SOLUTION BRIEF

Versa SASE (Secure Access Service Edge)

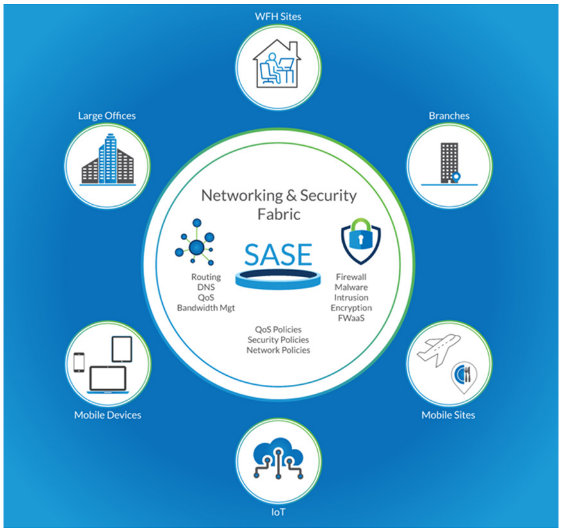
Finding Control in All the Commotion

Corporate applications and data are hosted in hundreds of private and public locations around the world with sensitive information constantly moving from branch offices, home offices, and thousands of remote users to and from private data centers and the cloud. These transactions are happening every second, every minute, every day. On top of this, users on different devices are accessing these applications from thousands, sometimes millions, of disparate locations around the world all requiring differing levels of security for each access request. It seems almost impossible to establish control in all the commotion. The only way forward to achieve visibility, security, and control is for organizations to reimagine their existing architectures to deliver consistent policies over who, what, and where access is taking place. Achieving this consistency requires the unification of networking and network security into a single solution that can be delivered anywhere in the world.

Enter Secure Access Service Edge, or SASE (pronounced sassy). SASE is an approach towards enterprise networking and security that unifies network and security services (such as Secure Web Gateway, Cloud Access Security Broker, Firewall as a Service, and Zero Trust Network Access) with networking capabilities (such as SD-WAN, routing, and access) and delivers these flexibly via the cloud, on-premises, or as a blended combination of both. By combining both networking and security, this modern architecture enables seamless and secure user access to everything that those users have privileges to, anytime, and from anywhere. SASE is the simplest and most scalable way forward to continuously secure and connect the millions points of access in and out of the corporate resources regardless of where they are located.

SASE is the Modern Network

SASE enables organizations to securely connect branch offices, users, applications, devices, and IoT systems regardless of their location. In addition to providing secure access, SASE enables fast, seamless, and consistent application performance, via the cloud, on-premises, or a blend combination of both, ensuring a positive user experience. SASE include many networking and network security services, but at the core require Software Defined Wide Area Networking (SD-WAN), Zero Trust Network Access (ZTNA), Secure Web Gateways (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Remote Browser Isolation (RBI). Several capabilities found in SASE, such as SD-WAN and SWG, have been leveraged by organizations as industry best practices for several years. SASE transforms the traditional networking model of networking and security capabilities being service chained together. SASE enables organizations to adopt an architecture that connect, secure, and monitor applications and users where they exist. SASE services are tightly integrated within a single software stack without the need to connect multiple disparate functions, therefore, achieving the control they need.



What Are the Key Considerations for SASE?

Organizations looking to implement SASE should consider the following requirements if they want the SASE implementation to be extensible and scalable to every user, device, and application, anywhere in the world:

1. Identity-aware: Traditional perimeter-based security model relies on source and destination IP addresses and TCP (Transmission Control Protocol) data for trusting users and devices with application access. SASE must take into context the identity of the user, device, and applications along with contextual security policies to authorize access.
2. Established trust: Establishing trust in the access of users and devices starts with the fundamental philosophy of trusting no one. Only validating the identity of the user and their access privileges, will trust be established.
3. Context-driven: SASE must understand the dynamic context of the user accessing corporate applications: the geolocation, the browser, the difficulty travel, the device health, the software versions, behavioral anomalies, and more, to understand the risk of the action being performed.
4. Cloud-delivered: A good architecture must integrate and deliver all networking and security capabilities in the cloud ("as a service"), making the enterprise network more agile, scalable, efficient, adaptable, and cost-effective.
5. Support for all network edges: SASE must support networking and security requirements of all network edges—branch offices, remote and mobile users, data center, and cloud environments.

6. Globally distributed: SASE must include a globally distributed system of Points of Presences (PoPs) to ensure all the network edges experience low latency and high performing connectivity regardless of where they are located.

Versa SASE

Versa began delivering SASE capabilities several years before SASE became an industry term. Versa's approach to network architecture is that services should not be chained or connected but built together to operate with the highest levels of performance and security. Versa SASE delivers a comprehensive integrated SASE solution within a single software stack which mitigates the requirement to perform service chaining, cascading, or virtual interconnect between SASE services required by other solutions in the market. Versa Single-Pass Parallel Processing architecture combines full-featured SD-WAN, complete integrated security, advanced scalable routing, genuine multi-tenancy, and sophisticated analytics into one software image.

With a single interface to configure and implement corporate policies, Versa SASE delivers visibility and control through a single pane of glass. Versa protects all corporate resources with unified security policies for every session for every user, on any device, accessing any application. Security is embedded which results in no security breakage from service chaining which leads to better security hygiene, true access authenticity and only one point of decryption.

Key Versa SASE services available via the cloud, on-premises, or as a blended combination of both include, but are not limited to:

Versa Services	
Software-Defined Wide Area Networking (SD-WAN)	A software-defined architecture for the Wide Area Network (WAN) increases network performance and agility.
Zero Trust Network Access (ZTNA)	Secure and private connectivity to corporate applications while implementing a least privileged model to access.
Secure Web Gateway (SWG)	Gateway protection against internet threats preventing unsecured traffic from compromising internal networks and users.
Cloud Access Security Broker (CASB)	Policy enforcement that secures data flowing between users and cloud applications to comply with corporate and regulatory requirements.
Firewall-as-a Service (FWaaS)	A cloud service that delivers firewall and other network security capabilities to inspect and control all network traffic
Remote Browser Isolation (RBI)	A risk mitigation solution that moves the execution of users' browsing activity to a remote server hosted in the cloud or on-premises

Versa SASE is designed to deliver secure and reliable client-to-cloud connectivity. It enables and delivers consistent security policies, network policies, business policies, user policies, and application policies seamlessly between on-premises and cloud services. Other key capabilities in the Versa SASE services: (1) Virtual Desktop infrastructure that allows the management of end user desktops over the network, (2) Web Application Firewall to protect web applications from threats like DoS attacks, (3) Sanitized Domain Name System (DNS) security, (4) Network sandboxing and obfuscation, (5) edge compute protection to protect all edge access, (6) traditional virtual private network (VPN) services to offer network access encryption, and (7) identity protection capabilities such as multi-factor authentication and risk-based access control.

Versa SASE Components

Versa SASE services are delivered through a single-pass architecture that is comprised of the following management, orchestration, and endpoint components:

Versa Operating System (VOS™)

The highly flexible Versa Operating System (VOS) enables Enterprises, organizations, and service providers to deploy SASE in branch offices, cloud, campus and data centers. Regardless of where VOS is deployed (on-premises or in the cloud), all network and security capabilities are provisioned and managed centrally through the Versa Director, a single-pane-of-glass management platform. Versa Analytics works in conjunction with Versa Director to provide visibility, baselining, correlation, and predictive analysis for network, application usage, and security events. With Versa Analytics, all network security, application usage, export reports and logs are analyzed, filtered and are easily searchable for events to derive actionable insights.

Versa Secure Access Client

Versa Secure Access Client (VSAC) is a mobile software agent/application that runs on and extends Versa SASE to client devices. Versa Secure Access Client creates a secure and encrypted connection from remote device to the distributed system of Versa Cloud Gateways with application segmentation and SD-WAN services. Upon user authentication and access authorization through Versa Cloud Gateways, users with VSAC can securely, reliability, and with high performance connect to enterprise applications in public and private cloud.

Versa Secure Web Gateway

Versa Secure Web Gateway (SWG) is hosted and maintained by Versa cloud gateways around the globe. SWGs provide low-latency and secure access to the Internet for Versa branches and secure access clients. Customer branch devices are automatically connected to all selected gateways via SD-WAN, ensuring best-path selection with SLAs, and cloud-based next-generation firewall for all traffic utilizing SWGs. This secure connection helps protect secure Enterprise sites, home office or traveling users with distributed applications without compromising on security or user experience.

Versa Cloud Gateways

Versa Cloud Gateways run industry leading VOS multi-tenant software. The Cloud Gateways are globally distributed and provide distributed secure, reliable, and high-performance access to cloud applications, services, and resources in addition to providing cloud-delivered SASE. Gateways authenticate users, authorize the application access and secure the enterprise network from external threats. Versa Cloud Gateways integrate scalable advanced routing, comprehensive security, industry-leading SD-WAN along with secure access. In addition to all of these services, they also securely connect to and integrate with existing infrastructure in Enterprise network and datacenter.

Versa Concerto

Versa Concerto is the orchestration platform that simplifies the creation, automation, and delivery of services using VOS from a single pane of glass. Versa Concerto provides a complete set of end-to-end orchestration functions of services including configuration design, implementation, zero-touch-provisioning, deployment, monitoring, and analytics capabilities for industry-leading SD-WAN, NGFW, UTM, Routing, uCPE, and Versa Secure Access (VSA) services. Versa Concerto is based on microservices architecture and is designed to run on public or private clouds, making horizontally scaling both easy and flexible for SASE initiatives.

Versa Titan

Versa Titan is hassle-free SASE solution with advanced application intelligence managed from the cloud, making it easier for IT to manage and secure their branch services. Powered by the marketing leading VOS, Versa Titan delivers an easy-to-deploy, cloud managed SASE solution for lean IT mid-market enterprises. With cloud managed Versa Titan, enterprises can expect accelerated business growth as well as simplified deployment and administration. Versa Titan includes multiple access types, automated multi-path site-to-site VPN, direct internet breakout to any application or user, dynamic application prioritization, and more.

Versa SASE Architecture

A successful SASE architecture begins with integrated security, advanced networking, full-featured SD-WAN, genuine multi-tenancy, and sophisticated analytics in a single software image. Versa SASE is cloud-native, software-based, and hardware neutral. Versa SASE is built on the Versa Single-Pass Parallel Processing architecture which dramatically lowers latency, significantly improves performance, and mitigates security exposure. Versa SASE is available via the cloud, on-premises, or as a blended combination of both while enabling consistent security, networking, business, and analytic policies anywhere in the world. These services may be deployed on any brownfield environement and can scale depending on the type, size, or requirements of each organization, individual branch office, or users.

Versa SASE is delivered through a globally distributed system of Versa Cloud Gateways in 90 POP locations which have peering relationships. Versa SASE supports highly scalable inline encryption and decryption and is built from the ground up to be multi-tenant.

Flexible Versa SASE Deployment

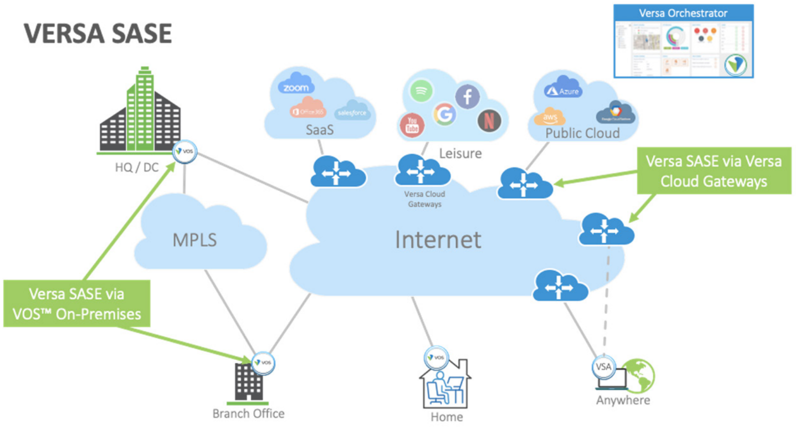
Versa SASE allows organizations to deploy SASE in the most flexible manner between light cloud to heavy cloud to light branch to heavy branch deployment options. Versa SASE is available:

On-Premises

Versa SASE services are deployed on-premises in branch offices, work-at-home, regional offices, headquarters, data centers, and cloud. An on-premises implementation includes the option to extends connectivity via SD-WAN to a distributed system of Versa Cloud Gateways which are located at the front doorstep of almost every cloud service available. This extension of the corporate network enables fast, reliable, secure access to cloud applications around the globe.

Versa management is typically deployed on the customer premises (Data Center) on bare metal appliances or virtual environments. Alternatively, Versa management may also be deployed in a public cloud environment.

In the on-premises deployment model, the administrative control is completely with the enterprise IT team. Based on requirements, Versa management can be deployed so



that data never leaves the enterprise network. The entire Versa management system can be air-gapped from the internet to provide additional level of security.

Hosted

Organizations who prefer implemented Versa SASE as a management service will typically leverage this deployment model, also known as "managed service provider. In the hosted model, the Service Provider is responsible for configuration management and monitoring of the enterprise SASE implementation.

Service Providers leverage Versa multi-tenancy capability to deploy a single Versa management system for multiple tenants. Versa Role Based Access Control (RBAC) allows the Service Provider to securely share the co-management of the enterprise network between the Service Provider and the enterprise IT team.

Cloud

Versa provides cloud managed orchestration for Versa SASE to both Enterprise and Managed Service Providers. Versa offers cloud managed orchestration as a service in a shared or dedicated option in both public and private cloud.

In this model, the Versa management is deployed in a geo-redundant design and is managed and maintained by Versa NOC 24 X 7. Role Based Access Control (RBAC) is leveraged to segregate different tenants and to provide private Versa management. In this model Versa NOC is responsible for managing and maintaining Versa SASE, while the customer IT team is responsible for management and monitoring of the CPEs.

Blended Combination

Most Enterprises, businesses, and organizations do not fit a one-size-fits-all implementation of either cloud or on-premises. Most organizations have a variety of locations which differ by size, services, and complexity. Some locations may require more SASE services be delivered on-premises (i.e., a power branch with several service available for clients and employees) while other locations benefit from more SASE services delivered via the cloud (i.e., a light branch offering basic services to clients) and still other locations may need a blended combination of SASE via the cloud and on-premises.

Versa SASE is flexible enough to be deployed seamlessly as a blended combination of both cloud and on-premises services. VOS (Versa Operation System) runs both on-premises and cloud SASE services which creates consistent services, features, policies, and configuration regardless of where the service is delivered.

One set of locations may be mostly on-premises SASE, another set of locations may be mostly cloud SASE, while the remainder is a balance of both cloud and on-premises. All of these are managed via the same management interface and policies are applied consistently and ubiquitously across cloud and on-premises implementations.

Benefits of a SASE Enterprise

Versa SASE is available to enterprises, organizations, and partners to build their own private SASE service on their own premises or in their own private cloud if they choose. This flexibility enables them to completely take control of their service, yet take advantage of performance, services, and capabilities of the market leading Versa SASE solution. Once deployed, Versa SASE customers can achieve:

1. End-to-End Visibility and Control
   Through a single-pane-of-glass interface, SASE offers complete visibility into users, devices, and applications across the entire network- whether on-premises or in the cloud. It automatically classifies application traffic on all ports to determine if there are any unsanctioned applications being run on non-standard ports. This readily available information helps the security team in making appropriate policy changes quickly to minimize security risks. By making network-wide security information available in a single central location, SASE enables the security team to derive critical insights, troubleshoot faster, and make better-informed decisions.
2. Consistent Security Enforcement
   SASE enables security teams to bring cloud platforms, data centers, branch offices, remote and mobile users under one umbrella and protect them with one unified security policy pushed to every user on any device, anywhere. Versa SASE allows security teams to dynamically make changes and roll out new updates from a single location, saving time and improving the security posture. Having centralized control over security policies helps eliminate fragmentation, blind spots, and policy misconfigurations.
3. Optimized Application Performance
   Versa SASE has application awareness and dynamic traffic steering capabilities that monitor traffic patterns in real-time to analyze performance parameters such as latency, jitter, and packet loss. Based on these parameters, Versa SASE automatically routes traffic over the ideal transport route. In doing so, it ensures all applications, especially voice and video, run seamlessly and reliably for an uninterrupted user experience.
4. Simplified Administration and Management
   As SASE operates from the cloud and delivers all the networking and security capabilities in a single unified framework, it eliminates the need for dedicated point devices that are deployed for different requirements. Versa SASE removes the administrative burden of procuring, installing, configuring,

and managing these devices at each branch location. Instead, security teams can streamline and manage all the network and security operations through a single solution.

5. Lower Capital and Operational Expenses
   Installing commodity point products in branch locations is costly. Operating and managing these products takes dedicated and trained IT resources with appropriate skills and expertise, in turn slowing down and eating into the core IT competency. Versa SASE helps cater to all network and security requirements with a single software stack with embedded security, saving the capital investment in disparate products and allowing the IT team to focus on strategic value-adding work.

Versa SASE Accelerates and Secures Digital Transformation

Today's legacy approach to putting piecemeal network and network security solutions together is not adequate to support and secure cloud-based applications, direct Internet access, unmanaged devices, mobile users connecting from anywhere in the world, bandwidth-intensive voice and video applications, and thousands or millions of IoT devices. Organizations need to adopt a SASE framework in order to achieve the benefits of a digital transformation. By doing so, a digitally transformed organization will be able to optimize their business processes, technologies, and customer experiences to meet changing IT and market requirements of a new age of access. Digital transformation will allow organizations to reduce the cost and complexity of stagnant and outdated technologies, processes, and architectures.

Versa SASE delivers on the promises of a digitally transformed enterprise with cost savings on bandwidth, network management and IT staff, security, and scalability. With a single management console to deliver all SASE services, Versa eases policy enforcement and deployment anywhere when scaling to new locations or remote users, eliminating the costs of installing and maintaining IT infrastructure. For network management and IT, Versa consolidates all components into a single-pane-of-glass, eliminating cost, complexity, and coordination of configurations and deployments.

About Versa

Versa Networks, the leader in SASE, combines extensive security, advanced networking, full-featured SD-WAN, genuine multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers. Versa Secure SD-WAN is available on-premises, hosted through Versa-powered Service Providers, cloud-delivered, and via the simplified Versa Titan cloud service designed for Lean IT. The company has transacted hundreds of thousands of software licenses globally through its global Service Providers, partners, and enterprises. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, Liberty Global Ventures, Princeville Global Fund and RPS Ventures.

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com