silver peak™ | Solution Brief

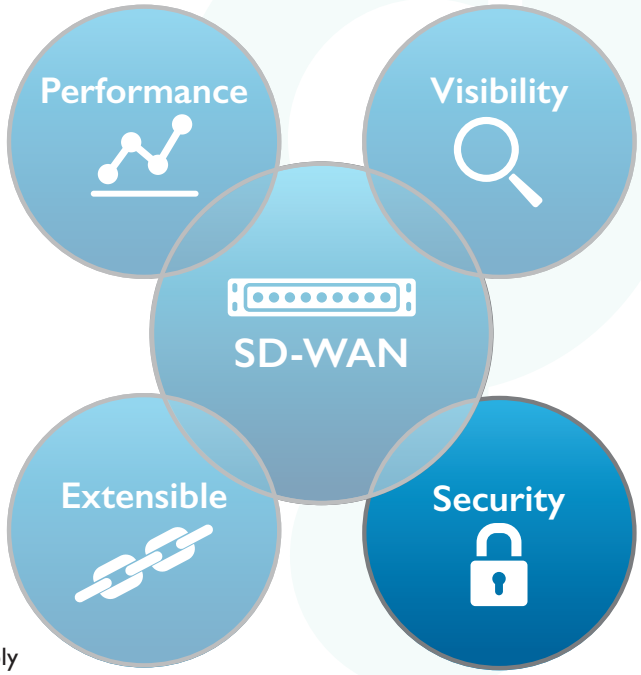
PCI Compliance Across the SD-WAN Protecting Personal Financial Data

PCI Compliance Mandate

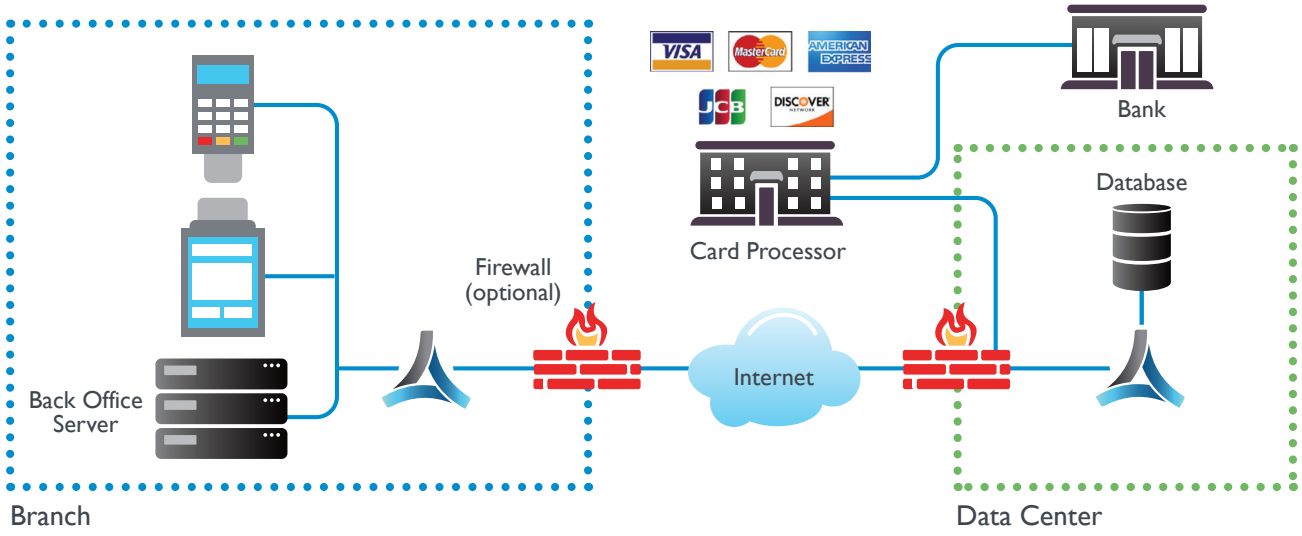
Highly sensitive personal identity and financial data have become enticing and highly lucrative targets for cyber criminals. According to Business Wire, fraud losses incurred on credit, debit, and prepaid payment cards reached $16.1 billion in 2014 and are expected to exceed $35 billion by 2020.[1] Vulnerabilities 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. A merchant, which is any organization that accepts, stores, or transmits cardholder data, must comply with PCI standards. The requirements apply whether card information is accepted in person, over the phone, or across the Internet or other data network, and violations may result in fines or even revocation of a merchant's ability to accept credit cards for transactions.

Robust security and micro-segmentation features of the Silver Peak EdgeConnect SD-WAN solution help customers meet PCI DSS compliance requirements



Building a Better WAN



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

[1] http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VcJZlvlVhBc

silver peak™ | Solution Brief

PCI Compliance Across the SD-WAN Protecting Personal Financial Data

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) solution 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

PCI DSS Requirements		Silver Peak
Build and Maintain a Secure Network and Systems		
1.	Install and maintain a firewall configuration to protect cardholder data	Also applies to SD-WAN appliances; protection of device and control plane; secure change and configuration 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 op network memory function may store packet contents on flash 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.	Use and regularly update anti-virus software or programs	Not applicable
6.	Develop and maintain secure systems and applications	Vulnerability assessments with each new release Issue patch updates as required. https://www.silver-peak.com/support/security-advisories
Implement Strong Access Control Measures		
7.	Restrict access to cardholder data by business need to know	Not applicable
8.	Assign a unique ID to each person with computer access	Multiple unique logins with different privilege levels Optionally support RADIUS or TACACS+
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

Clarifying the meaning of PCI Compliance:

PCI requirements apply to merchants or companies that accept credit card payments for transactions. Infrastructure products such as servers, storage arrays, network switches, routers, and SD-WAN appliances cannot be "PCI-compliant." Instead, these devices and their software must be designed with appropriate security measures and safeguards that follow the requirements set forth by PCI DSS in order to assist a merchant in maintaining PCI compliance.

silver peak™ | Solution Brief

PCI Compliance Across the SD-WAN Protecting Personal Financial Data

Building a Secure SD-WAN

Of the twelve requirements specified by PCI DSS, eight apply to the Silver Peak EdgeConnect SD-WAN solution. Robust security controls and features in EdgeConnect and the Unity Orchestrator enable enterprise IT administrators to secure credit card transaction data across the WAN. PCI DSSv3.1 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. The Silver Peak 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 flash or disk, so no card information will be stored. With the optional Boost 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 flash 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 Silver Peak SD-WAN solution.

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 the datapath, 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) is used for communication between Edge Connect and Orchestrator, EdgeConnect and Cloud Portal, the end user's web browser and Orchestrator or EdgeConnect. Weak protocols such as SSLv2, SSLv3, weak hashes like MD5, and weak encryption algorithms such as DES, RC4 are disabled.

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 security advisories can be accessed here: https://www.silver-peak.com/support/security-advisories

Requirement 8: Assign a unique ID to each person with computer access

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.

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.

Solution Brief

PCI Compliance Across the SD-WAN Protecting Personal Financial Data

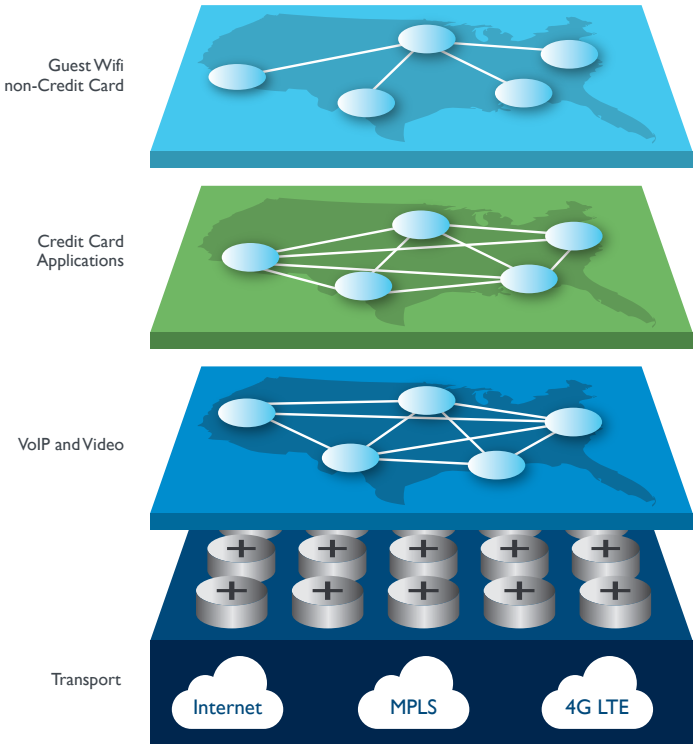
Requirement 10: Track and monitor all access to network resources and cardholder data
See response for Requirement 8.

Requirements 5, 7, 11, and 12 are not applicable to the EdgeConnect SD-WAN solution. However, organizations must design internal processes to address safeguards for any and all personnel and procedures as they apply to the SD-WAN.

Application-specific Overlays and Micro-Segmentation

A core capability of the Silver Peak SD-WAN architecture is the ability to configure and create application-specific virtual WAN overlays that abstract the virtual WAN overlay from the physical transport resource underlay. Multiple virtual WAN overlays may 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.

Advances in data center security now include the ability to segment traffic based on application characteristics and security policies, known as micro-segmentation. Creating an SD-WAN using virtual overlays allows micro-segmentation to extend beyond the data center. 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 a different virtual overlay. Secure application segmentation across the SD-WAN enables enterprise IT administrators to enforce compliance requirements when conducting credit card transactions across multiple locations.



Application-specific virtual WAN overlays extend micro-segmentation across the WAN

The Silver Peak Security Advantage

A Silver Peak SD-WAN solution enables customers to significantly increase application performance and lower WAN costs by using broadband internet connections to augment or even replace leased line services. However, the internet is notoriously insecure. A key attribute of an SD-WAN is the creation of secure, 256-bit encrypted tunnels between every endpoint. While this secure overlay model protects cardholder data as it is transmitted across the WAN, it is only one security measure required for an enterprise to adhere and comply to the provisions specified by PCI DSS.

The Silver Peak security architecture encompasses the management plane as well as the data forwarding plane. By configuring multiple virtual WAN overlays, Silver Peak enables enterprise IT organizations to segment and isolate sensitive customer financial data from other applications running across the WAN. By taking a holistic approach to security Silver Peak aids enterprises in meeting all PCI requirements relevant to the WAN.