riverbed®

TECHNOLOGY ANALYSIS

PCI DSS compliance in cloud environments

Requirement 6.6: Application Firewalls

The evolving cloud security landscape

PCI DSS is a pragmatic set of best practices and security measures that any organization must follow if they accept and handle cardholder data online. The standard encompasses network security, data protection, data encryption, system security, access control, ongoing monitoring and testing and security policy development.

As the world moves more towards cloud computing, there are evolving cloud service providers such as Layered Tech[1] with expertise in the specific challenges associated with credit card processing in the cloud, choosing to specialize in providing PCI compliant hosting. Other providers, such as Amazon[2], provide more general cloud services, but are nevertheless validated as a Level 1 service provider for PCI DSS. The evidence for a growing market need for PCI compliant cloud hosting is compelling.

PCI participating organizations selected cloud computing as a key area requiring additional guidance and clarification. In February 2013, the PCI Security Standards Council released an information supplement to the PCI DSS requirements to fulfill this need: *PCI DSS Cloud Computing Guidelines*[3]. These guidelines help merchants to understand the challenges involved when deploying payment processing systems in the cloud, and outline what needs to be considered so that they achieve PCI DSS compliance in this environment.

CSP: Cloud service provider

PCI: Payment Card Industry

PCI DSS: PCI Data Security Standard, a statement of best practices and security measures for organizations handling cardholder data.

PCI SSC: PCI Security Standards Council, an industry standard group that, amongst other activities, promotes the PCI DSS.

Particular concerns in a cloud environment

Cloud service providers (CSPs) vary widely in their understanding of payment card security and the services they offer that support it. The new guidance identifies a number of issues needing to be understood when selecting a CSP.

Control and responsibility

The most important factor when implementing cloud computing in a PCI environment is the knowledge of who is responsible for which parts of the PCI requirements, and how the CSP and merchant can work together to ensure that they are addressed appropriately. For example, a merchant might create and maintain a security policy, but require the CSP to configure the service.

API

In order for the best value to be obtained from deployment of cloud services, automation is key. Quick provisioning, configuration, maintenance and monitoring relies on appropriate APIs being available for all infrastructure components.

Segmentation

The major barrier to PCI compliance in the cloud is ensuring adequate segmentation between different merchants using the CSP. Whilst

[1] http://www.layeredtech.com/cloud-services
[2] https://aws.amazon.com/security
[3] https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

some CSPs provide excellent segmentation, others provide only a shared service for parts of their infrastructure.

Logging and the right to audit

In order to achieve PCI DSS compliance, full logs are required, including audit trails for all levels of infrastructure. These logs must not expose log entries from other entities on any shared infrastructure, but must be complete as far as the cloud customer needing PCI compliance is concerned.

The Riverbed solution

Riverbed's Stingray Application Firewall is used to satisfy PCI DSS requirement 6.6 for an Application Firewall, providing peace of mind at the application layer in both cloud and physical deployments.

Suitability for cloud architectures

Stingray Application Firewall was designed from the ground up using a modular software architecture, with large deployments in mind. It scales in the same way that cloud services do, fitting in with application needs as they grow and shrink.

A modern RESTful API provides immediate control, allowing automation and orchestration—meaning more efficient management and faster time to market.

Keeping control

As a pure software product, Stingray Application Firewall can be used directly by a merchant in the cloud environment itself. This allows merchants a choice over who has control of a service: when a CSP's application firewall offering does not satisfy PCI DSS requirements, the merchant can still achieve compliance by deploying Stingray Application Firewall as a component of their own cloud infrastructure. This maintains the required segmentation and log access, thus satisfying PCI DSS requirement 6.6.

Further Information

You can find out more about Stingray Application Firewall by visiting our web site:

http://www.riverbed.com/products-solutions/products/application-delivery-stingray/Stingray-Application-Firewall.html

Read more

Review the PCI DSS Quick Reference Guide, at https://www.pcisecuritystandards.org/documents/PCI SSC Quick Reference Guide.pdf

PCI DSS Quick Reference Guide

Understanding the Payment Card Industry Data Security Standard version 2.0

For merchants and entities that store, process or transmit cardholder data

Contents

ABOUT RIVERBED

Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize, and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization. Additional information about Riverbed (NASDAQ: RVBD) is available at www.riverbed.com

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell. RG42 1NG
United Kingdom
Tel: +44 1344 31 7100

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990