ZYNSTRA TECHNICAL BRIEFING NOTE

Deploying Zynstra in a PCI-DSS Compliant IT Environment

Introduction

This document identifies how Zynstra should be deployed in to a PCI-DSS Version 3.0 compliant IT environment.

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

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

The Importance of Compliance

PCI-DSS, the Payment Card Industry Data Security Standard, is a security standard for businesses that mandates compliance for any merchants who store, process or transmit credit card data, including cardholder information. The 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 merchants acquiring Bank

Failure to achieve formal compliance, or a card data breach, can result in substantial fines being levied 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.

Reducing PCI-DSS Compliance Effort

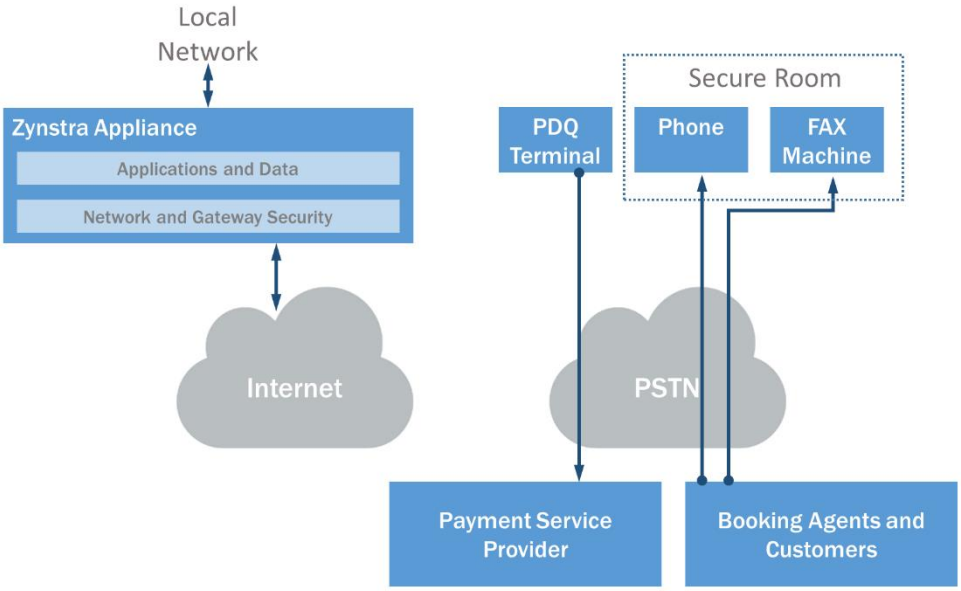
One of the most efficient ways to maintain PCI-DSS compliance is to minimize the number of IT resources that are 'in scope'.

Any systems that store, process 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 businesses' compliance effort and accelerate the compliance assessment process.

Separation of Network and Payment Processing

It is entirely possible to deploy Zynstra in to a PCI-DSS compliant business without introducing it as an additional in-scope system. For businesses using payment devices and processes that rely on the public telephone system (PSTN) the Zynstra appliance is out-of-the-loop for credit card processing and therefore out-of-scope for PCI-DSS compliance.



In this environment, a PCI approved PDQ device is connected to the PSTN network, avoiding any card transmission and processing taking place via the LAN and Internet gateway services supported by Zynstra.

In-bound orders from 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 Zynstra appliance 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 Zynstra's Internet gateway. Similarly 'soft faxes' via Internet services or email should not be used.
- Cardholder data should not be copied electronically on to Zynstra's file system nor on to other networked devices.

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

- The customer name
- The transaction value
- The transaction ID
- The first 6 and the last 4 digits of the credit card number

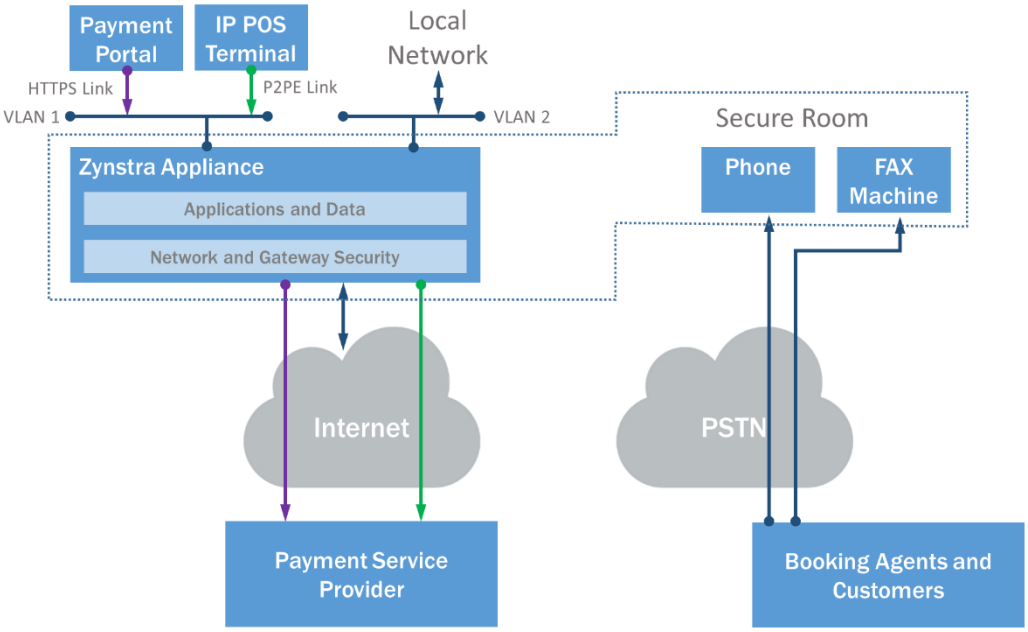
This information is often used for billing records, processing refunds, processing chargebacks and business intelligence reporting. If handled according to PCI-DSS guidelines, storing or processing this data on the Zynstra appliance will not result in the appliance being considered in-scope for compliance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

Using IP Devices and Web Payment Portals

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 Zynstra appliance typically serves as the Internet gateway for the site processing payment therefore the LAN and security configuration of the appliance should be carefully considered to ensure PCI-DSS compliance is maintained.



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 logon 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 good practice to connect payment devices, including PDQ devices and workstations, to a separate network to other office and public IT resources. Zynstra 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 analyses network and software for vulnerabilities. Zynstra's keep-current service updates and patches core IT services on the appliance to assist in maintaining conformance. A correctly configured firewall, part of the Zynstra appliances security gateway, in addition to the recommended use of VLANs, also contribute to network security compliance.

Avoiding Cardholder Data Contamination

Zynstra's appliance provides on premise file storage and private-cloud services, running applications within a number of virtual machines. As a result, organizations must be careful not to contaminate these data stores and applications with cardholder data.

Business process, polices and staff training are the first line of defense, ensuring individuals are aware of the limited number of situation that storing cardholder data is permitted and the proper storage location, namely a secure room.

Cardholder data contamination can come for other sources:

Emails from customers. The Zynstra appliance may be configured to host a local instance of Microsoft Exchange or other email services. Generally, merchants should not accept cardholder details via email as it is inherently insecure. If however a customer does send an email containing this data, staff should be aware that the email must be deleted and the customer requested to phone-in the details instead.

Legacy applications. Organizations must avoid deploying applications in to the appliance's private cloud that may collect cardholder data or bring cardholder data over when ported from their old server.

A recommended precaution against data contamination is to regularly run 3rd party cardholder data scanning software on the network and Zynstra appliance. These can identify data that appears to hold cardholder data that may have found its way on to the system. Such data should then be securely deleted and processes and policies reviewed to mitigate the risk of the contamination being repeated in future.

Additional Benefits

While the organization's primary concern regarding PCI-DSS should be minimizing systems that are in-scope, it is reassuring to know that Zynstra offers consistent, enterprise class security and monitoring across all sites, no matter their size.

This offers a number of benefits:

- Enterprise-quality firewall, and internet gateway software is deployed on each appliance to meet requirements for resisting penetration scanning.
- Consistency of server, security and software architecture across all offices and retail sites, reducing compliance auditing effort and complexity.
- Zynstra's Keep-Current service ensures server operating systems and security software is patched and updated as mandated by the PCI-DSS.
- The appliance security is managed by Zynstra, removing the need to distribute privileged access rights to large numbers of staff, further reducing security risks and training effort.

For further details about Zynstra's security gateway capabilities, please refer to the *Zynstra Technical Briefing Note - Security and Internet Gateway.*