CSP Network Automation Trends

Network automation trends at communications and cloud service providers

Executive Summary: Key Findings

- The Futuriom Networking Automation survey reflects the opinions of 130 network operators, including service providers and webscale cloud operators.
- Survey data indicates network operators have a high interest in using closed-loop network monitoring, network monitoring, and intent-based networking to automate their operations.
- The top goals of network automation are faster service delivery and increased revenue (79%), improved network security (75%), and improved ability to support dynamic/on-demand services. Secondary goals are reducing both operational costs (41.5%) and capital spending (37.7%).
- Respondents view automated fault resolution as a critical driver of reduced operating costs. Of those surveyed, 63.1% suggested automated intelligence and analytics are the best options for automating fault resolution. The two next preferred choices: automating network design, build, and deployment (55%) and the purchase of open white-box switches and open-source operating systems (42.3%).
- Networking telemetry, monitoring, and analytics are essential for network automation, according to 90% of those of those surveyed. Specifically, 61% rated those components "very important" and 30% rated them as "important" (30%) to network automation.
- Networking Functions Virtualization (NFV) is the top domain targeted by operators to address networking automation (29%). The next most popular domains are edge cloud (24.6%) and metro network (21.5%).
- An overwhelming majority (70%) of all network operators surveyed (service provider, cloud, webscale SAAS) plan to implement closed-loop automation within the next 24 months. Forty percent (40%) plan to implement it within the next 12 months.

Table of Contents

CSP Network Automation Needs and Challenges

The boom in cloud applications and services has put more pressure on networks to perform without failure. This means the operators of major networks, including communications service providers (CSPs), cloud operators, and web-scale enterprise operators, must find new solutions to automate their networks to respond to scaling demand.

These new challenges include scaling networks to meet an ever-increasing demand for cloud-based applications, as well as automating networks to enable improved service velocity, fault remediation, and network security.

For these reasons, traditional service providers are adopting the cloud network model. This will generate broad benefits as both CSPs and cloud operators move to common architectures and technology standards. The cloud model includes commodity off-the-shelf (COTs) hardware, automated server configuration tools, and virtualized network services such as software-defined networking (SDN) and Network Function Virtualization (NFV).

It offers numerous benefits, including as the acceleration of unified standards for building infrastructure that spans communications service providers, cloud providers, and webscale Software-as-a-Service (SaaS) providers. This will have the dual benefit of lowering costs and enabling cross-network interoperability. As the cloud model moves into CSP networks, it's important to understand which approaches are being used to automate cloud data centers today. In our survey of CSPs and webscale cloud providers, we asked participants to define the most common automation approaches.

Why is it important to look at the cloud data center model in the context of larger operator networks?

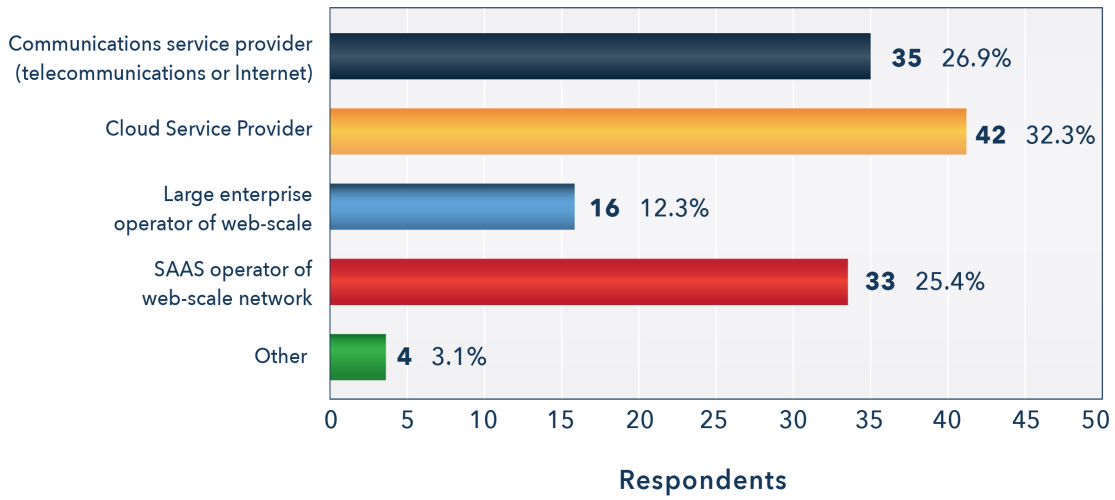
Many CSP networks were built in an era of proprietary hardware and custom software. Fortunately, the underlying technology of the Internet and the web hold promise for the unification of IT technologies that can be networked using a cloud model, whether it's a SaaS cloud, a manufacturing hub, a networked vehicle, or a service-provider Ethernet network. The opportunity to build an integrated "network of networks" has many benefits: Increased standardization drives costs down and provides more opportunity for automation.

Futuriom spent the past three months studying networking trends at large service providers and cloud service providers. We interviewed end users and surveyed 130 managers in the service provider and cloud infrastructure space. Based on our analysis, we have concluded there are several strong themes driving the development of networking automation technologies.

Futuriom Network Automation Survey and Methodology

The primary source of information for this report is the Futuriom Network Automation Survey. This online survey was sent to a large group of webscale network operators, including CSPs, cloud service providers, and "webscale" operators of networks. We sought a mixture of large-scale operators because Futuriom believes the technology sets of CSPs and webscale cloud operators are converging; both industries are gravitating toward a common toolset. The chart below shows the composition of the survey audience.

Which of the following best describes your organization? *(Choose the primary role)*



FUTURIOM.com

In addition to gathering this survey data, Futuriom regularly interviews service providers and cloud operators about their technology strategies. We also recently attended CSP events, including VMworld and MEF18, where we discussed technology platforms with dozens of network operators.

Key Goals of Network Automation

As part of this research, we sought to identify the key goals, challenges, and paths to network automation. Clearly, all IT managers view automation as a driver of efficiency and lower costs. We're all interested in saving time and money, and networking automation has much promise in this area.

But it turns out saving money isn't everything. Think about a CIO or CTO trying to present key performance indicators to the CEO or the board. It's not just about costs, but about efficiency and the capability to deliver faster revenue velocity.

Most businesses struggle to balance costs and growth, and business decisions attempt to balance the two. Automation for networks adds efficiency. It enables businesses to do things faster. Think of the check-in line at the airport. The addition of airport kiosks has greatly increased the speed, ease, and convenience of the check-in process — in some cases, eliminating the need for passengers to stand in lines at the counter. The network, which often requires heavy manual processes, needs an airport-kiosk model for setting up, orchestrating, and deploying new infrastructure and services.

In speaking with developers of CSP networks, we discovered common themes: They want to speed a wide range of tasks and functions, as well as lower the operating costs (opex) of their networks. But more critically, they want to automate the ordering and orchestration of new services because that helps drive revenue.

"We are looking for an integrated ecosystem," Verizon's Viraj Parekh, executive director of Global Product, SDN/NFV, Managed Services, PaaS and Edge Solution, said at the recent MEF2018 event in Los Angeles.

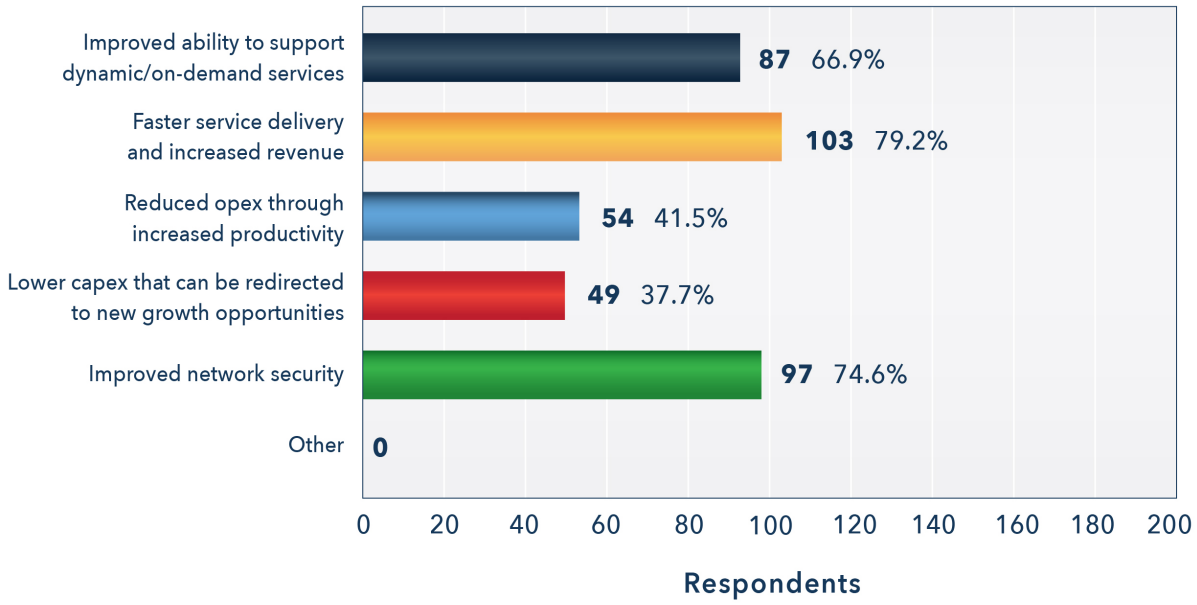
"The customer chooses a product, there is orchestration between products. This creates high operator value."

Futuriom finds that the goals of the new CSP cloud often fall into five major buckets:

- Supporting dynamic services and real-time services
- Faster service delivery and accelerated revenue production
- Lowering opex costs
- Lowering capex costs
- Improving network security with visibility

We incorporated these goals in our survey to find the source of highest demand. We asked 130 professionals in the CSP and cloud infrastructure business to choose the top three of five goals.

What are your three primary goals in driving network automation? *(Choose the top 3)*



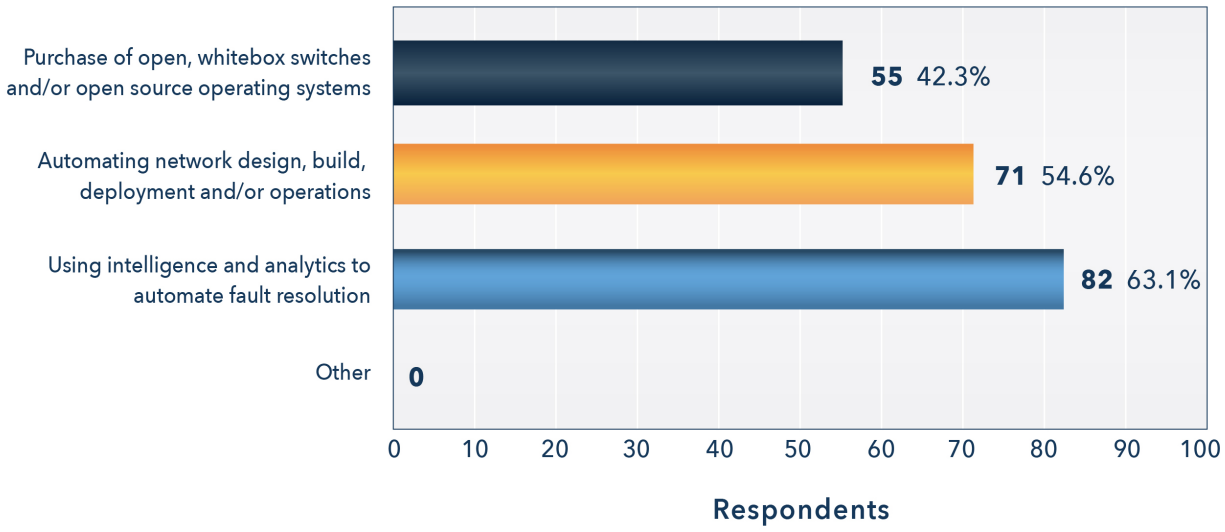
As you can see, faster service delivery and support of dynamic services ranks higher than pure cost savings. In other words, revenue growth trumps operational cost savings. Based on feedback from end-users, these responses fall into two tiers:

First-Tier Goals: Faster service delivery, revenue growth, and better security. Faster service delivery and increased revenue is the top goal, according to 79% of the survey participants. Next was improved network security (74.6%), which makes sense given the ever-present security risks of IT and network environments worldwide.

Second-Tier Goals: Lower Opex and Capex Costs. While lower opex and capex costs are certainly attractive to all, it's interesting that our survey respondents rank them as slightly lower priorities. Reduced opex through productivity gains from automation was selected by 41.5% of respondents and lower capex was selected by 37.7%. For further insight on end-user goals, we asked the survey panel to identify the approaches that show the most promise for reducing costs.

Interestingly, most (63.1%) see fault resolution as the most promising area. Next were automating network design and deployment (54.6%) and purchase of white-box switches and open-source operating systems (42.3%). From this question, it seems reducing costs is most aligned to reducing opex costs.

Where would you like to implement network cost savings over the next 6 to 24 months? *(Choose all that apply)*



FUTURIOM.com

Barriers and Challenges to Network Automation

Automation drives business productivity, which is always desirable. The challenge is achieving it in a cost effective way. The cloud has been efficient in streamlining the automation and use of IT infrastructure such as server virtualization and configuration, but network automation has been slower to evolve due to higher levels of complexity, especially in CSP networks which often cross an increased number of domains (cloud, mobile, WAN, and IT) and require higher levels of investment.

"Our industry has been characterized by the tyranny of boxes," Kevin O'Toole, senior vice president of Product Management at Comcast Business, said at the recent MEF2018 event. "The boxes are in charge. With computing and our ability to do those functions in software, you will see a revolution."

But as it turns out, there are many other challenges beyond the "tyranny of boxes." One major goal is simply planning and integrating new generations of technology on a grand scale. Network operators told us their challenges fall into four groups:

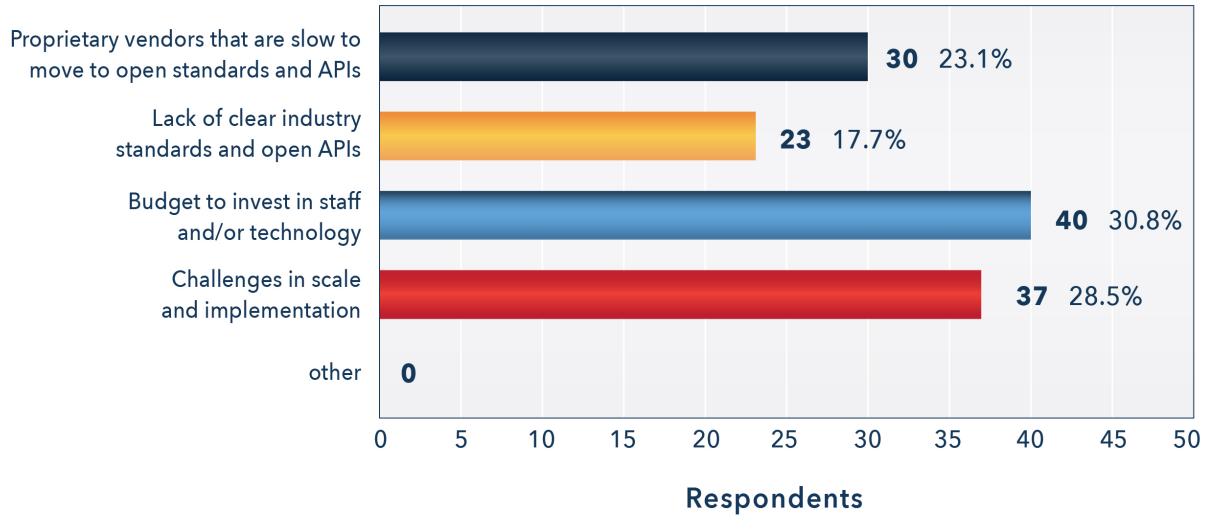
- Vendor interoperability, or managing how supplier equipment works together
- Data and configuration consistency such as standards and APIs
- Resources to implement network automation, notably people and money
- Implementing technology at scale

By grouping these challenges into a survey question to find the most common hot spots, we yielded interesting results. The largest number of respondents said they are challenged by resources — having enough budget to invest in staff and/or technology (30.8%). The second-most selected barrier was challenges in scale and implementation (28.5%). This finding was somewhat surprising, indicating that

network operators believe integrating and upgrading the technology is more challenging than the interoperability of the technology itself. In short, they suggest there is a strong need for integration assistance and expertise in addition to simply providing hardware or software.

While some critics of the networking industry point to the agenda of proprietary networking equipment vendors as an impediment to faster automation, only 23.1% of respondents selected this barrier. Fewer (17.7%) selected the development of standards and APIs.

Which of the following is the greatest barrier to implementing automation in service-provider or data-center operations & networks?



FUTURIOM.com

These results could send a powerful message to networking software and hardware providers that are looking to drive network automation.

The takeaway is that network operators need a high level of assistance to implement automation tools at scale.

Network Automation Technology Components

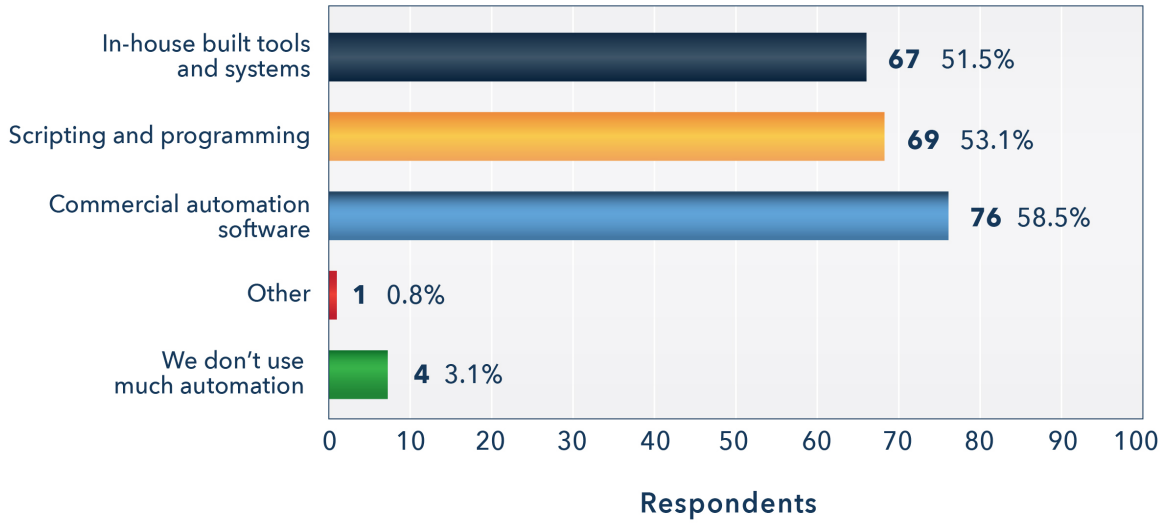
In speaking to CSPs in both the traditional communications market and the cloud world, there are common themes. Futuriom sees the wave of network automation requiring technology evolution in five areas:

1. **The continued adoption of standardized SDN and NFV platforms** by the major network operators, which provide more consistency of IT platforms in both cloud and traditional CSPs.
2. **Analytics platforms** to process network telemetry and drive automation.
3. **Wide adoption of data and applications programming interface (API) telemetry.** APIs have driven networking technology in the data center, and that's going to be a big driver of automation on WAN and CSP networks. This includes development of cross-domain standards and APIs for network configuration, as produced by standards organizations such as the Linux Foundation, MEF, and TM Forum.
4. **A move to intent-based networking (IBN) and intent-based analytics (IBA)** models that enable network programmability based on the intent, rather than the state.
5. The rapid pursuit of **closed-loop monitoring and automation**

How will this be accomplished? Futuriom believes that as adoption of the cloud model grows, CSPs and cloud providers will replicate some of the techniques and skillsets of cloud infrastructure, which include using commodity hardware, Linux-based tools, and a DevOps approach to software development. But this drive toward automation will result in demand for integrated systems that deliver commercial automation solutions.

As the survey results below indicate, CSPs, cloud providers, and webscale enterprises are already looking for commercial solutions to automate their network, with 58.5% of respondents saying they use commercial automation software today. Other techniques employed include the use of scripting and programming (53%) as well as in-house tools (51.5%).

How do you automate most of your data-center operations today? *(Choose all that apply)*



FUTURIOM.com

SDN and NFV Adoption: Ushering in Flexibility and Interoperability

We live in a world of technology buzzwords that are hyped and sometimes confused by marketing mavens. So Futuriom will try to be straightforward about technology feature sets and how they are related to network automation.

The first area to cover is NFV and SDN, which are often used to describe software-based virtualization and how they are applied to cloud data centers and service-provider networks.

Futuriom believes there are three key elements driving NFV and SDN:

1. Both SDN and NFV adopt a model of abstracting the software components of networking (such as an OS or a software function) away from the hardware.
2. They can both be implemented in a commercial off-the-shelf (COTS) hardware platform, enabling economics of scale to lower hardware costs.
3. The hardware can be controlled by an abstracted, programmable OS that can be more easily designed to gather telemetry and data to drive analytics functionality into the network. This enables more autonomous functions such as intent-based networking (IBN) and analytics software.

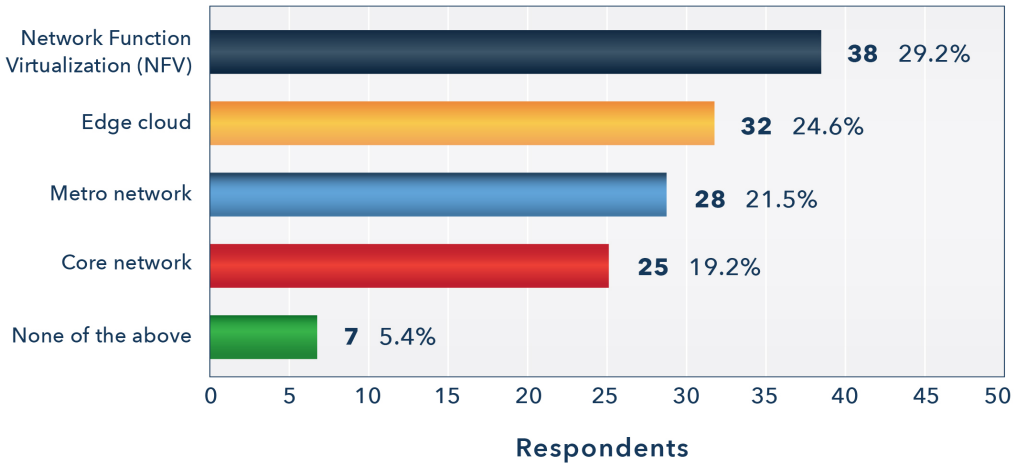
This ecosystem can be seen in the following diagram, which show how SDN and NFV abstracts the functionality of components that can be used to drive automation.

Network Automation Components

One of the key problems to be solved in networking automation is coordinating services and functions among CSPs and cloud providers. For example, imagine a software-defined wide-area network (SD-WAN) service that provides a secure Ethernet connection for a video circuit running from New York City to Singapore. Implementing such a service requires use of many communications carriers and networks. To provide a consistent experience, all of the equipment and software along the way must be programmed to provided resources consistent with a specified service-level agreement (SLA) to deliver a quality video experience.

Inter-carrier standards and interoperability are the last great challenges of the cloud. The advent of SDN and NFV simplifies implementing such services because it will facilitate interoperability among networks as broader standards are adopted (See "CSP standards" in the appendix at the end of this report). As the survey demonstrated, CSPs and cloud operators both see NFV as one of the highest targeted domains for implementing network automation, with 29.2% identifying it as a top target.

Which network domain or segment would be your company's top target for implementing closed-loop automation?



FUTURIOM.com

In fact, when you drill down and look at only the CSPs, the focus on NFV was even higher (as expected). **Approximately 40% of CSPs — 14 out of 34 — identified NFV as the top target for closed-loop automation.**

The large service providers will have a crucial role in elevating the ultimate goal of network automation. That's because no matter how large cloud networks scale — whether it's an Amazon or Microsoft public cloud, a large SaaS provider cloud such as Salesforce, or even an enterprise cloud — they must ultimately connect to each other over the WAN, which typically requires some sort of large public service provider. This is why many large service providers are being aggressive about this transition. For example, AT&T recently aimed to have 75% of its network virtualized by 2020. However, many large service provider technologists point to the complexity and size of this undertaking as they seek to "cloudify" their networks and drive automation.

The Future of the OSS and LSO

One of the key challenges of moving large CSP networks to a programmable SDN and NFV model is the large installed base of operation support systems (OSS). Over many decades, CSPs installed a variety of often proprietary OSSes from equipment vendors operating their own command-line interfaces or specific OSS vendors such as Amdocs, Ericsson, and Netcracker.

These OSSes were often tied into specific boxes and services and designed to perform functions such as service orchestration, service assurance, and business functions such as billing, provided in a billing support system (BSS). The emergence of SDN and NFV is pushing the requirement of a next-generation OSS that can be more agile, modular, scalable, and manageable. Organizations such as the MEF and TM Forum are defining the need for new, open OSS functionality that can integrate with NFV and

SDN platforms and enable quick, software-based configuration of services, a process known as Lifecycle Service Orchestration (LSO). Many networking technology companies are using LSO do coordinate services across CSP platforms. For example, Ciena's Blue Planet orchestration platform can be used to aid network automation in multi-vendor networks.

At the same time, as standards for LSO emerge, CSPs are building OSS systems that are based on open source to provide more interoperability and flexibility. An example of this is the OSS formerly known as ECOMP (Enhanced Control, Orchestration, Management & Policy). Built by AT&T, it has now been folded into the Linux Foundation as part of a group of open-source technologies including ONAP.

Futuriom believes modular, interoperable software packages, including open-source solutions, will gradually replace legacy proprietary OSSes in CSP networks, enabling a multi-vendor approach driven by LSO.

The Programmable OS

Just as OSS systems are becoming more open and programmable, so are network operating systems (OSes). Think of the network OS as the brain behind the networking hardware, telling the hardware box how to route and switch traffic. In a legacy system, this was generally controlled by a proprietary OS sold with the hardware. In the SDN and NFV world, the OS is often disaggregated or sold separately from the hardware and it can even be mixed and matched.

The disaggregated OS has given to the rise of a separate class of SDN OS. Some of these vendors, including Cumulus Networks, Big Switch, or Pluribus networks, either sell their own OS coupled with commodity hardware or team up with hardware OEMs.

Telemetry, Network Monitoring, and Analytics

Think of a self-driving car that is being driven down the highway. To operate properly, it needs a huge amount of data to be gathered to feed the system. This includes cloud highway and street information, visual inputs, GPS data, and speed and mechanical information.

Automation in the network requires that large amounts of data to be gathered from a wide array of sources using the technique of telemetry. This includes data about network hardware, packet flows, and applications behavior.

Data sources can include elements such as standardized networking data such as NetFlow and SNMP, packet-monitoring tools, and server and CPU data. This functionality is being integrated with leading SDN platforms. The drive to automate large-scale service provider networks will drive more integration between monitoring and telemetry tools with SDN platforms. Data sources might include:

APIs: Networks are using a wide range of APIs, including vendor-specific REST APIs allowing access to confirmation and operational data for specific vendor hardware. The opening of REST APIs to proprietary hardware has been one of the key enablers of SDN 2.0, facilitating the programmability of a heterogeneous network.

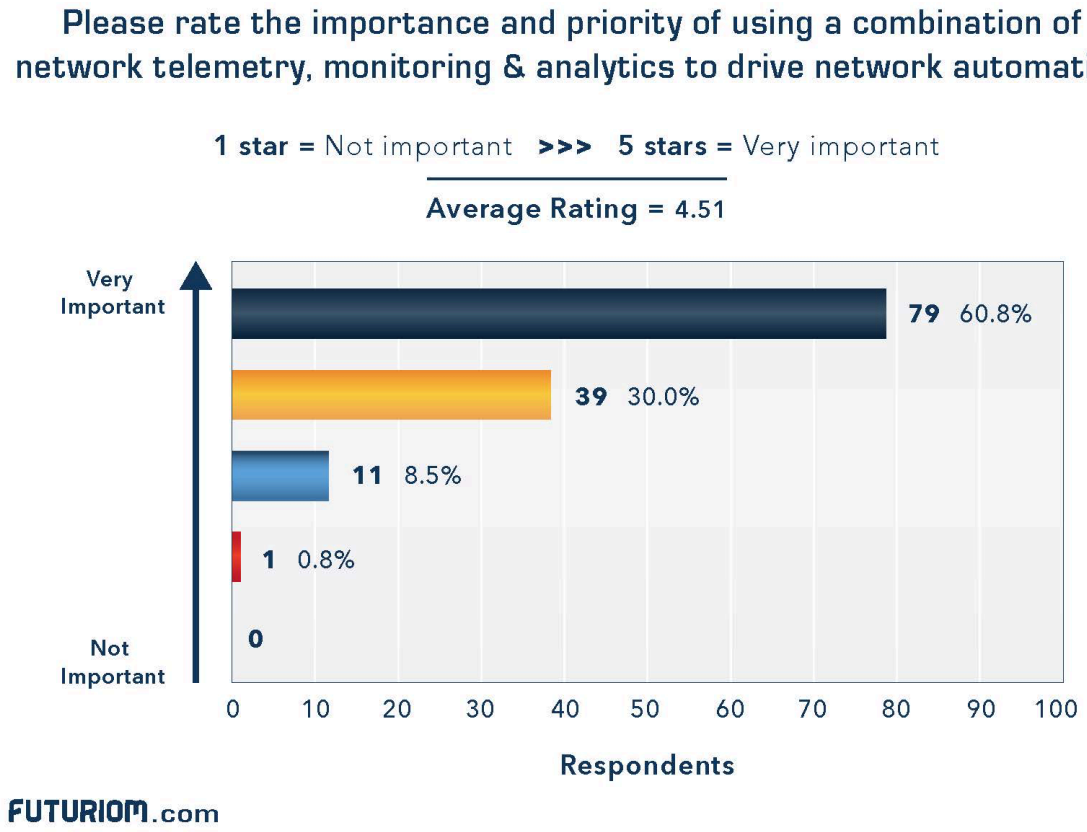
Data Models: Data models such as Netconf, YANG, and TOSCA have risen in popularity by enabling orchestration tools to automate configuration of network devices and software.

Network Management and Monitoring Protocols: Network protocols and standards such as SNMP, NetFlow, OpenFlow, SFlow and JFlow have enabled open, shareable

data on network status. This data can be used by SDN, NFV, and management and service assurance platforms to build real-time status information on the network.

Unix Tools: The cloud world has infiltrated networking. SDN systems are increasingly leveraging data generated by the systems of the server world, using Syslog and other Unix tools. To build an automation model, data is gathered and fed into analytics programs that can interpret the network behavior and apply programmatic changes.

It's clear from the survey that our audience rates this approach very highly.



Many networking monitoring and service assurance solutions are positioning themselves as tools for driving network automation. For example, EXFO is a broad-based networking test and measurement company that is rolling out a suite of

software monitoring products geared for SDN and NFV platforms. A cadre of service assurance specialists including InfoVista and CENX (now owned by Ericsson) are targeting SDN in the service provider networking market. Cisco has been emphasizing its Tetration product line, which is designed to monitor and collect data to drive analytics functionality that will integrate with Cisco's ACI platform, though the company is in the early stages of integrating these functions and did not respond to specific requests for information in this report. (See the appendix of this report for more information on these companies.)

Intent-Based Networking (IBN) and Intent-Based Analytics (IBA)

How are networks programmed to absorb data and automate network functions? One approach that's emerging is intent-based networking (IBN) and intent-based analytics (IBA) systems. This technology, pioneered by startups such as Apstra, uses the abundance of network data to gain visibility and control over networks and feed this data into a programmatic model describing the "intent" of the network. For example, you might describe a network that should never be more than 80% utilized, with .99999 reliable. The IBN and IBA systems then take it upon themselves to get this result, but also re-route applications or open up new resources to make sure the network doesn't break.

IBA uses real-time telemetry system to track the state of the network and compare it with the logical rules of a programmatic IBN system to automate network operations. For example, an intent model might describe the baseline network performance needed for a real-time video stream, and readjust network resources in real-time to ensure that this business intent is fulfilled.

The goals of IBA and IBN are to:

- Produce a "single source of truth" or data repository that can gather a wide range of network telemetry
- Create an IBA engine that can recognize and diagnose anomalies and initiate automated fixes to reduce operating costs
- Increase network resources by maximizing efficiency
- Enable automated modeling for planning and design to understand future needs.

Following the lead of Apstra, some larger equipment vendors such as Cisco have jumped on the IBN bandwagon. But the term can be used loosely by the marketing literature and some vendors define IBN in terms of their own proprietary tools.

Futuriom believes that true IBN is driven by active telemetry feeding a discrete IBA engine that can automate network configuration. IBN systems must be able to draw telemetry and monitoring data from a wide range of sources and operate in multi-vendor equipment environments.

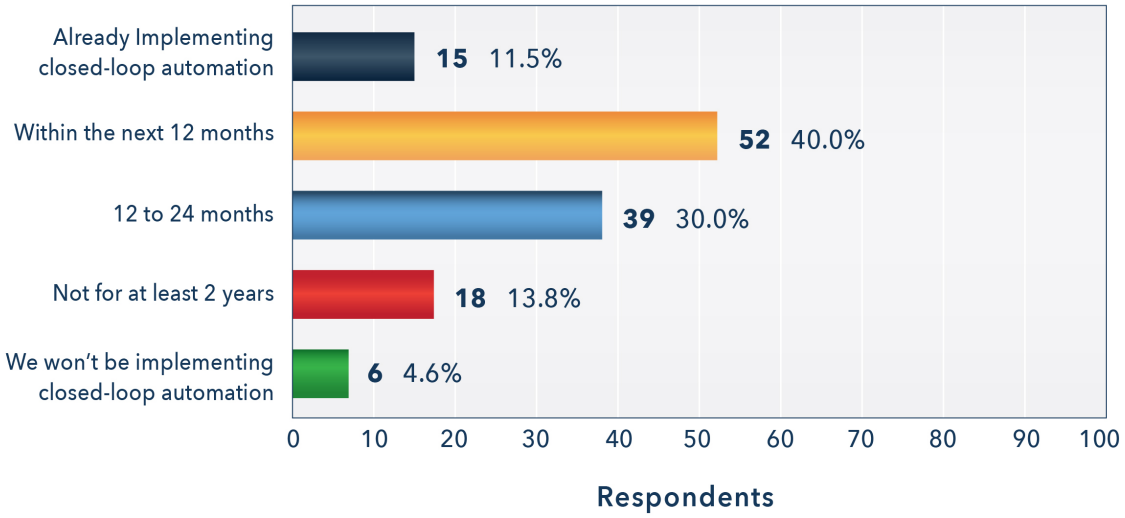
Integrated Monitoring, Service Assurance, and Closed-Loop Automation

As demonstrated, network automation requires integrating sophisticated telemetry, monitoring, and closed-loop automation approaches. While data telemetry, monitoring, and tools such as service assurance have always been available, full network automation approach requires increased integration of these approaches across the entire network infrastructure. The result is a notion known as closed-loop networking in which the entire system can monitor itself.

Closed-loop automation monitors the network and uses analytics to take corrective actions to meet network application performance goals and deliver service assurance. A closed-loop solution automates the necessary configuration changes to meet programmed goals.

This approach is identified as an urgent need in our survey, with a majority (70%) of respondents looking to adopt a closed-loop automation approach in the next 12 to 24 months, including 40% that expect to implement the technology within 12 months.

When is your company planning to implement closed-loop automation in operations?



FUTURIOM.com

In the ideal world, this closed-loop automation can extend over network domains including a variety of networking equipment and software.

Some of the larger integrated optical and CSP networking vendors are moving to integrated closed-loop monitoring functionality into their networking portfolios. For example, Nokia is integrating closed-loop monitoring into its Nokia Bell-Labs Future-X architecture.

Nokia says this will ensure QoE for every individual user and application across network domains.

In addition, it should be noted that closed-loop automation is often delivered through the integration of several types of products from multiple vendors and categories.

CSP networks often require specialized service monitoring and service assurance products to deliver Quality of Service (QoS) and enforce SLAs that can be packaged into closed-loop automation solutions. Some of the vendors focusing on service assurance and monitoring technology, for example, including Accedian, CENX (Ericsson), Infovista, and NETSCOUT.

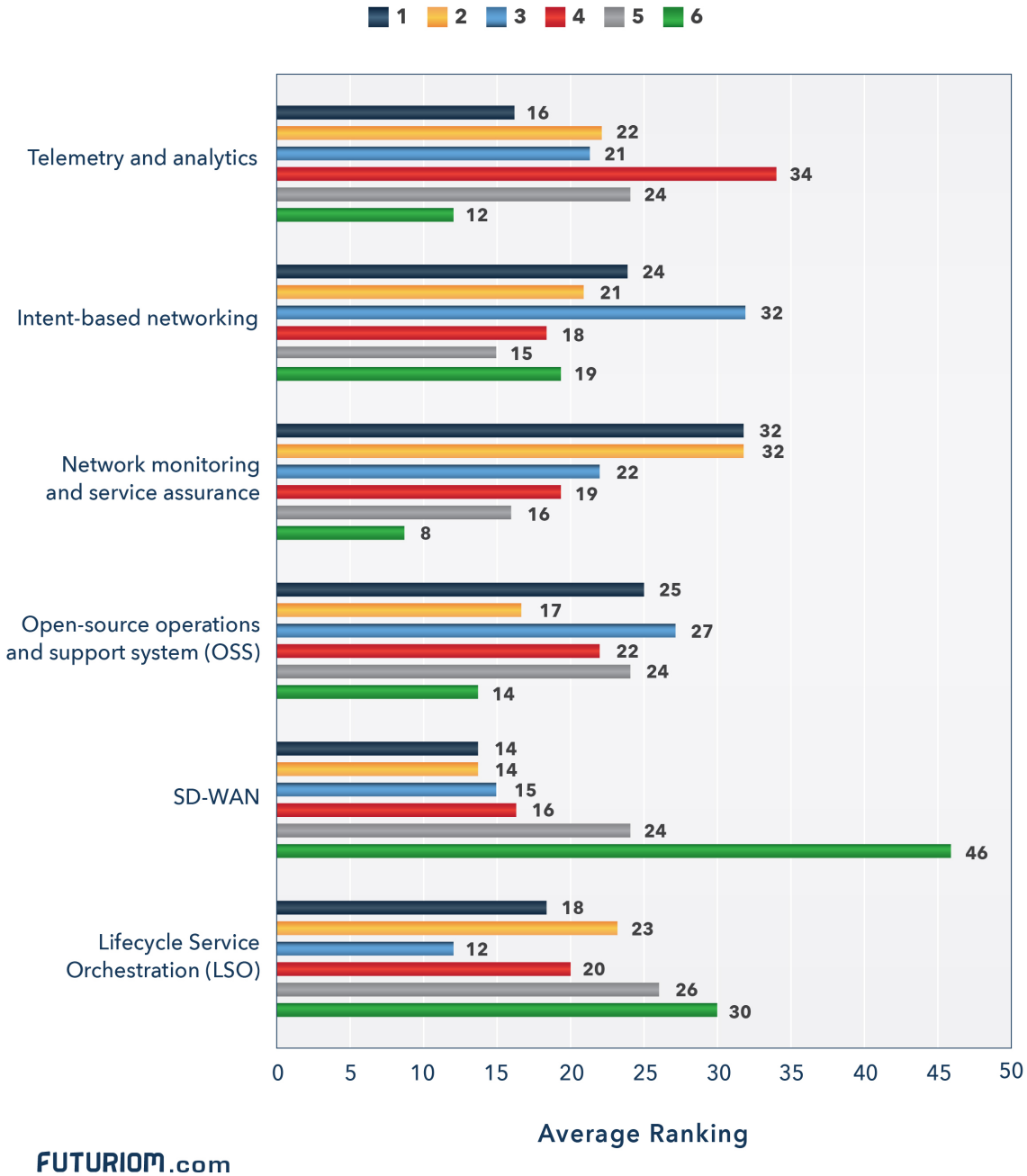
Futuriom's research has indicated that end-user in cloud and CSP networking roles are interested in a wide variety of these technologies to deliver a full, automated platform.

The MEF18 event included a wide range of network automation proofs of concept that included software and hardware from many vendors, integrated together. This trend is likely to continue as the range of automation software and tools proliferates from both startups and larger vendors.

How do all of these technologies break down in importance? Although it is clear that some or all of these technologies will be needed to deliver full automation, the end-user community perceives some of them differently.

To gauge this understanding of demand, Futuriom asked the survey participants to rank the wide range of technologies in their order of importance in contributing to network automation.

Please rank the following technologies in their contribution to delivering increased network automation.



FUTURIOM.com

Another way to look at the ranking of these technologies is to aggregate the scores into an average, which can be seen below.

The lowest score means the technology was ranked highest. Network monitoring and service assurance ranks the highest, with a score of 2.84, followed by intent-based networking (3.28), open-source OSS (3.35), telemetry and analytics (3.5), and Lifecycle Service Orchestration (3.80). Interestingly, SD-WAN, though it continues to be a popular and growing technology area, is not ranked high in terms of delivering automation.

Average ranking
(highest to lowest)

Network monitoring and service assurance	**2.84**
Intent-based networking	**3.28**
Open-source operations and support system (OSS)	**3.35**
Telemetry and analytics	**3.50**
Lifecycle Service Orchestration (LSO)	**3.80**
SD-WAN	**4.24**

FUTURIOM.com

Appendix A: Standards and Data Models for Network Aut

It's been established that a wide range of networking tools and data standards are needed to drive network automation. Data is the new oil, as they say. It is used to drive analytics and artificial intelligence (AI) engines which can automate infrastructure.

Data models, standards, and APIs are the lifeblood of network automation. They make it easier to feed analytics programs to build an automated system, as well as enabling interoperability among multi-vendor equipment.

The data-model trend means there is more configuration, traffic, and flow data available than ever before — whether the networking platform is open or proprietary. This information comes from a wide variety of standardized network protocols and data models such as SNMP, YANG, Netconf, NetFlow, and vendor APIs.

While this is easier to do in the relatively closed domain of a single public cloud offering — for example Amazon Web Services (AWS) and Microsoft Azure can more easily implement automation because they control all the of the infrastructure and their data in their own infrastructure — it is harder to executive in cross-domain WANs, for example. There is another issue. If you want to connect cloud applications across hybrid clouds using service-provider connections, how do you control the performance of that network or the SLAs if you don't own it?

This is why service provider cloud interoperability has become the holy grail of network automation. One of the key trends in service provider and large enterprise networks is the move toward data- driven infrastructure to make it easier to program

and configure hardware. These data models also make it easier to feed analytics programs to build an automated system.

In addition to the extensive use of APIs and network management protocols, a number of standards organizations are working on create new standards for interoperability among service providers.

These will be important for enabling SDNs that can span the WAN, from data center to data center or across clouds. It's easier to create an SDN in the closed environment of one cloud platform, but harder to manage an SDN that spans multiple service provider networks. To provide full automation, network service and control will need to be implemented across domains and clouds (e.g. carrier-to-carrier, or IP to optical), which requires industry standards.

Several groups are working on such standards. One of the more recent industry developments is the MEF's introduction of the MEF 3.0 framework at its annual event in November of 2017. The MEF has been progressing development of service and LSO API standards for orchestrating dynamic Carrier Ethernet, Optical Transport, IP, SD-WAN, Security-as-a-Service (SECaaS), and other virtualized services over automated networks.

The goal is to enable service orchestration across multiple providers and over multiple network technology domains (e.g., Packet WAN, Optical Transport, SD-WAN, 5G, etc.). This will be important for implementing SDN automation in cloud-to-cloud configurations.

Some of the key industry standards organizations focused on large enterprise and service provider networks are outlined below.

ETSI

The European Telecommunications Standards Institute this year published six new specifications governing the use of network functions virtualization (NFV) services, which enable operators to deploy services on a virtualized infrastructure. Because SDN will be used to configure and connect NFV platforms, it is important to track how NFV platforms connect to SDNs for management, monitoring, and analytics.

For example, the new ETSI NFV specifications defines APIs enabling multivendor interoperability for service deployments, according to ETSI. For example, these standards could be used to define how to configure security and SD-WAN services using NFV. ETSI says it is also working on standards for interoperability with Operations and Support Systems (OSS) in carrier networks, with the formation of a new Zero-Touch ISG group.

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers that has guided the Internet architecture and development of important standards. The most famous of these, of course, is Internet Protocol (IP). The IETF is involved in a wide range of standards governing the developing of the Internet. Some of the important networking standards it has created include MPLS, OSPF, and SIP.

While the IETF largely concerns itself with IP-based technology, it has a group looking at SDN, known as I2RS, which has done some work on southbound programming protocols, NFV and network service chains.

The Linux Foundation

The Linux Foundation oversees an immense range of open-source projects and standards focused on cloud computing and open-source software. Many of these are focused on SDN in the operator environment, including the carrier operating system project ONAP, SDN controller Open Daylight (ODL), OpenFlow, and CORD, which is a model for building cloud platforms for NFV.

The Linux Foundation has been consolidating many SDN projects and tools, most notably OpenFlow, CORD, ONAP, and ODL, which are being used to build virtualized infrastructure in carrier environments. This is an important role and further consolidation is welcome as it can help operators try to manage "standards sprawl."

MEF

The MEF is working with many of the world's leading service and technology providers, open source projects, standards associations, and enterprises to realize dynamic services orchestrated across automated networks.

The MEF 3.0 services framework family includes dynamic Carrier Ethernet, wavelength, IP, SD-WAN, Security-as-a-Service, and other virtualized services that will be orchestrated over programmable networks using LSO (Lifecycle Service Orchestration) APIs. The LSO Reference Architecture enables the standardized of LSO APIs that enable orchestration of services across multiple providers and multiple technology domains (e.g., Packet WAN, Optical Transport, SD-WAN, 5G, etc.). This will be important for implementing SDN automation in cloud-to-cloud configurations.

The MEF most recently released LSO Sonata APIs that will contribute to the automation of the potential $250+ billion market for MEF-defined services by enabling inter-carrier integration of service automation.

The Open Compute Project (OCP)

The Open Compute Project (OCP), is a community of technology leaders in the cloud computing environment which has been driving standardized hardware, software, and equipment design for cloud data centers.

The OCP's original focus is pure hardware, with standards for elements such as power supplies, server racks, and battery backup systems. But it has branched out into other areas, such as a universal customer premises equipment (CPE). The main goal of OCP is to drive standardized components that can be used to build cloud services.

TM Forum

The TM Forum works closely with service providers and other carrier standards groups such as the MEF to define carrier interoperability, which as discussed will be increasingly important to guiding connectivity of SDN and automation between clouds and carrier networks. The TM Forum maintains a suite of 50+ REST-based Open APIs collaboratively developed to be used in service provider networks. Many of these APIs are useful for monitoring and fault management. Some examples of the TM Forum APIs include the Alarm Management API, Customer Management API, Performance Management API, and Resource Function Activation and Control API.

In an important recent development, the TM Forum is cooperating to insure interoperability between the MEF's LSO and MEF 3.0 framework and TM Forum's Open API framework. The goal is to create standardized APIs to enable SDN architectures from different network service providers to interoperate with each other. The increased cooperation between the MEF and the TM Forum is encouraging because many service provider experts have regularly expressed concern about the volume of standards organizations and consolidation and cooperation should help streamline the process.

NOKIA

Technology Profile (Sponsored)

Nokia: Automation accelerating operations for digital times

Networks and businesses now operate with a speed and complexity that is beyond human capabilities to manage alone, limiting productive and financial gains. Automation is key to unleashing digital time for networks, operations and businesses.

The Nokia Bell-Labs Future-X architecture, uniquely offers industry-leading innovations that enable automation across multiple-technologies and domains. From managing connectivity to end-to-end service capability for 5G and Industry 4.0, this enables the transition to networking and operations that are ultra-automated, high-performance and massively-scalable.
Few vendors have Nokia's networking and automation depth-and-breadth, including products for 5G network slicing, service-lifecycle-orchestration, network-analytics, DC-SDN, SD-WAN, Carrier-SDN for IP/optical-networking, SON and transport optimization for mobile RAN/transport/core and SDAN for fixed DSL/xPON/Cable access networking.

With this end-to-end solution architecture from Nokia, operators gain insight-driven automation, delivering:

- Quality – to ensure QoE for every individual user and application
- Simplicity – to abstract the ever-increasing network complexity and diversity
- Efficiency – to best leverage people and network resources
- Agility – to become more responsive to fast changing market demands

Nokia Future-X network automation is powered by an open-and-programmable, insight-driven, smart-network-fabric. Nokia's collection of software-applications and networking-innovations enable this future-network. The elements (described-below) may be deployed as a complete-end-to-end-solution or as individual-best-of-breed-elements which fully-interoperate with other vendors.

Connected Intelligence for the 5G era

5G brings opportunities like never before, but new use cases and services need to be deployed, monitored and managed at the speed of business.

By connecting domains, deriving insights and triggering and/or automating actions, Nokia software brings new levels of intelligence and (closed loop) automation to service provider networks, helping our customers streamline operations, improve service offerings, monetize these services, enhance the customer experience, and differentiate themselves in a complex and competitive environment.

Related Nokia products: Software for Connected Intelligence.

Efficient-operations with E2E-orchestration and automation across hybrid-resources:

Nokia Service-Lifecycle-Orchestration enables operators to offer multi-domain hybrid VPN services across a mix of new virtualized resources (vNFs) plus traditional resources based upon availability, capability and cost structure. It improves operational efficiency and provides the ability to validate the steps required to assess their operations going forward.

Related Nokia products: FlowOne, CloudBand, Virtual Networks Orchestration (VNO)

Drive business-agility and simplify-operations with automation and SDN control:

Nokia SDN solutions reduce the complexity of operations and help operators to respond and adapt to the dynamic nature of cloud-based consumption models. These Nokia SDN control products lower TCO and maximize-operational-efficiency. In conjunction with analytics, Nokia SDN products are central to closed-loop automation for traffic-optimization and QoE improvement. This enables operators to make best use of available-network-assets and adapt-and-optimize networks in real-time.

Nokia domain controllers are purpose-designed to fit any overarching end-to-end MANO, NFVI, or SDN environment. Open and programmable SDN control across multiple domains is achieved through support for SDN API and protocol standards, such as, NETCONF/YANG, RESTful APIs, gRPC, IPFIX, and Kafka.

Related Nokia products: Network Services Platform (NSP), WaveSuite, SDAN (Altiplano Access Controller and Lightspan access nodes), NetAct

Multi-dimensional-analytics driven automation without dedicated-hardware:

Our software-based Deepfield-solutions deliver unprecedented context in cloud and network visibility-and-analytics for automating the mitigation of DDoS attacks and improving quality of experience (QoE). This helps to preserve and improve-brand-reputation, increase-customer-satisfaction and retention, as well as enable-value-added or premium-service-options to increase ARPU.

Related Nokia Products: Deepfield Cloud and network analytics.

Related Dynamic SD-WAN service automation:

Nuage Networks SD-WAN 2.0 solution creates a seamless and massively scalable end-to-end virtual network allowing for a single-network-governance-model across all DCs-WANs-public clouds-branch locations. This platform is the industry's first multi-cloud network automation platform to deliver IT services over any transport with full control, visibility and enhanced security across the entire network.

Related Nokia Products: Nuage Networks Virtualized Services Platform (VSP)