White Paper

# The Journey to Intent-based Networking

## Ten Key Principles for Accelerating Adoption

By Bob Laliberte, ESG Senior Analyst

January 2018


www.secureagility.com

This ESG White Paper was commissioned by Cisco and is distributed under license from ESG.

## Contents

Aligning IT to Business Intent ..... 3
The Network Needs to Evolve ..... 4
What Is Intent-based Networking? ..... 5
Three Key Elements of Intent-based Networking ..... 6
1. Intent ..... 6
2. Automation ..... 6
3. Assurance ..... 7
Benefits Associated with Intent-based Networking ..... 8
Ten Guiding Principles for Getting Started with Intent-based Networking ..... 9
1. Develop an IBN Roadmap ..... 9
2. Embrace Change ..... 10
3. Acquire Expertise ..... 10
4. Build Consistency ..... 10
5. Build on Existing Investments ..... 10
6. Start Locally, Think Globally ..... 11
7. Integrate Security ..... 12
8. Balance Open with Pragmatic ..... 12
9. Leverage AI and ML ..... 12
10. Integrate Automation and Assurance ..... 12
The Bigger Truth ..... 13

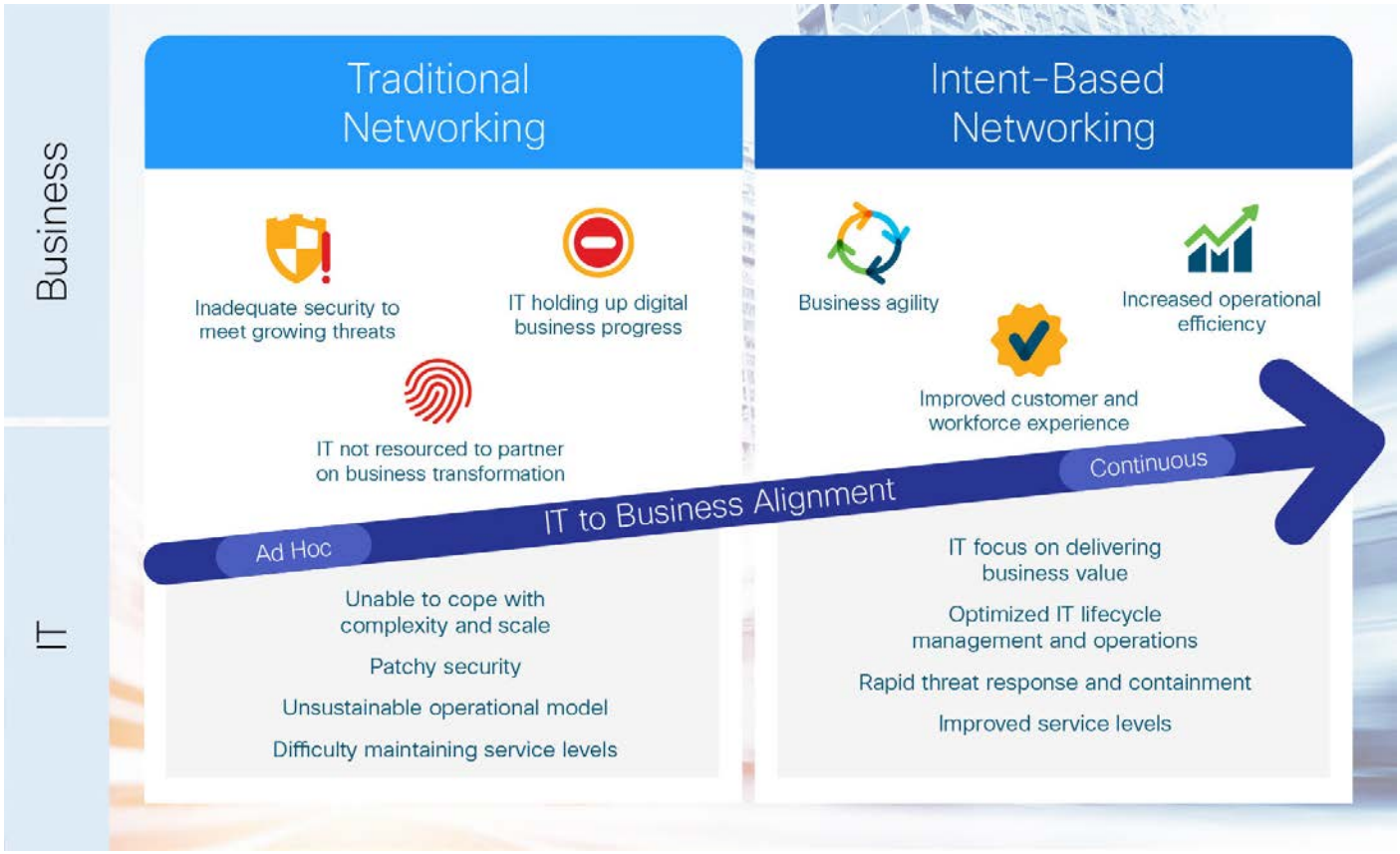
## Aligning IT to Business Intent

The current pace of business demands that organizations are agile and responsive to ever-changing customer demands. Organizations rely heavily on IT infrastructure to power their businesses and new digital initiatives, so that infrastructure also must be extremely agile and responsive. Ideally, IT would be in a position to provide continuous and seamless alignment of the infrastructure to new requirements, such as new business services and applications, security policies and regulations, and changing IT operational processes. Unfortunately that has not been the case until now because the interface between business and IT has typically required a manual and somewhat ad-hoc effort to translate business needs to IT execution.

> Intent-based networking allows automated, frictionless, and ongoing alignment of business needs to IT infrastructure execution.

To address this, the IT industry has initiated an effort to create a systematic approach to using "business intent" as the driver for IT infrastructure lifecycle management, whereby the translation of business needs to IT infrastructure execution is automated, frictionless, and ongoing. With the adoption of this new paradigm, commonly termed "intent-based networking," we can anticipate that within a number of years the approach to designing and managing IT infrastructure will have changed dramatically. Those companies that successfully adopt this approach will have achieved close and rapid alignment of IT to business needs, which results in improvements in business agility and customer experience and more IT focus on delivering true business value. Figure 1 captures some of the key business and IT challenges with traditional networks, and the promise offered by intent-based networks.

**Figure 1. IT to Business Alignment**




*Source: Enterprise Strategy Group*

While the journey to an intent-based architecture is still young, there are many reasons for IT leaders to take note today, so that they can chart a course to take advantage from incremental benefits of the architecture at each phase of the journey. In addition, certain foundational elements of an intent-based architecture, such as software-defined networking, virtualization, and analytics, have matured to the point that they can be deployed today as part of a longer term intent-based strategy.

In this paper we will outline some key principles and guidance IT leadership should consider as you embark on your own intent-based networking (IBN) strategy.

## The Network Needs to Evolve

Most organizations have invested in and implemented initiatives related to digital transformation, cloud computing, analytics, security, and IoT to enable the business to improve customer and workforce experience, and business and IT operational efficiencies.

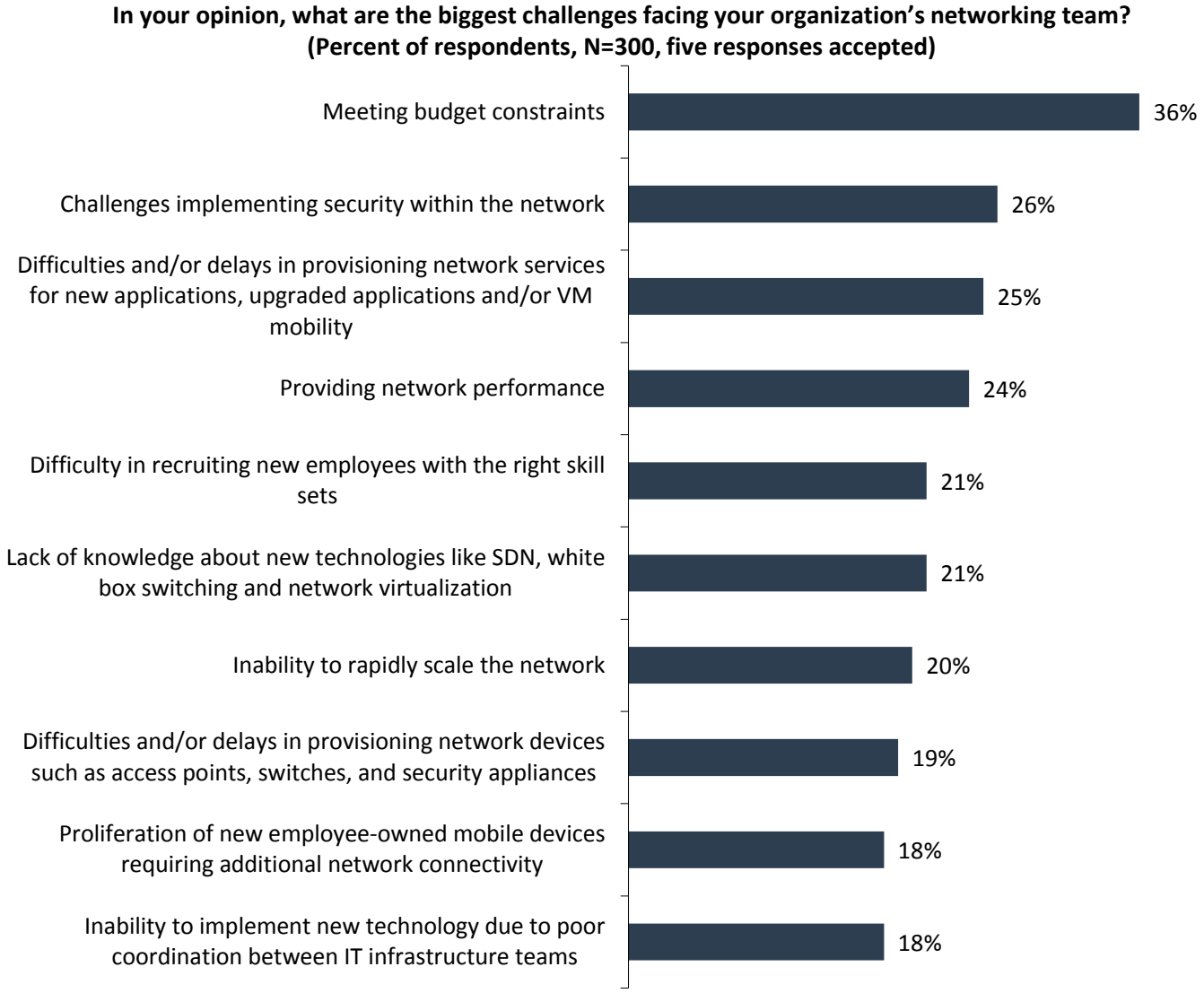
The new network will need to be far more agile, responsive, and relevant to the business, while protecting new digital initiatives from ever-more sophisticated attacks.

It is clear that these initiatives will place new requirements on the network—or more accurately, they will require a new network operations paradigm. The network needs to rapidly facilitate the connection of potentially millions of IoT devices; enable secure, highly performant connections to cloud computing sites from data centers and remote offices; and be far more agile, responsive, and relevant to the business. At the same time, the network will need to protect new digital business initiatives from ever-more sophisticated attacks. However, current network environments still need to overcome significant challenges. At a high level, CIO and IT executives are concerned with improving customer experience, accelerating cycle times for technology adoption and service delivery, mitigating risk, improving compliance efforts, and of course, trying to reduce costs by enhancing efficiencies and automation.

Networking teams struggle with day-to-day challenges as illustrated by ESG research in Figure 2, including implementing appropriate security in the network, delays provisioning network services, the ability to provide sufficient network performance, the limited availability of networking skills—especially for new technology, the ability to rapidly scale the network, and delays provisioning of network devices, among others. The most often cited challenge was meeting budget constraints.[1]

[1] Source: ESG Master Survey Results, *Trends in Network Modernization*, November 2017.

**Figure 2. Top Ten Challenges Facing the Networking Team**




*Source: Enterprise Strategy Group*

IT leaders need innovative solutions that will help them overcome these network challenges and enable them to evolve the network in order to help grow the business.

## What Is Intent-based Networking?

Intent-based networking allows the network team to simply describe, in plain language, what they want to accomplish and the network then makes it happen.

Given the current challenges, it is clear that the network needs to change, but how and in what way does it need to evolve? One area of networking innovation that holds significant promise is intent-based networking. It is likely that you may have heard about it, but what exactly is intent-based networking and how can it help your organization?

The concept of intent-based networking is that the network team could simply describe, in plain language, what they wanted to accomplish (the intent) and the network would be able to translate the intent into the numerous policies that would establish the appropriate configuration and settings changes across a complex and heterogeneous environment leveraging automation. Normally this activity would require a significant manual effort by highly skilled network engineers to modify each device impacted by the desired change.

> Intent can be stated as simply as, "Provide guests with a separate guest network, no access to corporate resources, and low-priority, protected Internet access."

In addition to quickly implementing new services, intent-based networking will leverage machine learning and artificial intelligence to ensure that any services deployed are still meeting their intended service levels. When the performance or other criteria is not met, the intent-based network system can either notify operations and suggest corrective action or eventually, automatically reconfigure the network to ensure compliance with stated levels. One of the most relevant examples is for security—a system like this would be able to quickly spot anomalous activity and bring it to the operations team's attention or potentially solve the issue automatically.

Many of the building blocks for intent-based networking are being deployed today. Organizations leveraging software-defined networking, virtualization technologies, and network analytics platforms should already be able to see how an intent-based architecture could orchestrate an information-rich and highly flexible network environment.

Let's now look at the key elements described in Figure 3, that together are required to deliver on intent-based networking:

**Three Key Elements of Intent-based Networking**

1. Intent: The first principle is intent, or the ability to apply business level objectives to the network. Essentially, your intent is "what you want to accomplish." It is not related to the CLI command, but rather is tied to an objective or outcome. This intent is captured in some form by the system (potentially plain language GUI) and then translated into *policies* that can be applied across the network regardless of the specific infrastructure deployed. For example, your intent could be: Connect to a specific cloud application, enable access to remote office workers, or segment guest traffic from corporate traffic. With intent-based networking, the concept is to simplify the provisioning, operation, and compliance requirements by abstracting all the network steps for each device, leveraging the aforementioned policies to define the appropriate access levels, security, service levels, and compliance with contextual understanding of the network infrastructure. Abstraction is an important consideration, as it will dramatically simplify the process of turning up new network services. Also, given the stated challenges in Figure 2 regarding lack of networking and new technology skills, simplifying the process of turning up new services should be welcomed by most organizations.

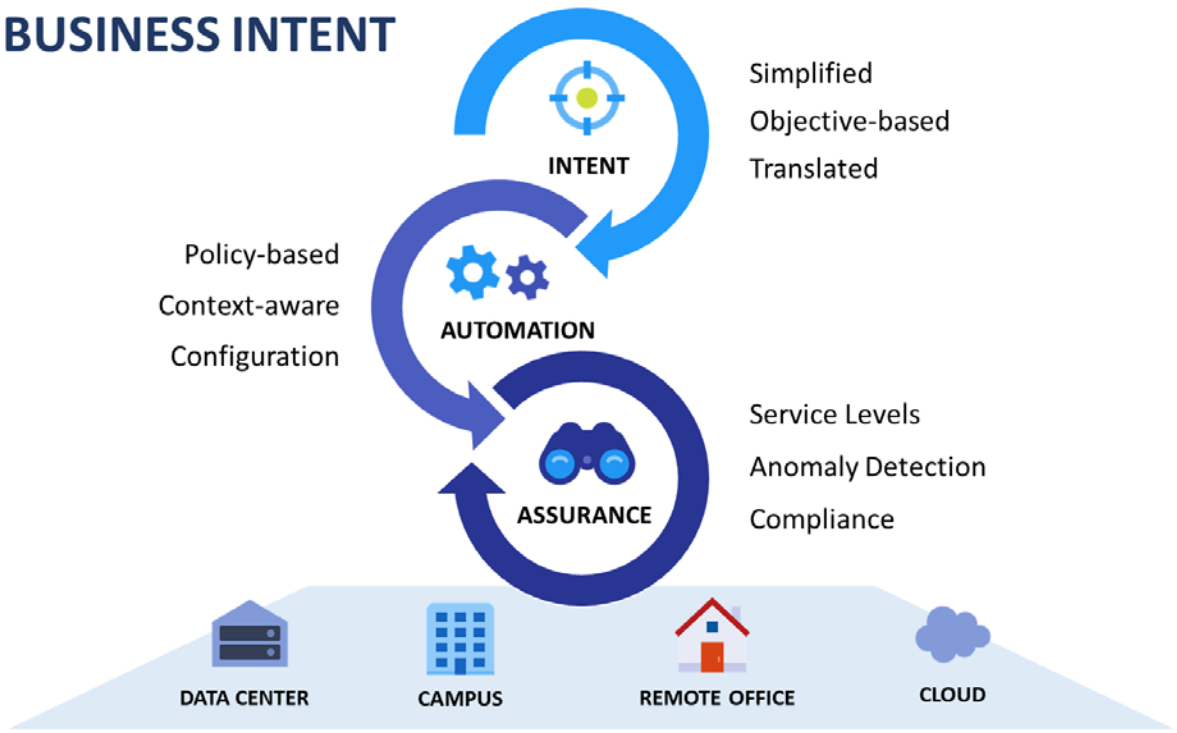
2. Automation: Once you have defined your intent and created policies, it will be critical to accelerate the time to provision. Automation will enable network teams to dramatically reduce the time to implement change. The same automation that will help accelerate initial provisioning cycles will also aid in automating future changes. As organizations continue to grow in size and complexity, adding cloud, IoT, and more remote workers, automation may be the only way to aid network administrators that are already unable to meet the service level and security demands of the users, applications and business. It will also be important to look for automation systems that allow for "semi-automatic" modes until existing staff are comfortable with the decisions being made automatically. Automation systems also need to seamlessly integrate with artificial intelligence (AI) and machine learning (ML) systems. Again,

based on the challenges cited above, organizations struggle to eliminate the delays associated with provisioning new services and devices, to implement security, and to rapidly scale the environment. Based on these challenges, automation is long overdue in the network space.

3. Assurance: The ability to assure that the correct services have been put in place will be critical. This starts with complete end-to-end visibility, across each domain or across all of them. The visibility and context should not be limited to devices in each domain, but rather will encompass the complex interactions between applications, users, and machines, across any location or cloud environment. The intent-based networking system needs to be able to provide verification of network-wide behaviors, predict the results of changes, track compliance with the stated intent and policies, and provide guidance on remediation when there is misalignment. Given the challenges related to network performance and security implementation, this principle of intent-based networking should be welcomed. To do this in large, complex environments, artificial intelligence and machine learning will be required. These technologies need to be part of a closed-loop system that is constantly checking network state, performance levels, and security status, providing context based on locations and devices and realigning resources in order to meet service levels or compliance regulations. Again, this is an area where IT teams may want to start with a "semi-automated" mode to personally verify the changes that will be made or not made. Ideally, organizations would decide what simple changes can be made in an automated fashion. The machine learning will be important to employ in order to create a baseline of performance and security so it can rapidly identify any deviation from "normal." This anomaly detection needs to occur in real time to mitigate risks.

The "Assurance" function provides verification of network-wide behaviors, predicts the results of changes, tracks compliance with the stated intent and policies, and provides guidance on remediation when there is misalignment.

**Figure 3. Foundational Elements of Intent-based Networking**




*Source: Enterprise Strategy Group*

## Benefits Associated with Intent-based Networking

Deploying a solution based on these principles should enable organizations to accelerate strategic initiatives like digital transformation, mobility, IoT, cloud computing, and security. How will it accomplish that? Intent-based networking has numerous potential benefits to organizations, including:

> Intent-based networking will encompass people, process, and technology that span data centers, campuses, remote locations, IoT devices, and the cloud.

- Agile and responsive network environment: Leveraging intent and automation will greatly accelerate an organization's time to respond to market changes. By eliminating time-consuming, repetitive manual processes, organizations can now dramatically reduce the time to provision network and security services. The amount of time saved will correlate to the extent to which you have deployed intent-based networking, the size of the environment, and its level of complexity. Regardless of these factors, policy-based intent and automation should help to accelerate provisioning and deployment in any size environment.
- Rapid scale: For organizations in high-growth mode or looking to ramp up their use of IoT devices, intent-based networking can help organizations quickly scale up resources, and not just for application to application, and application to user communication, but also for machine to application, machine to machine, and machine to user communication. Intent-based networking will not only enable rapid scale, but will also ensure that the associated service level agreements (SLAs) and security are in place according to the established policies.

- **Efficient use of highly skilled resources:** Intent- and policy-based automation will ensure networking team resources are not wasting time performing repetitive, manual tasks. Instead these valuable resources can be focused on more strategic initiatives like defining policies and programming the network. As a result, your current team will be able to manage much larger and more complex environments more efficiently and enjoy the challenge of high-value projects that drive innovation and result in business value.

- **Improved customer experience:** A closed-loop assurance system will constantly monitor the environment and ensure prescribed performance levels are met, and when they are not, either immediately notify operations or eventually based on the defined policy, take corrective action in real time. Providing optimized performance and availability will help to improve overall customer experience for both internal and external customers.

- **Threat detection and containment:** As an integral part of the intent-based architecture, the end-to-end visibility combined with machine learning technology will be able to quickly identify potential threats and either notify operations or take immediate action using automation to remediate them. Mitigating risk has always been a top concern for CIOs and is now top of mind for CEOs. Security concerns also slow down the adoption of new digital initiatives. Any solutions that help to mitigate risk will provide value to the business. Again, as security is deployed as part of the wider intent-based networking architecture, the greater the impact and value it will bring. For example, historically there has been limited deployment of network segmentation because it was too complicated. Fortunately, intent-based networking uses policy-driven automation and can make automated network segmentation widely deployed in the future, reducing or eliminating many security threats that exist today.

- **Accelerated cloud adoption:** ESG research shows that the most often cited way public cloud computing affected respondent organizations' network strategy was the creation of a seamless network that connects on-premises and off-premises resources.[2] Intent-based network solutions will integrate on-premises and cloud resources to ensure the appropriate performance and security to connect both data center and remote locations directly to cloud resources.

Now that we have defined the key elements of intent-based networking, it is also worth noting what intent-based networking is not. IT leaders should not think of intent-based networking as a single point product, technology, or piece of software that will cover all the issues discussed. IT teams need to think of intent-based networking as an evolution and work to create the appropriate architectural approach. Intent-based networking will encompass people, process, and technology that spans all relevant domains, including data center, campus, remote locations, IoT devices, and cloud. It will also cover communication from application to application; application to endpoint, regardless of machine or user; and machine to machine. Also, it is important to remember it can be deployed in a single area to start, but it will deliver incremental value as it is deployed across the entire environment. Organizations have the potential to benefit greatly from intent-based networking, but many may be unclear on the best way to get started.

## Ten Guiding Principles for Getting Started with Intent-based Networking

There is a clear need to change the current networking paradigm, but how should IT get started with transforming and evolving their network environments? Here are some essential guidelines IT leaders should embrace now to evolve their networks to intent-based networking. IT leaders need to:

1. **Develop an IBN Roadmap**: *Begin questioning all IT projects in the context of an intent-based networking roadmap*.

[2] Source: ESG Brief, *Impact of Cloud Computing on the Network*, October 2017.

Just as the evolution to private cloud was a journey, the evolution to intent-based networking will be a multi-step journey. Look at all your networking projects in the context of your intent-based networking strategy and make course corrections wherever there is serious misalignment. Ask questions like:

i. How will this new project get us closer to intent-based networking? (If the answer is "it won't," ask: Why are we doing it?)

ii. Do these new network devices provide the programmatic interfaces required for IBN?

iii. Does this system support or integrate with the intent-based networking elements of intent, automation, and assurance?

iv. What steps in my intent-based networking roadmap can be implemented for real immediate benefits?

v. How will this change impact other areas of the network? (Do I understand the current environment holistically?)

2. Embrace Change: *Transforming your network requires new skill sets.*
To provide value to their organizations, network teams should learn new skill sets, develop a broader repertoire, and be more open to collaborating with other departments. Digital transformation and the evolution to intent-based networking will require teams to be more flexible, much in the same way that the transition to server virtualization did, and will require the network team to interact more with the business. For executives, now is not the time to be a laggard. Empower your employees to learn new skill sets and help drive change in your organization.

Intent-based networking can build on existing software-defined networking solutions by orchestrating policy-based automation across multiple domains.

3. Acquire Expertise: *Build expertise in-house or augment with external services.*
IT leaders need to decide whether they are going to complete this transition using skills developed by internal resources or to also hire a trusted partner with intent-based networking expertise to help guide them through the process. This decision will be mainly guided by the organization's philosophy. For example, does your company develop skills and capabilities in-house or does it prefer to partner with organizations that can provide the necessary expertise? If going outside, be sure to understand what certifications and prior experience vendors have with intent-based networking. Can they provide references or proof of demonstrable value that they delivered? Also, you need to understand what biases your partner may have toward particular vendor solutions.

4. Build Consistency: *Define what intent means in your organization.*
Understand that not everyone may have the same definition of intent. Put in place definitions and training so that all team members can share a consistent vocabulary. In addition to intent, you should make sure that team members understand how to create policies. Also, understand what the biggest challenges are in your environment. Understand and articulate how intent-based networking can help overcome those challenges. It will be imperative that you develop some early use cases and outline the anticipated benefits for the business. Communicate any early successes widely.

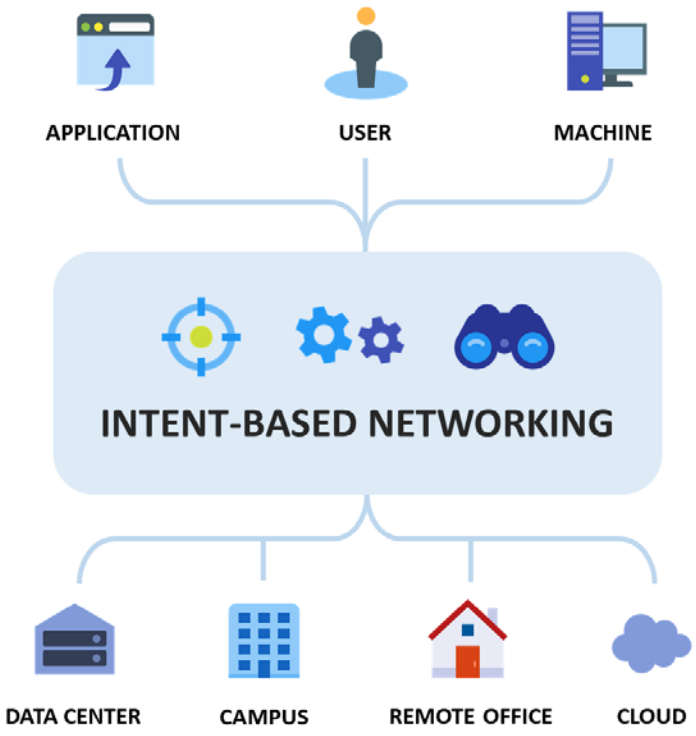
5. Build on Existing Investments: *Elements of your current network are already "intent-ready."*
Understand how existing technology investments will let you evolve to intent-based networking. Many facets of

intent-based networking can build on existing software-defined networking solutions by orchestrating policy-based automation across multiple, separate domains. As part of the process of evolving to intent-based networking, IT leaders should review existing investments with their network vendors and trusted partners. IT teams need to understand whether they can articulate a path to get from the current environment to a full intent-based networking solution. This is an important step, especially depending on where the organization is in its network infrastructure lifecycle. Once this path is understood, the team can build an effective roadmap.

6. Start Locally, Think Globally: *Identify domains to benefit most from initial intent-based network deployments.*
To really maximize the benefit of intent-based networking, IT needs to implement comprehensive, end-to-end architectures across all domains, such as DC, campus, branch, extended enterprise, cloud etc. However, that does not mean that you can't get tremendous value by starting intent-based networking in a single domain. Again, this should be based on which domains are the most important for an organization's digital transformation plan. Part of a global approach requires that IT leaders also consider how the network will connect users to applications and machines, machines to applications, or applications to applications. IT leaders need to build a roadmap and architectural model that allows them to deploy intent-based networking in stages, and define the incremental benefits possible with each stage (e.g., DC-branch-campus-cloud-devices, etc.).

To maximize the benefit of intent-based networking, it needs to be applied across all domains, such as DC, campus, branch, extended enterprise, and cloud.

**Figure 4. Comprehensive Coverage with Intent-based Networking**




*Source: Enterprise Strategy Group*

7. Integrate Security: *Security integration is key to a successful intent-based networking strategy.*
Incorporate security as an integral part of intent-based networking across "intent," "automation," and "assurance" functions. Network teams should start collaborating with the security team, primarily to educate the security team on intent-based networking and how it can help provide tighter security—in particular, the ability to use the intent-based network continuous loop framework to provide ongoing protection and alignment to security policy and compliance requirements. Specifically, your IBN implementation should provide traffic segmentation based on business roles for connections to remote or cloud computing sites to simplify threat protection and reduce the attack surface. The ability to continuously see network traffic activity, including in encrypted environments, across the distributed network and leverage of machine learning to detect anomalies would be another important asset. Anomaly detection can lead to fast quarantine and containment through automation. Eventually, the increased accuracy delivered with machine learning could lead to a fully automated response to mitigate attacks. Most important will be the ability to understand what policies need to be put in place to ensure the appropriate levels of security are used based on the application or services being deployed.

> Intent-based networking provides a continuous loop framework to provide ongoing protection and alignment to security policy and compliance requirements.

8. Balance Open with Pragmatic: *Solutions must integrate existing and emerging technologies without compromising reliability.*
Your intent-based networking system needs to integrate with technologies and systems that enable business agility and technical innovation. Certainly, open solutions with application programming interfaces (APIs) can enable organizations to connect different domains (DC, WAN, campus, cloud, etc.) and complementary systems (SIEM, ticketing, weather forecasts, etc.). However, this "openness" needs to be balanced with the need for a robust and proven solution. Given all the anticipated security and other benefits that are expected from intent-based networking, it shouldn't be a science experiment, full of trial and error, but rather a solid solution that will enable the organization to grow the business on day one. IT leaders should thoroughly evaluate solutions and their ability to openly connect with APIs to support the business and technical innovation they need.

9. Leverage AI and ML: *Scalability and complexity requires increased network intelligence.*
As the network environment scales, it will become exceedingly difficult to effectively manage it and ensure the prescribed service levels. The network is inherently difficult to manage today, and, once cloud computing and IoT are fully adopted, the complexity will be overwhelming. Solutions will need the assistance of artificial intelligence and machine learning to analyze the vast amounts of data generated from the network and take the appropriate action. Important note: Look for solutions that have the ability to run in "semi-automatic" mode until operations are confident that automation will make the right decision.

> The scale of IoT and cloud require artificial intelligence and machine learning to analyze the vast amounts of data generated from the network and to recommend the appropriate action.

10. Integrate Automation and Assurance: *The integration of automation and assurance are essential to continuously enforce intent.*
While defining the intent and related policies are necessary, in order to get started, a solid foundation of automation and assurance needs to be in place to configure, maintain, and optimize the stated intent. This begins with an assurance solution that provides complete visibility into the network devices and state, and the context to understand how to automatically configure all the devices in the data path to achieve the requisite performance

and security. Contextual data analysis is important before, during, and after deployment to help ensure that the network is delivering the desired outcome throughout the process. Once configured, closed-loop integration between assurance and automation systems is required to ensure service and security levels are adhered to on an ongoing basis.

## The Bigger Truth

The current reality is that business is moving at a faster pace than ever before. To cope with this, organizations are creating initiatives like digital transformation, deploying IoT devices, and leveraging cloud computing. These are variations of the same theme, which is to make the organization and the underlying technology more agile and adaptable to change. The ultimate goal is to improve customer experiences and help grow the business.

As all of these initiatives are implemented, the network will become more relevant to the business. As such, it needs to enable the business and not hold it back. To do, this the network needs to be able to dynamically align to changing business requirements. Also, given the volume of IoT devices and increased use of cloud computing, modern networks will scale to greater sizes and increase in complexity. As a result, IT needs solutions that are easier to use, that minimize manual intervention, and that help maintain service and security levels in dynamic environments. The network needs to help organizations drive growth.

Intent-based networking is well positioned to enable organizations to accelerate digital transformation, cloud adoption, and IoT as well as overcome existing and future challenges (speed, scale, complexity, and security) facing the network. It will be simpler to use, abstracting all the repetitive manual configurations with network-wide automated solutions that provide contextual awareness and deploy a closed-loop monitoring system with machine learning to take corrective action when there is a deviation from the norm to ensure service and security levels. IT leaders need to start evaluating intent-based solutions and assessing their own environments now in order to develop a clear roadmap to transition to a new network architecture. By engaging earlier, first movers will be able to take advantage of the benefits sooner and accelerate business growth.




**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.



www.esg-global.com contact@esg-global.com P. 508.482.0188