Secure SD-WAN from Omega TeleServe

Product Description

Omega FlexVNF software provides unmatched agility, cost savings and flexibility vs. traditional network hardware. Omega enables next-generation managed services for software-defined WAN (SD-WAN), software-defined security (SD-Security) and virtual customer premises equipment (vCPE). For enterprises, Omega enables highly scalable and secure SD-WAN projects.

Omega has combined FlexVNF software from Versa (including Versa's built-in Unified Threat Management software) with CybX Security's newly developed suite of virtually un-hackable software.

The software was developed by former National Security Agency (NSA) cybersecurity experts to provide a solution to the problem of ransomware and other web-based malware in a user-friendly way.

After decades of real world, hands on experience protecting national security systems at the highest level from cyber-attacks. These developers applied what they learned at the NSA to build a forward-looking, proactive solution to preventing malware attacks based on the idea of "what would it take to stop us?"

Covers All Network and Security Needs

CybX offers powerful, adaptable, and where necessary, disruptive technologies for preventing computer intrusions, detection and substantive computer security defenses. Its technology will detect and stop unauthorized network connections and passive attacks in real-time, and deter hacking tools from being successful.

Coupled with Versa's SD-WAN offering, Omega can cover all the networking and security needs of the branch office, hub site and data center edge node, including full routing, WAN connectivity, SD-WAN and network security.
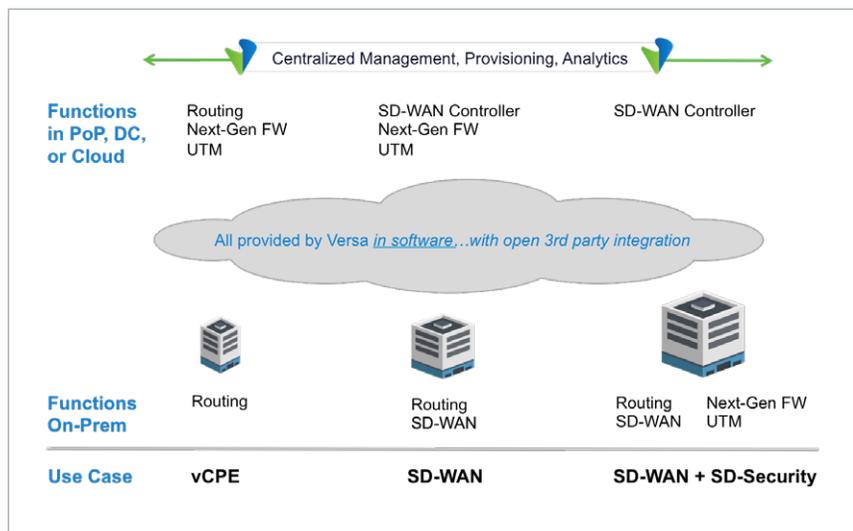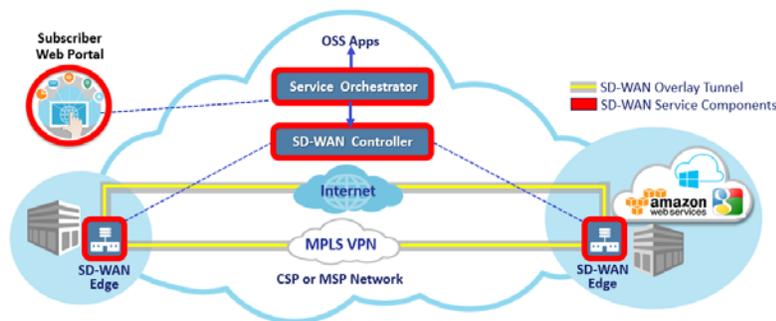
Purpose-built FlexVNF software provides network operators significant flexibility in how they can deploy FlexVNF – onto bare metal, VM and container environments – as well where – in the branch office, data center or central office, or public cloud. Regardless of the packaging and location, all network and security components are provisioned and managed centrally through the Director management platform.

Omega's solution includes the broadest set of VNFs in the industry – from a full set of networking capabilities, including market-leading SD-WAN functions, to a wide range of basic and advanced security functions – making it possible to design rich managed services and enterprise architectures, and deliver them with agility to work seamlessly together.

SD-WAN Service Components

Omega's solution is purpose-built with many carrier- grade capabilities, including a distributed control and data plane fabric with built-in elasticity and capacity on-demand. Powerful service chaining for both Omega and third-party services, including appliances, enables providers and large enterprises to easily integrate multiple network and security functions into complex managed services and enterprise architectures.

Another key Omega capability for improving operational efficiency and service agility, as well as lowering total costs, is multi-tenancy. FlexVNF, as well as the Director, Analytics and Controller, are built from the ground up with full multi-tenancy across all routing, SD-WAN and security features. Omega's comprehensive multi-tenancy allows network operators to share and better leverage underlying resources such as the FlexVNF and hardware infrastructure across many customers or internal organizations, providing more service agility, economy of scale and optimal cost structure for large deployments.

Omega FlexVNF is operations-ready and supports standard protocols and log formats, including Syslog, IPFIX and SNMP, making it compatible with existing network management, monitoring, and reporting systems.

The result is carrier-grade VNF-based services and architectures that can scale out / in, on-demand, while maintaining service continuity and delivery of both Omega and third-party network and security functions – all with significantly reduced hardware costs and better service agility.

Packaging Options

The Omega solution is fundamentally different than proprietary network hardware. Deployed as software on low-cost Intel-based servers and appliances, and utilizing advances in the latest processors and virtualization, Omega's solution radically reduces capital expenses and the costly upgrades/refreshes that are common with legacy network hardware devices.

Omega supports a wide set of deployment options and can be installed in both legacy network and new SDN environments. Deployment choices include an Omega appliance, bare metal servers, white box appliances, hypervisor VMs (VMware ESXi & KVM) and Linux containers. It takes full advantage of multi-socket and multi-core processors and Intel DPDK support for maximum use of underlying hardware resources, resulting in excellent performance and throughput.

For running in bare metal format, a vendor ecosystem has been established with pre-defined device models and specifications that are tested and validated for, ensuring the right configuration at different price and performance points.

These appliance models are directly orderable from approved vendor partners and distributors, and come with the FlexVNF image and encryption certificate pre-loaded from the factory.

The Omega appliance and those from approved vendors are available globally with return-to-factory, next-business- day advanced replacement, same-business-day advanced replacement and other service options. Omega has established innovative business and partnership models and a unified support process to cover all pre-sales and post-sales needs.

About Omega TeleServe

Omega TeleServe was early to the SD-WAN marketplace and has installed and managed nearly 550 endpoints for clients in the healthcare, insurance, and retail industries. We've discovered first-hand the difference between marketing claims of "no-touch installation" and the on-the-ground challenges of bringing an SD-WAN network online. We've also seen first-hand the limitations of the built-in security features in most SD-WAN offerings. They are not sufficient to block incidents like the SWIFT heist in February, the Equifax debacle, nor the increasingly sophisticated ransomware and malware attacks. Our security suite is. Our offering provides a unique and carrier-grade SD-WAN and SD-Security solution that is purely software- and NFV-based, and fully multi-tenant. The solution provides a wide range of virtualized networking and security functions that can be used to create highly scalable and high-value managed services that run on low- cost white box and x86 hardware.

About Versa Networks

Founded by network industry veterans, Versa Networks is an innovative vendor of software-defined WAN (SD-WAN) and security (SD-Security). Versa provides a unique and carrier-grade SD-WAN and SD-Security solution that is purely software- and NFV-based, and fully multi-tenant. The solution provides a wide range of virtualized networking and security functions that can be used to create highly scalable and high-value managed services that run on low-cost white box and x86 hardware. Versa SD-WAN and SD-Security are deployed by Tier 1 and 2 providers around the world, as well as several large enterprises. The company is backed by premier venture investors Sequoia, Mayfield, and Verizon Ventures.

About CybX Security

CybX Security was founded in January of 2016 with the intent of being the worldwide leader in attack and penetration prevention. It's core offering was designed by former National Security Agency (NSA) cybersecurity experts to meet these objectives in a user-friendly way. After decades of real world, hands on experience protecting national security systems at the highest level from cyber-attacks, these developers applied what they learned at the NSA to build a forward-looking, proactive solution to preventing malware attacks. The solution includes: Quantum Veil, a standards-based and patented key management encryption system that forms the foundation of the CybX product line; Quantum Enforcer, which provides any organization with complete control of its computer system's enterprise from a remote location; Quantum Shield provides a mechanism to detect and stop programs (payloads) before they are allowed to execute; and Quantum Browser, a full Isolation Platform that treats all web content as malicious and fully isolates each user's browsing session within a remote virtual environment.