SOLUTION BRIEF

VERSA NETWORKS

Achieving PCI DSS Compliance with Versa Secure SD-WAN

Information security in the age of internet banking

The Payment Card Industry Data Security Standard (PCI DSS) is a set of information security policies that protect credit and payment card data and transactions, which includes the cardholder name, card number, CVV code, authentication data, et al. Born in 2004 out of a collaboration among five major credit card companies, the PCI DSS governs any entity that stores, processes or transmits any such data and specifies 12 high-level requirements necessary to build and maintain secure networks and systems, irrespective of the point-of-sale application, the application server, or the network.

The Versa Secure SD-WAN, a cloud-native multi-tenant software platform that delivers software-defined Layer 3 [routing] to Layer 7 [security] services with full programmability and automation, enables business organizations to be compliant with PCI-DSS.

Summary of the PCI DSS requirements

	PCI DSS Requirement	Summary of Versa capabilities to meet compliance
1	Install and maintain a firewall configuration to protect cardholder data	The Versa SD-WAN has a stateful firewall and next generation firewall that provide zone-based access to different subnets/users. The configuration of the firewall is centrally managed and provides an audit of the change in configuration.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	During the installation process of Versa software components, it is mandatory to change default passwords for users. External identity servers like AAA servers can be used for identity management.
3	Protect stored cardholder data	No cardholder data is stored on the system.
4	Encrypt transmission of cardholder data across open, public networks	IPsec can be used for gateway-to-gateway encryption over public networks. The data is protected using Advanced Encryption Standard AES-256-bit ciphers using AES-CBC, AES-GCM and AES- CTR ciphers. Additionally, integrity of the data is protected using an SHA2 algorithm with 512-bit keys.
5	Use and regularly update anti-virus software or programs	Although this requirement applies to end-user systems, Versa provides protection against viruses or DoS attacks. Anti-virus protection is a feature of the Versa Secure SD-WAN platform, and when it is enabled, Versa software components and the end systems are protected from any malware attack from the network. The AV signature database is updated periodically once every 24 hours, with incremental updates available every 15 minutes.
6	Develop and maintain secure systems and applications	N/A
7	Restrict access to cardholder data by business need to know	Versa can be integrated with Active Directory and network policies to restrict access to only authorized machines/users for specific network segments using a centralized authorization server for the applications and services that require access to cardholder data. Additionally, the network access to the applications carrying cardholder data can be logged using Versa Analytics. This data can be audited to ensure no unauthorized data access has occurred.
8	Assign a unique ID to each person with computer access	The Versa Secure SD-WAN platform provides hierarchical Role-Based Access Control (RBAC) to authorize access to configure and manage any Versa software component. Active Directory integration with Versa's captive portal ensures that only authorized systems and users can reach the applications hosting payment card data using Versa's native firewall capability.
9	Restrict physical access to cardholder data	N/A
10	Track and monitor all access to network resources and cardholder data	Hierarchical RBAC controls access to configure and manage any Versa software component. In a multi-tenant system, the administrative rights for the network carrying payment card data can be restricted. Every action in Versa Director is logged and can be audited. Versa's integrated next-generation firewall and Versa Analytics log all activity and ensure it is traceable to the User ID for auditing.
11	Regularly test security systems and processes	N/A
12	Maintain a policy that addresses information security for all personnel	N/A

Securing the branch with Versa Secure SD-WAN

Versa's capabilities are uniquely placed at the edge of the branch network terminating SD-WAN access and transport. Through the SD-WAN, the branch network uses any available access network including the public internet access (broadband, ILL and 4G-LTE) along with private networks (Dark Fiber, MPLS, P2P links) to provide a dynamic virtual private network (VPN) overlay securely connecting the branch with other branches, data center and public or private cloud hosted applications.

Versa's secure SD-WAN solution provides a single-pane-of-glass portal to manage individual branch secure SD-WAN CPE appliances. Versa Director provides GUI-based access to configure, monitor and manage these appliances (virtual or physical). The branch CPEs are subjugated to Versa Director.

Versa's Secure SD-WAN uses the Versa Operating System (VOS), which has a single-pass pipeline design that provides data services, terminates WAN access network links, and dynamically creates the secure VPN fabric using IPsec to create a private overlay network. VOS also supports advanced application-level network security with native NGFW, UTM and IPS.

With this foundation, we will discuss how the Versa Secure SD-WAN platform addresses PCI DSS v3.2 requirements.

PCI DSS Requirement 1

Install and maintain a firewall configuration to protect cardholder data

Versa natively supports stateful firewall, next-gen firewall and ACL functions to protect the network from external and internal threats. Security policy and SD-WAN policy configuration is managed using Versa Director, thus ensuring a consistent policy configuration for both SD-WAN and firewall. Having a single device providing both WAN router functionality as well as security through stateful or next-generation firewall functionality reduces vulnerability and the attack surface for the network.

Versa Director provides portal-based configuration management of deployed Versa (on-premises or cloud). Versa Director maintains logs to track login attempts and configuration changes done by users. Role-Based Access Control (RBAC) ensures that only authorized users are allowed to make configuration changes. All configurations are maintained in a change history log maintained by Versa Director.

PCI DSS Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

Versa Director is the single-pane-of-glass portal for all management, configuration and monitoring of the Versa Secure SD-WAN platform. Versa Director provides different roles (administrator, operator, etc.) with specific access that can also be customized. Versa Director forces users to update the password upon first login and can be configured to force the use of smart passwords with expiration periods defined. Additionally, Versa Director can be integrated with standards-based AAA or SAML-based authentication services for user and identity management.

PCI DSS Requirement 3

Protect stored cardholder data

All components of the Versa Secure SD-WAN platform do not store the user or cardholder data. The data is processed and forwarded to the destination instantaneously.

PCI DSS Requirement 4

Encrypt transmission of cardholder data across open, public networks

Versa Secure SD-WAN platform can be configured to use IETF Standard IPsec-based cryptography to protect the data being transferred over public and private networks. The Versa solution can be configured to mandate specific encryption algorithms for specific networks to ensure the highest form of privacy for the cardholder data. Versa Secure SD- WAN supports advanced encryption standard-based (AES-256) ciphers for protecting the privacy of the communication. SHA2 using 512-bit keys can be used for maintaining the integrity of the communication.

PCI DSS Requirement 5

Use and regularly update anti-virus software or programs

The Versa Secure SD-WAN platform has native and built-in antivirus and IPS capabilities. The AV and IPS engines provide signature-based detection and prevention of known viruses and malware. Signatures are updated in real time when new threats are identified. Incremental updates to the signature database can be configured to be available every 15 minutes. When antivirus protection (AV) is enabled in the Versa software platform, end systems are protected from any known malware attacks from the WAN.

PCI DSS Requirement 8

Assign a unique ID to each person with computer access

The Versa SD-WAN can be integrated with Active Directory for authorizing access to the network. The integrated captive portal capability of Versa's NGFW enables every system or device access to be associated with a user within the organization. Additionally, all access to the network is logged using Versa Analytics for future audits. This can be used to control access to applications with access to payment card data.

Using Active Directory and Versa's captive portal, the access to the applications with payment card data access can be controlled and restricted, allowing only authorized users over the network segment. All the meta-data of users and systems accessing the application is logged by Versa Analytics for further analysis.

PCI DSS Requirement 10

Track and monitor all access to network resources and cardholder data

Versa Director manages the secure SD-WAN CPEs (physical or virtual). Versa Director provides RBAC, which restricts access only to authorized users. Versa Director maintains comprehensive audit logs to monitor all activities on Versa Director. Versa Director keeps track of all activity that happens in the network and provides the ability to roll back the changes if required.

Using Active Directory and Versa's captive portal, the access to the applications with payment card data access can be controlled and restricted, allowing only authorized users over the network segment. All network access meta-data is logged using Versa Analytics for further analysis. This creates an audit trail for analyzing network access attempts.

Requirements 6, 7, 9, 11 and 12 are applicable for the end-to-end payment card system architecture and not specifically applicable to the Versa Secure SD-WAN platform. Enterprises implementing Versa Secure SD-WAN must define processes to be compliant with the requirements.

Versa Secure SD-WAN multi-tenant architecture

The Versa Secure SD-WAN software platform supports multi-tenancy across all software components (Versa VOS, Versa Director and Versa Analytics) and across all layer 3, layer 4 and layer 7 services. The software solution allows segmentation of traffic by VLAN and VRFs. Multi-tenancy extends from Versa Director, with its per-tenant RBAC roles and configurations, Versa Analytics, with different views per tenant, and Versa Secure SD-WAN CPEs (physical or virtual), with separate IPsec tunnels per tenant and different cryptographic algorithms per-tenant.

The complete separation of configuration policy also extends to security policy. Enterprise customers can allocate PCI DSS-eligible traffic to a separate tenant with strict enforcement policies. Separate administration for banking transactions would allow specific administrative users to control those policies. Using the inherent multi-tenant capability, each tenant and segment can have unique topologies, to address how payment card data is delivered and access is controlled across the end-to-end network. For example, the payment card traffic can be restricted to a specific hub site for a hub-and-spoke topology while other application traffic can take other optimized or defined paths.