Versa Secure Private Access

Cloud has revolutionized the user experience for applications and data. Versa has led the transformation by providing software-defined networking with SD-WAN and with SSE. Versa's software-defined solutions provide integrated application, network and user intelligence in a single platform, with centralized management and monitoring, historical reporting, and automation at the WAN edge and on private and public cloud instances.

Today, enterprises are faced with the following reality:

- **Digital transformation** has accelerated the migration of enterprise applications and workloads from an enterprise datacenter to a variety of public clouds and/or SaaS services.

- **Users are connecting from everywhere**. COVID-19 has changed the workplace into a hy-brid workspace where employees are as likely to work from office as Work from Anywhere.

Challenge

Work From Anywhere (WFA) requires support for distributed users, distributed applications and multi-cloud for enterprises. In this new era, users and applications can be anywhere and everywhere, legacy remote access solutions that are appliance-based are challenging to scale, they do not meet the latest Zero Trust Network Access (ZTNA) security requirements, and they do not offer the best application experience.

In order to provide a secure, policy-controlled and reliable application experience for employees Working from Anywhere, there is a need to extend the principles of software-defined networking to provide the right ZTNA solution that meets today's requirements. It is no longer sufficient to just provide VPN connectivity for remote users. Enterprises need a solution which extends their security perimeter all the way to the user and provides enhanced user experience, visibility into the application performance and usage.

Presenting Versa Secure Private Access: a software-defined secure solution connecting your workers working from anywhere to your enterprise applications hosted in enterprise environment, private clouds or public clouds. Versa Secure Private Access (VSPA) protects both the applications and users using the latest Zero Trust Network Access framework.

Key Capabilities of Versa Secure Private Access

- ⊘ Secure Private Access
- ⊘ Policy Based Traffic Management
- ⊘ User Authentication and Authorization
- ⊘ End Point Information Profile
- ⊘ Application Firewall
- ⊘ Network Obfuscation
- ⊘ Application and User Visibility
- ⊘ Assured Application Experience

VSPA is a cloud-managed, cloud-delivered, private access service efficiently connecting distributed users with distributed applications without compromising security or the user experience. This ZTNA offering is based on the philosophy of verifying every network access request originated by the user. In the context of secure private access, Versa's ZTNA scope translates to:

• Enterprise grade authentication with Multi-Factor Authentication (MFA)

• Endpoint Information Profile and posture-based policies

• User/user-group-based policy control

• Network obfuscation and enterprise topology hiding/obfuscation

• Application and network visibility

• Application Policy Control to restrict access of the applications

• Application traffic segmentation to separate traffic for different classes or apps or devices

VSPA is a market-leading Zero Trust Network Architecture (ZTNA) solution offered within Versa's Secure Access Service Edge (SASE) framework. VSPA integrates security, identity management, cloud delivered services and software defined networking and security into a simple, hassle-free service that:

• Extends perimeter protection to the end-user device

• Delivers an always-on application experience

• Is highly scalable and extensible to allow users to work from anywhere

VSPA is a globally distributed solution that connects distributed users to enterprise applications and resources. Enterprise applications and resources can be distributed across private cloud, enterprise data centers, and public cloud instances.
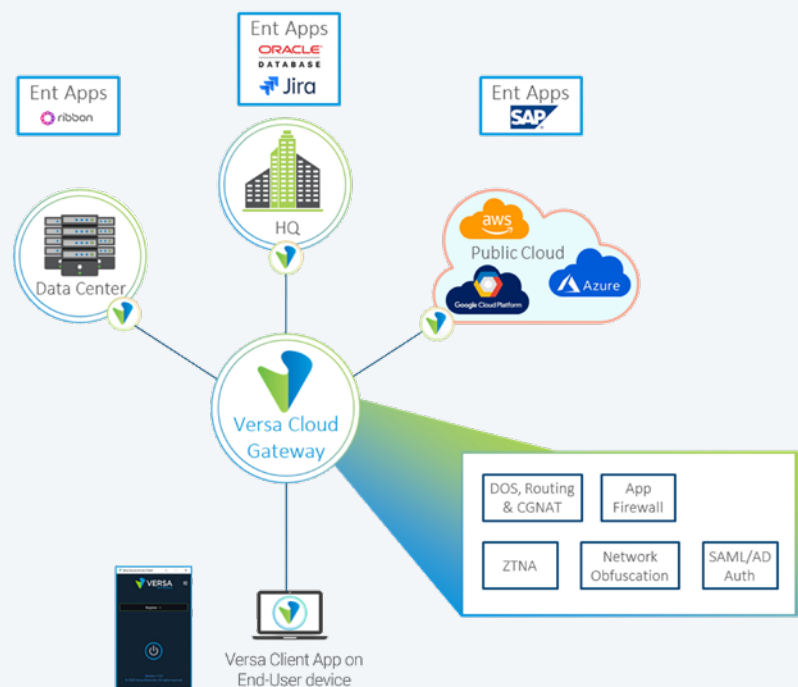
Service Components

Versa Cloud Gateways (VCG)

Based on the industry-leading Versa Operating System (VOS^{TM}), VCGs are globally distributed, located close to users to provide distributed, low latency secure on-ramp solution for access to enterprise applications. VCGs authenticate users, authorize the application access and secure the enterprise network from external threats. VCGs are built on VOS that integrates advanced routing, comprehensive security, market leading SD-WAN along with secure private access. VCGs securely connect to and integrate with existing infrastructure in Enterprise network and datacenter.

Versa SASE˙ Client

A software agent/application that runs on client devices (i.e., Windows, MacOS computers, smart phones), providing a secure, encrypted SD-WAN-like connection experience to client devices. Versa Client application uses secure and encrypted connection(s) from remote device to VCG(s). Upon authentication and access authorization through the VCG, users can now securely connect to enterprise applications in public and private cloud.

Versa SASE Portal

Providing enterprise administrators ability to manage and monitor the SASE service in real-time and with historical reporting capabilities at network, application and user levels, also leveraging Versa's big-data based analytics platform.

Key Service Capabilities

Secure Private Access

VSPA is a secure connectivity solution for remote users connecting to applications hosted by the enterprise. Versa Secure Private Access provides a Zero Trust connectivity to applications hosted in Enterprise Data Center, Private Cloud and/or Virtual Private Cloud instances of public cloud providers. Customers benefit from IPSec or SSL-VPN based secure connectivity for enterprise bound traffic from remote users towards the enterprise applications.

Policy!Based Traffic Management

VSPA uses granular policy based application traffic management to control and limit the application access and visibility capabilities. Users can be configured to use the Versa Client application to connect to different gateways for different applications. Application and Gateway combination is dynamically configured to give best application experience and provides an additional level of security is provided by preventing the user from the accessing gateways from which the application
is not accessible or not preferred. With support for multiple gateways*, customers can dedicate certain gateways for secure applications while allowing users to access generic applications from other gateways.

User Authentication and Authorization

VSPA leverages enterprise's preferred Identity Provider (or identity management solution) to authenticate and authorize the user. Versa Secure Private Access integrates with various types of authentication servers like Active Directory, SSO servers like OKTA and different authentication protocols like LDAP, RADIUS, and SAML. VSPA supports uses Enterprise Identity information to authorize users for application access policies.

Multi-Factor Authentication (MFA) using email is supported by VSPA. Additionally, time-based One-Time Password (OTP) integration with Microsoft Authenticator, Google Authenticator and Duo is also available. VSPA is integrated with SSO identity provider together with MFA as well.

Endpoint Information Profile

VSPA detects and enforces policies based on the current profile and state of the end device. The Versa client constantly monitors the security profile of the end user device including operating system details, presence of certain key security applications like Anti-Virus, use of disk encryption, disk backup, last run time of these applications etc. Such collected information forms the Endpoint Information Profile and VSPA enforces security policies based on the security posture assessed.

Application Firewall

Versa Secure Private Access enforces policies which authorize access to applications on a per application and user/user group basis. Enterprise applications can be defined using FQDN/Host name, wild cards, IP address subnet and ports or combination of these. The policies are based on the username/group information received during the authentication from enterprise identity servers.

Network Obfuscation

Network Obfuscation is a security technique to hide internal network topology from remote users. Network obfuscation such as hiding Enterprise network topology details protects applications from multiple attack vectors like lateral movement, port scanning etc.

Versa Cloud Gateway running VSPA obfuscates Enterprise's application server IP addresses from the user and user IP addresses from the application servers. The user traffic is authorized and translated towards the application and vice versa using Versa's built-in secure proxy functions. This provides highest level of protection from malicious actors and malware that may be running within Enterprise client devices w/out being detected by the Anti-Virus software of the client.

Application and User Visibility

Application, User and Network visibility is necessary to efficiently operate the network and to secure it from external threats. Versa Secure Private Access builds on top of big data based Versa Analytics platform to provide the network administrators with real time view as well as historical reporting of Users, Application and Network.
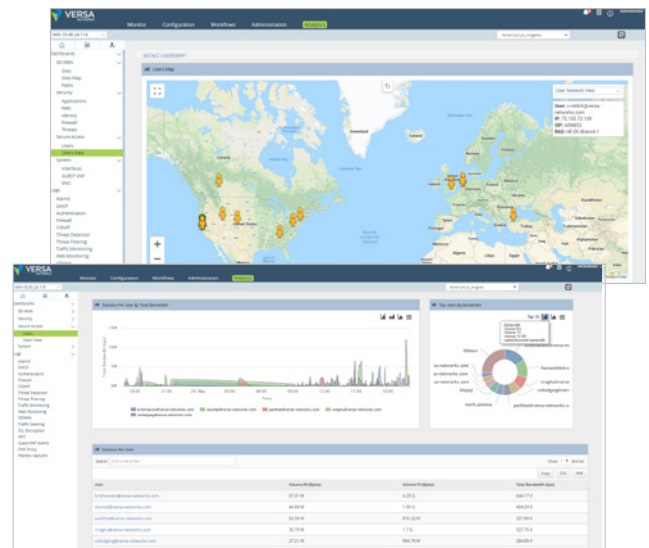
Assured Application Experience

Versa's market leading Secure SD-WAN functionality ensures the application experience for the users, no matter where they are connecting from. Versa Secure Private Access applies various techniques like SLA monitoring, Traffic engineering, that have been extensively deployed in connecting branches now to this software based service.

- **Intelligent gateway selection** ensures that the Versa client connects to the gateway which provides the best user experience. The Versa client chooses the best gateway based on various parameters like server load, cloud gateway proximity, network performance towards the gateway.

- **Hot stand-by** feature ensures that the Versa client is simultaneously connected to multiple gateways. The Versa client monitors the performance towards individual gateways. Flows are routed towards alternate gateways instantaneously upon detection of degraded performance towards the primary cloud gateway.

- **Traffic steering** is supported based on Application, FQDN and/or Routes. The traffic steering policy determines breakout of traffic, selection of gateway and whether encryption is needed for traffic tunneled towards the gateway.

- **VSPA service** also supports creation of encrypted and unencrypted tunnels towards the Cloud Gateways. The unencrypted tunnels provide better latency characteristics for real time traffic which might support application level encryption of the traffic.

VSPA supports geolocation, user, and application policy to ensure clients connect to the closest gateway based on current user location. Versa Client can connect to a multiple gateways based on which application is being accessed. Versa Client makes the routing decision to the best available gateway based on real time network information.

Cloud-hosted applications are accessed directly from the Versa Cloud Gateways. As the applications avoid hair pinning to enterprise DC only to break out into the cloud again, the application experience is improved. The resources required at the data center are also reduced.

Customers can also extend the connectivity to the Public cloud workloads and select SaaS applications over a private link.

Service Tiers

A Versa Secure Private Access subscription is available in two tiers:

Features	Essential	Professional
Versa SASE Client for Windows 11, Windows 10, MAC OS, IOS, Android, Chromebook, Linux, Windows 8 and Windows 7 The Versa client provides secure connectivity from end-user device to Versa cloud gateways.	✓	✓
Intelligent gateway selection The Versa client automatically chooses the nearest and healthiest gateway based on proximity to the gateways, load (CPU, memory, etc)	✓	✓
Authentication with enterprise authentication server Integration with LDAP/Active Directory, SAML based SSO, MFA support with Microsoft Authenticator, Google Authenticator, Duo	✓	✓
S2S tunnels to enterprise DC	✓	✓
Perfect Forward Secrecy and top-of-the-line enterprise-class encryption	✓	✓
Network obfuscation Network topology hiding	✓	✓
Built-in security (SFW, DOS Protection)	✓	✓
Application, network and user visibility	✓	✓
ISP and connection performance visibility Provide network performance analytics (including ISP, Region etc)	✓	✓
Service reliance (Cold standby)	✓	✓
App whitelisting per user (10 applications) Up to 10 applications can be controlled per tenant	✓	✓
Geo-redundant gateways for high availability	✓	✓
App whitelisting for unlimited apps		✓
Zero Trust policies based on posture of the user device		✓
Encrypted and unencrypted tunnels to gateway		✓
User and app policy-based traffic management		✓
Streaming to 3rd-party analytics server		✓
Clientless access to private resources using Terminal Server Agent (TSA), portal-based application access for HTTP(S)		✓

Versa also provides bundling options for Versa Secure Private Access with other Versa cloud-hosted SASE services. For details, please reach out to your Versa account representative.