


Solution Components

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

Versa Networks products deliver a broad set of functions, a single-pane-of-glass management and orchestration platform, and a near real-time, big-data-driven analytics platform. Figure 1 shows a high-level view of the Versa Networks products. This article describes the Versa Networks products.

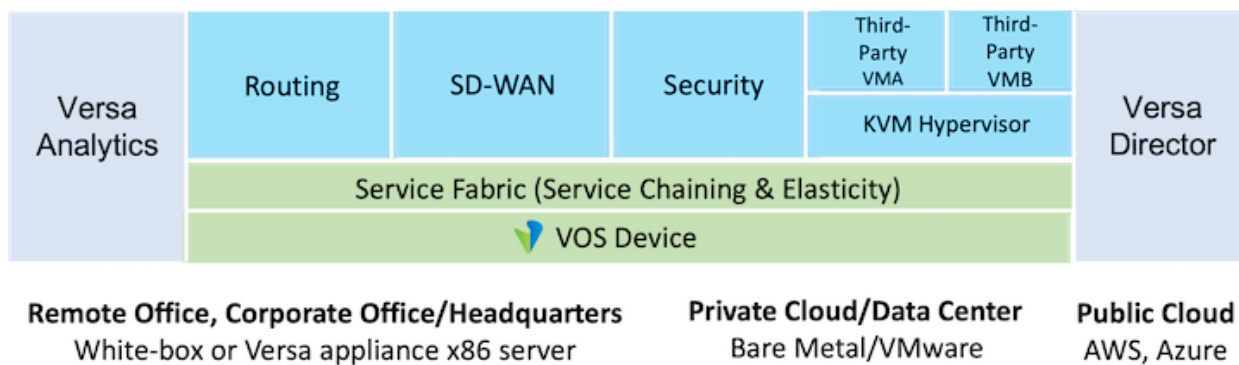


Figure 1: Versa Networks Products

VOS Device

A Versa Operating System™ (VOS™) device is a complete network and security software stack for configuring and managing Layer 4 through Layer 7 services.

VOS software consists of a multitenant, single software stack that natively runs multiple services, such as routing, security, and other network-based functions. These services can be combined into logical service node groups (SNGs), which can be chained together to deliver multiple services in a single path. The same software provides the data and control plane functionality (SD-WAN Controller).

You configure and manage VOS instances through the Versa provisioning and management platform, Versa Director. VOS devices also generate a rich variety of audit logs and exports them to Versa Analytics.

VOS devices provide fully integrated Layer 4 through Layer 7 functions in platform-based software packages, including

OVA, QCOW2, and ISO. VOS devices can be configured to be a data plane element (SD-Router; SD-WAN; or Secure SD-WAN at a branch, hub, or gateway) or a control plane element (SD-WAN Controller).

Versa-Native Networking and Security Services and Capabilities

VOS software provides a comprehensive set of built-in services for SD-WAN, basic networking and routing, security, and VPNs.

Basic networking and routing services include:

- Border Gateway Protocol (BGP) and Multiprotocol BGP (MP-BGP)
- DHCP relay
- DHCP server
- Ethernet OAM
- IPv6 extensions for routing protocols
- Multicast protocols (IGMP, PIM) (in Releases 20.2 and later)
- Open Shortest Path First (OSPF)
- QoS
- Route redistribution
- Route reflectors
- Routing Information Protocol (RIP)
- Static routing
- Virtual Routing and Forwarding (VRF)
- Virtual Router Redundancy Protocol (VRRP)

Layer 4 security features include:

- Carrier-grade NAT (CG-NAT)
- Denial-of-service (DoS) prevention
- Flow mirroring
- IPsec support
- Stateful firewall services

Layer 7 security features include:

- Application identification
- Device identification and filtering
- DNS proxy and load balancing
- Next-generation firewall (NGFW)
- URL reputation and filtering
- User and group control

Unified threat management (UTM) security features include:

- Antivirus
- File filtering
- HTTP and SSL proxy
- Lateral movement detection and prevention
- Next-generation intrusion prevention system (IPS)

VPN services include:

- Diffie-Hellman key exchange
- Encapsulating Security Payload (ESP) and ESP-hash-based message authentication protocol (ESP-HMAC)
- IKE Version 1 and Version 2
- PKI authentication
- Route-based and policy-based VPNs
- Site-to-site IPsec VPNs

SD-WAN services include:

- Centralized route and policy enforcement
- Integration with existing WAN optimization devices and branch routers
- Intelligent route selection
- Layer 3 and Layer 4 load balancers
- Layer 7 application SLA enforcement
- MPLS-over-VXLAN and IPsec-over-VXLAN overlays
- Service-level agreement (SLA) monitoring
- Template-based policies
- Zero-touch provisioning (ZTP)

VOS Device Roles

The VOS software provides a broad range of networking and security services and capabilities.

You can configure VOS devices to perform the following major roles in the network:

- SD-WAN Controller
- SD-WAN gateway and hub
- SD-Router
- SD-Branch
- uCPE platform

These roles are described in the [Solution Use Cases](#) article.

Versa Director

Versa Director is a provisioning and management platform that performs the following functions:

- Centralized single-pane-of-glass configuration, management, and monitoring of the controllers, branch sites, and hub sites
- Lifecycle management of Versa VOS instances
- System-level high availability (HA) deployed as an active-standby pair for redundancy
- Staging server during the bootstrapping process
- Virtual network function manager (VNFM)
- Zero-touch provisioning (ZTP) of VOS devices at branch and hub sites

Versa Director features include:

- Network overlay support—All VOS communication takes place using an overlay network tunnel, providing consistent management in diverse WAN environments.
- Role-based access control (RBAC)—Allows you to limit access and to define read and write capabilities.
- Hierarchical multitenancy—Partitioning of both management and connectivity, with up to five levels of hierarchy.
- Device monitoring—Dashboard capabilities across devices, including speed tests and bandwidth monitoring.

Versa Director provides the essential provisioning capabilities for Versa Networks network and security services. These capabilities include connectivity, configuration, deployment, orchestration, and monitoring. Versa Director uses multiple tools for orchestration and lifecycle management, including Netconf, RESTful API's, GUI, and CLI. RESTful APIs allow integration with existing third-party cloud management applications.

When multiple sites, branches, or VOS instances have similar configurations, you can build templates and apply them to the instances, ensuring consistency across sites. Configuration templates can contain variables to accommodate branch-specific parameters, such as LAN-side subnets, DHCP pools, access policy rules, and policy-based forwarding (PBF) rules.

Versa Director is typically deployed in pairs for redundancy in active-standby mode. For more information, see the High Availability section of the [Features and Capabilities](#) article.

Versa Analytics

Versa Analytics is an analytics platform that is purpose-built for VOS devices and managed services. Versa Analytics provides visibility into VOS devices. You can use the analyzed data to perform baselining, correlation, and prediction about the VOS devices. Versa Analytics provides real-time and historical data, and you can create reports about usage patterns, trends, security events, and alerts. Versa Director also provides role-based access to Versa Analytics.

Versa Analytics provides RESTful APIs for Versa Networks and third-party applications.

Branch Versa VOS instances continually provide to Versa Analytics status and quantitative information about their links, network paths, and services. Additionally, every service running on a VOS instance, such as NGFW and URL filtering,

generates flow-level and aggregate log messages that are sent to Versa Analytics. Using this information, Versa Analytics performs a number of functions, including networkwide analysis and optimization, troubleshooting, trending, capacity planning, dynamic application-based traffic steering, and security forensics. Versa Analytics passes the results of its analyses to Versa Director.

A Versa Analytics node consists of three components:

- Log collector and exporter—The log collector receives and stores logs from VOS devices and can stream the logs to third-party collectors. Logs can be sent over TCP, UDP, and SSL connections and in multiple logging formats, including IPFIX and syslog. Older logs are archived.
- Database, search, and analytics engine—The database, search, and analytics engine provides storage, search, and analytics services, and it automatically replicates data to one or more Versa Analytics nodes. Security, network, and application analytics leverage the Cassandra database management system, and they use Shark and Spark for high-speed, in-memory analytics. Searching can be done using generic and custom queries, and correlation services can be done using RESTful APIs.
- Versa Analytics application—The Versa Analytics application provides RESTful API-based services to the Versa Analytics user interface and to custom third-party applications. In conjunction with Versa Director, it also provides authentication and authorization services for access to the Versa Analytics node.

Because the search and analysis functions are resource intensive, you typically deploy a pair of Versa Analytics nodes as a cluster, with one node performing the search function and the second node performing the analysis function. For high availability (HA), each cluster should have a minimum of four nodes, two for analytics data and two for search data. Each pair of nodes in a cluster is in active-active mode, and data is replicated between each pair of nodes.

Each cluster of Versa Analytics nodes forms a Versa Analytics instance. The instance can reside in one or more data centers or regions.

You can deploy each node on bare-metal servers, Versa-certified third-party white-box appliances, or as a VM.

Figure 2 shows an example of a Versa Analytics cluster that consists of two analytics nodes and two search nodes for redundancy and that is located in a single data center. The Versa Analytics cluster connects to redundant Versa Directors (one in active mode and one in standby mode) and a Versa Controller, which can be configured to perform load balancing.

Note: A Versa Controller is a specially configured instance of a VOS device that provides the control plane entry point to branch nodes in an SD-WAN network. For more information, see the [Solution Components](#) article.

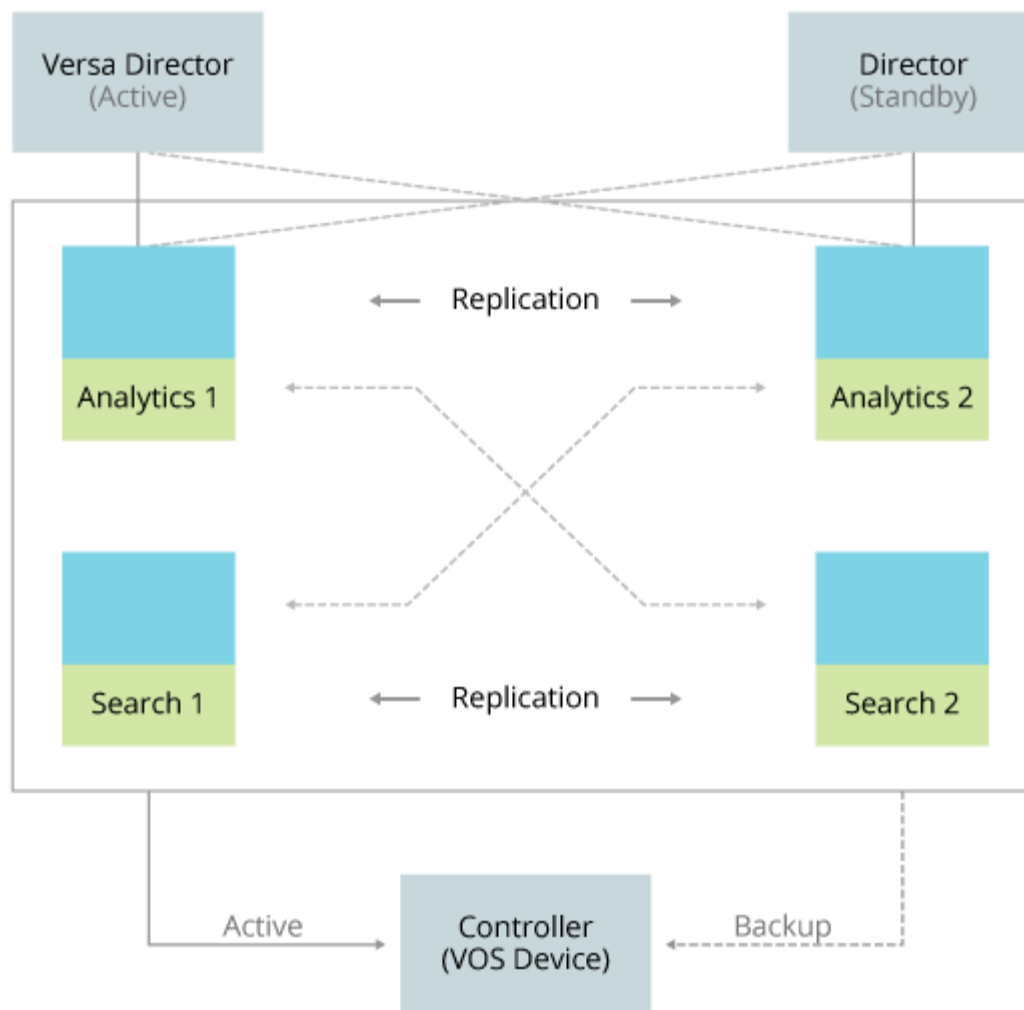


Figure 2: Versa Analytics in a Single Cluster with Redundant Nodes

Versa Analytics creates a number of reports, including:

- Bandwidth per site
- Bandwidth usage and access circuits per site and per application
- Carrier-grade NAT (CG-NAT), including pre-NAT source and destination IP addresses and post-NAT source IP addresses
- Destination and source addresses
- Firewall zones in use
- Forwarding classes in use
- High-risk, productivity, and high-bandwidth applications
- IP addresses by geography

- IP reputation
- Latency per site
- Per-tenant and per-appliance reports
- Predictions made by extrapolating trending data
- Security reports
- Session duration
- Top firewall rules called, by number of hits
- Top Layer 7 applications
- Top network destinations
- Top protocols
- Traffic usage and detection of anomalous protocols

For SD-WAN implementations, Versa Analytics provides historical and near real-time data reporting for:

- Application performance based on latency, jitter, and packet loss
- Application usage based on total sessions, traffic volume, and bandwidth usage
- Performance of paths between any two branches
- Utilization of different branch access circuits
- Versa Analytics natively integrates with third-party data-reporting products and existing Security Information and Event Management (SIEM) systems.

Versa SASE Solution

Available through Versa Networks cloud-hosted SASE services only.

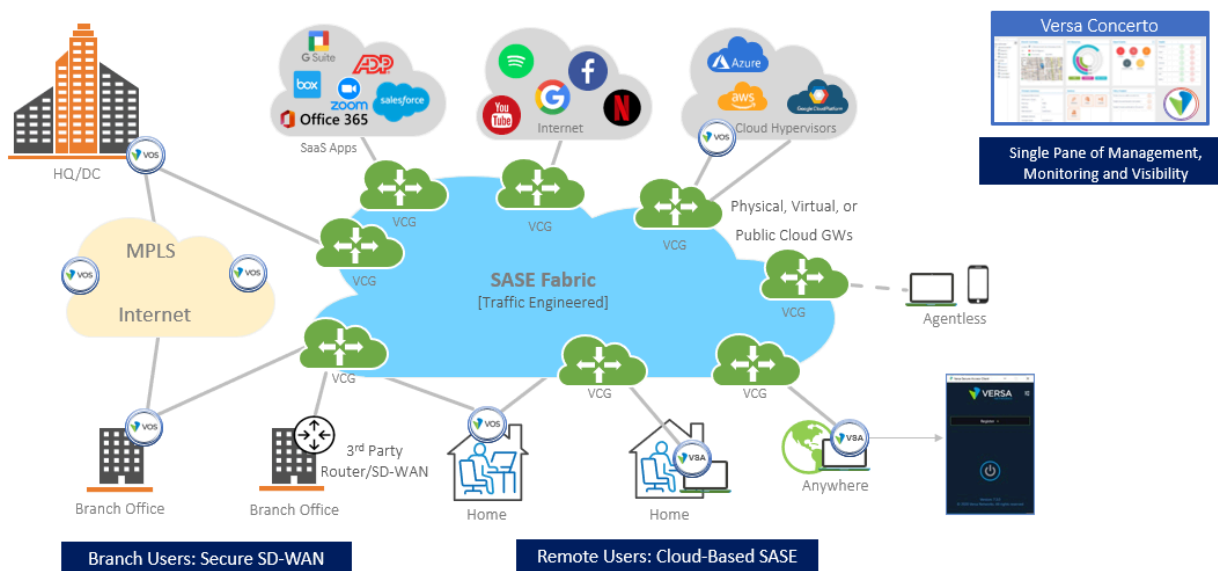
Over the last decade, enterprise applications have shifted away from data centers towards public clouds and software-as-a-service (SaaS), which has stressed legacy networking architectures. Earlier versions of software-defined wide-area networking (SD-WAN) reacted to this shift by enabling customers to utilize any access technology, enabling local breakout, and offering networking focused on application performance.

Currently, work from anywhere is common, and users and applications are exposed to the internet (SaaS or public cloud). Because of this, enterprises are moving from on-premises security and VPN appliances to the cloud to simplify the network, reduce bandwidth usage, and enable optimal paths between users and applications,

Secure Access Service Edge (SASE) is a cloud-native technology that integrates SD-WAN and network security into a single solution. SASE adopts dynamic and contextual security based on identity and delivers it primarily as a cloud service. SASE is an approach towards enterprise networking and security that unifies network and security services, including secure web gateway (SWG), cloud-access security broker (CASB), firewall as a service (FWaaS), and zero-trust network access (ZTNA) with networking capabilities such as SD-WAN, routing, and access. SASE delivers these flexibly via the cloud, on-premises, or a combination of both.

The Versa SASE solution comprises a set of globally distributed Versa Cloud Gateways (VCGs) that provide SD-WAN

and security as a service, as illustrated in the following figure.



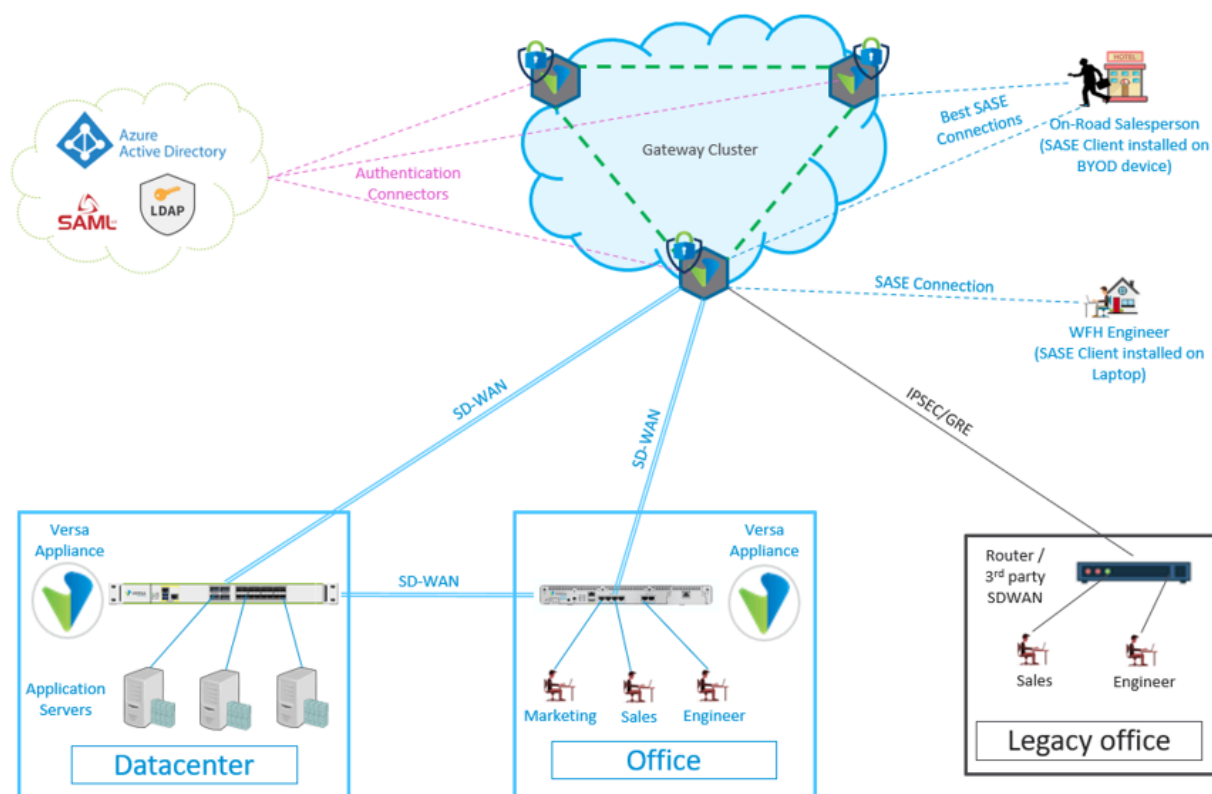
The Versa self-service portal based on Concerto (for secure SD-WAN and SASE users) and Versa Titan (for Versa Titan users) manages Versa SASE services. Versa Concerto also provides a single pane of glass using a self-service portal for both SD-WAN and SASE when using a Versa-hosted headend for SD-WAN. Versa Titan also provides a single pane of glass using the Titan portal.

Versa SASE Architecture

Versa SASE converges networking and security capabilities into a single-service, cloud-native architecture that shifts the focus of security from traffic flow to identity. SASE encompasses a package of technologies that embeds security into the global fabric of the network.

Versa SASE enables ubiquitous and direct client-to-cloud security based on user identity and context, which is fully integrated with optimal client-to-cloud WAN routing regardless of a user's location. This flexible and scalable network architecture provides embedded security and performance along the software-defined perimeter (SDP) edge.

The following figure shows a high-level view of the Versa SASE architecture.



The figure illustrates the following SASE components:

- Versa Cloud Gateways (VCGs) are spread around the world and are used for traffic coming from a branch or from remote users.
- Branch users can access the SASE network from Versa secure SD-WAN devices over an overlay tunnel or over an IPsec or GRE tunnel from a legacy router.
- Remote users can use the Versa SASE client installed on their laptops or mobile devices to access the network, or they can use agent-less methods, such as proxy auto-configuration (PAC) files and reverse proxy.
- SASE gateways are connected to each other over a traffic-engineered SD-WAN overlay, providing optimal routing for enterprise networks and SaaS applications.
- VCGs are also used for private connectivity in Versa Secure Access and for SWG functions for internet-bound traffic.
- For authentication, the Versa SASE solution supports all enterprise authentication systems, including Active Directory, Azure, LDAP, and SAML, to provide easy identity and authorization for users regardless of their location.

The Versa SASE solution attaches and anchors a SASE client to the optimal SASE gateway by taking into consideration the distance between the client and gateway, as well as the service load on the SASE gateways. Versa SASE covers technologies that embed security into the global network fabric and is always available irrespective of a user's location, location of the application, or the resource being accessed.

Legacy architecture provides security to on-premises users and is static, rigid, and requires constant updates and monitoring. The Versa SASE architecture helps overcome the challenges associated with traditional networking and includes the following core security components that identity sensitive information and malware:

https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/03_Solution_Components

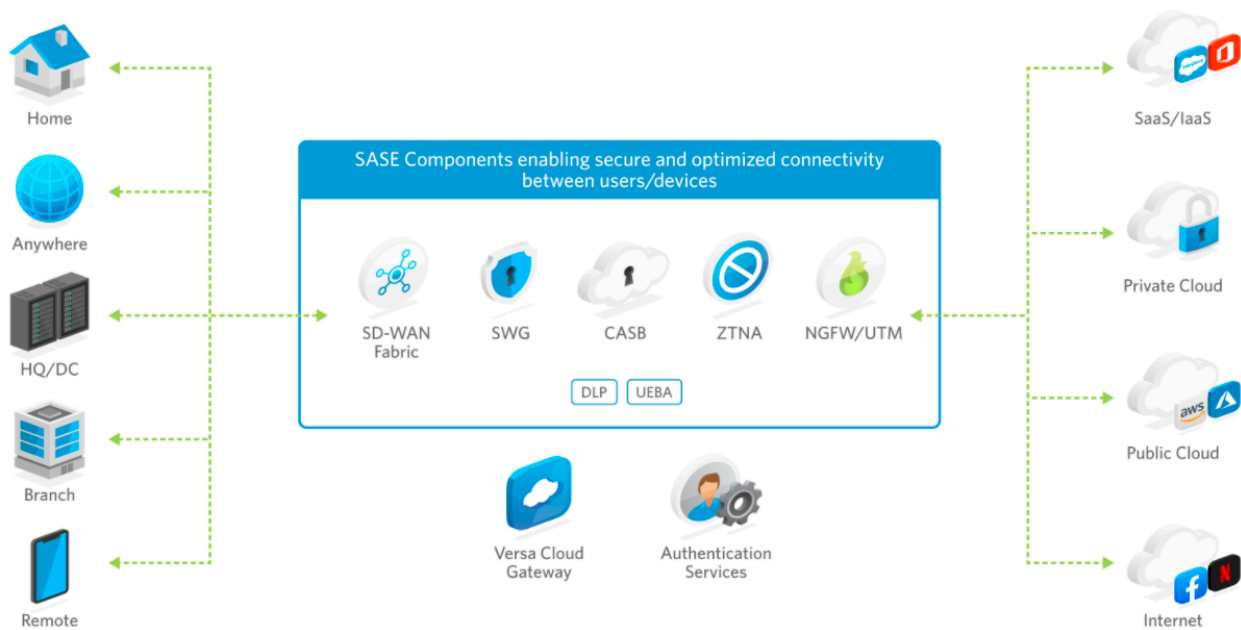
Updated: Wed, 23 Oct 2024 07:32:50 GMT

Copyright © 2024, Versa Networks, Inc.

- Cloud access security broker (CASB)
- Data-loss prevention (DLP)
- Firewall-as-a-service (FWaaS)
- Secure web access gateway (SWG)
- Zero-trust network access (ZTNA)

Versa SASE Solution Services

Earlier network architectures were designed with specific network policy enforcement points and force-routed traffic, often creating inefficient aggregation points and bottlenecks in the effort to enforce security checks. In contrast, Versa SASE enforces security where the traffic flow is located, which is at client and application endpoints, as well as at strategically placed gateways and proxies along the already established, most efficient path.



Versa SASE comprises the following components, which are described in the following sections:

- Secure SD-WAN
- Versa Secure Access (VSA)
- Secure web gateway (SWG)
- Cloud-access security broker (CASB)
- SASE cloud services

Secure SD-WAN

SD-WAN technology forms the foundation of a SASE solution by enabling optimal performance and intelligent routing in a client-to-cloud network architecture. Versa Secure SD-WAN provides a seamless SASE architecture, including

https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/03_Solution_Components

Updated: Wed, 23 Oct 2024 07:32:50 GMT

Copyright © 2024, Versa Networks, Inc.

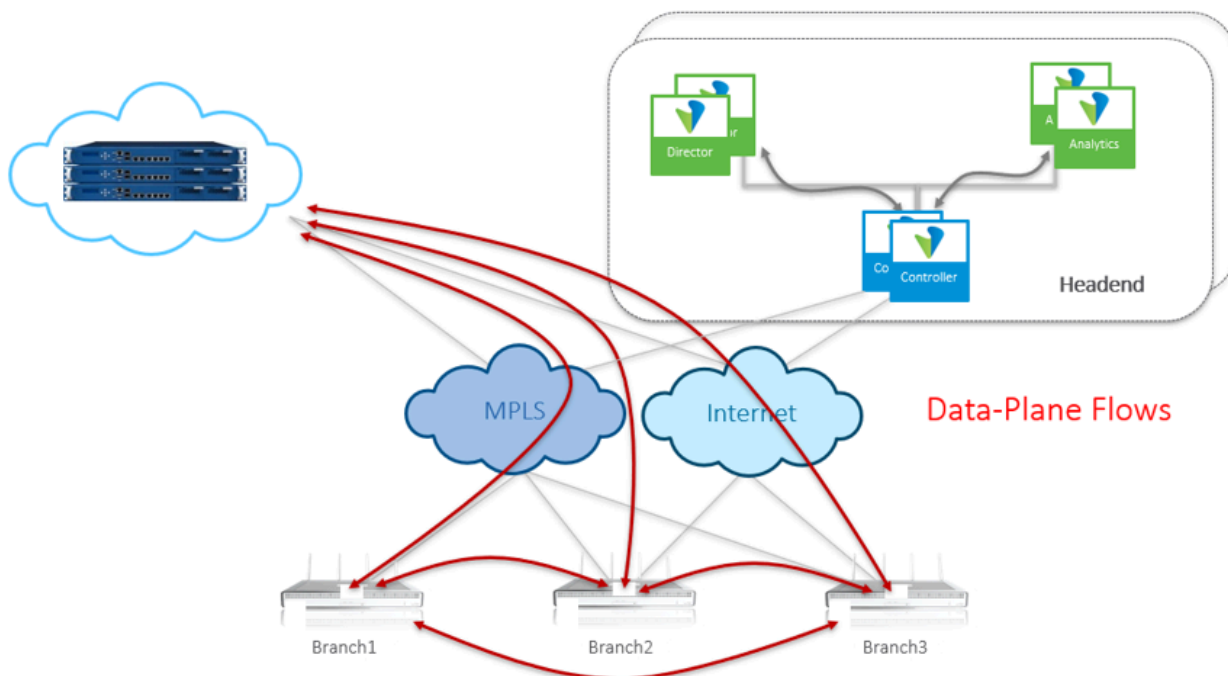
visibility into traffic traversing the network between users, applications, and devices regardless of their location.

Leveraging Versa Networks automation, you can manage the complete lifecycle of Versa Operating System™ (VOS™) devices from a single pane of glass, in just a few clicks. Zero-touch provisioning (ZTP) enables complete orchestration of VOS devices in the cloud and significantly reduces cloud instantiation times and operational involvement. Versa Secure SD-WAN eliminates multicloud complexity by automating dynamic multicloud overlay connectivity from any user, device, or branch.

Versa Secure SD-WAN offers extensive capabilities including the following:

- Subsecond packet steering across multiple WAN interfaces
- Packet loss reduction through services such as forward error correction (FEC), packet replication, and avoidance of poorly performing links
- Encrypted and unencrypted overlays with MPLS/GRE or VXLAN
- SD-WAN Controller node
- WAN circuit support
- Full-mesh and hub-and-spoke topologies
- Dynamic IPsec overlays
- Direct internet access (DIA)
- HTTP and HTTPS proxy

You can deploy a Secure SD-WAN topology quickly, in conjunction with legacy infrastructure, as shown in the following figure.



Secure SD-WAN supports native sandboxing, both on-premises and cloud-delivered, which supports malware analysis

for Windows OS and for mobile devices, including iOS and Android. Native sandboxing malware analysis is performed as follows:

- Check cloud-based reputation to match previously known deny lists and allow lists for the file checksum database.
- If a reputation-based match for the file is not found, use the built-in antivirus engine to scan the file for malware.
- Perform static analysis on the file to check for matches against known threat vectors.
- Process the file against the YARA rule engine to check for matches with previously known malware and malware variants.
- Based on the preprocessing of the files, reduce the number of files that are submitted to the malware sandbox for behavior analysis.
- Execute or open the submitted files in the malware sandbox to analyze the behavior of the payload.
- Monitor for activity using various techniques in the MITRE ATT&CK framework.
- Automatically generate a full behavior-analysis report for the payloads.
- Detect zero-day malware, in most cases within a few seconds, to block malicious files from being downloaded.
- Provide alerts and notifications about malicious files that take longer for the malware sandbox to analyze.

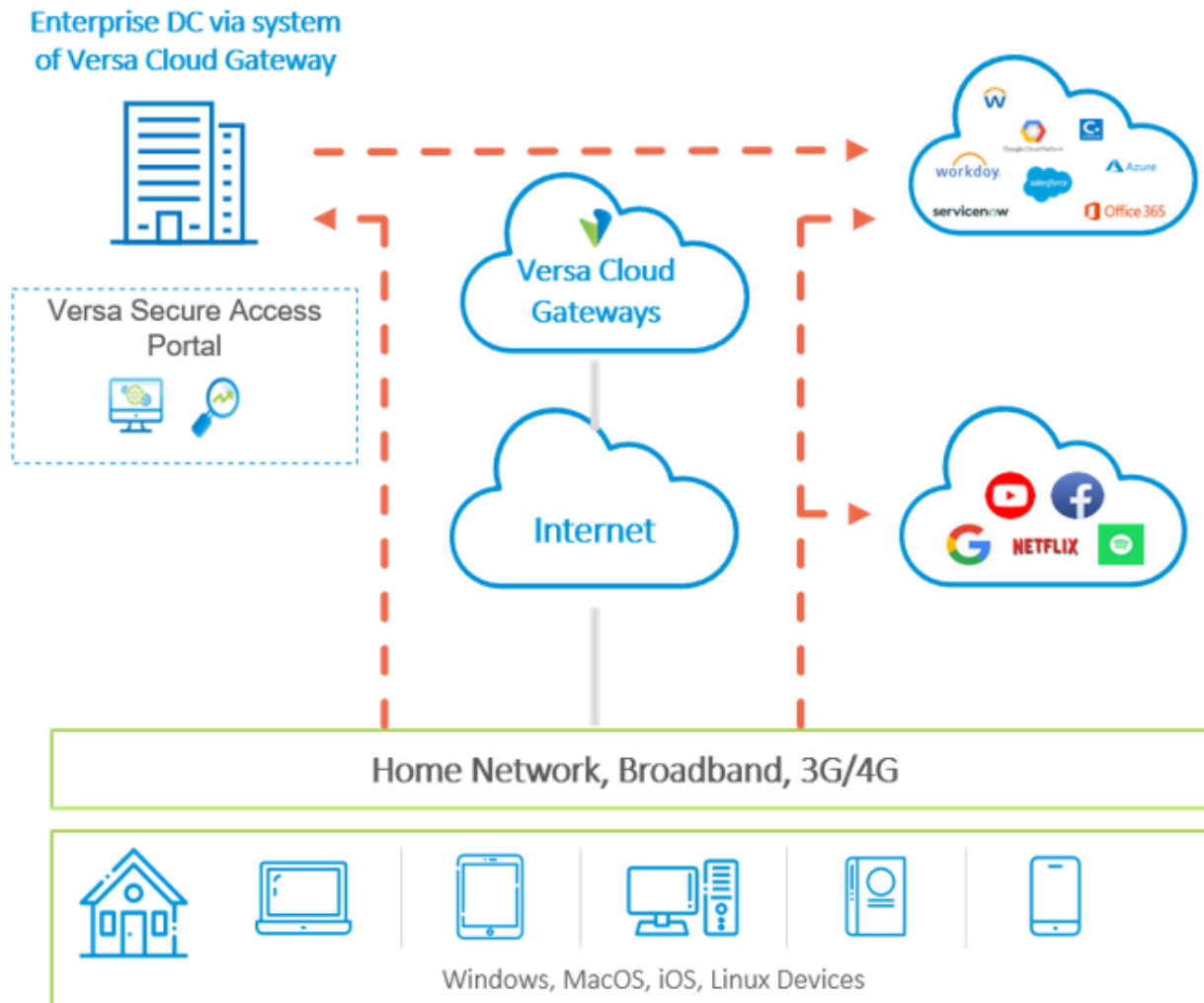
Versa Secure Access

Versa Secure Access (VSA) is a secure solution that connects an organization's employees working from anywhere to enterprise applications hosted in the enterprise environment, private clouds, or public clouds. VSA protects applications and users using zero-trust network access (ZTNA). VSA is a cloud-managed, cloud-delivered private access service that connects distributed users with distributed applications without compromising security or user experience. The fundamental philosophy of ZTNA is to verify each network access by the user. In the context of secure access, the ZTNA requirements translate to the following:

- Application segmentation to restrict access of the applications
- Enterprise-grade authentication with multifactor authentication (MFA)
- Per-user or user group-based application control
- Network obfuscation and hiding of topology
- Application and network visibility

The VSA solution is built on the SASE framework of integrating security, identity management, cloud, and SD-WAN into a hassle-free service that extends perimeter protection to the end-user device, delivers an always-on application experience, and is highly scalable and extensible to allow users to work from anywhere.

The following figure illustrates the VSA solution.



The VSA solution consists of the following components:

- Versa Cloud Gateways (VCG)—VCGs are globally distributed to provide distributed secure on-ramps for access to enterprise applications. Gateways 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, and market-leading SD-WAN along with secure access.
- Versa client—A software agent or application that runs on and extends SD-WAN to client devices, and provides SD-WAN-lite capability on the client side. The Versa SASE client creates a secure and encrypted connection from a remote device to the VCG. After authentication and access authorization through the VCG, users can use the SASE client to securely connect to enterprise applications in public and private clouds.
- Versa Secure Access portal—Allows enterprise administrators to monitor the service and leverages the Versa Analytics platform to provide real-time and historical network, application, and user-level reporting.

The following are the key capabilities of VSA:

- Microsegmentation—VSA uses microsegmentation to control and limit the application visibility to authorized users. Users can be configured to use the Versa SASE Client to connect to different gateways for different applications. An application-and-gateway combination is dynamically configured for a seamless application experience and it

provides an additional level of security by preventing the user from accessing gateways that are not accessible or are not preferred for the application. Support for multiple gateways enables you to dedicate certain gateways for secure applications while allowing users to access generic applications from other gateways.

- User authentication and authorization—VSA leverages the enterprise's preferred identity provider to authenticate and authorize the user. VSA integrates with various types of authentication servers such as Active Directory, SSO servers such as OKTA, and authentication protocols such as LDAP and SAML. The enterprise Identity is used to authorize the users for application access policies. VSA supports MFA using email and time-based OTP (TOTP) integration with Duo, Google Authenticator, and Microsoft Authenticator.
- Application firewall—VSA enforces policies that authorize access to applications based on user or user group. You can define applications using fully qualified domain names (FQDNs), hostnames, wildcards, IP address subnets and ports, or a combination of these. The policies are based on the username or group information received during authentication from enterprise identity servers.
- Network obfuscation—This security technique hides the internal network topology from remote users, thus protecting applications from multiple attack vectors such as lateral movement and port scanning. Versa Cloud Gateway obfuscates the application server IP address from the user and user IP address from the application server. The user traffic is authorized and translated towards the application and vice versa. This provides the highest level of protection from malicious actors on the internet.
- Application and user visibility—Application, user, and network visibility is necessary to efficiently operate the network and to secure it from external threats. VSA builds on the big-data-based Versa Analytics platform to provide network administrators with real-time and historical reporting about users, applications, and the network.
- Assured application experience—Versa Secure SD-WAN ensures application experience for users, no matter where they connect from. VSA applies techniques such as SLA monitoring, traffic engineering, and FEC to this software-based service.
 - Intelligent gateway selection ensures that the SASE client connects to the gateway that provides the best user experience.
- VSA supports traffic steering based on applications, FQDNs, and routes. Traffic-steering policy determines traffic breakout, gateway selection, and whether encryption is required for traffic tunneled towards the gateway.
- VSA supports the creation of encrypted and unencrypted tunnels towards cloud gateways. Unencrypted tunnels provide better latency characteristics for real-time traffic that might support application-level encryption.

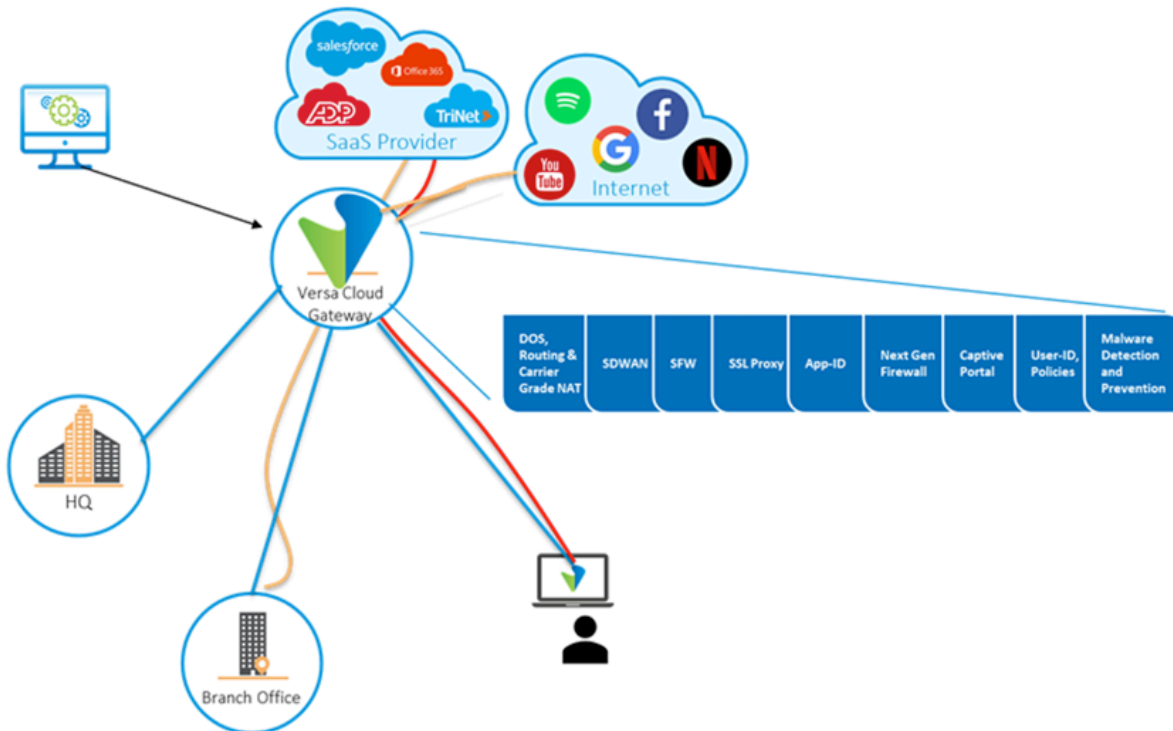
Secure Web Gateway

The Versa SASE secure web gateway (SWG) integrates full-stack security; identity management; cloud application security and SSL encryption and decryption; Versa Secure Access; and SD-WAN into a simple service that runs in the cloud, on-premises, or a mix of the two.

Versa SWG protects enterprises and users from malicious web traffic access and infection, and contamination by hijacked websites that contain malware or viruses. Based on the user, device, and location context, SWG evaluates application policy and grants access only if the policy allows the request based on identity context.

Versa Cloud Gateways are hosted around the globe and offer a variety of SASE services. When you subscribe to the SWG service, you leverage VCGs around the globe to secure the web and mobile traffic originating from the network users and remote users.

Versa SWG offers full security suite, including URL reputation and filtering, IP reputation and filtering, DNS reputation and filtering, Layer 7 (application-based) rules, SSL/TLS decryption, NG IPS, antivirus, DNS filtering, and file filtering.



The Versa SWG solution comes with a unified policy framework with single-touch deployment including sites that are leveraging Versa Secure SD-WAN. The Versa policy framework covers devices and applications independent of deployment and access, providing simpler policy deployment, configuration, and management through an automated and centralized policy engine.

Versa SWG provides the following features:

- Enterprise-grade device and user authentication with MFA.
- User-, group-, and device-level access control and policies—Active Directory, ID-Proxy integration to manage traffic by users.
- URL-based traffic identification—URL traffic management for millions of sites managed by categorization into 83 classes by type, risk and other factors, including encrypted HTTPS flows.
- Identification of applications with features such as deep packet inspection (DPI), URL, protocol and port numbers, and destination IP addresses, combined with comprehensive policy-based control.
- Next generation firewall (NGFW), DOS protection, CGNAT with application-level gateway (ALG) support.
- Web filtering to prevent traffic flow to undesired, out of compliance, illegal, or virus/malware-spreading sites.
- Comprehensive unified threat management including NG-IPS, antivirus, file filtering, malware protection, and sandboxing capabilities.
- SSL-TLS proxy to terminate encrypted sessions and to apply detailed security scans to ensure no vulnerability or malware hides within encrypted flows while enforcing security policies defined by the network administrator.
- DNS proxy and DNS security to secure and manage DNS inquiries and resolutions.
- Identity proxy and integration with third-party identity management services along with an enterprise's identity

management systems.

- Supports a rich set of routing protocols to enable traffic routing and management decisions.
- SD-WAN support provides an integrated, secure WAN-edge solution for enterprise branch, HQ, and DC WAN sites, enabling enterprises to choose the placement and management of security functions on-premises, on-cloud, or both, all managed through a single pane of glass.
- Flexibility to deploy mixes of thin branch and thick cloud, thick branch and thin cloud, or other options based on requirements.
- Seamless integration option with Versa Secure Access (VSA) to provide comprehensive security to VSA clients while using encrypted, private access to the network.
- Single-pass architecture for maximum performance and lowest latency.

Cloud Access Security Broker

Cloud Access Security Broker (CASB) is cloud-based policy enforcement software that secures the data flowing between users and cloud applications to comply with corporate and regulatory requirements. CASB applies enterprise security policies when users access cloud-based resources.

CASB addresses the following challenges to securing data as more applications move to the cloud:

- Implement data-centric policies to authorize or control.
- Analyze data access and changes to data stored in software-as-a-service (SaaS) clouds.
- Implement access control for files, applications, and users.
- Identify user downloads, uploads, and file sharing.

In addition, CASB secures cloud services and the growing deployment of direct cloud-to-cloud access.

The VOS CASB implementation functions as inline software, leveraging the VOS deep packet inspection (DPI) software to monitor user activity, enforce security policies, and provide granular access control for cloud applications. Versa Networks also supports API integration with SaaS applications. This API integration makes use of API calls to SaaS applications, inspects user activities and contents, enforces security policies, and provides granular access control for SaaS applications.

SWG protects internal resources from malicious activity. For example, URL filtering or DNS security protects internal users from accessing websites that violate the company policy or are potentially harmful to the enterprise. CASB is complementary to the SWG, as the primary role of CASB in the enterprise security architecture is to protect data, focusing on data stored in cloud platforms.

Inline CASB acts as a gateway in the path of users accessing the data seamlessly and uses some of the following techniques:

- Identity provider proxy—Managed SaaS offerings are configured with the CASB provider as the identity proxy. When a user tries to access a cloud resource, the authentication request is forwarded to the CASB provider, which forwards it to an identity provider (for example, PingID or OKTA) for authentication. After successful authentication, the request is redirected to the CASB provider. The CASB provider becomes the path in between by proxying the user access to the cloud service. This mechanism ensures that the user accessing the cloud service, using any device, is always redirected to the CASB server.

- When the enterprise network has proxy deployed, the CASB server can be proxy chained. The enterprise has to configure on-premises or cloud-based proxy to redirect the cloud applications to the CASB provider. Any user accessing the cloud application is scanned by the CASB provider.
- GRE/IPSec tunnels from on-premises appliances can also be utilized to tunnel the traffic to the CASB server.
- Reverse Proxy PAC files.
- Once the CASB server is in the path of user access, every API call, file upload or download, and configuration change are verified with the policy. The CASB server now has information, such as user information, historical activity, user baseline, access location, and time of day, to take an informed decision about the risk of certain activities.

Versa inline CASB is implemented by enhancing the Versa deep packet inspection (DPI) engine. It monitors user activity, enforces security policies, and provides granular cloud application access control.

You can create multiple CASB profiles and each profile can have multiple CASB rules. Each CASB rule can be configured to match the risk level and activity of multiple cloud applications and you can deny or restrict access to shadow IT. A CASB profile can be referenced for action by a security access policy rule. On matching a CASB rule in the profile, further processing can be performed using antivirus, file filtering, DLP, and sandboxing profiles.

Hardware and Virtualized Platforms

This section describes the hardware platforms and virtualized platforms that run VOS software.

Cloud Services Gateway

The Versa Networks Cloud Services Gateway (CSG) is a next-generation software-defined networking appliance that is based on the latest x86 architecture. It is designed to deliver Versa Networks Secure Cloud IP networking, SD-WAN, and security services for the enterprise WAN edge.

The CSG series appliances are designed for deployment in entry-level and mid-level branches to deliver Versa Networks Secure Cloud IP networking, SD-WAN, and security services for the enterprise WAN edge. Figure 3 shows the front and rear views of the CSG700 series appliance.



Figure 3: Versa Networks CSG700 Series Appliance

The CSG700 appliances are available in three models, CSG730, CSG750, and CSG770, which support different CPU, memory, and storage sizes:

	SD-WAN and NGFW	SD-WAN, NGFW, and AV	SD-WAN, NGFW, and IPS	SD-WAN, NGFW, AV, and IPS	Wireless Options (LTE and WiFi)	NIC Options	uCPE
CSG770	2 Gbps+	750 Mbps+	500 Mbps+	300 Mbps+	Yes	Yes	Yes
CSG730	200 Mbps	—	—	—	Yes	Yes	No
CSG750	800 Mbps+	250 Mbps+	180 Mbps+	150 Mbps+	Yes	Yes	No

For more information, see the [Cloud Service Gateway 700 Series guide](#).

White-Box Appliances

Versa Networks has certified the VOS software to operate on a range of bare-metal white-box appliances that come preloaded with VOS software. Versa-certified white-box vendors include Advantech, Caswell, Dell, Lanner, and Silicom.

The following hardware models are available:

- V100 and V200 series
 - Branch office deployments
 - Performance from 100 Mbps to 2 Gbps
 - Integrated LTE and WiFi options
 - Supports SD-WAN, NGFW, UTM (V110 and V120 only), and uCPE (V120 only)
- V800 and V900 series
 - Campus and hub deployments
 - Performance from 4 Gbps to 10 Gbps
 - Supports SD-WAN, NGFW, UTM, and uCPE
- V1000 series
 - Data center deployments
 - Performance up to 14 Gbps
 - Supports SD-WAN, NGFW, UTM, and uCPE

For more information about hardware requirements for Versa Networks solutions, see [Hardware and Software Requirements for Headend](#).

Virtualized Platforms

All Versa Networks software components can run in virtual machines (VMs) on virtualized platforms, including:

- Amazon Web Services (AWS) cloud platform

https://docs.versa-networks.com/Getting_Started/Versa_Product_Solution/03_Solution_Components

Updated: Wed, 23 Oct 2024 07:32:50 GMT

Copyright © 2024, Versa Networks, Inc.

- Google Cloud Platform (GCP)
- KVM hypervisor
- Microsoft Azure cloud platform
- Microsoft Hyper-V
- VMware ESXi hypervisor

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Versa SASE solution available through Versa Networks cloud-hosted SASE services only.

Additional Information

[Features and Capabilities](#)

[Solution Architecture](#)

[Solution Overview](#)

[Solution Use Cases](#)