IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Comcast Business

Multicloud adoption, the rise of the distributed enterprise, and demand for rich media experiences require the convergence of agile SD-WAN agile architecture with a holistic implementation of security.

The Convergence of SD-WAN and Security Brings Benefits to Support Hybrid Work, Cloud and Rich Media

June 2021

Written by: Ghassan Abdo, Research Vice President, Worldwide Telecom, Virtualization, and CDN; and Martha Vazquez, Senior Research Analyst, Security Services

Introduction

Four primary market developments have influenced the enterprise digital journey and demand for a secure and resilient network:

- **Multicloud adoption.** Multicloud adoption has accelerated of late as enterprises seek agility, operational efficiency, and cost savings. This is evidenced by the significant increase in cloud spend, which exceeded 30% in 2020 across all large public cloud providers. Multicloud adoption requires secure and direct access to cloud resources, which legacy networks struggle to provide in a cost-effective and efficient manner. An agile connectivity paradigm is underpinned by an SD-WAN architectural framework. SD-WAN offers multiple connectivity options, flexible policy management and, most critically, integration of secure access. Adoption of SD-WAN is key to the transformation of enterprises toward a digital-native enterprise.
- **The distributed enterprise.** COVID-19 has accelerated a trend toward a massively distributed enterprise moving network functionality to the edge of the network. The WAN architecture must cater to the needs of office and remote workers with parity in terms of routing policies, security profile, and management of the WAN. IDC refers to this emerging architecture to support remote worker connectedness as the "branch of one." The emergence of the branch of one will change the dynamics of network economics and architecture. A software-defined WAN is more aligned with the constantly changing demands of office, remote, and hybrid workers.

AT A GLANCE

KEY STAT

In an IDC survey, 58% of global respondents reported that they felt much more vulnerable to security breaches because of their organization's move to a multicloud environment.

WHAT'S IMPORTANT

The new normal demands tighter integration between SD-WAN and security to address the emerging business needs of the enterprise.

KEY TAKEAWAY

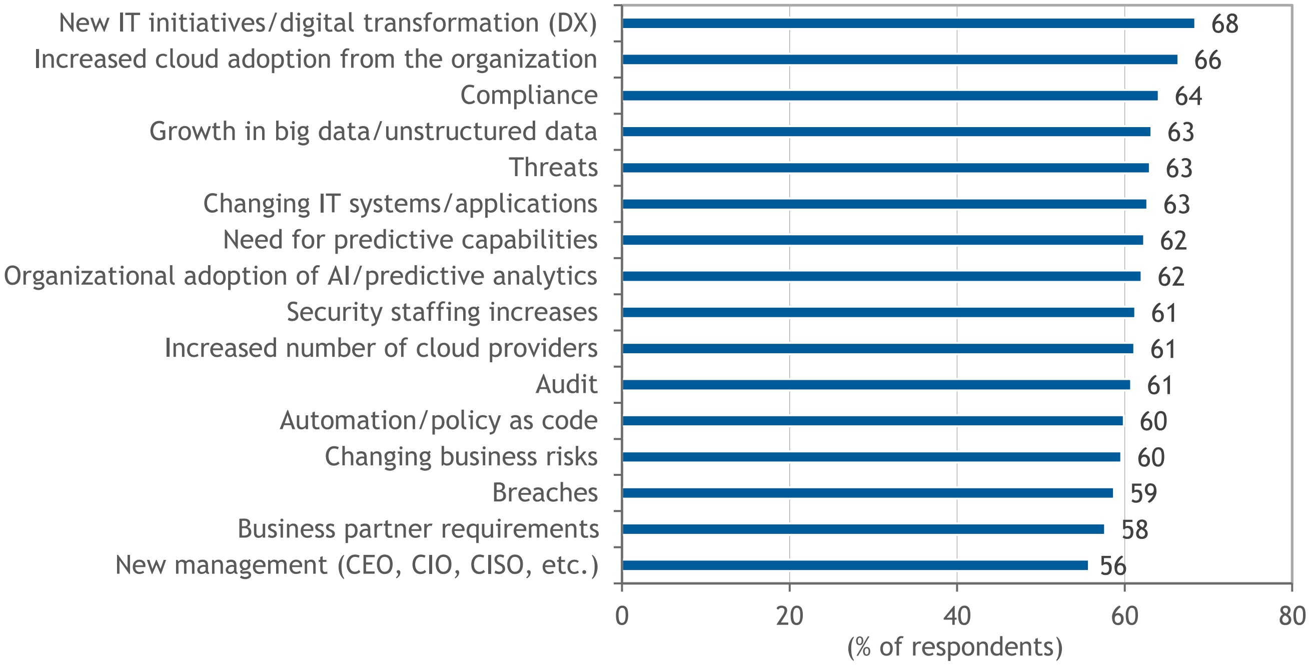
The convergence of SD-WAN and security is becoming a strategic imperative for enterprises because it optimizes the remote work environment, enhances connectivity to hybrid cloud, and facilitates access to applications from anywhere in a secure fashion.

- **Demand for rich media customer experiences.** As enterprises rely more actively on ecommerce, online marketing, and omni-channel to drive sales, a compelling customer online experience is key to competitive advantage. Advances in video streaming and communication technologies can enhance the online customer experience and create differentiation for enterprises that adopt those advances. Rich media or video-enhanced experiences are important to industries such as retail and finance because they drive a new dimension in a personalized, interactive, and high-fidelity online customer interaction. The evolution of streaming technologies targets improvements in lowering latency, enabling interactivity, delivering personalized video content, and ensuring secure access. These advances require a dynamic WAN architecture that adapts to changing bandwidth, performance, and low-latency needs. An agile and secure SD-WAN will provide the economically optimal connectivity options that rich media demands.

- **Enterprise security.** The current global pandemic forced the shift to a much more highly distributed workforce, causing enterprises to rapidly adopt a cloud-enabled infrastructure and pushing organizations to take an integrated and holistic approach to security. In fact, according to IDC's Security ServicesView 2020: Executive Summary, new IT initiatives/digital transformation (DX), increased cloud adoption, and compliance were the top 3 reasons for increasing security spending (see Figure 1). In addition, 58% of global respondents reported that they felt much more vulnerable to security breaches because of their organization's adoption of a multicloud architecture. With the widespread adoption of SD-WAN, the role of security had to evolve to address the expanding perimeter. Organizations are now considering new security strategies that include integrating network and security functionality onto their SD-WAN.

FIGURE 1: ***Factors Driving Increased Security Spending***

Q ***How important are the following in contributing to increases in security spending at your organization for the next two years?***



n = 1,500

Source: IDC's Security ServicesView 2020, November 2020

SD-WAN Is the Right Choice in the New Normal

Adoption of SD-WAN brings many benefits to enterprises. Key among them are the following:

- **Network resiliency.** Digital transformation and cloud adoption are key motivating factors driving the adoption of SD-WAN. A 2020 IDC survey of U.S. enterprises indicated that 68% of respondents will migrate to SD-WAN in the next two years. Enterprises are adopting cloud at unprecedented rates, and the shift to remote working requires an agile WAN architecture best served with SD-WAN. A highly distributed enterprise cannot rely on legacy networking solutions such as MPLS to meet the needs of remote workers. Remote workers require a cost-effective, flexible, and secure solution. SD-WAN provides remote workers with the same benefits as office workers in terms of policy, secure access, flexible bandwidth, and centralized management of resources. This hybrid work environment is expected to be the norm in the post-COVID-19 era. Software-defined architecture will continue to evolve to provide a cost-effective solution for remote workers and prioritize their personal and business communication needs.
- **Application awareness.** The WAN needs to adapt to the performance, security, latency, and priority needs of the multitude of applications that are hosted at public cloud providers or on premises. A software-defined architecture provides a framework to adapt routing policies and access policies for various applications independent of the hosting choice. Automatic configuration of these parameters is important to react to varying application needs and changes to networking performance. The integration of artificial intelligence/machine learning (AI/ML) technologies delivers a smart networking that offers the ability to achieve the goal of application-aware networking. By analyzing application performance, AI/ML can provide an SD-WAN orchestrator the required analytics data in real time to adapt network configuration to meet preset application policies. The use of AI/ML technologies can further optimize the demands of these applications.
- **Automated bandwidth management.** Rich media is key to a differentiated customer experience. Rich media is dynamic and variable in terms of bandwidth needs. Live streaming can experience unpredictable traffic peaks that demand an agile network that is able to react to these unplanned demands. It also requires a commercial framework that is cost effective and does not entail expensive upgrades during peak traffic. Automated bandwidth management is configured through the self-service portal. This allows centralized, autonomic, and dynamic bandwidth management or remediation.

Evolution of Security and SD-WAN

The wide adoption of SD-WAN among enterprise branch offices pushed the need for an integrated security approach to protect the network from being another attack vector for adversaries. The role of security within SD-WAN has evolved rapidly in the past several years to address the shifts that are occurring in combining networking, security, and the remote workforce. As organizations began utilizing SD-WAN to resolve network and latency issues, they were not initially prepared to address the security issues that would arise with a distributed enterprise.

Along with the increase in digital transformation, there is a drive to converge networking where security and IT teams are realizing the challenges of managing and protecting increasingly complex network across a wide scope of endpoints. As security has become a focus of conversation and less of an afterthought, organizations have reached an inflection point on the need to adopt new security frameworks to address the modern workforce. Traditional security controls deployed to secure the walled perimeter have expired, widening the perimeter to exist outside the datacenter to the edge and making any access point a potential attack vector.

That said, the attack surface has grown exponentially, leaving organizations even more susceptible to attacks. Integration of advanced security has become crucial as organizations need to take a more holistic view of security versus implementing more security point products such as firewalls, intrusion prevention systems, and secure web gateways. Organizations are faced with having to understand that if they are going to bring new digital capabilities into their infrastructure, they must anticipate the need to integrate security functionalities and controls that will help protect different IT architectures and environments, applications, and data. As a result, tight integration of advanced security tools into the SD-WAN has become even more important for organizations to reduce complexity and to assist in expanding security to any user access point.

Benefits of a Managed Unified Security Approach

For organizations struggling with managing multiple IT environments, utilizing a managed service provider to provide the management and monitoring for both the SD-WAN and security can help deliver a simplified experience. Security is complicated, and legacy security architectures tend to sprawl, including tens — if not hundreds — of security vendor products in the larger environments. In fact, IDC has found that organizations' top drivers for working with a managed security service provider include improved performance and efficiencies and the need for detection and response capabilities. Organizations are also likely to seek a service provider that can help gain access to emerging security functionality in which they could not invest on their own.

From a security perspective, there are several benefits for organizations to adopt security into their SD-WAN distributed networking model. A unified security approach for SD-WAN provides a simpler means to minimize the security risk by layering on additional security services that address the evolving security landscape. With changes constantly occurring with the modern workforce, SD-WAN with integrated advanced security functions can provide a more streamlined approach to managing policies by having consistent implementation of various security controls and configurations. In addition, organizations will minimize the complexity of implementing and managing separate security point products from different types of vendors.

The Future

At IDC, we expect two major trends to impact the future of SD-WAN. These trends will increase the adoption of SD-WAN as the foundation for a secure agile network:

- The underlying agile architecture of SD-WAN cements its important role in addressing connectivity and resource demands at the edge. Regardless of where SD-WAN functionality is hosted, on premises or at the provider edge, the underlying infrastructure can provide ample compute, storage, and networking to execute edge services. Depending on the latency requirements of edge services, the services can be hosted on customer premises equipment (CPE) devices or SD-WAN gateways or points of presence (POPs). In summary, SD-WAN provides both agile networking and edge resources needed to support the emerging edge services.
- 5G will emerge as a WAN connectivity choice because of its high bandwidth and low-latency capabilities, especially in the case of fixed wireless deployments. The integration of SD-WAN with 5G is ongoing, and we expect wider deployment of SD-WAN at the 5G edge in the coming years.

Preparing for the Future When Securing the Network

Organizations must take a "security first" mindset and view security as an enabler to improving the business itself. Making security a priority will drive internal conversations at the early stage of a project. In addition, organizations taking a holistic approach to security can help secure complex IT environments. Security investments should be focused on the specific needs of the business, and risks and should be fully considered at the outset of any project.

SD-WAN solutions are in a state of continuous evolution, and security tools are increasingly being embedded natively into these network platforms. Modern SD-WAN can deliver robust security capabilities across the enterprise without requiring the expansion of an on-premises security ecosystem, which can drastically decrease time to deployment, complexity, and both capex and opex while ensuring functional consistency. In addition, SD-WAN complements the added bandwidth from high-speed 4G and 5G networks.

Highly distributed organizations are migrating more workloads into a multicloud environment, creating more complexity for IT teams to manage data and applications from multiple devices and locations. Security controls, such as authentication, have become even more important because organizations need to give controlled access to end users. As organizations turn to adding in more security functionalities, many are considering new approaches such as those defined by IDC as pervasive application edge defense (PAED) and other frameworks such as Secure Access Service Edge (SASE). These approaches recognize that applications are a key control point for security and that keeping sets of applications secure all the way to the edge requires organizations to move what may have been just a collection of loosely affiliated point products to a fully integrated security framework that can recognize and integrate application-centric security into the digitally transformed enterprise.

The convergence of these tightly integrated security components, which include cloud security gateway functionality, data loss prevention platforms, and secure web gateways, enables the ability to unify user or group policies across the entire security stack and provide a single reporting mechanism. These emerging frameworks can also include areas of authentication to facilitate secure network access across on-premises and distributed cloud application environments. This converged security infrastructure shows promise in reducing the complexity of managing data governance policies across hybrid and multicloud environments.

Considering Comcast Business

Secure network solutions from Comcast Business

Comcast Business offers secure network solutions, which combine connectivity, network management, and integrated advanced security, powered by its ActiveCore software-defined networking platform. Secure network solutions from Comcast Business provide an efficient way to manage your network across multiple locations and platforms without sacrificing your network security options.

Network connectivity that scales

- Availability of broadband and dedicated Ethernet to keep businesses connected with fast, reliable Internet
- Comcast Business is powered by the nation’s largest Gig-speed network, offering business Internet speeds up to 100 Gbps
- Off-Net Internet Access available and provides businesses with off-net connectivity to help keep all locations across the country connected

Choice and efficiency

- Increase network visibility and manage security solutions with a unified digital experience
- SD-WAN provides network management combined with cybersecurity solutions
- Gain insights and control with ActiveCore, via desktop or through the ActiveCore mobile app

Integrated security

- Help protect against cyber threats like ransomware, malware, botnets, network intrusion, and volumetric attacks
- Integrated enterprise-grade network security solutions — all within a single platform
- Unified Security, Unified Secure Access, and DDoS Mitigation from industry leaders

Unified control and management

- Aggregate, orchestrate, and coordinate all network management across your locations
- Unified control, visibility, and management with ActiveCore
- Delivers real-time insights and powerful network control from anywhere
- Co-managed or fully managed offerings

Challenges

From a managed security services perspective, Comcast Business is up against a wide number of providers in the market. With organizations needing greater assistance to fight against the most current threats, offering advanced capabilities is now a crucial necessity. Keeping up with needs of the buyers for advanced security is difficult and takes a large number of resources to maintain a competitive position against other providers in the managed security services market.

Another challenge facing Comcast Business and the industry in general is interoperability. Enterprises expect their applications to operate in a multivendor environment and execute seamlessly across network boundaries. While efforts in orchestration and interoperability standards are ongoing, execution challenges remain. It behooves Comcast to address these issues in a collaborative approach with the wider ecosystem.

Conclusion

The industry is at an inflection point as it addresses the emerging demands for hybrid cloud connectivity, support of a widely distributed enterprise, and customer preferences for a rich media experience. Underlying these trends is a focus on security as vulnerabilities expand in the new normal. The convergence of SD-WAN and security is becoming a strategic imperative for organizations of all sizes because it optimizes the remote work environment, enhances connectivity to hybrid cloud, and facilitates access to applications from anywhere in a secure fashion.

> The convergence of SD-WAN and security is becoming a strategic imperative for organizations of all sizes.

About the Analysts

Ghassan Abdo, *Research Vice President, Worldwide Telecom, Virtualization, and CDN*

Ghassan covers the evolution of the Telco Cloud Ecosystem as well as the emerging Virtualized Enterprise Networking services. His primary focus areas include Service Provider SD-WAN and Managed Services, and emerging NFV-based Virtual Networking Services as well as other Managed WAN Services. In the Hosting and Cloud segment, Ghassan covers Service Provider Managed Hosting Services, including Hybrid Managed Private/Public Cloud Services, Colocation Services, Secure Cloud Connect and CDN Services.

Martha Vazquez, *Senior Research Analyst, Security Services*

Martha is responsible for IDC's worldwide research and analysis on enterprise and service provider security consulting, integration, and managed services as well as hardware and software support and deployment needs. She provides insightful market analysis and research to vendors, service providers, and end-user clients worldwide. Martha brings a breadth of knowledge and expert advice to assist vendors in developing marketing strategies, research, strategic alliances, and partners in this ever-evolving complex market.

MESSAGE FROM THE SPONSOR

Learn more about secure network solutions from Comcast Business:
https://business.comcast.com/enterprise/products-services/secure-network-solutions.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.