WHITE PAPER

# Secure Private Access

*A New Strategy for a Comprehensive "Working-From-Home" Solution*

## The Impact of the Pandemic on "Work-from-Home"

As the world has adjusted to the changes brought on by the COVID-19 pandemic, Enterprises in particular were wrestling with the new network challenge: how to allow employees to work remotely in a secure and optimal manner that does not disrupt business continuity. The previous remote networking model revolved around Virtual Private Network (VPN) appliances that had a fixed capacity and were implemented in Enterprise data centers. Historically, most Enterprises only allowed around 10 to 20 percent of their workforce to use a VPN connection to access resources in their data center. Enterprises that attempted to augment the traditional VPN solutions quickly realized that there existed three problems with expanding their VPN solutions. First, the hardware was in short supply and due to the restrictions on travel caused by the pandemic, wait times for new hardware to ship did not meet the strict timelines needed to support their workforce. Secondly, price became an issue during a time when organizations certainty around budgets. Third, the increase in Work-from-Home traffic (WFH) caused a bandwidth constraint at the VPN concentrator locations. This was due to all traffic being tunneled to the VPN concentrator; and then, if not destined to the Enterprise, forwarded to the Internet. And the same happened to the return traffic creating a double bandwidth utilization for all Internet traffic from WFH employees.

The hardware solutions required many different appliances to be purchased which increased the cost considerably. In addition, purchasing multiple components was not conducive to scaling a business. Lastly, Enterprises needed to factor in the time to install, configure, and test the new appliances before the solution were to be active for use and accepting remote employee connections.

These struggles lead the enterprises to explore cloud-delivered security services or SD-WAN services as a method to augment the current VPN solutions already implemented because services allowed Enterprises to offload much of the administrative and management pain points. The migration to "As-A-Service" model accelerated the delivery of the Secure Private Access because it met the immediate remote working needs caused by the COVID-19 pandemic.

## Emergence of SASE

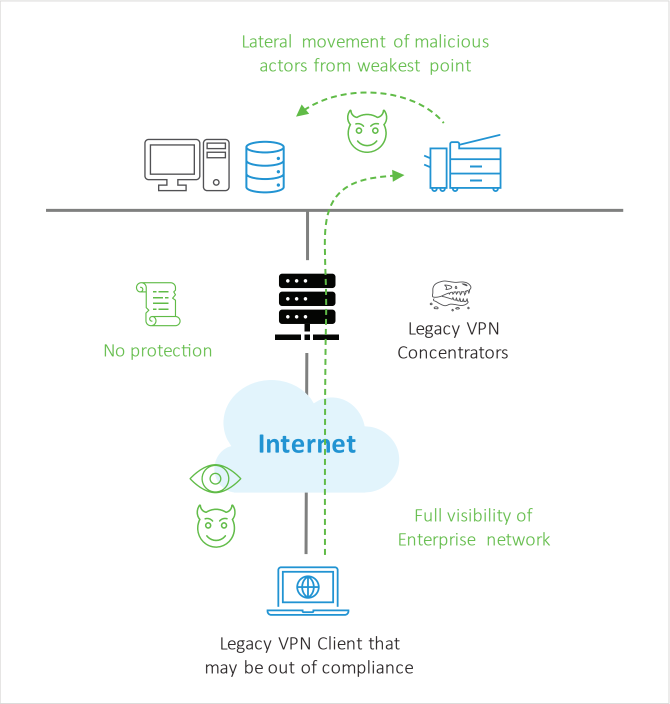
The emergence of Secure Access Service Edge (SASE) melded the security and SD-WAN together in a way that optimally provided Enterprises an architecture to protect users, devices, and applications anywhere in the world. In SASE deployments, remote working is considered Secure Private Access. Currently there are many existing and legacy vendors that offer varying portfolio of products on what they believe Secure Private Access consists of. This variance in definition of Secure Private Access has led to much consumer confusion and market obscurity.

## What is Secure Private Access?

What is a Secure Private Access? What are the components that make up Secure Private Access? What are the benefits? Why is a native SASE Vendor the best choice to deliver a strong and resilient Secure Private Access solution?

In a traditional VPN solution, there are many components that are similar to a SASE Secure Private Access solution. Below is a diagram of how a traditional VPN client can access database resources and be left exposed to vulnerabilities and threats.

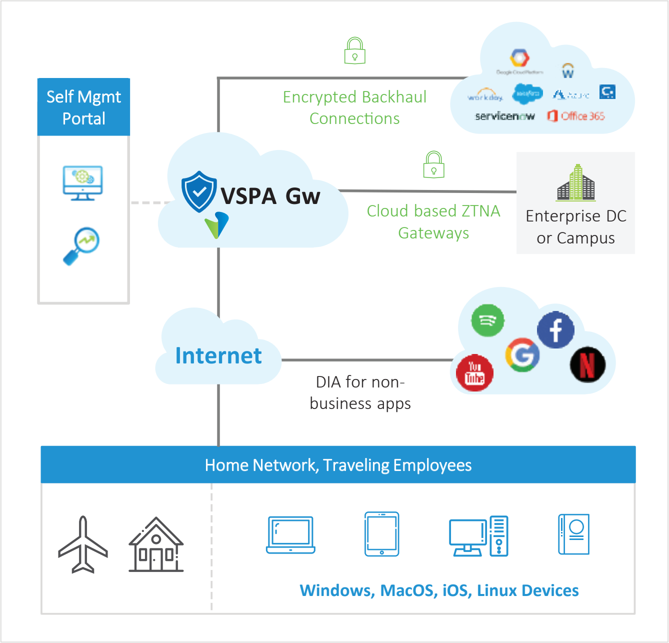
A typical VPN solution is composed of a VPN concentrator (appliance) installed on the Enterprise network (normally at a data center) and a VPN client installed on the device that the employee would utilize to create the secure connection to and from. For redundancy and capacity planning, multiple VPN appliances would be located at different locations inside the Enterprise network. The VPN client would then have a drop-down selection to choose which location to use for the connectivity. Some of the clients would have a global auto-selection mechanism but normally the connection was based on DNS and not on the actual performance of the VPN appliance. This was problematic because the VPN appliance would not be able to choose the most optimal path and connection.


Lateral movement of malicious actors from weakest point
No protection
Legacy VPN Concentrators
Internet
Full visibility of Enterprise network
Legacy VPN Client that may be out of compliance

Another feature of typical VPN model is the L3 authorization. The traditional VPN applies the policy that an authenticated user is provided with authorization to access any or all network resources. The application servers are responsible for authenticating and authorizing users for individual applications. This makes the system vulnerable to scanning attacks and other forms of attacks which exploit the existing vulnerabilities in the applications.

In a SASE model, Secure Private Access has the same two components as the VPN service, the VPN concentrator and the VPN client, but has added much more comprehensive and up-to-date capabilities. In this model, the Secure Gateway replaces the VPN Appliance. Unlike the VPN appliance that is installed within the Enterprise premises, the Secure Gateway is instantiated in the Cloud which allow for flexibility, scalability, and elasticity. A cloud instantiation provides multiple access points to a single Secure Gateway allowing the gateway to scale and be flexible enough to also instantiate multiple Secure Gateways in different availability zones or regions around the world.

As seen to the right, a SASE Secure Private Access solution include a SASE Client that is installed on the employee device and will connect to a Secure Gateway when accessing corporate resources. This connection provides an encapsulated and encrypted path to the SASE Service which provides numerous security and performance benefits.

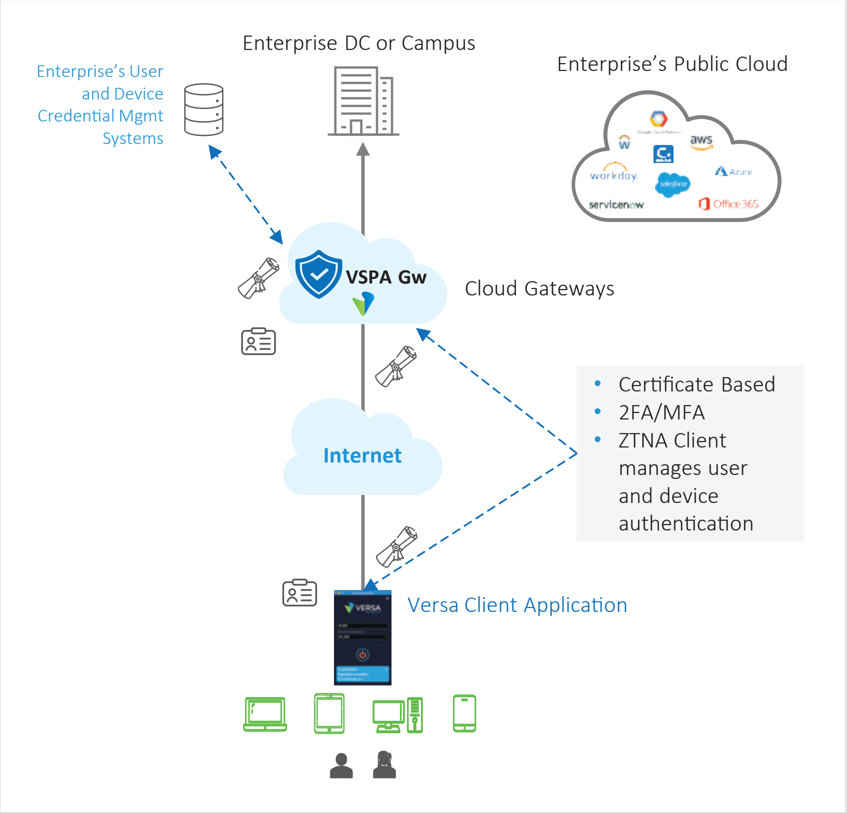

Self Mgmt Portal
Encrypted Backhaul Connections
workday
servicenow
Office 365
VSPA Gw
Cloud based ZTNA Gateways
Enterprise DC or Campus
Internet
DIA for non-business apps
Home Network, Traveling Employees
Windows, MacOS, iOS, Linux Devices

The next component of SASE Private Secure Access is the connection to the Enterprise network. In a traditional VPN solution, this was a direct connection at the Enterprise data center. In the SASE Service, this is a network connection, usually with an IPSEC tunnel or a private network connection to the Enterprise. For redundancy, multiple Enterprise network connections can be established.

Since Secure Private Access is part of a SASE Service, the SASE Service will provide security services either at the Secure Gateway or in the SASE Cloud. This set of security services may be extensive, but for the Secure Private Access, it should offer the following security functions at minimum: Network Firewall, Identity and Access Management, Cloud Access Security Broker, Malware Detection and Response, Data Loss Prevention, Intrusion Detection and Prevention, Domain Name Filtering, URL Filtering, and Full Forward IP Proxy. Each of these security services are necessary for assuring that the access and data that is entering and leaving the Enterprise network and cloud services are protected. In this new model, the SASE Secure Private Access solution is an evolution of the traditional VPN.

## Versa Secure Private Access (VSPA)

Versa Secure Private Access (VSPA) is Versa Network's implementation of the Secure Private Access technologies. Versa Secure Private Access is an integral component of the Versa SASE Solution. Secure Private Access can be purchased as Versa SASE Service (SASE-as-a-Service) or as a stand-alone remote access service (VSPA-as-a-Service). Both options come with a SASE Client, Secure Gateways (as a Cloud Service), and an extensive suite of security services. However, the Versa SASE solution has more security services than the stand-alone VSPA such as the ability to utilize SD-WAN for the network connectivity.



The Versa Client has the ability to connect to multiple Secure Gateways anywhere in the world. This approach provides resiliency because it does not have to re-establish a connection to the SASE Service in the event of a network failure, allowing optimal up-time. The Versa Client can select the best Secure Gateway based upon performance metrics of the network connectivity to a given Secure Gateway and the performance of the Secure Gateway itself.

The Versa Client is available on the following platforms:

- MacOS
- Windows10
- iPhone
- Android
- Linux

The Versa Client acts as a policy enforcement point. As an enforcement point, the client captures data regarding the connecting device and the user requesting access. Based upon appropriate corporate policy, the client will determine what applications get steered to the SASE Service and which applications can go directly to the Internet. The Versa Client also has the ability to direct traffic based upon policy through a secure, private connection.

Policies for the Secure Private Access are broken into two parts: (1) the authentication and authorization of the user to use the SASE Service and (2) the authorization of the user to actually perform an action through the service. The Versa Client authenticates the user based on multiple methods per the corporate policy. For example, this policy could require that the authentication be issued via SAML, LDAP, SSO and just include a traditional login-password combination, multi-factor authentication, one-time Password, or certificate authentication. Based on the policy, different authentication methods could also be triggered based on the contextual access of the user: geolocation, time, device health, and more. For example, an LDAP authentication is required when accessing from the employee's home, but multi-factor authentication is required for when the employee is traveling and accessing from new locations.

The Versa Secure Private Access service protects the clients as well as applications by:

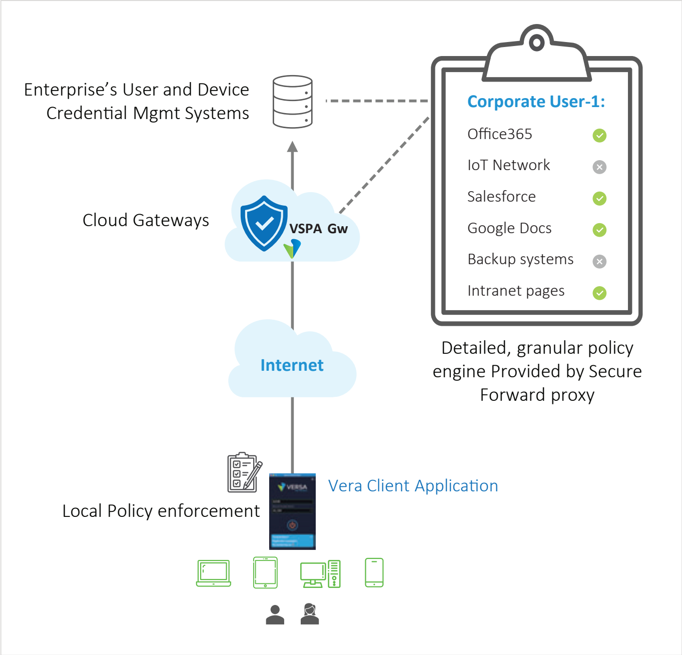
- Applying per user policies to ensure that users who are authorized to access specific applications are only allowed to reach the application.
- Applying policies which hide the network topology of the applications from the users and vice versa

VSPA intelligently applies combination of Forward proxy, CGNAT, ALGs and DNS proxy to ensure that the end user clients are not exposed to actual IP Address space where the applications are hosted. Thus, a malicious actor who may have access to the device will not be able to glean more information about the network internals creating a barrier for further attacks. The solution works seamless with variety of applications including FTP, Voice, and Video.

The Versa Client has the ability to enforce device compliance based upon many different factors like:

- Anti-Virus version
- Anti-Virus signature version
- Operating System type and version
- Operating System patch
- Corporate device or personal device
- Specific software installed on device
- And other parameters

By inspecting parameters on the device, the granularity of the context allows for organizations to establish an End Point Information Profile (EIP) when devices are connecting to the Enterprise network. Included in the EIP are additional checks such as a compliance check and reporting about the remote access. All this information is available through the Versa Analytics platform that is include in the Versa SASE dashboard.



The EIP must also authenticate and authorize a user when they are accessing via their compliant device and once authenticated, the corporate polices will determine if the user is allowed to actually perform the requested actions. Corporate policies can be applied at the application level to give a wide granularity of control such as requiring session authentication or restricting access within an application. In addition, corporate policies can be further narrowed to include a specific user and a specific application flow with a specific set of contextual parameters such as not allow a remote, traveling user to access sensitive HR files within an application.

For Bring Your Own Device (BYOD) scenarios, connections to the Versa SASE Service can be made without the installation of a Versa Client. The Full-Forward IP proxy would provide a captive portal for these devices to register, get authorization, and then get access granted. Where a Versa Client is not utilized to the secure connection, the secure connection can only send the traffic to the Versa Cloud Gateway and at that point the SASE Service would be the enforcement point to implement the corporate security policies.

## Leveraging Cloud Gateways

The Versa Cloud Gateways can be implemented in numerous cloud services such as AWS, Equinix, and Microsoft Azure. Versa Cloud Gateways allow for greater flexibility in where multiple SASE services can be offered. Having a global, dispersed network of cloud service Points of Presence (PoPs) provide greater flexibility and fault tolerance. In addition, having more PoPs provides better customer performance because connection can be determined by the best performance path through a Versa Cloud Gateway to leverage the Versa SASE Services.

Since the Versa SASE solution utilizes a Full-Forward Proxy, the Enterprise private networks are obscured from the public and does not expose the actual IP addresses of the Enterprise resources. This network obfuscation extends to the Enterprise cloud instances if the SASE service is utilized to connect to the Enterprise private cloud instances.

The Versa SASE solution allows the Enterprise to establish multiple network connections either over a public Internet or via a private network access method, such as a SCI (AWS) or Express Track (Azure). This flexibility provides a better customer experience as the traffic would not need to be back-tunneled to the Enterprise data center but could still be secured by the SASE service.

In addition, Versa SASE has the ability to connect to an Enterprise's private virtual cloud instances. By using Versa Cloud Gateways in cloud instances, the Versa SASE Service can utilize

SD-WAN capabilities within the Versa Cloud Gateways to route the appropriate applications to the target Cloud instances based upon network performance and the performance of the application cloud instances.

Lastly, where the Versa's Multi-Cloud Service is used to connect to the Enterprise private cloud or public cloud instances, Versa can arbitrate over the private cloud Enterprise connection or utilize an encrypted path via the public internet, thus providing a built-in secure failover for the public or private cloud instances.

## Versa Security Services

Versa has numerous security services that can be utilized to protect traffic and assure that the Enterprise is protected against breaches and threats. For example, any information that is crossing the Enterprise network should be analyzed for malicious content and any data that is leaving the Enterprise network needs to be cross referenced against the Data Loss Prevention policies and ensure that no Intellectual Property is being lost. In addition, devices accessing the Enterprise network need to meet the minimum corporate software compliance check and that all sensitive information has been secured.

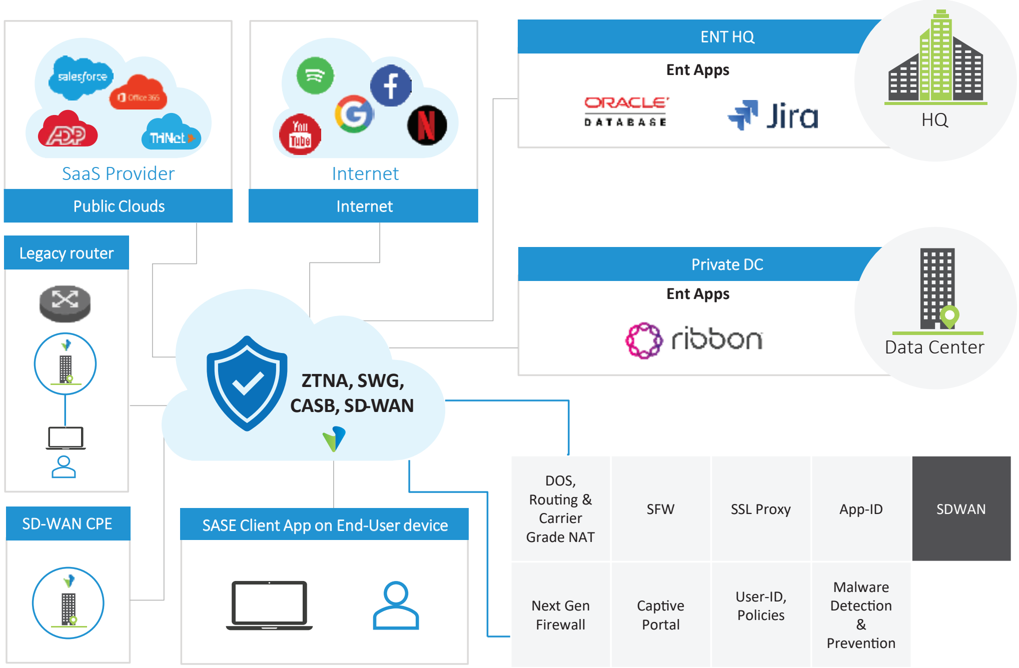
Versa offers the following security services:

- Next Generation Firewall
- Application Aware Access Control
- Identity and Access Management
  - SSO
  - SAML
  - Active Directory
  - Multi-Factor Authentication
- Endpoint Security Compliance
  - Operating System Version
  - Anti-Virus Version
  - SASE Client Level
  - Firmware Level
  - Patch Level
- Cloud Access Security Broker
- Malware Detection and Response
- Data Loss Prevention
- Intrusion Detection and Prevention System (IPS/IDS)
- Secure DNS Proxy
- Domain Name Filtering
- URL Filtering
- Full-Forward IP Proxy
- Captive Portal

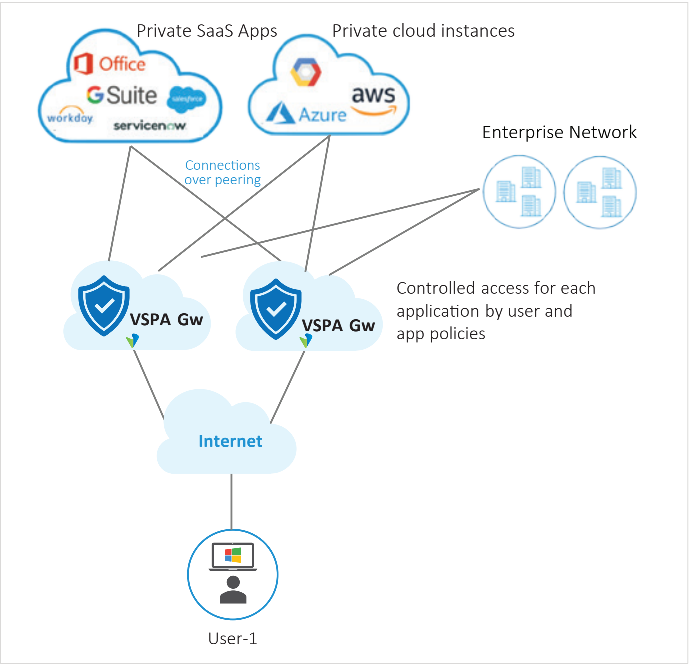
Versa VSPA and Versa SASE Services offer multiple methods to consume the security services listed above. Both Versa VSPA and Versa SASE provides for multiple tiered levels of security to meet any business need.

## The Enterprise Advantage with Versa SASE

Utilizing Versa SASE provides benefits to the Enterprise customer in five different ways:

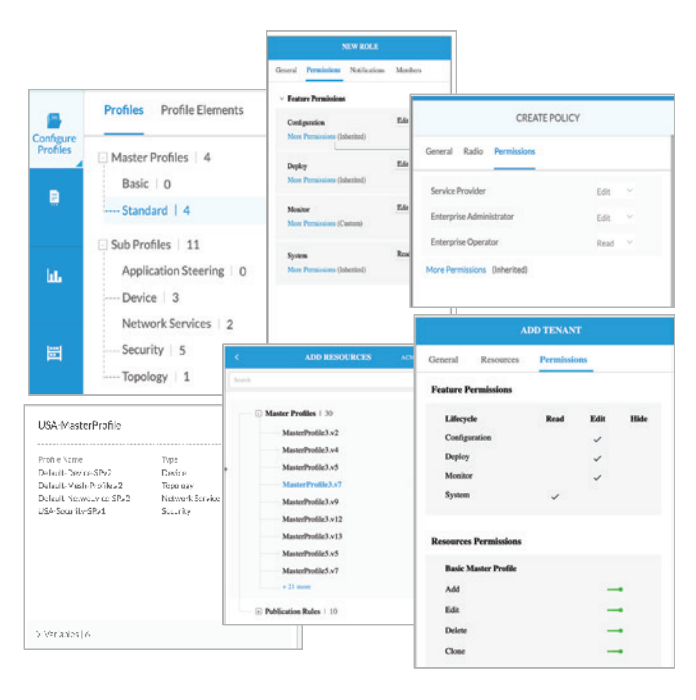


1. Since all the security services are being provided by the Versa SASE Service, application performance is improved by utilizing a single-pass architecture where networking and security services are being performed in one transaction without chaining together appliances, connections, or other services. The single-pass architecture allows for the IP packet to be inspected once and then security enforcement is performed on the IP packet concurrently. In a traditional architecture, many third-party security services would not receive the benefit of a single-pass architecture because the data packet would need to be analyzed in multiple products and services and every time would require rescanning the IP packet, thus causing delay and jitter.
2. The Versa SASE Service provides the ability to scale the security services to meet IP traffic flow demands. Based upon performance metrics, multiple security services can be instantiated at once. Also, different security services can be applied to the Enterprise traffic based upon specific Enterprise policies such as the ability to use the Endpoint Security Compliance to either



force compliance or add security services to devices that are not compliant. For example, Malware Detection and Response might be added to an application flow for a given user where the user's device does not have the latest revision of Anti-Virus software.

3. By utilizing Versa SASE, Versa Cloud Gateways, and Versa Client, the Enterprise gets the best application flow performance as these components will use the industry's leading SD-WAN to determine the most optimal path. In this flow, the path to the application is optimized all while ensuring that all security checks are being enforced as dictated by the Enterprise policy.
4. Versa SASE allows for the security and network policies to be instantiated in a single orchestrator in a single pane of glass. In a central management, there is no need to configure multiple platforms. Through an easy-to-use configuration portal, Versa SASE allows for easy administration and management of security and network policies that are being enforced to all access points within the network.



5. Versa SASE allows for a common telemetry plane that has centralized analytics that visualizes all the pertinent information regarding the SASE Clients, Versa Cloud Gateways, security services, and SD-WAN. Analytics is critical to providing a seamless and complete view of the Enterprise traffic both from a forwarding and security perspective. In addition, the Versa Analytics platform has the ability to integrate with any existing and current Network Management systems.

Versa Networks realizes that any network transformation requires Enterprises to have the ability to protect the network investment that have already been made. Therefore, the Versa SASE Service does not mandate that all the security services or devices be exclusively from Versa, and the SASE platform integrates seamlessly with many leading vendors.

However, leveraging a single-pass architecture with Versa SASE delivers all the benefits of a "As-A-Service" model where you get optimal networking and security with low latency and costs. To meet the demands of a post-pandemic workforce that demands a new approach to the legacy VPN model, Versa Secure Private Access is the best solution for delivering Secure Private Access from anywhere in the world all while protecting users, data, devices, and applications.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com