E-GUIDE

What are the benefits of SASE?

The cloud and the urgent need to secure data everywhere are dramatically changing the network and security. These forces are demanding a new type of IT infrastructure--one where the network and security come together into one cloud platform and one service from a single provider. This is the concept behind secure access service edge (SASE). It's the latest SD-WAN solution framework from Gartner. While SD-WAN is a network-as-a-service, SASE is a network-security-as-a-service. See **"What is SASE?"** Here's how SASE solutions deliver real business value.

Why do businesses need SASE?

The cloud moved your network off premise

IT has grown up focusing on the data center and IT security, but today IT users and networks are behaving quite differently than in the past. According to **Nemertes Research**, the WAN as we knew it is over. Just 39% of enterprise WAN traffic originates from, and terminates on, enterprise premises. The remaining 61% either originates

from an off-premise site (such as a home-office), terminates on an off-premise location (such as an IaaS, PaaS, or SaaS cloud workload) or both (remote office to cloud). This is due to the fact that:

- User's now commonly work with resources outside the enterprise network, accessing IaaS and SaaS workloads.

- Sensitive data is located in several cloud services located outside of the enterprise data center such as unified communications and contact center operations.

- Work from home (WFH) users and branch offices only accelerate this trend. Remote users increase the access to cloud services.

Today, companies must secure data everywhere

Moreover, today centralized data center security no longer delivers the required protection. Data will still exist in the data center but it will also exist in sites such as Salesforce, social media, and many other services. The level of security at each of these locations may or may not be adequate, meaning most enterprises may need to take significant action so that its entire environment meets security, privacy, and compliance requirements. Here are some of the challenges driving the need for SASE's converged network and security model:

- Network security architectures that employ the enterprise data center for connectivity can limit the dynamic access requirements for digital transformation.

- Enterprises have more users, devices, applications, services, and data located in multiple cloud services, not in enterprise data center.

- Increasing complexity and application latency require a change in the security architecture.

- Additionally, digital transformation requires new approaches to IT services where security is not an afterthought. Modernization should require secure IaaS and SaaS deployments especially for real time applications, edge computing and IoT, and other cloud-based services.

SASE solutions solve these challenges because it's a cloud-based network and security service that can be applied anywhere--it's not data center focused. SASE also uses an identity-based approach to security--network access is evaluated based on the individual user or endpoint device. Solutions and services include:

- **Key SASE Capabilities:** SD-WAN, firewall as a service, Cloud Access Security Broker (CASB), secure web gateway, and Zero Trust network access

- **Key SASE Characteristics:** Distributed policy enforcement, multi-tenant cloud service, and identity-driven routing and access.

This real-time solution employs security and compliance policies all while evaluating risk during the sessions.

Plus, it helps with today's more distributed IT environment. Secured entities can be internal and external people or groups of people and devices--think group collaboration sessions, at-home devices, cloud applications, IoT systems, and edge computing.

What are the benefits of SASE? Does it help with WFH?

Combining SD-WAN and SASE together in a single market with a single provider allows the enterprise to respond faster with greater control in response to COVID-19 and the expansive growth of work-from home (WFH) users. SASE improves sensitive data awareness, secures the data, and provides threat protection especially for WFH and branch users.

Business benefits of SASE

Moving to SASE should be justified on a business foundation as well as a technical foundation. Business rewards include:

- **IT Agility:** Much like SD-WAN, SASE solutions are software-defined and cloud-based solutions, delivering agility advantages. Without agility (the ability to change direction and respond to competitive changes) companies move more slowly.

- **Cost reduction:** SASE can help reduce IT staff costs, improving 24/7 coverage for the both the network performance monitoring and security threat monitoring and response. Operational overhead will be reduced because the SASE service supports new capabilities without requiring the investment in new hardware and software. SASE may also reduce the cost and complexity by delivering more technologies and services through a single provider.

- **Network performance:** Constant network monitoring reveals the quality and performance of all connections including those distributed across virtualized cloud environments and data centers. It provides a real-time picture of all inbound and outbound process connections in a single portal or network interface.

- **Security and reliability:** SASE includes a wide array of security technologies, which can Improve security support by inspecting content and locating sensitive data and malware. Ultimately, this reduces downtime due malicious behavior.

- **Greater visibility and transparency:** Because SASE condenses a variety of functions into a single offering, network and security transparency gains can be significant, reducing the number of software agents required and delivering consistent network visibility.

- **Local security enforcement:** SASE delivers centralized policy management with local enforcement employing distributed enforcement points.

- **Consistent security enforcement:** Existing network security architectures were designed for

the centralized data center and are not well suited to remote users that connect to diverse services as well as the data center. SASE delivers consistent and global security control no matter where the user connects to for services.

Can I take a do-it-yourself approach to SASE?

Technically you can take a DIY approach to each of SASE's five core capability areas, but doing so may increase your IT complexity. SASE is extremely valuable for companies seeking to cut down on the number of technology providers, technology integrations, day-to-day network performance management, as well as the security firewall alert management and responsibilities of threat response. The technologies, people, and skill sets needed for 24/7 IT operations have become significant pain points for businesses of every size, and SASE is uniquely designed to address this issue in today's multi-cloud business model.

Whereas traditional SD-WAN solutions typically include only bundled firewalls and secure web gateway, SASE multiplies the security value of an SD-WAN investment by condensing five different individual industries into a single cloud platform delivered as a service from one partner. As the SASE market matures and the interoperability between its five core capabilities becomes even more seamless, only the largest enterprises (with more IT resources) will want to continue a point-based or multi-vendor approach to all those IT needs.

This becomes particularly evident today when companies are leveraging the cost benefits of the public internet. Firewalls are necessary, meaning that unified threat management and SOC response teams work best when delivered by the SD-WAN or SASE managed service rather than DIY. This aspect alone can cost justify a managed service over a DIY approach.
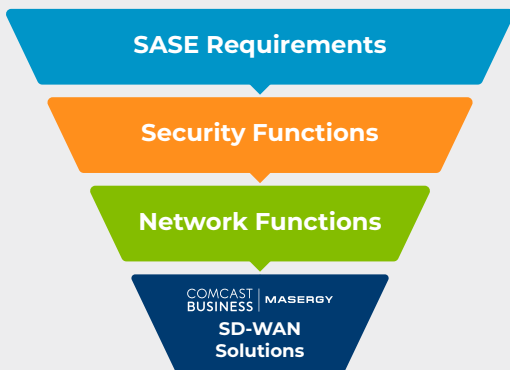
In the end, security must be intrinsic to the network infrastructure with a variety of ancillary security functions all working in unison with SD-WAN. SASE makes that far easier, and a managed service model leads the way, freeing your IT resources to focus on transformative initiatives.

[Read more articles in the SASE Straight Talk series](#)

About the author: Ray Watson

Ray Watson is VP of Innovation at Masergy. He brings over 17 years of expertise in IT strategy, application solution design and next-generation network architectures. Ray has enabled numerous global enterprises in transforming their IT infrastructures to guarantee business outcomes. Ray is an industry thought leader in IT transformation and is a frequent speaker on topics such as hybrid networking, SDN, NFV, cloud connectivity and advanced security. He holds a B.S. from Purdue University.

SASE Requirements

Security Functions

Network Functions

COMCAST BUSINESS | MASERGY
SD-WAN Solutions

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled, secure application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS and Managed Security solutions. Industry leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.