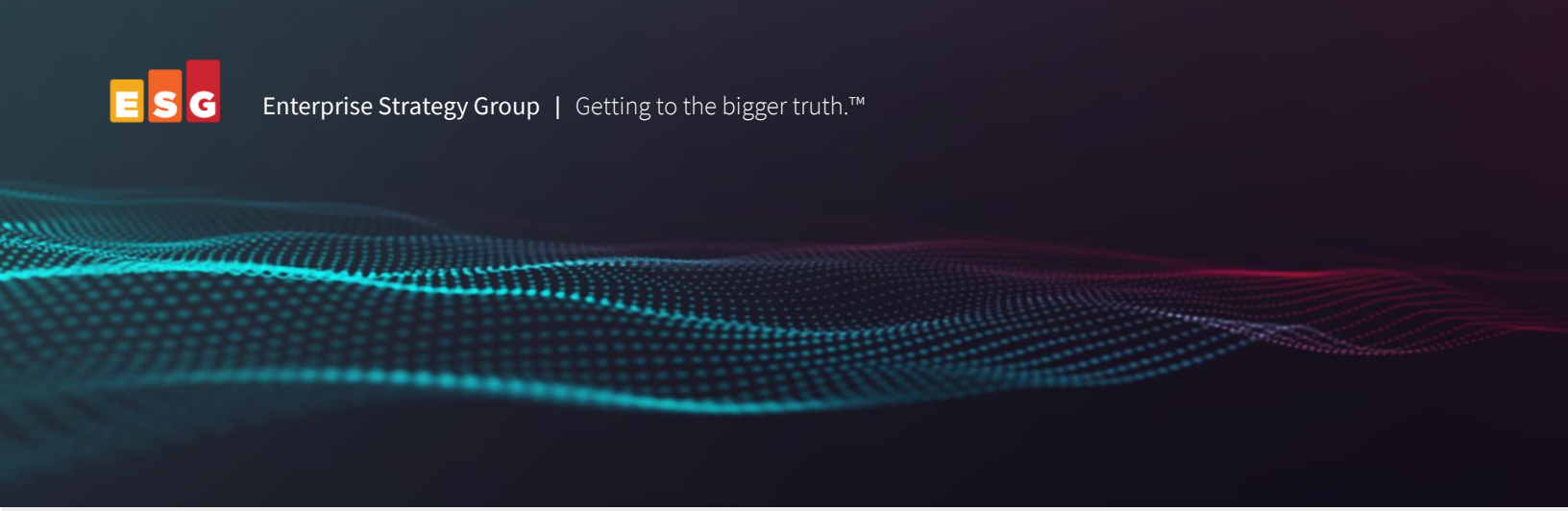

ESG WHITE PAPER

Dell Technologies: The Foundation for a Flexible SASE Journey

Improving Operational Efficiency, Decreasing Risk, and Reducing Costs

By Bob Laliberte, ESG Senior Analyst; and Leah Matuson, Research Analyst

April 2021

This ESG White Paper was commissioned by Dell Technologies and is distributed under license from ESG.

Contents

Introduction

To better support highly distributed, modern environments, organizations are becoming increasingly aware of the need to converge network and security functionality. With a rapidly growing number of applications distributed across private data centers, multiple public clouds, and edge locations—and more employees working remotely than ever before—the need for reliable, secure connectivity is at an all-time high.

Network and Security are Converging

Highly distributed application and employee environments are accelerating digital transformation initiatives across virtually all industries and driving greater adoption of cloud-based applications.

In fact, according to ESG research, 24% of organizations believe that one of the most significant lasting changes of the current COVID-19 business disruption on their longer-term IT strategy will be the increased adoption of cloud applications.[1] Additionally, nearly half (45%) of respondents report that their organizations now have a cloud-first strategy for deploying new applications, up from 38% last year. Further, an overwhelming majority (97%) of companies currently allow for some remote work, while 72% indicate that they are moving to a more pro-remote work mindset. As a result, the IT environment has become far more complex.

According to ESG research, three-quarters (75%) of respondents indicate that IT has become more or significantly more complex than just two years ago. But what is driving this complexity? Top drivers include an increase in remote workers (49%), new data security and privacy regulations (38%), and higher data volumes (38%).

What's more, network security at the edge has become harder. Based on ESG research, 64% of respondents cite that network security is somewhat or much more difficult at the edge than it was two years ago, with data indicating even higher percentages for those that found it much more difficult for more distributed environments incorporating public clouds, remote offices, and roaming or remote users.[2] This results in an increased attack surface that organizations have to defend.

As a result of the increased levels of complexity and need for secure connectivity, new frameworks are being recommended for organizations to consider the convergence of network and security functionality as a viable solution. Enter secure access service edge (SASE).

What is Secure Access Service Edge (SASE)

A number of different terms have been used to describe the convergence of networking and security, including elastic cloud gateway (ECG), zero-trust network access (ZTNA), and secure access service edge (SASE). However, the one that has gained the most traction to date is SASE. It has essentially become the de facto naming convention that represents the convergence of networking and security services.

But what exactly is SASE and what does it provide?

SASE is a framework that outlines both the network and security capabilities required for managing highly distributed environments (i.e., on-premises, hybrid cloud, remote, edge, and remote worker environments). These functions are typically delivered as a cloud service, but will usually require a hardware platform to deploy any required on- premises software or virtual functionality (SD-WAN, FW, etc.). The goal of frameworks like SASE is to help ensure reliable, centralized,

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020. All ESG research references in this white paper have been taken from this master survey results set unless otherwise noted.

[2] Source: ESG Research Report, *Transitioning Network Security Controls to the Cloud*, August 2020.

policy-based management, and provide organizations with the ability to easily scale to meet the quickly changing demands of the business or macro environment. The key components include:

- Security functionality. This includes cloud-based capabilities such as next-generation firewalls as a service (NGFWaaS); zero-trust network access (ZTNA; secure web gateways (SWG); cloud access security brokers (CASB); and remote browser isolation (RBI) services, web application and API protection (WAAPaaS) and domain name system (DNS), and is typically delivered from a centrally managed cloud console.

- Network functionality. This functionality includes SD-WAN; network-as-a-service (NaaS); service provider links; broadband links; WAN optimization, CDNs and Carrier networks.

The reality is that many organizations may already employ one or more of these technologies in their environment and SASE provides a framework to illustrate the need to converge networks and security for highly distributed environments.

Choices for Deploying SASE Solutions

Because the SASE framework encompasses so many different capabilities, finding a single vendor that can provide a complete, fully integrated SASE solution today can be difficult. With that in mind, organizations have two choices: work with a single vendor with a portfolio of its own solutions or take a best-of-breed approach. The two strategies are highlighted below:

1. Working with a single vendor may provide more functionality under the same roof, but it also means being locked into that vendor and solely relying on them to provide all capabilities. This could also mean higher costs over time as you have committed to this vendor and their roadmap. Ultimately, a solution like this should have a single central console to manage all solutions from.

2. Utilizing a best-of-breed strategy enables organizations to leverage different vendors to deliver the requisite functionality. This approach ensures best in class technology and will help to keep costs in line. However, this level of flexibility may require IT staff to spend the time to monitor and manage these separate solutions or integrate them.

But before organizations can reasonably choose which path they should pursue in building out a SASE solution, it's imperative to understand the existing environment and determine the appropriate criteria for selecting a SASE solution that will fit their unique business needs now—and in the future.

Selecting a Comprehensive SASE Solution

Use the following criteria as a guide to selecting the right SASE solution. Consider the following:

- Standardized hardware. Organizations should use a proven, universal hardware platform to ensure consistency across all sites that require hardware and the capability to deliver the requisite performance, scale, and reliability. This includes hosting all virtual network functions as well as potentially custom business applications. Taking a best-of-breed approach may require deploying different appliances or a rip and replace if changing vendors.

- Existing capability. The solution should be able to work with or integrate with any existing security capabilities. As many organizations already have solutions in place, the ability to leverage those assets as others are added to fill out the framework will be important. This would minimize the need to rip and replace existing solutions.

- Global support to ensure that any potential issues will be rapidly addressed before becoming urgent network or security problems than can negatively affect productivity, security, user experience, and the business.
- Flexibility to select the best-of-breed solutions for specific business needs. As this space evolves and functionality is delivered in the cloud, will organizations be able to choose the best solution for their environments? Or will they simply use what is included in the platform?
- Walk before you run. Organizations should be realistic about getting started with SASE. Do they need to deploy every piece of functionality at once? How much new technology can the organization realistically absorb? Organizations should consider getting started with just one or two functions and expand over time.
- Leverage experts to help get started. Organizations should work with a trusted partner throughout the SASE journey that can provide support, services, and an ecosystem of partners.

Dell Technologies Delivers a Flexible Approach to SASE

A trusted technology leader for decades, Dell Technologies has been providing customers with innovative products and services, helping them navigate a maze of complex technologies and dynamic markets. Dell Technologies offers flexibility and freedom of choice in how organizations interact and consume technology.

Leveraging a growing ecosystem of networking, security, and managed services partners, Dell Technologies offers a flexible approach to SASE, enabling organizations to build and scale secure, global connectivity. This ecosystem includes:

Dell's Virtual Edge Platform (VEP)

Dell Technologies Virtual Edge Platform (VEP) accelerates network transformation, enabling organizations to modernize and secure wide area networks (WAN). Built on a standards-based hardware platform, Dell VEP enables organizations to seamlessly integrate virtualized network or security functions or existing infrastructure. This allows organizations to future-proof their investment, enabling them to implement new technology/add new virtualized functions without having to make major changes to existing IT infrastructure (saving time, resources, and expense). The solution provides peace of mind for enterprises, as the technology has been fully proven and tested in demanding Telco environments and is backed by Dell Technologies global support, services, and supply chain.

Dell Technologies Networking Partners

Dell Technologies offers customers proven enterprise SD-WAN solutions from trusted networking partners and provides a variety of managed network services through its extensive partner network.

Dell Technologies Network Partners include the following vendors:

VMware SD-WAN

VMware SD-WAN simplifies deployments and WAN operations, ensuring reliability, improved application performance, and ease of cloud adoption. The solution is comprised of SD-WAN Edges, over 130 cloud Gateways, and an Orchestrator to optimize connectivity from branch offices (including remote and work-from-home locations) to cloud providers, data centers, and other branch offices. It enables organizations to optimize application traffic over MPLS, broadband, or cellular service.

Versa SD-WAN

Versa SD-WAN was built from the ground up based on the vendor's security and network software. Leveraging the Versa operating system (VOS), using Versa's Single-Pass Parallel Processing Architecture, the Versa Director, and Versa Analytics, organizations can reduce WAN connectivity costs and branch network expenses (integrating Internet, LTE, and broadband alongside MPLS), as well as decrease the time and resources required to securely manage the network, (e.g., scale capacity, provision new branches, add new security and network functionality, etc.). This includes the ability to leverage zero-touch provisioning and Versa security offerings.

Dell Technologies Security Partners

Dell Technologies partners with leading security providers to streamline deployment and mitigate risk, while protecting business-critical and confidential data across an organization's infrastructure, devices, services, and supply chain.

Dell Technologies Security Partners include the following vendors:

SonicWall. SonicWall offers next-generation firewall capabilities. The NSv series firewalls provides next-generation cloud security for organizations deploying hybrid and multi-cloud environments. Leveraging SonicOSX, organizations have centralized policy control and end-to-end visibility. SonicWall's real-time deep memory inspection (RTDMI) technology ensures threats and malware are proactively blocked.

Versa Networks. Versa offers SASE functionality, simplifying the deployment and operation of multiple security solutions by integrating network and security functionality into a single software stack. Versa offers cloud security, next-generation firewall, threat management, and role-based access control via a single management console that also includes its network management.

VMware. The VMware SASE Platform unites cloud networking, cloud security (secure web gateway, cloud access service broker (CASB), and remote browser isolation (RBI)), Layer 7 NSX service-defined firewalls, and zero-trust network access, providing organizations with agility, flexibility, and scalability. A cloud-first solution, VMware SASE offers application quality assurance, intrinsic security, and operational simplicity—answering the need for reliable support for massive numbers of staff working in remote locations and home offices.

Zscaler. Zscaler's SASE solution, the Zscaler Cloud Security Platform, offers organizations improved performance and scalability. With its cloud-first architecture, the SASE solution comprises Zscaler's Secure Web Gateway working in conjunction with VMware SD-WAN and VMware Secure Access. Zscaler's comprehensive portfolio of integrated security tools offers threat prevention, access control, and data protection, allowing customers to enjoy a total solution with trusted vendors.

Dell Technologies Service Capabilities

To help accelerate the journey to deploying SASE, Dell Technologies has a number of service offerings to ensure organizations maximize the value of their SASE deployments. They include:

Dell ProDeploy Enterprise Suite

Working with Dell Technologies and its trusted partner network, customers gain the benefit of working with experts through all aspects of deployment—from pre-deployment planning to configuration, to installation, knowledge transfer, and integration, to post-deployment. The ProDeploy Enterprise Suite enables organizations to accelerate the journey to a SASE framework specific to their environment. These deployment services are available today in 118 countries.

Dell ProSupport Enterprise Suite

Dell ProSupport with multivendor capabilities helps organizations improve productivity and efficiency and decrease costs, providing 24/7 assistance through certified hardware and software experts and collaborative support with third-party vendors. Dell ProSupport Suite covers hypervisor, operating environment software, and OS support, with onsite parts and labor response options that include next business day, or two-, four-, or eight-hour mission-critical.

Dell Managed Services Provider Partners

Dell Technologies' partners are able to offer these SD-WAN networking and security solutions as an end-to-end managed service. These partners will help reduce IT complexity, mitigate risk, and decrease costs, managing and optimizing an organization's security and WAN environment, including all ISP and cellular connections.

Dell Collaborative Support Model

Unlike many organizations that employ a tiered support model, Dell subscribes to a collaborative support model. To ensure issues are resolved quickly and efficiently, the collaborative approach is proactive and customer-focused. The process involves working with a number of support agents, teams, and even departments across ecosystem partners. By facilitating rapid, reliable support, they enhance the customer experience, building a reputation for dependable support, and enabling the development of a loyal base of satisfied customers now and into the future.

The Bigger Truth

The global pandemic is accelerating the shift of applications and workloads to the cloud and edge, while simultaneously enabling employees to work remotely. Work is what you do, not where you do it—and this worldwide scenario creates a highly distributed environment that must ensure secure connectivity from employees to applications.

Due to this large-scale change, the convergence of network and security is gaining momentum. The advent of cloud-based security capabilities is helping to change the paradigm that deploying more security would result in decreased network performance. The SASE framework has been created to educate users about the cloud-delivered capabilities necessary to deliver a secure access service edge—and there are a multitude of security and network vendors developing and supplying solutions.

As organizations begin their SASE journey, it is important they consider the most appropriate SASE approach to take, and then choose either a single vendor to work with or use best-of-breed solutions. Dell Technologies provides a tested and proven universal platform for organizations to build a best-of-breed approach to SASE, along with its expanding ecosystem of networking and security technology partners. Working with a collaborative support model and its own global support and services organizations, Dell Technologies is well suited—and ready—to help organizations accelerate the adoption of a flexible and best-of-breed converged network and security environment.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188