Lumen® SASE with Versa

Versa Secure Private Access (VSPA)

Versa Secure Private Access is a cloud-managed, cloud-delivered private access service efficiently connecting distributed users with distributed applications without compromising on security or user experience.

Versa Secure Private Access benefits

Application segmentation

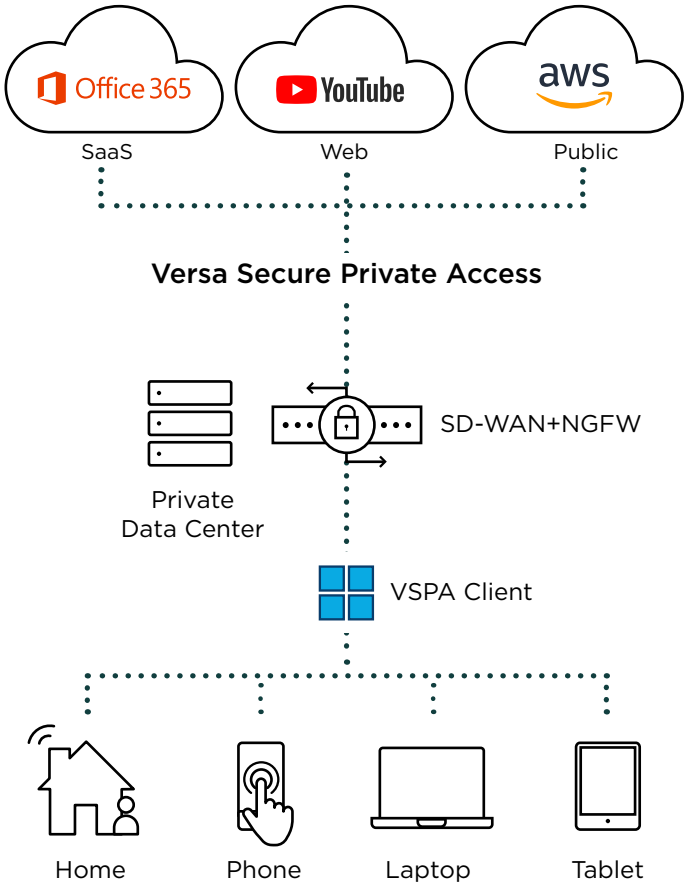
Restrict application access to the right user, on the right device, using the right network with Zero trust security policies

Centralized control

Single-pane-of-glass visibility into application access and usage with the ability to quickly respond to changing workforce application needs

Multi-layered secure access

Onboard remote users and devices with multi-factor authentication and network access control using a single, easy to implement software – Versa Secure Private Access Client (VSPAC)



LUMEN® TECHNOLOGIES

VERSA NETWORKS

Service components

Versa Secure Private Access is a distributed solution to connect distributed users to enterprise applications. The applications can be distributed across private cloud, enterprise data center, and public cloud. The Secure Access Solution consists of:

Versa Secure Private Access Client (VSPAC)

- Versa Secure Private Access Client (VSPAC) is a software agent/application that runs on and extends SD-WAN to client devices (ie: Windows, MacOS computers, smart phones). Versa Secure Private Access Client creates a secure and encrypted connection. Upon authentication and access authorization, users with VSPAC can securely connect to enterprise applications in public and private cloud.

Versa Secure Private Access Portal

- Versa Secure Private Access Portal provides enterprise administrators the ability to monitor the service and provides real-time and historical reporting at a network, application, and user level leveraging the Versa big database analytics platform.

Key service capabilities

Micro-segmentation

- Versa Secure Private Access uses microsegmentation to control and limit the application visibility to authorized users.

User authentication and authorization

- Versa Secure Private Access leverages the enterprise's preferred identity provider 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, and SAML2. Enterprise identity is used to authorize users for application access policies. Multi-Factor Authentication (MFA) using SMS and Email is supported by Versa Secure Private Access. Additionally, Time-based One-Time Passcode (OTP) integration with Microsoft Authenticator, Google Authenticator, and Duo is available.

Application firewall

Versa Secure Private Access enforces policies which authorize access to applications on a per user/user group basis. The 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.

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 the big data based Versa Analytics platform to provide network administrators with real time views as well as historical reporting of users, applications, and network.

Assured application experience

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

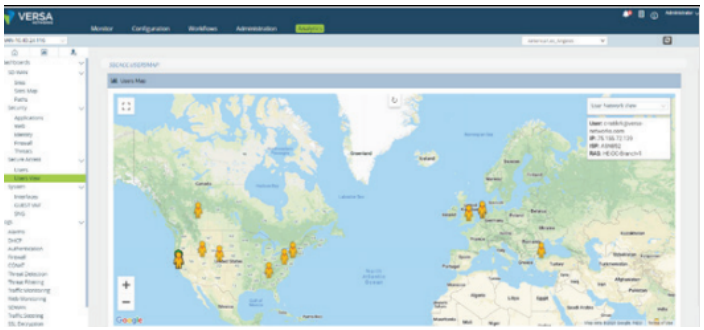
Traffic steering

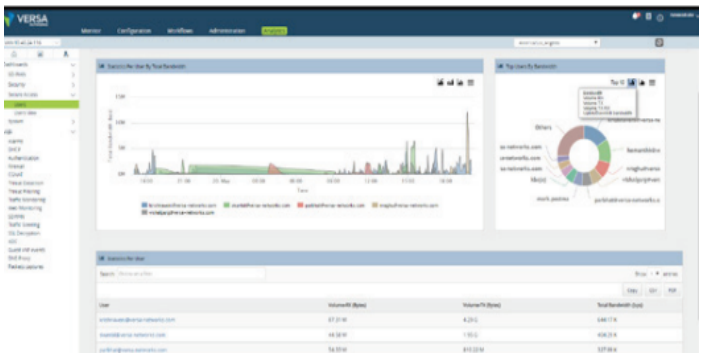
- Traffic steering is supported based on application, FQDN, and/or Routes. The traffic steering policy determines breakout of traffic, and whether encryption is needed for traffic tunneled to the device.

Visit us to get started today at lumen.com/sase

VSPA service

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





VERSA NETWORKS

Why Lumen?

Built on the most expanse highly peered IP backbones in the world connecting to 2,200+ public and private data centers, Lumen attracts leading SASE service partners to our application delivery platform.

We focus on empowering our customers with technology solutions that help address today's hybrid work environment.

866-352-0291 | lumen.com | info@lumen.com

LUMEN® TECHNOLOGIES