How the Unity EdgeConnect SD-WAN Edge Platform Supports PCI DSS Compliance

PCI DSS: Protecting Cardholder and Authentication Data

Highly sensitive personal identity and financial data have become enticing and highly lucrative targets for cyber criminals. According to the latest Nilson Report, worldwide payment card fraud losses reached $24.3 B in 2018 and are expected to exceed $34 B by 2022[1].

Vulnerabilities to credit card fraud exist anywhere in the transaction process including point-of-sale devices, personal computers, servers that store credit card or transaction data, Wi-Fi hotspots, web sites and web shopping applications and more. Protecting cardholder information is not only a challenge for any enterprise transacting credit card payments but a government mandate.

The Payment Card Industry (PCI) council was founded in 2006 to establish security standards for protecting credit cardholder data. The council publishes the PCI Data Security Standard (PCI DSS) which defines requirements for protecting customer credit card information and other financial data. PCI DSS "applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers...[and] to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)."[2] Violations may result in fines of $5,000 – $100,000 a month, or even revocation of a business' ability to accept credit cards for transactions.

Clarifying the meaning of PCI Compliance:

PCI requirements apply to merchants and companies that accept credit card payments and to entities that store, process, or transmit cardholder data. Network and security products cannot be "PCI-compliant" themselves, but if designed with features that protect security and privacy, they can help organizations achieve and maintain PCI compliance.

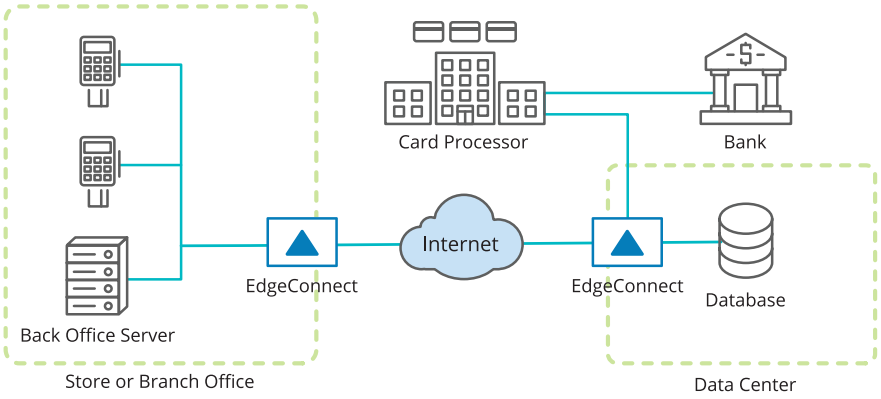

Figure 1: Credit card processing data flow: Personal financial information and card data must be protected end-to-end, even while data is in flight across the WAN.

Some organizations incorrectly assume that PCI compliance applies only to cardholder data stored on servers in databases. However, this information, which includes the cardholder name, credit card number, expiration date and CVV code, must be protected end-to-end throughout the transaction, even while data is in flight across the WAN. The Silver Peak Unity EdgeConnect™ Software Defined WAN (SD-WAN) edge platform helps enterprises proactively address vulnerabilities to data transmitted across the WAN. Robust security and application micro-segmentation features help organizations meet PCI compliance requirements.

PCI Requirements Overview for Merchants and Enterprises

Silver Peak helps organizations achieve and maintain PCI-DSS compliance, by creating virtual overlays to segment applications across the WAN and by using zones for end-to-end segmentation from LAN, to WAN, to LAN.

Network Segmentation – Strongly Recommended

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD, V3.2.1, PAGE 11:

"Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation…the entire network is in scope of the PCI DSS assessment."

SILVER PEAK:
Segment networks and applications into zones; control of access to zones containing cardholder data

PCI DSS REQUIREMENTS		HOW SILVER PEAK SUPPORTS COMPLIANCE
Build and Maintain a Secure Network and Systems		
1.	Install and maintain a firewall configuration to protect cardholder data	Protection of device and control planes; secure configuration and change management
2.	Do not use vendor-supplied defaults for system passwords and other security parameters	Password policies including default password warning
Protect Cardholder Data		
3.	Protect stored cardholder data	Boost WAN optimization network memory function may store packet contents on a flash drive or disk in which case it is encrypted using AES-128
4.	Encrypt transmission of cardholder data across open, public networks	Data and management interface encrypted using AES-256
Maintain a Vulnerability Management Program		
5.	Protect all systems against malware and regularly update anti-virus software or programs	Direct selected network traffic to anti-malware and sandboxing products from Silver Peak security partners using automation, orchestration, and drag-and-drop service chaining
6.	Develop and maintain secure systems and applications	Vulnerability assessments with each new release Issue patch updates as required
Implement Strong Access Control Measures		
7.	Restrict access to cardholder data by business need to know	Not applicable
8.	Identify and authenticate access to system components	Multiple unique logins for different user roles with appropriate privilege levels; Optionally support authentication with RADIUS or TACACS+; Enforce the use of multi-factor authentication for all non-console administrative access and remote access to the cardholder data environment
9.	Restrict physical access to cardholder data	Provisions for backup and disaster recovery; Silver Peak configuration and snapshots may be stored offsite
Regularly Monitor and Test Networks		
10.	Track and monitor all access to network resources and cardholder data	Full audit logs of user logins and all change management actions
11.	Regularly test security systems and processes	Not applicable
Maintain an Information Security Policy		
12.	Maintain a policy that addresses information security for all personnel	Not applicable

Building a Secure SD-WAN

EdgeConnect can help organizations comply with nine of the twelve requirements specified by PCI DSS. Robust security controls and features in EdgeConnect and the Unity Orchestrator™ management software enable enterprise IT administrators to secure credit card transaction data across the WAN. PCI DSS version 3.2.1 is used as the reference.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

This requirement applies to routers and other network infrastructure equipment including SD-WAN appliances. Orchestrator maintains audit logs for all logins and configuration changes. All management communications between Orchestrator and EdgeConnect appliances are encrypted using TLS. With WAN hardening, one can deny all other traffic except for protocols necessary for the cardholder data environment.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Industry best practices recommend always changing default login IDs and passwords. Silver Peak provides a warning to users that cannot be cleared without changing the default passwords. All non-console administrative access to the system can be encrypted using HTTPS for the UI and SSH for terminal sessions. For network management, SNMPv3, which provides authentication and encryption, is recommended, rather than using SNMPv1or v2.

Requirement 3: Protect stored cardholder data

In its default configuration, EdgeConnect does not store any packet payload information on a flash drive or disk, so no card information will be stored. With the optional Unity Boost™ WAN optimization performance pack, it is possible to apply WAN optimization to all or any subset of the traffic. As part of Boost, the network memory function may store packet contents on a flash drive or disk, in which case it is encrypted using AES encryption. If Boost is configured to operate on a protocol which carries cardholder data, any cardholder information contained in packets that is stored will be AES encrypted. Other cardholder data storage mechanisms are outside the scope of the EdgeConnect platform.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

All data transmitted across the SD-WAN is fully encrypted using NIST recommended cryptographic algorithms and security protocols. In each data path, EdgeConnect virtual WAN overlay tunnels employ 256-bit AES encryption for IPsec tunnels. For message authentication, SHA2 hashing is supported. In the management plane, Transport Layer Security (TLS) 1.2 is used for communication between EdgeConnect and Orchestrator, EdgeConnect and Cloud Portal, the end user's web browser and Orchestrator or EdgeConnect. Weak protocols such as SSLv2, SSLv3, TLS 1.0, and TLS 1.1, weak hashes like MD5, and weak encryption algorithms such as DES and RC4 are disabled.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

EdgeConnect appliances can ensure that network traffic containing protected data is routed through anti-malware products and other security tools. The EdgeConnect traffic steering feature with First-packet iQ™ classification identifies applications based on the first packet in a session. Through service chaining, applications that process or transmit cardholder data can be automatically directed to next-generation firewalls, cloud-hosted security services, anti-malware tools, and sandboxing products from security companies like Check Point, Forcepoint, McAfee, OPAQ Networks, Palo Alto Networks, Symantec, and Zscaler. The anti-malware tools can be located in stores and remote branches, in remote data centers, or in the cloud.

Requirement 6: Develop and maintain secure systems and applications

Silver Peak performs vulnerability assessments for new releases including maintenance releases. Silver Peak issues critical patch releases when a new vulnerability is discovered that may compromise security. Software development engineering follows secure coding principles to thwart cross-site scripting and other web application vulnerabilities as published by the Open Web Application Security Project (OWASP). Silver Peak publishes security-advisories on a regular basis.

Requirement 8: Identify and authenticate access to system components

Silver Peak supports unique user login IDs as well as multiple user roles with different privilege levels. For example, the "Administrator" role has change privileges and the "Monitor" role does not. Audit logs provide traceability to all user logins and all user activity. Authentication to the Orchestrator and EdgeConnect can optionally employ RADIUS or TACACS+ authentication servers. Passwords are not stored. Rather, random data or password salts are added before hashing the passwords. Silver Peak can enforce the use of token-based multi-factor authentication for all non-console administrative access and remote access to the cardholder data environment.

Requirement 9: Restrict physical access to cardholder data

While this pertains to restricting physical access to systems in the cardholder data environment, it also applies to backup and disaster recovery of systems and applications. Scheduled back-up to a secure off-site location and restore from a back-up server are fully supported across Orchestrator and EdgeConnect.

Requirement 10: Track and monitor all access to network resources and cardholder data

See response for Requirement 8.

Requirements 7, 11, and 12 are not applicable to the Unity EdgeConnect SD-WAN edge platform.

However, organizations must design internal processes to address safeguards for any and all personnel and procedures as they apply to the SD-WAN.

Network Micro-Segmentation to Limit the Scope and Cost of Assessments

The PCI DSS standard strongly recommends the use of network segmentation because it can reduce the cost and scope of PCI DSS assessments, make it easier to implement and maintain controls, and reduce risk to the organization. (See the text box on page 2). Silver Peak provides a simple, reliable way to implement end-to-end micro-segmentation through zone-based firewall features and virtual WAN overlays that span LANs, WANs, and data centers.

With EdgeConnect zone-based firewall capabilities, administrators can easily create secure zones, assign applications to them, and create unique security policies for each zone. The policies can completely block access between zones, allow traffic in one direction only, or restrict inter-zone traffic to specific uses. Orchestrator dynamically updates policies when the underlying infrastructure changes. These capabilities help isolate cardholder data environments from the rest of the organization's network.

Zones work with another core capability of the Silver Peak SD-WAN architecture: application-specific virtual WAN overlays. These overlays abstract network traffic flows for business processes from the physical transport resources underneath. Multiple virtual WAN overlays can be created and defined, each with its own unique QoS, reliability, and security parameters. A virtual WAN overlay may consist of one, two or more WAN services including MPLS, internet, and LTE, aggregated together to create a bonded tunnel. Each overlay is a secure, 256-bit encrypted tunnel providing the highest levels of security and segmentation edge-to-edge.

Virtual overlays help extend micro-segmentation over the WAN. For example, a virtual WAN overlay can be created to transport a financial application with specific QoS and security requirements, while isolating and handling guest Wi-Fi traffic across another virtual overlay. Secure application segmentation across the SD-WAN enables enterprise IT administrators to enforce compliance requirements when conducting credit card transactions that span multiple locations.

Beyond Compliance

The Silver Peak Unity EdgeConnect SD-WAN edge platform enables customers to simplify PCI DSS compliance — and much more. It also helps them create business-driven networks where resources are deployed to match the business priority of every application. Application users enjoy the highest quality of experience, IT and networking professionals benefit from improved network visibility and simplified management, and businesses are able to increase agility and lower costs related to networks and IT security.

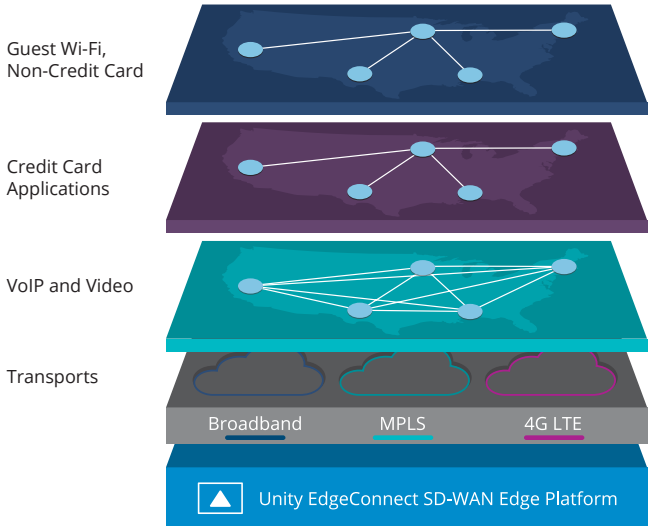

Figure 2: Application-specific WAN overlays extend microsegmentation across the WAN.

FOOTNOTES

1. https://apnews.com/74da23904a3c4d35b5c6067efbfbb18e
2. Payment Card Industry (PCI) Data Security Standard, v3.2.1, page 5

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com

SP-SB-EDGECONNECT-SD-WAN-EDGE-PLATFORM-PLATFORM-PCI-COMPLIANCE-062019