Connecting and Securing a Distributed Enterprise and Remote Workforce

AN IDC INFOBRIEF **I MARCH 2021**

IDC ANALYZE THE FUTURE

Sponsored by VIEWQWEST

IDC #AP241229IB

Executive summary

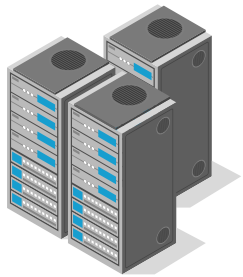
Enterprises across the Asia/Pacific continue to face growing challenges and uncertainties, whether due to the current pandemic or the next shock to global markets.

Compounding the challenges is the move to becoming more distributed than ever as enterprises pivot to support remote workers, leading them to rely more on cloud services.

With connectivity as the glue and key to successful digital transformation in the next normal, security is a growing imperative and cannot be addressed independently of the network.

Asia/Pacific enterprises will need to adopt a secure, software-defined hybrid networking approach in network architectures and invest in next-generation technologies such as SD-WAN and other virtual network services (VNS) to address their changing network and security needs to accommodate their remote workforces.

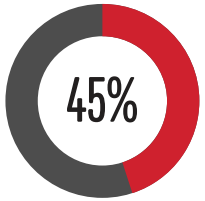
The question is, therefore, not whether to enable software-defined networking and cloud-based tools, but how and where, and what's next.



This IDC InfoBrief explores the importance of a software-defined networking approach to connecting and securing the digital enterprise, SD-WAN deployment models, and the steps in the journey to securing a software-defined organization.

Borderless connectivity top agenda

Connectivity is now recognized by CEOs as one of the top three strategic elements in their digital transformation strategy.



IDC predicts that through 2022 across the Asia/Pacific region, 45% of enhanced digital customer experiences continue to fail due to underinvestment in intelligent, dynamic network architectures and technologies required for modern applications.

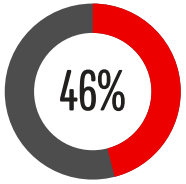
Source: IDC FutureScape: Worldwide Future of Connectedness 2021 Predictions: APEJ Implications

Key trends driving network requirements of the hyper-distributed enterprise

Enterprise networks have become a lifeline for connectivity in the race to accelerate digital transformation. The increased adoption of cloud-based solutions, coupled with the rising need to address Internet of Things (IoT) integration and to interconnect an increasingly remote workforce, is driving a rethink of network requirements.

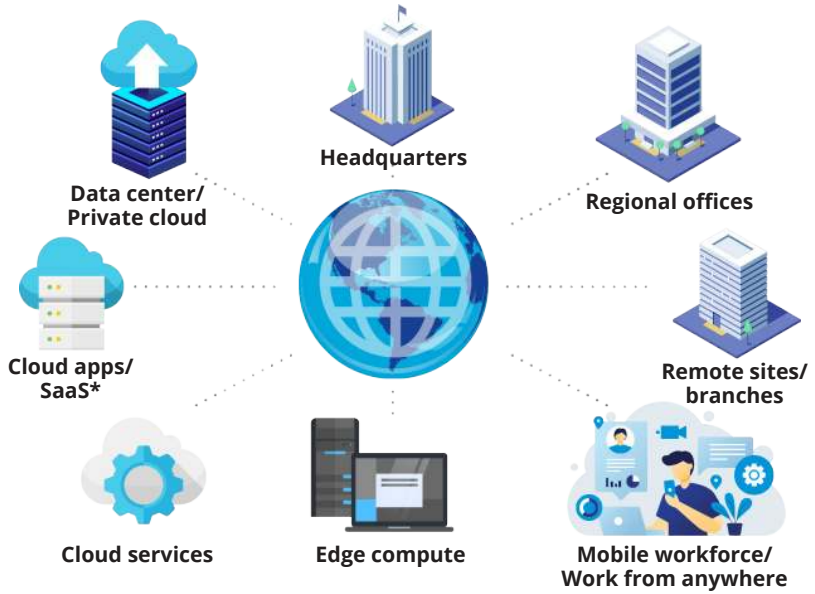
Increased adoption of cloud

Asia/Pacific enterprise spending on cloud applications around applications development, applications, and systems infrastructure software is expected to rise from 13.7% of the total software spend in 2015 to 42.2% in 2020[1]



of Asia/Pacific organizations use 2-4 cloud providers[1]

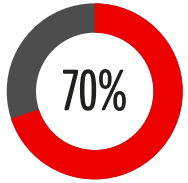
In 2020, ~60% of Asia/Pacific organizations responded with no cut or a moderate/significant rise in the number of cloud providers after COVID-19.[2]



Steady growth in IoT

IDC estimates the number of IP connections to grow at a compound annual growth rate (CAGR) of 18.6% over the forecast period from 3.78 million in 2018 to 11.94 billion in 2024.[3]

Supporting the remote office

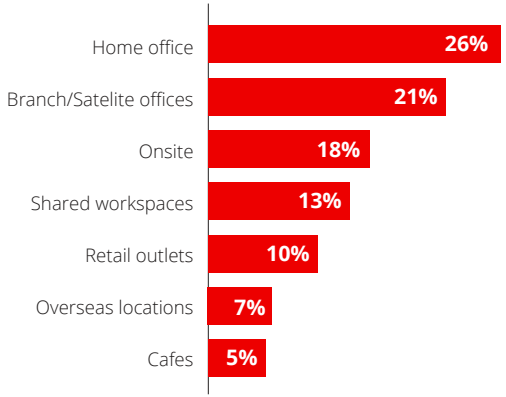


70% of Asia/Pacific organizations are expected to make changes to their business models, ICT infrastructure investments and work environments to accommodate for a widely dispersed workforce, according to IDC's COVID Wave Survey 2020.[4]

Work from anywhere scenarios have permeated into every sector

Securing a mobile and remote workforce has become an urgent imperative, with corporate resources being accessed from unprotected locations and devices.

Preferred primary workplace post-COVID-19 vaccine[4]



Traditional network architectures are not enough to cater to this distributed environment and result in significant challenges around security, application performance, resiliency, and inter-dependencies.

[1] Asia/Pacific excludes Japan and China. Source: IDC's Asia/Pacific Public Cloud Services Spending Guide, 2020
[2] Asia/Pacific excludes Japan. Source: IDC's Asia/Pacific IT Services 2020 Survey (fielded Apr-Jun 2020
[3] IDC's Asia/Pacific (Excluding Japan) Internet of Things Connectivity Forecast and Analysis, 2020-2024
[4] IDC's COVID Wave Survey 2020

Challenges facing distributed organizations with a remote workforce

Asia/Pacific enterprises' top 3 network and ICT challenges:

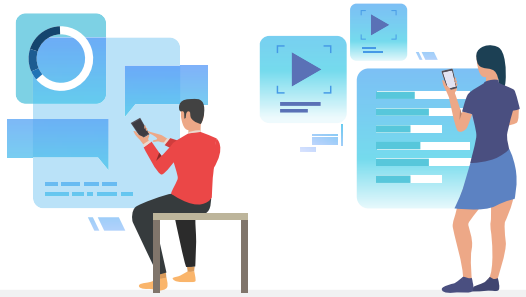
#1 Limited flexibility and agility with in-house management of WANs

- Lack of central monitoring, control and troubleshooting to manage today's complex and distributed network environment.
- Troubleshooting network and access issues for remote workers on their home networks.

Business Impact

Inefficient network management and outages

Finance/Banking: Frequent outages and long network resolution times result in Internet/ mobile/ATM banking access issues, impacting customer experience and increasing churn.



#2 Ensuring consistent application performance for better user experience

- Subpar application performance for hosted enterprise as well as SaaS applications is a big challenge.
- In addition to the corporate environment, monitoring and ensuring application performance for a widely dispersed workforce through VPNs has proven to be difficult.

Business Impact

Subpar application performance

Retail: Slow checkout at a retail store resulting in only being able to serve 1/3rd of customers; slow checkout of self-service kiosks forces a half day shut down

#3 Managing security and compliance of mobile workers and for a widely distributed organization

- Securing a distributed environment where the network connects to a variety of unprotected devices, 'things' and clouds.
- Piecemeal approach to securely connect a mobile workforce that requires remote access to business applications
- Lateral security risks due to interconnected branches and applications

Business Impact

Compromised network security

Manufacturing: Network hackers manipulated control systems so that a German steel mill's blast furnace could not be shut down, resulting in massive damage to the machinery.

*IDC Asia/Pacific COVID-19 Wave Survey and IDC Communications Survey 2020

Software-defined approach to networks and security for a new era

The increasing reliance on cloud services and applications, along with the need to connect a widely dispersed workforce, is driving organizations across the Asia/Pacific region to rethink how their enterprise WAN is architected.

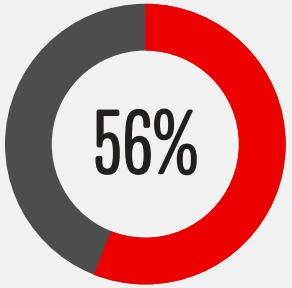
This has led to the advent of a software-defined approach to networking, starting with a software-defined WAN (SD-WAN).

An SD-WAN provides a secure, flexible, and agile network to the business, through centralized management of hybrid WAN connectivity and dynamic path selection of network traffic.

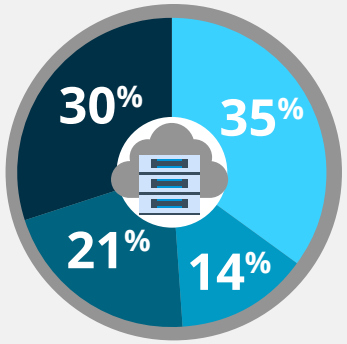
Benefits of a software-defined approach

However, as SD-WAN deployments have scaled, integrated security has become increasingly important to organizations, in an effort to respond to the move to a hyper-distributed and hybrid working model.

SD-WAN is fast becoming an integral part of enterprise recovery strategy following the pandemic



of Asia/Pacific organizations have either already deployed or are planning to deploy an SD-WAN solution by the end of 2021



> **"Working from home has led to changes in the way we work and how we collaborate internally and externally, permanently changing our internal processes in a post-COVID world."**
>
> **A leading Asian bank**

Source: IDC Communications Survey 2020

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.

Source: IDC Communications Survey 2020

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 ensure greater resiliency and security of remote operations.

MYTH 1
SD-WAN will replace all multiprotocol label switching (MPLS) networks with broadband Internet connections

MYTH 2
SD-WAN can always guarantee QoS

MYTH 3
SD-WAN lowers ICT spending

MYTH 4
SD-WAN is secure by design and practice

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

FACT 2
The performance of the SD-WAN integrated network heavily depends on the QoS of the underlay utilized

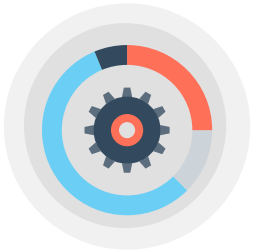
FACT 3
SD-WAN might help to lower costs and deliver higher cost efficiency, but it is subjective and depends on many factors such as bandwidth requirements and the mix of underlay used

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

Choosing the 'right' deployment model is critical

As much as the technology itself, choosing the "right" deployment model is critical to the network transformation journey. With multiple flavors from a number of start-ups, established technology vendors, communications service providers (CSPs), and managed service providers (MSPs) flooding the market, making an informed decision is imperative.

There are primarily 3 types of SD-WAN deployment models today:



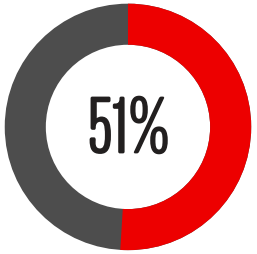
DIY

Fully managed service

Co-managed

Each of the above approaches has its own benefits and pitfalls. While a DIY approach seems more cost-effective at first, it necessitates manpower and competencies not readily available to most organizations.

Given the complex nature of the migration to a software-defined paradigm, there is a noticeable shift in the market towards a fully managed solution from CSPs.



of organizations highlighted that they would prefer to work with telecom service providers for their SD-WAN implementations — largely due to CSPs' ownership of the underlay as well as for their understanding of how the SD-WAN overlay integrates with the underlying network infrastructure.

Essential guidance for a secure SD-WAN roadmap and selecting the right partner

Today's network and security investments are being made for strategic, rather than tactical, reasons. Organizations are rethinking network architectures to accelerate their race to become a "Future Enterprise" — the gold standard in digital transformation. However, organizations must realize that this network transformation is not a straightforward activity but a journey.

Hence, selecting the right partner and working with them to break down the journey into phases is critical. Carefully evaluate your network transformation partners on the following parameters:

Examine the service provider's technology roadmap

SD-WAN is just the beginning, so understand how a service provider's roadmap can help you evolve your software-defined journey, not just today but over the next 5 years.

Match the service provider's network coverage with that of your organization

Look for service providers that can operate and provide connectivity to all your branches, either by themselves or through partners.

Test the solution's security maturity

Look for solutions that start with zero trust network access and a cloud access security broker; moving onto browser capabilities, and more advanced endpoint protection platforms with web application firewalls.

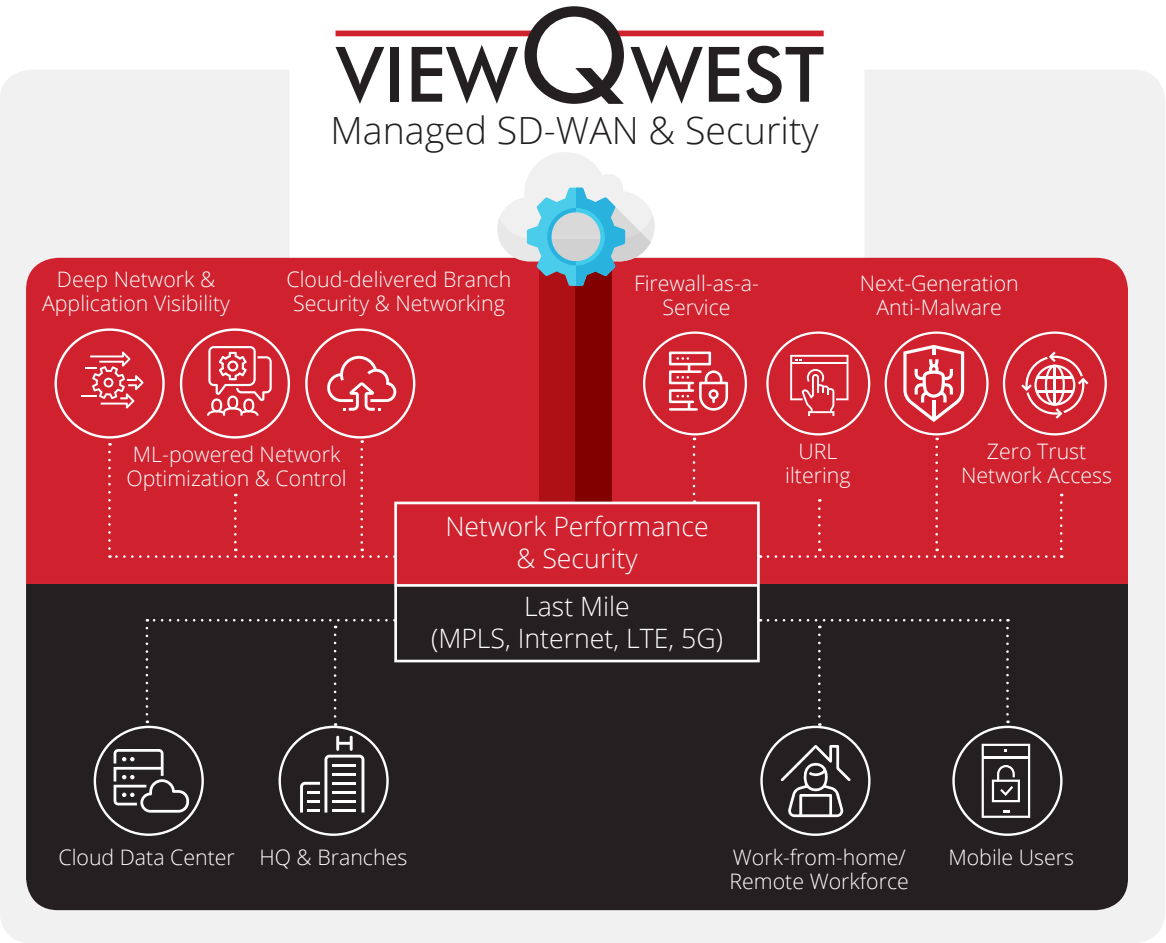
Evaluate the breadth of the services offered by the service provider

This is in terms of the underlay and overlay network, security, managed services, and analytics. Network transformation can be overwhelming and risky, so be sure your chosen service provider will be able to support and execute on your plans.

Consider the partner's overall track record

Be aware that there is no one size fits all. Evaluate the service provider's capabilities and approach based on your business requirements. Every company is different, and the right partner is one that focuses not on the technology or product but on designing solutions for your business.

ViewQwest Secure SD-WAN: Creating a Secure Work Space from Any Location



ViewQwest believes that the network and security are one. The network and security architecture must be designed together and for the cloud, and integrated into a single architecture and practice for organizations to truly be agile, competitive, and secure.

Remote work will be the new norm & organisations are potentially doing away with traditional office spaces. ViewQwest helps enterprises transform with confidence & enable the post-Covid organisation to work efficiently & securely in this new world. Through next-generation SD-WAN & cloud security technologies, ViewQwest can connect company sites & employee homes securely, and turn them into Secure Work Spaces.

SD-WAN Portfolio

Partnering with multiple industry-leading SD-WAN technology providers, ViewQwest can design and implement tailor-fit solutions for enterprises — without the burden of proprietary or legacy technologies.

Last-Mile Simplification and Management

With its own network assets and global carrier relationships, we can aggregate the sourcing and management of a multi-carrier last-mile network, helping organizations simplify implementation and network management for their SD-WAN environments.

Managed Network Services

ViewQwest has helped enterprises transition from their traditional MPLS networks to SD-WAN from detailed planning, design and implementation, to network monitoring and optimization, and proactive resolution of issues.

IDC Asia/Pacific
80 Anson Road
#38-00 Fuji Xerox Towers Singapore
079907
T 65.6226.0330

idc.com

@idc

About IDC

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

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Permissions: External Publication of IDC Information and Data

Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason. Email: ap_permissions@idc.com

IDC Doc #AP241229IB