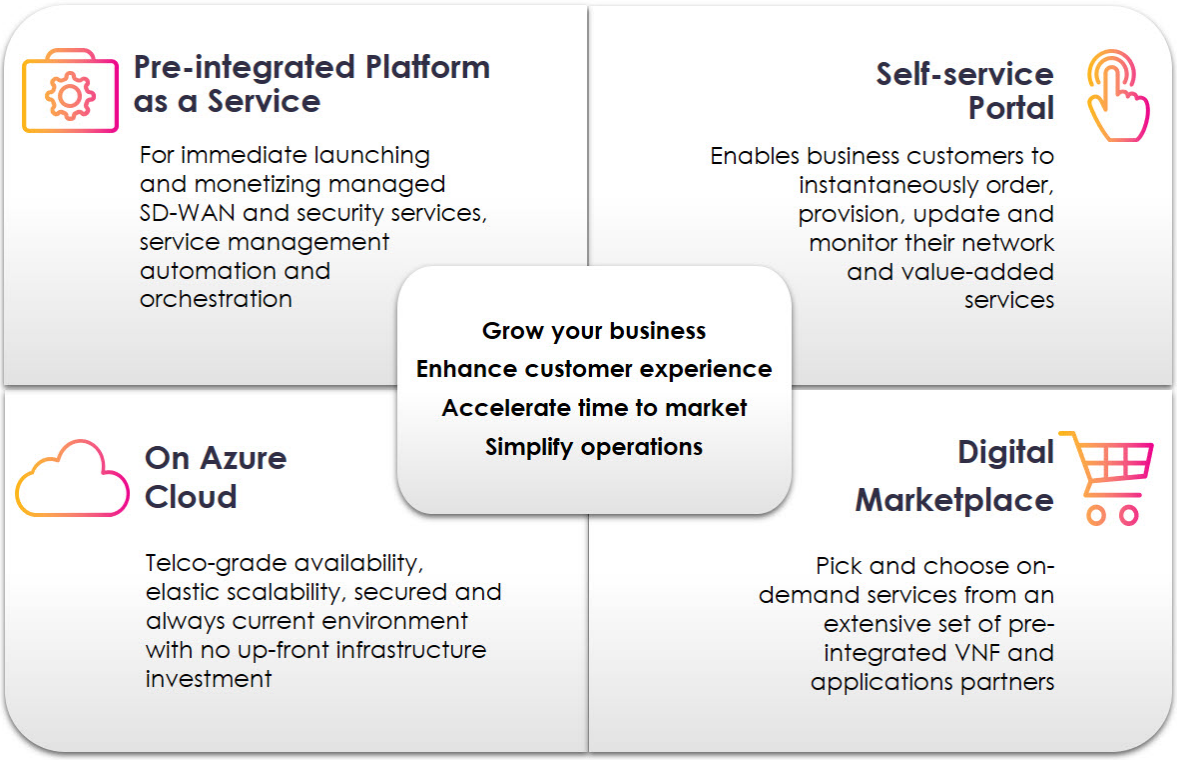
NFV SD-WAN package on Azure

SD-WAN introduces an opportunity for CSPs (Communication Service Providers) to increase revenue by growing their variety of network services offerings and upselling new software-defined network services to existing customers. The drawback, however, is that the associated complexity and cost of introducing these services can cause CSPs to miss revenue opportunities due to the inability to bring such services to the market at the necessary speed. In most cases, the business enablement system's awareness of network capabilities and resources is wanting, while a lack of integration between the network and BSS makes new service introduction a very complex and manual process that could last months. Other major challenges include an increasingly competitive environment and Business users' sophistication and expectation for an instantaneous service ordering and control experience.

Amdocs' NFV SD-WAN package on Azure addresses these challenges and enable CSPs to gain fast time-to-market and benefit from a pre-integrated, highly scalable, flexible, resilient and proven cloud-based PaaS solution while eliminating massive upfront investments. Amdocs' NFV SD-WAN package on Azure allows service providers to easily manage SD-WAN and VNF-based network services over the highly scalable Microsoft Azure public cloud infrastructure. The solution also allows CSPs to offer their business customers an unprecedented experience for ordering and managing on-demand services through a digital marketplace leveraging an extensive set of pre-integrated VNF and applications partners using a self-service portal.



SD-WAN's ability to leverage inexpensive broadband internet bandwidth poses a threat to CSPs' traditional WAN services (such as MPLS), as well as their revenue from existing managed services. Indeed, there is a very large variety of SD-WAN options available to enterprise customers to choose from. While some opt for a DIY (do-it-yourself) approach, others turn to OTT (over-the-top) SD-WAN providers. Nevertheless, for many business customers, the business case for managing and administering many ISPs and OTT providers in order to ensure high WAN availability is questionable. This is because typically, such organizations lack the technical, personnel and capital resources to implement significant WAN upgrades and would prefer to benefit from a managed SD-WAN service offered by CSPs.

Increasingly, CSPs are looking to leverage SD-WAN as an opportunity to increase revenue by growing their variety of data services offerings and upselling new software-defined network services to existing customers. However, many CSPs are missing revenue opportunities because they are unable to bring services to the market at the necessary speed. For the majority of CSPs it takes some time to identify and then standardize modern technologies such as SD-WAN and integrate them with their business enablement systems to offer a basic service offering and related managed services.

In most cases, the business enablement system's awareness of network capabilities and resources is wanting, while a lack of integration between the network and BSS makes new service introduction, as well as fulfillment of customers' service orders, a very complex and manual process that could last months. Other major challenges include an increasingly competitive environment and an increase in user sophistication and demands.

Business customers are expecting to get from CSPs the same experience they get from cloud service and applications providers. They are looking for an instantaneous online ordering service, better visibility and co-managing of their network services.

For CSPs, this means that the ability to provide self-control, flexibility, fast processing, easy-to-use and intuitive user experience has become essential. CSPs are responding to these challenges by looking for solutions that enable faster time to market, simplifying their operations and turning their focus to customer experience. Achieving these goals requires them to utilize a harmonized, SLA-aware platform capable of managing network service and resource scaling in multiple domains and locations in real time.

The implication is that to be successful, the networks must be fully aligned with both CSPs' business requirements and strategies, while maintaining the ability to respond rapidly to changing and evolving business customer's needs.

SD-WAN security

SD-WAN provides secure, IP-based virtual overlay networks that typically utilize IPsec tunnels over internet or MPLS underlay networks. Many SD-WAN vendors are currently undergoing a process to improve their security capabilities with advanced built-in security features that will meet the needs of some of their business customers.

However, other business customers may still prefer security solutions delivered by specialty security solution vendors. While SD-WAN embedded security capabilities are similar to those supported by current routers, several other advanced features are not supported by the majority of SD-WAN products. Examples include intrusion prevention systems (IPS), content-specific controls, URL filtering and anti-malware protection. The implications for business customers and enterprises with high-security needs will be to opt for an NGFW (Next Generation Firewall), sourced from a security-specialist vendor.

The above explains why security integration capabilities are becoming an important differentiator, as well as playing a key role in the managed SD-WAN service provider selection process. Other security considerations for business customers include DDoS mitigation and session border controllers.

CSPs are looking to offer business customers a variety of differentiated SD-WAN services that are complement with value-added services (VAS) and advanced security features enabled by best-of-breed NGFW platforms. To achieve this, NGFWs and VAS VNFs need to be deployed in accordance with performance, business requirements and cost perspectives. The optimal path to achieving this comes by combining SD-WAN with both NFV-based virtual functions and existing underlay WAN resources.

Amdocs' NFV SD-WAN package on Azure

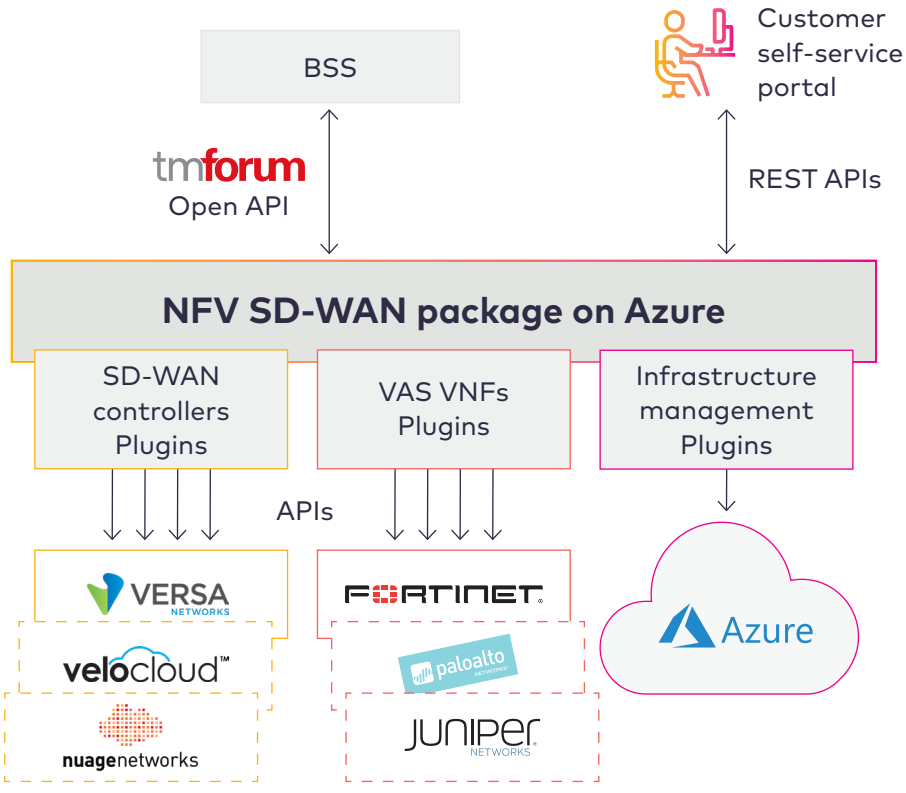
Amdocs' NFV SD-WAN package on Azure is a pre-integrated PaaS solution enabling CSPs to deliver managed SD-WAN and value-added network services, with the benefits of NFV/SDN, public cloud scalability and service automation. This multi-vendor and multi-domain pre-integrated service orchestration solution reduce barriers, accelerates and simplifies the journey for CSPs and empowers them to offer and monetize managed SD-WAN and other network services with low investment and risk.

Amdocs' NFV SD-WAN package solution utilizes pre-integrated plugins to control SD-WAN, security, and cloud infrastructure resources. TMF open APIs are used northbound towards the BSS, and in particular, the ordering system, thereby maximizing the solution's openness and interoperability for seamlessly integrating multiple SD-WAN solutions with existing OSS/BSS platforms.

The solution also leverages a vendor-agnostic service model for composing SD-WAN service connections, VNF service chaining and all network resources required to operate the service. The result is unmatched flexibility, agility and cost savings when operating managed SD-WAN services.

Amdocs NFV platform configures and manages the end-to-end SD-WAN managed service between SD-WAN edges and SD-WAN gateways over one or more underlay WANs (for example, internet and MPLS). It also enables automation of the managed SD-WAN service lifecycle, which includes service fulfillment, performance, control, assurance, usage, analytics, security and policy. In addition, it provides an open and extensible platform that reduces the complexity and cost associated with developing and deploying services across multiple vendor, technology and network domains.

Moreover, a service order decomposition function decomposes orders into service items used by the NFV platform, which then utilizes the plugin interfaces to communicate with the SD-WAN service building blocks, and instantiates the resources and network connections needed for service order fulfillment. The Amdocs NFV platform constantly monitors SD-WAN service performance throughout, according to the predefined policy, thereby assuring its availability and providing end-to-end service visibility.



VNF Marketplace and self-service portal

Business customers are looking for an instantaneous service ordering and control experience. Amdocs' NFV SD-WAN package on Azure enables CSPs to meet this demand and enable their business customers to order on-demand services from a digital marketplace leveraging an extensive set of pre-integrated VNF and application partners. The solution's self-service portal enables business end-customers to order, provision, update and monitor their networks and value-added services. With a few clicks of the mouse an enterprise network administrator is be able to place orders that are delivered in minutes, not months. The portal is integrated with the CSPs' CRM and ordering systems, and eventually with the Amdocs NFV SD-WAN package that manages fulfillment of SD-WAN and other network services orders and service change/modification requests that were initiated by the customer via the portal.

Leveraging Azure cloud agility, flexibility and scalability

Amdocs NFV SD-WAN package solution is deployed in a containerized fashion on Azure, providing a cloud-based PaaS solution that enables CSPs to move up the value chain beyond connectivity and immediately launch SD-WAN and other network services, increasing their revenue opportunities. The solution's NFV platform manages VNFs and services on Azure and other clouds, customer premises and data centers. Microsoft Azure provides a telco-grade environment that efficiently and safely supports network traffic and applications and allow CSPs to benefit from the following:

Cost saving – By avoiding investments for setting up and running the solution in the CSP's data center

Scalability – Computing, storage and networking resources can be provisioned in minutes on demand giving businesses a high level of flexibility and taking the pressure off capacity planning

Security – Take advantage of the latest in security innovation as well as the broadest compliance coverage of any cloud provider

High Availability – Disaster recovery and business continuity through unprecedented coverage and multiple fail-over options

Versa Networks Secure Cloud IP Platform SD-WAN

Versa Networks Secure Cloud IP Platform is a cloud-native multi-tenant software platform that delivers software-defined Layer 3 networking to Layer 7 NSS Recommended security services with full programmability and automation. The Versa software platform enables partners and customers to deliver managed SD-WAN, SD-Security and SD-Branch service offerings for the WAN Edge. Versa's approach is unique by integrating networking and security with full contextual policy management, analytics and application experience-driven infrastructure automation in a single software platform that can be deployed as uCPE, bare metal or virtual, on premise or in the cloud. Amdocs' NFV SD-WAN package on Azure is pre-integrated with Versa Director, which provides unified management and control for all Versa FlexVNF as well as management of application traffic steering policies, security policies, provisioning, monitoring and configuration.

Fortinet FortiGate Virtual Next Generation Firewall

Fortinet delivers the industry's best threat protection, unified threat management and performance in a virtualized form factor, based on the award-winning FortiGate. Fortinet FortiGate is a Leader in Gartner's 2017 Magic Quadrant for Enterprise Firewalls.

FortiGate-VM offers the highest performance and scalability of any virtual firewall available today, with a comprehensive set of validated security capabilities including application control, intrusion prevention, anti-virus, web filtering, mobile security, sandbox, SD-WAN, CASB, security rating service and industrial control services. FortiGate is independently tested and validated for best security effectiveness and performance. It has received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin and AV Comparatives. Amdocs' multi-domain NFV platform allows customers to decouple their network functions from the hardware appliance and deploy the broad portfolio of Fortinet security virtual functions at customer premises, data centers or public cloud as required by the customer and can scale at ease based on demand.

Features

- Pre-integrated platform as a service for quickly creating, deploying and monetizing managed SD-WAN, security and value-added network services
- Multi-domain, multi-vendor service orchestration across data centers and distributed branches
- Plugins for seamless integration with SD-WAN, NGFW, VNFs and Azure cloud resource manager
- Service and resource (VNF) instance orchestration and lifecycle management
- Real-time enforcement of VNF and service-related policy
- Automated continuous service fulfilment and assurance
- Predefined use cases and service model; configurable service parameters
- Seamless BSS integration for service order lifecycle management via TMF Open APIs
- Extensive set of pre-integrated VNFs and applications partners Marketplace
- Self-service portal enables business end customers to order, provision, update and monitor their network and value-added services

Benefits

- Affordable, scalable, pre-integrated, tested and certified platform reduces deployment and entry barriers
- Enables service providers to move up the value chain beyond connectivity and immediately launch SD-WAN and other networks services, increasing their revenue opportunities
- 70% operational efficiency improvement due to service orchestration automation
- Accelerates innovation and service agility through ease of VNF onboarding and service chaining
- Access to Amdocs' rich partner ecosystem of VNFs to drive innovation and VAS
- Operational efficiency, flexibility and profitability of managed services through service automation and orchestration, zero-touch provisioning, centralized management and multi-tenant software running on the cloud
- Meet business customers agility, responsiveness and experience expectations
- Vendor-agnostic platform enables a multi-vendor strategy that addresses a broader set of customers

Amdocs is named a Leader in Gartner's 2019 Magic Quadrant for Operation Support Systems. Gartner recognized Amdocs for its completeness of vision and ability to execute.

Amdocs NFV SD-WAN package on Azure PaaS solution allow CSPs to immediately launch managed SD-WAN services with low investment and risk, and improve operational efficiency by 70% thanks to service-orchestration automation.

Case study: Network services automation and cloudification over Microsoft Azure

One of the world's leading global service providers has selected Amdocs NFV SD-WAN PaaS to rapidly and efficiently tailor industry-focused network solutions that are powered by its fleet of satellites and extensive ground infrastructure to provide seamless scalability to hard-to-reach places, including rural and maritime areas, and to restore connectivity in areas affected by natural disasters. The service provider has selected Amdocs' pre-integrated NFV SD-WAN PaaS solution on Microsoft Azure cloud to gain fast time-to-market and benefit from a highly scalable, flexible, resilient and proven technology solution while avoiding massive upfront investments.
The service provider will use Amdocs' Network Functions Virtualization (NFV) orchestration to integrate and orchestrate existing and new network capabilities for delivering managed network services over both satellite and terrestrial connections.

Amdocs NFV platform allows service providers to easily configure, customize and assure VNF-based network services over the highly scalable Microsoft Azure public cloud infrastructure.

Selecting Amdocs' open, standard based, and scalable solution will allow this service provider to expand into new applications beyond traditional connectivity.

The Amdocs platform will enable the service provider to offer its broadcast, telecom, corporate and government customers innovative NaaS (Network as a Service) offerings such as SD-WAN, WAN optimization, security, Unified Threat Management (UTM) and other highly-flexible and scalable cloud-based network services.

Case study: Using NFV orchestration for managed SD-WAN from day one

A leading North American service provider implemented an award-winning, carrier-grade, SD-WAN platform, designed for enterprises, SMBs and multi-site businesses. Subsequently, to future-proof the platform and provide customers with value-added services (VAS), they engaged Amdocs to implement its multi-vendor, multi-domain NFV orchestration, integrated with Versa's SD-WAN platform. The NFV SD-WAN platform combines secure IP-VPN, application-aware routing and a stateful network firewall – all delivered over the public internet via a carrier-class IP-backbone, with secure internet connectivity to the public cloud. Specifically, the role of Amdocs' NFV orchestrator is to streamline deployment and instantiation of cloud- and premises-based virtual network functions, as well as data center and distributed wide area network connectivity.

The agile and dynamic solution development process provided by Amdocs and Versa networks significantly reduced time to market from design/inception to production, enabling the operator to bring its new SD-WAN service to market very quickly. Furthermore, Amdocs NFV orchestration service automation contributed to a 65% reduction in service fulfillment operations.

As a result of employing an NFV orchestrator from day one, the service provider achieved its objective of creating an extensible, end-to-end future-ready platform for providing additional VAS beyond SD-WAN.

www.amdocs.com