White Paper

Benefits of Managed Network Services in a Software-Defined Era

Sponsored by: Comcast Business

Ghassan Abdo Curtis Price
June 2020

EXECUTIVE SUMMARY

Enterprises globally have embarked on initiatives to transform their business processes to become digital-first enterprises. IDC predicts that the worldwide spending on digital transformation (DX) technologies will expand at a compound annual growth rate (CAGR) of 17.9% through 2021 to more than $2.1 trillion. DX has been shown to bring significant benefits to enterprises in terms of improved operational efficiencies, creation of new revenue streams, and enhancing customer experience. The COVID-19 pandemic is a testament to the resiliency and competitive differentiation of digital enterprises as ecommerce, a key pillar of their business, has flourished.

A successful DX journey will require enterprises to adopt key 3rd Platform technologies such as cloud, Internet of Things (IoT), mobility, and artificial intelligence/machine learning (AI/ML). The adoption of these technologies has elevated the wide area network (WAN) as a strategic initiative for enterprises. This is further underscored by market transformations that demand an agile WAN architecture, including:

- The accelerating growth of global IP traffic, estimated at a CAGR of 40%, is impacting the economics of network expansion.
- The proliferation of IoT and growth of global ecommerce are moving intelligence to the edge.
- The continued adoption of the cloud is transforming WANs.
- The increasing demand for rich media by customers is driving higher bandwidth at the branch.

Responding to these transformational forces will require an adaptable WAN architecture. Advanced networking at the branch is hence key to business agility and enterprise success measured in terms of improved employee productivity, customer satisfaction, and revenue growth. This demands a paradigm shift from reliance on discrete networking appliances toward a more agile software-defined and virtualized networking architecture. Enterprises are rapidly embracing software-defined WAN (SD-WAN) as the technology of choice for upgrading their current legacy WAN environment. In real deployments, SD-WAN has been proven to support direct and secure access to cloud applications, provide cost-effective growth in bandwidth, and improve network availability.

The choice of managed network services further complements the technical benefits of this new architecture with a commercial framework that provides full life-cycle advantages. Integrating a software-defined architecture presents deployment challenges for enterprises that are considering a do-it-yourself approach. Foremost are lack of technical resources and managing integration complexities. Besides de-risking SD-WAN deployment, a managed services provider can bring significant commercial

benefits including a cloud consumption model, integration of full-scale security capabilities, uniform service-level agreements (SLAs), access to pretested multivendor virtual functions, integrated self-service portals, and global reach. Further innovation in virtualized network services has been embraced by key participants such as communications service providers and vendors toward a fully automated and intent-based networking architecture. Enterprises will benefit considerably from these investments as they strive to enrich customer experience by incorporating modern AI and ML tools.

In summary, this document makes the case that managed network services bring significant benefits to enterprises as they undertake the journey toward a software-defined networking implementation.

ENTERPRISES FACE CHALLENGES WITH WAN IMPLEMENTATIONS

Modernizing the WAN is a critical decision by enterprises as they embark on the DX journey. Legacy WAN lacks the agility and ability to respond to increasing adoption of cloud services and demands for higher bandwidth. Most enterprises have identified four key challenges with current WAN implementation:

- Providing secure connectivity to cloud applications in a multicloud environment
- Managing hybrid connectivity options such as MPLS, ethernet, and 4G/LTE
- Allowing a common customer experience in varying deployment models (e.g., on premises and cloud hosted)
- Cost-effective management of applications at the branch

Enterprises, however, are cautious with the rollout of a new technology and its potential impact on mission-critical applications. Implementing a software-defined architecture has proven to be more challenging than various claims of zero-touch provisioning advertised by SD-WAN vendors. Some of the challenges that face enterprises in adopting a virtualized networking architecture are:

- Most enterprises lack internal resources or knowledge of these new technologies. Except for very large enterprises with deep technical resources, most enterprises will be challenged to pursue a do-it-yourself (DIY) approach for deploying SD-WAN services.
- Despite early promises of quick deployment and plug-and-play potential for SD-WAN, experience with real deployments indicates integration challenges, especially as it relates to legacy environments. As with any integration project, the deployment has to progress through a full cycle of planning, design, proof of concept, pilots, and live cutover.
- The management of a software-defined architecture is substantially different from the management of standalone network elements. A virtualization layer separates the overlay from underlay, introducing complexities related to configurations, monitoring, fault management, and security.
- Hosting multivendor virtual functions, a key benefit of a software-defined architecture, introduces risks related to interoperability and security vulnerabilities.
- For multilocation and multinational enterprises, managing an underlay provided by several last mile providers will introduce technical as well as commercial complexities. Deciding on who owns the SLA and managing problem resolution can challenge the best-equipped IT departments.
- Deciding on a security strategy that spans connectivity and applications and guards against external and internal threats can be complex but critical in today's environment.

This document explains how these challenges are best handled by choosing a managed services provider with deep experience in deploying and managing software-defined and virtualized networking services.

SHIFT TO VIRTUALIZED NETWORK SERVICES IS ACCELERATING

Virtualized network services are the new paradigm in networking, driven by a desire to create a cost-effective increase in network capacity and implement a cloud-based commercial framework. The architectural underpinning is based on separation of software functionality (e.g., virtual network function [VNF]) from the underlying hardware. As such, the economic model transforms from reliance on discrete hardware appliances toward a software-based functionality. Hardware-based appliances do not scale as easily as software and are not portable. VNFs, on the other hand, can be hosted anywhere — spanning datacenter, aggregation point, provider edge, and customer premise. In addition, multivendor VNFs can be hosted on a common commercial hardware.

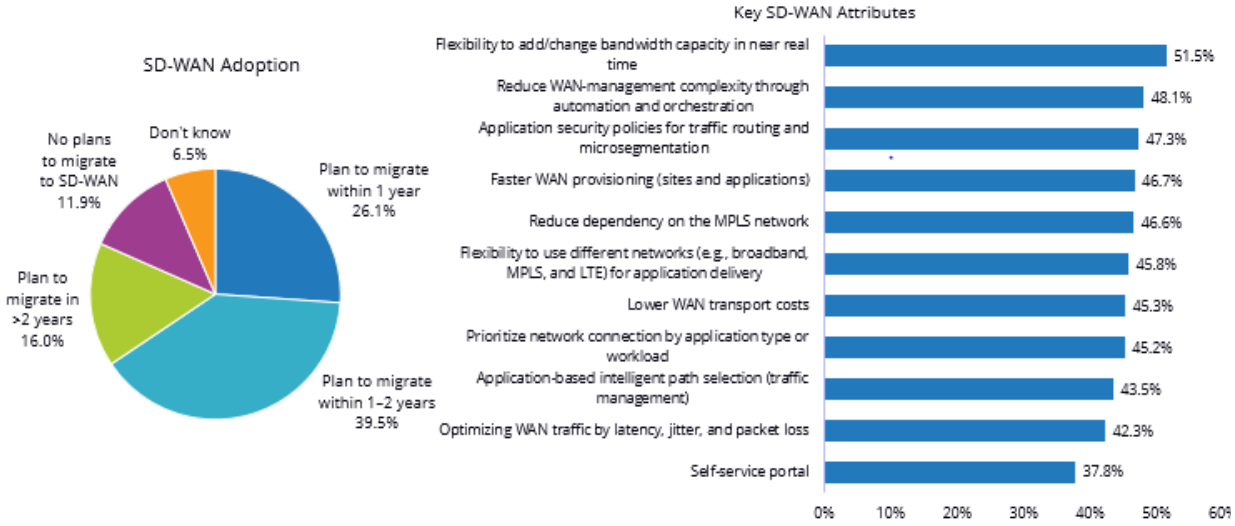
SD-WAN is one of the most prevalent use cases of this emerging software-defined and virtualized networking architecture. It is gaining strong momentum as indicated by various enterprise surveys. SD-WAN has emerged as the new architecture that enhances secure connectivity to the cloud, supports multi-connectivity options, and simplifies customer experience across various deployment modes. SD-WAN enables enterprises to deliver an automated, application-optimized, and integrated hybrid WAN. It presents a solution to the rapid shift in application and WAN traffic characteristics and an opportunity to rationalize network costs in the face of rapidly growing data traffic. SD-WAN addresses the limitations of traditional enterprise WANs in areas such as support for cloud applications (SaaS and IaaS), simplified deployment and management, cost-effective bandwidth utilization, greater overall WAN flexibility and efficiency, and improved WAN security. The provision of multiple connectivity options, including cellular in an active/active configuration, improves network availability — a key contributor to business continuity.

Considering these benefits, it is no wonder that SD-WAN adoption continues to rise in the enterprise market. IDC's 2018 *U.S. Enterprise Communications Survey* of 800 global enterprises indicated that 66% of those enterprises plan to adopt SD-WAN technology over the next two years (see Figure 1).

FIGURE 1

SD-WAN Adoption and Key Consideration Factors

Q. Do you plan to migrate any of your existing WAN/network connections to an SD-WAN alternative? Which of the following attributes of an SD-WAN service/solution are the most important considerations when choosing an SD-WAN solution for branch office connectivity?



SD-WAN adoption is accelerating as 66% of enterprises plan to migrate to SD-WAN within two years. Flexibility to change bandwidth in real time is a key consideration for SD-WAN, followed by reducing WAN complexity and improved application security.

n = 800 for pie chart, n = 653 for bar chart

Base for bar chart = organization plans to migrate existing WAN/network connections to SD-WAN

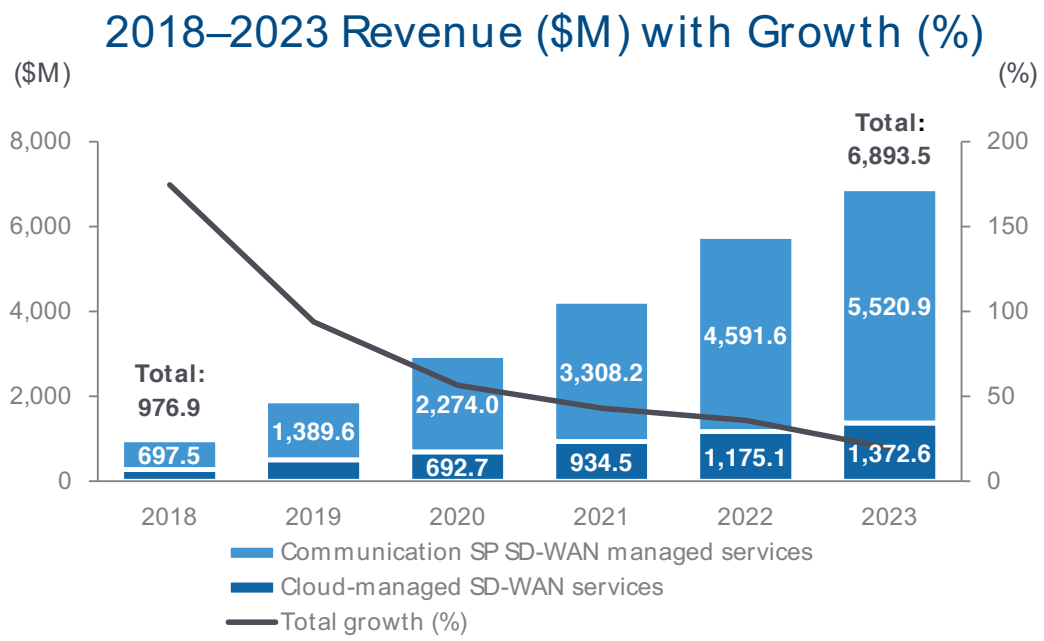
Note: For additional information, see (IDC #US44793119, September 2019) and *U.S. Enterprise Survey, 2018: SD-WAN Uptake* (IDC #US44751118, January 2019).

Source: *U.S. Enterprise Communications Survey,* 2018

IDC's 2019 SD-WAN managed services forecast projects an overall 47.8% CAGR for the period 2018-2023 (see Figure 2). The communication service provider SD-WAN segment is expected to grow at a faster pace (51.2%) than the cloud-managed WAN services segment (37.5%) during this period.

FIGURE 2

Worldwide SD-WAN Managed Services Revenue Snapshot



Selected Segment Growth Rate

- ▲ Communication SP SD-WAN managed services CAGR 51.2%
- ▲ Cloud-managed SD-WAN services CAGR 37.5%

Total Market CAGR

47.8%

Notes:

Chart legend should be read starting with the top row.

For more details, see *Worldwide SD-WAN Managed Services Forecast, 2019-2023* (IDC #US44050619, May 2019).

Source: IDC, 2019

The adoption of software-defined networking brings about many benefits but also entails a set of challenges. In IDC's 2019 *U.S. Enterprise Communications Survey,* enterprises' top 3 considerations for deciding on SD-WAN are flexibility to change bandwidth in real time, reducing WAN complexity, and improved application security. These considerations have proven to be critical in the era of the new pandemic and unpredictable economic time. Enterprises were forced to shift toward remote working, reliance on secure VPN connectivity for branch locations, and increasing dependency on cloud applications to conduct ecommerce. SD-WAN has proven to be resilient as it was architected with these working assumptions: direct and secure cloud connectivity, increased bandwidth, and high availability. The topic of business continuity is important with the shift of work toward a distributed edge environment versus centralized datacenters with built-in redundancy. A key tenet of SD-WAN is hybrid connectivity, configured with active/active communication links and backed up by 5G/4G/LTE mobile access. This configuration has allowed some managed services providers to advertise 100% availability as a key feature of their managed services offer.

The adoption of virtualized network services brings about challenges primarily related to lack of skills and resources to handle the shift to this new architecture. This is further compounded with the need to manage diverse underlays distributed across multiple geographies. This can be technically and commercially challenging for most enterprises. As this document argues later, the choice of a managed services provider becomes a critical decision point in the adoption of virtualized network services. Service providers have embraced this new architecture as a strategic initiative, backed by significant R&D funding, and have rolled out multivendor SD-WAN services to support the various enterprise segments they serve. A managed services provider should be viewed as the strategic partner of choice for deploying and managing a virtualized network services environment.

Simplified Self-Service Portal Enhances Management Experience

A key capability of a software-defined and virtualized networking offering is the self-service portal. The self-service portal was designed to mitigate the limitations of today's management portals that rely on cryptic CLI commands to manage configurations of the networking infrastructure.

A well-designed self-service portal should be vendor agnostic, provide end-to-end visibility, manage third-party components, aggregate underlay and overlay monitoring, and support a holistic security approach. The self-service portal is a key component of an orchestration strategy that provides optimal allocation of VNFs and integrates AI/ML technologies to provide predictive monitoring and facilitate configuration automation.

Early experiences with self-service portals have received positive feedback from customers. The primary usage was mostly limited to reporting and monitoring of events. Configuration management was generally left to the managed services provider because of concern among enterprises of comprising the network. We expect more enterprises to take responsibility for configuring end-to-end services as service providers are integrating advanced configuration tools enhanced with AI/ML to limit exposure to adverse configurations. A self-service portal will also support the evolution toward intent-based networking, further streamlining end-to-end management.

Self-service portals will provide enterprises with a powerful toolkit that goes beyond configuration and monitoring toward an enriched customer experience. The real-time reporting and analysis of usage provide invaluable data that can be leveraged to enrich the customer experience.

SECURITY IS FOUNDATIONAL TO MANAGED SERVICES

As enterprises look to managed services to help address technical and organizational challenges associated with effectively managing their IT architecture, the ability to address cybersecurity concerns at every layer of the IT stack has become foundational. Cybersecurity is a business imperative, and it is forcing enterprise security teams to develop a comprehensive strategy for minimizing the impact of cyberthreats to corporate assets, data, and employees. However, the challenges associated with the ongoing management of cybersecurity operations have opened opportunities for managed services to play a key role in an enterprise's security strategy.

Managing an enterprise's security posture and mitigating technical and business risk continue to be top of mind concerns for corporate executives. IDC estimated that in 2019, organizations worldwide spent nearly $50 billion in professional and managed security services to help minimize cybersecurity risk. Enterprises are devoting more attention, and resources, to not only put the proper security strategy and security controls in place to prevent attacks but also establish operating procedures for effectively responding to and remediating an evolving array of security threats.

The task of managing security has always been costly and complex, but it has been made even more difficult by enterprise digital transformation initiatives. The shift to a more digitally connected business model that has cloud at the core of the IT architecture has created a broader attack surface with new threat vectors, which in turn has created the need for increased investment additional security controls and personnel to operate and manage these tools. This has compounded an already difficult situation for enterprises that must take into consideration a number of issues as they look to optimize the efficiency of their security operations. These issues include:

- The need for skilled security resources
- Technical complexity of the tools required to manage security operations
- The budget needed for staff and technology to defend against attacks

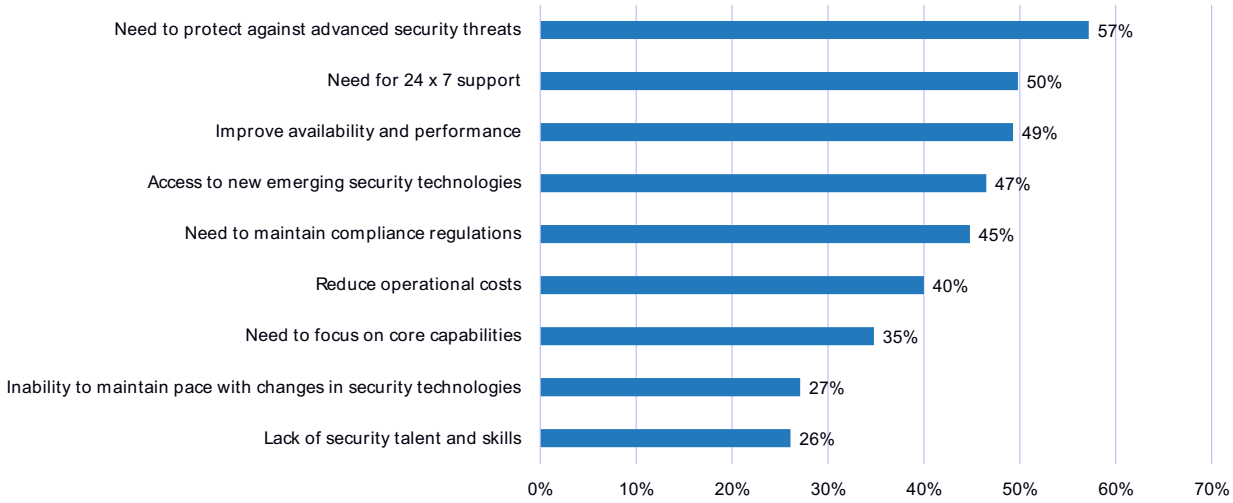
All these elements must be balanced against the need to ensure that security threats do not compromise business goals and objectives. For this reason, the decision to manage security operations in-house versus outsourcing the task is a key consideration. IDC has seen a significant shift in preference on the part of enterprises that are increasingly choosing to outsource security operations to a managed security service provider. In a recent survey of 400 U.S. enterprises, respondents were asked to rank the reasons for choosing to outsource their security operations for a managed security service provider (see Figure 3).

As Figure 3 depicts, the threat landscape has become more advanced with well-organized attackers using leading-edge technologies to launch their attacks. This has resulted in the need to have "eyes on glass" at all times monitoring the environment to accelerate the time to detect a breach. In addition, the costs associated with a security breach continue to rise every year, and the impact on organizations that suffer a breach can be felt on the financial and reputational sides of the business. For this reason, maintaining availability and performance is paramount for enterprises.

FIGURE 3

Top Reasons for Using a Managed Security Service Provider

Q. What are your organization's top reasons for using a managed security service provider?



n = 402

Source: IDC's *Managed Security Services Survey,* January 2019

KEY DRIVERS FOR MANAGED SECURITY SERVICES

IDC believes that there are a number of reasons for the shift to managed services, but the factors that are driving it center around complexity, cost, and people skills. Some of the key drivers for managed security services are highlighted in the sections that follow.

The Evolving Cybersecurity Threat Landscape

There is no doubt that the investments made by enterprises to improve their security posture are compromised by the increasing sophistication and ever-advancing capabilities of adversaries. Organizations have a myriad of highly motivated and well-funded adversaries that are now using advanced technologies and tools to exploit vulnerabilities, which has resulted in an increase in the volume of attacks. In addition to known threats, organizations are dealing with an increase in the number of unknown threats as attackers are finding new ways to circumvent the technologies that were designed to thwart their attacks.

Moreover, as enterprises rethink their IT architecture as part of their transformation initiatives, deploying new technologies, migrating to cloud, and integrating business processes with suppliers, partners and customers have created a much wider attack surface for adversaries to utilize and exploit vulnerabilities.

Lack of Skilled Security Expertise

Organizations have found it difficult to build an effective internal organization to manage their security posture, largely because of the lack of in-house security expertise. Companies looking to build the requisite capabilities in-house can also find it challenging because of the cost of hiring in-house staff with expertise across a range of potential security threats. Even though the number of security professionals continues to grow, at an industry level, there is still a talent shortage for qualified security professionals. This puts compensation for security professionals with deep experience at a premium price level. For organizations, the challenge to find security experts can be both a budgetary issue and a human resource issue.

Perimeter-less Enterprise

Protecting corporate resources has become very difficult for enterprises given the widespread adoption of multicloud architectures; the proliferation of end devices that include PCs, laptops, smartphones, and increasingly IoT devices; and the anytime, anywhere access that these devices have to corporate resources. As workloads move to and from the cloud, enterprises can no longer rely on existing methods of network security that were based on protecting assets in a defined network perimeter.

Organizations instituting bring-your-own-device (BYOD) programs have added to the complexity by introducing unmanaged devices that can potentially expose an organization to theft of sensitive data or password theft. As the adoption of IoT increases, the challenge for enterprises will be even greater with sensors being placed on a variety of "things" that will be connected to the network.

Compliance Mandates

Regulatory compliance for data protection and privacy from various vertical industry regulatory agencies, as well as from multiple governmental bodies, continues to expand and create complexity for organizations putting controls in place. This has placed additional strain on organizations as they monitor adherence to mandates such as General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

Evolution of Managed Security Services

In response to the security challenge organizations are facing, there is currently a shift in the security services market toward a new approach to threat detection and response. Using a combination of artificial intelligence, analytics, automation, and orchestration, managed security service providers can adopt a proactive posture when responding to security threats by augmenting human analyst efforts to achieve faster detection and response. IDC believes that enterprises are placing higher value on managed security service providers that possess expertise with advanced technologies such as machine learning, analytics, and automated orchestration that are used to accelerate threat detection, response, and remediation. These are technologies that many enterprises are struggling to implement because of their lack of in-house expertise; however, the use of these technologies by managed security service providers has become a top-of-mind consideration for enterprises when they evaluate managed security service providers.

IDC believes that managed security services will continue to play a key role in helping enterprises defend against cyberattacks. The complexity of the threat landscape will continue to rise, and the ability of enterprises to keep pace will become more costly and difficult because of the dearth of security expertise. Transferring the cost of ownership for security operations to a third-party managed security service provider that has broad security skills and expertise in advanced technologies will prove valuable for enterprises and their cyber-defense operations.

MANAGED SERVICES DRIVE BENEFITS BEYOND COST OPTIMIZATION

IDC's *U.S. Enterprise Communications Survey* confirms the increased adoption of managed network services. Enterprises with more than 5,000 employees remain the most enthusiastic adopters of managed network services, further indication of the growing scale and complexity challenges of distributed networks.

The top drivers of investment in legacy managed network services are cost reduction, refocusing IT staff, and gaining access to skills. The new era of software-defined and virtualized network services extends the motivations to deploy these managed services beyond cost. This new architecture has been shown to bring significant technical benefits as a result of the move toward an agile software architecture. The full benefits of this new architecture can be realized only with a complementary commercial framework as follows:

- **The ability to provide a single SLA that integrates multiple SLAs pertaining to several underlay network providers.** Multilocation and multinational enterprises will be key beneficiaries of this common SLA framework as it reduces contractual and operational risks.
- **The flexibility to deploy VNFs across multiple deployment models spanning the CPE, provider edge, centralized datacenter, or cloud hosted.** Most service providers allow for hybrid hosting models, deployed in strategically located points of presence (POPs). These flexible deployment models will optimize opex and reduce overall TCO.
- **The support of a cloud consumption model based on monthly recurring charges.** The pricing model can be optimized to match the needs of the branch based on criteria such as branch size and bandwidth requirements.
- **The provision of bandwidth on demand in real time.** This is a critical capability that most global service providers offer to help address the varying needs of bandwidth and ability to configure in real time from a self-service portal.
- **The choice of fully managed services model (i.e., fully outsourced model) or co-management.** Depending on the size and technical capabilities of the enterprise, these options are tailored to provide cost-effective models for network management.
- **The ability to host multivendor VNFs that have been certified by the service provider.** This rationalizes the sprawl of standalone appliances that historically provided a range of networking functionality including routing, security, and WAN acceleration. Hosting these functionalities on a common uCPE appliance simplifies the management and interoperability of these functions. As an added benefit, it sets the stage for integrating other third-party networking and IT functions.
- **The availability of an orchestrator that simplifies configuration management and potentially drives a richer customer experience with real-time analytics, especially when enhanced with AI/ML technology.** This is a key investment area for major service providers in collaboration with technology vendors as they strive to achieve the goal of a fully automated network.
- **The ability to scale globally.** This is an important decision criterion for enterprises that operate in distributed locations and are keen on common management of the distributed underlying network.

In summary, the motivation for managed network services extends beyond cost optimization, especially in the new era of software-defined and virtualized network services. The benefits that accrue from integrating this new paradigm align well with the motivation to transform to a digital-native enterprise. These types of benefits are important to realize, especially during an economic downturn.

ESSENTIAL GUIDANCE

Market developments have made the decision to implement a software-defined WAN a strategic imperative for enterprises. IT decision makers face important decisions in embarking on this transformation journey and ensuring successful implementation. The following guidelines may help them navigate through these decision choices:

- The risk of not implementing a software-defined architecture far outweighs the implementation risks. Software-defined WAN enables enterprises to be agile and respond quickly to unforeseen circumstances such as a pandemic.
- Managed network services provide considerable benefits as they alleviate key challenges related to the adoption of new technology. These include lack of skilled resources, ability to onboard third-party solutions, and dealing with integration issues.
- An experienced managed network services provider brings about important commercial benefits that a do-it-yourself approach lacks. Cloud-based pricing model, uniform SLA framework, single pane of glass for managing and monitoring the network, and extensive agreements with last mile internet service providers are some of the key benefits.
- As the security threat landscape evolves, and defense against cyberattacks becomes more challenging for security operations teams, enterprises should look to the advanced detection capabilities that many managed security providers now offer.
- Adoption of managed security services will prove to be a valuable strategy for optimizing existing investments in people and security tools as enterprises seek to address today's security challenges with limited budgets and limited skilled security resources.
- As cloud replaces the on-premises datacenter as the core of an enterprise's IT infrastructure, networking strategies for connectivity to cloud resources are evolving. Managed network service providers are key enablers of this connectivity shift, and IT decision makers should ensure that a robust plan for network security is embedded into the managed network services providers' offerings.
- IT decision makers should work with a managed network services provider that has the vision and road map to achieve the goal of full network automation underpinned by AI and ML technologies.

About IDC

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

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com