IDC
Analyze the Future

VIEWQWEST
Internet Made Better

Demystifying software-defined to uncover its true qualities

With a continually evolving landscape, different vendors have positioned SD-WAN differently, and that has created a lot of confusion and resulted in a disconnect in terms of expectations of what SD-WAN can or cannot do. Organizations need a closer alignment between the business and IT leaders to ensuregreater resiliency and security of remote operations.

MYTH 1

SD-WAN will replace all multiprotocol label switching (MPLS) networks with broadband Internet connections

FACT 1

SD-WAN will co-exist with all business connections and demonstrate resiliency to prove itself by eliminating the bottlenecks and resiliency, through dynamic path selection

MYTH 2

SD-WAN can always guarantee QoS

FACT 2

The performance of the SD-WAN integrated network heavily depends on the QoS of the underlay utilized

MYTH 3

SD-WAN lowers ICT spending

FACT 3

SD-WAN might help to lower costs and deliver higher cost efficiency, but it is subjective and depends on many factors such as bandwidth requirements and the mix of underlay used

MYTH 4

SD-WAN is secure by design and practice

FACT 4

SD-WAN in itself is not secure but allows for tighter integration with security solutions and helps bake a superior level of trust into the network

This is an excerpt from the IDC Infobrief "Connecting and Securing a Distributed Enterprise and Remote Workforce", sponsored by ViewQwest.

Integrated security and SD-WAN driving enterprise conversations

As SD-WAN deployments have scaled, enterprises are realizing that this important technology does not solve all of their pain points at the edge of their networks. There are a variety of other network, security, and management tasks that they must consider when architecting their branch and WAN connections. **Security tops the list of considerations** as organizations grapple with an ever-widening enterprise perimeter. However, there's a challenge.

Challenge

SD-WAN integrations with third-party security services, and with other network services in a branch context, have been pursued by enterprises, but they are complex and difficult to execute.

Service insertion, service chaining, and orchestration of third-party virtual network functions (VNFs) are invariably difficult, as highlighted by both service providers and enterprises.

Top Priority

When asked to identify features that are required in a next-generation SD-WAN platform, **integrated security functions and services** came out on top of the list, according to IDC's Worldwide Communications and SD-WAN Survey 2020.

The integration of network, security, and management functions represent an evolution of the SD-WAN market towards a broader software-defined branch, an IDC reference architecture when enterprises deploy multiple virtual or container network functions, either on-premises or in the cloud, in a tightly integrated network and security solution environment.

IDC believes that by opting for a unified suite of network and security VNFs from a single vendor for both SD-WAN and security, organizations stand to gain several benefits, including a holistic view and management of network and security policies, as well as operational efficiency of the ir network and security teams.

This is an excerpt from the IDC Infobrief "Connecting and Securing a Distributed Enterprise and Remote Workforce", sponsored by ViewQwest.