Hewlett Packard Enterprise

Deploy HPE ProLiant Easy Connect in a PCI-DSS compliant IT environment

Contents

Technical white paper
For HPE and Channel Partner internal use only.

Introduction

This document identifies how HPE ProLiant Easy Connect can be deployed into a Payment Card Industry Data Security Standard (PCI-DSS) compliant IT environment.

Merchants have the option to benefit from the security and keep-current features of HPE ProLiant Easy Connect to deploy their own compliant solutions, or to reduce compliance costs by adding a product option that delivers certified compliant features and support services.

The resources and services provided by Hewlett Packard Enterprise comprise just one part of the environment against which PCI-DSS compliance will be assessed. The configuration of other devices on the network, the payment terminals used, physical security, staff training, business processes, procedures, and policies must all also be considered.

Nonetheless, the IT services supported by HPE ProLiant Easy Connect, including file storage, user security credentials, network protection, and secure VMs for hosting applications are critical systems for any retail or hospitality business. Proper use of HPE ProLiant Easy Connect services within a PCI-DSS compliant environment can result in reduced cost and effort to meet compliance requirements and simplified compliance auditing.

The importance of compliance

PCI-DSS is a security standard for businesses that mandates compliance for any merchants who store, process, or transmit credit card data, including cardholder information. PCI-DSS is supported by all major card brands. It exists to reduce credit card fraud by ensuring organizations use secure IT systems and follow good business practices while handling credit card data.

Adherence to PCI-DSS standards is mandatory for organizations wishing to process any of the major card brands, requiring an annual compliance assessment by either an external PCI Qualified Security Assessor (QSA) or by self-assessment, depending either on the volumes of transaction handled or the requirements of the merchant's bank.

Failure to achieve formal compliance, or a card data breach, can result in substantial fines and ultimately the suspension of the merchant's license. This would inevitably lead to additional security requirements being enforced and forensic audits required, all incurring significant cost to the business.

Options for reducing PCI-DSS compliance risk

HPE ProLiant Easy Connect benefits

HPE ProLiant Easy Connect offers consistent, enterprise-grade security and monitoring that can be used to meet PCI-DSS compliance standards.

- The unique HPE ProLiant Easy Connect keep-current service ensures server operating systems and security software is patched and updated as mandated by the PCI-DSS.
- A next-generation firewall option and internet gateway software are deployed on each server to meet requirements for resisting penetration scanning.
- The consistency of server, security, and software architecture across all retail stores, reduces compliance auditing effort and complexity.

PCI-DSS compliant product option

Hewlett Packard Enterprise offers enhanced PCI-DSS support to merchants who want to significantly reduce the cost and effort of achieving compliance for their in-store IT. This add-on product option delivers HPE ProLiant Easy Connect with enhanced security policies and additional support processes, backed by a PCI-DSS Matrix of Responsibility (MoR) and Attestation of Compliance (AoC).

Enhanced features and services

In order to achieve compliance for the HPE ProLiant Easy Connect software and services, the PCI-DSS product option adds a number of features to the standard product offering. The highlights include:

- Implementation of policy and procedures ensuring the HPE ProLiant Easy Connect Support Team operate as a PCI-DSS tier-1 service provider
- Heightened security event and log auditing by the HPE ProLiant Easy Connect Support Team
- Provision of dedicated cloud management platform resources
- Hardened security features enabled in the cloud management platform and on HPE ProLiant Easy Connect servers
- Enforcement of compliant intrusion prevention measures such as password policy, failed logon blocking, and port blocking

In addition to the features that are provided to meet compliance, HPE ProLiant Easy Connect has been audited to PCI-DSS 3.2 standards by an independent QSA. This allows the PCI-DSS compliant product option to be provided with MoR and AoC.

Matrix of Responsibility
MoR clearly defines the parties responsible for each PCI-DSS requirement.

HPE ProLiant Easy Connect services runs on both the HPE ProLiant Easy Connect server and on the HPE ProLiant Easy Connect cloud management platform, which is hosted on Amazon Web Service (AWS). HPE ProLiant Easy Connect includes a managed services element, which the Support Team is able to provide assistance with. It includes monitoring, configuration, fault handling, and other administrative tasks on the server.

The HPE ProLiant Easy Connect MoR documents the division of responsibilities between the HPE ProLiant Easy Connect team, the merchant, and AWS for the 12 primary PCI-DSS (version 3.2) responsibilities along with the two appendixes (A1 and A2).

- Hewlett Packard Enterprise for maintaining HPE ProLiant Easy Connect software on the server and in the cloud
- Hewlett Packard Enterprise for ensuring secure administrative and security monitoring processes are in place relating to HPE ProLiant Easy Connect
- AWS for secure hosting of HPE ProLiant Easy Connect cloud services
- The merchant (or their IT service provider) for other PCI-DSS requirements

A summary of the standard HPE ProLiant Easy Connect PCI-DSS MoR can be found in this document's annex.

Attestation of Compliance
A merchant is responsible for their own PCI-DSS compliance certification. For the parts of the IT environment deployed on HPE ProLiant Easy Connect, the auditor can refer to the provided AoC. Because HPE ProLiant Easy Connect has already been audited, those parts that remain the responsibility of Hewlett Packard Enterprise and AWS in the MoR, will not require further investigation by the merchant's auditors.

Therefore, by providing an AoC, the HPE ProLiant Easy Connect PCI-DSS compliance product option significantly reduces the scope, cost, and time taken to complete a retail store's own compliance audit.

Reducing PCI-DSS scope

One of the most efficient ways to maintain PCI-DSS compliance is to minimize the number of IT resources that are "in scope."

Any system that stores, processes, or transmits card payment data will be in scope and, therefore, assessed for compliance. Minimizing the number of in-scope systems and using only approved payment devices, where possible for in-scope systems, will reduce a business' compliance effort and accelerate the compliance assessment process.

If a merchant opts to not use the HPE ProLiant Easy Connect PCI-DSS compliant product option, they should aim to create an IT environment that keeps HPE ProLiant Easy Connect out of scope. HPE ProLiant Easy Connect continues to deliver IT services to the retail store, but must not be involved in directly handling cardholder data.

For businesses using payment devices and processes that rely on the public telephone system (PSTN), HPE ProLiant Easy Connect is out of the loop for credit card processing and, therefore, out of scope for PCI-DSS compliance.

The annex, Separation of network and payment processing, shows how HPE ProLiant Easy Connect can be deployed into a PCI-DSS compliant business without introducing it as an additional in-scope system.

Many modern payment processing relies on internet technology, such as IP-POS PDQ devices that connect over a secure IP connection, rather than PSTN, to the payment processor, or a secure web portal connecting to the payment processor.

The annex, Using IP devices and web payment portals, shows how HPE ProLiant Easy Connect can further assist with PCI-DSS compliance by using its network functions to securely separate payment and office data on the network, supporting modern IP-POS terminals and payment portals running on client devices.

Table 1. Annex—PCI-DSS Matrix of Responsibility.

PCI-DSS requirement	HPE ProLiant Easy Connect responsibility	Customer responsibility	AWS responsibility
Requirement 1 Install and maintain a firewall configuration to protect cardholder data	**Cloud management system** HPE ProLiant Easy Connect team maintains all firewall configuration and network segmentation within the cloud management system using published AWS APIs. **On-premises servers** HPE ProLiant Easy Connect team maintains instance isolation of host operating systems and the hypervisor. HPE ProLiant Easy Connect will implement VLAN configuration as requested by the customer to support the required network segmentation.	**On-premises servers** The customer maintains virtual firewall software and all firewall rules enforced by the software. The customer provides the VLAN segmentation requirements to HPE ProLiant Easy Connect to support the required network segmentation.	**Cloud management system** AWS maintains instance isolation for host operating systems and the AWS management environment including host operating system, hypervisor, firewall configuration, and baseline firewall rules. AWS meets all requirements for implementing and managing firewalls for the AWS management environment. Amazon EC2 and Amazon ECS: Amazon VPC Security Groups and network ACLs implement stateful inspection network access control and are suitable for compliant network segmentation.
Requirement 2 Do not use vendor-supplied defaults for system passwords and other security parameters	**Cloud management system** HPE ProLiant Easy Connect team develops and maintains configuration and hardening standards for all virtual machines (VMs) that comprise the cloud management system, including ensuring that supplier-provided default credentials are not used. **On-premises server** HPE ProLiant Easy Connect team develops and maintains configuration and hardening standards for the hypervisor and all HPE provided VMs that comprise the on-premises server, including ensuring that supplier-provided default credentials are not used.	**On-premises server** The customer develops and maintains configuration and hardening standards for all custom VMs hosted on the HPE ProLiant Easy Connect on-premises server, including ensuring that supplier-provided default credentials are not used.	**Cloud management system** AWS develops and maintains configuration and hardening standards for the AWS management environment that provides the virtualization technologies and applications for providing the cloud services. AWS maintains configuration and hardening standards for the underlying operating systems and platforms for these services.
Requirement 3 Protect stored cardholder data	**Cloud management system** HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data. **On-premises server** HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data.	**Cloud management system** The customer is responsible for alerting HPE ProLiant Easy Connect to any potential leakage of cardholder data into the cloud management system. **On-premises server** The customer is responsible for ensuring that any storage of cardholder data is strongly encrypted on any of the custom VMs configured for the on-premises server. Encryption keys are not to be made available to the HPE ProLiant Easy Connect team.	**Cloud management system** AWS is not responsible for any capture, storage, processing, or transmission of cardholder data.
Requirement 4 Encrypt transmission of cardholder data across open, public networks	**Cloud management system** HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data. **On-premises server** HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data.	**On-premises server** The customer is responsible for ensuring all transmission of cardholder data from custom VMs is strongly encrypted before it is transmitted from any virtual network port within the custom VM. The customer is responsible for the management of any encryption keys used for the transmission of cardholder data. Encryption keys are not to be made available to the HPE ProLiant Easy Connect team.	**Cloud management systems** AWS is not responsible for any capture, storage, processing, or transmission of cardholder data.

PCI-DSS requirement	HPE ProLiant Easy Connect responsibility	Customer responsibility	AWS responsibility
Requirement 5 Protect all systems against malware and regularly update antivirus software or programs	**Cloud management system** HPE ProLiant Easy Connect manages antimalware software for all HPE provided VMs that comprise the cloud management system. **On-premises server** HPE ProLiant Easy Connect manages antimalware software for all HPE provided VMs that comprise the on-premises server.	**On-premises server** The customer is responsible for the management of antimalware software for all custom VMs hosted on the on-premises server.	**Cloud management system** AWS manages antivirus software for the AWS management environment and, where appropriate, for identified services.
Requirement 6 Develop and maintain secure systems and applications	**Cloud management system** HPE ProLiant Easy Connect team maintains security-patching, development, and change control of all HPE provided VMs that comprise the cloud management system including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. HPE ProLiant Easy Connect team develops and manages changes of all HPE provided VMs that comprise the cloud management System including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. HPE ProLiant Easy Connect complies with all requirements for secure development and testing for all provided VMs that comprise the cloud management system. **On-premises server** HPE ProLiant Easy Connect team maintains security-patching, development, and change control of all HPE provided VMs that comprise the on-premises server including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. HPE ProLiant Easy Connect team develops and manages changes to all HPE provided VMs that comprise the on-premises server including web interfaces, APIs, access controls, provisioning, and deployment mechanisms.	**On-premises server** The customer is responsible for maintaining security-patching, development, and change control of all custom VMs that are hosted on the on-premises server including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. The customer is responsible for developing and managing changes to all custom VMs that are hosted on the on-premises server including web interfaces, APIs, access controls, provisioning, and deployment mechanisms.	**Cloud management system** AWS maintains security-patching, development, and change control of the applications that support the services utilized by the cloud management system including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. AWS develops and manages changes to applications that support the services utilized by the cloud management system including web interfaces, APIs, access controls, provisioning, and deployment mechanisms.
Requirement 7 Restrict access to cardholder data by business need to know	**Cloud management system** HPE ProLiant Easy Connect implements policies and procedures in order to manage all logical access control within the cloud management system in-line with PCI-DSS requirements. **On-premises server** HPE ProLiant Easy Connect implements policies and procedures in order to manage all logical access control to HPE provided VMs within the on-premises server in line with PCI-DSS requirements.	**On-premises server** The customer is responsible for access control of all custom VMs hosted on the on-premises server.	**Cloud management system** AWS is not responsible for any capture, storage, processing, or transmission of cardholder data. AWS maintains the access controls related to the underlying infrastructure systems and the AWS environment.

PCI-DSS requirement	HPE ProLiant Easy Connect responsibility	Customer responsibility	AWS responsibility
Requirement 8 Identify and authenticate access to system components	**Cloud management system** HPE ProLiant Easy Connect implements policies and procedures in order to manage all logical access control within the cloud management system in-line with PCI-DSS requirements. HPE ProLiant Easy Connect utilizes AWS-provided access control and MFA to secure access to AWS management functions. Access to HPE ProLiant Easy Connect provided VMs is via VPN. AD operator credentials with MFA are required to establish a VPN connection. AD operator credentials are required for operator access to all web-based management UI within the cloud management system. Separate AD administrative credentials are required to access all administrative functions of web-based management UIs and OS level access within the cloud management system. Passphrase-protected SSH certificates are used to control OS access to Linux®-based HPE ProLiant Easy Connect provided VMs. **On-premises server** HPE ProLiant Easy Connect provides AD-based access control to the HPE provided VM OSs comprising the on-premises server. AD-based access control is also used to authenticate users to web-based UIs provided by the on-premises server.	**On-premises server** The customer is responsible for Access Control of all custom VMs hosted on the on-premises server.	**Cloud management system** AWS provides each user in the AWS management environment a unique ID. AWS provides additional security options that enable its customers to further protect their AWS account and control access—AWS Identity and Access Management (AWS IAM), Multi-Factor Authentication (MFA), and Key Rotation.
Requirement 9 Restrict physical access to cardholder data	**Cloud management system** The HPE ProLiant Easy Connect team has no control over the physical security of the cloud management system as they are installed in locations owned and managed by the customer. HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data. HPE ProLiant Easy Connect does not operate any POS/POI devices. **On-premises server** The HPE ProLiant Easy Connect team has no control over the physical security of the on-premises server as they are installed in locations owned and managed by the customer. HPE ProLiant Easy Connect is not responsible for any capture, storage, processing, or transmission of cardholder data. HPE ProLiant Easy Connect does not operate any POS/POI devices.	**On-premises server** The customer is responsible for the physical security of the on-premises server. The Customer is responsible for all capture, storage, processing, and/or transmission of cardholder data. The customer is responsible for any POS/POI devices.	**Cloud management system** AWS maintains the physical security and media handling controls of all services used by the cloud management system.

PCI-DSS requirement	HPE ProLiant Easy Connect responsibility	Customer responsibility	AWS responsibility
Requirement 10 Track and monitor all access to network resources and cardholder data	**Cloud management system** HPE ProLiant Easy Connect team maintains and monitors audit logs for all HPE provided VMs and AWS resource management that comprise the cloud management system. HPE ProLiant Easy Connect team maintains time synchronization for all HPE provided VMs that comprise the cloud management system using AWS NTP servers. HPE ProLiant Easy Connect monitors the filesystem for unauthorized changes to critical system files on all HPE provided VMs within the cloud management system. **On-premises server** HPE ProLiant Easy Connect team maintains and monitors audit logs for all HPE provided VMs that comprise the on-site appliance. HPE ProLiant Easy Connect team maintains and monitors audit logs for all HPE provided VMs and AWS resources that comprise the on-premises server. HPE ProLiant Easy Connect team maintains time synchronization for all HPE provided VMs that comprise the on-premises server using customer NTP servers. HPE ProLiant Easy Connect monitors the filesystem for unauthorized changes to critical system files on all HPE provided VMs within the on-premises server.	**On-premises server** The customer is responsible for monitoring audit logs on custom VMs hosted on the on-premises server. The customer is responsible for maintaining time synchronization for all custom VMs on the on-premises server. The customer to provide NTP time source for HPE ProLiant Easy Connect provided VMs within the on-premises server. The Customer is responsible for monitoring the filesystem for unauthorized changes to critical system files on all custom VMs within the on-premises server.	**Cloud management system** AWS maintains and monitors audit logs for the AWS management environment and AWS service infrastructure.
Requirement 11 Regularly test security systems and processes	**Cloud management system** HPE ProLiant Easy Connect manages vulnerability scanning, penetration testing, segmentation testing, intrusion detection, and file integrity monitoring of all VMs that comprise the cloud management system. **On-premises server** HPE ProLiant Easy Connect conducts vulnerability assessments of all HPE provided VMs prior to releasing the software. HPE ProLiant Easy Connect provides intrusion detection and file integrity monitoring for all HPE provided VMs that comprise the on-premises server.	**On-premises server** The customer is responsible for vulnerability assessments, penetration testing, and segmentation testing of all on-premises servers once in operation. The customer is responsible for intrusion detection and file integrity monitoring of all custom VMs that are hosted on the on-premises server.	**Cloud management system** AWS manages rogue wireless access point detection, vulnerability, and penetration testing, intrusion detection and file integrity monitoring for the AWS management environment for all AWS services utilized by the cloud management system. AWS implements and monitors IDS/IPS on networks that implement AWS services used by the cloud management system.
Requirement 12 Maintain a policy that addresses information security for all personnel	**Cloud management system** HPE ProLiant Easy Connect team maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI-DSS requirements for all HPE staff that develop, maintain, or operate the cloud management system. **On-premises server** HPE ProLiant Easy Connect team maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI-DSS requirements for all HPE staff that develop, maintain, or operate the HPE provided VMs and the on-premises server.	**On-premises server** It is the customer's responsibility to address this requirement to all customer personnel who have access to the cloud management system and the web interfaces of the HPE ProLiant Easy Connect on-premises server.	**Cloud management system** AWS maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI requirements.

PCI-DSS requirement	HPE ProLiant Easy Connect responsibility	Customer responsibility	AWS responsibility
Appendix A1 Additional PCI-DSS requirements for shared hosting providers	**Cloud management system** The HPE ProLiant Easy Connect cloud management system is dedicated for the customer's use only. It is not multitenant. **On-premises server** All on-premises servers are dedicated for the customer's use only.	N/A	**Cloud management system** AWS customer instances and data are protected by instance isolation and other security measures in the AWS management environment.
Appendix A2 Additional PCI-DSS requirements for entities using SSL/early TLS	**Cloud management system** HPE ProLiant Easy Connect encrypts access and manages transmission encryption both to/from and within the cloud management System using TLS 1.2 or greater. **On-premises server** HPE ProLiant Easy Connect encrypts access and manages transmission to/from and between HPE provided VMs using TLS 1.2 or greater.	**On-premises server** The customer is responsible for any risk mitigation plan for the use of broken encryption algorithms used on custom VMs hosted on the on-premises server.	**Cloud management system** AWS encrypts access and manages transmission encryption within the AWS Management Environment using TLS 1.1 or greater.

Annex—Separation of network and payment processing

In many cases, merchants make use of secure point of sale payment terminals that provide encrypted transactions between the customer and the payment processor. Because the payment data never resides on the store's server, HPE ProLiant Easy Connect is out of scope for PCI-DSS auditing as it never handles restricted cardholder information.

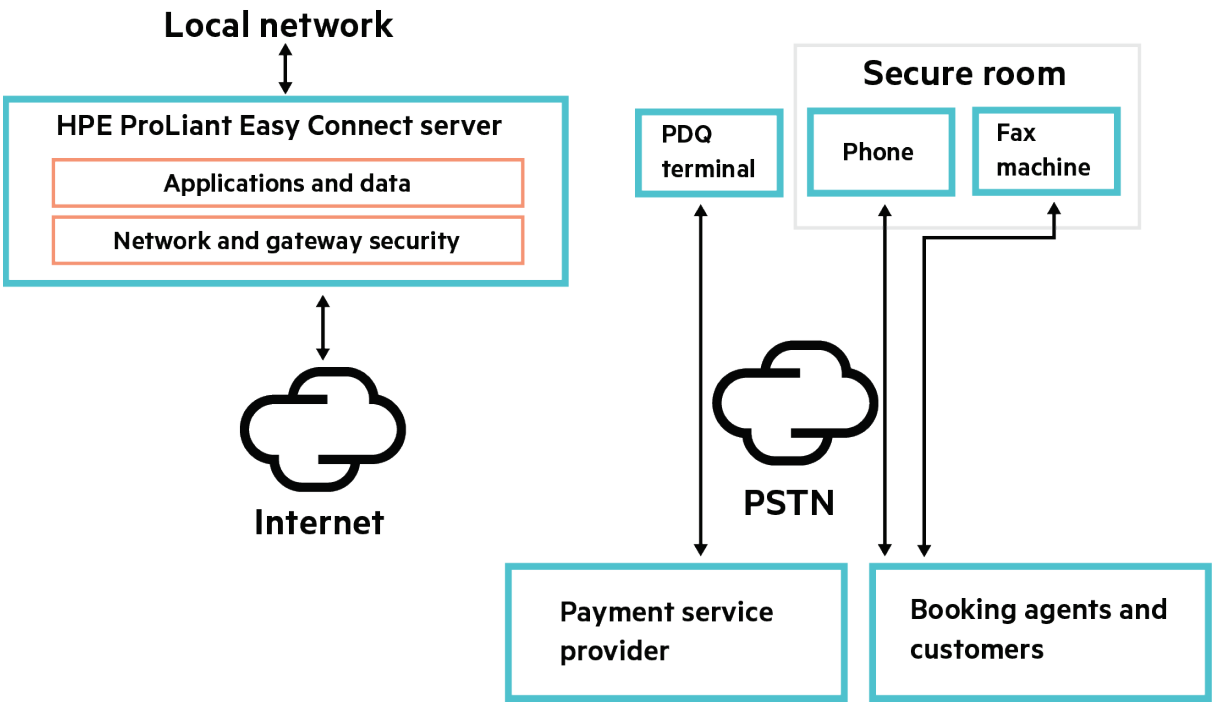

Figure 1. Separation of network and payment processing

In this environment, a PCI-approved PDQ terminal is connected to the PSTN network, avoiding any card transmission and processing taking place via the LAN and internet gateway services supported by HPE ProLiant Easy Connect.

Inbound orders from the customers, carrying credit card information, are via phone and fax, again over the PSTN network. Paper records of faxes and PDQ receipts are stored in a secure room.

The HPE ProLiant Easy Connect server and the LAN remain out of scope providing:

- PDQ machines must be hard wired to the PSTN network.
- Phone and fax are both hardwired to the PSTN network. In this environment, they must not be supported by VoIP services using the internet connection via the HPE ProLiant Easy Connect's internet gateway. Similarly, soft faxes via internet services or email should not be used.
- Cardholder data should not be copied electronically onto the server's file system nor onto other networked devices.

Note that it is acceptable to hold a subset of card, customer, and transaction data on the server provided it is limited to:

- The customer name
- The transaction value
- The transaction ID
- The first six and the last four digits of the credit card number

This information is often used for billing records, processing refunds, processing chargebacks, and business intelligence reporting. If handled according to PCI-DSS guidelines, storing or processing this data on the HPE ProLiant Easy Connect server will not result in the appliance being considered in scope for compliance assessment.

Assuming the PDQ devices are on the approved list, and the correct business process and staff training has been carried out, this IT environment is a good candidate for achieving PCI-DSS compliance.

Annex—Using IP devices and web payment portals

The HPE ProLiant Easy Connect server typically serves as the internet or WAN gateway for the retail site processing payment, therefore, the LAN and security configuration of the appliance should be carefully considered to ensure PCI-DSS compliance is maintained.

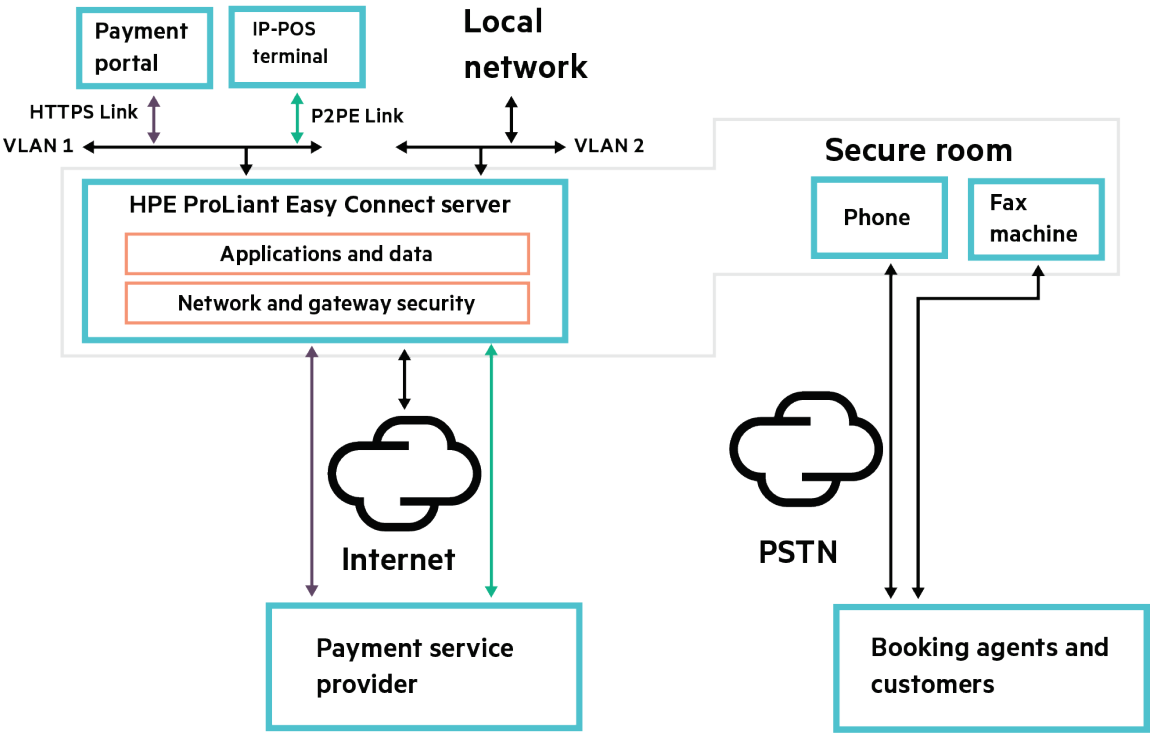

Figure 2. Using IP devices and web payment portals

Maintaining compliance is significantly helped by using approved IP-POS PDQ devices. These will use point-to-point encryption (P2PE) between the device and the payment processor, ensuring cardholder data cannot be intercepted on either the LAN or public internet.

Payment portals require staff to log on to a secure payment processing page, via a workstation, laptop, or other terminal. This connection should always be made using HTTPS secured connections. HTTPS will, again, ensure cardholder data cannot be intercepted on either the LAN or public internet.

As a further precaution, it is a good practice to connect payment devices, including PDQ devices and workstations, to a separate network to other office and public IT resources. HPE ProLiant Easy Connect can support the creation of two or more VLANs, ensuring packet data from payment processing devices cannot be seen by devices connected to other VLANs.

When using IP-based payment processing, PCI-DSS compliance assessment may require vulnerability scanning of the network perimeter. Scanning automatically analyzes network and software for vulnerabilities.

The keep-current service from HPE ProLiant Easy Connect updates and patches core IT services on the server to assist in maintaining conformance. If a third-party firewall is deployed in the store, the retailer should ensure this is also kept up to date with the latest firmware and software updates.

Learn more at

knowledge.prolianteasyconnect

Share with colleagues

a00027505ENW, October 2017