velocloud™
by Broadcom

SOLUTION BRIEF

KEY BENEFITS

Securing customer data is essential for retail organizations because any breach can be a devastating blow to the retailer's brand and value.

Broadcom® architecture and solutions protect customer points of sale and transaction data.

VeloCloud™ SD-WAN

PCI Compliance

Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard created by the Payment Card Industry Security Standards Council (PCI SSC). Designed to help organizations securely process card payments and prevent credit fraud, compliance with the PCI DSS is mandatory for businesses who transact payments for their goods and services with any of the major credit card brands associated with the payment card industry.

PCI-Compliant, Cloud-Delivered SD-WAN

Businesses that use cloud-delivered services to support a cardholder data environment (CDE) must ensure that the cloud-delivered service meets PCI DSS requirements. The easiest way for companies to do this is to partner with third-party service providers that undergo an annual PCI DSS audit and maintain an attestation of compliance (AoC). Significant value of a software-defined wide area network (SD-WAN) solution comes from a cloud-delivered management and control plane, greatly reducing total cost of ownership for adopters of SD-WAN. However, few SD-WAN vendors offer PCI-compliant cloud-delivered services, making it prohibitive for businesses with a PCI requirement to use cloud-delivered SD-WAN services that are not PCI compliant.

VeloCloud™ SD-WAN is the first SD-WAN solution to offer PCI-compliant hosting services. Enterprises and service providers that purchase the PCI add-on license will have their VeloCloud Orchestrator and VeloCloud Gateway tenant provisioned in PCI Level 1-compliant points of presence (PoPs). Customers provisioned in PCI-compliant PoPs will be provided with a PCI AoC which can be used to simplify and accelerate their own PCI audit. Additionally, a responsibility matrix is provided to customers that outlines the Broadcom DSS responsibilities, merchant DSS responsibilities, and Broadcom/merchant shared DSS responsibilities. Broadcom can furnish non-sensitive elements of its report on compliance upon request per the DSS.

PCI-Compliant, On-Premises SD-WAN

Whether customers use Broadcom PoPs or self-host the Orchestrator and Gateway, customers are responsible for ensuring their VeloCloud SD-WAN Edge is fully compliant with the DSS. The Edge is the sole responsibility of the customer because it physically or virtually resides in the customer's CDE. Key capabilities in the product, such as segmentation, enhanced firewall service (EFS), and other security features, simplify configuring the Edge to be compliant with PCI DSS.

The #1 point of entry for attacks against brick-and-mortar merchants is insecure remote access.

PCI SECURITY STANDARDS COUNCIL

For enterprises and service providers that prefer to self-host and self-manage the Orchestrator and Gateway, each component can meet PCI DSS security requirements. However, by self-hosting the Orchestrator and Gateway, the customer is entirely responsible for ensuring their deployment meets the security requirements outlined in the DSS. This deployment option is recommended for those customers with expertise in owning and operating network and virtualization infrastructure and security teams intimately familiar with applying security controls to meet DSS requirements.

Cardholder Data Flow

The following deployments are most common in a merchant environment with immediate benefits from a cloud-delivered SD-WAN solution.

Hub-and-Spoke Deployment

If all cardholder data (CHD) is transmitted from the retail branches to the hub, the hub will create an IPsec backhaul path to the PCI network. If the PCI network is in the data center on the LAN side, CHD will be transmitted from the retail branch directly to the PCI network.

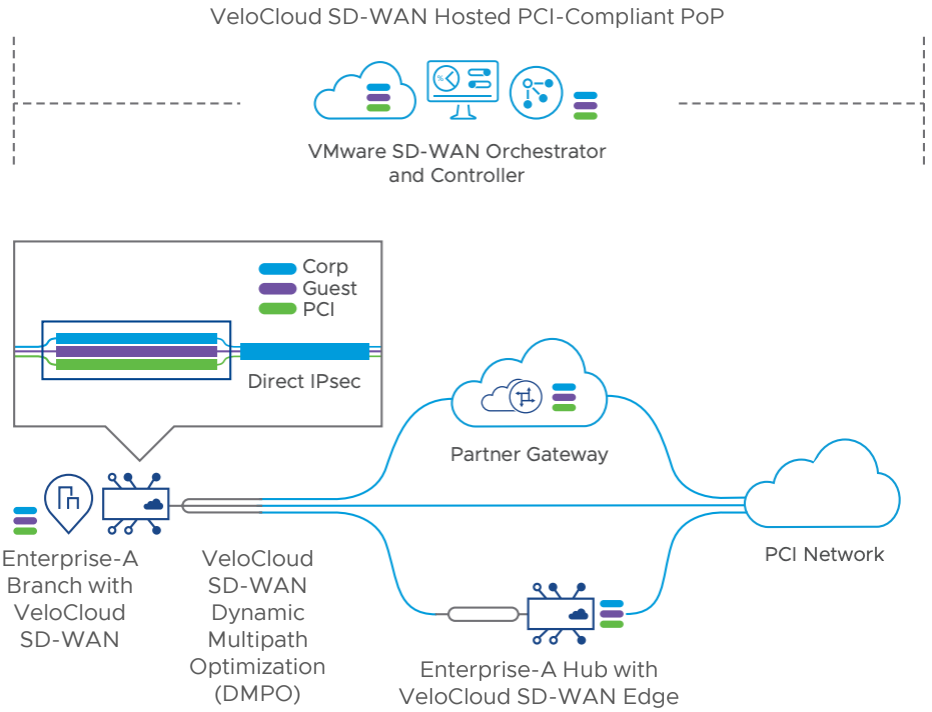
VeloCloud SD-WAN Gateways Hosted by a Channel Partner (Partner Gateway), including Service Providers

CHD flows are transmitted from the Edge to the partner gateway. From the partner gateway, traffic is handed off (802.1 or QinQ) to an MPLS private network to reach the customer data center and exit via the firewall in the data center to the PCI network. Alternately, from the partner gateway, a direct IPsec tunnel is created from the gateway to the PCI network.

Direct PCI Network Access

CHD can also be transmitted from the retail branch to the PCI network via an IPsec tunnel.

Figure 1: PCI-Certified VeloCloud SD-WAN



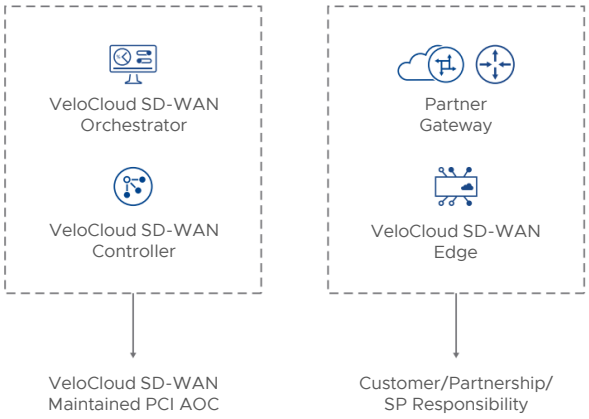
For any organization connected to the Internet, it is not a question of if but when their business will be under attack. With 42.8 million cyber attacks expected this year alone, and the cost of global cyber crime soaring to $465 billion a year, businesses cannot afford to take a reactive approach to security.

PCI SECURITY STANDARDS COUNCIL

Simplified Path to PCI Compliance

Customers who purchase the PCI add-on benefit from a simplified getting started process. Orchestrator and Gateway services are hosted in PCI-compliant PoPs. Broadcom maintains the PCI AOC by undergoing an annual audit of its PCI PoPs by a qualified security assessor. The resultant AoC from the audit can be used by customers of the PCI add-on service to simplify their own annual audit requirements. This shared responsibility model is illustrated in the figure below, which indicates that Broadcom is responsible for securing the hosted Orchestrator and Gateway, and the customer is responsible for Edge and Partner Gateway components.

Figure 2: Shared Responsibility Model



Global Segmentation and Security

Customers can reduce the scope of a PCI audit through segmentation, which enables isolation of the cardholder data environment from the rest of the retail network that is not subject to PCI DSS. This helps reduce general risk to the organization, as well as reduce scope and cost of PCI DSS assessment.

Global segmentation automatically isolates and carries segments across nodes. Customers do not have to put in firewall rules and extend segments with VPN. Segments are carried from branches to hubs or gateways across the VPN. Customers can also define segments to isolate traffic and insert business policies specific to each segment. The PCI segment can be isolated and securely delivered for payment processing.

Summary

The VeloCloud PCI add-on solution offers a simple, secure, cost-effective way for customers to achieve PCI compliance. With combined critical segmentation and security features, VeloCloud SD-WAN enables merchants to tap into the benefits of genuine SD-WAN while seamlessly meeting the requirements of PCI. With cloud-hosted centralized control through the VeloCloud Orchestrator, merchants can scale to thousands of retail locations.

To learn more, visit www.broadcom.com/products/software/velocloud-sd-wan.

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

VC-SD-WAN-PCI-Compliance-SB100 January 14, 2025