challenges. 59% of respondents at the Optimized stage of the maturity index do not report any technical issues.



# Overcoming Organizational and Technical Barriers with Training, C-Level Sponsorship, New Processes and Technologies

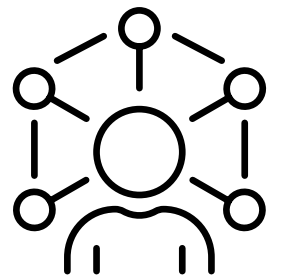
Overcoming key hurdles such as a lack of consistency in network automation initiatives and difficulties implementing changes in processes and organization requires strong **support from C-level executives**. Network automation requires a holistic and systemic approach and the involvement of management across the enterprise.

## Seven ways to remove barriers



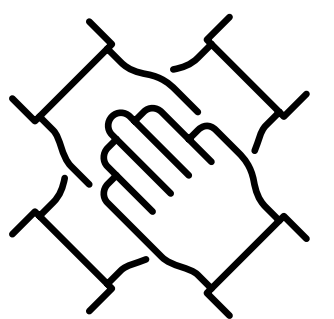
### Talent and skills are paramount.

Networking engineers and technicians must develop new skills in AI/ML, data modeling, API management, scripting, CI/CD tools, cross-domain expertise, data gathering, etc.



### Process changes and team collaboration are crucial.

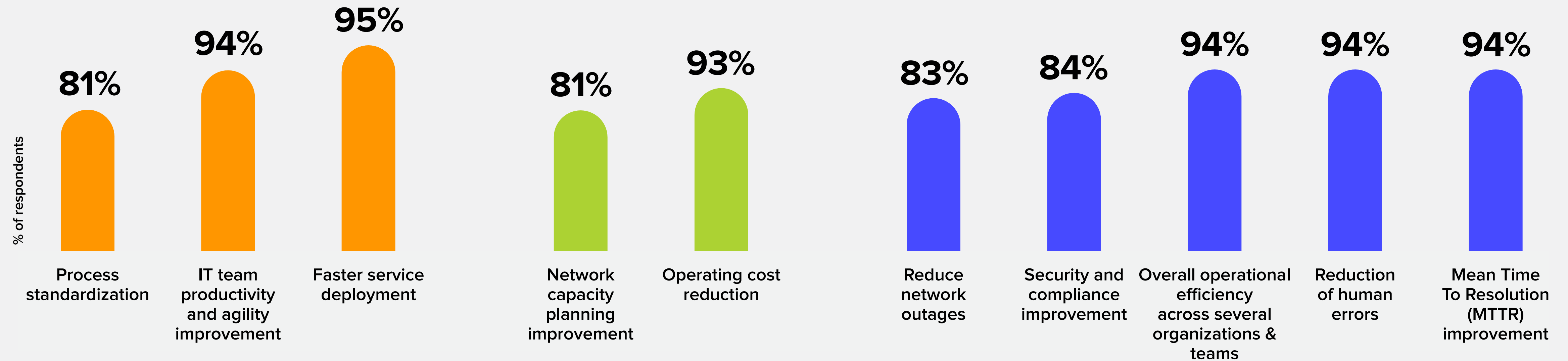
Organizations at the Optimized maturity level have changed their organization: **70% have fully integrated teams** between networking and other domains (DevOps, ITOps, SecOps, etc.). Agile frameworks are also implemented by 52% of organizations.



**New technologies and vendors** play a key role in unlocking network automation implementation. APIs, plugins (no-code/low-code), and network source of truth are **essential** to build network automation.

# Significant Multifaceted Benefits Aligned with Business Drivers

## Achieved benefits



### Create value

With faster service deployments, process standardization, and IT agility improvements, IT teams are now better equipped to realize their business transformation goals.



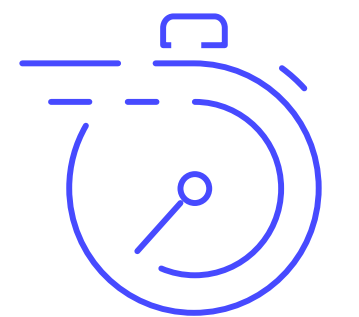
### Control costs

Operating costs have been reduced, even though a third of organizations were not expecting such benefits.



### Improve operational efficiency

With improved MTTR and fewer human errors and network outages, organizations can deliver a better customer experience and build a resilient and reliable infrastructure.



**Whatever the position in the maturity grid, organizations always get significant benefits in terms of speed, cost, and efficiency. At every step in their network automation journey, they can harvest low-hanging fruit before moving to wider initiatives. Network automation ultimately delivers more than expected.**



# All Verticals and Company Sizes Benefit From Network Automation with Specific Strategies, Inhibitors, and Benefits

Only 41% of midsize enterprises (500–999) versus 65% of large and very large companies (1,000+) use network automation. 49% of midsize enterprises are at the Initial stage in the Network Automation Maturity Index. They pursue the same goals and have the same drivers, but they suffer from specific organizational inhibitors:

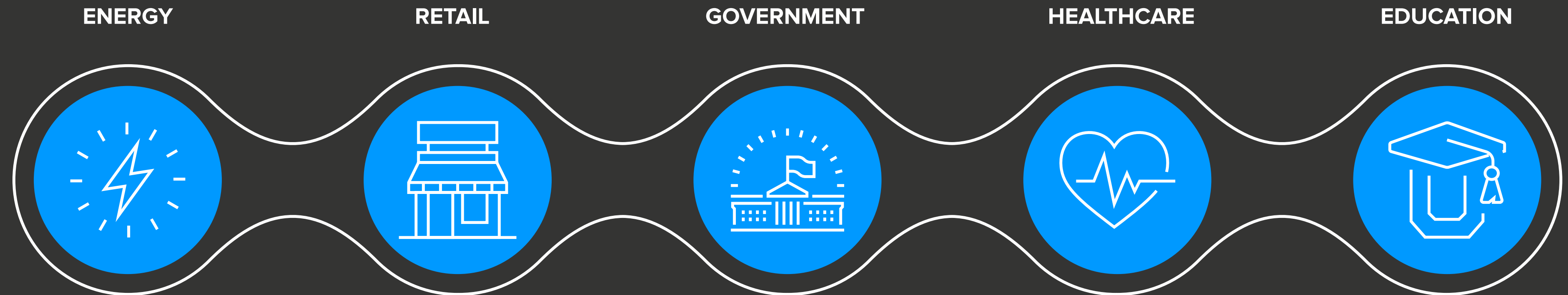


- **Lack of skills:** midsize enterprises (42%) versus large and very large enterprises (30%)
- **Lack of consistency and coordination between network automation initiatives:** midsize enterprises (37%) versus large and very large enterprises (26%)



	FINANCE	MANUFACTURING	PROFESSIONAL SERVICES	TELCO, MEDIA, AND ENTERTAINMENT	TRANSPORTATION AND LOGISTICS
<b>Network automation maturity level</b>	<b>35% of organizations are Repeatable or Managed</b>	<b>53% of organizations are Limited or Repeatable</b>	<b>39% of organizations are Managed or Optimized</b>	<b>61% of organizations are Limited or Repeatable</b>	<b>27% of organizations are Managed or Optimized</b>
<b>Top 3 business drivers</b>	Business flexibility and agility, business model transformation, customer experience	Operating cost reduction, business model transformation, business flexibility and agility	Business model transformation, business flexibility and agility, customer experience	Business model transformation, operating cost reduction, business flexibility and agility	Customer experience, operating cost reduction, business model transformation
<b>Top 3 organizational inhibitors</b>	Lack of necessary skills, lack of consistency/coordination in network automation initiatives, difficulty implementing changes in processes and organization	Difficulty implementing changes in processes and organization, lack of necessary skills, lack of consistency/coordination in network automation initiatives	Difficulty implementing changes in processes and organization, security concerns, lack of necessary skills	Lack of necessary skills, not possible to automate some tasks, lack of consistency/coordination in network automation initiatives	Not possible to automate some tasks, difficulty implementing changes in processes and organization, lack of necessary skills
<b>Top expected and achieved benefits</b>	IT team productivity and agility improvement, MTTR improvement, faster service deployment	Overall operational efficiency across several organizations/teams, operating cost reduction, MTTR improvement	Overall operational efficiency across several organizations/teams, reduction of human errors, network capacity planning improvement	IT team productivity and agility improvement, operating cost reduction, MTTP improvement	Overall operational efficiency across several organizations/teams, MTTR improvement, faster service deployment

# All Verticals and Company Sizes Benefit From Network Automation with Specific Strategies, Inhibitors, and Benefits

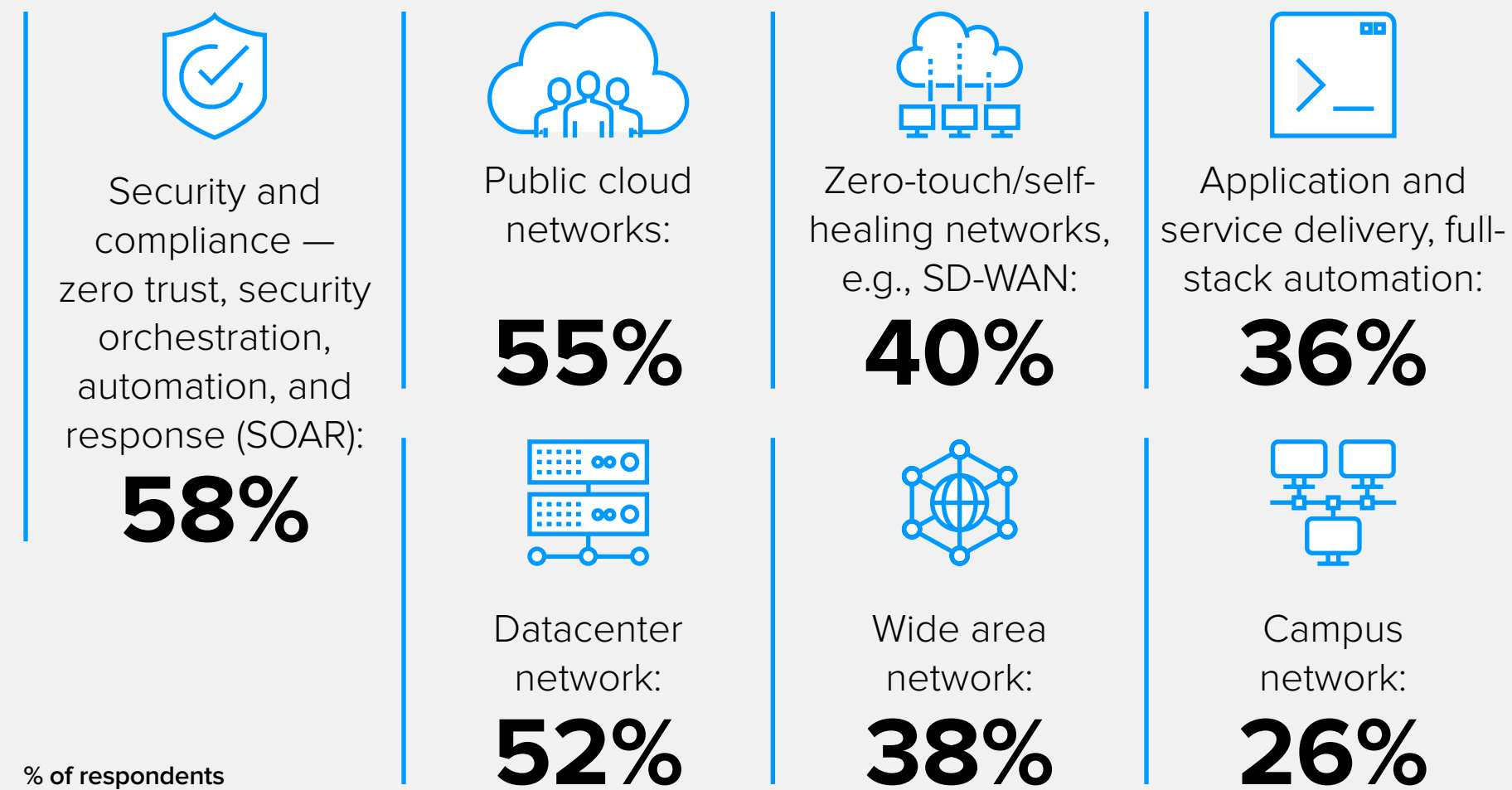


	ENERGY	RETAIL	GOVERNMENT	HEALTHCARE	EDUCATION
<b>Network automation maturity level</b>	<b>63% of organizations are Initial or Limited</b>	<b>62% of organizations are Initial or Limited</b>	<b>69% of organizations are Initial or Limited</b>	<b>67% of organizations are Initial or Limited</b>	<b>46% of organizations are Limited</b>
<b>Top 3 business drivers</b>	Customer experience, business flexibility and agility, customer experience	Operating cost reduction, business model transformation, business flexibility and agility	Operating cost reduction, customer experience, business flexibility and agility	Operating cost reduction, business model transformation, customer experience	Operating cost reduction, customer experience, business flexibility and agility
<b>Top 3 organizational inhibitors</b>	Lack of necessary skills, not possible to automate some tasks, lack of consistency/coordination in network automation initiatives	Lack of necessary skills, not possible to automate some tasks, lack of consistency/coordination in network automation initiatives	Difficulty implementing changes in processes and organization, lack of necessary skills, lack of consistency/coordination in network automation initiatives	Difficulty implementing changes in process and organization, lack of necessary skills, lack of consistency/coordination in network automation initiatives	Not possible to automate some tasks, difficulty implementing changes in processes and organization, security concerns
<b>Top expected and achieved benefits</b>	Overall operational efficiency across several organizations/teams, MTTR improvement, faster service deployment	Faster service deployment, MTTR improvement, overall operational efficiency across several organizations/teams	Overall operational efficiency across several organizations/teams, IT team productivity and agility improvement, reduction of human errors	MTTR improvement, operating cost reduction, IT team productivity and agility improvement	IT team productivity and agility improvement, faster services deployment, reduction of human errors

# Road Map for a Successful Network Automation Journey

On average, it takes three to five years for enterprises to reach their final targeted automation level. **36%** of organizations are in this case. However, depending on the network automation maturity level, it can be reduced to one or two years for 30% of respondents, while 54% of Optimized companies have already reached their network automation goals.

## Key network domains of focus over the next two years:



For each of these network domains, organizations must consider where they are on the time horizon and prioritize key network automation initiatives accordingly.

## Horizon 3 — three to five years; continuously improve and experience full agility with:

- Network policies
- Network change provisioning and deployment, use of zero-touch provisioning end to end
- Inventory and visibility

## Horizon 2 — one to two years; iterate and grow with:

- Network efficiencies, resource management, and quality of service
- Network security analysis, anomaly detection
- Security incident remediation

## Horizon 1 — immediate; start small with:

- Network maintenance: automated upgrades and changes, patches, and security updates
- Network state monitoring and observability, analysis, troubleshooting, and remediation

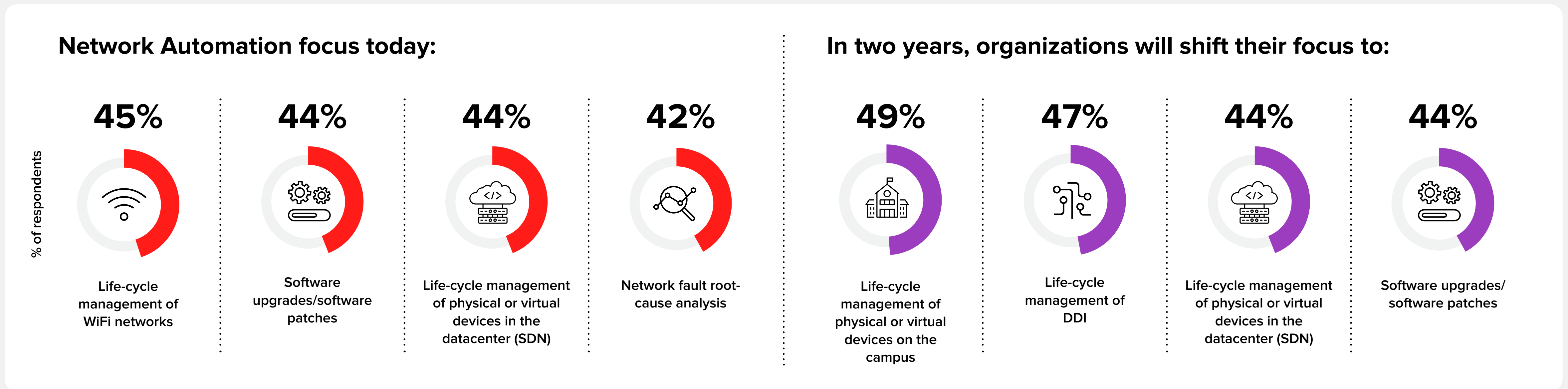


**Enterprises must start small now then iterate to grow their maturity level and change horizon. They will achieve the first quick wins with network maintenance, observability, monitoring, and inventory, before tackling network security, compliance, provisioning and deployment according to their network domain priorities.**

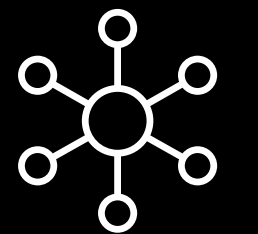


# Organizations Focus on Network Automation Implementations in Datacenter, Campus, and Wide Area Networks

Enterprises have mostly invested in datacenter network automation while WAN and campus networks are lagging, with the exception of WiFi. This is reflected in the level of maturity of organizations that have adopted automation in DC: **60%** have reached the most mature level, ranging from Repeatable to Optimized, against 46% for WAN and 39% for campus network. But this may change over the next two years.



Networks are no longer static, and enterprises must focus on the complete end-to-end networking life cycle of resources (VMs, VPC, access points, etc.), from provisioning to decommissioning. This is where DDI comes into play. By storing any IP-related and network data, as well as activating DNS services, DDI is instrumental in implementing end-to-end life-cycle management and automated workflows.



# Leveraging Network Security Automation for NetSecOps

Many organizations have adopted automation for network security, but they are quite advanced on the maturity index as 28% of Repeatable organizations have achieved a high level of security automation (against 71% for Optimized). **78%** of organizations already use DNS telemetry to share data and security events with SecOps teams, **29% of which as a fully automated process.**



**The visibility of actionable network and security data can improve incident remediation, observability and monitoring, experience, and productivity. Organizations can move a step forward by automating the sharing of such data between NetOps and SecOps and integrating with their security analysis tools and data repositories for efficient threat intelligence.**

Romain Fouchereau, Research Manager,  
European Security, IDC

## Network security automation focus:

**51%**  
Cloud security policies

**50%**  
Incident remediation

**44%**  
Observability and monitoring

**43%**  
Firewall policy management

## In two years, organizations will shift their focus to:

**37%**  
Firewall configuration changes

**29%**  
Vulnerability scanning

**32%**  
Ongoing cloud security policies

**27%**  
SASE solutions life cycle

% of respondents

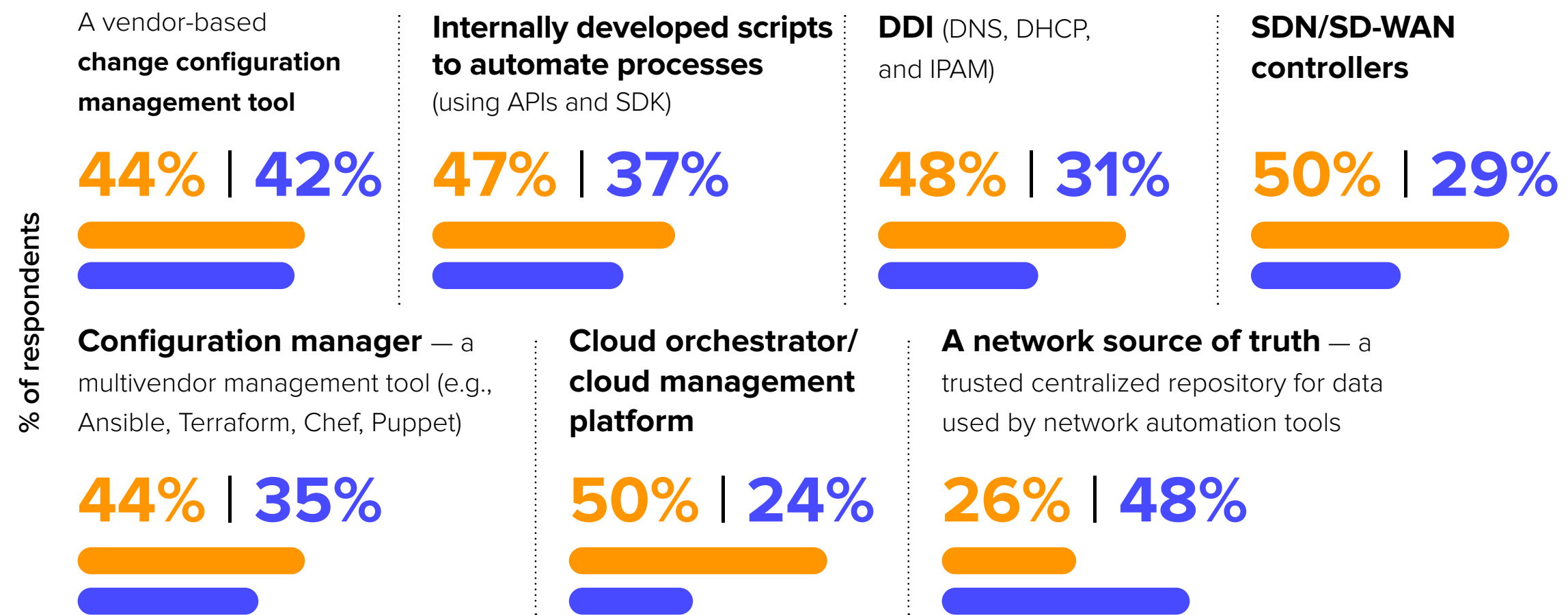
Networks and IT teams are facing growing complexity and pressure from the increase in cyberthreats. Actionable data that enables quick decision making and remediation, policy management, and configuration changes in almost real time are critical to strengthen organizations' security posture. By including DDI in their network security automation, organizations empower NetSecOps and accelerate security policy and configuration change rollout, with greater reliability and agility than with manual operations. Organizations also benefit from actionable data on the overall traffic that can feed their threat intelligence and help in early attack detection.



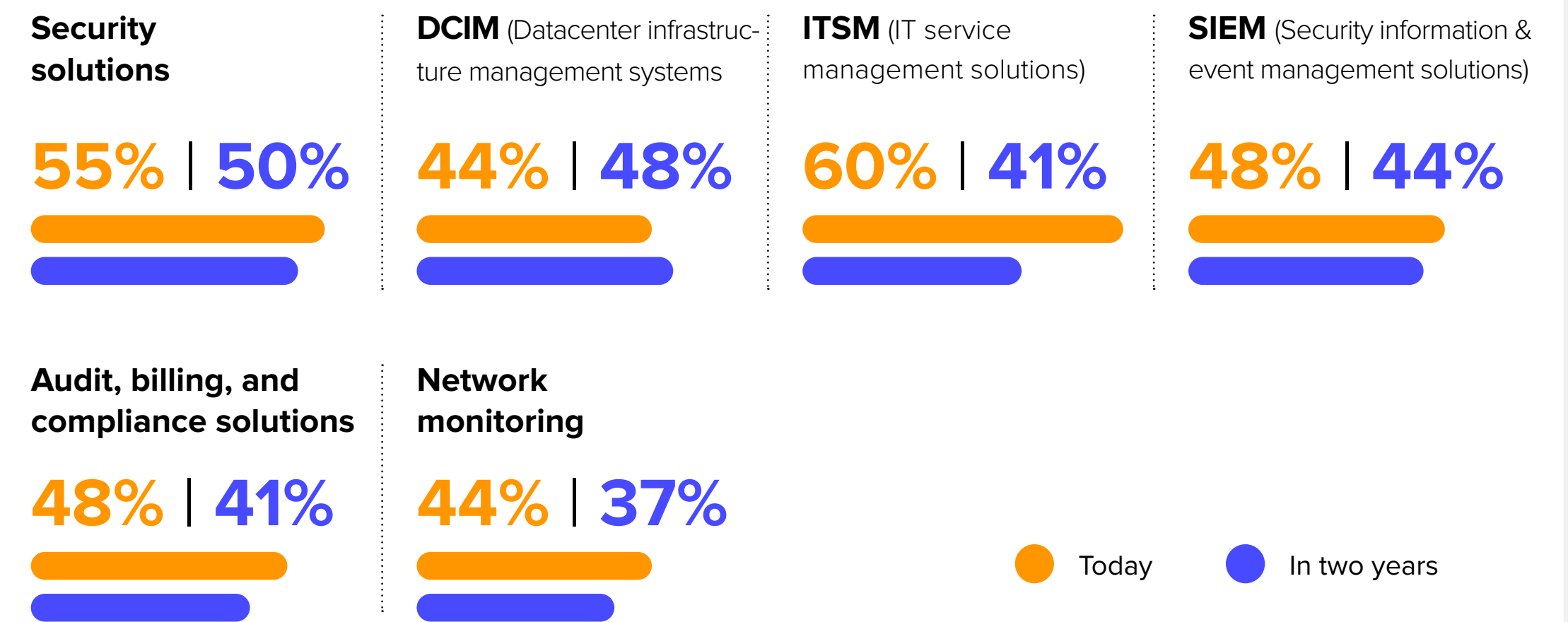
# Get Started with Essential Network Automation Tools

Organizations that have kicked off their network automation journey use the tools listed below. Not using a tool is not an option. The three top tools used by Optimized organizations are internally developed scripts (APIs and SDKs), cloud orchestrators, and DDI.

## Network automation tools use: today versus in two years



## Top IT systems integrated with network automation tools: today versus in two years



Open APIs are the glue that enables interconnection of the whole IT infrastructure, systems, and application management ecosystem to create value. They are a foundation to automate workflows, streamline processes, and unlock network automation potential by delivering contextual and actionable data back and forth.

Romain Fouchereau, Research Manager, European Security, IDC

**66%** of organizations with network automation plans say DDI is their main tool in their network automation strategy for the next two years, ahead of internally developed scripts (63%) and SDN/SD-WAN controllers (53%).

**48%** of organizations plan to use an NSoT in the next two years, compared with just 26% today. To do so, they will need to leverage DDI to consolidate all IP and networking information in a unique, trusted, and always up-to-date repository.

# NSoT and Open API Adoption Is Foundational to Network Automation

An NSoT is a centralized, open, and comprehensive repository for data and metadata used by network automation tools. While adoption is still limited, organizations recognize its importance over the next two years. Its importance is steadily growing along with the network automation maturity level, e.g., **from 32%** for Initial and Limited organizations **to 63%** for Optimized organizations.



**Secure and seamless integration between third-party solutions to implement end-to-end life cycle management of their infrastructure, applications, and devices is made easy with APIs - from the moment of provisioning, all the way through decommissioning.**

**Romain Fouchereau**, Research Manager,  
European Security, IDC

## NSoT is already a key component of a network automation strategy:



**78%**

of organizations say it is already important or very important



**81%**

of organizations say it will be important or very important in the next two years



Only

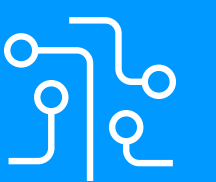
**2%**

say it will **NOT** be important at all in the next two years

## Organizations using network automation with an NSoT at the same time use a wide range of solutions:

- **55%** CMDB
- **49%** network controllers
- **46%** IPAM solutions
- **42%** DCIM systems
- **42%** network discovery solutions
- **41%** Excel
- **30%** homegrown solution

**NSoT is a key enabler of technical and business benefits from network automation. Consolidating all sources of truth into a unique, accurate, and always up-to-date repository will enable consistency and better control across the network to ensure that it behaves and performs as intended. DDI is an essential NSoT, as it is the foundation of all networking resources (including IP addresses, subnets, and domain names).**



# DDI Is Key to Accelerating Network Automation and Maximizing Benefits

Whatever their level of maturity, organizations say DDI is instrumental to making progress on their network automation journey. **58% of organizations already use DDI solutions for network automation; in two years, this is expected to grow to 74%.**

% of respondents

## DDI is a key component of any network automation plan:

- 81% say it is important or very important today
- 88% say it will be important or very important in the next two years

## Current DDI usage in:

- Security compliance: **55%**
- Infrastructure and application life-cycle management: **52%**
- Management and security policy enforcement: **49%**
- Multivendor DNS DHCP management: **47%**

DDI as a true NSoT plays a pivotal role in network automation with improved visibility, a trusted repository, and consistent control for end-to-end management. At every stage of the Network Automation Maturity Index, DDI delivers positive and measurable benefits. Initial and Limited organizations can start with automated changes and upgrades while Repeatable organizations can focus on security remediation and process standardization. Managed and Optimized organizations leverage DDI for zero-touch provisioning and new use cases such as SASE and 5G slicing. Network automation without DDI makes no sense.

**Bruno Teyton**, Associate Vice President, Telecommunications and Networking, IDC

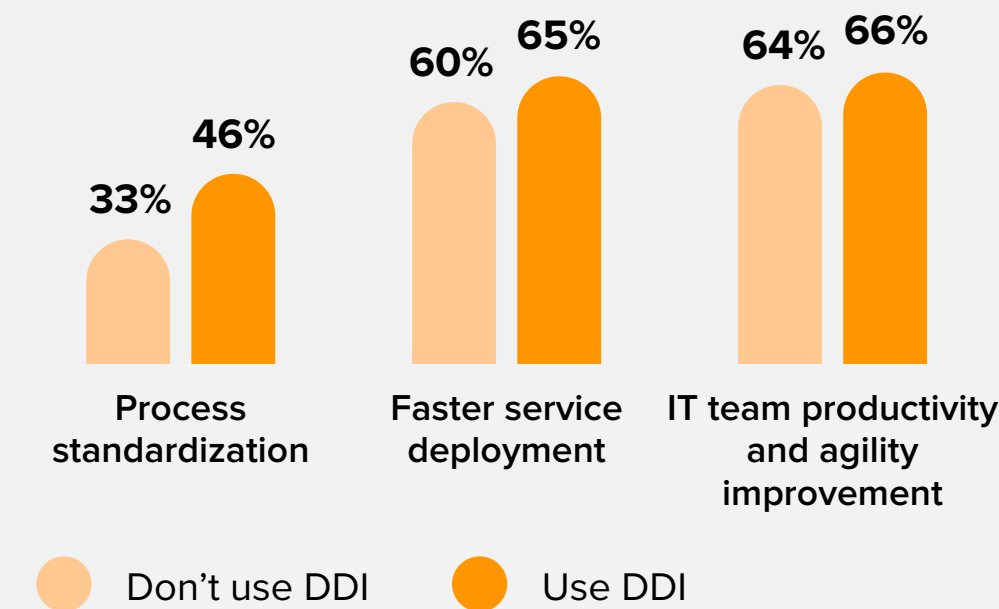
## Network automation expected and achieved benefits are maximized for organizations using DDI

### Main DDI benefits of network automation:

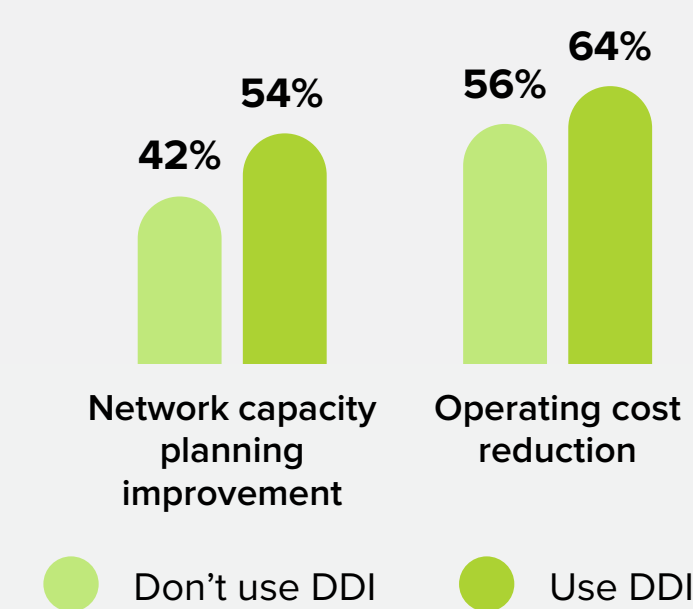
- Risk reduction: **40%**
- Consolidated and trusted network data: **35%**
- Management simplification and agility: **35%**
- Service continuity improvement: **33%**
- Process standardization: **33%**
- Financial benefits: **26%**

% of respondents

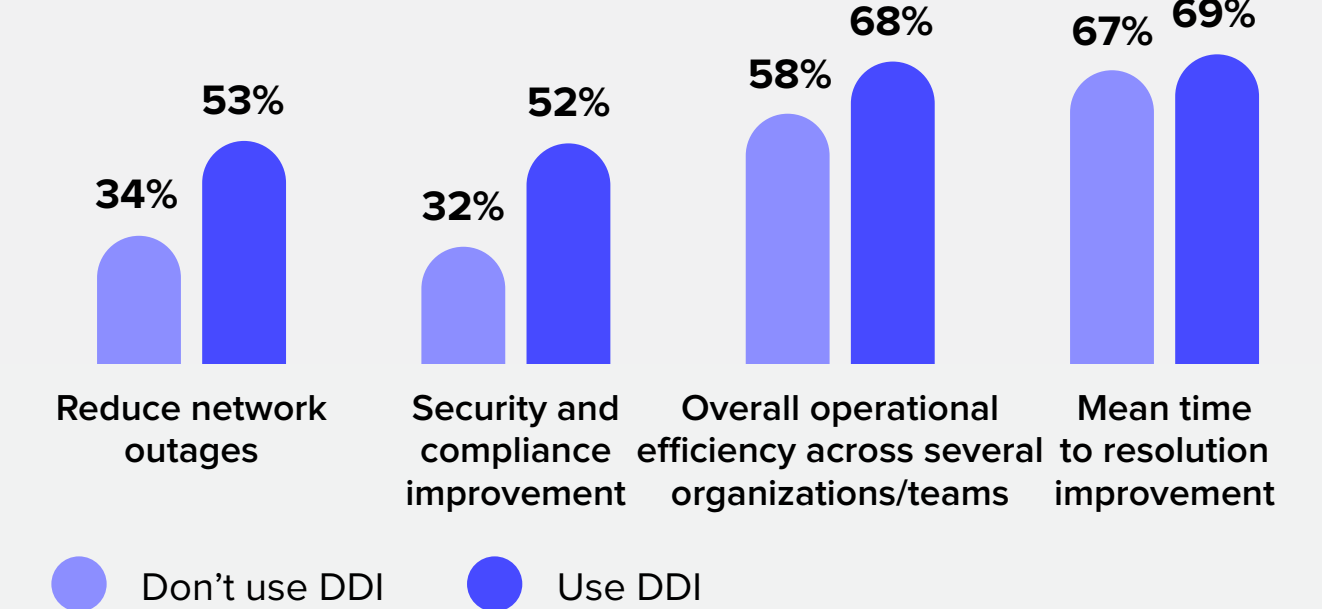
### Create value



### Control costs



### Improve operational efficiency



Non-DDI users n = 384, DDI users n = 278

DDI is future-proof and a key success factor when it comes to accelerating network automation, especially leveraging IPAM, DHCP, and DNS services. With DDI, enterprises can achieve significant benefits aligned on business drivers whatever their network automation maturity. Using DDI further removes obstacles, accelerates network automation initiatives, and delivers superior outcomes.



# Essential Guidance

Network automation is key to achieving business goals such as value creation, cost control, and operational efficiency improvement. Enterprises can start their automation journey small with ad hoc or limited initiatives, then iterate with broader initiatives to maximize their maturity level. They will quickly see the initial gains in terms of outage and cost reductions, as well as productivity and security improvements. DDI and NSoT are foundational to the success of network automation initiatives, serving as a true network automation hub that pulls and pushes actionable data through automated workflows. Whatever their position on the network automation maturity index, organizations using DDI have already achieved greater benefits than non-DDI users.

## DDI levels up enterprises' network automation strategy and plans

1

**DDI provides a consolidated, trusted, and always accurate built-in NSoT to enable full-stack end-to-end network automation.**

2

**Using open APIs, DDI unlocks value by interconnecting the IT system tools and ecosystem to enable end-to-end life-cycle management of networking operations from provisioning to decommissioning of resources.**

3

**Organizations can leverage DDI to automate NetSecOps and accelerate deployment of security policies, and ensure rules configurations are always up to date and accurate.**

# About EfficientIP

EfficientIP is a network security and automation company that specializes in DNS-DHCP-IPAM (DDI). We promote business continuity by making your IP infrastructure foundation reliable, agile, and secure. Since 2004, we have continued to expand our reach, providing solutions, professional services, and support all over the world with the help of select business partners. Our teams have delivered successful projects to over 1,000 customers globally and ensured operational efficiency through dedicated customer care.

**Our goal is to enable secure and dynamic IP communication between users and apps/services. We achieve this by:**

- Securing DNS services to protect users, apps, and data, and ensure service continuity
- Simplifying life-cycle management of DDI resources, via smart automation, cross-platform visibility, and policy control through a single pane of glass

Companies rely on us to help control the risks and reduce the complexity of the challenges they face. This applies particularly to modern IT initiatives such as cloud applications, virtualization, mobility, digital transformation, and SDN.

**For more information, visit**

**[www.efficientip.com](http://www.efficientip.com)** and follow **@efficientip** on Twitter.



# Methodology

This IDC InfoBrief is based on a survey IDC conducted on behalf of EfficientIP of 1,100 organizations around the world in December 2022 and January 2023 with CATI or CAWI methodologies.



All 1,100 respondents are responsible for setting network automation strategy in their organization.



662 respondents use network automation.



438 respondents plan to use network automation in the next two years.



Enterprises not using and not planning to use network automation in the next two years were excluded.

## 5 Business size segments



### Midsize enterprise:

- 500 to 999 employees: **216**

### Large enterprise: **884:**

- 1,000 to 2,499 employees: **235**
- 2,500 to 4,999 employees: **225**
- 5,000 to 9,999 employees: **212**

### Very large enterprise:

- 10,000 or more employees: **212**

## 10 countries



### North America:

Canada: **75**  
U.S.: **225**

### Europe:

France: **100**  
Germany: **100**  
Italy: **100**  
Spain: **100**  
U.K.: **100**

### Asia:

India: **150**  
Malaysia: **75**  
Singapore: **75**

## 11 industry sectors



Finance: **164**  
Manufacturing: **146**  
Professional services: **61**  
Telco, media, and entertainment: **160**  
Transportation and logistics: **60**  
Energy (utilities, oil, and gas): **152**  
Life sciences\*: **15**  
Retail, hospitality, and wholesale: **162**  
Government: **59**  
Healthcare: **60**  
Education: **61**

All data in this IDC InfoBrief is based on 1,100 respondents, unless specified otherwise.

# Definitions

- **CloudOps:** Cloud operations refers to any managerial activities related to the continuous updates or optimization of IT services being run through a public cloud.
- **DCIM:** Datacenter infrastructure management systems are solutions that manage, optimize, and aid in planning for resources in datacenters, including IT hardware, network, power, cooling, and physical space. DCIM solutions measure and control components on the IT side (such as servers, storage systems, network switches, routers, and virtual machines) and components on the facilities side (such as cooling unit, power distribution unit [PDU], uninterruptible power supply [UPS], sensors, and generators). Access to these resources requires input and coordination between the facilities organization and the IT organization to create a holistic view of the datacenter.
- **DDI:** DNS, DHCP, and IP address management are core networking technologies critical for every IT organization. DNS servers deliver the association between host names and IP addresses that keeps HTTP web traffic and network traffic flowing, whereas DHCP provides a dynamic address assignment capability for nodes logging on to the network. IPAM supports these technologies by enabling efficient tracking and management of the IP addresses within a network and consolidating IP data into a central repository (see below for more details).
- **IPAM:** IP address management is a method used to plan, track, and manage information associated with a network's internet protocol address space. Using IPAM, administrators can make sure the repository of assignable IP addresses stays up to date. IPAM solutions help simplify and automate the administration of several tasks related to IP space management, including writing DNS records and configuring DHCP settings.
- **ITOps:** Information technologies operations is the process responsible for acquiring, designing, deploying, configuring, and maintaining the physical and virtual components of an IT infrastructure.
- **ITSM:** IT service management software discovers, tracks, records, and manages configuration, incidents, problems, assets, and information related to IT end users, devices, infrastructure, and operations. This category includes IT helpdesk applications, IT asset management and discovery systems, resource tracking, credentials management, and related problem determination and resolution applications, including knowledge bases.
- **MTTR:** Mean time to resolution represents the average time required to repair a failed component or device. It is the total corrective maintenance time for failures divided by the total number of corrective maintenance actions for failures during a given time.
- **NSoT:** A network source of truth is a repository of data that provides network and automation managers with insights into the intent of the network and the intended state of the network.
- **NetSecOps:** Network and security operations is a movement that seeks to integrate the workflows of network (NetOps) and security (SecOps) teams for successful integration projects.
- **SecOps:** Security operations is a collaboration between IT security and operations teams that integrates tools, processes, and technology to remove silos within the organization.
- **SDN:** Software-defined networking is as an approach to network architecture that addresses the limitations of traditional networks as they struggle to accommodate increased virtualization and cloud-native application environments. SDN architectures introduce abstractions that are designed to facilitate automated provisioning, programmatic management, support for insertion of network and security services, and integration with open source and industry-standard orchestration systems. Through extensive application-oriented automation, SDN aims to make the network and network operations more agile and flexible.
- **SIEM:** Security information and event management is an approach to security management that combines event, threat, and risk data into a single system to improve the detection and remediation of security issues and provide an extra layer of in-depth defense.
- **SOAR:** Security orchestration and automation response platforms are security software solutions and tools for coordination, execution, and automation of tasks between various people and tools.

# About IDC



International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## **IDC UK**

5th Floor, Ealing Cross,  
85 Uxbridge Road  
London  
W5 5TH, United Kingdom  
44.208.987.7100  
Twitter: @IDC  
idc-community.com  
www.idc.com

## **Corporate Headquarters**

140 Kendrick Street,  
Building B, Needham,  
MA 02494 USA  
508.872.8200  
www.idc.com

## **Copyright Notice**

---

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or [permissions@idc.com](mailto:permissions@idc.com). Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit [www.idc.com](http://www.idc.com). For more information on IDC Custom Solutions, visit [http://www.idc.com/prodserv/custom\\_solutions/index.jsp](http://www.idc.com/prodserv/custom_solutions/index.jsp).

Corporate Headquarters: 140 Kendrick Street, Building B, Needham, MA 02494 USA P. 508.872.8200 [www.idc.com](http://www.idc.com)

© 2023 IDC. Reproduction is forbidden unless authorized. All rights reserved.