White Paper

trustgrid

Building Your SASE Strategy

The victors in the evolving SASE market will solve the security service chaining problem while competing head-on with the legacy security solutions that dominate IT security spending today.

They will build their solution on a platform that integrates software-defined networking with secure remote acces and edge computing to solve the expensive problems of managing distributed applications. This will lead them to capturing more revenue and a dominant market share by securing a far broader portion of their customers' infrastructure. In doing so, they will deliver a low latency and highly secure experience while their competitors argue with buyers about the need to sacrifice performance for security.

What is SASE?

Secure access service edge (SASE) combines the components of SD-WAN, remote access and edge computing with cloud-delivered security.

SASE is a convergence of WAN connectivity and security. Bringing these two functions together allows security providers to deliver security services to any system, user or device from the cloud.

This integrated network and security architecture has been gathering steam since Gartner defined the term in 2019, with many security providers already strategizing ways to address this growing trend.

With SASE, network and application security policies are defined in the cloud and tied to authenticated identities. This enables IT to quickly make network and security policy changes and automatically deploy them across the entire network within minutes.

These policies can be tied to cloud-based identities and applications, but enforced locally by rerouting traffic to different security services, such as SWG, CASB, DLP, or whatever is appropriate for the traffic type.

As the number of security point solutions in an organization grows, so does the need for centralized management and orchestration. SASE architectures build a new software-defined perimeter, supported by a variety of security applications, and defined by zero trust access to all IT resources.

The Security and Networking Industries are Converging

Today, almost all SASE solutions are being built on large deployment footprints and existing customer relationships held by security and networking providers. To this point, Palo Alto's recent acquisition of CloudGenix combined the forces of two industry heavyweights to add features and cross sell opportunities to their respective install bases. This merger is just one of many that the industry will see over the coming year.

The SASE solutions that seamlessly address both cloud and on-premise security will be the big, early winners in the space. History has repeatedly shown that the early market share leaders can build large moats quickly. The rise of SASE will be no different and the tectonic plates have already begun to shift across the security industry in response.

Hybrid Cloud Is the Market

While some vendors have begun assembling the required components to deliver robust SASE platforms, the race to produce a minimum viable product has many vendors narrowing the scope of their solution.

Today many vendors offer secure web gateway (SWG) or remote access to end users through agentless or proxy solutions that support only HTTP/S traffic. This is fine for those customers that have fully migrated to the cloud, but that doesn't address the vast majority of enterprise applications in the world that rely on Layer 3 connectivity between data centers and other on-premise resources. With these solutions, wins are possible with cloud-only companies (the few and the small) and as bolt-ons to the real security solutions that will continue to take the largest share of IT spending.

Security solutions will ultimately be divided into two camps... Those that support "cloud-only" versus those that support the far more ubiquitous hybrid cloud environments.

Realize That Proxy Alone Is Not Enough

As the market begins wider scale adoption, SASE is going to compete against a stack of entrenched technologies that are tightly integrated and market hardened. When newer remote access solutions go head to head against legacy VPN, it will have to support Layer 3 connectivity offered by traditional VPN clients AND deliver the enhanced value that justifies replacing thousands of software endpoints. For SWG to replace existing legacy on-premise gateway security solutions it must address the on-premise/private cloud architectures still in use by nearly every large organization in the world.

Distributed Architectures Crush Centralized Security Services

In the battle between security and convenience, minimizing the impact on users usually wins.

SASE aims to eliminate this zero sum decision by providing better security while also enhancing a user's experience. Delivering a better user experience in SASE depends on the decentralization of security. Black / white listing, reputational-based filtering and routing are best delivered at the edge, but high compute services such as sandboxing are best delivered in the cloud. Security solutions such as SIEM benefit from low cost storage across hybrid cloud environments. Instead of addressing the needs of these services individually and dealing with the impact to users and complexity, the right SASE architecture allows each service to move to its most efficient location.

This reorganization of service delivery allows SASE to provide a better overall security and user experience, but it can also address the ever increasing cost of computing in cloud-delivered security. When SASE leverages edge computing platforms it allows security intelligence to move closer to the sessions, instead of backhauling sessions to intelligence. When inspection is pushed to the edge, costs (and latency) are lowered as the compute burden is shifted closer to the data source and traffic bottlenecks are removed.

In a race to be the first to market, many vendors claiming to have SASE offerings are simply chaining multiple security services and vendors together and punishing the user. Without thoughtful consideration of the resulting latency this will lead to a diminished customer experience. Providers that build, buy or partner to create a SASE solution must deliver frictionless security, uninterrupted user experience, and differentiated value to their customers.

Ultimately, the challenge and promise of SASE resides in the management of distributed application architectures. And SASE is a perfect use case for distributed application architectures that span from the edge to public cloud. Managing these distributed architectures depends on automated edge computing solutions to operate efficiently. When you solve the challenges of edge deployment and management, you solve the larger problems of service chaining.

Why Trustgrid

The components needed to complete a SASE vision currently reside in multiple silos. Security providers hold the domain expertise in things such as cloud brokers, data loss prevention (DLP) and secure web gateways... while networking companies provide the routing, encryption and traffic optimization functions.

As a platform providing integrated Zero Trust networking, remote access and edge computing capabilities, Trustgrid simplifies the ability for security providers to quickly bring SASE solutions to market.

The Trustgrid Platform Provides

- Full L2 / L3 / Proxy SDN feature set
- Cloud-based tools for troubleshooting and remote monitoring
- Cloud-native control plane and elastic cloud gateways for scalability
- Proprietary cloud PKI and CA for securing devices and cloud services
- Cloud software repo for delivering continuous code and security updates at scale
- Edge computing platform tools for rapid development and deployment of new features

Built as an API-first software-defined networking solution, Trustgrid integrates easily with cloud security technologies and provides centralized deployment and support services.

Trustgrid's managed services and automation capabilities are optimized for security providers that see networking as a necessary component of their SASE solution, and desire the operational efficiencies of a software-defined networking platform designed for 1000s of customers. And because Trustgrid is one of the only solutions on the market offering edge computing on the same platform as core networking features, the extensibility of the platform to new use cases is limitless.

888.308.8995
info@trustgrid.io

Learn more about
Trustgrid's Zero Trust connectivity,
visit **www.trustgrid.io**