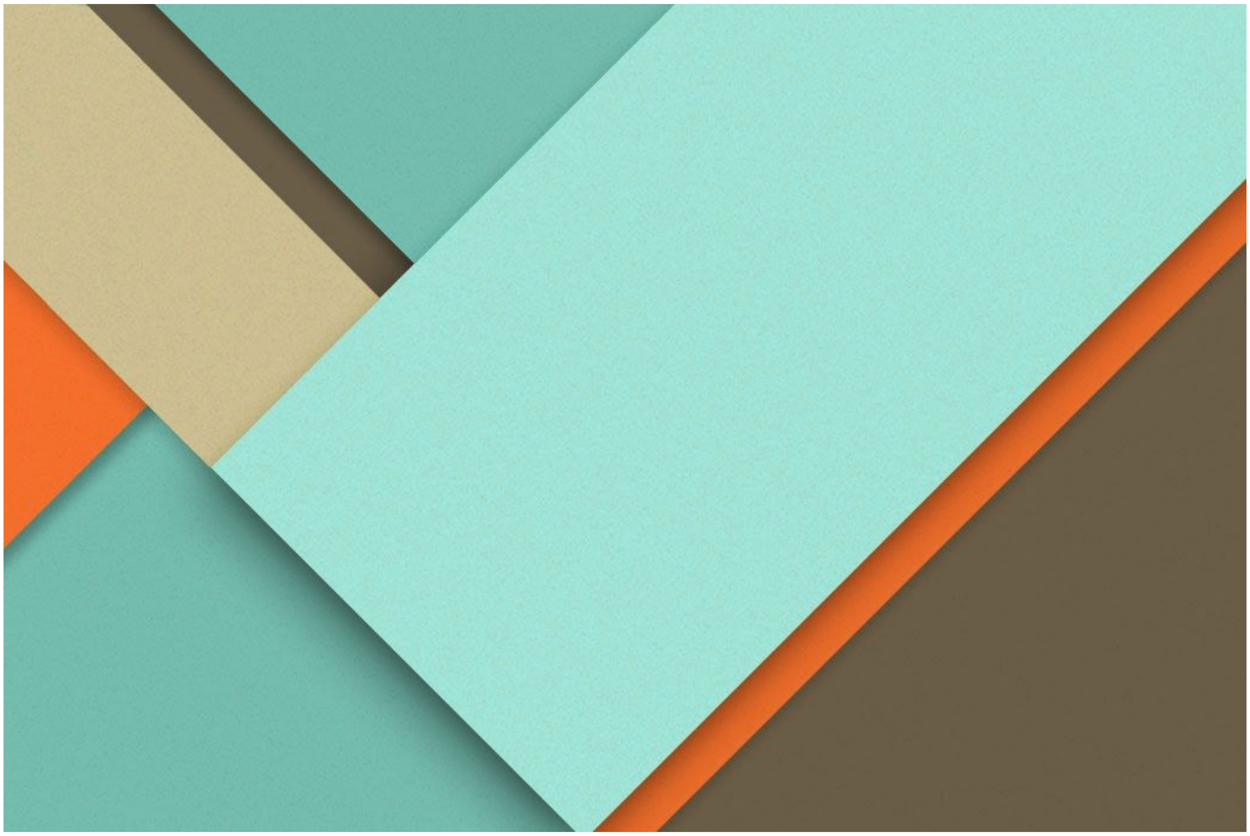

Amazon Inc AWS Architecture

02.06.2020

Overview

Amazon Inc company intends to build an ecommerce application which accepts credit cards as a mode of payment from its users on their platform. This document describes the standardized architecture as far as PCI DSS compliance which ensures the implementation of storing, processing and transmitting credit card information.

PCI DSS Scoping on AWS

The system is designed to conform to the following PCI DSS guidelines:

1. ***Building and maintaining a secure network.*** - Data is secured in the cloud environment by setting a firewall around resources. Data access is secured by using a VPN gateway between the cardholder systems and the out-of-scope systems.

2. ***Protecting the cardholder data*** - PCI data is masked using a non-reversible hash key. Cloudflare's WAF was deployed to scan and secure data transmitted to open, public networks.

3. ***Maintain a vulnerability management program*** - To protect against malware, nessus tool will be used for security scans done weekly in the cloud environment.

4. ***Implement strong access control measures*** - Any access request is authenticated and authorized and their actions are logged for audit trails. Multi-Factor Authentication (MFA) used to reduce reliance on a single password.

5. ***Monitor and test networks*** - Network and application access is monitored and analyzed 24x7 for any issues by Cloud watch.

6. ***Maintain an information security policy*** - Security policies work best when they are succinct and to the point and are created and operationalized to identify roles and responsibilities of each person involved.. These policies are maintained and kept up-to-date based on evolving needs of the business.