PCI Compliance with VMware SD-WAN

vmware SD-WAN™

The Payment Card Industry Data Security Standard PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). Designed to help organizations process card payments and prevent credit fraud, PCI DSS is the de facto standard to ensure secure transactions.

PCI-compliant, cloud-delivered SD-WAN

VMware SD-WAN™ is the first and only software-defined wide area network (SD-WAN) solution to offer PCI certification with SD-WAN services. VMware SD-WAN offers a simple, cost-effective means of achieving PCI compliance. Retailers and service providers can use VMware SD-WAN to establish their own PCI-compliant environments along with taking advantage of cloud-based solutions. Solution users can leverage the VMware SD-WAN attestation of compliance (AOC) to simplify and accelerate their own PCI audit process.

Centralized visibility and management with the VMware SD-WAN Orchestrator enables geographically distributed networks to implement PCI-compliant architectures across large numbers of retail locations.

PCI compliance components PCI DSS security requirements apply to all system components that process cardholder data or sensitive authentication data. PCI audits can be expensive and time-consuming, and the VMware SD-WAN AOC greatly simplifies the PCI audit process for retailers. All VMware SD-WAN components—including VMware SD-WAN Orchestrator, VMware SD-WAN Gateway, and VMware SD-WAN Edge—meet PCI requirements.

VMware SD-WAN also provides optional PCI-compliant points of presence (PoPs) with VMware SD-WAN Orchestrator and VMware SD-WAN Controller for customers who prefer to leverage the VMware SD-WAN AOC to further simplify their PCI audits. VMware SD-WAN will provide a PCI responsibility matrix upon purchase of the service.

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

PCI Security Standards Council

Securing customer data is essential for retail organizations because any breach can be a devastating blow to the retailer's brand and value. VMware provides architecture and solutions to protect customer points of sale and transaction data.

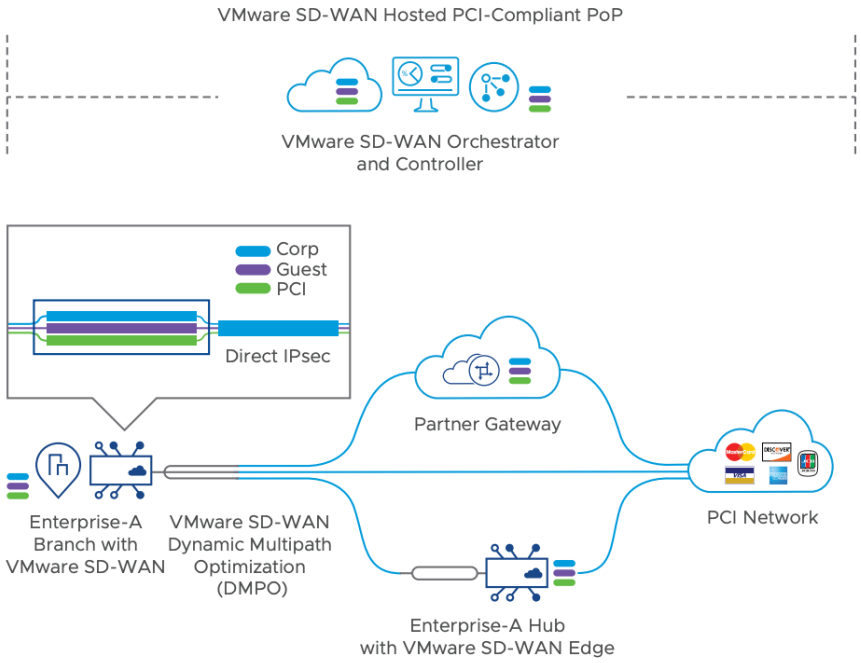

Figure 1: PCI-certified VMware SD-WAN

Cardholder data flow

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

VMware SD-WAN Gateways hosted by a channel partner (partner gateway), including service providers

Cardholder data (CHD) flows are transmitted from the VMware SD-WAN 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. Or from the partner gateway, a direct IPsec tunnel is created from the gateway to the PCI network.

Hub-and-spoke deployment

If all 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.

Direct PCI network access

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

Simplified path to PCI compliance

VMware SD-WAN customers benefit from an extremely simple process to get started. A PCI-compliant PoP is assigned to each customer. VMware SD-WAN maintains the PCI AOC on a regular basis for the VMware SD-WAN Orchestrator and the VMware SD-WAN Controller, helping customers with their certification and audit. Retailers will need to work with their PCI Qualified Security Assessor (QSA) to meet overall PCI guidelines such as store

"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 cyberattacks expected this year alone, and the cost of global cybercrime soaring to $US 465 billion a year, businesses cannot afford to take a reactive approach to security."

PCI Security Standards Council

security. The VMware SD-WAN Orchestrator and VMware SD-WAN Controllers are maintained by VMware SD-WAN, while the customer or service provider will assume responsibility for the partner gateway and the VMware SD-WAN Edge along with other components.

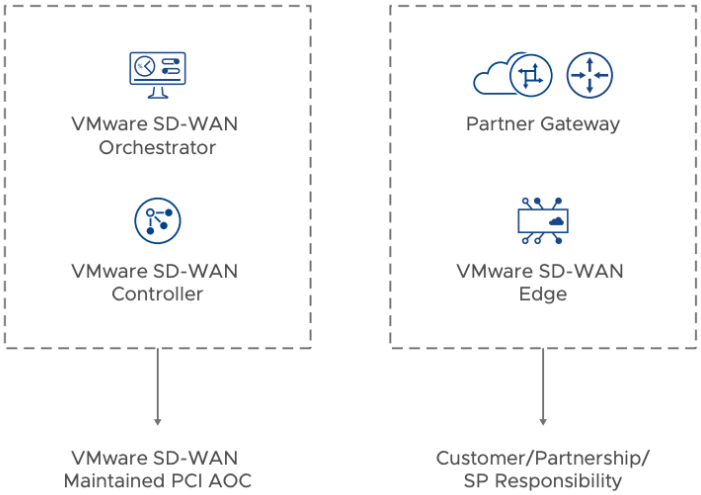

Figure 2: Shared responsibility model with VMware SD-WAN and customer/partner/service provider (SP).

Global segmentation and security

Customers can reduce the scope of a PCI audit through segmentation. Segmentation 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 the 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

VMware SD-WAN offers a simple, secure, and cost-effective way for customers to achieve PCI compliance. As a PCI-certified solution that includes critical segmentation and security features, VMware SD-WAN enables retailers to combine the benefits of genuine SD-WAN while seamlessly meeting the requirements of PCI. Additionally, centralized control with the VMware SD-WAN Orchestrator ensures scalability with hundreds of retail locations.

Learn more at www.vmware.com/solutions/sd-wan.html.