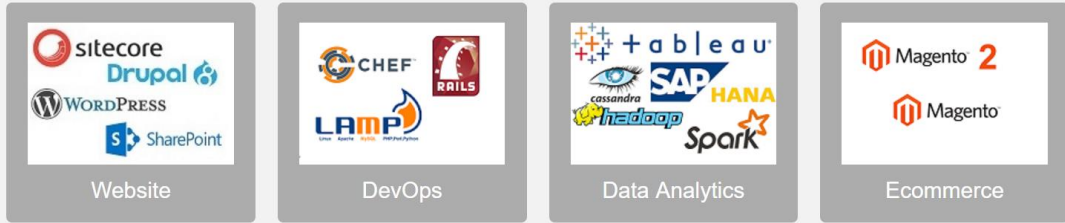


Build your stack in minutes. We will armor it for you.

1 Select Workload 2 Describe Workload 3 Configure Environment 4 Review Cost 5 Submit Request 6 Build Info.

Step 1. Click icon for Free Estimate



SECURED HOSTING OF A PCI DSS COMPLIANT WEB APPLICATION ON AWS

White Paper

This document is provided for informational purposes only. Readers are responsible for making their own independent assessment of the information in this document and any use of products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances.

stackArmor AWS Solutions Team

Contents

Abstract	3
What is PCI DSS?	3
Key objectives of PCI DSS	3
PCI DSS Requirements.....	3
Secured hosting on AWS and PCI DSS Compliance	4
Architecting for PCI-DSS Compliance on AWS	Error! Bookmark not defined.
Jumpstart your PCI DSS compliant Web application in AWS	5
About stackArmor	7
References	8

Abstract

Protecting card owner information has become very important for e-commerce companies as they have become frequent targets for hackers. In order to safeguard the interests of the card owners, four industry majors, VISA, MasterCard, Discover and American Express, joined hands to create a set of policies and procedures to protect the debit, credit and cash card transactions and to safeguard the personal information of the cardholders. These policies and procedures are collectively known as the Payment Card Industry Data Security Standard (PCI DSS). In simple terms these standards alert companies that they are wholly responsible for the credit card information of their customers. The PCI directs companies to use the information diligently and to store only that information that is required for their business. This white paper provides an overview of architectural features in the AWS cloud that ensure the hosting of e-commerce web applications that are PCI DSS compliant.

What is PCI DSS?

The PCI DSS consists of a set of 12 directives that set industry standards for all companies who directly or indirectly process credit card information.

Key objectives of PCI DSS

Some of the key objectives of the PCI DSS are:

- Build and maintain a safe and secured network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks for any malicious activity
- Maintain an information security policy

PCI DSS Requirements

PCI DSS has development a set of 12 requirements. Any system or application that intends to use the credit card information must ensure strict compliance to these requirements. The scope of PCI DSS requirements include:

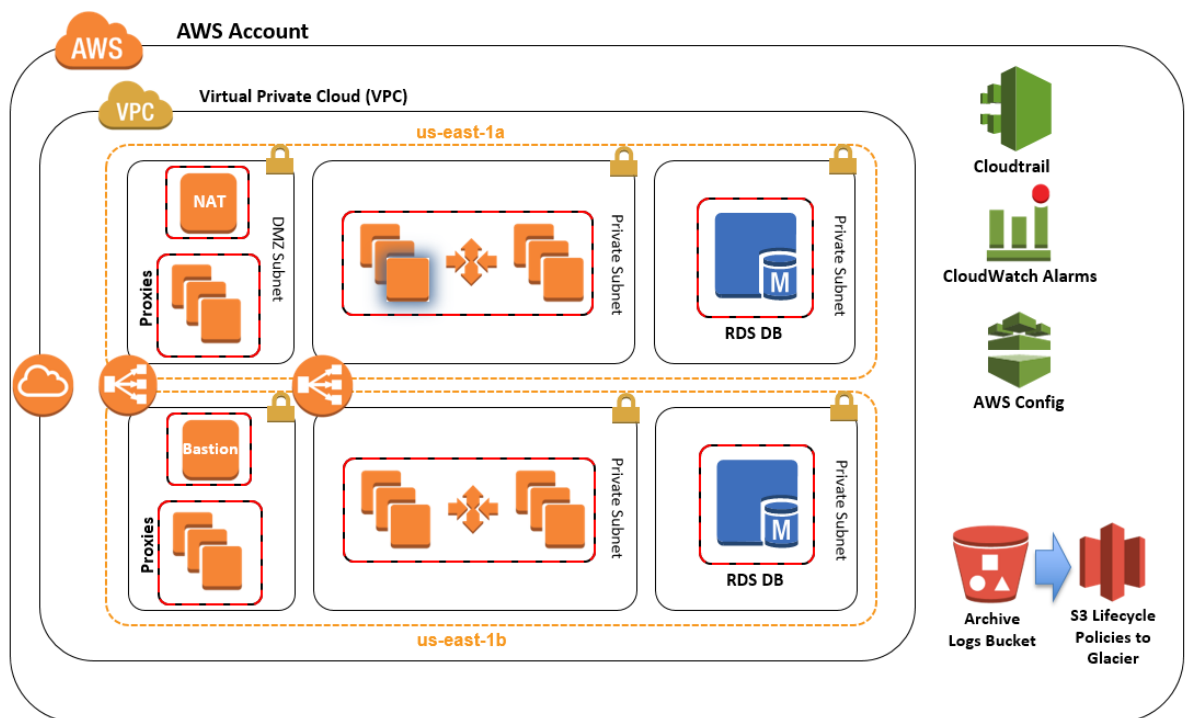
- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Protect all systems against malware and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need to know
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

Secured hosting on AWS and PCI DSS Compliance

Amazon Web Services (AWS) provides a secure, elastic and compliant hosting environment with the requisite tools to ensure PCI-DSS compliance. The architectural blueprint for hosting applications and data in AWS includes:

1. Basic AWS identity and Access management configuration with custom IAM policies with associated groups, roles and instance policies.
2. Amazon Virtual Private Cloud multi A-Z architecture with separate subnets for different application tiers and private subnets for application and database.
3. Amazon simple storage service (Amazon S3) buckets for encrypted web content, logging and backup data.
4. Standard Amazon Virtual Private Cloud security groups for Amazon Elastic compute cloud instances and load balances used in the sample application stack
5. 3-tier Linux web application using Auto Scaling and Elastic Load balancing, which can be modified and /or boot strapped with customer applications
6. A secured bastion login host to facilitate command line secure shell access to Amazon EC2 instances for troubleshooting and systems administration activities.
7. Encrypted, Multi - AZ Amazon Relational Database service (Amazon RDS) MySQL database.
8. Logging, monitoring and alerts using AWS Cloud Trail, Amazon Cloud watch and AWS configuration rules.

The diagram below provides an overview of the architecture and solution elements for a PCI-DSS hosting environment on AWS.



Build your stack in minutes. We will armor it for you.

- 1 Select Workload
- 2 Describe Workload
- 3 Configure Environment
- 4 Review Cost
- 5 Submit Request
- 6 Build Info.

Jumpstart your PCI DSS compliant Web application in AWS

StackBuilder™ is an easy to use cloud app store front that allows users to quickly select and operate an AWS cloud hosted website, dev & test, data analytics or ecommerce service. The StackBuilder™ cloud app store allows users to quickly deploy and use their PCI DSS compliant e-commerce website hosted on AWS. StackBuilder’s intelligent cloud deployment engine takes care of instance selection, AWS VPC configuration and software installation.

In order to get started with Magento e-commerce website on AWS application go to <https://stackbuilder.stackarmor.com>

Step 1: Select E-commerce as the workload profile and click Next

Build your stack in minutes. We will armor it for you.

- 1 Select Workload
- 2 Describe Workload
- 3 Configure Environment
- 4 Review Cost
- 5 Submit Request
- 6 Build Info.

Step 1. Click icon for Free Estimate

Step 2: Describe the workload environment in terms of size, security by industry and management model

Build your stack in minutes. We will armor it for you.

- 1 Select Workload
- 2 Describe Workload
- 3 Configure Environment
- 4 Review Cost
- 5 Submit Request
- 6 Build Info.

Step 2. Describe your Workload

Step 3: Configure environment by selecting stack – PCI DSS Web App

stackArmor stackBuilder^{Beta}

Build your stack in minutes. We will armor it for you.

1 Select Workload 2 Describe Workload 3 Configure Environment 4 Review Cost 5 Submit Request 6 Build Info.

Build your stack in minutes. We will armor it for you.

1 Select Workload 2 Describe Workload 3 Configure Environment 4 Review Cost 5 Submit Request 6 Build Info.

Step 3. Configure your Environment

Previous Step

Select your Stack

PCI-DSS Web App

Stack Description:

Deploys a Wordpress sample application in a PCI-DSS (Payment Card Industry Data Security Standard) compliant environment.

Next Step

Step 4: Review Hosting Cost inclusive of software and maintenance fees

stackArmor stackBuilder^{Beta}

Build your stack in minutes. We will armor it for you.

1 Select Workload 2 Describe Workload 3 Configure Environment 4 Review Cost 5 Submit Request 6 Build Info.

Step 4. Review Estimated Cost

Previous Step

Select your utilization

Specify run time

- High - 100% utilization
- Medium - Mainly business hours
- Low - Light day time usage only

Step 5: Fill out form and submit request to provision environment. Once, the environment has been provisioned you will get an email with the access URL and a User Name & Password.

stackArmor stackBuilder^{Beta}

Build your stack in minutes. We will armor it for you.

1 Select Workload 2 Describe Workload 3 Configure Environment 4 Review Cost 5 Submit Request 6 Build Info.

Step 5. Get Free Quote

Fill out the form below to receive a no-obligation detailed specification for your customized cloud environment. All fields are required.

First name

Job title

Phone number

By checking this checkbox, I agree to [Term of Services](#).

Last name

Organization / Employer

Email address

Yes, send risk-free quote

Please Note: We will use your submitted information to send you a detailed specification and price quote for your customized cloud environment.

Step 6: Login into the e-commerce application

Build your stack in minutes. We will armor it for you.

- 1 Select Workload
- 2 Describe Workload
- 3 Configure Environment
- 4 Review Cost
- 5 Submit Request
- 6 Build Info.

Build your stack in minutes. We will armor it for you.


- 1 Select Workload
- 2 Describe Workload
- 3 Configure Environment
- 4 Review Cost
- 5 Submit Request
- 6 Build Info.

You will receive an email with login instructions.


Please Note: Your reference number is 076fa4d9-1fa9-4c37-980c-daa19993d5ff. It may take from half an hour up to 4 hours for the job to finish. If you do not get an email within a day please contact us at solutions@stackArmor.com for support.

Visit www.stackArmor.com for information on our Cloud Solutions and Services.

Step 7: You have now successfully launched the standardised architecture for PCI DSS







Welcome to stackArmor StackBuilder!



You have successfully launched the **Standardized Architecture for PCI on the AWS Cloud**

What Now?

-  StackBuilder installs a sample WordPress application that you can [configure](#). The PCI DSS compliant hosting environment incorporates security best practices and provides a consumable environment for your applications. Other applications can easily be added to this environment.
-  View the [Security Control Matrix](#) that maps the specific AWS security controls to the PCI DSS requirements.
-  If you need further assistance, please contact [stackArmor Support](#).



Architecture

StackBuilder created an architecture in your account similar to [this diagram](#). The architecture is:

- **Compliant**
Helps meet compliance requirements specified in the Security Control Matrix
- **Secure**
The system includes security controls that restrict access to resources
- **Elastic**
The instances reside in Auto Scaling Groups that allow them to shrink or grow based on demand
- **Fail-tolerant**
The system is deployed over two Availability Zones to increase availability

About stackArmor

stackArmor is a AWS Certified partner with experienced cybersecurity and AWS solution architects with an experience deploying compliant applications for Healthcare, Financial Services, Public Sector, Department of Defense and Commercial customers including Non-profits. We help customers in the following areas:

- AWS Cloud Architecture and Migration Services
- DevOps and Automation Architecture and Implementation Services
- AWS Managed Services and Cloud Operations
- AWS Value-Added Resale and Hosting Support Services
- Cybersecurity Compliance and Penetration Scanning Services

Additionally, we have an out-of-the-box solution - stackArmor StackBuilder™ is a “Turbo Tax” like wizard for helping application owners quickly configure a fully functional AWS environment. The wizard walks the user through a series of simple questions through a 5 step process. Upon submission



1 Select Workload

2 Describe Workload

3 Configure Environment

4 Review Cost

5 Submit Request

6 Build Info.

of the request, the user is presented with login credentials to a fully configured and operational environment ready to go.

StackBuilder™ has been designed and developed by cloud computing experts who have spent many years implementing secure cloud hosting environments for large security focused organizations such as the US Treasury, Defence, Healthcare, Commercial and Non-profit customers. StackBuilder™ automates the entire provisioning process using an advanced capacity planning and provisioning automation engine that makes it easy for users to leverage the power of the AWS cloud computing platform without having to get into the details of infrastructure estimation, provisioning and software media installation & configuration.

StackBuilder™ provides a rich and easy to use consumer-grade experience for non-technical users to jumpstart their projects by answering a series of simple questions. StackBuilder's intelligent provisioning and capacity estimation engine leverages the rich set of services provided by the AWS cloud platform including wide variety of EC2 instances, Virtual Private Cloud (VPC), Auto Scaling Groups, Clustering and Elastic Load Balancers (ELB) amongst others. The user of StackBuilder™ does not have to go through the various steps associated with configuring and setting up the AWS infrastructure as they are handled automatically. This allows the user to focus on his project without waiting for costly consultants or the need for cloud infrastructure expertise.

Please contact us at solutions@stackarmor.com or call at 888-964-1644.

References

1. <https://aws.amazon.com/about-aws/whats-new/2016/05/pci-dss-standardized-architecture-on-the-aws-cloud-quick-start-reference-deployment/>
2. <https://blogs.aws.amazon.com/security/post/Tx2ZHLDGY0EL8Z1/Now-Available-PCI-DSS-Quick-Start-for-Deploying-PCI-DSS-In-Scope-Workloads>
3. <https://aws.amazon.com/compliance/shared-responsibility-model/>
4. <https://www.coalfire.com/The-Coalfire-Blog/May-2016/AWS-releases-PCI-DSS-Quick-Start-for-Deploying-PCI>
5. https://www.pcisecuritystandards.org/pci_security/
6. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
7. <http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>
8. http://www.theukcardsassociation.org.uk/security/What_is_PCI%20DSS.asp