HUGHES Europe

WHAT IS SASE — AND WHY DO YOU NEED IT?

Optimised Network Performance & Security for the “Work from Anywhere” World

A HUGHES EUROPE GUIDE

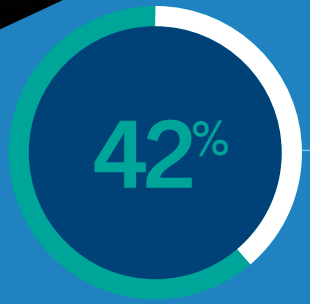
WHAT IS SASE?

The term Secure Access Service Edge, (abbreviated to SASE and pronounced “sassy”) was first coined by Gartner in 2019. According to Gartner, **“SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices, applications, services, IoT systems or edge computing locations.”**

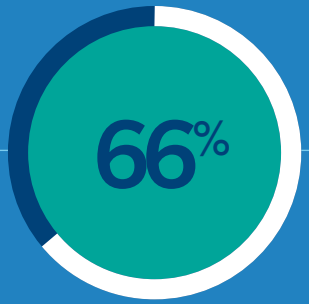
SASE moves the control of network security to the network edge, thereby enhancing security in today’s distributed network without compromising network performance. SASE allows organisations to apply secure access no matter where their users, applications or devices are located.

Today, **Hughes Managed SASE** combines SD-WAN, secure network access, and cloud-delivered security to provide secure, optimised, and reliable access to modern applications for branch office, home office, and remote workers.

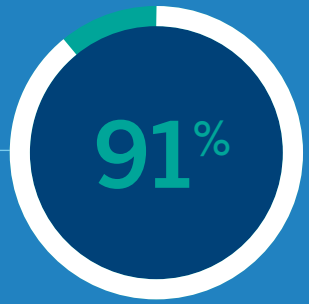
The new way of working has created new network vulnerabilities – and these have a high cost.



of workloads in the cloud by 2024. [1]



of CIOs plan to use multiple clouds to control costs. [2]



of companies plan to use a hybrid work model. [3]

The average cost of a data breach in 2021 was $4.24 million.[4]

Number of vulnerabilities identified by ethical hackers in 2022 alone, up 21% on 2021. [5]

Average no. of days for security teams to identify and contain a data breach. [6]

Sources: [1] Morgan Stanley Research: CIO Survey, Q4 2021 [2] Bain & Company: Technology Report 2020 [3] Gartner: 2021 Remote Workforce Survey [4] IBM Security. Cost of a Data Breach Report 2022 [5] The HackerOne 2022 Hacker-Powered Security Report [6] IBM Security. Cost of a Data Breach Report 2022

WHY SASE, AND WHY NOW? THE WORLD IS CHANGING

SASE puts security at the network edge. To put it at its simplest, it moves security close to the user, at the network periphery, rather than locating it at the data centre. In this way it reduces network congestion, thereby improving application performance at the network edge.

SASE = enhanced security + improved performance

The changing nature of work and business has driven the need for SASE. In the past, network users and applications were typically located in a limited number of geographical locations. Today, users and applications are everywhere. An employee could be working in a remote office in a rural area, in a coffee shop, onsite with a customer or at home. And the applications they use are no longer on a corporate computer, local server or even a PC. Increasingly they reside in "the cloud".

This new normal requires secure and optimised access to cloud services where employees and customers can connect anytime, anywhere, and with any device. The downside is that this new normal brings with it many new security risks.

Better resiliency is especially crucial when you have many small branch offices or a distributed retail network. With limited bandwidth at remote locations, you need cost-efficient and high-performing connections that are easy to deploy and manage.

But with traditional network security, this creates new vulnerabilities.

The pandemic accelerated a trend that was already in progress: the adoption of hybrid working models centred on cloud-based networks. This posed new challenges for networking and data security teams. High-latency networks at the network edge adversely impact user productivity and customer experience, and security gaps emerge. A Secure Access Service Edge (SASE) architecture is now critical to the deployment of successful hybrid deployments.

According to Gartner, "by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."

SASE converges cloud networking with security for enhanced performance, simplicity, scalability, flexibility, and pervasive security. Combining network security functions with SD-WAN routing capabilities, SASE delivers secure, optimal, and automated access to applications and workloads in the cloud. Regardless of the location of users and applications, SASE provides users of cloud-based applications with secure access from a single management platform.

SASE is now more relevant than ever. The accelerated and sustained transition to a hybrid workforce has made converged cloud networking and cloud security a necessity.

WHAT SASE IS NOT – COMMON MISCONCEPTIONS

1

"SASE is a product"

Think instead of SASE as an architectural framework that provides a cloud-delivered networking and security infrastructure, enabling organisations to connect users to the applications they rely on to be productive, efficiently and securely. Security that matches the needs of the digital enterprise. When fully implemented, SASE may integrate products and solutions from several vendors, although the whole solution is best offered by a managed services company, especially when the user organisation has limited IT resources.

2

"SASE is not suitable for SMEs"

The benefits of SASE can be realised by any organisation that has a distributed workforce or operates a number of branch offices. And because SASE is delivered via the cloud and can be priced at a per-user level, the barrier for entry is low enough for even small and medium-sized enterprises to pursue.

3

"SASE is just a new buzzword for SD-WAN"

While SD-WAN offers many advantages, it also introduces some challenges, including new security risks, reliability and performance issues, together with increased complexity resulting from the need for multiple network overlays. SASE takes SD-WAN to the next level by offering a unified framework for SD-WAN and security services, providing a single point of view and a simplified management approach to protect the network.

4

"SASE is too complex to manage"

As a high-level strategic initiative, a comprehensive SASE solution does indeed require an upfront investment in terms of capital and resources if implemented in-house. Many organisations are understandably concerned that costs might spiral out of control. But SASE can also be implemented by a managed services company with a clear, transparent and predictable cost structure. The benefits that can be realised will then be well worth the costs in the short as well as the long term: when provisioned in this way, SASE will scale according to your organisation's needs.

5

"My organisation has too much legacy infrastructure to make SASE viable"

In fact, the complexity of legacy network infrastructures is a motivating factor to pursue a SASE solution; SASE enables you to simplify IT operations by migrating application management to a unified cloud-based environment. Reducing the IT operational overhead can free up your resources, especially when administered by a specialist managed network services provider.

6

"MPLS is simple whereas SASE seems awfully complex"

It is true that multiprotocol label switching (MPLS) networks have become the predominant WAN architecture, because they create simplified network connections between a central headquarters and the branch network. Unfortunately, in most cases they are no longer fit for purpose with today's data volumes and hybrid users who need access anytime, anywhere. Enterprises can migrate from MPLS to SASE solutions that maintain the same simplified connectivity, routing data to a distributed point of presence (PoP) rather than through the data centre.

7

"The complexity of SASE makes it difficult to troubleshoot"

In fact, one of the benefits of SASE is that cost and complexity do not grow at the same rate as the network. That said, SASE is not in and of itself a "silver bullet" and should be viewed as part of a complex security picture so that it can fully defend against the threats emerging from the darkest parts of the Internet. SASE can create duplication and introduce inefficiencies which may make troubleshooting more difficult. In-house technicians will need to be trained in the new technology and security and network teams brought together as one – another reason why a managed service SASE solution might be the best option.

SASE TAKES SD-WAN TO THE NEXT LEVEL

In the 2010s a transformation took place with the emergence of SD-WAN (Software Defined – Wide Area Network) by decoupling the hardware components of a wide area network from the control mechanism.

This made more sense than routing everything to a central data server because most applications were no longer hosted on the server. They lived in the cloud. SD-WAN uses encrypted overlay tunnels for communication of data to locations within the organisation. This was fine so long as the users were based in branch offices, retail stores etc. But with the explosion in the numbers of employees working in a variety of remote locations, in particular in home office, something more was needed.

Hence SASE, which is the combination of SD-WAN with Security Service Edge (SSE) functions such as Zero Trust Network Access (ZTNA), takes SD-WAN into a new era of networking. SASE enables a much more flexible, user-centric approach to providing secure and high-performance for remote workers and cloud applications.

“SASE DELIVERS CONVERGED NETWORK AND SECURITY SERVICES FROM A SINGLE, GLOBALLY DISTRIBUTED AND CLOUD-NATIVE PLATFORM.”

THESE PAIN POINTS MAY SOUND FAMILIAR

SASE addresses the following pain points, which will be familiar to many network administrators and their organisations:

Inefficient cloud or SaaS access

Most enterprises run their applications across multiple public and private clouds, which puts an additional strain on operational resources, security, and quality of service. Cloud and SaaS applications require efficient, optimised access and an infrastructure specifically designed to support them. In the future, more complex, modern applications will drive even higher demand for secure and reliable connectivity, and a traditional hardware-heavy, transport-dependent network that relies on backhauling all cloud traffic through a single choke point in the data centre will not be able to support the requirement for quick, efficient cloud and SaaS access.

Poor application quality

Corporate networks were engineered to provide reliable, optimal performance for mission-critical applications and to support day-to-day operations. This need will persist for the branch office or store, even as the next generation of modern applications are deployed. In addition, as many workers transition to remote and home-based work, IT teams must ensure that these workers can reliably serve customers and work efficiently when consuming bandwidth-intensive services, downloading imaging files, and conversing via conferencing services.

Compromised security

IT teams are already faced with the challenges of separate networking and security stacks for their own networks. While the need to address these challenges remains, this will be compounded by the rise in the number of remote and home workers. Remote workers accessing corporate networks via unsecure personal devices can compromise security and may lead to data breaches and attacks. IT teams need a way to secure home networks and workers' devices.

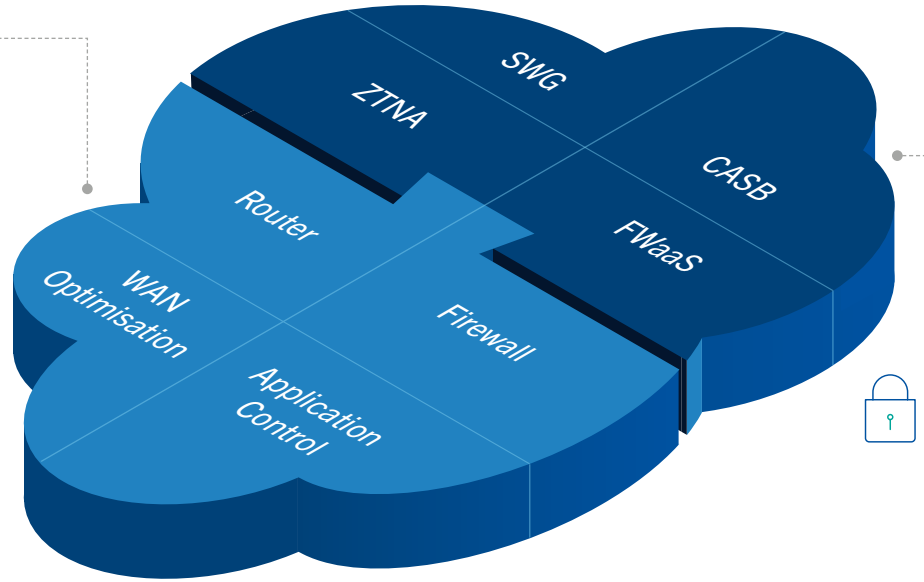
Operational complexity and costs

Traditional hub-and-spoke, hardware-centric networks are not designed for cloud and SaaS access, and they are not designed to scale rapidly and cost-effectively. Ensuring that workers remain optimally productive will mean the size of the network will have to increase, as home and remote workers need reliable connectivity to serve internal and external customers. Leveraging separate stacks for the branch network, remote access, network security, and content security is operationally inefficient and creates support complexities.

SASE COMPONENTS

From a technology perspective, according to Gartner's definition of SASE, **SASE** = **SD-WAN** + **SSE**. So let's consider each of these in turn.

SD-WAN
Network



SSE
Network Security

SD-WAN

The networking-as-a-service component of SASE uses the SD-WAN networking model, as offered by Hughes for many years. SD-WAN uses software and cloud-based technologies (routing, firewall, WAN optimisation and application control) to simplify the delivery of wide area network services. Networking intelligence is delivered as a service through a cloud-based orchestrator and cloud gateways, which communicate with simplified hardware appliances in branches.

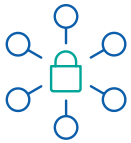
With SD-WAN networking intelligence, a SASE solution can treat edge traffic differently depending on where that traffic is going. For example, the solution can route cloud application traffic to nearby cloud exchanges, while sending other traffic to the corporate data centre or the Internet. SASE can also extend that intelligence from the application all the way to each user's device, whether at the corporate HQ, in a branch, in a home office, or on the go.

SASE also abstracts network functions via software-based virtualisation, thereby uncoupling network intelligence from physical infrastructure. You can run your network as a flexible cloud service to simplify your IT operations, leveraging Internet-grade high bandwidth transport to reduce costs while delivering a better user experience.

Security Service Edge

With SASE, security starts at the DNS layer. The network is the security; threats are stopped at the port, before they get near the application layer.

SSE is a collection of integrated, cloud-centric security capabilities that facilitates safe access to websites, software-as-a-service (SaaS) applications and private applications. It typically consists of four elements: SWG, CASB, ZTNA and FWaaS. That's a lot of abbreviations so let's look at each in turn.



Secure Web Gateway (SWG)

SWGs prevent unsecured Internet traffic from entering your internal network. It shields your employees and users from accessing and being infected by malicious web traffic, vulnerable websites, Internet-borne viruses, malware, and other cyberthreats.

Zero Trust Network Access (ZTNA)

The second major element in SSE is Zero Trust Network Access. ZTNA assumes that every entity trying to connect to a network is potentially hostile. Unlike traditional network security systems, under a ZTNA model, a user's role and permissions are irrelevant. If a user (a person or an app or other resource) wishes to connect to other applications or resources on the network, they must authenticate and then continuously validate their identity. This is typically achieved via strict access controls combined with contextual and behavioural flags.

ZTNA has emerged in the current era of highly distributed networks and supply chains. As businesses continue to scale their ecosystems, directly controlling every device and endpoint becomes impractical. On the other hand, extending unrestricted access to remote users exposes a network to an array of threats and risks.

Cloud Access Security Brokers (CASB)

Cloud Access Security Brokers (CASBs) are on-premise or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. These include authentication, single sign-on, authorisation, credential mapping, device profiling, encryption, tokenisation, logging, alerting and malware detection/prevention.

Firewall as a Service (FWaaS)

FWaaS is a firewall delivered as a cloud-based service. It allows companies to simplify IT infrastructure by providing next-generation firewall capabilities like web filtering, Advanced Threat Protection (ATP), Intrusion Prevention System (IPS), and Domain Name System (DNS) security. Functionally speaking, FWaaS is much like an on-premise hardware firewall. However, it comes with distinct advantages, such as the ability to scale nearly instantaneously to suit an expanding network or to provision new services. Because it is based in the cloud, FWaaS can be remodelled and calibrated according to the size, configuration, demand, and unique security needs of your network.

HUGHES MANAGED SASE

In response to the changing needs of customers and to the trends in networking and security, Hughes Europe offers the Hughes Managed SASE solution.

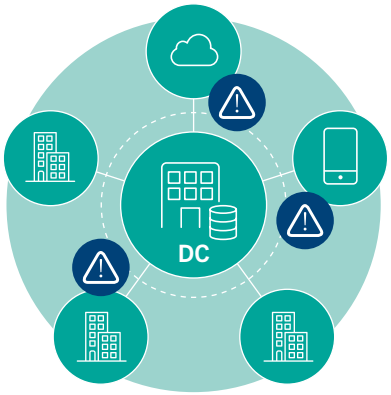
This solution brings together networking and security in the cloud. The uniqueness of the solution is in its many SASE points of presence (PoP), which are strategically distributed around the world and serve as an on-ramp to SaaS and other cloud services, combined with Hughes expertise in managing SD-WAN networks.

Hughes Managed SASE is a cloud-native extensible platform that combines industry-leading SD-WAN capabilities with cloud-delivered security – including cloud web security, ZTNA, and firewalling – to provide branch office, home, and remote workers secure, optimised, and reliable access to modern applications deployed in public and private clouds, SaaS, and at the edge. The Hughes Managed SASE solution leverages a global network of cloud service nodes, which provide unparalleled access to major cloud and SaaS providers, all available as a managed service from Hughes Europe.

The global footprint of more than 150 points of presence delivers cloud-based networking and security services that easily scale to customers' SASE needs.

SASE Highlights

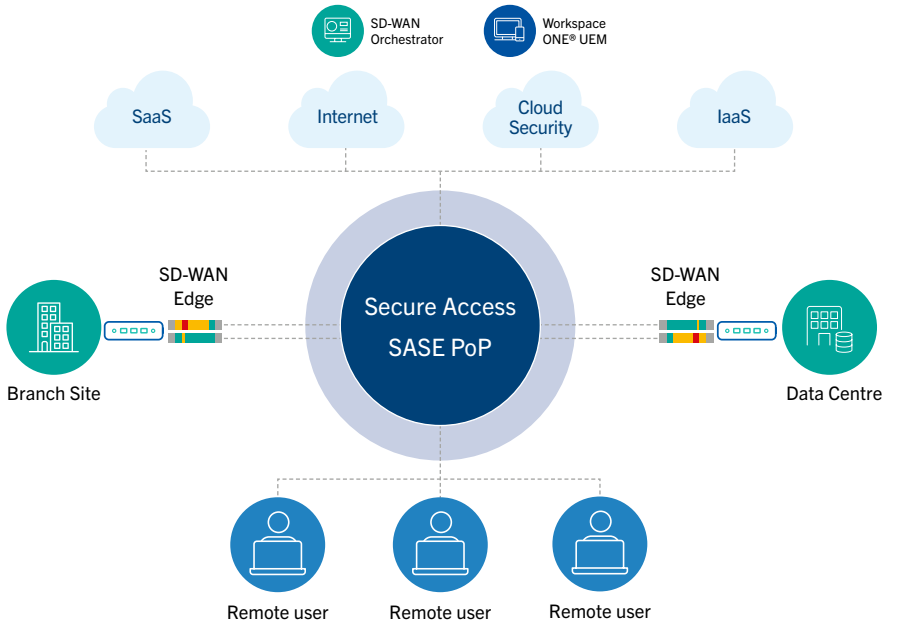
Zero Trust Network Access (ZTNA)



vmware

Source: VMware

- One-time credential check
- Generic access policy
- Access to all apps
- Inefficient cloud app routing



Source: VMware

- How much do I trust this device?
- How much do I trust this user?
- Granular access to applications and data
- Optimal access to DC and cloud apps

→

- Device posture assessment
- Continuous authentication, contextual policy
- Per-application VPN
- Intelligent policy-based routing

WHY CHOOSE HUGHES MANAGED SASE?

Comprehensive distributed workforce solution

By combining key elements of unified endpoint management, desktop and app virtualisation, Secure Access Service Edge, and endpoint security technologies, Hughes Managed SASE enables IT teams to meet the needs of today's distributed workforce. This unique convergent infrastructure provides reliable, optimal connectivity paired with visibility and context across all service elements. And this in turn ensures that network and security coverage is broader and more effective, following users, data, and apps wherever they are.

Proven global cloud platform

Hughes Managed SASE is based on the idea that the cloud is the network, and the service operates on an extensible, scalable cloud services platform to execute on this idea. The platform supports integrated networking and security services, along with handoffs to cloud, SaaS, and third-party services while also allowing for the services of tomorrow, like edge computing. The platform provides reliable, secure, and optimal access to cloud, SaaS, and legacy applications around the world.

Single integrated management platform

Hughes Managed SASE lowers operational complexity and expenses by enabling organisations to deploy, configure, manage, and troubleshoot networking functions—including managed SD-WAN and ZTNA/remote access with security functions for web, cloud, SaaS, and the data centre. All of this is provided via a single comprehensive management platform that uses intelligent business policies to govern the application of underlying services. The management platform incorporates artificial intelligence and machine learning to automate troubleshooting while providing insightful analytics on the end-user experience.

Broad ecosystem and open architecture

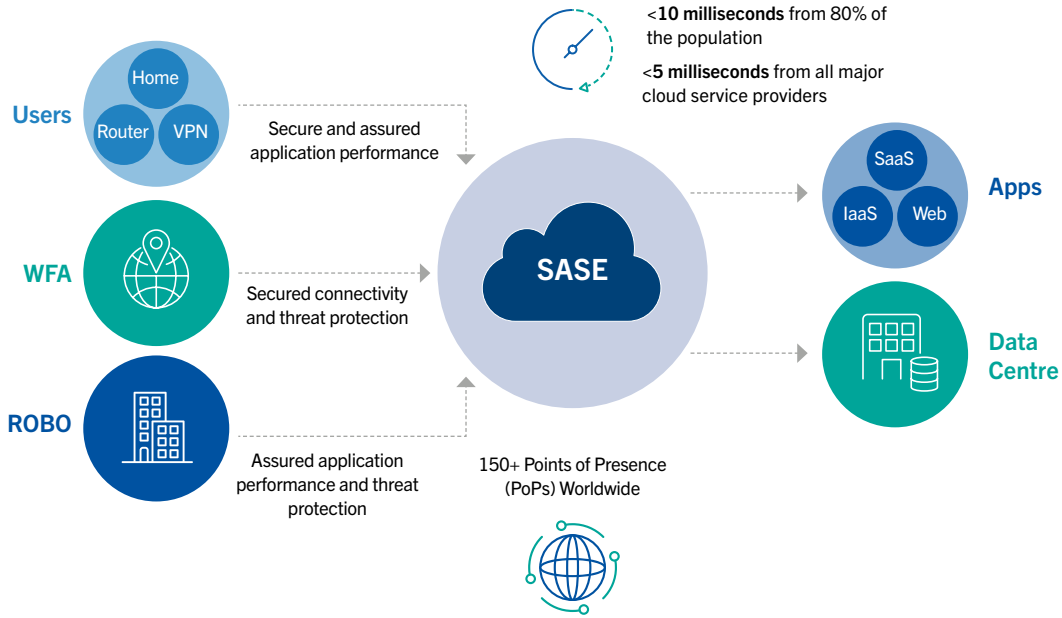
As part of the migration journey, many organisations will need to transition away from existing solutions at a pace aligned to their business needs. To make this transition as smooth as possible, Hughes Managed SASE employs a flexible architecture, allowing customers to leverage managed services delivered by Hughes Europe.

BENEFITS OF HUGHES MANAGED SASE: THE “WORK FROM ANYWHERE” SOLUTION

Hughes Europe offers Hughes Managed SASE as the solution to all the pain points listed above. It is a comprehensive cloud-delivered SASE platform that brings together industry-leading network solutions, all integrated in a single platform and delivered via a SaaS model for users on the move, remote offices and branch offices (ROBO).

SASE Work from Anywhere (WFA)

Better quality of experience, secure access, and threat protection



With Hughes Managed SASE, IT teams can:

- Optimise access to applications as well as hybrid cloud, multi-cloud, and SaaS.
- Protect users, networks, applications, and data against emerging inside and outside threats.
- Deliver high quality digital experiences to customers, employees, and partners, no matter where they reside.
- Maximise IT and operational efficiency through innovation and automation.
- Accelerate edge transformation to a multi-cloud edge architecture.

SASE FACILITATES NEW BUSINESS APPLICATIONS AND SCENARIOS

The face of business is changing. Take retail, for example. Today's customers have new expectations. They walk into a store and expect a secure in-store Wi-Fi connection to social media or mobile payment gateways, quick checkouts and interaction with rich media. Users have set high standards for instant gratification and a great shopping experience.

This sets new challenges for networking and data security professionals. They need to ensure that business-critical applications perform reliably across various channels, devices and platforms. In many cases, 24/7. The volumes of data retail networks handle have increased exponentially with cloud-based applications for businesses and customers, data analytics, Internet of Things (IoT) devices such as RFID, sensors and smart cameras, mobility and rich media content.

Traditional network connectivity has proved too expensive and rigid to meet today's expectations. Multiprotocol label switching (MPLS) is too expensive while the public Internet, although easy to deploy at remote locations and cost effective, presents latency and performance issues as well as concerns about security.

Most retailers today have multiple branches, applications and platforms, each of which is a potential point of vulnerability for malicious attacks. A centrally managed SD-WAN and console make it easy to integrate new services and locations while adjusting policies remotely for immediate results, without having to worry about the cost, resources and logistics associated with setting up a new cybersecurity infrastructure at a new location.

Hughes Managed SASE brings the demands of network security, manageability, operational efficiency and performance into harmony. It enables retail organisations to maintain business resilience and deliver the kind of service levels that will delight customers through improved application performance while simplifying branch management and compliance.

HUGHES MANAGED SASE SOLUTIONS

As mentioned above, SASE is not a product. It's an approach that combines the flexibility of SD-WAN with the security of SSE.

How this best works for you depends on your organisation and its business goals. This is the starting point for a Hughes Managed SASE solution: designing and implementing the ideal solution in a way that fits your IT trajectory and is rolled out without disrupting your day-to-day business.

A Hughes Managed SASE solution, with all network and security capabilities embedded in a single software stack for ease of monitoring and control, reduces capital investment and frees your IT staff to focus on strategic work. It enables you to create a coherent security policy deployment, reduces hardware complexity and cost, and moves your organisation's network to an on-demand, pay-as-you-go model in which costs are transparent and predictable.

Hughes closely monitors your network traffic from the cloud, round the clock, 365 days a year. Our systems check every interaction, authentication, and transaction to give you complete peace of mind no matter how extensive your network of users and devices and no matter how great your traffic volumes. With Hughes Europe on your team, security and flexibility is now within reach.

Get started today by talking to a Hughes Europe networking and cybersecurity expert.

A NAME YOU CAN TRUST

Our flexible networking solutions combined with our multi-vendor approach means we take modern technology capabilities and identify the right solution to meet our customers' commercial needs. Our long-standing relationships with our customers, which span many years, are testament to our collaborative and quality-focused approach. We deliver our services throughout Europe with offices in the UK, Germany and Italy and offer a single point of contact with a single, aggregated service level agreement for all sites irrespective of size or location. As the European business unit for Hughes, we work in collaboration with our sister business units in North America, South America, India and International to deliver fully integrated solutions on a global scale.

For further details about our products and services contact us today.

$2 BILLION Dollars in revenue

Supporting **425,000** business and government sites worldwide

2,100 employees globally

7+ million terminals of all types delivered in **more than 100 countries**

Deployed **50,000** SD-WAN sites to date

Customers on **6 continents**

5 decades of networking expertise

WANT TO KNOW MORE? GET IN TOUCH

TELEPHONE
UK: +44 (0) 1908 425 300

E-MAIL
sales@hugheseurope.com

WEBSITE
www.hugheseurope.com

About Hughes Network Systems

Hughes Network Systems, LLC (HUGHES) is the global leader in broadband satellite technology and services for home and office. Its flagship high-speed satellite Internet service is HughesNet®, the world's largest satellite network with over 1.3 million residential and business customers across the Americas. For large enterprises and governments, the company's HughesON™ managed network services provide complete connectivity solutions employing an optimized mix of satellite and terrestrial technologies. The JUPITER™ System is the world's most widely deployed High-Throughput Satellite (HTS) platform, operating on more than 20 satellites by leading service providers, delivering a wide range of broadband enterprise, mobility, and cellular backhaul applications. To date, Hughes has shipped more than 7 million terminals of all types to customers in over 100 countries, representing approximately 50 percent market share, and its technology is powering broadband services to aircraft around the world. In Europe alone, where we have been helping our customers to achieve optimal value from their network infrastructure for more than 30 years, we manage 55000 sites, across 28 countries supporting more than 5 billion transactions every year. Headquartered outside Washington, D.C., in Germantown, Maryland, USA, Hughes operates sales and support offices worldwide, and is a wholly owned subsidiary of EchoStar Corporation (NASDAQ: SATS), a premier global provider of satellite operations. For additional information about Hughes, please visit www.hughes.com and follow @HughesConnects on Twitter.

About EchoStar

EchoStar Corporation (NASDAQ: SATS) is a premier global provider of satellite communication solutions. Headquartered in Englewood, Colo., and conducting business around the globe, EchoStar is a pioneer in secure communications technologies through its Hughes Network Systems and EchoStar Satellite Services business segments. For more information, visit echostar.com. Follow @EchoStar on Twitter.

HUGHES Europe