White Paper

Outcome-Driven Networking – Automation and Intelligence for the Network

By Bob Laliberte, ESG Senior Analyst

November 2017

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

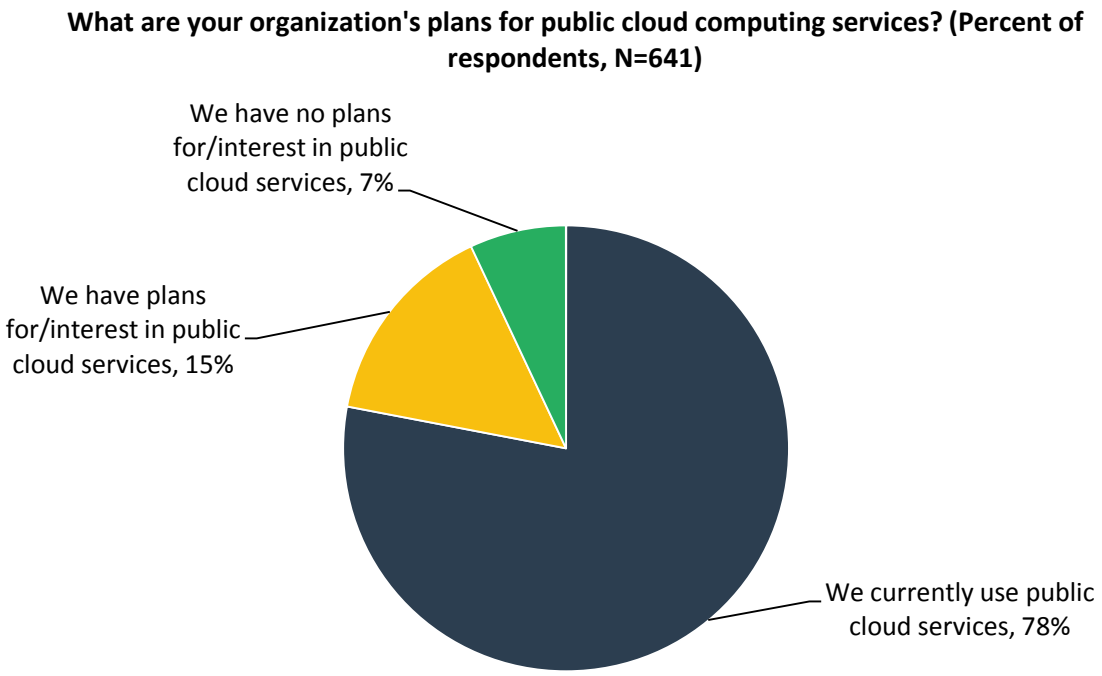
Contents

Introduction

The pace of business continues to accelerate as it strives to keep up with a dynamic economy and demanding consumers. Organizations are responding by embarking on digital transformation initiatives, solidifying their role in a global economy by opening geographically dispersed branch offices and increasing their use of cloud computing. The desired result of these initiatives is to create a foundation upon which the company can respond more quickly to the needs of customers, partners, and a global market. From an IT perspective, this means it needs to deploy solutions with higher levels of agility, security, and performance and ensure that the network underlying all these activities is robust and flexible enough to withstand the adaption necessary to keep up with this rapid transformation.

ESG research supports this transformation as the *2017 Public Cloud Computing Trends* report revealed that more than three-quarters (78%) of midmarket (100 to 999 employees) and enterprise (1,000 or more) organizations report actively using public cloud services. This indicates widespread adoption across all industries and a rapidly maturing market.

Figure 1. Plans for Public Cloud Computing Services



Source: Enterprise Strategy Group, 2017

To be clear, this transformation isn't isolated to just data center solutions; the implications extend far beyond the walls of the data center. In fact, as cloud computing and IoT initiatives continue to expand, the WAN will play a far more important role in enabling an organization to transform. This is especially true for those organizations with remote and branch offices as legacy compute paradigms for these locations are rapidly shifting to direct to the cloud. The network and WAN, in particular, are poised to play a significant role in the future, and organizations need to ensure they contribute to an agile environment and don't become a costly anchor.

Moving forward, organizations need to focus on how the network (including WAN) can help grow the business. ESG research asked 300 respondents to identify which network infrastructure capabilities they believed would have the

greatest impact on that goal, and the responses indicate that network security (cited by 46% of respondents), network visibility (25%), enabling new applications (23%) and IoT (23%), application performance (23%), and availability (21%) are all critical to growing the business.[1] In addition, 25% of respondents cited the ability to enable more choice and flexibility in the adoption of cloud computing as a capability that would be important to growing the business in the next 24 months. This is important to note because the dedicated WAN links needed to connect to cloud computing sites are not typically described with words such as choice and flexibility—rather, words such as costly, long provision cycles, and limited bandwidth come to mind.

The network needs to be more focused on delivering a positive outcome in a simple, timely, and cost-effective manner. Modern SD-WAN solutions are helping to change that perception, as early adopters have recognized significant value by leveraging software to automate, optimize, and accelerate WAN deployments. Most importantly, these solutions need to be driven by business outcomes.

Challenges

Organizations that are adopting a necessary digital transformation and embracing cloud computing are quickly realizing that legacy WAN solutions and architectures are holding them back. Specifically, organizations are challenged by:

- **Complex manual solutions.** The requirement to deploy resources to enable remote sites or even enact changes on a site-by-site or device-by-device basis will not only take a lot of time, but repetitive manual process can also be prone to human error. These errors can result in further delays while the NOC team troubleshoots the problem. Plus, in many organizations, any changes to the network or to systems may have to occur during a maintenance window. The inability to complete all changes requires another maintenance window cycle to complete them.

- **Costly and inflexible MPLS solutions.** While MPLS solutions have been an industry standard for WAN links, they tend to be costly, and organizations often must make price versus bandwidth tradeoffs to accommodate budget constraints. Also, because they are sourced from Telcos and typically have lengthy provisioning cycles, changing an existing service or bringing up a new one may create delays in projects or deployment to new locations.

- **Bandwidth-constrained, unsecure, and unreliable Internet connections.** In some cases, organizations turn to Internet connections, which are more cost-effective, but may be unreliable shared connections and quickly become bandwidth constrained. Organizations are also concerned about how secure these Internet connections are, especially if sensitive data is being transferred, such as PCI or HIPAA related content.

- **Time-consuming network operations.** Network operation centers need to have dedicated monitoring tools to closely monitor network performance across all connected sites and devices and then adjust as needed. As mentioned, manual solutions will require device-by-device changes and, depending on the scope of the change, may require another maintenance window.

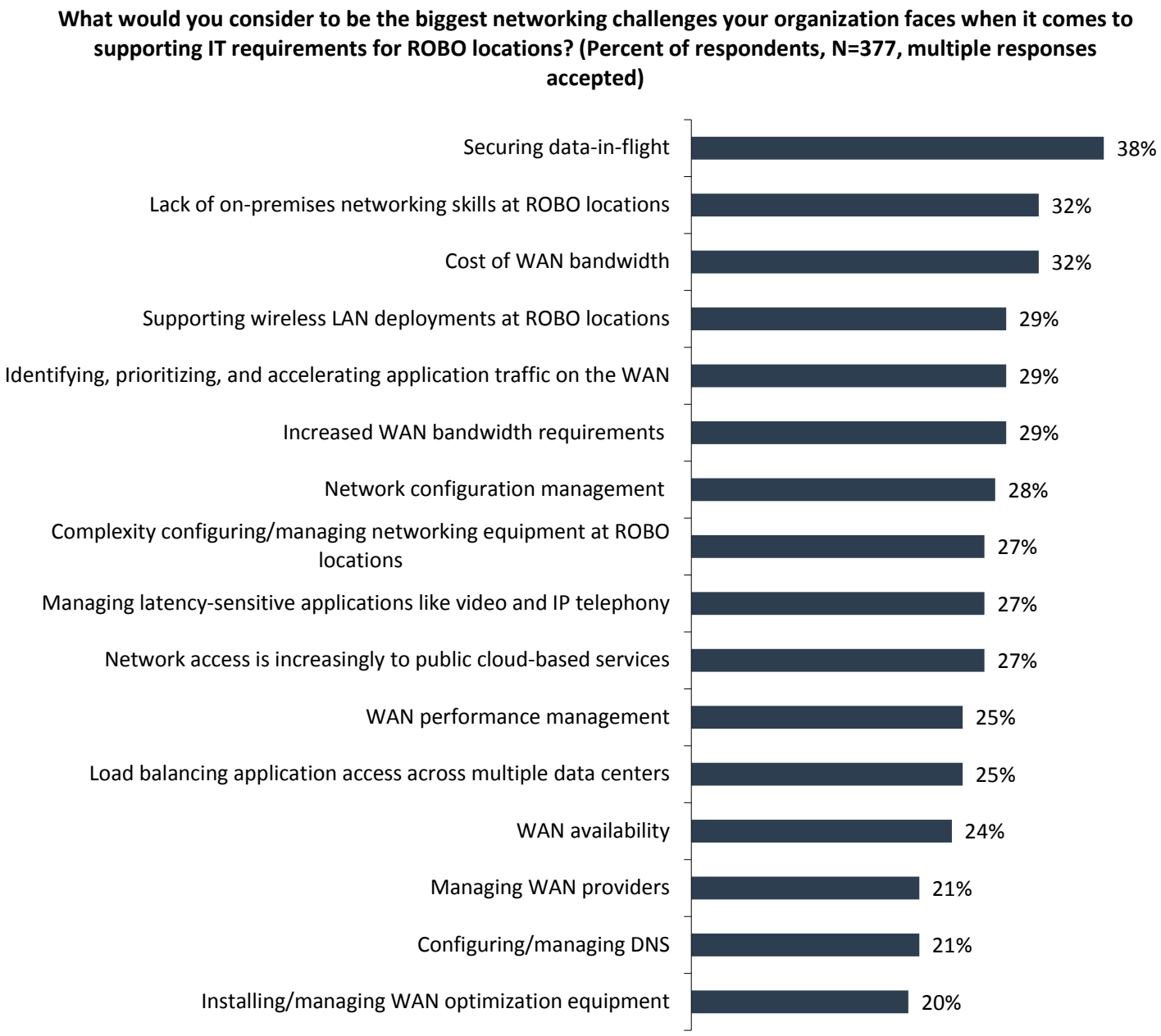
- **Security concerns.** Security is now a major business concern as any data breach will not only result in lost data, tarnished reputation, and huge costs, but could also ultimately cost the CEO and/or CISO his or her job. As mentioned, this is a top concern with Internet connections, but organizations also need to understand the security implications of implementing direct-to-the-cloud solutions for remote branches and offices.

- **Immature SD-WAN solutions.** Solutions are emerging to overcome many of these challenges, but it is still a fragmented market with dozens of solutions with varying levels of maturity and capabilities. Some offerings may still require

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

manual configuration via CLIs at the edge, tying up resources and keeping the focus on the network and not a business outcome. It is up to the organizations to perform their due diligence to match the best solution to their particular needs and evaluate its ability to enable an outcome-driven network and scale in a simple manner. Figure 2 illustrates the reported network challenges in supporting IT requirements for remote and branch offices.[2]

Figure 2. Biggest Network Challenges Supporting IT Requirements for ROBOs



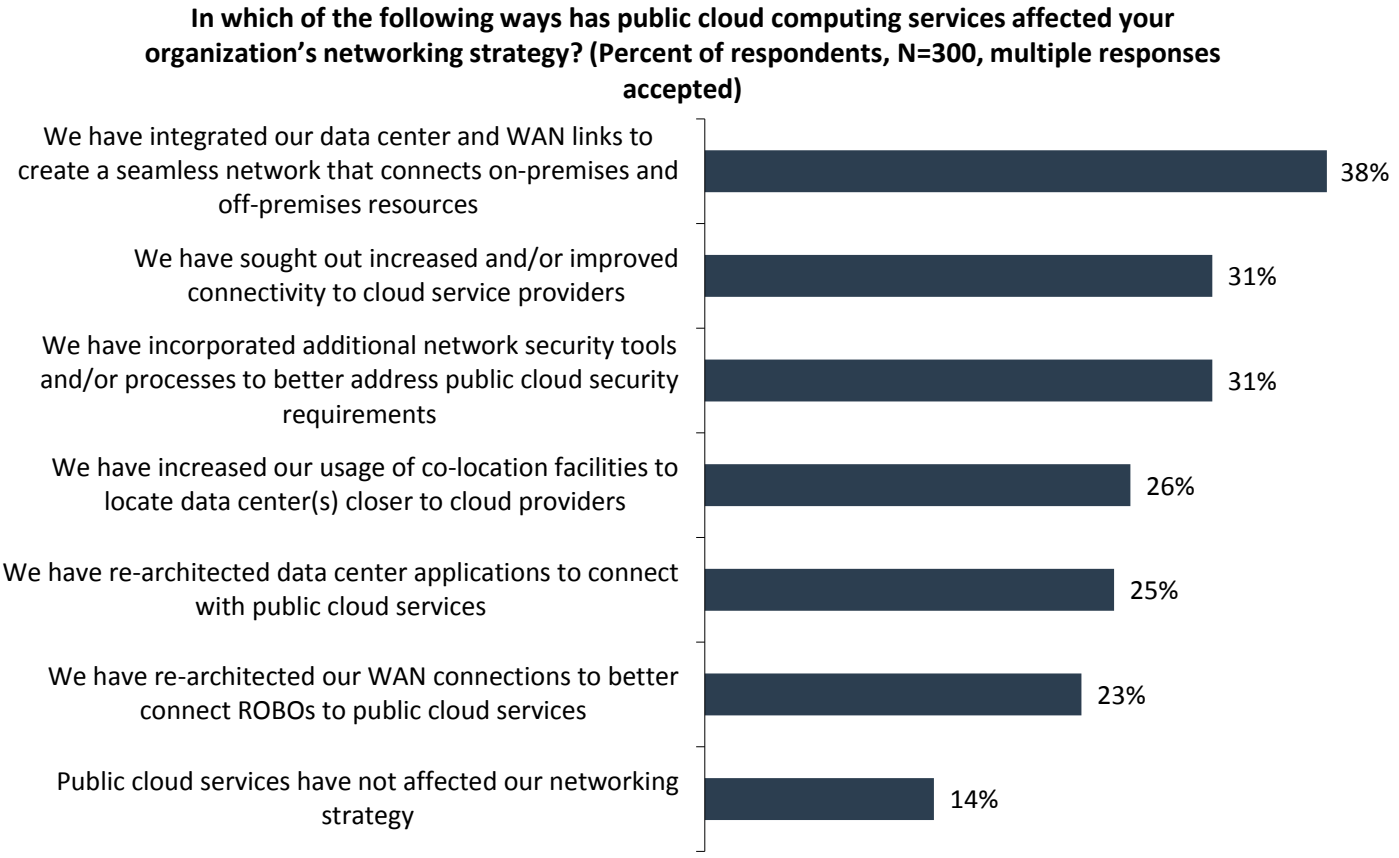
Source: Enterprise Strategy Group, 2017

- **Public cloud connections.** ESG research asked respondents how public cloud computing was impacting their network environments. The results are shown in Figure 3.[3] Respondents cite creating seamless network connections to the

[2] Source: ESG Master Survey Results, *Remote Office/Branch Office Trends,* to be published.
[3] Source: ESG Brief, *Impact of Cloud Computing on the Network*, October 2017.

cloud, obtaining additional or improved connectivity to the cloud, adding more network security to these connections, and re-architecting WAN links to enable better cloud connectivity as impacts.

Figure 3. Public Cloud Computing Impact on the Network



Source: Enterprise Strategy Group, 2017

Overcoming These Challenges

To change the paradigm and overcome these challenges, organizations need a different approach for their network and more specifically for their WAN connectivity. Instead of starting out any process or network change by thinking about each step that needs to be taken for it to happen, organizations need to start by thinking about the desired final outcome and then work backward to determine the processes that are required to make that happen, simplifying or consolidating stages and steps. This new approach is referred to as "outcome-driven networking." The key tenet is that changes to the network and its control are dictated by the desired business outcome.

Certain requirements need to be implemented to build an outcome-driven network. Specifically, outcome-driven networking solutions need to have the following capabilities:

- Abstraction and automation. Abstraction will take the form of being able to translate a desired outcome into the discrete actions that the network and any adjacent functional areas need to take. For example, this could include understanding the context of an application-centric policy to determine the appropriate prioritization, network links, gateways, and security functions that need to be allocated. This abstraction layer is critical to aligning business outcomes to the underlying infrastructure. It is not a simple task and will require solutions that have a new level of intelligence and comprehensive understanding to be effective. Automation that goes beyond adopting an intuitive GUI to replace a standard CLI will be critical for organizations to accelerate the time to provision network and security

functions. This is really about shifting from relying on manual device-by-device processes, which may require maintenance windows and take weeks to complete, to leveraging policy-based automation, which can reduce network-wide deployment time to just minutes. As DevOps and cloud computing continue to force networks to be more agile, organizations are going to have to rely more on automated solutions leveraging application-centric policies to meet the needs of the business.

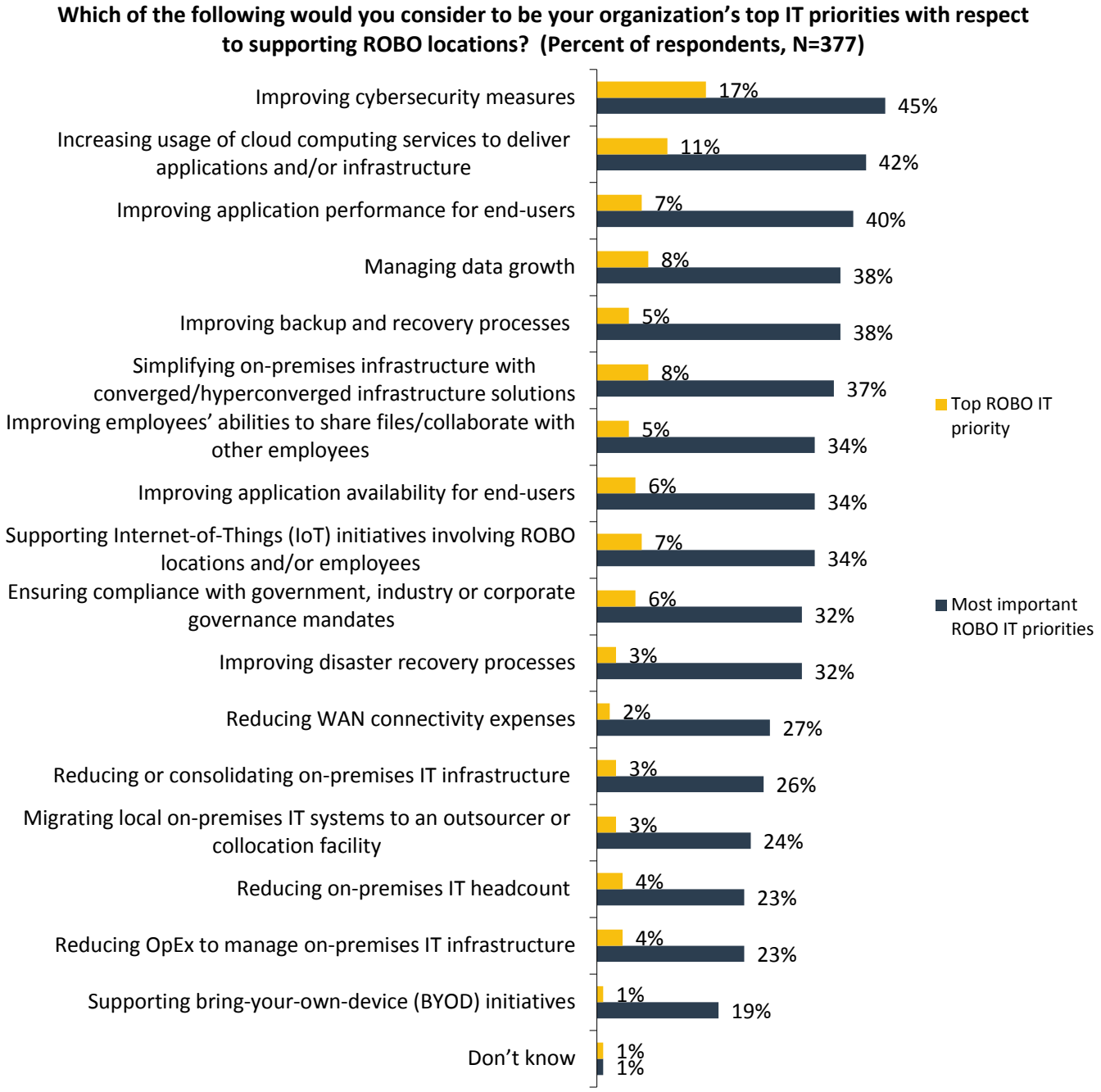
- **Ubiquity.** Configurations and application-centric policies need to extend across the entire environment. Because organizations operate with globally dispersed data centers and branch offices and a majority already leverage cloud computing, pervasive WAN connectivity is critically important. However, so too is the ability to ensure that the desired outcomes and underlying configurations are intelligently deployed universally and maintained or adjusted as required. This means that systems need to maintain context, so that different configurations can be applied to different devices as long as the outcome criteria is met. In addition, it also needs to be simple to use and have a centralized console. As technology progresses, sophisticated solutions will make the overall management, configuration, and network evolution that much easier. To ensure the appropriate outcomes, any new policies and resulting new WAN configurations need to be easy to create and even easier to deploy across a potentially complex global network in real-time.

- **Self-awareness and self-learning.** In order to have these attributes, the solution needs to leverage advanced technology such as artificial intelligence (AI) and machine learning (ML). These innovative technologies are key to enabling continuous availability and optimized performance. Essentially, once policy and performance levels have been established by the network team based on business requirements, SD-WAN self-monitors, learns, and takes corrective action in real-time. Organizations will be able to reduce dependence on error-prone manual interactions from resources with varying skill sets. Most importantly, these capabilities will empower the network to react to any anomalies in real-time and take corrective action.

These capabilities are critical to building an outcome-driven networking environment, and if deployed correctly, should yield several benefits. Organizations investing in this technology will dramatically reduce the amount of time and resources spent on mundane and routine configuration changes, instead freeing up time to work on more strategic business initiatives. The ability to rapidly add policies for new applications will reinforce the company's commitment to DevOps and deliver an agile WAN environment that reduces cycle times and enables revenue-producing applications to be brought online sooner. Spotting anomalies in the network and taking proactive corrective action will mitigate any financial or security risk to the business. Centralized and simplified management will allow fewer resources to manage a much larger and more complex WAN environment. Figure 4 confirms enterprises' top IT priorities with respect to supporting ROBOs. The networking responses are in line with the capabilities listed above.[4]

[4] Source: ESG Master Survey Results, *Remote Office/Branch Office Trends,* to be published.

Figure 4. Top IT Priorities with Respect to Supporting ROBO Locations



Source: Enterprise Strategy Group, 2017

Businesses operating on a global scale, adopting digital transformation and cloud computing, are quickly realizing that legacy WAN architectures are holding them back and are learning that not all SD-WANs have the necessary capabilities. These organizations need to have greater levels of agility and a future-proof architecture that will enable direct-to-the-cloud access from data center and branch offices.

Key Benefits to Deploying an Outcome-Driven SD-WAN

To enable IT organizations to focus on business outcomes rather than manual tasks and processes for the WAN, organizations need to shift to an outcome-driven networking approach. The goal is to eliminate as many of the manual and

time-consuming processes associated with complex WAN environments as possible and replace them with automated and intelligent solutions capable of implementing and maintaining the desired state of the network for any application or policy. Organizations need solutions that save them time and money, and mitigate risk.

To build a strong outcome-driven network for the WAN, solutions need to provide:

- **Improved application performance.** Since the policies will be focused on the application and prioritized based on the importance of that application to the business, organizations need to ensure they have defined priorities for each application. This priority should exist regardless of transport (private, public, or wired/wireless). It should also include priorities for failover and remediation. Solutions should ensure consistently great user experiences with manual intervention or configuration changes. The solution needs to have the ability to self-learn and adapt to meet business policies by enabling dynamic mid-flow steering and remediation, and applying prioritization policies at every node, hub, or spoke in the network automatically. Access to low-priority SaaS applications and services, such as watching video or peer-to-peer file sharing, will overwhelm bandwidth use and service levels. After appropriate examination of network traffic by application type and destination, low-priority network traffic may be carried by less expensive and low-reliability circuits while important uses such as VoIP may be kept on high-quality circuits.

- **Single click secure provisioning.** Operators should be able to quickly and easily create a secure link when needed to data centers, and cloud or branch offices. The elimination of time-consuming manual steps currently required to enable a secure VPN via gateways or hubs across public and private links will be critical to success. Ideally, this would occur via a single click that implements these configurations and changes across all connected locations and the cloud, and that creates tunnels instantaneously for branch-to-branch connectivity. Given the continued adoption of cloud computing and direct-to-the-cloud links from ROBOs, PKI integration will be required to scale effectively as more cloud connections are established. This will mitigate risk and save organizations time as it accelerates the adoption of new applications or cloud services.

- **True global segmentation.** Organizations can't afford to mis-configure firewalls, IPsec tunnels, or VLANs, which results in guest traffic mixing with corporate or PCI traffic. Therefore, outcome-driven solutions should automate the segmentation and security for guest, corporate, PCI, or any other similar traffic that needs to be treated differently from other traffic, based on global end-to-end policies. It will be important for each segment to have a set of unique policies to define application priority, security rules, and configuration information to provide scale, flexibility, and security. One size may not fit all in this case. Implementing this granular level of policies per segment will dramatically mitigate risk of a data breach due to human error and will be much more efficient. This can include as many segments that are governed by the same policies and necessary to keep traffic optimized and secure, thus freeing up time for IT to focus on strategic business initiatives.

- **Intelligent routing.** Driven by established global policies and not time-consuming manual processes, organizations need to leverage abstracted routing policies based on a desired business outcome. This will enable coordinated configurations across multiple locations and dramatically reduce the amount of time IT spends sending commands to various different and geographically dispersed devices. One of the keys to this functionality is having complete visibility across the environment, enterprise, and cloud, to properly determine configuration and routing options. This allows organizations to trust but verify that abstracted policies and automation functions are performing as expected. The goal is to reduce the time required to bring up a new cloud data center or integrate a newly acquired business or branch office. It is important to keep in mind that IT needs to become more agile and responsive to the needs of the business.

- **Service integration.** The ability to quickly and easily insert services at each branch will be imperative, especially for organizations with a large number of ROBOs. By reducing the number of devices deployed at a branch location,

organizations can reduce CapEx and OpEx, and simplify management. Today this may encompass the creation of third-party firewall services, such as a VNF within an SD-WAN solution, or leveraging the SD-WAN solution for network routing capabilities instead of relying on a traditional edge router. This will eliminate deploying multiple devices in each remote location as well as future truck rolls, and the resulting consolidation will deliver the aforementioned savings. It will also be essential that the service insertion extends to the cloud and enables third-party cloud-based security services to be automatically inserted as well. This is an area that bears watching as virtual network functions are added and greater benefits are achieved.

- Zero-touch operations. Once global policies have been defined, any devices rolled out to remote or cloud locations should not require manual configuration or reconfiguration of the network. This is also applicable to initial rollouts as well. Organizations deploying SD-WAN solutions to hundreds or thousands of remote offices or cloud locations will dramatically reduce the time and cost associated with bringing solutions online by having the ability to automatically connect, authenticate, and receive configuration instructions over the Internet. Furthermore, once deployed, solutions leveraging innovative AI and ML technology will provide dynamic self-learning and automatically adapt to changes by adjusting the configuration and services as needed to achieve the requisite business outcome. In a dynamic environment, solutions should not tie logical profiles to physical devices or serial numbers so policies can be quickly and easily applied to groups. Implemented correctly, zero-touch operations will save organizations a significant amount of time and accelerate the rollout of new locations or cloud applications. By starting with the desired business outcome, and leveraging outcome-driven network solutions, organizations can truly achieve significant benefits in time, money, and risk mitigation across a global environment, as well as accelerate their digital transformation. Organizations can start by evaluating SD-WAN solutions today and incorporating other parts of the network as they become available.

The ROI of Outcome-Driven SD-WAN

The previous section covers many key technologies and functionality, that, when implemented correctly, can yield significant savings in time, CapEx, OpEx, risk mitigation, and improved customer experience for a geographically dispersed business. To understand the impact to an organization, take as an example a global enterprise with 75 remote sites. Assume the prior mode of operation included legacy WAN solutions that back-hauled traffic to the data center over dedicated MPLS circuits.

In the current model, no segmentation is being done, unless the organization has deployed dedicated firewalls at each remote location—which adds significant CapEx and OpEx. It will also require organizations to dedicate IT staff with the skills to configure and operate those devices. Global segmentation functionality in SD-WAN solutions eliminates the need for firewalls to be deployed at each site in order to segment traffic. Global segmentation will mitigate risk by separating sensitive PCI or HIPAA traffic from guest and corporate traffic. Depending on the size of the remote office, removing a firewall from each site could result in a savings of between several hundred to tens of thousands of dollars per location, plus, with one year of annual maintenance, total cost savings could range between $20,000 and $1,500,000[5].

Intelligent routing and service integration would allow organizations to go direct to the cloud from remote locations as well, provided that SD-WAN performs the necessary routing functions. This would have multiple benefits, as it would reduce the amount of traffic backhauled to the data center by as much as 20% and would eliminate the need for a router at each remote location. Total savings, including one year of annual maintenance, could range between $23,400 and $914,580.[6]

[5] Assumes firewall list prices of $230 to $17,500 per site and 20% annual maintenance costs.
[6] Assumes branch router list prices of $261 to $10,162 per site an 20% annual maintenance costs.

Deployment and time associated with ongoing operations would be dramatically reduced with zero-touch capabilities and single-click secure provisioning, as rolling out sites in a legacy environment are typically limited to deploying two to four sites per week. This would result in a timeframe of four to nine months to deploy to all the sites. Leveraging global policies, single-click secure provisioning, and zero-touch deployment and operations, organizations teams should be able to roll out 75 sites in less than a week. This results in a time savings of almost 95%. In addition, this could accelerate the rollout of new revenue-producing applications and enable IT to focus on other strategic priorities.

Perhaps one of the hardest areas to quantify, but one that could yield the highest return, is the improvement in customer experience achieved by establishing priorities on an application-by-application basis (including SaaS or cloud-based applications), ensuring that customer-facing voice and video applications are assured performance, even in the event of an outage. Given how impatient modern consumers are, ensuring consistently high performance will help to reduce churn.

Combining these benefits, an enterprise with 75 remote locations has the potential to save up to $2,414,580 on equipment and a single year of maintenance, up to 20% of bandwidth costs, over eight months of deployment time, plus additional time savings in ongoing operations due to efficiencies (global policies, zero-touch, AI, and ML) and most importantly, improved customer experience by leveraging outcome-driven SD-WAN solutions.

The Bigger Truth

As the pace of business accelerates, organizations need to find innovative technologies and solutions to ensure they are leading the market. Digital transformation, cloud-based computing, and DevOps are all driving more agile and responsive IT environments capable of responding to the needs of the business.

Ultimately, this is more than just agile and responsive networking, but an intelligent solution that can actually enable the business by focusing on and maintaining a desired business outcome. Because the WAN will play an increasingly critical role, it needs to be considered a strategic asset to the business. Organizations need IT teams to focus on being aligned with and concentrating on the outcomes that impact business, not configuring and managing network devices in isolation.

Outcome-driven networking changes that paradigm and tightly aligns IT and the WAN with the business. To make this transition, organizations need to acquire innovative technology capable of redirecting IT teams' efforts from tedious, manual tasks for configuring and maintaining a reliable and secure WAN, to driving positive business outcomes. The key is focusing on abstraction and automation of tasks, artificial intelligence and real-time awareness, as well as ubiquitous policy distribution via centralized management. Outcome-driven networking will enable organizations to transition from complex, costly, and time-consuming manually operated WANs to fully automated, self-aware, and application-centric policy-driven SD-WAN environments focused on the business outcome.

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