ISG Provider Lens™ Quadrant Report | June 2019

About this Report

Information Services Group, Inc. is solely responsible for the content of this report.

Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by and are the sole property of Information Services Group, Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that was current as of June, 2019. ISG recognizes that many mergers and acquisitions have taken place since that time but those changes are not reflected in this report.

The lead author for this report is Dr. Kenn Walters. The editor is Ambrosia and Grant. The research analyst is Dr. Kenn Walters and the data analyst is Bhanwar Chauhan.
EXECUTIVE SUMMARY

Existing managed LAN and WAN services, multiprotocol label switching (MPLS) and related technologies form the backbone of the enterprise customer installed base for telcos and other communication services providers and account for most of the revenues generated worldwide. This trend, however, is rapidly changing. The software-defined network (SDN), which is closely related to network function virtualization (NFV) and software-defined WAN (SD-WAN) technologies and services, is evolving and rapidly penetrating the market. A similar trend exists with related network services such as performance assurance (management), managed networks and devices (MND), and 4G and 5G mobility (4G/5G) with associated additional (non-core) mobile services based on those faster mobile data stream standards, along with their triggers and influences. The main factors that drive this rapid change for enterprises are:

**Increasing flexibility and agility:** Enterprises have become more focused on improving the integration, automation, orchestration and management of network resources and processes. This has evolved to encompass NFV and has since led onto software-defined networking in a wider sense. This trend is being driven by enterprises’ desire to seamlessly add applications and network resources in order to meet business and user goals more efficiently and securely without creating silos or depending on vendors. This is often expressed by the business itself as “increasing flexibility and agility.”

**Improving customer satisfaction while boosting sales:** The ability to respond quickly and seamlessly to customer queries and quickly provide (often automatically) new services via SDN helps in elevating client experience and boosting sales.

**Reducing costs and improving usage efficiency:** Enterprises can improve the utilization efficiency while reducing network usage costs even beyond the savings achieved by adopting an NFV strategy. This is particularly relevant with the explosion of data usage in mobile devices, often in areas that are not business critical, and while using social media applications or other related services. Traffic can be routed over lower cost connections and at reduced reliability and quality levels automatically via software-defined pathways with little or no human interaction involved.

The aforementioned factors, together with cloud networks, have been driving significant changes to networks and their operations over the past 30 years. Some telecommunication service providers, such as AT&T, have announced plans to make at least 75 percent of their networks SDN-compliant and functional by 2022. Others have introduced SD-WAN implementations to reap benefits in a shorter term. Many service providers that are reviewed in this study are involved in pilot projects and are regularly converting them into production-level deployments. Some have already completed such activities or have many demonstrated instances of doing so on behalf of their clients. This progression, coupled with the relative newness of SDN, has led ISG to expect that many of the companies that are currently categorized as Product Challengers or Market Challengers in this study will be able to improve their positioning over the course of the year to enter leadership positions in their respective segments.
It must be noted that significant volatility exists in the constellation of market providers, partly due to the multitude of mergers and acquisitions that occurred during the last 18 months. This trend is set to continue and may even increase during the remainder of 2019 as SDN becomes mainstream.
**Introduction**

The ISG Provider Lens™ study examines the different kinds of global network offerings related to SDN, SD-WAN and associated security, core-branch and mobility service offerings related to those segments. It also assesses the more traditional managed WAN market offerings. For users, both markets are extremely important. This study accounts for changing market requirements and provides a consistent market overview of the segments. It also offers concrete decision-making support to help user organizations to evaluate and assess the offerings and performance of service providers.

The areas described in the following sections are associated with SDN and more traditional managed WAN provisioning.

---

### Simplified Illustration

<table>
<thead>
<tr>
<th>Network - Software Defined Solutions and Services</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managed WAN - Services</strong></td>
<td>The ISG Provider Lens™ study examines the different kinds of global network offerings related to SDN, SD-WAN and associated security, core-branch and mobility service offerings related to those segments. It also assesses the more traditional managed WAN market offerings. For users, both markets are extremely important. This study accounts for changing market requirements and provides a consistent market overview of the segments. It also offers concrete decision-making support to help user organizations to evaluate and assess the offerings and performance of service providers. The areas described in the following sections are associated with SDN and more traditional managed WAN provisioning.</td>
</tr>
<tr>
<td><strong>SDN Transformation Services (Consulting &amp; Implementation)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SDN Security Services</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SD Network Technologies (Mobile to edge)</strong></td>
<td></td>
</tr>
</tbody>
</table>

* section not included in this excerpt

Source: ISG 2019
Definition (cont.)

Scope of the Report

Managed WAN Services

Managed WAN services cover the features and functionality that carriers offer in their WAN and at the customer point of demarcation. They are a collection of value-added services (VAS) that offer monitoring and reporting, security and outsourced customer-premises equipment (CPE) functions. Many enterprises see managed WAN services as a way to outsource IT functions and purchase them along with consulting and professional services to assess, design and implement their enterprise networks. At the basic level, the managed WAN services offered by carriers provide monitoring and alerts for critical problems such as network outages. Higher tiers of service can add configuration management, proactive troubleshooting and trouble resolution, service-level agreement (SLA) management, more sophisticated and granular monitoring and reporting, on-the ground CPE installation and hardware support to ensure that CPE software is up to date and configured correctly, and the overall lifecycle management. This section should cover all the major suppliers of managed WAN services for enterprises.

Mobile Network (4G/5G) Additional (non-core) Services*

Fifth generation (5G) mobile networks and wireless systems are the next telecommunication standards after the current long-term-evolution (LTE) or 4G technology, operating in the millimeter wave bands (28, 38, and 60 GHz). 5G is aimed at a higher capacity than the current 4G, which would allow for an increased density of mobile broadband users and support more device-to-device, reliable and massive machine communications. It is also aimed at lowering latency and battery consumption compared to 4G equipment and is targeted at the internet of things (IoT). This segment covers specific mobility-targeted services or solutions, applications, management systems and methods, end-device control and management and related services. These services are either offered by service providers or suppliers as discrete solutions or as modules that will integrate with or are reliant on SDN or SD-WAN.

This section should cover all the suppliers of these additional services that make use of software-defined systems via LTE/4G or 5G delivery. It does not cover the core licensed mobile telephony/data services themselves.

* section not included in this excerpt
Definition (cont.)

SDN Transformation Services (Consulting & Implementation)

SDN and SD-WAN provides the benefits of SDN technology to traditional hardware-based networking and is considered complementary to NFV. It is an overlay architecture with a networking foundation that is much easier to manage than legacy WANs. It essentially moves the control layer to the cloud and in the process, centralizes and simplifies network management. This overlay design abstracts software from hardware, enabling network virtualization and making the network more elastic. SD-WAN architecture reduces recurring network costs, offers network-wide control and visibility, and simplifies the technology with zero-touch deployment and centralized management. The key aspect of the SD-WAN architecture is its ability to communicate with all network endpoints without the need for external mechanisms or additional protocols. Suppliers have been increasingly active as advisors/consultants as well as implementation enactors of managed services to supply complete solutions to enterprises. Consulting companies, large vendors and managed network services providers have been actively involved in offering SD-WAN as managed service packages in this space (independently or as part of partnership/consortium deals).

This quadrant should cover all the advisory/consulting, hardware and software, management/reporting tools, applications and services associated with delivering SD-WAN to enterprises, starting from consulting to managed services delivery.
SDN Security Services

An SD-WAN is a logical overlay network that encompasses any WAN transport — public, private, even LTE/4G or 5G, and is independent of any single carrier or service provider. The overlay occurs between any two SD-WAN nodes, called edges, which can be deployed at the branches and/or data centers. A cloud-delivered variation extends the overlay to any cloud point-of-presence (PoP) or data center. A key value in security services for the network is that SD-WAN unifies secure connectivity over all transports while supporting transport independence. There is no need to use/provide a different security mechanism for different transport types or to depend on the transport provider for their secure network. The network overlay can support a wide range of security capabilities and can enhance its inherent security capabilities by adding advanced security systems in the form of discrete overlays, services or applications. It can be managed both automatically and centrally as well as at local levels.

This section should cover all suppliers of software and/or hardware associated with additional and discrete security services based on SDN or SD-WAN systems.
SDN technologies enable improvements in network agility and automation and can substantially reduce the cost of network operations compared to traditional network deployments. The implementation of an industry-standard data plane abstraction protocol (such as OpenFlow) allows the use of any type and brand of data plane devices as all the underlying network hardware is addressable through a common abstraction protocol. It allows the dynamic and automatic provisioning of virtual network segments and virtual routing services on both physical and virtual networking devices. Security policies can be automatically provisioned via a cloud orchestration platform, such as OpenStack, or through workloads assigned according to attributes, such as MAC, subnet, VLAN and IP protocol, in an automated manner.

The main companies covered in this segment of this study will be vendors of SDN and NFV equipment and core services that are purchased either directly by enterprises or by service providers for specific enterprise projects.

* section not included in this excerpt
Definition (cont.)

Network Technologies Suppliers (Mobile to Edge)

SDN technologies enable improvements in network agility and automation and can substantially reduce the cost of network operations when compared to traditional network deployments. The implementation of an industry-standard data plane abstraction protocol, such as OpenFlow, allows the use of any type and brand of data plane devices as all the underlying network hardware is addressable through a common abstraction protocol. It also allows for the dynamic and automatic provisioning of virtual network segments and virtual routing services on both physical and virtual networking devices. All edge components may be managed in the same manner as core and SD-WAN components. With software-defined access out to branch/edge, including all customer premises equipment (CPE, referenced as virtual CPE or vCPE in SDN terms) and associated Wi-Fi networks, access points (APs), software-defined mobile networks (SDMN), and SD-LAN (includes both wireless [SD-WLAN] or mobile [SD-WMLAN], the management protocol can be further improved.

This segment assesses all the main vendors and service providers (such as telcos) in the SD-LAN space, including vCPE, SDMN and SD-LAN specific vendors.

In this independent study, following the format of the internationally successful Provider LensTM series, ISG sets out to deliver a comprehensive but defensible research program based on an extensive evaluation of criteria that cover all major telcos and service providers of relevance in the global, Germany, the Nordics, the U.K. and the U.S. regions.
Introduction

The ISG Provider Lens™ quadrants were created using an evaluation matrix containing four segments, where the providers are positioned accordingly.

Provider Classifications

Leader

The “leaders” among the vendors/providers have a highly attractive product and service offering and a very strong market and competitive position; they fulfill all requirements for successful market cultivation. They can be regarded as opinion leaders, providing strategic impulses to the market. They also ensure innovative strength and stability.

Product Challenger

The “product challengers” offer a product and service portfolio that provides an above-average coverage of corporate requirements, but are not able to provide the same resources and strengths as the leaders regarding the individual market cultivation categories. Often, this is due to the respective vendor’s size or their weak footprint within the respective target segment.

Market Challenger

“Market challengers” are also very competitive, but there is still significant portfolio potential and they clearly lag behind the “leaders.” Often, the market challengers are established vendors that are somewhat slow to address new trends, due to their size and company structure, and have therefore still some potential to optimize their portfolio and increase their attractiveness.

Contender

“Contenders” are still lacking mature products and services or sufficient depth and breadth of their offering, while also showing some strengths and improvement potentials in their market cultivation efforts. These vendors are often generalists or niche players.
Introduction

Rising Star

Rising stars are mostly product challengers with high future potential. When receiving the “rising stars” award, such companies have a promising portfolio, including the required roadmap and an adequate focus on key market trends and customer requirements. Also, the “rising stars” has an excellent management and understanding of the local market. This award is only given to vendors or service providers that have made extreme progress towards their goals within the last 12 months and are on a good way to reach the leader quadrant within the next 12-24 months, due to their above-average impact and innovative strength.

Not In

This service provider or vendor was not included in this quadrant as ISG could not obtain enough information to position them. This omission does not imply that the service provider or vendor does not provide this service.
Network - Software Defined Solutions and Services Quadrants
Managed WAN Services

Definition

Managed WAN services are increasingly described as traditional in light of the SD-WAN offensive globally. They cover the features and functionality that carriers offer in their network and at the customer point of demarcation. They are a collection of value-added services (VAS) that include monitoring and reporting, security and outsourced customer premise equipment (CPE) functions. Many enterprises choose managed WAN services to outsource IT functions and purchase them along with consulting and professional services to assess, design and implement their enterprise networks.

At the basic level, managed WAN services offer monitoring and alerts during critical problems such as network outages. They also include configuration management, proactive troubleshooting and trouble resolution, service-level agreement (SLA) management, on-the-ground equipment installation, hardware support and the overall lifecycle management.
Managed WAN services cover the scope of services and functionalities of various network solutions, including core solutions such as the MPLS protocol for IP-VPN services and multiple access technology. WAN services allow end customers to access resources for network operation centers (NOCs), disaster recovery, active fault clearance and customer portals.

Traditional managed WAN services, often based on MPLS, have come under increased pressure due to the growing prominence and prospects of SD-WAN which would continue over the next two years. MPLS is the most widely used WAN technology in companies with distributed locations and is being developed continuously. Today, it is possible to prioritize types of applications depending on their respective jitter, packet loss and deceleration to allow a performance boost in individual applications based on customer requirements or policies. While MPLS VPNs provide certain advantages in connecting locations, they are an expensive medium when it comes to connecting mobile devices, especially with the growth of traffic that is not business critical. Mobile usage is also exploding due to the internet of things (IoT), the growing mobile workforce and the addition of decentralized locations within enterprises. In addition, enterprises are demanding networks to provide more flexibility and business-oriented SLA metrics such as performance per application and quality of experience. Such demands are causing a strain and affecting the smooth functioning of traditional WAN services and managed services. These newer flexibility and metric requirements require a more flexible infrastructure compared to what MPLS networks provide, making SDN increasingly relevant.

ISG does not expect MPLS networks to be replaced by alternate software-driven networks any time soon. Instead, these networks would be increasingly complemented by SD-WAN technologies during 2019–2021.
MANAGED WAN SERVICES

Eligibility Criteria
- Product/service portfolio coverage, completeness and scope
- Ability to deliver and manage all hardware and software aspects
- Management capability for the orchestration and control of the overall architecture
- Stability and roadmap planning
- Reference customer/site volume in deployment
- Competitiveness of offerings and commercial terms

Observations
- **AT&T** has a vast array of business and technology streams in the networking space and has a large client base in managed WAN services. The company is also a leading proponent of SDN/SD-WAN, making it well positioned in migration programs.
- **BT** has a strong global backbone with a commitment to continue delivering traditional managed WAN services as well as SDN/SD-WAN services and managed services for its domestic and international client base.
- **CenturyLink** has capabilities to extend management into IT infrastructure and application management in three services tiers in a complementary manner for network management. It has been ranked consistently as one of the best-performing managed WAN companies on a global level.
- **IBM** has a strong portfolio of its own network, service and security solutions. It has also built a world-class partner ecosystem of major players in the managed network, SDN, SD-WAN, multi-cloud network and multi-network integration space. These assets, together with IBM's consulting and project management abilities, facilitate the delivery of a comprehensive, provider-agnostic solution for enterprises.
MANAGED WAN SERVICES

Observations (cont.)

- **Orange Business Services** covers a large area of managed network services. These include MPLS and SD-WAN and internet services, which can be integrated or combined with managed security, WAN optimization and application visibility services. They can be provided either on appliance or on virtual network functions (VNFs) as well as on various levels of service management. Orange Business Services also offers multi-sourcing integration (MSI) as a service.

- **Tech Mahindra** is globally known for its managed WAN and SD-WAN offerings at competitive price points with advanced service delivery. The company leverages its experience in traditional WAN services and SD-WAN transition programs to develop a strong portfolio of off-the-shelf framework offerings. It also has a strong consulting-led practice focused on customizing offerings to address the needs of each client.

- **T-Systems** provides high-quality services throughout Europe and many other international markets. It covers over 180,000 sites with more than 2,500 networks, delivering a four-fold redundancy at a platform level. The firm offers high-quality secure solutions that are custom packaged for specific industry verticals and enterprises.

- **Wipro**'s managed network services are consulting led, covering both off-the-shelf and highly tailored client-specific solutions. These include Wipro Digital's Designit, ITIL integrated service platforms, governance via Wipro SmartView, Cloud Trust Security framework, Wipro HOLMESTM RPA/AI methods and toolsets and Wipro WANTAGE. It also offers partner solutions and products from companies such as Riverbed and Cisco.

- **Rising Star Logicalis** has an extensive portfolio of managed and hosted managed services that encompass the end-to-end management of multi-vendor, multi-technology ICT environments. It enables customers to take a flexible approach to IT operations and major transformation projects that are available on a global basis.
**CenturyLink**

**Overview**

CenturyLink has been ranked consistently as one of the top-performing managed WAN companies globally. It has a string of acquired companies such as Qwest, Time Warner Telecom, Global Crossing and Level 3. In the past year, the company has made various announcements on ethernet, ethernet-LAN, SD-WAN, wavelengths, security services, unified communications and collaborations (UCC) services VPN, VoIP and other internet applications, including access extensions. It has a wide infrastructure network in more than 60 countries, served by a staff of 47,000, along with an extensive partner network.

**Strengths**

**Network management:** CenturyLink offers three service sets with design and implementation for different levels of WAN management depending on the depth and skill set required. Managed services provide 24/7 monitoring throughout the year. Advanced managed services allocate a dedicated resource to monitor, manage and remediate contracted fault and performance criteria. Customer managed services offer a fully outsourced network management solution.

**IT and data center management:** CenturyLink uses three service tiers of network management to extend into IT infrastructure and application management in a complementary manner.

**Client and end-customer centric:** The company has implemented a slew of new tools and methods to enhance customer experience for clients and end users. It incorporates artificial intelligence, fault and engineering fix information, order and remedial management, and billing and usage systems.

**Caution**

CenturyLink has a strong foothold in Europe and the Americas but lacks a deep presence in APAC and Africa. The company has been investing heavily to improve its position and gain strong client references over the next two years.

Despite its significant experience in acquisitions, CenturyLink faces some risk in its expansion plans and absorption capabilities while penetrating the markets in APAC and Africa.
Traditionally, modifications or new installations of IT devices in a data center and its external WAN networks involved making changes to each network component, which could take days or longer. This traditional, rigid architecture has been increasingly challenged by today’s business requirements for more agility, flexibility, automation and security enhancements. Private, public and hybrid cloud computing, explosive mobile application usage in the workplace, internet of things (IoT), Industry 4.0, big data and infrastructure as a service (or XaaS) now require a flexible network environment that can adapt to changes quickly and with minimum human intervention.

SDN and NFV are making strides towards responding to some of these issues using network abstraction. SDN and NFV differ in how they separate functions and abstract resources. SDN abstracts physical networking resources (switches, routers, etc.) and moves the decision-making process to a virtual network control plane that would determine where to send traffic, while the hardware continues to direct and handle the traffic. It uses an open source protocol, such as OpenFlow, to enhance/enable this. NFV is aimed at virtualizing all physical network resources beneath a hypervisor, which allows the network to
Definition (cont.)

SDN architecture separates the control plane from the data plane and introduces several layers that are managed by software-defined policies and rule-based controls and management. The network elements are configured, administrated and controlled centrally by a separate software-based SDN controller or multiple SDN controllers. The data transport path and routing, including the quality of service level, bandwidth assignment, provisioning and modification of switches and hubs and their rules, are performed automatically. Overall security is maintained from the edge to the data center. Based on the centralized network infrastructure management and the open architecture provided by SDN product vendors, it is also possible to use SDN-enabled third-party switches, including white box switches at low price points (also used in hyperscale data centers). These switches help reduce costs and vendor lock-in risks. Applications and new network services can be provisioned rapidly on a management platform, which are all converged into a single-pane-of-glass type dashboard. This platform often combines a view of all network tasks and incidents plus all the applications and programs that are running. The controller provides a complete overview of applications, network components and data throughput rates; problems are detected and resolved quickly.

SD-WAN provides the benefits of SDN technology to traditionally hardware-based networking. It is an overlay architecture with a networking foundation that is much easier to manage than legacy WANs. It essentially moves the control layer to the cloud and, in the process, centralizes and simplifies network management. This overlay design abstracts software from hardware, enabling network virtualization and making the network more elastic. SD-WAN architecture reduces recurring network costs, offers network-wide control and visibility, and simplifies the technology with zero-touch deployment and centralized management. The key aspect of this architecture is its ability to communicate with all network endpoints without the need for external mechanisms or additional protocols.
Advisory and consulting companies have been highly active in assisting enterprises in the transition from traditional networking to NFV/SDN and SD-WAN. They are also increasingly engaged in project management, implementation assistance, or as the “front end” of partnering with vendors or consortiums related to implementation. Managed SD-WAN suppliers have been increasingly active as both managed network services providers (MNS) and as suppliers of complete and partial solutions to other traditional MNS companies. MNS providers have been aggressively marketing complete SD-WAN solutions as managed services packages to enterprises as replacements or alternatives to traditional managed WAN solutions. SD-WAN is expected to see a high uptake by enterprises that are seeking a managed service alternative to their WANs, with aggressive growth in both pan-European and Asia Pacific regions during 2019-21.

Eligibility Criteria

- Product/service portfolio coverage, completeness and scope
- Ability to deliver in consulting and implementational areas
- Understanding of overall market and contributions to it
- Scope of partnerships and offerings; management capability for the needed orchestration within a customer project
- Stability and roadmap planning of the provider
- Reference customer/solutions in post pilot/commercial deployment
- Competitiveness of offering and types of commercial terms
SDN TRANSFORMATION SERVICES
(CONSULTING & IMPLEMENTATION)

Observations

- **AT&T** has a vast array of business and technology streams in the networking space. It was early in realizing the potential benefits of SDN and SD-WAN, with its internal and external proofs of concept (POCs) taking place ahead of most of the other providers. The company has converted many of its POCs into commercial deployments, enabling it to issue dividends.

- **CenturyLink** has been ranked consistently as one of the top performing networking companies on the global stage. Its 2019 organization format, Adaptive Networking and IT Solutions, which include networking, hybrid cloud and IT solutions, security, voice and unified communications, and managed services & IT consulting business units, is an impressive new line-up fully supported by products and services.

- **IBM** has been at the forefront of enterprise network and digital transformation for some time. Its managed service offerings are provided by IBM Global Technology Services (GTS), with additional focus from its telecom and media and entertainment divisions. IBM has an extremely strong portfolio of its own solutions along with a vast and well-qualified partner ecosystem that includes leading players. This enables the firm to deliver comprehensive, provider-agnostic solutions for enterprises, locally and globally.

- **Juniper** is a highly respected and well-known network equipment and solutions provider for many carriers internationally. It was an early proponent of NFV/SDN and SD-WAN. Juniper’s Contrail SD-WAN solutions, which can be bought or licensed, cover end-to-end software-defined delivery from the customer premises equipment (CPE) to the cloud or service provider. Juniper offers full orchestration and in-built security and also covers MPLS, broadband internet and 4G/ LTE transport paths.

- **Orange Business Services** is primarily focused on providing consulting services to ensure client requirements are met. Its SDN offerings include Flexible SD-WAN with full multi-network compatibility that is ensured through virtual SD-WAN gateways globally.

- **Tech Mahindra** has innovative and robust solutions and products, coupled with the best-of-breed solutions from partners such as AT&T FlexWareSM, Silver Peak and Rakuten, which allows it to deliver optimized solutions from its SD portfolio.
Observations (cont.)

- **T-Systems** has an SD portfolio that is vast in coverage and deep in scope. It includes integrated SD-WAN, (managed end-to-end SD-WAN), managed overlay (SD-WAN selection dependent upon technology), IntraSelect SD-WAN (Cisco/Viptela solutions), and managed services (based on Riverbed, Silver Peak or Citrix). T-Systems offers custom and packaged solutions to specific industry verticals along with enterprise-wide packages in the SDN space. It covers end-to-end enterprise deployments and offers enhanced security through its Magenta Security portfolio.

- **Verizon** has a very large and comprehensive portfolio of SDN products and services such as virtual network services, Intelligence Edge, SDN 2.0, CX platform and business outcomes. These cover many areas such as artificial intelligence (AI), orchestration, 4G/5G, SD-WLAN, containerization, bring your own switch (BYOS), SD-LAN/SD-WAN integration and multi-vendor/multi-cloud.

- **Wipro’s** SD network services portfolio falls under its “connected future” practice and includes data center networks, WAN, SD-WAN and SDN/NFV areas, utilizing Swift SDN and WANFreedom. The company offers consulting-led delivery of both off-the-shelf solutions and highly tailored client-specific solutions. Delivery is supported throughout the operational deployment and is managed by a vast array of toolsets, products and processes.

- **Apcela** is continuing its impressive transformation into an enterprise-centric provider of deterministic networking services, aligning enterprise application and network performance requirements. The firm has network as a service (NaaS)-oriented products that are based on its AppHUB platform. It also offers low latency with high frequency SD-WAN as a service based on its modular Alpha platform.
CenturyLink has an extensive portfolio, robust infrastructure, vast partner ecosystem and competent consulting unit, which are important aspects for a provider to maintain its position on the global stage.

CenturyLink has a strong foothold in Europe and the Americas, but it lacks a deep presence in APAC and Africa. The firm is aiming to achieve a truly global position with strong client references in all regions by 2020.

CenturionLink has been ranked consistently as one of the top-performing networking companies globally. Its 2019 organization format, Adaptive Networking and IT Solutions, has an impressive new line-up of fully supported products and services that cover networking, hybrid cloud and IT solutions, security, voice and unified communications, managed services, and IT consulting business units. With an extensive combination of its own portfolio assets, recent portfolio announcements, own infrastructure network and partner network of products, infrastructure and services, CenturyLink has a solid set of offerings for clients.

Reach and scale: CenturyLink offers a full range of MPLS-VPN, hybrid WAN, ethernet, wavelength and broadband connectivity, public and private cloud connections. Its combined network reach and scale position it as a strong service provider on the global stage.

Breadth of offering in SD and beyond: CenturyLink has a range of offerings that cover network business units, SD-WAN, managed enterprise networks, Cisco Meraki, content services, managed services and IT consulting, making it a solid and dependable provider in the SD space. The company is extending its service offerings to other business units, which its consulting group takes into account. This makes it a one-stop shop for all current and future enterprise network needs.

Deep industry verticals know-how: CenturyLink has examples of numerous implementations and case studies of significant players from different industries such as manufacturing, precision engineering, food and beverage, and medical/recycling.

The company has an extensive portfolio, robust infrastructure, vast partner ecosystem and competent consulting unit, which are important aspects for a provider to maintain its position on the global stage.
An SD-WAN is a logical overlay network that encompasses any WAN transport — public, private, even LTE/4G or 5G, and is independent of any single carrier or service provider. The overlay occurs between any two SD-WAN nodes, called edges, which can be deployed at the branches and/or data centers. A cloud-delivered variation extends the overlay to any cloud point-of-presence (PoP) or data center. A key value in security services for the network is that SD-WAN unifies secure connectivity over all transports while supporting transport independence. There is no need to use or provide a different security mechanism for different transport types or to depend on the transport provider for their secure network. The network overlay can support a wide variety of security capabilities and can be enhanced in its inherent security capabilities by the addition of advanced security systems that are added as discrete overlays, services, or applications and can be managed both automatically and at central as well as local levels.

Generally, the top requirements that should be mandatory within every SD-WAN security regime are:
Secure connectivity
SD-WAN provides end-to-end encryption across any network type, including the internet with full and secure authentication. It has massively scalable key exchange capabilities with automatic management. It also enables secure communication among branches and data centers, as well as communication to the cloud via gateways. All devices and components are fully authenticated in the network and all traffic across that network is encrypted.

Segmentation and micro segmentation
Many enterprises require segmentation to isolate different types of traffic for regulatory reasons or to give different business groups like finance, marketing and HR their own network segments. Enterprises typically address these needs by using either virtual LANs (VLANs) or virtual routing and forwarding (VRF). SD-WAN allows segmentation in a much more secure manner compared to MPLS (which doesn’t encrypt the traffic) as SD-WAN automatically encrypts all traffic.

Secure services insertion
An SD-WAN will have built-in foundational security capabilities (such as a Layer 7 firewall) in the edge devices, but SD-WAN alone may not be a best-of-breed security solution for all enterprise requirements. Additional security services can be inserted at various locations (for e.g. at the branch, in the cloud, and on-premise at the data center or within headquarters) to provide enhanced security capabilities to meet enterprise needs. SD-WAN service insertion brings functions, such as virus scanning and data loss prevention, close to the appropriate traffic as much as possible. SD-WAN can perform deep application recognition, allowing granular control over routing of specific traffic to flow through specific and targeted security services.

Secure deployment
SD-WAN allows the enterprise to ship an edge device to a branch or for the branch to be acquired from a local supplier based on a provider list. The box can be installed in a plug-and-play manner by local non-IT/technical/engineer staff. The headquarter network staff centrally creates a configuration, typically using a group profile, that can be pulled down by the box following the authentication of a unique activation key or be pushed to the box from a cloud redirector after the box pings. A branch can be onboarded to the enterprise system or add resources within hours.
There is no risk of losing shipped equipment or compromising the overall security of the enterprise system as it does not contain network security keys or encryption tokens.

**Visibility and compliance**

A significant attribute of SD-WAN that extends to the cloud is its ability to recognize thousands of different applications. This can be combined with analytics, monitoring and metrics that an orchestrator and controller can collect from each of the edge and gateway devices. The operation allows the enterprise to perform critical activities such as looking for anomalies in application usage, screening for unsanctioned applications and dropping the packets of unwanted applications. The enterprise can also apply policies around specific applications such as routing them through a specific additional security service if required. Traffic steering and segmentation in this manner can also assist in meeting regulatory or internal compliance requirements.

**Additional overlay security and infringement tracking services**

With the emergence of SD security, multi-layer security can be more easily integrated into an SD-WAN solution via software, which isn't possible with a standalone appliance-based approach. The benefits for providers and enterprise IT teams alike are a much simpler insertion of security into the branch to protect internet access, far more timely service deployment and upgrades, and greatly reduced chances of one standalone network or security component breaking another.
SDN SECURITY SERVICES

Eligibility Criteria

- Product/service portfolio coverage/focus, completeness and scope
- Understanding of overall security and SDN/SD-WAN and additional focus areas
- Scope of partnerships and offerings, management capability for the needed orchestration to deliver integrated product
- Completeness and pro-activeness of customer support and advisory post delivery
- Third-party accreditation of solution/test results and confidence delivery
- Stability and roadmap planning of the provider
- Reference customer/solutions in post pilot/commercial deployment
- Competitiveness of offering and types of commercial terms

Observations

- **BT** has a risk-based methodology, working with customers to understand their current exposure and therefore avoiding overinvestment in one area while leaving gaps in another. Its depth of understanding of both networks and overall security helps protect customers from design flaws and places security controls when there is exposure in their SDN.
- **IBM's** current roadmaps and plans is based on the philosophy that philosophy that security is network integrated, software defined, critical to SD-WAN and will programmable. The firm also believes that networks are becoming highly secure environments.
- **Masergy** added a new option to its SD-WAN service in 2017 called SD-WAN Go, which includes embedded firewalls, zero-touch provisioning from the Masergy portal and WAN optimization. Other aspects of its security portfolio include Masergy Unified Enterprise SecurityTM (UES), security operations, (with centers around the globe) and managed security services coupled with professional services.
- **Orange Business Services** covers a large range of network security services such as managed security options based on both cloud security and SD-WAN security. Cloud security is based on
Observations (cont.)

- Its own products together with its strategic partner Zscaler. Secure by Orange SD-WAN service is also available.

- **Symantec** has a wide and deep coverage in terms of network and enterprise security as well as security within SDN environments. Its portfolio covers network forensics (security analytics, endpoint detection and response) and content and malware analysis (integrated with Symantec Proxy, ASG, WSS, endpoint protection, ATP platform, secure message gateway, CASB, email security service and WAF).

- **T-Systems** mainly cover security services and products and is specifically focused on SD security from the Magenta Security. This division covers embedded security, SAP security, classified security, cloud security, consulting, bespoke solutions, on-premise security services, building security and automotive security operations centers.

- **Vodafone** provides security within all areas of its services range, both built-in and as additional or value-added service (VAS) products, including within its SD-WAN, internet access and cloud connect ranges. The Secure Network Gateway (SNG) proposition introduced the web security add-on and the internet and SD-WAN proposition (Zscaler). There is also a new tiered proposition that covers firewall sourcing, deployment, management and monitoring (BAE Systems).

- **Wipro’s** SD network services portfolio is part of its connected future practice. This covers data center networks, WAN, SD-WAN and SDN/NFV areas that utilize Swift SDN and #WANFreedom together with SDX Security. Security is considered an integral part of Wipro’s overall deliveries. The firm has subject matter experts for each technology and process area, as well as in industry verticals, to bring in the required knowledge to consulting-led delivery teams.
Definition

SDN technologies enable improvements in network agility and automation, while substantially reducing the cost of network operations compared to traditional network deployments. Deploying an industry-standard data plane abstraction protocol (such as OpenFlow) allows the use of any type and brand of data plane devices as all the underlying network hardware is addressable through a common abstraction protocol. Such a protocol allows for a dynamic and automatic provisioning of virtual network segments and virtual routing services on both physical and virtual networking devices. Additionally, with SD access in branch/edge, including all customer premises equipment (CPE, referenced as virtual CPE or vCPE in SDN terms) and associated WiFi networks, access points (APs), software-defined mobile network (SDMN), software-defined local area network (SD-LAN), which includes both wireless (SD-WLAN) or mobile (SD-WMLAN), the management protocol can be further improved.
**vCPE**

The traditional CPE deployment model, which requires multiple specialized devices at customer premises with each involving complex installation and possibly pre-installation of enterprise-specific codes or software, is extinct. vCPE is replacing multiple hardware appliances with a generic CPE that is vendor independent and based purely on performance points, utilizing SDN and/or SD-LAN and delivery capabilities rather than branding. This enables enterprises to provide services on-demand with the required flexibility to rapidly scale up/down services at high reliability and quality levels without the need for trained technical or support staff.

**SDMN**

SDMN is relatively new and stems from the complexity of network management in 5G mobile networks and beyond, driven by the growing mobile traffic demand, heterogeneous wireless environments, and diverse service requirements. This environment has driven a perceived need to introduce new radio network architecture by taking advantage of software-oriented design, the separation of the data and control planes, and network virtualization to manage complexity and offer flexibility in 5G networks. SDN in mobile networks is fundamentally different from SDN for the internet. Mobile networks deal with the wireless access problem in complex radio environments, while the internet mainly addresses the packet-forwarding problem. Specific requirements in mobile networks shape the development of SDMN. As the proposed micro networks and enterprise-specific networks within 5G move towards reality and piloting, SDMNs (as part of the enterprise managed portfolio) are gaining prominence.
SD-LAN is an emerging solution built on the principles of software-defined networking. However, there are key differences in topology, network security, application visibility and control, management and quality of service compared to a wider reaching SDN or SD-WAN system. SD-LAN is similar in concept to cloud managed LAN systems. It decouples control management and data planes to enable a policy-driven architecture for wired and wireless LANs. SD-LANs are characterized by their use of a cloud management system and wireless connectivity without the presence of a physical controller. They may be found both in more traditional network environments with cloud management services, or as part of overreaching SDN/SD-WAN deployments and strategies.

SD-LAN builds an application and policy-driven wired and wireless access architecture, offering self-organizing and centrally managed networks that are simpler to operate, integrate and scale. It can prioritize and change the behavior of the network based on application requirements and policies of what can be accessed by users, clients and IoT. Typically, it has self-optimizing, self-healing and self-organizing wireless access points and access switches and is cloud managed. It has fully open APIs that allow tight integration of network and applications infrastructures that are not vendor dependant.

This segment will look at all main vendors and service providers (such as telcos) in the SD-LAN space, including vCPE, SDMN and SD-LAN specific vendors.
Eligibility Criteria

- Product portfolio coverage, focus areas, completeness of broader solutions
- Ability to deliver equipment and service to customer, inclusive of prerequisite training
- Understanding of overall market area, technology environment and evolutions and contributions to that area
- Scope of partnerships and offerings, management capability for the needed orchestration within a customer project
- Openness of offering to avoid vendor lock-in
- Completeness of customer support and assistance post delivery
- Stability and roadmap planning of the provider
- Reference customer/solutions in post pilot/commercial deployment
- Competitiveness of offering and types of commercial terms

Observations

- **AT&T** FlexWareSM covers the SD-WAN area and is responsible for core-to-edge functions. AT&T vCPE services under FlexWareSM shifts control intelligence from CPE or edge devices into a centralized software-based controller.

- **BT** has set up its Connected Edge platform that is based on open technology (x.86 devices with future-proofed solutions utilizing established providers, with global logistics capability and migration path for existing Cisco infrastructure).

- **Cisco** solutions, which are based on Meraki, are innovative for SME business on a larger scale than Viptela SD-WAN offerings. Both invoke and utilize intelligent edge functionality, control and capabilities.

- **CenturyLink** offers adaptive networking solutions, SD-WAN as a service, and application and performance-aware routing with full flexibility in appliance deployments based on uCPE.

- **IBM** has put significant focus on its network engineering, integration and innovation services within GTS over the last two years. It also offers SD-LAN, intelligent edge and u/vCPE devices and virtualized devices at the edge. The firm has a strong portfolio of its own technology and solutions together with those from a vast partner ecosystem.
Observations (cont.)

- **Orange Business Services** uCPE is a key enabler for flexible SD-WAN and covers VNF primary functional areas (VNF vRouter, VNF SD-WAN, VNF Security, VNF WAN Op), orchestration (deployment and chaining of VNF, Ciena, BluePlanet), middleware (operating system supporting virtualized functions) (Cisco, Juniper) and hardware, x86 platform, uCPE vendor platform (Cisco ENCS, Juniper NFX) or whitebox.

- **Vodafone** has made significant investments in edge technologies and services and has many developments of its own. The packaging of solutions, support and consulting services on those service-wrapped items are its focus of delivery. It relies on key partners to deliver the individual VNF and edge/branch product and technology sets.

- **Rising Star Apcela** has a strong base in high-performance/low-latency networks, hybrid networks and multi-cloud and SD networking. It is particularly known for allowing smooth and accelerated application use and delivery. It has gained recognition in this segment by utilizing its in-house development to create a range of important NaaS-oriented products.
CenturyLink has been ranked consistently as one of the most dynamic and delivery-oriented WAN and SD-WAN companies with an impressive portfolio of its own assets. It has recently made various announcements on ethernet-LAN, SD-WAN, uCPE, internet applications, including access extensions and management that are highly relevant to edge. CenturyLink offers adaptive networking solutions, SD-WAN as a service, and application and performance-aware routing with full flexibility in appliance deployments based on uCPE*. The company can host multiple virtual network functions (VNF) with a virtual appliance that can consolidate multiple functions on a single device, thus bringing immense operational and cost efficiencies to the enterprise WAN edge.

Strengths

uCPE edge with managed capabilities in SD-WAN: CenturyLink offers SD-WAN as a service to cover both core and edge, including uCPE functionality and control.

Client and end-customer centric: The firm has implemented a slew of new tools and methods to improve customer experience, both for its clients and end users. It incorporates AI, fault and engineering fix information, order and remedial management as well as billing and usage systems, making edge or branch accounting simple.

Caution

CenturyLink has a strong foothold in Europe and the Americas but lacks a deep presence in APAC and Africa.

The company is well known for its managed service delivery as opposed to providing solutions, which may deter those wanting non-managed solutions.
Methodology
METHODOLOGY

The ISG Provider Lens™ 2019 – “Network - Software Defined Solutions and Services” research study analyses the relevant software vendors and service providers in the Global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

The study was divided into the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Definition of Network - Software Defined Solutions and Services</td>
</tr>
<tr>
<td>2.</td>
<td>Use of questionnaire-based surveys of service providers/vendor across all trend topics</td>
</tr>
<tr>
<td>3.</td>
<td>Interactive discussions with service providers/vendors on capabilities &amp; use cases</td>
</tr>
<tr>
<td>4.</td>
<td>Leverage ISG’s internal databases &amp; advisor knowledge &amp; experience (wherever applicable)</td>
</tr>
<tr>
<td>5.</td>
<td>Detailed analysis &amp; evaluation of services &amp; service documentation based on the facts &amp; figures received from providers &amp; other sources.</td>
</tr>
<tr>
<td>6.</td>
<td>Use of the following key evaluation criteria:</td>
</tr>
<tr>
<td></td>
<td>− Strategy &amp; vision</td>
</tr>
<tr>
<td></td>
<td>− Innovation</td>
</tr>
<tr>
<td></td>
<td>− Brand awareness and presence in the market</td>
</tr>
<tr>
<td></td>
<td>− Sales and partner landscape</td>
</tr>
<tr>
<td></td>
<td>− Breadth and depth of portfolio of services offered</td>
</tr>
<tr>
<td></td>
<td>− Technology advancements</td>
</tr>
</tbody>
</table>
Authors and Editors

Dr. Kenn Walters, Author
Lead Analyst & Distinguished Analyst, ISG Research

Kenn is a thought leader and practitioner in networks, smart infrastructure and services and application of advanced technologies globally. Authoring and lead analyst of Software Defined Networking and Digital Transformation IPLs, as well as authoring multiple ISG Insights. He supports clients with customer engagement activities and events on SDN, Future Networks, ICT Network Services, IoT, Smart Cities and Infrastructure, Mobile Enterprise client strategies, Digital Transformation, market development and trends. Kenn is a known expert in these fields in many countries internationally, with over 40 years of experience in the ICT sector.

Jan Erik Aase, Editor
Director

Jan Erik Aase is a director and principal analyst for ISG. He has more than 35 years of collective experience as an enterprise client, a services provider, an ISG advisor and analyst. Jan Erik has overall accountability for the ISG Provider Lens™ reports, including both the buyer-centric archetype reports and the worldwide quadrant reports focused on provider strengths and portfolio attractiveness. He sets the research agenda and ensures the quality and consistency of the Provider Lens™ team.
ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 70 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry’s most comprehensive marketplace data. For more information, visit www.isg-one.com.