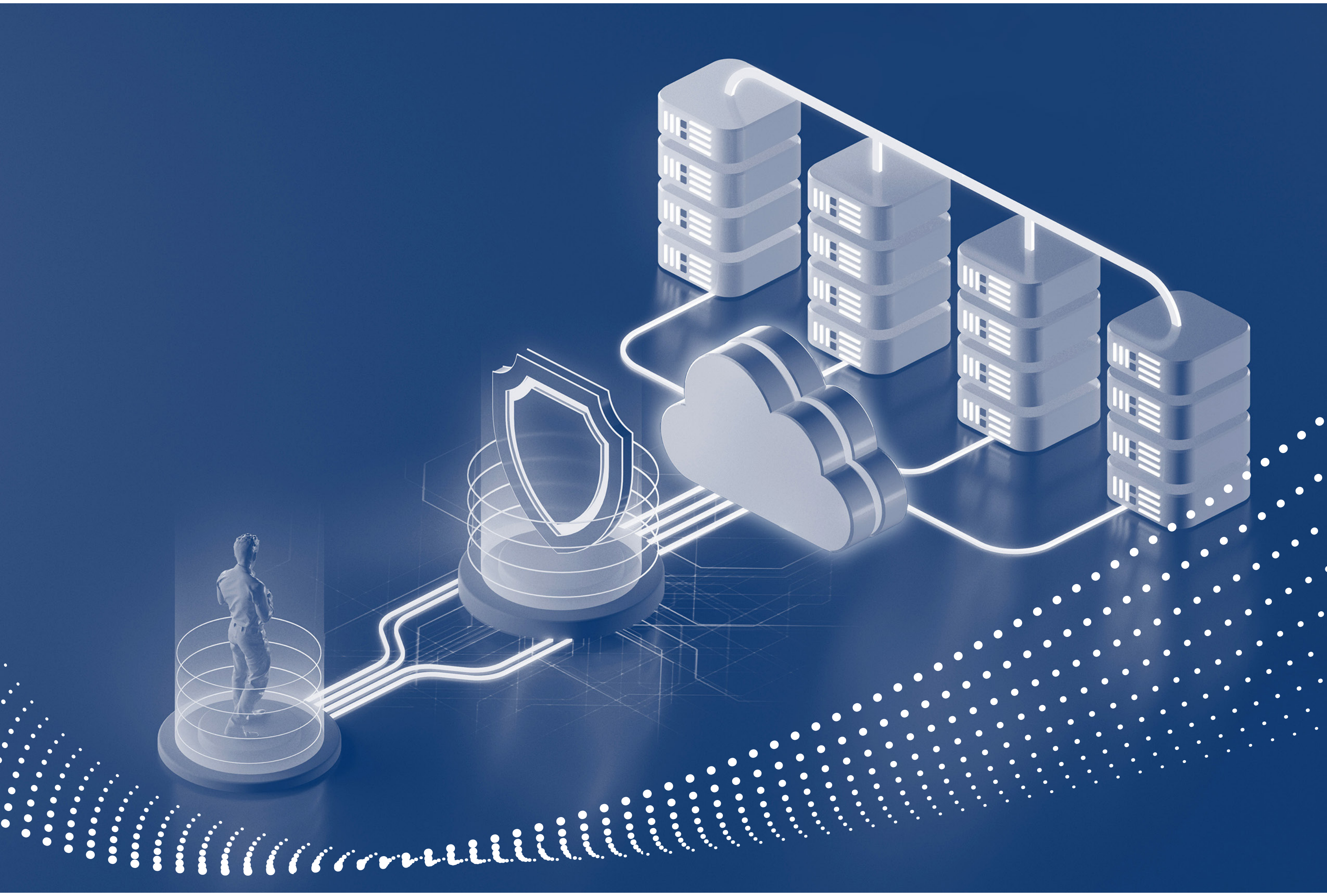
HughesON™

SD-WAN's New SASE ("Sassy") Friend



INTRODUCTION

Struggling with inconsistent connectivity across your branches or offices, and increased security risks with so many working from home? Learn how your enterprise can transform its networking digital operations.

Over the last several years, across all industries and types of enterprises, there has been a titanic shift away from traditional data centers to the Cloud. Then, there was the pandemic, which forced millions of employees to work from home and to struggle with accessing resources on their networks. Legacy security architectures simply aren't equipped to support this type of mass-scale remote work arrangement or to safeguard against growing threats.

That's because the old approach involved securing physical locations or access points along the network—an entirely insufficient option when there are seemingly endless numbers of devices and users needing secure network and cloud access.

A better solution is a security fabric that brokers identity-based control and context.

Enter SASE (pronounced "sassy") the acronym for Secure Access Service Edge. SASE is a relatively new concept promoted by Gartner that "combines network security functions with Wide Area Network (WAN) capabilities to support the dynamic secure access needs of organizations." While not a new technology, SASE integrates several existing security technologies and practices, and looks at deploying them primarily via the Cloud to create a new security framework. As Gartner explains, SASE can transform enterprise networking and security and "provide a holistic, agile, and adaptable service to the digital business." In this e-book, we'll explore the many attributes of this promising approach.

SASE Meets SD-WAN

Imagine marrying SASE's improved security architecture with the benefits of a Software Defined WAN (SD-WAN). There are a few different ways in which SASE and an SD-WAN solution work better together. The first is by ensuring that security envelopes the network, expanding network protection to cover any access or endpoint. This secures each device and user rather than just points along the network itself.

Another way is by facilitating the network through a "Cloud-native" environment—one which supports all apps, but especially those that are built in, run from, and reside in the Cloud. Having the Cloud as a host adds both flexibility and the type of robust security processing (and updating) required by networks today. Combining this with a secure SD-WAN network that successfully deploys the latest firewall, intrusion detection, and virus/ransomware alert technologies provides increased control to augment the access and resource controls offered by SASE.

SASE essentially combines the mobile, cloud, and site access capabilities into a single service, reducing network threats from remote employees and meeting the needs of the enterprise. Together, SASE and an SD-WAN solution provide the reliably secure connectivity and service level assurance that applications, devices, and users expect.

Today, however, for most enterprise networks, security and connectivity operate largely independent of one another. They are usually premise-based. Even with an SD-WAN solution, the buying decisions still happen separately from each other. Yet secure access and stable connectivity are essential for every enterprise. For true digital transformation to occur—where users and endpoints alike are able to connect to networked resources, no matter where and when they need it—both must be addressed in tandem. To address how such convergence can happen effectively, let's first look at the issues of security and of connectivity, then we'll look at both holistically.

Security and the Issue of Exploding Endpoints

With more remote users and mobile devices (or endpoints), networks become more vulnerable to sophisticated and targeted cyber-attacks, such as ransomware. But endpoint risk isn't just limited by the number of users on the network. The Internet of Things (IoT) compounds the challenge. IoT includes all the smart devices or machines on a network, like thermostats, heat pumps, refrigerators, flood sensors, security cameras, healthcare equipment, wearables, emergency monitoring, and management tools, and so much more. Collectively, these users and endpoints comprise (and increase) the "attack surface." One approach for reducing risk associated with a growing attack surface that has gained prominence over the past few years is the "Zero Trust" Model, which maintains that organizations should not automatically trust anything just because it originates from inside their network perimeter or is a known end device. While the Zero Trust Model has been around since 2010, its rise is due to advances in the technology that make it easier to deploy and scale and its strength in bolstering security and stopping data breaches.

Leveraging the Zero Trust Model

SASE depends on a centralized security broker to provide the visibility, policy framework, management structures, and service level agreements necessary to effectively execute endpoint access, security, and control measures. This varies from the more typical approach in which any authenticated device “inside” the network is deemed to be a trusted device. Under this scenario, if a hacker attacks and hijacks a device on the network, the network is vulnerable from this insider attack.

Zero Trust models assume that no request can be trusted automatically. In this way, when Zero Trust is applied to a SASE framework, every access request is verified before permission is granted, no matter where that request comes from. With SASE incorporating a Zero Trust approach, the security fabric between users and resources tightens and reduces the attack surface. The result? Significantly decreased risk and heightened security across the entire enterprise network—regardless of how many endpoints or how distributed it may be.

Identity-based Control and Context

Other factors that enterprises must consider are the risks associated with the shift to a cloud environment, largely driven by Software as a Service (SaaS). Because SaaS gives customers access to their enterprise applications over the Internet, rather than having software be hosted at a data center or installed across network devices, applications can be built, maintained, and updated automatically in the Cloud. While SaaS provides flexibility, it expands the network attack surface since provider locations are not under enterprise control. That causes challenges for existing or legacy network protections to provide adequate security coverage.

That’s where SASE comes in. SASE protects against this explosion of network entry points, even when they are not controlled by the enterprise. SASE provides the security fabric that enables identity-based control and context, where the identity is associated to users or user groups. This allows for the granting of access to all employees or even access based on roles, or by the creation of sub-groups for specific teams or by management level.

An identity-based approach can also be set by type of device, including IoT and mobile devices. This includes being able to limit system access to only approved devices and setting roles for “non-human” users, for those networks involving machine-to-machine connectivity requiring little to no human input.

With SASE, all of these endpoints that interact with various network resources and SaaS applications, public and private cloud resources, data centers, and others (like vendor and partner resources) are authenticated and secured within the context of that particular access or communication request. Requests can also be set based on other parameters, such as enterprise policies for governance, geo location, and time of day.

The Need for Connectivity to Everything, Everywhere

With COVID-19, we've seen how indispensable the network is for enabling an enterprise to remain operational and connected to employees, customers, constituents, vendors, and partners. Applications and devices that are hosted by the network require a continuous, secure, and stable connection to maintain session integrity and functionality. Network users also expect a certain level of application performance and security so they can complete their tasks safely and efficiently. And we all expect ubiquitous coverage, wherever we are, all hours of the day (and night!) Failing to meet these types of expectations creates significant dissatisfaction in the user experience.

Continuous, Robust Connectivity

Within standard network architectures, having control and visibility into the devices and systems on a network are critical—and equally dependent on robust connectivity. Issues of reliability and security cannot be allowed to hamper monitoring, productivity, or mobility. This holds true when considering SASE; seamless connectivity is simply a must to securely envelope all users and devices along an entire network.

Achieving and maintaining such connectivity is one of the benefits of implementing a strong SD-WAN solution; one that optimizes application performance and uptime in spite of whether the network has vastly different broadband access types and infrastructures (which is commonly found in distributed enterprises). The fact is, despite the continued growth in broadband availability, speed, coverage, and quality, all still vary considerably based on geography and infrastructure capability. This is especially true for branch or office locations in exurban areas. It's SD-WAN that can enable the continuous and robust connectivity to support a distributed environment—connecting everything, everywhere.

When Security and Connectivity Converge

So, what does all of this mean for an enterprise?

Because SD-WAN is “the foundation that SASE is built upon,” according to SDX Central, integrating the two and making holistic buying decisions better ensures an end-to-end approach to optimized security and connectivity. Because SASE is a Cloud-based approach, the security fabric can be scaled up or down based on need; enhanced or upgraded with additional feature-rich functionality; and expanded to accommodate an ever-growing network perimeter.

Here are some examples, taken from use cases, to illustrate what it looks like for the enterprise and its users:

- A large enterprise has thousands of employees working from home, connecting with colleagues and customers via video conference calls to do their jobs.
- Users at a mid-sized healthcare organization access MS Office365 and the company’s medical records system and experience consistent application performance regardless of whether they are working at corporate headquarters or the branch office.
- An oil and gas company monitors a network of remote device sensors collecting and reporting data in a cost-efficient and secure manner, so they can guard against outages and protect public safety.
- A retailer establishes pop-up locations quickly and easily to mirror seasonal customer demand, all the while having secure access to its back-office and point-of-sale applications.

These are just a few examples of what becomes possible when security and connectivity converge, as they do when SASE and SD-WAN are integrated.

Deploying the Dynamic Duo

Deploying this dynamic duo can be a complex undertaking. Turning to an experienced Managed Service Provider (MSP) can reduce your risk, improve time to deployment, streamline the process, and ensure success.

Reduce Risk

An MSP can help to reduce your risk in a variety of ways. First, MSPs bring entire teams of experts to the task—not just a few IT professionals. These experts have deployed such technologies many times over, each time gaining insights and experiences to simplify and improve subsequent deployments. Second, MSPs specialize in operating networks to peak performance and efficiency, conforming to any required regulatory or compliance measures (e.g., PCI and HIPPA). Their efforts demand concrete and repeatable processes to support all aspects of implementation (including monitoring and updates). This leads to regular refinement and adoption of best practices and the employment of continuous improvement programs. Plus, their core business model is focused on keeping customer networks up and running smoothly. Consequently, MSPs are quick to identify and solve problems or challenges as they arise.

They are also expert at orchestrating and delivering security to the edge in a distributed world and to tens of thousands of sites. They have vast experience deploying different security architectures, and even hybrid architectures, blending premises, data center, and web/cloud-based security capabilities to achieve the critical level of access and network security demanded by SASE. MSPs have also been investing in the capabilities required to manage these multifaceted networks and security architectures effectively.

When viewed through the CFO lens, the monthly service plans that MSPs offer move much of the CAPEX to OPEX, providing predictable costs and fee structures—and the ability to avoid surprises or large sunken costs.

Improve Time to Deployment and Scalability

For the typical enterprise, deploying a complex SASE and SD-WAN solution can be resource intensive and result in unplanned delays and costs. That's because organizations may have separate IT and Security teams; and few of the teams are built to support large scale rollouts to hundreds, or even thousands of sites. It can also be difficult to anticipate (or staff for) every potential obstacle or problem. MSPs that have delivered these solutions to similar types of enterprises, however, are familiar with the challenges and best practices associated with such implementations. In addition, the larger MSPs have resources in most regions and states, enabling them to provide timely on-site support to any and all locations. Their depth of expertise and resources can address and overcome issues along the way, and their size and scale mean they can flex the delivery schedule to expedite deployment if needed. Another under-appreciated capability is the MSP's ability to slow a deployment when required without prompting additional costs or impacting the overall rollout plan.

Streamline the Process

As we noted, despite the continued growth in broadband availability, the speeds, coverage, and quality all vary considerably by location and provider. Combine that with the number of partners and resellers that deliver broadband—over 2,600 by last count—and it becomes clear that it is a herculean job to manage the dozens of vendors and hundreds of service level agreements and contracts typical for a large multi-regional or national deployment. It also requires significant time and technical effort.

Top MSPs, on the other hand, can mobilize a nationwide network of strong and established service provider relationships—partnerships that have been cultivated over many years. MSPs understand which vendors do the best job at bringing the connectivity where and when it's needed and how to make and secure a network that will operate as a homogenous system. Key to this is applying the right security, application performance, and network optimization techniques and policies to make sure each and every site delivers the same user experience as intended by the brand.

Lastly, MSPs have invested heavily to develop the tools and processes to integrate these partners into their service delivery model. This integration with each ISP's provisioning, help desk, billing, trouble ticketing, analytics and many other systems, can be built one time by an MSP and then leveraged across all of its service customers. Consequently, customers don't have to recreate these systems themselves, and don't have to add to them if they decide to switch to new providers in the future. All of that work and effort rests with the MSP. That's where an MSP can dramatically streamline and improve the implementation process and eliminate the headaches that an enterprise would otherwise have to tackle on their own to achieve similar service capabilities.

Ensure Success

The best MSP will partner with the IT department as well as the Security team, becoming an extension of both groups in a fully collaborative approach. The MSP provides particular expertise, tools and technologies to develop, maintain, and monitor the security and operation of a network and troubleshoot issues around the clock. It would be impossible for a single individual or set of small IT and Security teams to match the level of knowledge, skills, and resources that an MSP delivers in this specific area.

Yet a good MSP will work collaboratively with all internal departments to help develop the right solutions and policies to achieve specific goals. An example may involve helping internal teams to make the shift that's required away from focusing solely on connecting and securing devices, to managing users and user permissions to devices, resources, and data. Here, the MSP, IT, and Security teams must work closely together because each will have a different perspective required for success. For example, the MSP may understand how to implement the technologies cost-effectively, while the internal teams will better understand individual user needs, access requirements and how the workforce may be changing.

Other scenarios where MSPs can guide decisions involve scaling the solution or its offerings, adding new technologies and capabilities, or adapting to changes in the business environment, like we experienced as part of COVID-19. What is certain is that change will be required; having an agile and robust security and network foundation is critical to supporting whatever change may come.

The MSP service delivery model also fits well with SASE, which will open a world where services are defined, refined, and deployed on demand, allowing cost-efficiencies, scalability, and simplicity. As a result, MSPs will be poised to bring a variety of offerings to market to leverage both SASE and SD-WAN more fully. These elements add up to the ability to successfully create a customer network environment where users and endpoints alike can securely connect to networked resources, no matter where and when they may be.

For all of these reasons, an enterprise that has a high performing MSP to rely on as a partner will have little to worry about when it comes to deploying a complex solution like SASE paired with SD-WAN.

For additional information, please call 1-888-440-7126
or visit business.hughes.com.

HUGHES®
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

business.hughes.com