



Cheetah Loyalty Security Overview

Features and Best Practices

June 2019



Cheetah Digital, Inc., 72 W Adams St 8th floor, Chicago, IL 60603

Copyright © 2019 Cheetah Digital, Inc.

All rights reserved.

Printed in the United States of America

No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photographic, magnetic, or other record, without the prior agreement and written permission of Cheetah Digital, Inc.

Cheetah Digital, the Cheetah Digital logo, and other Cheetah names referenced herein are trademarks of Cheetah Digital, Inc., and may be registered in certain jurisdictions.

Other product names, designations, logos, and symbols may be trademarks or registered trademarks of their respective owners.

PRODUCT MODULES AND OPTIONS. This guide contains descriptions of modules that are optional and for which you may not have purchased a license. As a result, your software implementation may differ from descriptions in this guide. To find out more about the modules your organization has purchased, see your corporate purchasing agent or your Cheetah Digital sales representative.

U.S. GOVERNMENT RESTRICTED RIGHTS. Programs, Ancillary Programs and Documentation, delivered subject to the Department of Defense Federal Acquisition Regulation Supplement, are “commercial computer software” as set forth in DFARS 227.7202, Commercial Computer Software and Commercial Computer Software Documentation, and as such, any use, duplication and disclosure of the Programs, Ancillary Programs and Documentation shall be subject to the restrictions contained in the applicable Cheetah Digital license agreement. All other use, duplication and disclosure of the Programs, Ancillary Programs and Documentation by the U.S. Government shall be subject to the applicable Cheetah Digital license agreement and the restrictions contained in subsection (c) of FAR 52.227-19, Commercial Computer Software - Restricted Rights (June 1987), or FAR 52.227-14, Rights in Data—General, including Alternate III (June 1987), as applicable. Contractor/licensor is Cheetah Digital, Inc., 72 W Adams St 8th floor, Chicago, IL 60603.

PROPRIETARY INFORMATION NOTICE

Stellar Loyalty, Inc. considers information included in this documentation and all Stellar Loyalty documents to be Confidential Information. Your access to and use of this Confidential Information are subject to the terms and conditions of: (1) the applicable Stellar Loyalty software license agreement, which has been executed and with which you agree to comply; and (2) the proprietary and restricted rights notices included in this documentation.



Contents

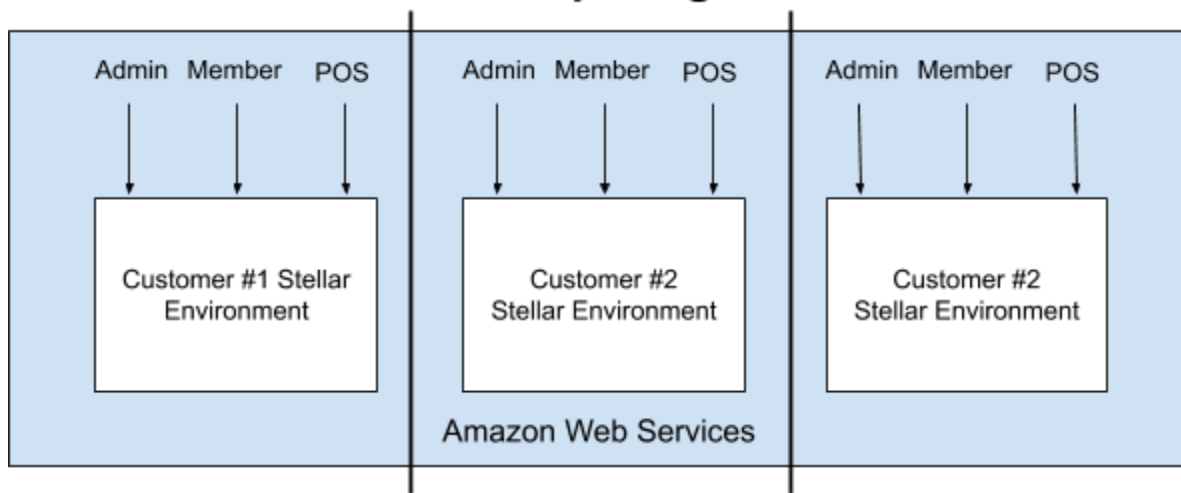
Benefits of the Cheetah Loyalty Cloud	5
Operational Security	6
Application Security	7
Admin Access Control	8
Disaster Recovery	9
Certifications	10
References	11



Introduction

At its core, Cheetah Loyalty uses a single-tenant architecture, which ensures that each Cheetah Loyalty environment is isolated from every other Cheetah Loyalty environment. Physical computing resources are virtualized and may be shared to achieve cost-effective, massive scalability, but physical storage, software, and application processes are never shared among customer environments. In summary, no commingling occurs between any two Cheetah Loyalty environments, including those for the same customer (say for test and production or for different loyalty programs).

Single Tenant Architecture on Shared Computing Resources



Isolated Software, Storage, and Computing



Benefits of the Cheetah Loyalty Cloud

The Cheetah Loyalty Cloud provides unmatched benefits and world-class security unmatched by on premise deployments.

- Operational Cost
 - Lower computing costs via use of commodity clusters
 - All-inclusive installation, upgrades and monitoring
- Elasticity
 - Fine-tune Cheetah Loyalty environment size based on application usage
 - Dynamically increase and decrease customer environments for peaks and valleys
 - Joint-use of Cheetah Loyalty's large-scale analytics cluster
- Always current
 - Automatic updates to latest Cheetah Loyalty software releases
 - Zero-downtime rollouts with Cheetah Loyalty schema versioning
- Proactive Security
 - Automated updates to latest security releases
 - Proactive system-wide monitoring of resource utilization, application performance, and operational health via Amazon CloudWatch



Operational Security

Cheetah Loyalty leverages Amazon Web Service's world-class security capabilities to deliver built-in security features (see <http://aws.amazon.com/security>):

- Secure data transport via SSL/TLS
- Encrypted data and file storage using Advanced Encryption Standards (AES) 256
- Private Subnets and built-in firewalls for each Cheetah Loyalty environment via AWS Virtual Private Cloud (VPC) (option)
- Unique users via AWS Identity and Access Management (IAM) with Multi-factor authentication (MFA)
- Security Logs via AWS CloudTrail
- Highly secure data centers with electronic surveillance and trained security guards
- Resiliency and failover via multiple geographic regions and availability zones



Application Security

Cheetah Loyalty's single-tenant architecture delivers secure computing by isolating application software, storage, and processing.

- Separate, isolated application binaries for each customer environment
 - No commingling of software binaries
 - Ability to upgrade and patch each environment
- Separate, isolated, encrypted application storage for each customer environment
 - Program definitions and all application data in separate MySQL databases
 - Activity queues in separate, dedicated Apache Kafka topics environment
 - Member data in CRM system (e.g. salesforce.com)
 - Member activities in separate, dedicated HBase tables
 - Files in separate, dedicated S3 buckets
 - Isolated Apache Hadoop cluster per Cheetah Loyalty environment (option)
- Separate, isolated application processing for each customer environment
 - Dedicated Cheetah Loyalty App Servers per customer environment
 - Dedicated Cheetah Loyalty Finagle Servers per customer environment
 - Dedicated Apache Storm topology per customer environment
 - Dedicated Apache Spark context per customer environment
- Secure Authentication and Authorization
 - Strict password policies for admin and member logins
 - Multi-factor Authentication (MFA) for admin users
 - Dedicated member authentication services per customer environment
 - Role-based authorization for marketing users
 - Audit trail for marketing users
- Deliberate Handling of Member Personal Identifiable Information (PII)
 - Member PII stored in CRM system (e.g. Salesforce)
 - Member PII separated from Member Activity data
 - No Member PII in aggregate and analytics processing
- Penetration Testing
 - Verified x-site scripting, SQL injection, and DOS attacks
 - Security audit by Salesforce.com



Admin Access Control

Cheetah Loyalty utilizes the following mechanisms to prevent Cheetah Digital and Customer Employees from unauthorized access to customer data:

AWS Access

- Fine-grained, secure access to AWS accounts and resources
 - Individual IAM-user access for each Cheetah Digital employee per customer environment: no shared credentials
 - User authentication via Multi Factor Authentication (MFA) devices and X.509 certificates.
- AWS Audit trails
 - AWS CloudTrail activated to log IAM actions, STS actions, and AWS Management Console sign-ins

Cheetah Loyalty Marketing Console

- Strong Passwords
 - Use of strong passwords (e.g. minimum length, special characters, etc) can be enforced for Cheetah Loyalty Marketing Console admins
- Effectivity Dates
 - Each Cheetah Loyalty Marketing Console admin has a start and end date that controls the dates when their logins are valid.
 - Set end dates to ensure that admins access is automatically terminated in the future.
- Roles and Permissions
 - Each Cheetah Loyalty Marketing Console admin has one or more roles that give the admin read, write, and admin access to one or more Marketing Console screens.
 - Use roles and permissions to give the minimum amount of access to each admin.



Disaster Recovery

Cheetah Loyalty leverages Amazon Web Services' low-cost offline backups, multi-availability zones, and network of data centers for disaster recovery.

- Automated Backups
 - Automated backups and database snapshots via Amazon RDS
 - Hbase region snapshots and table snapshots
 - Store backup snapshots into AWS Glacier for long-term storage (option)

- High availability and failover support for customer data
 - Utilize Amazon RDS multi-AZ deployment for MySQL databases
 - Hbase on highly redundant setup with multiple Zookeeper servers and dedicated Master servers
 - Amazon S3 files written automatically to at least three AWS facilities

- Near real-time replication to disaster recovery data center (option)



Certifications

Cheetah Digital conducts regular security review and certifications to minimize the risk of data loss and security breaches.

- SOC 2
 - Review of Amazon Web Services SOC 2 certifications
 - Annual SOC 2 Type 1 and Type 2 audits of Cheetah Loyalty's processes and procedures
- Security Testing
 - Use best-of-breed security tools to run internal security tests of Cheetah Loyalty's production landscape
 - Engage a third-party security firm to conduct security tests against Cheetah Loyalty's production landscape
- GDPR
 - Review and verify Stella Loyalty's production landscape and procedures to ensure compliance with European Union General Data Protection Regulations



References

Cheetah Loyalty

- Cloud Platform ebook
- SOC 2 Audit Report
- EU GDPR White Paper

Amazon Web Services

- Security Features: <http://aws.amazon.com/security/>
- Global Infrastructure: <http://aws.amazon.com/about-aws/global-infrastructure/>