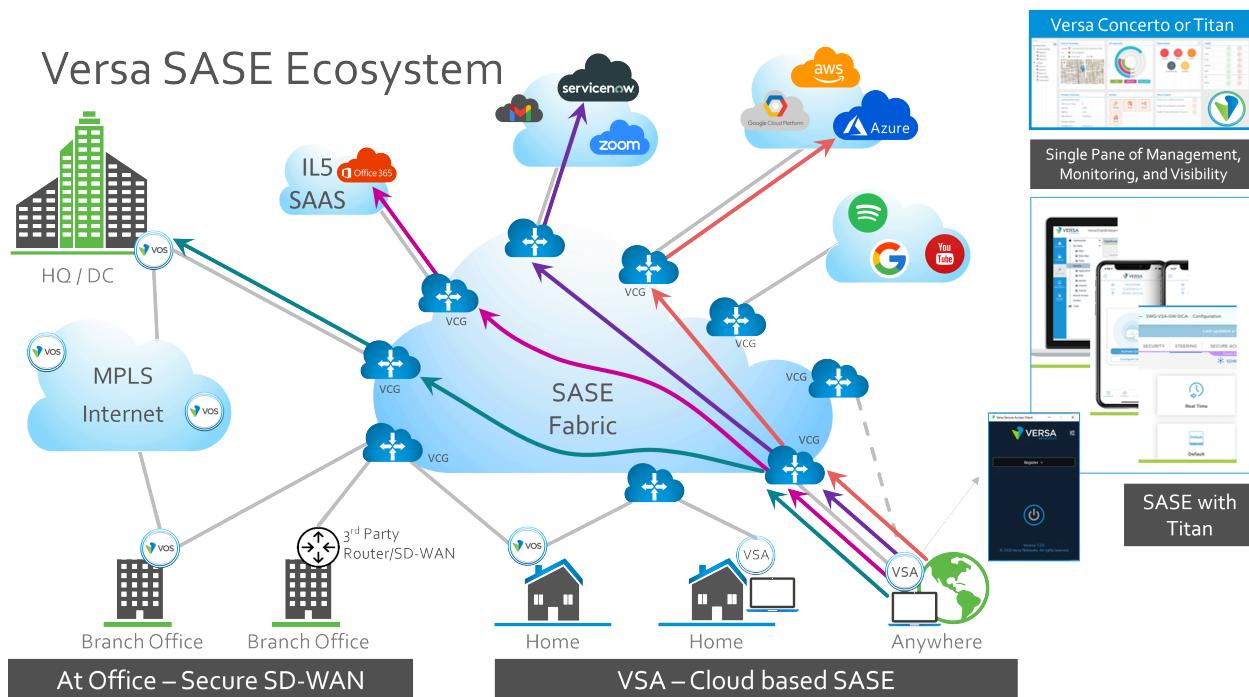


## Versa SASE Ecosystem

 For supported software information, click [here](#).

The Versa SASE solution has the following components, as shown in Figure 1.



**Figure 1. Versa SASE Ecosystem.**

1. Versa Cloud Gateways (VCGs) are Versa SASE Gateways which are deployed in Point of Presence (PoP) locations around the world. Each VCG is connected to multiple global service-service providers, and multiple regional service providers. Each VCG is strategically deployed to be at front-door of dominant web scale providers and Cloud Service Providers. If traffic must be carried from one VCG to another, then it is always routed along a path which has least end-to-end latency and end-to-end packet-loss. This is accomplished by Versa SD-WAN Traffic Engineered network which uses multiple global and regional providers for the underlay. Once traffic is delivered to VCGs, they perform comprehensive contextual security processing based on application, content, user, group, and posture of the device. Versa VCG has native support for multiple services. It holistically integrates them to provide the capabilities shown below and in Figure 2. A Versa VCG does single-pass parallel processing of traffic to deliver the lowest latency.

### a. Secure Private Access

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Director/Ecosystem/Versa\\_SASE\\_Ecosy...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Ecosystem/Versa_SASE_Ecosy...)

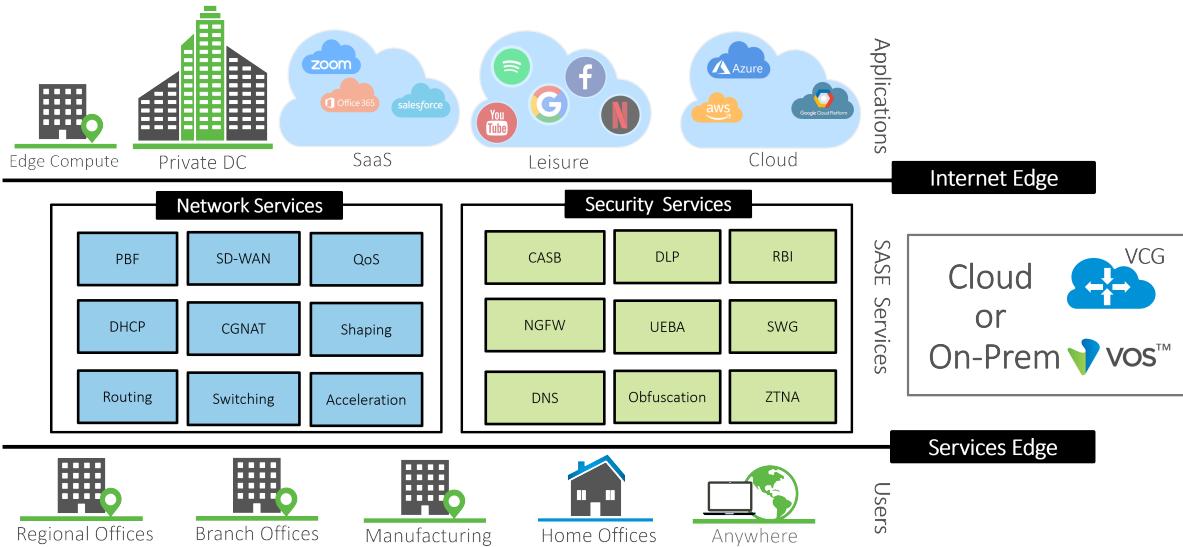
Updated: Wed, 23 Oct 2024 08:44:05 GMT

Copyright © 2024, Versa Networks, Inc.

- b. Zero Trust Network Access
- c. Secure Internet Access or Secure Web Gateway
- d. Cloud Access Security Broker
- e. Data Loss Prevention
- f. Remote Browser Isolation
- g. Advanced Threat Protection including Security based on AI/ML, Multi-AV, and Sandboxing
- h. User Entity Behavior Analytics

## VERSA SASE

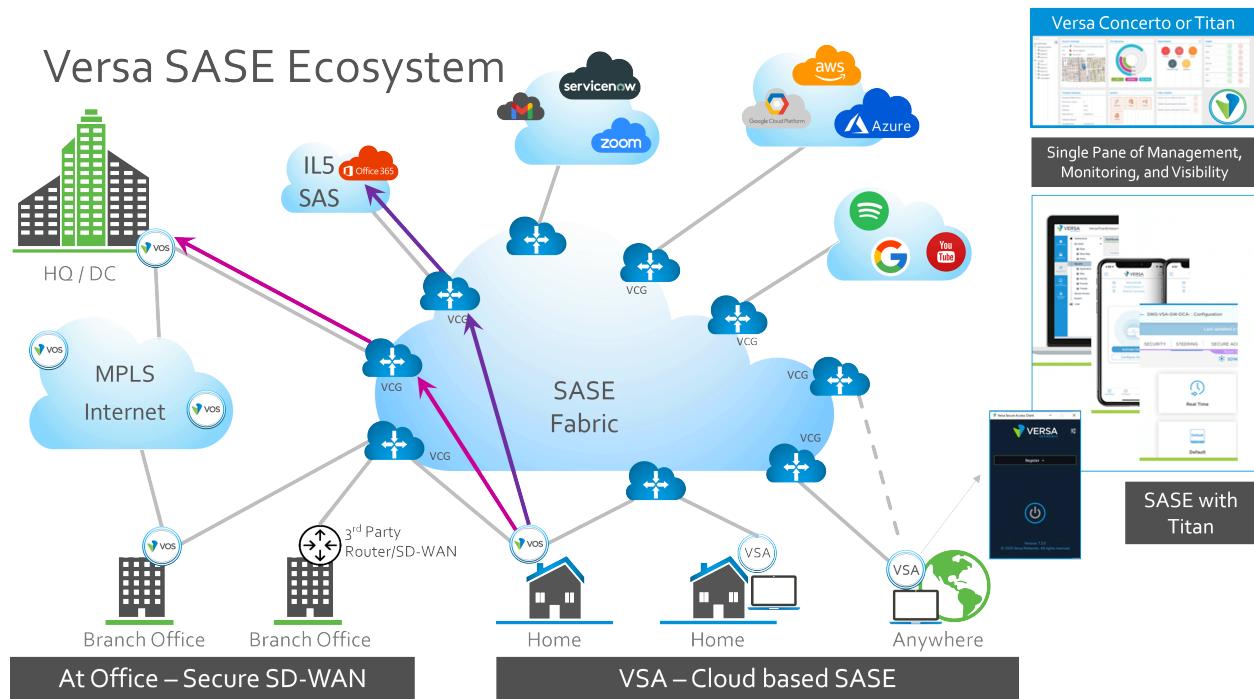
The Convergence of Networking and Security via the Cloud, On-Premises, or a Blended Combination of Both



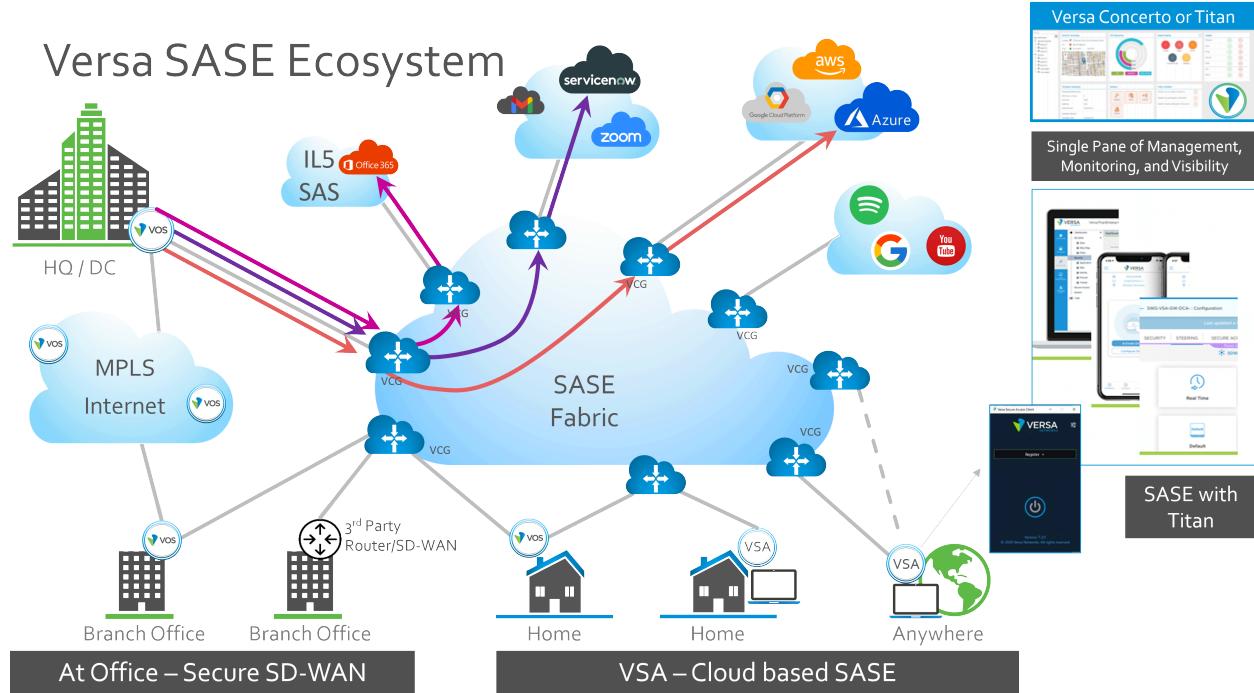
**Figure 2: Security and SD-WAN SASE Services Supported by Versa Cloud Gateways.**

2. Versa Secure Access Client is Versa's SASE Client that is available for Windows, MAC OS, iOS, Android, Chromebook, and Linux. A Versa SASE Client connects to the best VCG that offers lowest latency and packet-loss between the SASE Client and the VCGs. On successful completion of exhaustive security processing, the VCG to which a SASE client attaches, would route the SASE-Client traffic optimally to Private Data Centers, Public Cloud Service Providers, SaaS Providers, or other internet destinations. This is shown in **Figure 1**. The Versa SASE Client supports split-tunneling based on application, FQDN and prefixes. The Versa SASE solution also works with BYOD endpoints which do not have any Versa SASE Client or Proxy Auto Configuration file configured on them.
3. VOS based SD-WAN branches connect to two or more VCGs and benefit from the resiliency, transport-agnostic

and application-based traffic-steering capabilities of SD-WAN technology. Application traffic from the SD-WAN branches is brought to a VCG over the best path based on the end-to-end SLA offered by the underlay-path and the application's SLA requirements. The SD-WAN branches and VCGs can also do packet-replication and forward error correction if required. After successfully completing comprehensive security processing, traffic from VCGs is optimally steered to various destinations as shown in **Figure 3** and **Figure 4**.



**Figure 3: Traffic Steering from VOS-based SD-WAN Device at Branch or Home to Different Destinations.**



**Figure 4: Traffic Steering from VOS-based SD-WAN at Data Center to Different Destinations.**

4. 3rd Party Routers and SD-WAN devices at branch-sites typically connect to two or more VCGs using GRE or IKE based IPsec tunnels. If required, static-routes or External BGP is configured for routing traffic between 3rd Party device and VCG. Once traffic is delivered to the VCG, it undergoes exhaustive security processing. On successful security processing, traffic from VCGs is optimally steered to various destinations as shown in Figure 3 and Figure 4.
5. Versa Concerto Portal and Versa Titan Portal provide a single pane of management and monitoring for all SD-WAN and Security services on the Versa Cloud Gateways as well as on the VOS based SD-WAN branch devices.

## Supported Software Information

Releases 21.2 and later support all content described in this article.