

***ISG** Provider Lens™

Network - Software Defined Solutions and Services

SDN Security Services

Global 2019
Quadrant
Report



A research report
comparing provider
strengths, challenges
and competitive
differentiators

Customized report courtesy of:



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 editors are Sabrina Ambrosia and Grant Gross. The research analyst is Srujan Akurathi and the data analyst is Bhanwar Chauhan.

ISG Provider Lens™

ISG Provider Lens™ delivers leading-edge and actionable research studies, reports and consulting services focused on technology and service providers' strengths and weaknesses and how they are positioned relative to their peers in the market. These reports provide influential insights accessed by our large pool of advisors who are actively advising outsourcing deals as well as large numbers of ISG enterprise clients who are potential outsourcers.

For more information about our studies, please email ISGLens@isg-one.com, call +49 (0) 561-50697537, or visit ISG Provider Lens™ under [ISG Provider Lens™](#).

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +49 (0) 561-50697537 or visit research.isg-one.com.



1	Executive Summary
3	Introduction
18	SDN Security Services
31	Methodology

© 2019 Information Services Group, Inc. All rights reserved. Reproduction of this publication in any form without prior permission is strictly prohibited. Information contained in this report is based on the best available and reliable resources. Opinions expressed in this report reflect ISG's judgment at the time of this report and are subject to change without notice. ISG has no liability for omissions, errors or completeness of information in this report. ISG Research™ and ISG Provider Lens™ are trademarks of Information Services Group, Inc.



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."

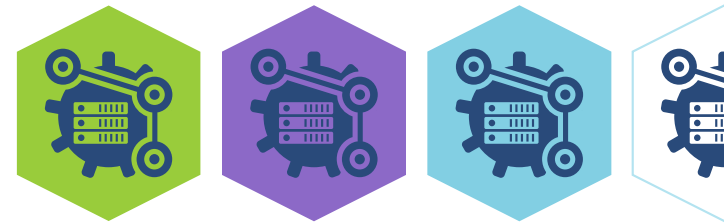
Improving customer satisfaction while boosting sales: The ability to respond quickly and seamlessly to customer queries and quickly provide (often automatically) new services via SDN helps in elevating client experience and boosting sales.

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.

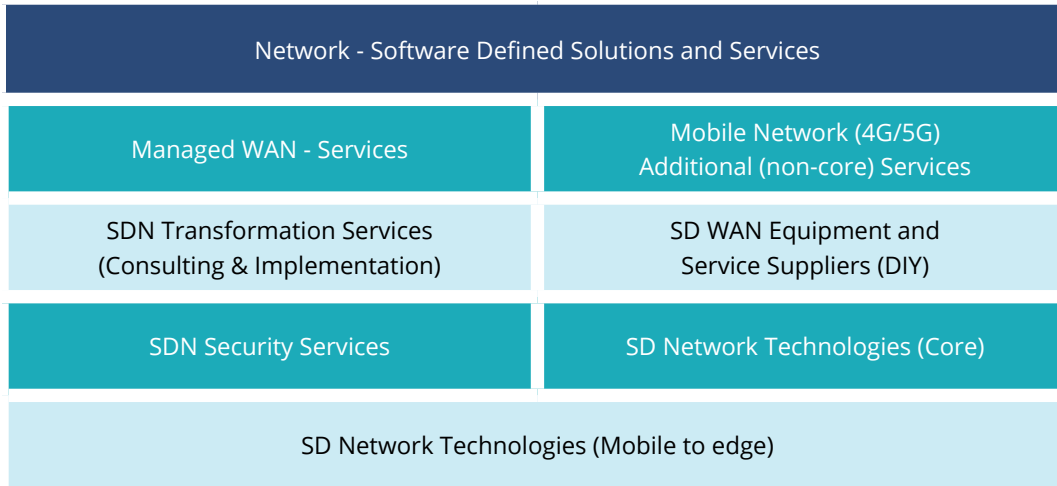
Many service providers that are reviewed in this study are involved in pilot projects and are regularly converting them into production-level deployments. Some have already completed such activities or have many demonstrated instances of doing so on behalf of their clients. This progression, coupled 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

Simplified illustration



Source: ISG 2019

Definition

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.

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.**

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.

Definition (cont.)

SD-WAN Equipment and Service Suppliers (DIY)

SD-WAN provides the benefits of SDN technology to traditional hardware-based networking. It has 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 then centralizes and simplifies network management. This overlay design abstracts software from hardware, enabling network virtualization and making it 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 active in selling directly SD-WAN solutions to enterprises for their “DIY” (enterprise owned and non-managed) implementations. They are also increasingly partnering with licensed telco/service providers to offer delivery packages in this space.

This section should cover all hardware and software, management/reporting tools, applications and services associated with delivering SD-WAN for enterprise-owned operations.

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.

Definition (cont.)

Network Technologies Suppliers (Core)

SDN technology is a networking approach that eliminates the complex and static nature of legacy distributed network architectures by using a standards-based software abstraction layer between the network control plane and underlying data forwarding plane in both physical and virtual devices. It is fundamentally different from NFV in terms of end results and ability, although both approaches are mutually supportive. A network virtualization program eliminates the conventional shortcomings and provisioning tasks related to legacy network segmentation technologies, such as switched VLANs, routed subnets, and firewall access lists (ACLs). An SDN-based network virtualization application supports arbitrary assignment of IP/MAC addressing schemes, automates network configuration tasks and enforces the expected network segmentation. Data plane abstraction provides a standards-based approach to dynamically provision the network fabric from a centralized (or distributed) software-based controller or multiple controllers.

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.

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 Lens™ 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.

Provider Classifications

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

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.

Provider Classifications (cont.)

Each ISG Provider Lens™ quadrant may include a service provider(s) who ISG believes has a strong potential to move into the leader's quadrant.

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 - Quadrant Provider Listing 1 of 5

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
Aerohive	● Not in	● Market Challenger	● Not in	● Not in	● Not in	● Not in	● Not in
America Movil	● Not in	● Contender	● Not in	● Not in	● Not in	● Not in	● Not in
Apcela	● Not in	● Rising Star	● Rising Star	● Rising Star	● Contender	● Rising Star	● Rising Star
Arista	● Not in	● Not in	● Not in	● Contender	● Not in	● Product Challenger	● Not in
Aryaka	● Not in	● Not in	● Market Challenger	● Market Challenger	● Not in	● Not in	● Not in
AT&T	● Leader	● Leader	● Leader	● Not in	● Product Challenger	● Leader	● Leader
ATOS	● Not in	● Not in	● Not in	● Not in	● Contender	● Not in	● Not in
Belkin	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in	● Contender
BT	● Leader	● Leader	● Product Challenger	● Not in	● Leader	● Product Challenger	● Leader
Cato Networks	● Not in	● Product Challenger	● Product Challenger	● Product Challenger	● Not in	● Product Challenger	● Product Challenger
Centrify	● Not in	● Product Challenger	● Not in	● Not in	● Product Challenger	● Not in	● Not in

Network - Software Defined Solutions and Services - Quadrant Provider Listing 2 of 5

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
CenturyLink	● Leader	● Not in	● Leader	● Not in	● Product Challenger	● Not in	● Leader
China Telecom	● Contender	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in
Cisco	● Not in	● Not in	● Product Challenger	● Leader	● Product Challenger	● Leader	● Leader
Citrix	● Not in	● Product Challenger	● Not in	● Not in	● Product Challenger	● Not in	● Not in
Cloudgenix	● Not in	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in
Colt	● Product Challenger	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in
Computacenter	● Not in	● Not in	● Product Challenger	● Not in	● Not in	● Not in	● Not in
Datto	● Not in	● Not in	● Not in	● Not in	● Contender	● Not in	● Not in
Dell EMC	● Not in	● Not in	● Market Challenger	● Leader	● Not in	● Leader	● Market Challenger
D-Link	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in	● Market Challenger
DXC	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Not in

Network - Software Defined Solutions and Services - Quadrant Provider Listing 3 of 5

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
Ericsson	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Product Challenger	● Product Challenger
Extreme Networks	● Not in	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger
Fortinet	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Not in
GTT	● Product Challenger	● Not in	● Contender	● Not in	● Not in	● Not in	● Product Challenger
Harman	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Product Challenger	● Product Challenger
HCL	● Product Challenger	● Not in	● Product Challenger	● Leader	● Market Challenger	● Leader	● Not in
HPE	● Not in	● Not in	● Contender	● Contender	● Not in	● Contender	● Product Challenger
Huawei	● Not in	● Not in	● Not in	● Contender	● Not in	● Product Challenger	● Not in
IBM	● Leader	● Product Challenger	● Leader	● Leader	● Leader	● Leader	● Leader
Infosys	● Not in	● Not in	● Product Challenger	● Leader	● Product Challenger	● Product Challenger	● Product Challenger
Juniper	● Product Challenger	● Not in	● Leader	● Leader	● Not in	● Market Challenger	● Not in

Network - Software Defined Solutions and Services - Quadrant Provider Listing 4 of 5

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
Logicalis	● Rising Star	● Not in	● Contender	● Not in	● Not in	● Contender	● Not in
Masergy	● Market Challenger	● Market Challenger	● Not in	● Market Challenger	● Leader	● Not in	● Not in
Microsoft	● Not in	● Product Challenger	● Not in	● Not in	● Product Challenger	● Not in	● Not in
NTT	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Market Challenger	● Product Challenger	● Product Challenger
Nuage Networks (Nokia)	● Not in	● Product Challenger	● Product Challenger	● Product Challenger	● Not in	● Contender	● Not in
Orange Business Services	● Leader	● Leader	● Leader	● Leader	● Leader	● Not in	● Leader
PCCW	● Market Challenger	● Product Challenger	● Not in	● Not in	● Not in	● Market Challenger	● Not in
Pica8	● Not in	● Contender	● Not in	● Not in	● Not in	● Not in	● Not in
Prodapt	● Not in	● Not in	● Product Challenger	● Not in	● Not in	● Not in	● Not in
Riverbed	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Not in	● Not in
Silver Peak	● Not in	● Product Challenger	● Product Challenger	● Product Challenger	● Not in	● Not in	● Not in

Network - Software Defined Solutions and Services - Quadrant Provider Listing 5 of 5

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
SingTel	● Product Challenger	● Leader	● Product Challenger	● Not in	● Not in	● Product Challenger	● Not in
Sprint	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Not in	● Not in	● Not in
Swisscom	● Market Challenger	● Product Challenger	● Product Challenger	● Not in	● Not in	● Not in	● Not in
Symantec	● Not in	● Not in	● Not in	● Not in	● Leader	● Not in	● Not in
Talari Networks	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Product Challenger	● Not in
TCS	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Product Challenger	● Not in	● Product Challenger
Tech Mahindra	● Leader	● Not in	● Leader	● Not in	● Not in	● Not in	● Product Challenger
Telstra	● Product Challenger	● Not in	● Product Challenger	● Not in	● Not in	● Not in	● Not in
Telus	● Contender	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in
TP-Link	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in	● Contender
Trend Micro	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in	● Not in

Network - Software Defined Solutions and Services - Quadrant Provider Listing 6 of 6

	Managed WAN Services	Mobile Network (4G/5G) Additional (non-core) Services	SDN Transformation Services (Consulting & Implementation)	SD-WAN Equipment and Services (DIY)	SDN Security Services	SD Network Technologies (Core)	SD Network Technologies (Mobile to Edge)
T-Systems	● Product Challenger	● Leader	● Leader	● Not in	● Leader	● Not in	● Not in
Verizon	● Product Challenger	● Leader	● Leader	● Not in	● Not in	● Not in	● Product Challenger
Versa	● Not in	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Not in
Vmware	● Not in	● Not in	● Not in	● Leader	● Product Challenger	● Not in	● Not in
Vodafone	● Product Challenger	● Leader	● Product Challenger	● Not in	● Leader	● Leader	● Leader
Wipro	● Leader	● Not in	● Leader	● Not in	● Rising Star	● Not in	● Not in
ZTE	● Not in	● Not in	● Not in	● Not in	● Not in	● Not in	● Contender



Network - Software Defined Solutions and Services Quadrants

SDN SECURITY SERVICES

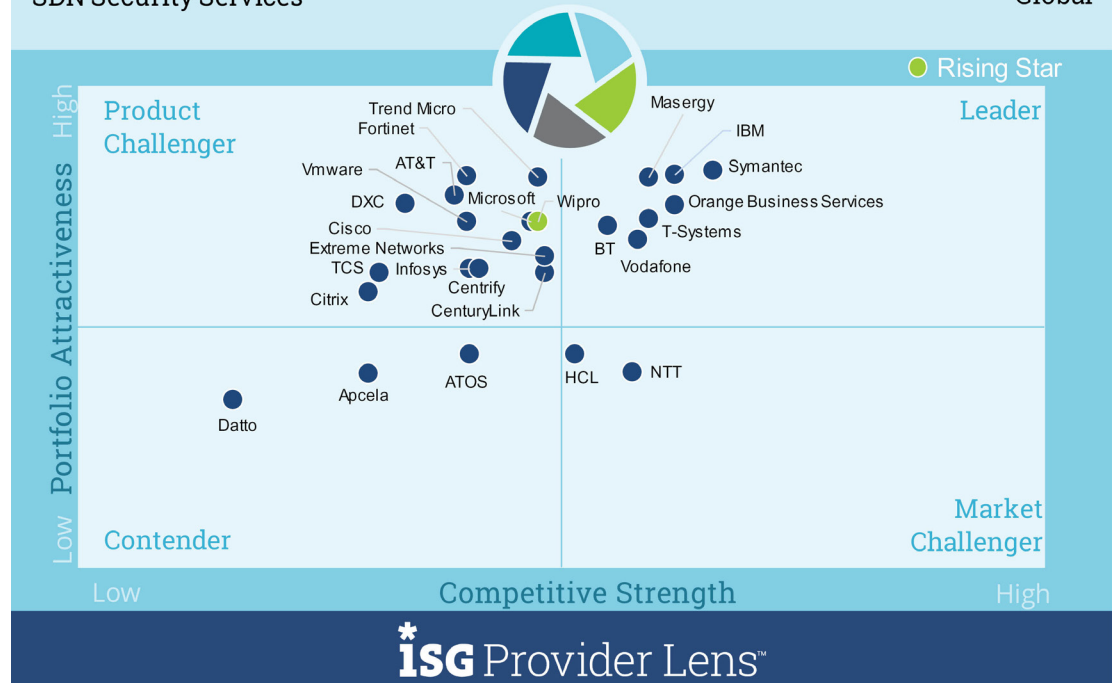
Definition

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:

Network - Software Defined Solutions and Services
SDN Security Services

2019
Global



Source: ISG Research 2019

SDN SECURITY SERVICES

Definition (cont.)

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.

SDN SECURITY SERVICES

Definition (cont.)

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 security is network integrated, software defined, critical to SD-WAN and will be 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 Security™ (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

SDN SECURITY SERVICES

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.

BT



Overview

BT is a longstanding provider of security services in the networking and cloud areas. It has many certified and compliant security solutions and monitoring centers running on a global basis. The firm has recently been applying these security solutions to the SDN area. BT's SDN security approach is to provide a global offering that combines network and security into one solution, instead of treating them as separate entities. The firm has adopted a risk-based methodology, working with customers to understand their current exposure and therefore preventing 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 their SDN faces exposure.



Strengths

End-to-end portfolio: BT has a strong end-to-end portfolio and a global reach, protecting customers and their businesses in 180 countries. BT Security can monitor, track and react to threats across the network and has an integrated internal and commercial security team. The firm has highly experienced business and solution consultants as well as technology practitioners to advise and formulate delivery for client-specific projects.

Portfolio flexibility: BT has a mix of its own and partner solutions to deliver highly capable managed security solutions to different client sizes.

Assuring existing investments are safeguarded: BT ensures that its customers' existing security controls are deployed effectively, patched and fine-tuned accordingly. This centralized management is provided globally from 15 SOCs to ensure that the latest threats are covered and taken care of in near real time.



Caution

BT has a large portfolio and certified solutions. However, its marketing and PR on a global level, specifically on SDN security, is not that aggressive or reaching the coverage levels of many of its competitors. This should be rectified with a new market approach campaign.

Many global enterprises believe that firm is (erroneously) is more focused on the U.S. and EMEA instead of being a truly global player.



2019 ISG Provider Lens™ Leader

BT is a strong global provider of managed security solutions within the SDN space and has strong monitoring capabilities.

IBM

Overview

IBM Global Technology Services (GTS), together with the telecom and media and entertainment divisions, has a strong portfolio of its own solutions along with a vast partner ecosystem of leading players. IBM's current roadmaps and plans are based on the philosophy that security is network integrated, software defined, critical to SD-WAN and will be programmable. The firm also finds that networks are becoming highly secure environments. IBM's paradigm "Security-Enabled with cloud, AI and orchestration, driven by collaboration" underpins all its SD initiatives and forms a basis for its discrete security-focused practice for services within the firm.

Strengths

Highly secure core-to-edge network: IBM has a strong visionary approach towards SDN and SD-WAN and its associated security. With the provisioning of SDN services and built-in/add-on security, the firm offers a core-to-edge high security innovative network.

Global portfolio: IBM has an almost unrivaled global footprint and is an established provider of network and technology infrastructure as well as integration and operation services. It was one of the first to offer a network as a service (NaaS) delivery/pricing model and is continuing to innovate in this area.

Excellent solution ecosystem: IBM has a strong portfolio of its own security solutions but is also expanding its world-class partner ecosystem in the SDN, SD-WAN and security space. These assets, together with IBM's consulting and project management abilities and deep industry vertical expertise, allow it to deliver comprehensive built-in or add-on solutions.

Caution

IBM may not be taking advantage of the SME marketplace and is instead concentrating on larger clients. It may not be emphasizing its security enough as an add-on service to attract players in this segment.



2019 ISG Provider Lens™ Leader

IBM has a strong security built-in philosophy that supports the on-going transformation from traditional WAN to SD-WAN in enterprises.

MASERGY

Overview

Masergy delivers secure hybrid networking, cybersecurity and cloud communications to global enterprise clients in industries such as manufacturing, healthcare, entertainment, finance and broadcasting. Its cloud services include network and application management, global cloud communications and hosted remote access. Its managed services focus on disaster recovery and security. In 2017, Masergy added a new option to its SD-WAN service 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 Security™ (UES), security operations (with centers around the globe) and managed security services coupled with professional services.

Strengths

Ability and maturity: Masergy has a comprehensive and wide-reaching set of its own developments. It also has decades of experience in the security areas of networking and enterprise protection.

Strong global coverage for managed services: Masergy has an extensive global coverage with 24/7 operations centers to protect its clients' networks and businesses.

Consultative and practitioner advisory: Masergy's team of professional service experts have extensive security expertise and industry knowledge to detail the needs and possibilities during their engagements with enterprise clients.

Caution

Masergy may not be visible to the SME marketplace as it primarily perceived as a supplier for large enterprises in many regions. Due to the product and service range on offer, this may be a wasted opportunity for the company.



2019 ISG Provider Lens™ Leader

Masergy offers a highly capable portfolio of security services in the SDN space for enterprises globally.

ORANGE BUSINESS SERVICES

Overview

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 its own products together with its strategic partner Zscaler (where joint development and deployment plans exist) and includes control of internet usage, clean-up of browsing traffic and secure remote access, security as a virtual function, uCPE or SDN Pop and Orange uCPE as an enabler. SD-WAN appliance with advanced security (due in second half of 2019). Secure by Orange SD-WAN service utilizes Secure SD-WAN management platform in hosting zones across multiple global locations. Orange has 1,300 cyber defense experts around the globe, 30 years in securing critical infrastructures, 4 cyber security operations center (SOCs) and 9 SOCs, 3 scrubbing centers and 720 multinational customers.

Strengths

Global reach and competence: Orange Business Services offers large coverage through its hosting zones and cyber defense experts. It has a strategic partnership with Zscaler along with joint development roadmaps.

Multiple routes to meet requirements: The firm offers flexible security solutions and managed security services for most scales and types of enterprise deployments.

Consulting services for commercial roll-out: Orange Business Services provides a highly collaborative, open and consultative approach, guiding the customer through the decision-making process beginning with the proofs of concept (POCs) till commercial rollouts.

Caution

Larger enterprises do not always understand the level and scope of security services offered by Orange Business Services. To address this concern, the firm should provide a comparative chart and use cases that demonstrate which products are suitable based on the type and scale of deployment.



2019 ISG Provider Lens™ Leader

Orange Business Services offers high-quality and flexible security products for most enterprise types and scales.

SYMANTEC

Overview

Symantec is a leading provider of cybersecurity software and services and operates one of the world's biggest cyber intelligence networks. Founded 36 years ago, the firm employs 13,000 people in more than 35 countries and has over 2,000 global patents. Its software and services are used by corporations, government agencies and individuals. It has deep coverage on 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).

Strengths

Mature and capable provider: With four decades of experience, Symantec offers a comprehensive range of security solutions and has deep knowledge in the security areas of networking and enterprise protection.

Consultative practitioners: Symantec has a large pool of advisors who work exclusively in the enterprise and government security areas to support client-specific engagements and deliveries.

Global reach, local knowledge: Symantec is focused on global businesses and clients, while also retaining its ability to consult and deliver locally in numerous countries.

Caution

Symantec is erroneously perceived in some enterprises as a technical solution/upgrade choice rather than a business partner or full-service provider. It has both the expertise and products to deliver complete corporate-level network solutions to large enterprises and SMEs. The firm should continue to demonstrate these capabilities to its customers.



2019 ISG Provider Lens™ Leader

Symantec is a highly capable service provider with innovative and strong security products along with full security coverage capabilities for enterprises in the SDN space.

T-SYSTEMS

Overview

T-Systems provides high-quality services throughout Europe and many other international markets in SDN and SD security. The firm covers security services and products and is specifically focused on its SD security offerings from Magenta Security. This division covers embedded security, SAP security, classified security, cloud security, consulting, bespoke solutions, on-premise security services, building security and automotive SOC. To keep up with the market trends, T-Systems has recently expanded its coverage areas with enhanced security consulting services for SDN/SDN-WAN (consulting, assessments, testing), managed next-generation firewall @ AWS/Azure, continuation of IBM QRadar SOC/SIEM services, DDoS backbone and cloud protection, APT Protect Pro and Protect Pro for email (available as cloud).

Strengths

Strong existing and expanding portfolio: T-Systems is expanding its existing portfolio of products and services this year in areas such as network security services from cloud, (IDS/IPS from the cloud, web application firewalling, customer dedicated web security) cloud access security broker 2.0, and automated service provisioning and operation.

On-track planning: The company's security portfolio is clearly structured, and its coverage and initiatives are well defined and funded. Portfolio upgrades are strategically planned and executed, and the roadmap is shared with industry observers.

Ability and stability: T-Systems has a comprehensive and wide-reaching set of developments with deep knowledge in the security areas of networking and enterprise protection, based on several decades of knowledge.

Caution

T-Systems has a larger portfolio than many of its competitors. However, it should clearly define its offering to the SME market with specific use cases from its vast reference base.



2019 ISG Provider Lens™ Leader

T-Systems provides a broad and extensive portfolio of security services and products. It also caters to some industry vertical-specific cases.

VODAFONE

Overview

Vodafone provides security within all areas of its services range, both built-in and as additional or VAS products, including within its SD-WAN, internet access and cloud connect ranges. Its security offerings include Cisco MSX orchestrated SD-WAN, Cisco security (ASAv), cloud security (Zscaler), advanced live action analytics, cloud connect (managed security services: NAT service for public peering, WAN optimization), internet access (web security, DDoS protection and BGP route hijack security support) and SD-WAN overlay onto internet.

The group has introduced web security add-on with the recent proposition of secure network gateway (SNG). It also has an SD-WAN proposition (Zscaler) to ensure secure internet access. A new tiered proposition covers firewall sourcing, deployment, management and monitoring (BAE Systems).

Strengths

Flexible applications and security offerings: Vodafone applies different models to ensure that specific enterprise needs are met with both inherent and optional VAS security deployments.

Differing vendor-agnostic delivery models: The firm also offers solution products from BAE systems, Cisco and Zscaler to ensure neutrality with a choice of an optimum delivery method to suit client requirements.

Caution

Use cases for specific instances and applicability of different solutions on offer could be improved to assist enterprises in making critical decisions.



2019 ISG Provider Lens™ Leader

Vodafone offers a strong portfolio of security products with SDN at the highest standard.

RISING STAR: WIPRO

Overview

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 and 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 in each technology and process area, as well as industry verticals to bring the overall range of required knowledge together within consulting-led delivery teams. Wipro offers both off-the-shelf solutions and highly tailored client-specific solutions. Some of these include NetFactory, ServiceNXT, governance via Wipro SmartView, Cloud Trust Security framework, Wipro Holmes RPA/AI methods and toolsets as well as partner solutions and products from many companies.

Strengths

Productized offerings are advanced and flexible: SDX Security, an end-to-end highly secure SDN/SD-WAN security system, is productized and can be fully tailored to meet individual enterprise requirements.

Addressing rolling out to in-operation phases: Wipro provides a plethora of advanced tools and methods for commercially rolling out and managing SD network security implementations, including the use of AI and single-pane-of-glass management systems.

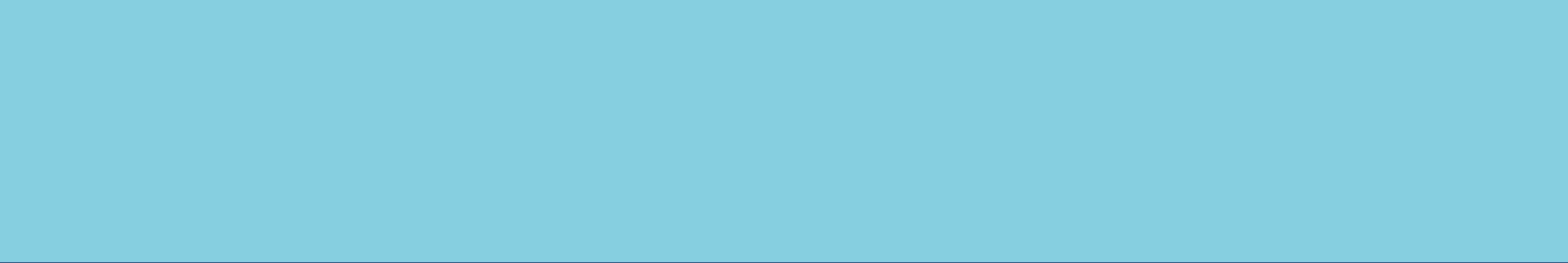
Caution

The need to focus on industry-specific solution areas, such as FSI, manufacturing and energy, medical and chemical production, may push Wipro to undertake a significant recruitment program to maintain a consistent level of expertise.



2019 ISG Provider Lens™ Rising Star

Wipro is an important provider of advanced security packages within SDN on a global level.



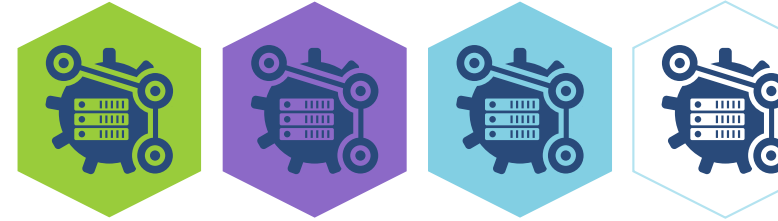
Methodology

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:

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



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 Provider Lens™ | Quadrant Report June 2019

© 2019 Information Services Group, Inc. All Rights Reserved



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.