Fulcrum Security

Overview of Approach

Version 1.0 - June 2019

ISSUED BY
Spatial Networks

Table of Contents

Introduction

We make Fulcrum 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

Spatial Networks' security team is led by its Chief Information Officer (CIO), who coordinates security issues with the Chief Technology Officer (CTO) and Vice President of Product. Under the CIO, 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 CTO, is responsible for designing, implementing, and testing security features within the Fulcrum platform. This includes mitigation of any findings from internal or customer-driven penetration tests or security assessments.

Data Protection

The goal of Fulcrum's security program is to protect customer data from unauthorized access as it is collected in the field, transmitted to the hosted Fulcrum infrastructure and stored in the Fulcrum 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 Fulcrum development process is closely aligned with the GitFlow process. Our process includes consideration for emergency releases or hotfixes as part of the lifecycle. 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 Fulcrum product roadmap, based on the results of the assessment, with fixes for more severe findings prioritized for faster release.

Encryption

In Transit

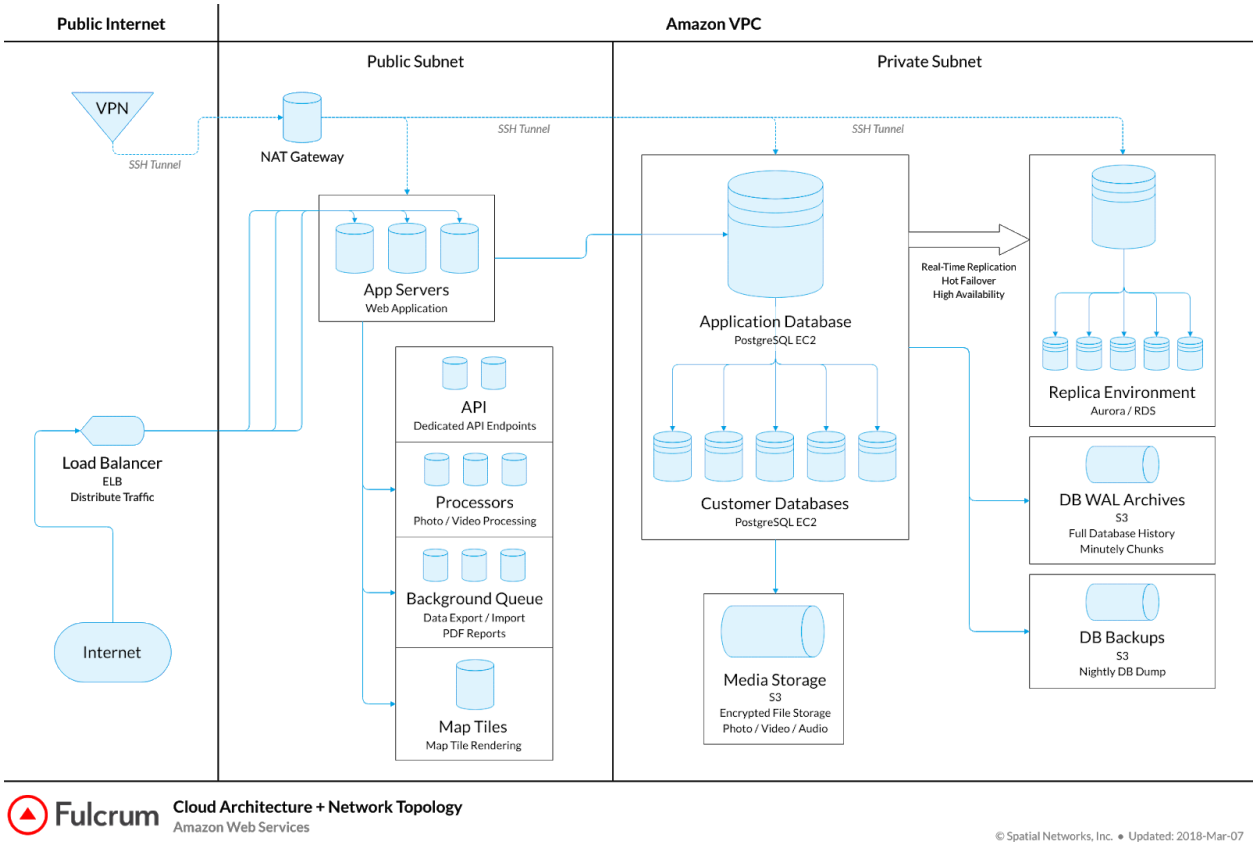
All interaction with the Fulcrum service, whether from Fulcrum client applications or from user-developed applications, uses the Fulcrum API. All data transmitted between client applications and the Fulcrum API is done so using strong encryption protocols. Fulcrum supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.1 or higher, AES-256 encryption, and SHA2 signatures, whenever supported by the clients.

At Rest

Data at rest in Fulcrum is encrypted using FIPS 140-2 compliant encryption standards (AES-256), which applies to all types of data at rest within Fulcrum — 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). Fulcrum has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

The Fulcrum service is hosted in AWS US East Region 1, with physical protection for the infrastructure that comprises the Fulcrum operating environment described in AWS white papers. Each Fulcrum 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



Fulcrum 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 Fulcrum 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 Fulcrum production environment from open, public networks (the Internet) is restricted, with only a small number of production servers accessible from the Internet. Only those network protocols essential for delivery of the Fulcrum 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, Fulcrum logs all system calls and uses AWS GuardDuty to provide alerting for behaviors that indicate a potential intrusion.

Endpoint Security

All workstations issued to Spatial Networks personnel are configured to comply with our standards for security. All workstations are configured, updated, and be tracked and monitored by Spatial Networks mobile device management (MDM) solution. Our default configuration sets 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. These tools include MDM policies and MacOS-native tools such as Xprotect and Gatekeeper. Company-owned mobile devices are required to be enrolled in the appropriate mobile device management system.

Access Control

Least Privilege

To minimize the risk of data exposure, Spatial Networks 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 Okta single sign-on (SSO) and are granted access only to applications and data needed for their role.

Authentication

To further reduce the risk of unauthorized access to data, Fulcrum employs layered authentication for all access to our production environment that houses customer data. The Okta SSO environment previously described, enforces additional VPN requirements for access to production instance on AWS. Staff must first authenticate against Okta,

which will then require users to be on the Spatial Networks VPN prior to accessing our AWS infrastructure. Once on the VPN, Okta will then manage access to segments of our AWS infrastructure based on assigned role(s).

Fulcrum 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 Fulcrum account holders and can be accessed via the Fulcrum API for manual or automated analysis. Additionally, all Fulcrum API calls are logged across the entire Fulcrum application. Fulcrum 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 Fulcrum account for the life of the subscription, unless the data is deleted by the customer. Fulcrum databases are fully backed up nightly, with backups retained for 30 days. A warm stand-by of Fulcrum is maintained via streaming replication. Any actions taken by customers on their data are replicated immediately.

Data collected via Fulcrum mobile applications on customer-owned mobile devices exists only on those mobile devices until it is synchronized with the Fulcrum 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 Fulcrum 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. Spatial Networks 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 Fulcrum production system is deployed within Amazon Web Services (AWS). AWS is the only sub-service vendor we use to support Fulcrum operations. Our underlying AWS infrastructure is governed by several applicable service-level agreements (SLAs) which exceed our requirements and have enabled Fulcrum 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

Spatial Networks, Inc. (SNI) performs 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. Passive information gathering to enumerate all public websites belonging to SNI and mirror their contents locally for examination.
2. Analysis of the Fulcrum Android application to discover application programming interface (API) endpoints.
3. Port scanning SNI assets hosted at AWS to determine open ports and operating system/application versions.
4. Scanning these assets using Nessus/OpenVAS to determine any existing vulnerabilities.
5. Active attempts at exploitation using the standard Metasploit framework.

The findings of each test are reviewed with the Fulcrum 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).

Customer Penetration Testing

Our customers are welcome to perform either security controls assessments or penetration testing on Fulcrum'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.