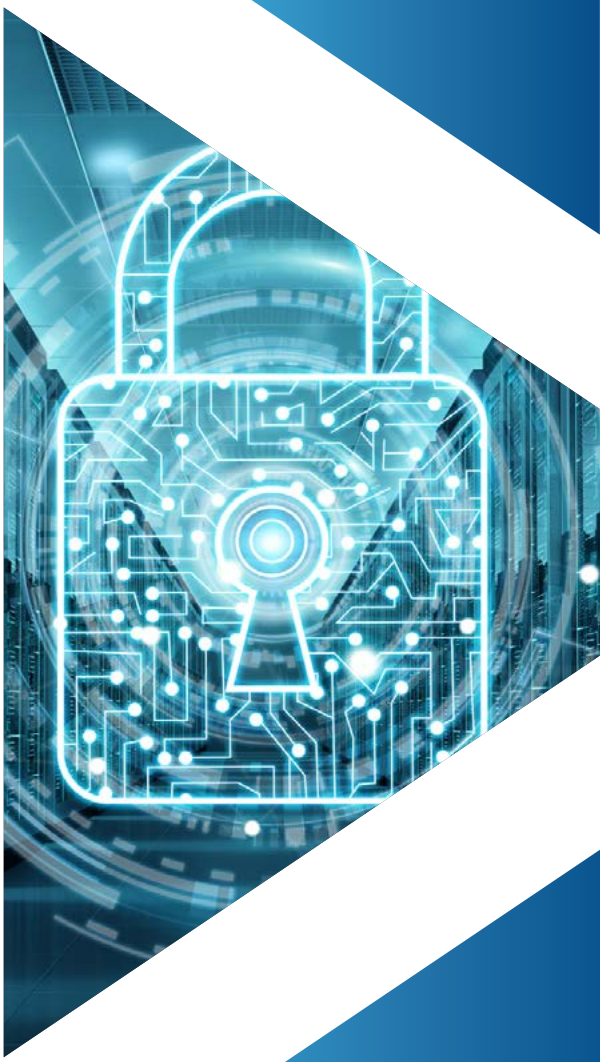
Powering clients to a future shaped by growth



A Frost & Sullivan White Paper

NETWORKING AND SECURITY ARE CONVERGING IN THE CLOUD: ARE YOU READY?

By: Roopa Honnachari, Industry Director,
Network Services & Edge Computing
Frost & Sullivan

FROST & SULLIVAN

Contents

Introduction

Cloud is front and center of businesses' digital transformation strategies, with adoption rates increasing for all types of clouds. In Frost & Sullivan's 2020 Global Cloud Survey, 52% of the respondents said they have deployed cloud infrastructure as a service (IaaS) and 42% said they currently use hybrid cloud. While cloud adoption continues to grow, enterprises have generally struggled to implement and maintain a secure, high-performing wide area network (WAN) that allows for efficient access to cloud-based applications across their user base. In traditional networks such as MPLS, branch network traffic is still routed via headquarters or hub locations to ensure data security and compliance, thus adding delays and potential jitter and packet drops. Software-defined wide area network (SD-WAN) solutions automate the process of network selection and put traffic steering control in the hands of an organization's network administrators to do direct internet breakout to cloud-based applications.

The power of cloud and connectivity became especially apparent during the first weeks of the COVID-19 pandemic when global organizations had to quickly transition the majority of their workforce (wherever applicable) to a remote working environment. With businesses across industries embracing the public cloud to host key applications, and with advances in residential broadband and wireless speeds, remote workers can access most enterprise applications from home. While cloud has disrupted enterprise IT application deployment models, COVID-19 is disrupting how these applications are accessed. In a recent FlexJobs survey, 65% of respondents report wanting to be full-time remote employees post-pandemic, and 31% want a hybrid remote work environment, resulting in 96% who desire some form of remote work.

If one considers the distributed nature of enterprise applications, and now the increasingly distributed nature of employees working from home, the traditional branch networking method of backhauling traffic (from users and devices) to a centralized location is highly inefficient. Frost & Sullivan believes SD-WAN edge devices (physical and virtual) that can be easily deployed and centrally orchestrated wherever needed (at the branch, in the cloud, or any edge locations) will play an even more critical role in enterprise WANs, as remote working becomes the new normal.

However, the rise in remote working and distributed users accessing cloud-hosted applications means that the enterprise perimeter is no longer limited to the company's base. Think about it: if your applications are in the cloud, and the users are at home or at a branch location (spread across the globe), why is your organization's security sitting at the headquarters location? The traditional model is time-consuming and inefficient, to say the least. Secure Access Service Edge, or SASE, aims to address the need for centralized, software-defined security architecture when the apps and users are highly distributed. SASE combines the flexibility of SD-WAN with a full suite of virtual security services, all delivered from the cloud.

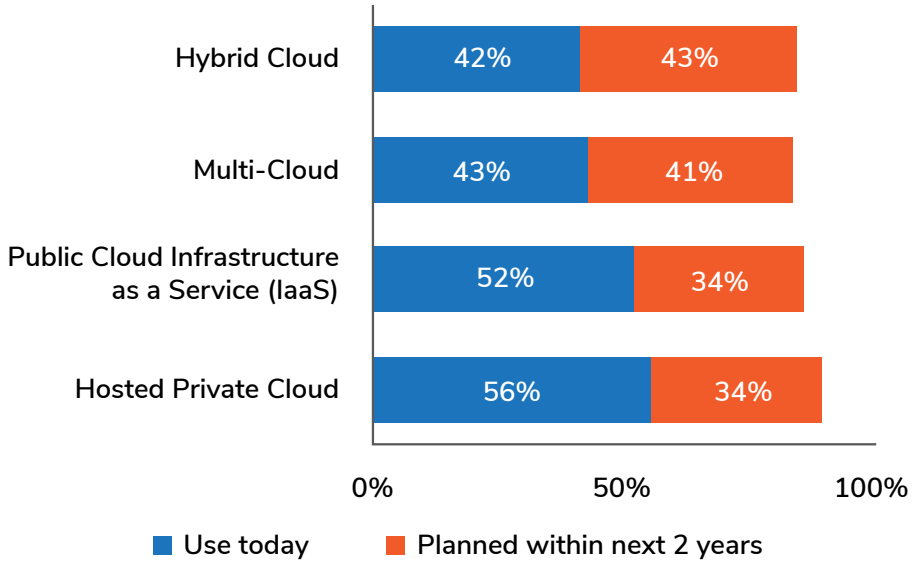
In this white paper, Frost & Sullivan discusses the market and technology trends driving the need for SASE, the power of SD-WAN and security together, and the value proposition of VMware's cloud-delivered, gateway-centric approach to SD-WAN that offers a superior SASE solution for global businesses.

The Business Case for SASE

Support Enterprise Cloud Networking

Cloud-based solutions have made significant inroads into enterprise IT architectures. In fact, most organizations are taking a cloud-first approach to any IT solutions before considering other options. Frost & Sullivan's 2020 cloud survey results indicate that globally, enterprises are evenly split between software applications deployed in the cloud and organization-managed infrastructure (e.g., on-premises data center, edge/branch, co-location). Exhibit 1 shows the various infrastructure models that businesses currently use or plan to use in the next 2 years.

Exhibit 1 Infrastructure Models Businesses Currenlty Use and Plan to Use



Source: 2020 Frost & Sullivan Global End-user Survey

SD-WAN technology automates the network selection process (based on pre-defined business policies) to enable businesses to use public and private network links effectively. This allows users to connect to cloud applications over the internet directly. However, best-effort internet links present inherent security risks and make it challenging for IT teams to ensure network and application security. While most security functions traditionally have resided in the enterprise data center because that is where most of the applications resided, the increasing adoption of cloud is dictating the need to deploy and deliver security functions in the cloud. In the cloud survey, 48% of IT decision makers stated that they decided to repatriate applications from public cloud after experiencing security incidents (e.g., unauthorized access). That is a staggering percentage, and the entire cloud model will be unsustainable in the long run if cloud, network, and security planning is not done holistically.

The Rise in Remote Working

Pre-COVID-19, enterprise IT teams had to deal with a limited percentage of remote and mobile workers in terms of ensuring secure access to enterprise applications. COVID-19 completely disrupted that model as most enterprise workers transitioned to a remote working environment. A year after the global pandemic was declared, most businesses have continued to support remote working for a majority of their employees. Frost & Sullivan predicts that the lessons learned from the pandemic, combined with the benefits of sourcing talent and resources based on qualifications without location limitations, and businesses' cost savings from less office infrastructure will make remote working a fixture across industries.

As working from home becomes prevalent it is critical for businesses to optimize and secure user connectivity to cloud-based applications. Considering that many remote workers depend upon a single residential broadband link at their home, SD-WAN can bring tremendous value to users by optimizing the link through continuous monitoring and traffic steering features. Users with company-provided mobile devices can add their wireless 4G/LTE links to SD-WAN to aggregate available bandwidth. However, extending secure access to remote users on broadband links (which are inherently prone to security risks) and ensuring identity and device-based access permissions is a huge challenge for enterprise IT teams.

Support the Growth in Edge Locations: Branches, Remote and Mobile Worker, Internet of Things

While cloud adoption has been growing in enterprise IT architecture, something very different from the cloud has been gaining traction as a parallel trend: edge computing. The term "edge computing" refers to pushing intelligence, data processing, analytics, and communication capabilities down to where the data originates, that is, at network gateways or directly at the endpoints. By bringing computing closer to the data source, edge computing enables latency-sensitive computing, offers greater business agility through better control and faster insights, lowers operating expenses, and results in more efficient network bandwidth support.

"Edge" can refer to a device (such as an Internet of Things node, a mobile device), or a location (such as a branch location, home office, or a carrier point of presence [PoP]) that combines compute and network resources. However, in most edge deployments, while the data processing happens locally, edge locations often connect to cloud-hosted applications. Cloud is typically where data is aggregated from multiple sources and integrated with the latest analytics and machine learning software to relay back instructions to edge devices. In short, the edge locations are further expanding the enterprise perimeter for security risks as the data is stored and processed across a much broader array of systems. For example, data from wearable sensors for remote health monitoring is collected and processed locally at an edge location before the aggregated data is sent to cloud for storage and securely accessed by healthcare professionals. The growth in edge locations is driving the need to optimize and securely connect these edge locations back to data centers and cloud-hosted applications.

The Power of SD-WAN and Security Together

SD-WAN Brings Virtualization to WAN

In today's distributed, cloud-centric world, SD-WAN has revolutionized the enterprise WAN by bringing much-needed agility to the otherwise static and inflexible traditional hub-and-spoke networking architecture for branch site connectivity. An SD-WAN architecture uses software-defined networking (SDN) principles to separate the data plane from the control plane in the WAN. It abstracts the underlying transport networks (including MPLS, Ethernet, wireless, and satellite) and shifts control intelligence from customer premises equipment (CPE) or edge devices into a centralized, software-based controller. A graphical user interface (GUI)-based management platform allows network administrators to define application-specific business policies that the controller translates into routing policies enforced in the edge devices.

The ability to use public and private networks in a hybrid WAN and make real-time changes to routing based on predefined policies is of value to enterprises. SD-WAN solutions offer businesses the choice to connect to cloud-based applications directly over internet links. For example, while MPLS could be the right choice to connect to an enterprise resource planning application in a hosted private cloud (for reasons of security and compliance), internet links could suffice for accessing a less-critical software-as-a-service (SaaS) application.

If Networking Can Be Software-Defined, Why Not Security?

While the WAN is evolving to a software-centric approach to support distributed users and applications, security has largely remained centralized. Traditional infrastructure-based security is not sufficient when applications are deployed across multiple clouds. Frost & Sullivan believes the right approach is to apply security profiles at the user and application level rather than the infrastructure level. To mitigate business risk and protect digital assets, organizations should address security holistically so that it can be automatically applied based on the user or device

identity and context while accessing enterprise applications. With the application awareness facilitating granular and dynamic network routing decisions, SD-WAN leverages this same awareness to follow a security model where security features and policies are provisioned at an application level. The potential benefits of an application-granular security model are numerous:

• Security policies are simplified and the potential of policy conflict is minimal, reducing instances in which one policy partially or fully negates the security objective of another. Security policies are applied consistently across different applications to ensure that when a user downloads a file from an SaaS application or an email attachment it is not exposed to security threats.

• With an application-specific set of features and policies, behavioral anomaly detection becomes more precise (less noisy), which not only improves security assurance but also reduces security analyst time in incident investigation and response (fewer incidents to investigate).

• As malware threats mutate, or as newer security encryptions get integrated into applications, companies do not need to invest in more appliances since the cloud characteristics of security can adapt to the threat landscape or business needs.

• With security features and policies automatically provisioned with each application, manual effort is minimized (reducing time and administrative error); scalability in security operations gets a boost; and the top security talent can shift time and energy from mundane operational tasks to strategic endeavors (optimizing scarce resources).

With SASE, Both Network and Security are Software-Defined

SASE combines network and security functions in one framework that is software-defined and delivered from the cloud through distributed SASE PoPs. Users and devices connect to the nearest SASE PoP (deployed in on-premises or third-party data centers, network PoPs, security PoPs, or cloud PoPs), which determines the optimal routing and security policies for the endpoint trying to access cloud (IaaS, SaaS, and platform-as-a-service) applications. The routing and security policies for each application are based on the identity of the entity, real-time context, enterprise security/compliance policies, and continuous assessment of risk/trust throughout the sessions. While the aim of SASE is to deliver a comprehensive set of security services (typically deployed on-premises on a physical appliance at enterprise data centers) virtually from the cloud, the critical components included are shown in Exhibit 2.

Exhibit 2: SASE Components

SD-WAN	Zero Trust Network Access (ZTNA)	Cloud Web Security	Next-Generation Firewall (NGFW)
• An SD-WAN architecture uses SDN principles to separate the data plane from the control plane in the WAN. It abstracts the underlying transport networks (MPLS, Ethernet, wireless, satellite) and shifts control intelligence from CPE or edge devices into a centralized, software-based controller. • SD-WAN functionality is enabled by deploying physical or virtual CPEs at customer sites or in the cloud, which makes it uniquely suited to combine routing and security at the edge. • Network administrators can centrally define application-specific business policies, which the controller translates into routing policies enforced in the edge devices.	• ZTNA is an overall strategy and framework to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network. • With ZTNA, the network can make access decisions based on user identity and context. These attributes include role, location, device type, and security posture, instead of just looking up an IP address. • Each user is mapped to a per-application policy that applies no matter where that application is hosted. There is a single set of policies for every user.	• This includes secure web gateway (SWG) and cloud access service broker (CASB). • SWGs serve as barriers between internet traffic and the organization's network, blocking suspicious or unknown data and allowing trusted and approved data to move smoothly in and out. • CASB is software that acts as a security control point between users and cloud services. While CASB began as a way to detect shadow IT practices, it has since grown to include more functionality for visibility, compliance, data security, and threat protection. • CASB offers additional layers of protection via malware protection and data encryption.	• NGFWs perform a range of security functions, including stateful packet filtering, virtual private networking (VPN), application visibility/control, user identity-based control, intrusion detection/prevention, gateway anti-virus, URL filtering, anti-spam, data leakage prevention, and advanced malware sandbox inspections.

SASE can help enterprise IT teams to programmatically right-size their security features and policies to each business application, scale their administration, improve security efficacy, and even bend the trend line on their security expenditures (particularly on the operational side). With SASE, all networking and security oversight for the distributed locations is orchestrated through a centralized controller. Due to the software-defined, cloud-delivered model of SASE, there is zero-touch involvement by branch personnel, network and security administration is highly scalable, and features and policies are uniformly defined and applied across all locations.

VMWARE SASE Solution: Delivering Cloud-Centric Networking And Security

The VMware SASE platform builds on its cloud-delivered SD-WAN solution that consists of VMware SD-WAN Edge devices, VMware SD-WAN Gateways, and the VMware SD-WAN Orchestrator. While the edge device and the orchestrator are typical of most SD-WAN solutions, VMware Gateways are unique to the company and enables it to rapidly roll out global SASE PoPs.

Expansive Global SASE Pops

VMware's network of PoPs consists of more than 3,000 stateless, horizontally scalable Gateways hosted in it. Each of these PoPs will combine networking (SD-WAN) and security functions to act as a SASE PoP. The globally distributed PoPs dramatically bridge the gap between users and cloud-based applications, and consist of a rich ecosystem of partners that include:

- Leading cloud IaaS providers (e.g., Azure cloud)
- SaaS clouds (e.g., Microsoft Office365)
- Security clouds (e.g., Zscaler cloud)
- Telco clouds (e.g., AT&T MPLS PoPs)
- Network exchanges (e.g., Equinix)

Since the entire value proposition of SASE is to deliver networking and security functions in a cloud model and closer to the user, the diversity of partners hosting SASE PoPs ensures that users have optimized and secure connectivity no matter where they are located or what applications they are trying to access.

Centrally Orchestrated, Intrinsic Security

VMware SASE PoPs offer intrinsic networking and security components that can help an organization protect users, applications, data, and networks through a single management interface. VMware SASE cloud security includes the following components:

- VMware Secure Access combines ZTNA with VMware Workspace ONE to deliver consistent security and quality of service policies across various endpoints: mobile clients, branches, and campuses.
- Cloud Web Security includes SWG, CASB, data loss prevention, sandbox, SSL traffic inspection, and remote browser isolation functions. The SWG technology comes integrated with the VMware

SD-WAN Orchestrator to enable network administrators to centrally define and apply security features across all locations. VMware also has a strong partnership with Zscaler and other security vendors to support best-of-breed security providers.

• VMware SD-WAN Gateways offer optimized paths for users trying to access cloud IaaS and SaaS applications. Gateways are at major geographic POP locations around the world, eliminating the need to backhaul traffic to the data center. The SD-WAN Gateway architecture eliminates the need for multiple manual VPNs to be set up between branch sites and the cloud, as the gateway acts as a VPN concentrator to create a single VPN from the branch to the cloud.

• Firewall includes VMware NSX NGFW, intrusion prevention system, and intrusion detection system features.

Operational Simplicity Through Edge Network Intelligence

As enterprise users and devices continue to be distributed, the biggest challenge for IT teams is the lack of visibility into endpoints to detect, analyze, and remediate network operations. The complexity of network management will be even more pronounced as the remote working continues and the number of Internet of Things devices increases. The concept of self-healing WAN has been at the core of SD-WAN discussion since its inception because of its SDN roots. Vendors and providers alike are investing and integrating artificial intelligence (AI) and machine learning tools to deliver on the promise of application-aware or intent-based networking to automate routine network operational tasks, set policies, measure network performance against set targets, and respond to and rectify the networks as needed.

VMware Edge Network Intelligence is a vendor-agnostic AIOps solution that employs machine learning algorithms and big data analytics to process high volumes of data from a wide range of network, device, and application sources at the Gateways. The AIOps solution can pinpoint with clarity whether a perceived application problem is due to issues with the local Wi-Fi network, broadband network, WAN, network services, or application. This greatly simplifies network operations and management for the IT teams. While the solution available today is capable of predicting and notifying IT staff of events, plans include incorporating robotic process automation to eliminate manual intervention, and instead have the WAN self-correct.

Built-In Resiliency To Ensure Business Continuity

The cloud-delivered infrastructure of VMware SASE PoPs is backed by a 99.99% uptime service-level agreement and 24x7 automated failure detection to ensure reliable and secure WAN connectivity for an organization. VMware SD-WAN Gateways are distributed across VMware and its partner PoPs in active-active mode, offering inherent resiliency in that each SD-WAN site is assigned to primary and backup SD-WAN Gateways and Orchestrators . If the primary SD-WAN Gateway fails, the traffic is automatically rerouted to the backup SD-WAN Gateway. Similarly, if the primary VMware SD-WAN Orchestrator fails, the customer can simply log on to the backup Orchestrator.

The Last Word

With the arrival of SD-WAN, organizations are finally able to transform their WANs to keep up with IT transformation initiatives, which are heavily cloud-centric. However, security planning is most often done separately, thus derailing network and IT initiatives. More organizations are realizing that for their digital transformation plans to succeed, holistic thinking about networking, security, and cloud deployments is required. SASE addresses this requirement. For an organization to reap the full benefits of SASE, the scale of SASE PoPs, the breadth and depth of security functions, and the ability of the SD-WAN provider to orchestrate and administer network and security policies centrally are all important factors to consider. VMware, with its market-leading SD-WAN solution combined with the global reach of SASE PoPs and deep data analytics and intelligent network management features, could be a vendor of choice.

To learn more about the VMware SASE solution, visit: https://sdwan.vmware.com/secure-access-service-edge.

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?