Software Defined Network Interface Card for Remote Device Deployments

Enterprises may need to deploy remote devices in untrusted or 3rd party environments. Remote devices with pre-installed apps might be deployed in environments that are not within the jurisdiction and control of the enterprise. The Enterprise might not be able to consistently apply security policies due to the deployment environment being untrusted or unsecured.

Examples of these deployment scenarios are as follows:

- Financials: Trading or market news servers deployed in 3rd party broker environments
- Financials: ATM Machines in convenience stores, gas stations or fairgrounds
- Government: Government field offices may deploy remote devices with pre-installed apps that are managed centrally and need heightened security postures.
- Various Rapid Deployment models: Disaster recovery vehicle, Fire, Rescue and Response vehicle, pop-up retail locations
- Infrastructure: Mobile Cell Tower, Wind turbines, Oil Rigs
- Defense: Tactical deployments

Each of these scenarios have tight space requirements. A solution that consists of multiple elements for network and security would be too large. Each scenario has limited power requirements, and deployments that require multiple devices require additional power and cooling considerations. Lastly, all these scenarios require that the remote device is securely connected to the enterprise network with a persistent security solution that prevents unauthorized access and prevents, in the event of the theft of the remote device, the capability to repurpose the remote device to gain unauthorized access to the enterprise network.

These solutions require employment of zero-touch provisioning (ZTP) in a secure manner which can deploy and securely connect devices to the enterprise network. Typically, for these remote devices, the operating system (OS) is hardened in such a way that installation of a security agent or any other 3rd party software is not possible. And with the possible theft of the device, measures need to be taken to assure that once the device does connect to the network, that the user implementing the remove device is a validated and trusted entity of the enterprise.

In today's world in which attacks and hackers becoming more sophisticated, expectations are raised. New class of security solutions are required to provide true zero trust network access, detailed cloud access control and data leakage prevention. Traditional remote edge-based security solutions do not provide such capabilities. So, a new class of solution is required to address problems outlined up until here of this solution brief.

Versa offers market leading products and technologies to address security concerns between Enterprise branches, campus sites and data centers. Thanks to rich set of native connectivity and network / data security functions of VOS, Versa customers can now enjoy fully secured network connectivity and deployments capabilities whether they are connecting to LAN or to WAN or to cloud or working from home. VOS can provide comprehensive connectivity to enterprise network, cloud resources, enterprise's own data centers or for other deployment scenarios.

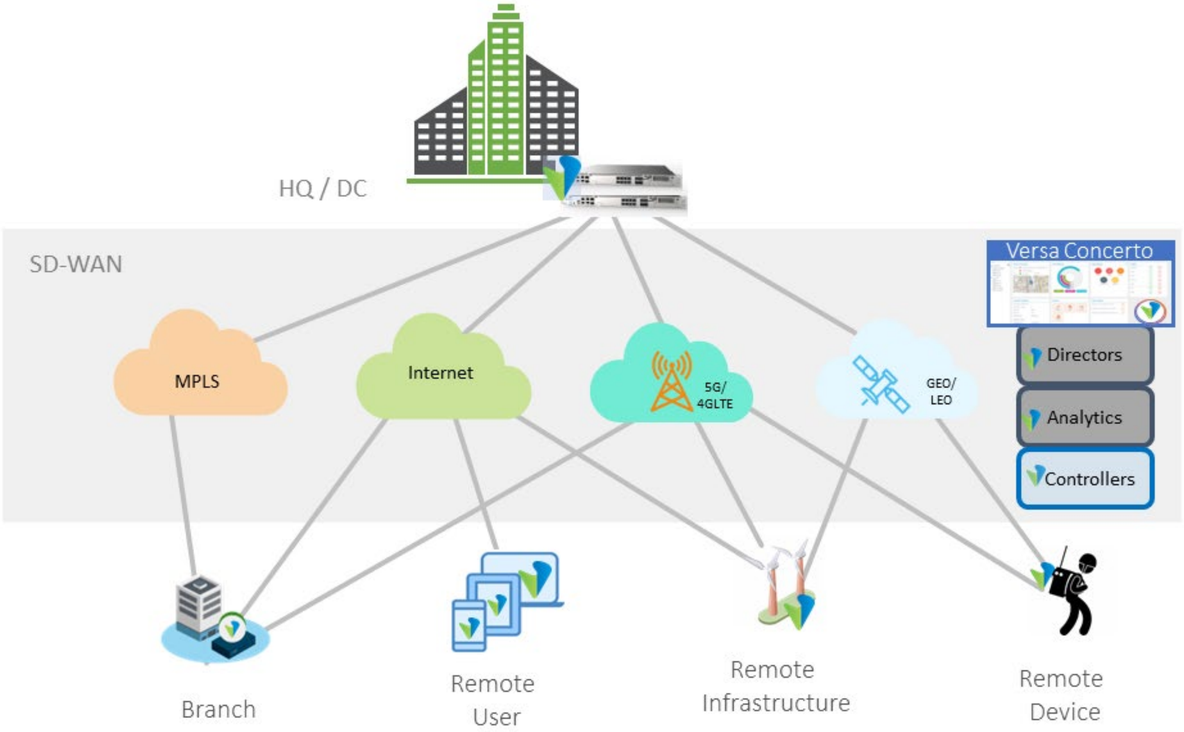
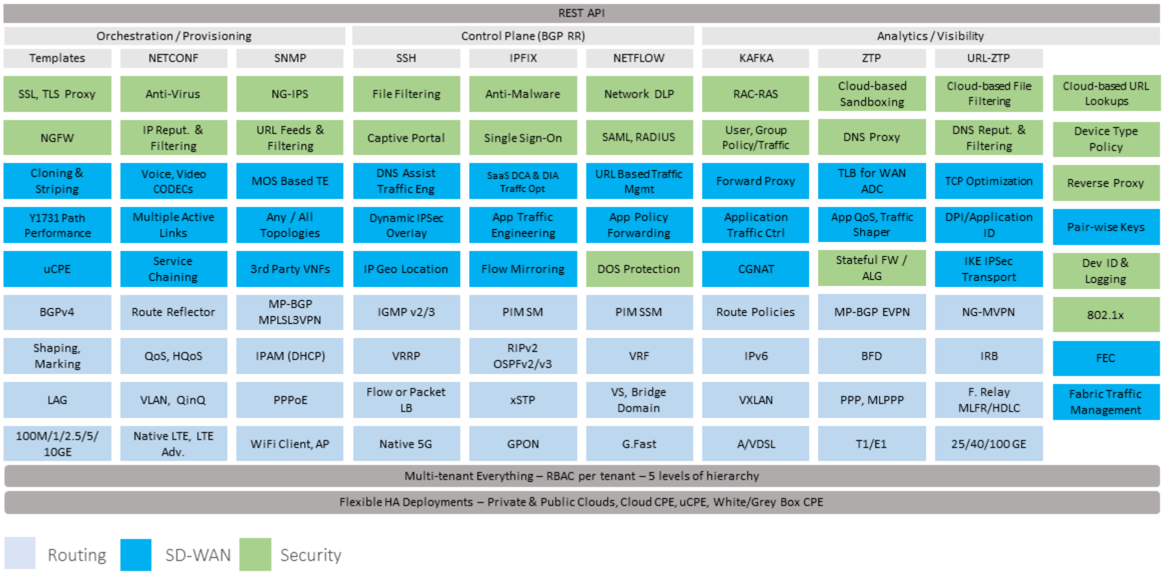


Figure 1 - Versa SD-WAN

Versa's comprehensive network and data security capabilities allow IT and security administrators to define security functions and policies once and apply them on all VOS nodes deployed across the network uniformly.

Versa now offers the same set of comprehensive connectivity and security functions on Versa's Software Defined Network Interface Card (SD-NIC) providing additional deployment options and flexibility for IT and security administrators.



REST API									
Orchestration / Provisioning			Control Plane (BGP RR)			Analytics / Visibility			
Templates	NETCONF	SNMP	SSH	IPFIX	NETFLOW	KAFKA	ZTP	URL-ZTP	
SSL, TLS Proxy	Anti-Virus	NG-IPS	File Filtering	Anti-Malware	Network DLP	RAC-RAS	Cloud-based Sandboxing	Cloud-based File Filtering	Cloud-based URL Lookups
NGFW	IP Reput. & Filtering	URL Feeds & Filtering	Captive Portal	Single Sign-On	SAML, RADIUS	User, Group Policy/Traffic	DNS Proxy	DNS Reput. & Filtering	Device Type Policy
Cloning & Striping	Voice, Video CODECs	MOS Based TE	DNS Assist Traffic Eng	SaaS DCA & DIA Traffc Opt	URL Based Traffic Mgmt	Forward Proxy	TLB for WAN ADC	TCP Optimization	Reverse Proxy
Y1731 Path Performance	Multiple Active Links	Any / All Topologies	Dynamic IPSec Overlay	App Traffic Engineering	App Policy Forwarding	Application Traffic Ctrl	App QoS, Traffic Shaper	DPI/Application ID	Pair-wise Keys
uCPE	Service Chaining	3rd Party VNFs	IP Geo Location	Flow Mirroring	DOS Protection	CGNAT	Stateful FW / ALG	IKE IPSec Transport	Dev ID & Logging
BGPv4	Route Reflector	MP-BGP MPLSL3VPN	IGMP v2/3	PIM SM	PIM SSM	Route Policies	MP-BGP EVPN	NG-MVPN	802.1x
Shaping, Marking	QoS, HQoS	IPAM (DHCP)	VRRP	RIPv2 OSPFv2/v3	VRF	IPv6	BFD	IRB	FEC
LAG	VLAN, QinQ	PPPoE	Flow or Packet LB	xSTP	VS, Bridge Domain	VXLAN	PPP, MLPPP	F. Relay MLFR/HDLC	Fabric Traffic Management
100M/1/2.5/5/ 10GE	Native LTE, LTE Adv.	WiFi Client, AP	Native 5G	GPON	G.Fast	A/VDSL	T1/E1	25/40/100 GE	
Multi-tenant Everything – RBAC per tenant – 5 levels of hierarchy									
Flexible HA Deployments – Private & Public Clouds, Cloud CPE, uCPE, White/Grey Box CPE									

Figure 2- Versa Operating System Feature Set

Leveraging Versa's comprehensive networking and security stack (see in Figure 2), Versa's Software-Defined Network Interface Card (SD-NIC) extends the security perimeter to within compute devices providing ZTNA, network and data security within the remote device.

By placing the security appliance inside the remote device, the security posture checks, and network & data security functions get placed as internal constructs within the remote device in the path of the traffic without the need for sending the traffic to outside for such assessments / functions.

VOS's feature set allows for the use of geo-location to define a security policy to limit the access of the remote device based upon the remote device's position. This could be very useful to deter acts of theft as once the geo-perimeter is violated, the device would become inoperable. Infrastructure could utilize this to prevent theft from the location as infrastructure is not expected to have mobility. Even in devices that are mobile, geo-location could be utilized to create regions of operation and violation of those regions would enact security policies to prevent or limit the access.

The Versa SD-NIC, as seen in Figure 3, is based on a PCI card, running VOS natively, and is inserted into a standard PCI slot(s) inside the remote device, just like a traditional NIC expansion card. Versa SD-NIC card has a multicore processor on it which runs the Versa Operating System (VOS). With this, now Versa can instantiate a Versa SASE node within the remote device.

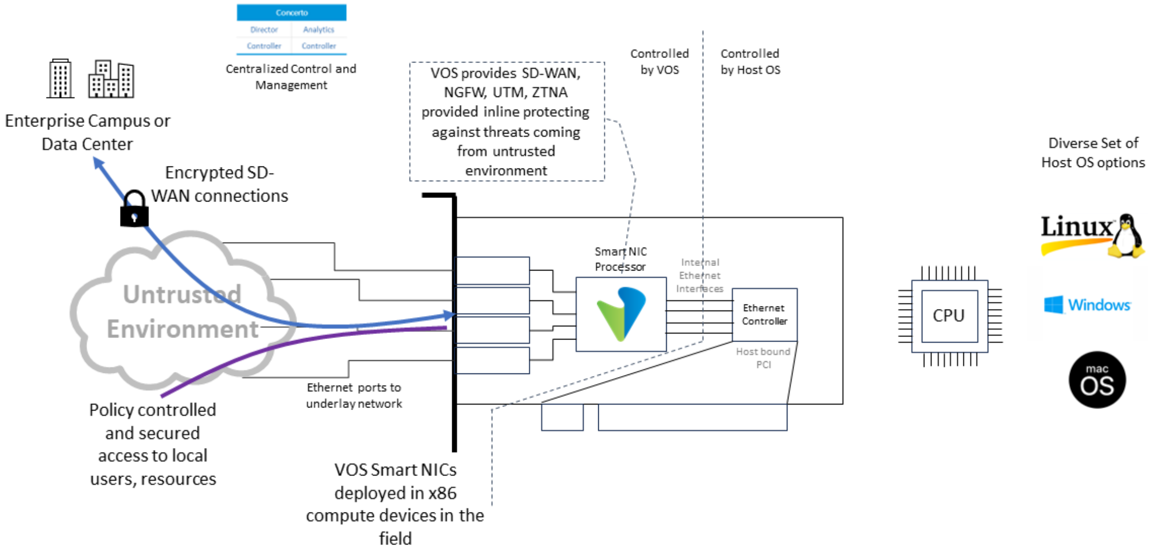

Concerto
Director
Analytics
Controller
Controller
Centralized Control and Management
Enterprise Campus or Data Center
Encrypted SD-WAN connections
Untrusted Environment
Policy controlled and secured access to local users, resources
VOS provides SD-WAN, NGFW, UTM, ZTNA provided inline protecting against threats coming from untrusted environment
Controlled by VOS
Controlled by Host OS
Smart NIC Processor
Internal Ethernet Interfaces
Ethernet Controller
Host bound PCI
Ethernet ports to underlay network
VOS Smart NICs deployed in x86 compute devices in the field
CPU
Diverse Set of Host OS options
Linux
Windows
mac OS

Figure 3 - SD-NIC Untrusted Environment

The Versa SD-NIC runs the same software, VOS, as with any other Versa device. Therefore, the SD-NIC has the full set of capabilities of VOS including SD-WAN, SD-LAN, Next-Gen Firewall (NGFW), Unified Threat Management (UTM), Zero-trust Network Access (ZTNA), micro-segmentation, Cloud Access Security Brokerage (CASB), Network based Data Leakage Prevention (DLP) and more. VOS is application-aware which allows for different security postures per application, segment, user, or device.

Since the Versa SD-NIC has its own CPU, memory, and storage, this SD-NIC can be installed into hardened devices where a traditional software agent would not be allowed. There is no dependence on the host software. If the remote device allows for the PCI card to be installed, then the Versa device can secure the traffic. Additionally, the SD-NIC includes a Trusted Platform Module (TPM) - TPM2.0. This enables the remote device to recognize the SD-NIC as valid and allows the SD-NIC to securely connect to the enterprise network. Additionally, the SD-NIC can be configured to use the TPM chip of the compute platform (if it has one) to create a secure authentication relationship between the compute platform and the SD-NIC. This would prevent movement of the SD-NIC from one remote device to another one possibly made to spoof the genuine server by bad actors. If the remote device does not have a TPM chip, a security profile can be created to secure the VOS from operating within a different remote device. Device fingerprinting would be used to create a host remote device profile and the VOS would only allow that fingerprint profile to pass through the security posture.

Versa offers numerous methods to onboard and deploy a remote device. The ZTP process utilizes security mechanisms to assure that the appropriate device connects to the appropriate service before any configuration can be applied to the SD-NIC. Global zero-tough provisioning is offered which utilizes factory installed certificates with the keys from the TPM chip. This process would connect to the Versa global provisioning system and then based upon serial number of the device, the Versa global provisioning system would redirect to the appropriate enterprise staging environment. This can be accomplished without physical access to the device since it automatically occurs upon boot sequence. The next two methods require some form of access to the device, either by ethernet cable or USB cable. URL based provisioning requires that a URL is communicated with the field user and then the URL is activated by the field user plugging an ethernet cable into the device. The URL is an encrypted URL that has the certificate for that session encrypted in the string. This prevents the usage of this URL for any other remote device provisioning. Script-based provisioning requires the USB console cable and the insertion of script string at the command line.   The Versa SD-NIC has the capability to perform a Secure Boot. Secure Boot utilizes keys stored in on the SD-NIC to validate that the bootable image is a trusted image and from a trusted source.

Each one of these provisioning methods can be configured to support multi-factor authentication (MFA). With MFA a token is sent to a pre-authorized device and the field user would need to either respond to the MFA or in the URL or script-based scenarios, enter the MFA token into the device to authenticate and authorize the provisioning.

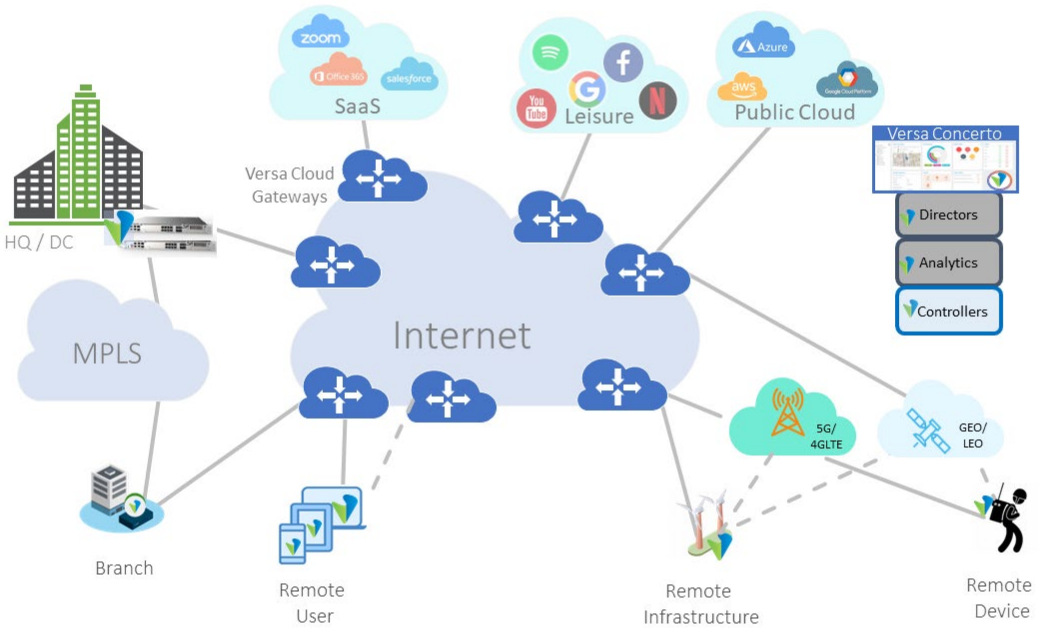


Figure 4 – Versa SASE

The remotely located compute platform can be configured to either connect to a SASE solution, as shown in Figure 4, or a be part of a Secure SD-WAN solution, as seen in Figure 1, over any type of transport. Versa supports connectivity over a variety of transport types. However, for most remote cases, the connectivity is either via an ethernet cable to a service provider (Internet), cellular connectivity (4GLTE or 5G), or satellite connectivity.

Versa anticipates ZTNA to be utilized to provide access control to/from the remote device and the rest of the network under strict policy guidance and based on dynamically assessed security posture. Versa's ZTNA solution assesses the security posture of the remote device by factoring in variety of parameters including OS details, whether any security package is used within remote device, if other security best practices have been implemented or not. VOS's native ZTNA capabilities can be configured in full (forward or reverse) proxy mode to terminate remote device-initiated sessions / flows to scan them using rich set of NGFW, UTM, SWG, ATP functions looking for malware or any other suspicious activity. Furthermore, VOS can be configured to provide detailed access control using built-in inline CASB functions and to scan for data for DLP purposes. Lastly, traffic to/from workloads can be micro-segmented based on dynamically assessed security posture, application, user, or other parameters.

Furthermore, since the Versa appliance is now installed into the compute appliance, the solution no longer requires extra space, power, nor additional cabling requirements. Thus, this reduces the physical footprint needed to support the compute, network, and security devices.

Traditionally, security appliances require one set of management tools and routers and switches require another set of management tools, perhaps even a different management tool set per vendor. Increased set of management tools implies that the security policies need to be configured separately in each of the management tools, and when changes are made to the security policies, this needs to be replicated to all the different management tools. Since the SD-NIC runs VOS natively, the Versa SD-NIC does not require any additional management tools if the customer already deployed Versa solution in any part of their network. Security policies can be instantiated for SD-WAN, SASE, ZTNA, or any other Versa offering from a centralized management tool. This simplifies the policy creation and deployment. Also, this simplifies the compliance process. Versa's policy engine has extensive capabilities to define policy at a granular level. Policies can be written based upon application, user, location, device, micro-segmentation, network, context (location, mobility, time), and many more. This provides for great flexibility when developing and implementing security postures. Versa also employs to assist with identification and remediation of threats or exfiltration of sensitive data. This provides for a more modern and advanced approach to threat discovery and remediation.

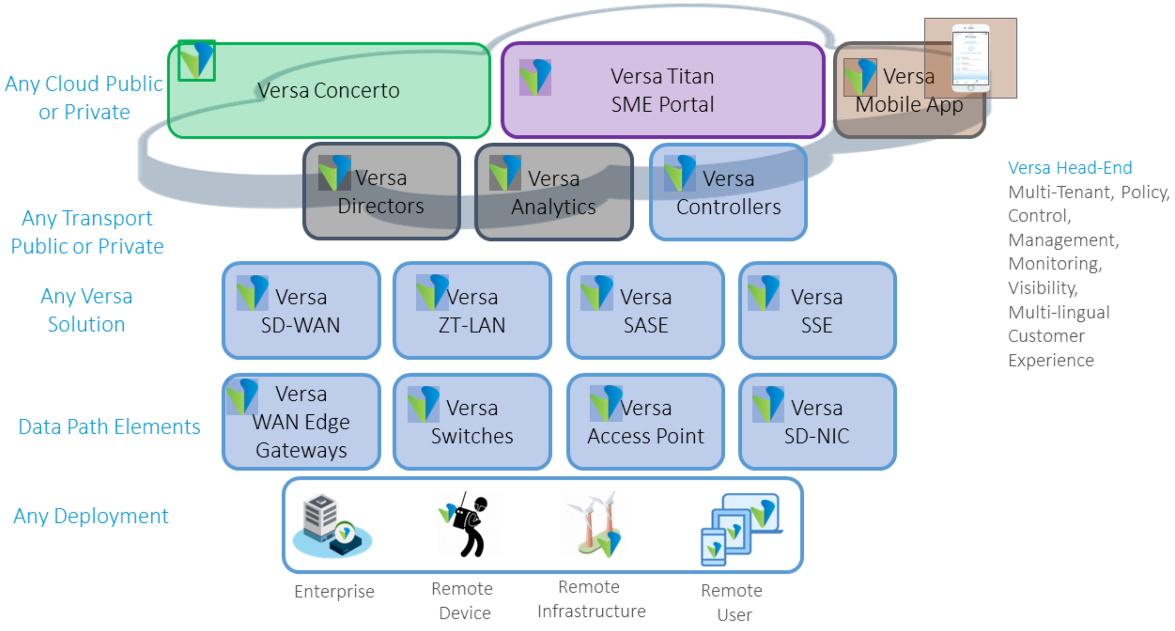


Figure 5- SD-NIC and Versa Solutions

As seen in Figure 5, the Versa management is centralized and controlled by the Versa Director, Concerto and Controllers. Additionally, the information data store is centralized in the Versa Analytics. This centralized management design allows for security policies to be applied uniformly across VOS instances across the network and on the cloud to deliver SD-WAN, SD-LAN, ZTNA, SASE and SSE. Utilizing the Versa SD-NIC, these security policies extend into the remote and IOT devices. This Versa management complex can be hosted in any Cloud Computing environment or in the enterprise environment. Versa offers multiple methods for managing the Versa management environment: Versa hosted and managed, Versa hosted but customer managed, customer hosted and Versa Managed, or both customer hosted and managed. In each of these management methods, the management of the components can be a hybrid model where Versa performs some of the management and the customer performs the remaining tasks.

The Versa SD-NIC is available in two different configurations today. Both configurations require no extra power and fit into a standard PCI slot. Both SD-NIC configurations have a USB 3.0 console port and a 1Gb Ethernet management interface.

The first is a 2x25G/10G interface card. This SD-NIC provides for approximately 4 Gbps throughput of SD-WAN with NextGen Firewall enabled. This SD-NIC provides for approximately 750 Mbps throughput for SD-WAN with UTM features enabled. This SD-NIC is ideal for those devices that transmit data at lower rates or utilize transport media with constrained bandwidth.

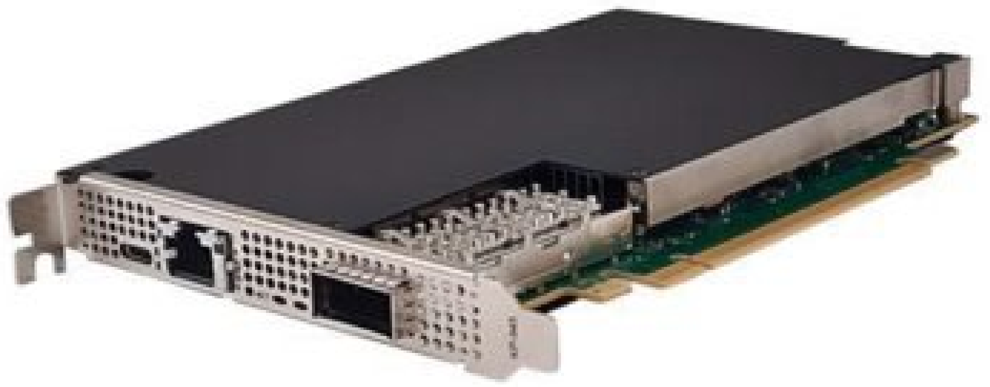


Figure 6- SD-NIC 100Gb

The second SKU is a 1x100G which is capable of 4x25G/10G breakout configuration, as seen in Figure 6. This SD-NIC provides throughput of approximately 8 Gbps of SD-WAN with NextGen Firewall enabled. This SD-NIC provides for approximately 1.5 Gbps throughput for SD-WAN with UTM features enabled. Given the high throughput rate with all security features enabled, this SD-NIC is capable of handling almost any remote device bandwidth needs.

Our customers can deploy multiples of these cards in each remote device. This can be a perfect example of providing for high bandwidth transport media; however, the remote device would need to support multiple PCI cards for this scenario. This is more likely in infrastructure deployments than mobile remote devices.

Furthermore, Versa is working to provide higher performance SD-NIC options in the near future.

For more details on Versa Secure SD-NIC or to request a demonstration, please visit *https://www.versa-networks.com/products/sd-nic* or contact a Versa sales representative.