Security Policy at FeetPort

FeetPort Security

Overview of Approach

Introduction

We make FeetPort to help our users improve data quality by giving them a platform optimized for ensuring field data capture is streamlined and error-free. Protecting the data of our customers while it is in our custody is a responsibility we take seriously. Information security can be complex and we are committed to helping our customers understand our approach and the practices we employ to keep their data safe.

Organizational Security

Competent Groove’s security team is led by its Technical Architect, who coordinates security issues with the Chief Executive Officer (CEO). Under the CEO, responsibility for on-premises

information technology security and security of our cloud infrastructure is segmented between our Information Technology Manager and our Senior Cloud Architect, respectively.

The engineering team, under the direction of the Tech Arch., is responsible for designing, implementing, and testing security features within the FeetPort platform. This includes mitigation of any findings from internal or customer-driven penetration tests or security assessments.

Data Protection

The goal of FeetPort’s security program is to protect customer data from unauthorized access as it is collected in the field, transmitted to the hosted FeetPort infrastructure and stored in the FeetPort database. The approaches below represent the current state of our security efforts, which are being constantly re-evaluated in response to the changing security landscape.

Secure Development Process

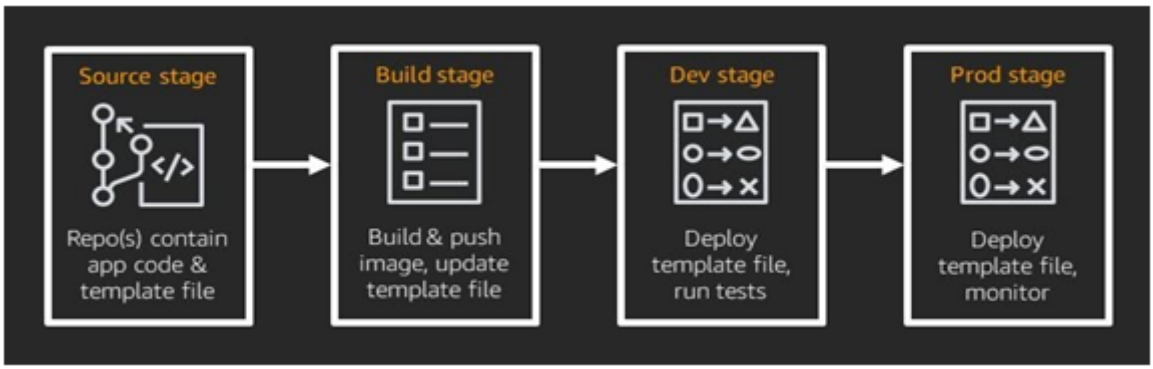
The FeetPort development process is closely aligned with the GitFlow process. Our process includes consideration for emergency releases or hotfixes as part of the life cycle. This enables us to address security issues as part of our normal system development process, based on severity.

As our security team monitors security alerts, such as CERT alerts and MITRE CVEs, and develops findings from our own penetration testing program, they coordinate with the engineering and product management teams to assess the impact of findings and the complexity of mitigations. Remediations are then added to the FeetPort product roadmap, based on the results of the assessment, with fixes for more severe findings prioritized for faster release.

Secure Development Process

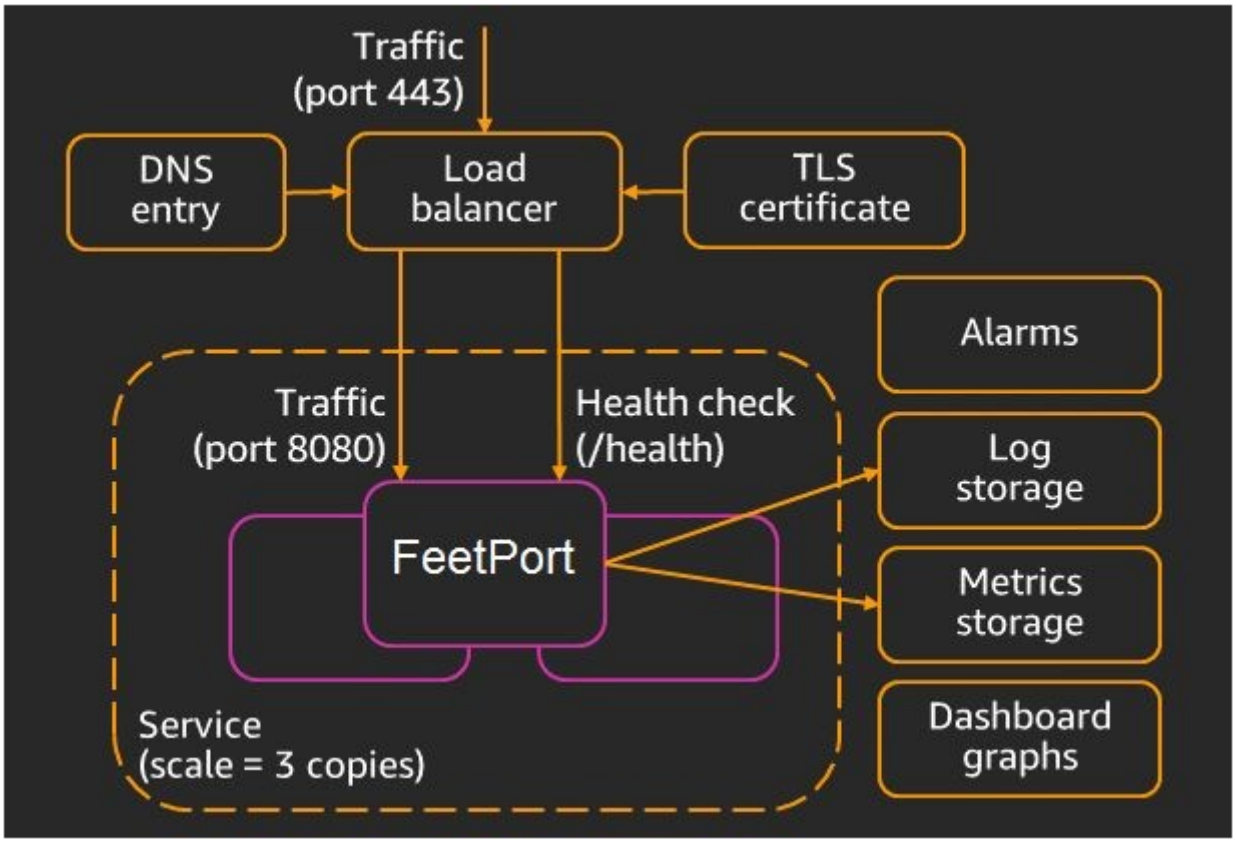
For FeetPort applications internally, our best practice is to deploy API's and front-end with CI/CD release pipeline. A simplified example of our release process is shown below. The template contains the API infrastructure (for example, a load balancer). In the "build" stage of the pipeline, the container image is built and pushed. Each stage of the pipeline like "Dev" and "Prod" then deploys the same infrastructure. This practice gives us confidence that deployments

of the entire application are repeatable and testable, and we have full visibility in the pipeline into the exact application code that is currently deployed in the production environment.



Infrastructure

We are hosted on AWS and use EBS container service to run applications, which is guarded by security groups and strong VPC. EBS uses an application load balancer with sticky sessions to control multiple EC2 machines. EBS is so flexible to grow depending upon load. An example of our Application architecture is shown below.



Encryption

In Transit

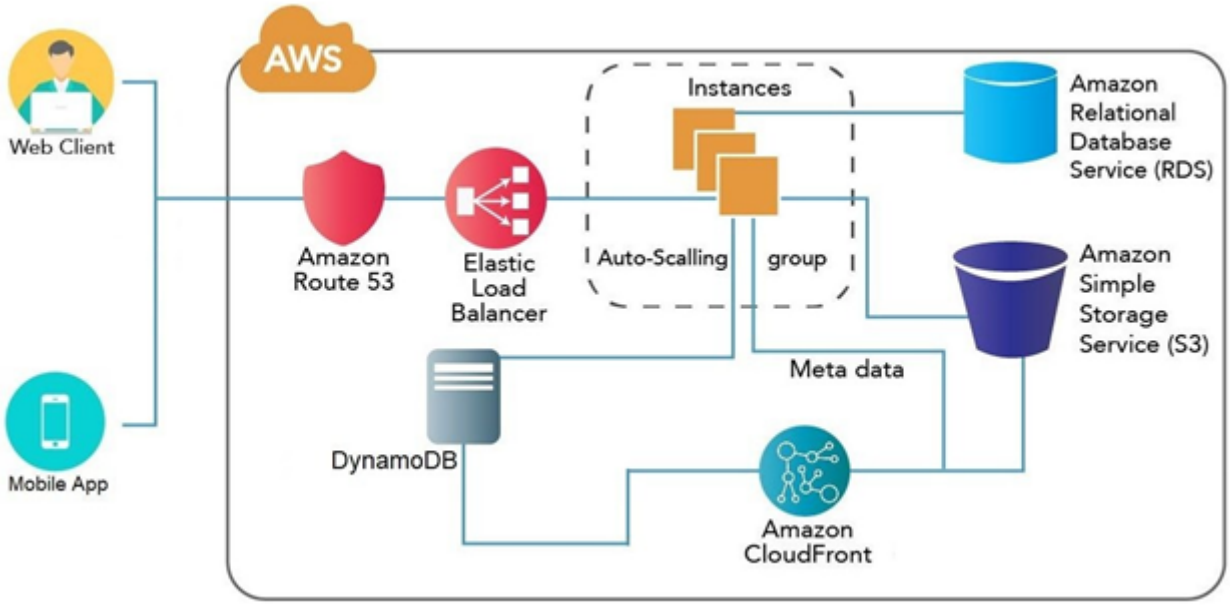
All interaction with the FeetPort service, whether from FeetPort client applications or from user-developed applications, uses the FeetPort API. All data transmitted between client applications and the FeetPort API is done so using strong encryption protocols. FeetPort supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.1 or higher, AES-256 encryption, and SHA256 signatures, whenever supported by the clients.

At Rest

Data at rest in FeetPort is encrypted using compliant encryption standards (AES-256), which applies to all types of data at rest within FeetPort — relational databases, file stores, database backups, etc. All encryption keys are managed through either AWS Key Management Service (KMS) or Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). FeetPort has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

The FeetPort service is hosted in AWS US South 1 (Mumbai), with physical protection for the infrastructure that comprises the FeetPort operating environment described in AWS white papers. Each FeetPort customer’s data is hosted in our multi-tenant infrastructure and logically separated from other customers’ data. We use a combination of strategies to ensure customer data is protected from failures and returns quickly when requested. These strategies include the use of write-ahead logs (WALs) to ensure data integrity as it is written. Databases are backed up fully

each night. In addition, we maintain a streaming replica in a warm stand-by in a separate availability zone to protect against AWS outages.



Network Security

FeetPort segments its cloud-based instances into separate networks to better protect sensitive data. Instances supporting testing and development activities are hosted in a separate network from instances supporting the FeetPort production infrastructure. All instances within our production system are hardened (e.g. disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Network access to the FeetPort production environment from open, public networks (the Internet) is restricted, only load balancer of production servers accessible from the Internet and has only 80 and 443 Ports are open. further 80 Port will redirect to 443 forcefully.Only those network protocols essential for delivery of the FeetPort service to its users are open at our perimeter and there are mitigations against distributed denial of service (DDoS) attacks deployed at the network perimeter. Additionally, FeetPort logs all system calls and uses AWS GuardDuty to provide alerting for behaviors that indicate a potential intrusion.

Endpoint Security

All workstations issued to Competent Groove personnel are configured to comply with our standards for security. Our default configuration implements encryption at rest, strong passwords, and lock when idle. Workstations use up-to-date monitoring tools to detect potential malware, unauthorized software, and mobile storage devices.

Workstations use secure internet protected by Firewalls and separate networks for Computers/Mobile devices with proper network security.

Access Control

Least Privilege

To minimize the risk of data exposure, Competent Groove adheres to the principle of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly. Staff are provisioned onto corporate systems using separate accounts and are granted access only to applications and data needed for their role.

Authentication

To further reduce the risk of unauthorized access to data, FeetPort employs layered authentication for all access to our production environment that houses customer data. Every Employee account who has access to AWS is guarded with 2 step authentication.

FeetPort uses private keys for authentication to gain administrative access to production database instances, in addition to the previously mentioned layered authentication. Password access to production database instances is disabled and private keys are only available to authorized administrative staff.

Monitoring and Logging

Account-level audit logging is available to all FeetPort account holders and can be accessed via the FeetPort API for manual or automated analysis. Additionally, all FeetPort API calls are logged across the entire FeetPort application. FeetPort instances and databases have system logging enabled, to capture administrative access, privileged commands, and system calls. Logs are retained for 60 days and stored separately from production systems and backups. Logs are accessible by administrative staff only for manual and automated analysis.

Data Retention, Disaster Recovery, Business Continuity

All customer-collected data, including full record histories are retained within a customer's FeetPort account for the life of the subscription, unless the data is deleted by the customer. FeetPort databases are fully backed up daily, with backups retained for 30 days. A warm stand-by of FeetPort is maintained via streaming replication. Any actions taken by customers on their data are replicated immediately.

Data collected via FeetPort mobile applications on customer-owned mobile devices exists only on those mobile devices until it is synchronized with the FeetPort production system, hosted on AWS. If data is deleted prior to synchronization, or if the mobile device is corrupted, destroyed, or otherwise rendered inoperable, unsynchronized data cannot be recovered.

The FeetPort warm stand-by is housed in a separate AWS availability zone (AZ) to provide sufficient isolation in the event of the unavailability of the primary AWS infrastructure.

Competent Groove technical staff are geographically dispersed via remote-work to ensure coverage in the event of a natural disaster or other event affecting corporate headquarters. Our business continuity plan includes remote-work/temporary relocation of staff from headquarters to other locations in the case of such an event.

Vendor Management

With the exception of the native mobile applications, the FeetPort production system is deployed within Amazon Web Services (AWS). AWS is the only sub-service vendor we use to support FeetPort operations. Our underlying AWS infrastructure is governed by several applicable service-level agreements (SLAs) which exceed our requirements and have enabled FeetPort to meet its availability goals.

https://aws.amazon.com/compute/sla/ https://aws.amazon.com/s3/sla/

https://aws.amazon.com/rds/sla/

As AWS customers, we are able to access AWS SOC 1 and SOC 2 reports. The AWS SOC 3 report is available publicly.

Validation

We perform quarterly penetration tests of the company's public-facing systems housed in Amazon Web Services (AWS). This testing follows the industry-standard Penetration Testing Execution Standard (PTES) found at http://www.pentest-standard.org/index.php/Reporting. This process includes:

1. Analysis of the FeetPort Android application to discover application programming interface (API) endpoints.
2. Port scanning assets hosted at AWS to determine open ports and operating system/application versions.
3. Scanning these assets using Nessus/OpenVAS to determine any existing vulnerabilities.
4. Active attempts at exploitation using the standard Metasploit framework.

The findings of each test are reviewed with the FeetPort product management and addressed the development lifecycle, based on severity. The summary of these results can be made available to enterprise subscribers under a non-disclosure agreement (NDA).

Front end Validation

We have implemented high level security for our front-end applications. Our application has been rated A grade in terms of web security by https://securityheaders.com/ The report of live test can be found here https://securityheaders.com/?q=web.feetport.com&followRedirects=on

Customer Penetration Testing

Our customers are welcome to perform either security controls assessments or penetration testing on FeetPort’s public-facing environment. Because some kinds of tests may trigger automated mitigation measures from AWS, please contact your account manager to coordinate scheduling of your tests.

Revision #3
Created 26 August 2020 04:27:11 by Kamna
Updated 26 April 2022 09:23:03 by Kamna