SOLUTION BRIEF

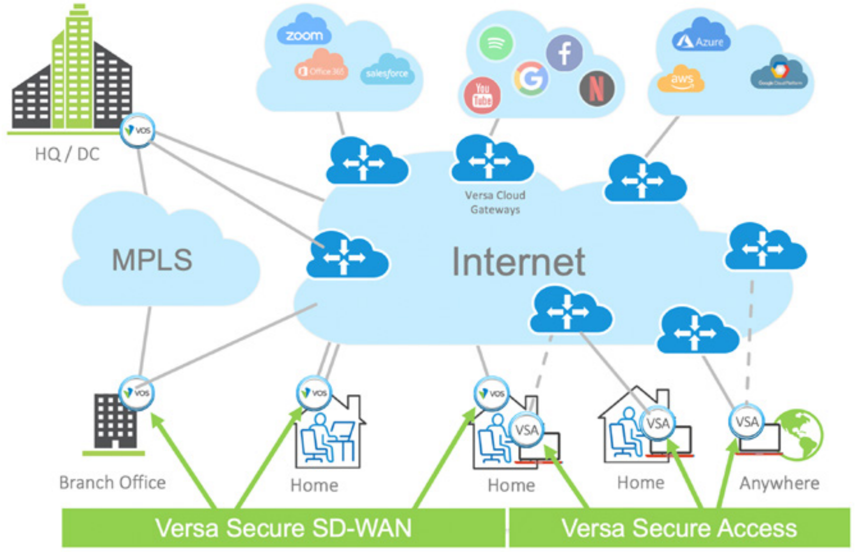
VERSA NETWORKS

Versa for Work-From-Home

The outbreak of COVID-19 and the ensuing global lockdowns have shifted the paradigm of work and the workplace. Months into the pandemic, with the entire workforce working from home, organizations have come to realize that what once seemed like an immediate temporary solution to sail through the storm might well be the new normal of the future. Switching to a mainstream WFH mode has compelled organizations to reflect on the buttoned-down 9-to-5 office practices and test new and effective ways of collaborating and delivering business services remotely. The results of this experiment have made it increasingly clear that when enabled with the right technology, WFH can be a smart viable option for organizations to cut down on the operational costs, reduce corporate real estate needs, and bring a healthy work-life balance to their employees.

New Requirements for Work-from-Home (WFH)

Creating a seamless WFH experience for the remote workforces has been anything but simple for organizations. With a vast number of users accessing corporate data and applications over their home networks, the IT teams are confronting unique networking, security, and visibility headaches that the legacy VPN networks and other remote access solutions are not equipped to address.

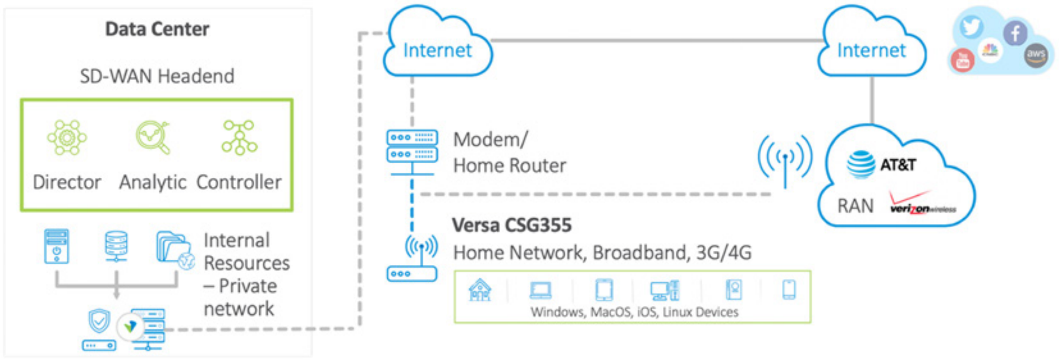


To bridge the complexity, security, and user experience gaps in the WFH landscape, organizations are looking at WFH alternatives that can:

1. Secure network connectivity for mobile workers
2. Offer the ability to scale-up/down on demand
3. Deliver reliable application performance for business-critical applications
4. Be non-intrusive to the home network and corporate IT

Versa Secure SD-WAN for the Home

Versa Secure SD-WAN is available on home appliances for work-from-home users. Organizations can leverage the appliance model to cater to even the most demanding WFH users who require multiple internet connections, high quality voice/video, and support for multiple WFH devices. In this approach, the Versa appliance is installed at the remote user's home via zero touch provisioning to deliver all the Secure SD-WAN capabilities directly inside the home network.



Versa CSG300 Series Appliances for WFH

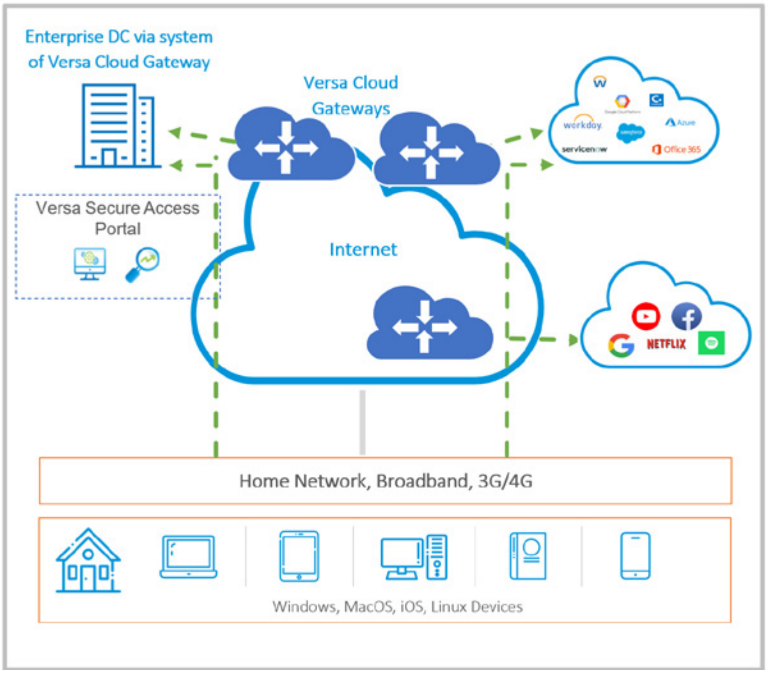
Versa offers the leading edge Versa CSG300 series appliances for deploying Versa Secure SD-WAN at branch sites and home offices. Based on Intel's x86 architecture, the CSG300 series is ideal for easy deployments in home offices requiring robust security, consistent high performance, and complete visibility. The versatile Versa CSG300 series appliances deliver carrier-grade reliability with enterprise-grade routing, SD-WAN, and Next-Generation Firewall—all while supporting a diverse set of WAN access technologies (MPLS, Broadband) and wireless LAN & WAN access technologies (3G, 4G-LTE, LTE Advanced). The CSG300 series appliances scale SD-WAN performance up to 500 Mbps and up to 125 users.

Versa Operating System (VOS™)

Running on the Versa 300 appliances is the highly flexible Versa Operating System (VOS™), which powers Secure SD-WAN networks on-premises and in the cloud. It is a cloud-native, multi-tenant, and multi-service software stack with a full set of networking capabilities, including full-featured SD-WAN and advanced scalable routing, along with a wide range of comprehensive, integrated security functions.

Versa Secure Access For "Work-from-Anywhere"

Versa Secure Access is a cloud-managed and cloud-delivered solution built to efficiently connect remote workers with distributed applications regardless of their location or device. It is the industry's first solution to deliver the leading Secure SD-WAN services and private connectivity for employees who are working from home or are remote. At the heart of the Versa Secure Access is Zero Trust Network Access (ZTNA) built on the SASE framework—integrating security, identity management, cloud, and SD-WAN into a simple, hassle-free service.


Enterprise DC via system of Versa Cloud Gateway
Versa Cloud Gateways
Versa Secure Access Portal
Internet
workday
servicenow
Azure
Office 365
NETFLIX
Home Network, Broadband, 3G/4G
Windows, MacOS, iOS, Linux Devices

Versa Secure Access consists of:

1. **Versa Cloud Gateways** that are globally distributed to provide secure on-ramps for access to enterprise applications. They are built on VOS that integrates advanced routing, comprehensive security, market-leading SD-WAN, along with secure access. These Gateways authenticate users, authorize the application access, and secure the enterprise network from external threats.
2. **Versa Secure Access Client (VSAC)** is a software agent that runs on client devices and creates a secure and encrypted connection from the remote device to the Versa Cloud Gateway, segments applications, and supports SD-WAN services. Upon authentication and access authorization through the Versa Cloud Gateway, users with VSAC securely and reliably connect to enterprise applications hosted in the cloud.
3. **Versa Secure Access Portal** is the management interface that provides enterprise administrators with a granular view of the entire network and the ability to monitor users and applications in real-time.

Versa WFH Solutions Deliver the Following Capabilities:

1. **NSS recommended integrated security:** the most comprehensive range of built-in security services that include stateful firewall, DOS protection, NGFW, IPS, and URL filtering on end-user client devices connecting privately to enterprise resources.
2. **Micro-segmentation:** role-based access that controls and limits application visibility to authorized users. Organizations can dynamically configure applications and Versa Secure Access Gateways to prevent users from accessing applications they are not authorized to access.
3. **User authentication and authorization:** leverages the enterprise's preferred Identity Provider to authenticate and authorize users for application access policies.
4. **Application Firewall:** enforces policies on a per-user/user group basis for application access. The applications can be defined using FQDN/Hostname, wild cards, IP address subnet and ports or a combination of these.

5. **Application and user visibility:** built on top of the big data based Versa Analytics platform to provide the network administrators with the real-time view as well as the historical reporting of users, application, and network that helps monitor and prevent insider threats and illicit lateral movement.
6. **Application performance optimization:** SLA monitoring, Traffic engineering, and Forward Error Correction to ensure the application traffic is directed to the best available gateway and the transport link for optimum application performance. Versa Secure Access also supports geolocation, user, and application policy to take users to the closest gateway to minimize latency. Further, it allows cloud applications to be accessed directly from the cloud gateways, eliminating data center backhauling, which undoubtedly improves application performance.

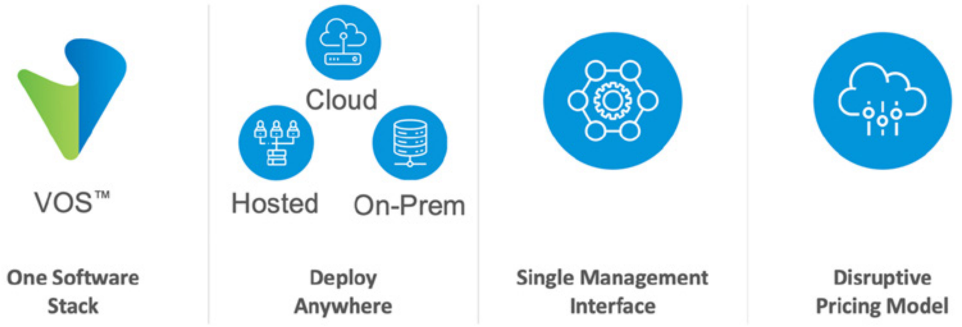
Choosing Versa for Your WFH Solution

Versa WFH enables IT to establish security, visibility, simplicity, and performance at the home office or anywhere employees perform their jobs with Versa Secure SD-WAN in the home and Versa Secure Access in the home or anywhere. Organizations are able to expand the Versa Secure SD-WAN corporate network directly into the home ensuring security, performance, and visibility as if the home was part of the corporate network. In addition, organizations can also extend secure access, applications identification and segmentation, and quality of experience for the most important applications down the physical device whether it is corporate-issued or employee owned.

Organizations deploying Versa WFH achieve:

1. Secure application access regardless of user and application location. Versa is NSS Labs recommended for NGFW and NG-IPS.
2. Assured application performance and remote user experience
3. Flexibility to choose a Secure Access Client and a WFH network appliance
4. Pervasive visibility into applications, remote users, and the network
5. Quick to deploy, easy to operate, and non-intrusive to the end-user home network

Unlike other solutions on the market that require service chaining and multiple management consoles, Versa WFH has:



About Versa Networks

Versa Networks, the leader in Secure SD-WAN, combines full-featured SD-WAN, complete integrated security, advanced scalable routing, genuine multi-tenancy, and sophisticated analytics to meet WAN Edge 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. For more information, visit https://www.versa-networks.com or follow us on @versanetworks.