

# How the HPE Aruba Networking EdgeConnect SD-WAN platform supports PCI DSS compliance

PCI DSS: Protecting cardholder and  
authentication data

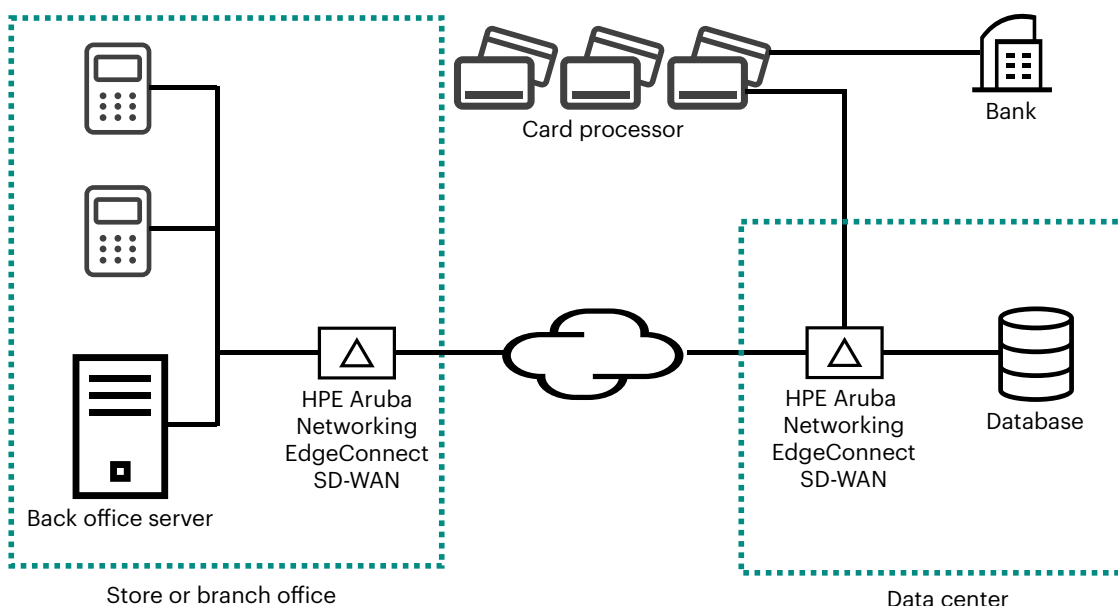
Highly sensitive personal identity and financial data have become enticing and highly lucrative targets for cyber criminals. According to the Nilson Report, worldwide payment card fraud losses reached \$33.45 B in 2022.<sup>1</sup>

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, websites 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.

## 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.

<sup>1</sup> [Issue 1254, Nilson Report](#), December 2023.

“PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing—including merchants, processors, acquirers, issuers, and other service providers.”<sup>2</sup> Violations may result in fines of \$5000 – \$100,000 a month, or even revocation of a business’ ability to accept credit cards for transactions.

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 EdgeConnect SD-WAN platform helps enterprises proactively address vulnerabilities to data transmitted across the WAN. Robust security and application microsegmentation features help organizations meet PCI compliance requirements.

## Network segmentation—Strongly recommended

The Payment Card Industry (PCI) Data Security Standard V4.0, page 12, states that: “Segmentation (or isolation) of 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
- Cost of the PCI DSS assessment
- Cost and difficulty of implementing and maintaining PCI DSS controls
- Risk to an organization relative to payment card account data (reduced by consolidating that data into fewer, more controlled locations)”

The EdgeConnect SD-WAN platform helps segment networks and applications into zones and control access to zones containing cardholder data. Additionally, HPE Aruba Networking SSE (security service edge) provides ZTNA (zero trust network access) capabilities that enforce least privilege access at the application level based on identity, ensuring that users and third-party users only access the resources they need.



<sup>2</sup> Payment Card Industry (PCI) Data Security Standard, v4.0, page 4

**Table 1. How EdgeConnect SD-WAN supports PCI DSS compliance**

DSS requirements	How EdgeConnect SD-WAN supports compliance
<b>Build and maintain a secure network and systems</b>	
1. Install and maintain network security controls	Next-generation firewall, dynamic segmentation; secure configuration and change management
2. Apply secure configurations to all system components	Password policies including default password warning
<b>Protect account data</b>	
3. Protect stored account 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. Protect cardholder data with strong cryptography during transmission over open, public networks	Data and management interface encrypted using AES-256
<b>Maintain a vulnerability management program</b>	
5. Protect all systems and networks from malicious software	Secure access service edge (SASE) platform from HPE Aruba Networking and built-in EdgeConnect SD-WAN next-generation firewall
6. Develop and maintain secure systems and software	Vulnerability assessments with each new release Issue patch updates as required
<b>Implement strong access control measures</b>	
7. Restrict access to system components and cardholder data by business need to know	EdgeConnect SD-WAN next-generation firewall and HPE Aruba Networking ZTNA enforce a zero trust architecture and apply least privilege access principles.
8. Identify users and authenticate access to system components	The integration of HPE Aruba Networking ClearPass Policy Manager with EdgeConnect SD-WAN adds identity knowledge of users, devices and roles to manage network access anywhere on the network—wired or wireless infrastructure
9. Restrict physical access to cardholder data	Provisions for backup and disaster recovery; EdgeConnect SD-WAN configuration and snapshots may be stored off-site
<b>Regularly monitor and test networks</b>	
10. Log and monitor all access to system components and cardholder data	Deny, accept, and drop events related to traffic sessions and intrusion detection are logged and monitored. This information can be sent to SIEM solutions
11. Test security of systems and networks regularly	EdgeConnect SD-WAN next-generation firewall includes intrusion detection and prevention capabilities (IDS/IPS)
<b>Maintain an information security policy</b>	
12. Support information security with organizational policies and programs	EdgeConnect SD-WAN helps improve incident response by providing dashboards and alerts to monitor network health.

## Building a secure SD-WAN

EdgeConnect SD-WAN can help organizations comply with requirements specified by PCI DSS. Robust security controls and features in EdgeConnect SD-WAN and the Orchestrator management software enable enterprise IT administrators to secure credit card transaction data across the WAN. PCI DSS version 4.0 is used as the reference.

### Requirement 1: Install and maintain network security controls

This requirement describes what is necessary to ensure that network traffic between logical or physical network segments is controlled such that the organization is protected from exposure to untrusted networks.

EdgeConnect SD-WAN integrates a next-generation firewall that provides advanced security features such as network segmentation, intrusion detection and prevention, DDoS defense and mitigation, as well as application and user/device identity awareness.

To limit traffic between highly sensitive areas, such as cardholder environments (CDE) and less sensitive areas, network administrators can configure microsegmentation in EdgeConnect SD-WAN. Virtual overlays are mapped to LAN-side zones and each zone is assigned security policies. The connectivity between zones is then limited by allowing or denying traffic. Additionally, HPE Aruba Networking ClearPass integration with EdgeConnect SD-WAN adds user and device identity and role-based context, enabling fine-grained segmentation. For example, organizations can protect their network from the exploding number of IoT devices, such as payment terminals, by isolating network segments and restricting access based on identity and role in the business. Fine-grained segmentation is critical in helping financial institutions meet PCI DSS compliance requirements.

With zero touch provisioning, security policies are automatically pushed to branches from Orchestrator. Security policy changes can be configured centrally and automatically distributed to hundreds or thousands of branches in minutes while minimizing errors that often occur when manually programming on a device-by-device basis. All management communications between WAN Orchestrator and EdgeConnect SD-WAN are encrypted using TLS.

### Requirement 2: Apply secure configurations to all system components

This requirement is intended to prevent malicious individuals from using default passwords and other vendor default settings to compromise systems and ensure secure configuration. EdgeConnect SD-WAN provides a warning to users that cannot be cleared without changing the default passwords. All nonconsole administrative access to the system can be encrypted using HTTPS for the UI and SSH for terminal sessions. For network management, SNMP v3, which provides authentication and encryption, is recommended, rather than using SNMP v1 or v2.

### Requirement 3: Protect stored account 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 WAN boost 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: Protect cardholder data with strong cryptography during transmission over open, public networks

All data transmitted across the SD-WAN is fully encrypted using NIST recommended cryptographic algorithms and security protocols. In each 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) 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 SSL v2, SSL v3, 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 and networks from malicious software**

To ensure protection against malicious software, EdgeConnect SD-WAN seamlessly integrates with HPE Aruba Networking (security service edge) SSE. This integration supports advanced security services such as secure web gateways (SWG), cloud access cloud access security broker (CASB), zero trust network access (ZTNA), all delivered in the cloud.

Additionally, EdgeConnect SD-WAN can integrate with third-party SSE vendors. Through service chaining, applications that process or transmit cardholder data are automatically directed to cloud-hosted security services, anti-malware tools, DLP, and sandboxing services in a SASE architecture.

### **Requirement 6: Develop and maintain secure systems and software**

This requirement describes the secure development of software code for all system components. Regarding EdgeConnect SD-WAN, HPE Aruba Networking performs vulnerability assessments for new software releases, including maintenance releases. HPE Aruba Networking 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).

### **Requirement 7: Restrict access to system components and cardholder data by business need to know**

This requirement describes limiting access to systems and data based on the need to know and according to job responsibilities. Coupled with HPE Aruba Networking ClearPass Policy Manager, the EdgeConnect SD-WAN next-generation firewall enforces a zero trust architecture by dynamically segmenting the network. It ensures that users and devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

Additionally, EdgeConnect SD-WAN seamlessly connects to HPE Aruba Networking SSE that provides ZTNA capabilities for users accessing corporate resources from anywhere. Unlike VPNs that grant broad access to the corporate network, ZTNA restricts user access to specific applications or microsegments that have been authorized for each user. This approach enforces the principle of least-privilege access. It allows remote workers to connect securely from anywhere. Additionally, with agentless ZTNA, third-party users can simply access the corporate network without the need to install a ZTNA agent on their device.

### **Requirement 8: Identify users and authenticate access to system components**

The integration of ClearPass Policy Manager with EdgeConnect SD-WAN adds identity knowledge of users, devices, and roles to manage network access anywhere on the network—wired or wireless infrastructure. With ClearPass, organizations can deploy standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT. Multiple authentication methods can be used to concurrently support a variety of use cases including support for multifactor authentication based on log-in times, posture checks, and other contexts such as new user, new device, and more.

For networks managed by HPE Aruba Networking Central, the cloud authentication feature enables on-boarding of end users and client devices either through MAC address-based authentication or through integrations with cloud identity stores such as Google Workspace™ or Azure Active Directory to automatically assign the right level of network access.

### **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 backup to a secure off-site location and restore from a backup server are fully supported across WAN Orchestrator and EdgeConnect SD-WAN.

### **Requirement 10: Log and monitor all access to system components and cardholder data**

EdgeConnect SD-WAN captures deny, accept, and drop events related to traffic sessions and intrusion detection. This information can be sent in syslog message format to logging tools, third-party SIEM solutions, and security analytics tools, to help analysts more quickly identify and respond to security incidents.

The EdgeConnect SD-WAN Security App for Splunk, a leader in the SIEM space, provides a dashboard view of all security event notifications exported from EdgeConnect SD-WAN devices. Network administrators can easily configure EdgeConnect SD-WAN to forward all security event notifications to Splunk, centralizing logging, visualization, and analysis of security events alongside other telemetry or network events. From Splunk, users can filter, sort, navigate and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help them pinpoint network events that require further investigation.



Figure 2. Splunk security dashboard

### Requirement 11: Test security of systems and networks regularly

This requirement prescribes testing systems and networks frequently to ensure security. It includes one paragraph requiring that network intrusions are detected and responded to.

EdgeConnect SD-WAN next-generation firewall offers intrusion detection and prevention capabilities (IDS/IPS) and DDoS defense. The signature-based intrusion system monitors network traffic to find patterns that match a particular attack signature and provides actions such as inspect, drop, and allow traffic when an intrusion is detected. The signature set is automatically updated on a regular basis. Threat events can be streamed to Security Information and Event Management (SIEM) systems for log review.

EdgeConnect SD-WAN also detects and prevents DDoS attacks such as protocol attacks, ICMP floods, and SYN floods. Using firewall protection profiles, the solution limits the number of malicious requests with actions such as rapid aging, drop excess, and block source.

### Requirement 12: Support information security with organizational policies and programs

This requirement describes how an organization should implement an overall information security policy so that all personnel are aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Even though this requirement is mainly organizational, the last paragraph requires that security incidents are responded to immediately by monitoring and responding to alerts from security monitoring systems:

EdgeConnect SD-WAN provides centralized network visibility and control into network health and performance. A health map monitors in real-time network health based on configured thresholds for packet loss, latency, and jitter. All HTTP and native application traffic are identified by name and location, and alarms and alerts allow for faster resolution of network issues. Additionally, the integration with popular SIEM tools like Splunk allows network administrators to monitor the network for intrusion and set alerts to detect intrusions.



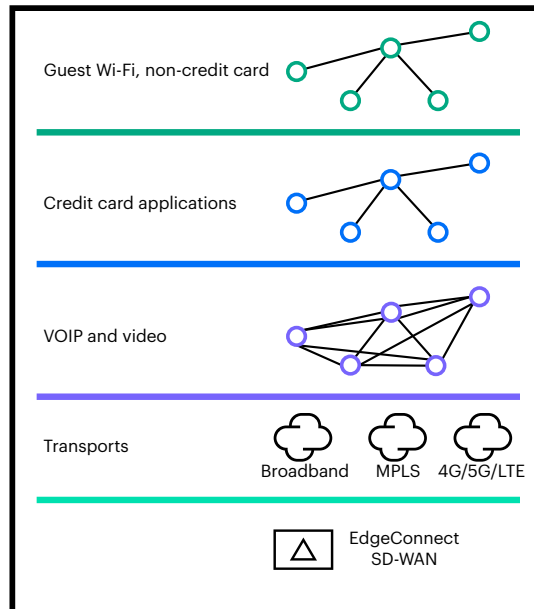
## Network microsegmentation to limit the scope and cost of assessments

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. HPE Aruba Networking provides a simple, reliable way to implement end-to-end microsegmentation through next-generation firewall features and virtual WAN overlays that span LANs, WANs, and data centers. With EdgeConnect SD-WAN next-generation 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 EdgeConnect 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 microsegmentation 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 EdgeConnect SD-WAN platform enables organizations 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 3.** Application-specific WAN overlays extend microsegmentation across the WAN.

[Visit HPE.com](https://www.hpe.com)

### [Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google Workspace is a trademark of Google Inc. Active Directory and Azure are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a00119355ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

