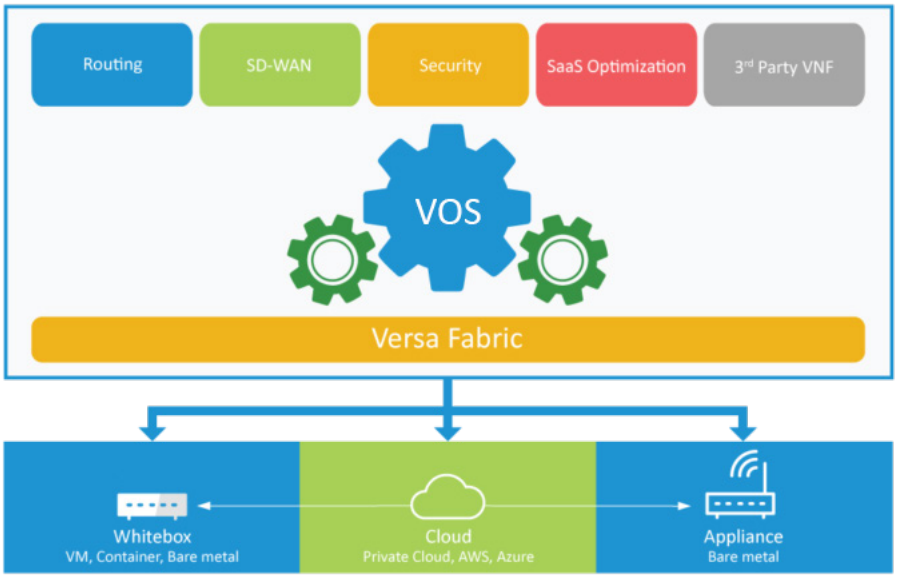
VOS™ (Versa Operating System)

Product Description

The highly flexible Versa Operating System (VOS) enables businesses, organizations, and service providers to deploy a broad spectrum of software-defined solutions including Secure SD-WAN and Secure Access Service Edge (SASE) in branch offices, cloud, campus and data centers. Regardless of where VOS is deployed (on-premises or in the cloud), all network and security capabilities are provisioned and managed centrally through the Versa Director, a single-pane-of-glass management platform. Versa Analytics works in conjunction with Versa Director to provide visibility, base-lining, correlation, and predictive analysis for network, application usage, and security events. With Versa Analytics, all network security, application usage, export reports and logs are analyzed, filtered and are easily searchable for events to derive actionable insights.



VOS 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 – making it possible to seamlessly design rich managed services and software-defined enterprise architectures that allow for agility.

VOS is purpose-built with enterprise-class carrier-grade operational capabilities, including a distributed control and data plane fabric with built-in elasticity and on-demand capacity. Powerful service chaining for both third-party services, including appliances, enables Enterpirses and service providers to easily integrate advanced network and security functions into any type of infrastructure.

Another key Versa capability for improving operational efficiency and service agility, as well as lowering total costs, is multi-tenancy. VOS has built-in multi-tenancy that enables service for hundreds of customers, segments, and organizations providing deployment flexibility, security, and economies of scale.

VOS is fundamentally different than proprietary and expensive network equipment. Deployed on low-cost x86 architectures and appliances utilizing the latest advances in processors and virtualized infrastructure, VOS radically reduces capital purchases and expensive upgrades/refreshes that are common with legacy network hardware devices.

VOS supports the widest set of deployment options in the industry and can be deployed in both legacy networks, cloud, SASE, and new SDN environments. VOS is designed to run directly on bare metal Versa Cloud Service Gateway (CSG) set of appliances with industry leading features and competitive price points. VOS is also supported to run oncertified and preconfigured white box platforms, hypervisor VMs (VMware ESXi, KVM, Xen and Microsoft Hyper-V), and IaaS platforms (Amazon, Google and Microsoft). VOS takes full advantage of multi-core processors and Intel DPDK support for maximum use of the underlying compute resources, thus resulting in high performance and throughput.

VOS is operations-ready and supports standard protocols and log formats, including Syslog, IPFIX, SNMP and Netconf, making it compatible with existing network management, monitoring, and reporting systems. In addition, Versa provides a centralized, automated management platform for device and service workflows, removing laborious manual tasks, and eliminating the need for unnecessary human intervention.

The result is a multi-tenant, cloud-native software services platform that integrates networking and security services in a manner that scales and is on-demand. Versa does this all while maintaining service continuity and delivery of both Versa and third-party network and security functions – all with significantly reduced hardware costs and better

Product Features

Platform	
Form Factor	Bare metal (ISO), Virtual Appliance (OVA, QCOW2), Amazon AMI (Amazon Machine Image), Azure VHD
Hypervisor	VMware ESXi 5.1 & above, KVM, Xen, Hyper-V
uCPE	250 Mbps
(Universal CPE)	Versa hosts operating systems with embedded KVM, Support for 3rd party VNFs (contact Versa for full list of certified VNFs)
Hardware Acceleration	Native QAT support, Rangeley, Denverton, Skylake-D Intel processor family support, ColetoCreek, Lewisburg QAT chipset support (contact Versa certified white-box vendors for specific capabilities and support)
802.11 Wireless AP Support	2.4 and 5 Ghz support, Multiple SSIDs per AP, MU-MIMO support (Wi-Fi module dependent), MRC support (Wi-Fi module dependent)
LTE Support	CAT-6, CAT-12 and 5G modems support, Firmware driven modem (internal LTE modem), USB attached LTE Modem support (optional), Dynamic probing support
Ethernet	802.1Q (VLAN Tagging), 802.3ad Link Aggregation (LACP) – Active or Standby, 802.1ag CFM (Connectivity and Fault Management), 802.3af (POE) and 802.3at (POE+) support (hardware device dependent)
Layer 2	Virtual-switch, bridge-domain, xSTP, IRB, VLAN access/trunk modes, VLAN normalization, LLDP
DSL*	Annex A / B based connectivity (see DSL Module Datasheet for more details)
T1/E1*	T1 or E1 based connectivity with PPP, HDLC, Frame Relay, MLPPP MLFR options
Resiliency	HA: Active-Standby, Multiple controller per Versa Operating System, CPE fallback using Out-of-Band IPsec, Inter-VNF High Availability (Control and Data Plane replication)
Operations and APIs	CLI, Telnet/SSH, Syslog, NetFlow, IPFIX, Flow mirroring, NTP v4/6, SNMPv1, SNMPv2, SNMPv3, Netconf/Yang, Packet capture utility

Network & Security Functions		
DHCP IPv4 & IPv6	Client, Relay and Server	
Routing IPv4 & IPv6	Static routing, BFD, VRRP, VRF/Multi-VRF, RIP v2, OSPF v2/3, BGP, MP-BGP+ (MPLS, IPv6 and L2 extensions), ECMP, Route redistribution, BGP Route-aggregation, MPLS-L3VPN, MPLS-EVPN, VXLAN-EVPN	
Multicast	PIM SM across SD-WAN, PIM SM with neighbor support on LAN and WAN interfaces, PIM SSM, PIM SM Bootstrap RP, •PIM Rendezvous- Point, IGMP v2/v3	
Policy Based Forwarding (L3-L7)	Match Conditions	Source Address, Source Zone, Source Region, Destination Address, Destination Zone, Destination region, Application of stream, Schedule, IP version, IP-Flags, DSCP, IEEE 802.1P, MOS support
	Actions	Permit, Drop, Set Nexthop
QoS	Whitelist/Blacklist on any L2-L4 field, Tenant level policing, Control plane protection, Traffic Classification & Profiles, DSCP/802.1P Marking, Rate-Limiting, Scheduling, Queuing, Shaping, HQoS: Interface Level Shapers, Tenant Level Shapers	
CG-NAT	Static NAT, Dynamic NAT, NAPT, Destination NAT, Static NAT with Port Translation, Inter-Tenant NAT, ALG support: FTP, TFTP, PPTP, SIP, ICMP, IKE, Endpoint Independent Mapping (EIM) support, Endpoint Independent Filtering (EIF) support, Port Parity, Port Block Allocation (PBA) support, Random Port Allocation (RPA) support, Syslog and IPIX logging	
Stateful Firewall	Zone-based, Address Objects, Address Groups, Rules, Policies, DDoS (TCP/UDP/ICMP Flood), Syn-Cookies, Port Scans, Host Scans, ALG support: SIP, FTP, PPTP, TFTP, ICMP	
Application Visibility	Identify more than 3600+ applications and protocols, Application group support, Application filter support, Application visibility and log support, 190+ codecs	
Next-Generation Firewall	Policy Match Triggers: Applications, App filters, App Groups, URL Categories, Geo Location, Application Identity (AppID) based policy rules, Application Groups and Filters, Packet capture on AppID, IP Blacklisting, Whitelisting, Customer App-ID signatures, SSL Certificate- based protection, Expired certificates, Untrusted CAs, Unsupported cyphers and key lengths, 802.1x, DNSSEC	
Anti-Virus	Network/flow-based protection with auto-signature updates. HTTP, FTP, SMTP, POP3, IMAP, MAPI support, 35+ file types supported (exe, dll, office, pdf & flash file types), Decompression support, Storage profile support, Auto signature updates	
URL Categorization & Filtering	URL categories & reputation, including customer-defined, Cloud-based lookups, Policy trigger based on URL category, URL profile (blacklist, whitelist, category reputation), Captive portal response including customer defined, Actions include block, inform, ask, justify, and override	
NG-IPS	Default & customer defined signatures & profiles, Versa & Snort rule formats, L7 DDoS, Layer 7 Anomaly detection, Lateral movement detection and prevention, Support for JavaScript attacks, Security package with incremental updates	

Network & Security Functions	
SD-WAN	Secure, zero touch provisioning, Template-based policies with parameterization, Centralized route and policy enforcement, L7 Application SLA enforcement, SLAs with QoS, Intelligent path selection – default and user-defined, Dynamic bandwidth measurement of SD-WAN paths, Support Active/Active and load balancing of Transport, Overlay encapsulation: MPLS over VXLAN, IPsec over VXLAN, Redundant SD-WAN controller, Integration and support for 3rd party legacy appliances, Flexible topology support – Full-Mesh, Partial- Mesh, Hub-Spoke, Controller behind branch, branch-behind-branch, Spoke-hub-hub-spoke, Custom
Advanced SD-WAN Features	Packet Striping for best throughout across bundle of low speed interfaces, Packet Cloning / De-cloning for replicating, important flows to ensure best performance and availability, Forward Error Correction to restore traffic in lossy and over-congested links, MOS Based Traffic Steering to measure VoIP flows quality and to steer VoIP flows to achieve best voice session qualities, Cloud Provider DIA Traffic Optimizations; Probe based, as well as Inline Traffic Measurements and more
IPsec VPN	Site-to-site, route/policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESP-HMAC support, Symmetric Cipher support (IKE/ESP): AES-128 and AES-256 modes: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication with RSA certificates, Diffie-Hellman key exchange (Group 1,2,5), Per-tenant and VRF aware, MD5 and SHA1 based HMAC
Load Balancing	Virtual Server support, Load Balancing algorithms: RR, WRR, Src. IP, Dest. IP, IP Hash, Least connections, Layer 4 load balancing, monitoring, persistence (Src, Dst, Src-Dest, Mac), Deployment modes: Transparent, Routed and Direct Server Return
SSL Inspection	HTTPS proxy (forward & reverse), SSL v3, TLS 1.0, 1.1, 1.2 and 1.3 proxy, Captive Portal for HTTPS requests
DNS Proxy	DNS Split Proxy, Transparent Proxy
User & Group Level Authentication	Support for Active Directory, LDAP, Radius, Kerberos, SAML, Captive Portal Form for LDAP
Service Function Chaining (SFC)	Encapsulation and tagging types: VLAN, VXLAN, MPLS, MPLS over GRE, NSH, SFC

System Requirements

Hypervisor Supported	VMware vSphere 5.5 & 6.0, KVM – RHEL/CentOS 6.4, Ubuntu 12.04, 14.04, Xen, Hyper-V
	KVM – RHEL/CentOS 6.4, Ubuntu 12.04, 14.04
VMware vCloud Director Support	vCloud Director 5.5 & 6.0
OpenStack Version Support	Havana, Icehouse, Juno, Kilo
OpenStack Distro Support	Red Hat, Canonical Ubuntu, Piston CloudOS
Cloud Platform Images	Amazon Machine Image (AMI), Google Compute Engine (qcow2), Microsoft Azure VHD(VHD)

**The features are dependent on the hardware capability. For CSG appliances, please refer to 'Cloud Services Gateway Appliance' data sheet for details on the hardware capability of CSG devices*

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 Versa Networks on Twitter @versanetworks.

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com