**CHAPTER 1: SASE Introduction**

**Define SASE**

Secure Access Service Edge (SASE) is pronounced sassy. Andrew Lerner at Gartner coined the phrase in a blog post December 23, 2019. That post can be found at: <https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/> He explains that SD-WAN needed a security package. SD-WAN, Software Defined, Wide-Area Network, effectively replaces router-based WAN solutions in a next generation package. The SD-WAN solution varies from vendor to vendor but incorporates secure packet forwarding with policies that leverage application specifications to guarantee the best handling of traffic for each application. This increases the user experience as well as the network’s resilience.

We now refer to SASE as a framework. SASE leverages multiple security services into a framework approach. Not all services offered as SASE solutions are required to be compliant but an adherence to a comprehensive secure framework approach is expected. Currently there is no SASE certification instead most of the SASE hype comes from intense competition through effective marketing.

The idea of SASE was not far from what security consultants were already doing by integrating multiple security solutions into a stack that ensured a comprehensive, layered, secure access solution. This approach is something I was already doing for my customers in ensuring Next Generation Firewall, (NGFW), Intrusion Detection (IDS), Intrusion Prevention (IPS), and other necessary security solutions were a part of every SD-WAN installation. Somehow by calling it a SASE Framework, the approach to a comprehensive solution felt more focused than what my peers and I felt was just best security practice.

Commonly SASE services include SD-WAN, ZTNA, CASB, NGFW, SWG, unified management and orchestration. Just what constitutes a “Real SASE Solution” varies greatly by source. Several organizations such as the MEF Forum are trying to establish neutral industry standards for SASE. These standards will pave the way for a universal understanding, the ability to integrate multiple manufacturers into a solution, and a method for teaching SASE.

Most network communications and security vendors have been working to create a full SASE framework under their brand. Their marketing presents the idea that a full SASE solution from a single vendor is the way to ensure security. Current customer feedback from the Fortune 500 class of businesses is that 2-3 OEM vendors will need to be integrated to allow for “best of breed” solutions. This provides an opportunity for a Managed Services Provider to provide orchestration across multiple platforms to achieve optimal security.

**Market SASE**

In the market today scores of different manufacturers offer “SASE” products. The potential list of services across their portfolios that may be a part of a complete SASE Service could be in the dozens depending on their market approach. Calling a service “SASE” does not make it so and as there is no “SASE” certification for solutions at the time of writing this book, no vendor or managed services provider is exclusively correct in their marketing.

Gartner started a fire with that simple blog post in 2019. Overnight every SD-WAN solution in the market offered a path to SASE. The SASE idea itself multiplied the SD-WAN market’s potential revenue of over $11 Billion (USD) by 2028. “The global secure access service edge (SASE) market size is expected to reach $11.29 billion by 2028, registering a CAGR of 36.4%, a ResearchAndMarkets report reveals.” <https://www.helpnetsecurity.com/2021/08/17/sase-market-2028/>

The reality is that an 11 billion US Dollar market is only the core SASE product offering for the market. Hardware, Software Licensing, Hosting, Maintenance, and Support make up the core products whereas managed services and professional services can multiply the market impact by up to 25 times of the core product revenue.

The market challenge for realizing revenue potential will be primarily impacted negatively with the lack of skilled labor for design, build, and deploy services. This skill gap and the operational expenses preference of most CIO/CFO strategies will drive more than 70% of the market to contract SASE as a managed services offering. In the market there is a trend of up to 78% of SD-WAN contracts leveraging managed services as opposed to utilizing in-house engineering teams. The primary reason for this change is not tied to SASE as CIO and CFO focus has been to rely on technical services as Operational Expense (OPEX) as opposed to Capital Expense (CAPEX). OPEX has been the goal for what is considered by an organization as non-business value cost. Generally, the CIO direction of the largest organizations is to convert operational support staff costs in order to leverage the cost savings on DEVOPS staff costs which can offer a business return on investment. Support teams are a cost center where as the DEVOPS team can provide the potential to be a profit center to the company.

The complexity of SASE Services is driving the need for technology engineering careers to move to a continual learning path. The time has passed where an engineer can rest on traditional education or certification paths. Traditional academic education can provide perspective, historical knowledge, foundational knowledge, and soft skills required for functioning in an organizational environment. Industry and manufacturing certifications provide core technical knowledge for functional understanding in a vertical role within an organization. Both methods are beneficial for building a foundational understanding of a skill set. Both are effective filters for recruiting for a specific role. Unfortunately neither can move at market pace which is today at an average of 3 DEVOPS or SECDEVOPS “Sprint Cycles” from being out of date and ineffective.

Software development follows a continual improvement path and so must its practitioners. The goal of the DEVOPS mentality is to leverage iterative development in a modular fashion as opposed to legacy, ground up development and go-to-market practices. DEVOPS practitioners continually develop, continually improve, and continually release. Agile Sprint Cycles vary by organization, but an average of 2 weeks can be used as a model to understand the phases of development. New network and security software releases are no longer tied to hardware releases as they can function as a virtual machine, virtual network function, cloud native function, application, or a service independent of platform. The entire go-to-market process could be as little as one Sprint Cycle or two weeks. Network and Security practitioners operate on a N-1 (New – 1), N-1+validated, or wait for a triggering event to validate a new software release. The market average for consumption of new software releases is moving to an average of 3 sub-versions of code which could average 6 weeks between the last production upgrade of software and the next production upgrade.

The market has been slow to admit that network or security engineering is no longer a discrete skillset from software development. In fact, SASE Services will receive major software updates every 2-6 weeks depending on the development cycle or security issues with each independent SASE service within the overall solution. Minor updates may occur in real time. Education for engineering teams must align with software release cycles.

**Value SASE**

Effective security is inherently valuable but how do we accurately estimate that value? How do we quantify the value of a solution for an unknown risk impact? Former President of the US, Ronald Reagan was quoted saying; "Information is the oxygen of the modern time. It seeps through the walls topped by barbed wire; it wafts across the electrified borders." If information is oxygen, what is the accurate value of oxygen to human life? Effective security pays for itself in reduced risk, liability, and loss of unknow quantities by protecting that oxygen or in this case non-public information.

To evaluate SASE in a value proposition or ROI the investment should be first quantified. Steven Ross, an Executive Principal of Risk Masters Inc., points to ROSI, the return on security investment which is a calculable assessment as a way of identifying a monetary value of the security investment. This may be important to the CFO or investors as a model for understanding financially the inherent value of secure information technology investments. <https://www.isaca.org/resources/isaca-journal/past-issues/2011/what-is-the-value-of-security#1>

Without effective security solutions, an organization will cease to achieve primary return of investment for time and capital invested. A recommended value proposition for security is the ability to conduct, unobstructed the primary business of the organization on whose behalf the secure solution is employed. SASE provides cost effective security and builds value by reducing inefficiencies in previously developed generations of secure communications. Cost reductions can be achieved by reducing labor, time, capital, focus, outages, performance issues, and educational requirements for staff members trying to build their own perfect technology. Simply speaking, the investment required to develop secure technology solutions in house with home grown or “best of breed” market solutions has been providing a negative ROI which has driven the market to leverage a managed service provider (MSP) that specializes in a specific technology. This method also allows for the transfer of liability to the MSP which provides some relief for executives not choosing to develop their own secure communications solution in house.

Leveraging SASE with SD-WAN prepares networking and security solutions for a future of automated, secure information technology provisioning with real-time operations remediation. In order to eliminate the inefficiencies that every network has experienced, the solution starts with abstracted components and the disaggregation of data and control plane activity (separating components). By leveraging a deconstructive process, smaller changes may be made, reducing the risk of any one change causing a major impact to secure network communications. The smaller the change, the quicker the change can provide business value. The target process is analogous to a garden pruning process that makes small changes until the overall desired effect is achieved. Unlike physical garden pruning, small changes in SASE can be reversed quickly if a negative outcome is realized. Overall this methodology allows IT organizations to move much quicker than we could even 5 years ago which allows us to do more with less in a business time, considerate model.

Orchestration allows for solutions to be templated. The orchestrator allows templates to be overlain upon any of the logical components in the overall solution or service. The creation of a template-based design offers rapid deployment across the abstracted solution. An additional benefit of orchestration is that template continuity may be enforced by the orchestrator and variance be reported to security operations systems for tracking and mitigation. This process allows the achievement of compliance with approved network or security designs and immediately identifies violations for action.

SASE provides value in efficiencies, scale, automation, enforcement, and orchestration over similar secure communications technologies in production today. This overall value reduces the design, build, deploy, and operate labor required to keep an organization communicating securely.

**Embrace SASE**

SD-WAN adoption was extremely slow from inception and into 2021. The main reason for the slow adoption was due to the lack of education prior to intense market demand based on inflated cost savings estimates over MPLS and other legacy network types. Gartner defined the “Gartner Hype Cycle” as a method for evaluating when to leverage a new to market technology. In their five phases they identify levels of understanding a shiny new market idea prior to consumption. The benefit of this approach is that it gives perspective necessary to make an educated decision. <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>

Educated decisions require available educational material which does materialize in the market until phase three, the “Trough of Disillusionment”. Phase three is roughly where the lessons learned are documented and effective curriculum is developed allowing training to start. At the time of writing this book, the “Hype Cycle” for SASE is still effectively in the phase one where there is much more excitement than factual data.

The promise of SASE is tied to the value; faster, easier, more secure, more automation, and rapid deployment. Better, faster, cheaper is the market’s battle cry. SASE can deliver on all of the above when designed leveraging correct mindset and qualified resources. The correct mindset is that security is done in layers and the best security leverages as many layers as is productionally sound. The best security does not come from a product but through best practice frameworks implemented correctly. The qualified resource can come from networking, security, or software backgrounds but is the continually self-educating resource that is concerned about being right for the sake of those served as opposed to for righteousness’s sake. There is no “silver bullet” for solving the resource / market / skill gap however, the right resources will self-educate perpetually, allowing themselves to be wrong in knowledge so they can remediate their gap and their solution will be right in production.

**Present SASE**

To present SASE to executive, administrative, or technical audiences, a framework for discussion is provided below with the key understanding per topic.

1. Introduction
   1. Secure Access Service Edge (SASE) is pronounced sassy.
   2. Gartner defined the term to describe what was happening in the market.
   3. SASE services may include SD-WAN, ZTNA, CASB, NGFW, SWG, as well as other services.
2. From Framework to Managed Service
   1. The SASE framework provides for integration of solutions from multiple vendors.
   2. The market is buying SASE services on a consumption basis.
   3. Most organizations will leverage 2-3 SASE vendors and one Managed Service Provider.
3. SASE Managed Service
   1. The effective managed service offering allows for OPEX instead of CAPEX.
   2. Managed services are being consumed for SASE due to rapid software development ahead of effective education for engineering or operations staff.
   3. The right managed service offering provides; orchestration, open API integration, AIOps, and multivendor seamless integration.
4. SASE Service Stakeholders
   1. For secure, compliant, resilient, and high performing solutions, a framework for feedback and participation into business impacting decisions is required.
   2. Stakeholders may be defined leveraging PMI-PMP best practice.
   3. Governance is required
5. Actors and the Managed Service
   1. SASE defines subject actors, target actors, and the role managed service providers play.
   2. A “subscriber” contracts a service on the actor’s benefit
   3. The managed service must provide layers of security that account for real time access in Zero Trust.
6. Identity, Context, Situation
   1. Identity, as in who or what is authorized by the service.
   2. Context must be defined as the same user may be allowed or restricted access by policy.
   3. Situation builds upon the context for the access role and further defines access.
7. SASE Sessions
   1. Sessions are the heart of SASE and may be considered as a wrapper for network sessions.
   2. Sessions incorporate application specific policies.
   3. Sessions leverage Zero Trust Framework as well as SD-WAN.
8. SASE Security
   1. Security is not a product but builds effective layers upon a secure foundation.
   2. SECDEVOPS necessitate production software code updates as often as every 2 weeks.
   3. SASE will require integration across vendors for “best of breed” capabilities.
9. SASE Policies
   1. Legacy firewall or router policies force specific behaviors that are not sensitive to external changes in the factors by which that policy was written.
   2. Automation and Orchestration allow policies to be changed based on real-time conditions.
   3. Effective SASE policy considers all available data in the decision process.
10. SASE Connectivity
    1. Most commonly SASE connectivity will come from SD-WAN
    2. SD-WAN allows SASE to leverage quality, performance, and application awareness tools.
    3. Remote access solutions, 5G services, satellite services, Ethernet circuits, and legacy wide-area networks may be incorporated into SASE.
11. SASE Services Use Cases
    1. The primary SASE use case is SD-WAN plus security.
    2. SASE may be leveraged for both Cloud infrastructure and applications.
    3. SASE can be used to create on-demand, secure communications across any network type.
12. Looking Forward
    1. The future is SASE as it is possibly the last step in the “pure cloud” transformation journey that all organizations must take.
    2. AIOps with SASE allows for consistent, reliable, secure, and on demand application access.
    3. SASE education must follow the continual learning, continual improvement path for staff.