White Paper

trustgrid

The Platform for Secure Access Service Edge (SASE)

What is SASE?

SASE is a new category of network security that integrates networking and security into a cloud-delivered service. At its core, SASE converges Zero Trust networking capabilities from SD-WANs and remote user access with security such as firewalls, cloud access security brokers (CASB), secure web gateway (SWG) and other services into a single identity-centric solution.

By Gartner's definition*, "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."

The assembly and orchestration of these services is managed from the cloud and delivered as a service that provides a blanket of protection over all users, devices, data and applications.

Why SASE and Why Now?

Today's users work from all kinds of devices to access corporate data and applications from a range of geographical locations. The rise of cloud computing and mobility have uprooted the fundamental assumptions of legacy technology infrastructure. The days of guarding a fortified perimeter (ie. the corporate data center) have given way to perimeter-less environments that spread applications across a variety of cloud, data center and on-premise environments. Data is now flowing everywhere, causing a general lack of control across all user and network activity.

Over the last 5 years, organizations have been able to reduce costs and increase agility by leveraging cloud and SaaS. But in that trade-off, they have lost their iron-fisted grip on network security. SASE attempts to protect these new heterogeneous environments by delivering cloud network security services based on a centralized set of policies. These policies are tied to the identity of the end user instead of the perimeter of a physical location.

By 2024, Gartner predicts 40% of companies will have a plan to adopt SASE architectures.

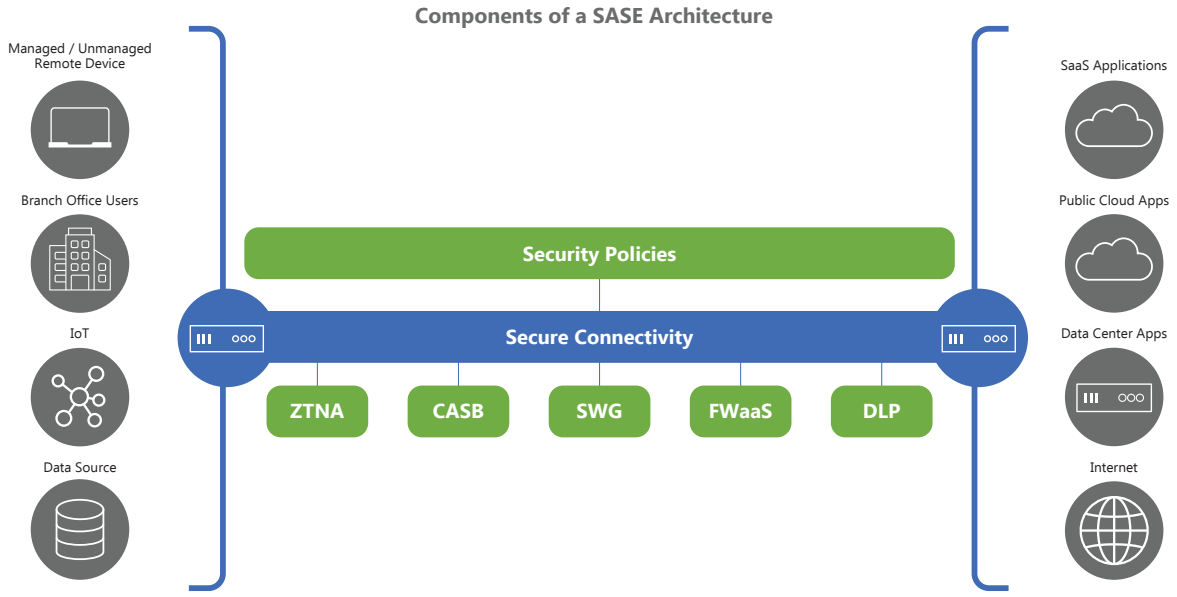
This combination of identity, networking and security into a single cloud-centric delivery model greatly simplifies the architecture of IT infrastructure and creates a continuously updating security posture that can evolve to the ever-changing threats and needs of the business.

www.trustgrid.io/sase

Components of SASE

In the name of speed, agility and simplicity, SASE converges network (SD-WAN, Zero Trust Network Access) and security services (SWG, CASB, FWaaS, DLP, etc). All of these services are integrated and delivered based on user identities and device context. The integration with an IdP or IAM solution allows identity-centric policies to be applied centrally and enforced at the edge. These policies guide all access and security related decisions.

A SASE architecture creates personalized micro-perimeters around users, devices, and applications, that are then additionally hardened by pushing network traffic through its integrated security functions.



While these components can be manually assembled and managed, the resulting service chaining causes management complexity and latency. SASE architectures seek to minimize the number of times that encrypted traffic is inspected through a deeper convergence of network and security capabilities. This requires moving security inspections out to the sessions instead of moving sessions to centralized inspection points. This is accomplished by running and managing security application components across a mesh of network points of presence (PoPs). These centrally managed PoPs each support the full range of networking and security capabilities and ensure low-latency service to users regardless of where they are accessing the network.

Orchestrated identity, networking and security services distributed through a network of PoPs eliminates bottlenecks at centralized data centers and balances the need for security with user experience, management and cost considerations. This dedicated SASE network ensures that data is protected without becoming overly burdened by latency and management overhead.

Trustgrid - The SASE Enablement Platform

The components needed to complete a SASE vision currently reside in multiple silos. Security providers hold domain expertise in things such as inspection, prevention and response; while companies like Trustgrid provide networking features such as Zero Trust networking, routing, encryption and traffic optimization. It is the integration of these components that make SASE transformational.

Gartner predicts** that the market for SASE will be divided. Some buyers will adopt a single vendor end-to-end approach while others will favor a multi-vendor approach that pulls services from both a WAN edge provider and curated elements of network security. Believing that most organizations will favor the flexibility to select best-in-class security services, Trustgrid enables customers and partners to build their own SASE architectures on a global zero trust network.

Separating Trustgrid as the ideal SASE platform for these security providers - when compared against most competitive networking solutions - is the integration of edge computing features. As a platform providing integrated SD-WAN, Zero Trust remote access, AND edge computing capabilities, Trustgrid simplifies the ability for security providers to convert to 'as-a-service' security models and quickly bring SASE solutions to market.

Edge computing provides a key element of a SASE architecture by allowing security applications to run at the edge. Through its edge computing powered network, Trustgrid allows security providers to move all solutions to a distributed, managed service model that addresses both cloud and legacy on-premise environments.

Many security vendors have spent 100s of millions of dollars building out proprietary PoP networks to enable SASE architectures. This may be a viable strategy for some solution providers, but others may not have the appetite to build or maintain this kind of overhead. While these dedicated PoP networks have been the standard, rapidly evolving solutions from AWS and Azure have increased the available options. The rationale of building massive PoP networks begins to erode when compared to the option of leveraging the global networks of public cloud operators to stand up new regions quickly. And for enterprises building their own internal SASE architectures, a more economical solution may include the coordinated use of both existing data centers and public cloud infrastructure.

Trustgrid has taken a more flexible approach to the PoP problem. As a platform delivering both networking and edge computing capabilities, we empower our customers to build their own PoP infrastructure as they need it. In each PoP security applications - seamlessly connected via the Trustgrid SD-WAN - are run and centrally orchestrated within containers on the Trustgrid edge computing platform. And because the platform has been designed from the ground up to deploy at massive scale, new sites can be turned up relatively quickly in 1 or 1000 locations with minimal effort.

Regardless of each PoPs location, a Trustgrid-enabled SASE architecture leverages these distributed points of presence to provide flexibility in addressing each organization's latency and data residency requirements. Once established, traffic can traverse dedicated connections or the public internet between PoPs. Public internet, secured end-to-end with mTLS tunnels, is used for a short hop to the SASE fabric where it is then inspected based on policy and optimized for best performance via intelligent routing.

Trustgrid Delivers the Fundamental Components of a SASE

Assembly of a SASE can be daunting. Where do I start? What do I do with my existing investments?

Trustgrid provides a turnkey answer to many of these questions. As a platform providing integrated remote access, site to site networking and edge computing capabilities, it simplifies the process for security providers to quickly bring robust SASE solutions to market in a fraction of the time it would take to build capabilities in-house.

Dedicated SASE networks can be created in parallel to existing infrastructure or swapped out as hardware appliances experience their normal end-of-life. Existing identity solutions can be leveraged and, in some cases, legacy hardware appliances may still be utilized. The flexibility of the platform gives it the ability to adapt to both existing infrastructure and make it extensible to new additions.

www.trustgrid.io/sase

The Cloud Networking Platform

The Trustgrid cloud networking platform contains all of the tools to build and manage secure networks between any on-premise or cloud environments.

The platform connects all relevant systems, gives system wide visibility and allows any security provider to deliver a full-fledged multi-tenant SASE service. It delivers zero trust access in coordination with an organization's identity provider, but also contains the ability to issue certificates for network devices with a cloud-native certificate authority (CA).

Network and security admins can automate the tasks of configuration, provisioning, and node deployment. This allows new edge locations to be stood up in hours and new users added in just minutes.

Platform tooling pushes code updates to nodes, centralizes logging, monitors status, as well as other security and application management functions. It is equipped with a variety of support tools to enable less technical staff to extend Level 1 support into tasks previously reserved for Level 3 engineers.

As an API-first platform, management APIs enable the scripting of common tasks, bulk configuration management and custom UI integrations. Trustgrid gives customers the ability to manage each of these systems themselves or provides advanced support for a more turnkey experience.

The Trustgrid's Cloud Management Portal is the control center of the platform. Serving as the primary interface for all platform management features, the portal provides intuitive control and visibility over all components on the network.

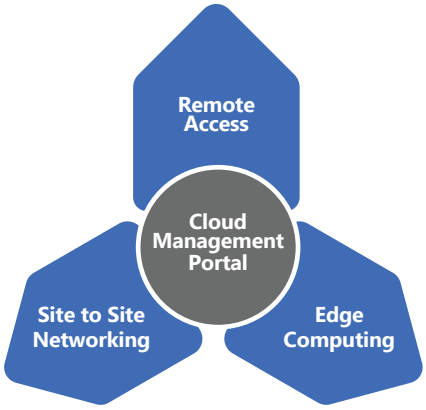
Remote User Access

Securing the access to applications with Zero Trust Network Access (ZTNA) is an ideal place to start a SASE architecture. In the Trustgrid platform, private applications (from the cloud or data center) move away from a network-centric security approach and instead provide users secure connectivity directly to the individual applications they need to access.

Trustgrid ZTNA features an agentless remote user access portal to extend encrypted connectivity to cloud and data center applications without any local agent. Trustgrid ZTNA was purpose-built for overcoming the challenges of secure application access without deploying and managing agents on user systems.

Access to applications is based on contextual access policies and adapts based on a user, device or application and never implies trust. To improve visibility and control over the environment the service tracks user activity in real-time and can stream access logs to the company's SIEM.

The Trustgrid Connectivity Platform



Remote user access also supports existing open-source security clients such as WireGuard and OpenVPN.

Site to Site Networking

Trustgrid's application-centric SD-WAN is designed to build cloud-to-on-premise, branch-to-branch and multi-cloud networks. Network nodes can run in most public and private cloud environments and be deployed via a virtual machine image, off-the-shelf hardware or virtual appliances for simple on-premise installation without networking expertise onsite. These nodes provide secure tunnels between edge locations and can be used to optimally route traffic to improve latency challenges.

Tunnels work over private circuits such as MPLS, AWS Direct Connect or Azure ExpressRoute or handled over standard broadband connections.

www.trustgrid.io/sase

Edge Computing

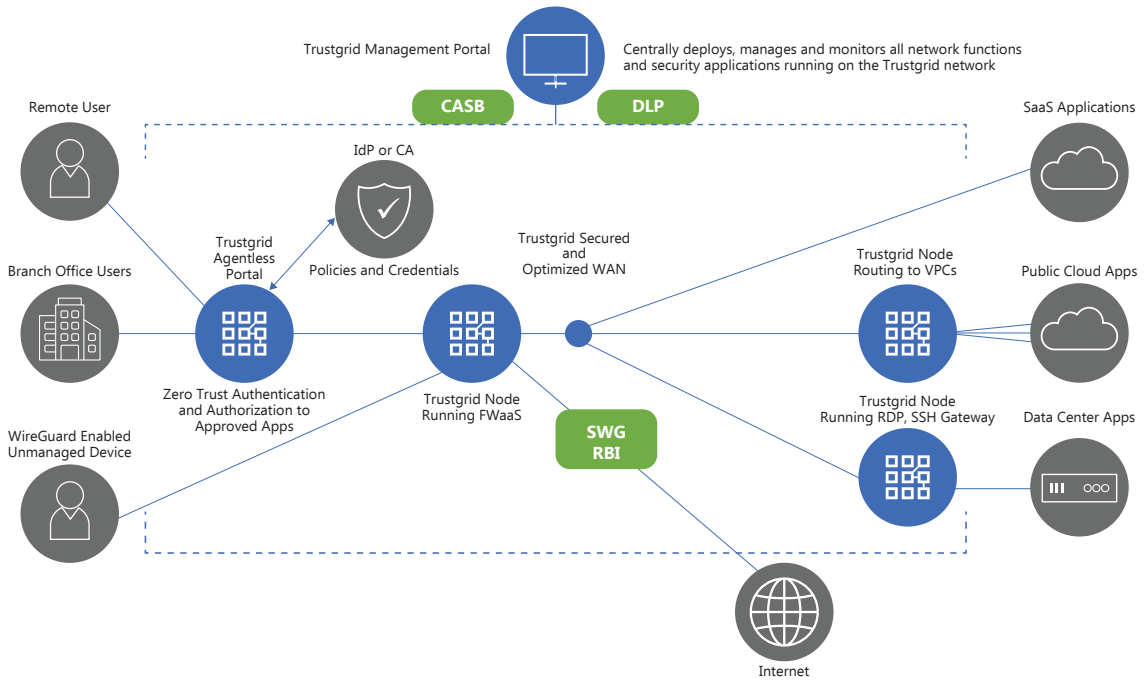
Trustgrid's EdgeCompute seamlessly integrates with ZTNA and site to site networking capabilities to provide a serverless computing platform for deploying and supporting applications at the edge.

EdgeCompute uses the network's edge nodes to run applications across the network and incorporates centralized device and application lifecycle management.

When used in secure access service edge (SASE) architectures, EdgeCompute eliminates the need to funnel all network traffic to centralized inspection points by moving security and policy intelligence to the edge.

The processing and throughput of an EdgeCompute node can be adjusted based on the hardware it is deployed on and is capable of handling any sized workload.

A Trustgrid Enabled SASE Architecture



Additional Features

The Trustgrid platform provides full networking-as-a-service capabilities including:

- Full L2 / L3 / Proxy SDN feature set
- The flexibility to connect any user, device or environment
- 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

Built as an API-first software-defined networking solution, the Trustgrid platform is able to integrate into any existing security management portal and provides centralized deployment and management services allowing for any security solution to become a cloud-delivered service.

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 an SDN 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.

*Gartner, Initial Secure Access Service Edge Forecast (Aug 2020)
**Gartner, The Future of Network Security Is in the Cloud (Aug 2019)

www.trustgrid.io/sase

888.308.8995
info@trustgrid.io