RunMyProcess.

a Fujitsu company

Security in RunMyProcess:

An Overview

Introduction

RunMyProcess solves digital problems and helps enterprises evolve using the power of connected technology.

To achieve this we operate a cloud platform for quickly and securely building applications which connect enterprise systems to the people, clouds and devices of the digital world. By making connections our platform helps enterprises safely evolve towards new digital business models and make a real difference to the lives of their customers and employees.

In delivering these services the availability, confidentiality and protection of our customer's data is at the heart of our thinking, our architecture and our daily operations. This document describes the business, organizational and technical measures in place to meet these critical commitments.

In order to cover the broad range of perspectives that fall under a consideration of security this document will cover the following topics:

Each topic will be covered in its own section to give a fully rounded view of the way in which RunMyProcess addresses security related concerns.

Business Governance

In this section we consider the major business policies which ensure our customers can fulfill their data protection and IP due diligence responsibilities.

Data Protection

Customers retain sole responsibility and ownership for any data (including personal data) they process using the RunMyProcess service. We provide a number of data protection guarantees and benefits, however, to aid customers in fulfilling their responsibilities.

Firstly all applications and data are hosted in a highly secure data center operated by Amazon Web Services in Frankfurt. The Federal Republic of Germany operates one of the strongest data protection regimes in the world and using this country as our base ensures that our customers benefit from these world-leading data protection standards. Equally this also serves as a differentiator for our customers in terms of evidencing the importance of data protection, enabling them to build strong trust-based relationships with their employees and customers irrespective of their region of origin.

Secondly, RunMyProcess does not make any direct or indirect use of customers' data for any purpose other than that required for provision of the service (or unless otherwise previously instructed in writing).

Finally, our service ensures the confidentiality of customers' data in a number of ways:

- Every customer's account and Applications are compartmentalized and only available to authorized users within their organization;
- Data are encrypted using Transport Layer Security (TLS);
- Users' passwords are used and stored in an encrypted format;
- The connection/login process is designed to withstand brute force attacks;
- Users' passwords have a minimum of 8 characters; and
- All servers are protected with a firewall.

Intellectual Property Protection

We assert that all of the intellectual property required to deliver the RunMyProcess service belongs to the company and we further secure our customers against any third party claims challenging their right to use any of the technologies and practices it contains. Full details of the terms of this cover are made available within the customer contract.

Organizational Governance

In this section we consider the major business policies which ensure our customers can fulfill their data protection and IP due diligence responsibilities.

Access Policies

Access to Servers

Only a strictly limited subset of RunMyProcess personnel – designated within our policies as nominated "Operations Engineers" – have the ability to access our production servers. This access is only possible via a combination of VPN together with a specific PKI certificate. Local control and access to all servers is deactivated.

Access to Server Logs

Server logs are only accessible to designated "Operations Engineers" via VPN and certificate. Where customers produce additional / custom logs during process execution these logs are only accessible to the customer via the provided APIs.

Access to Customer Environments

RunMyProcess personnel do not have access to customer environments during normal operation. For support purposes, however, a designated account administrator within a customer's organization can grant access to an explicitly named RunMyProcess support engineer for a defined amount of time. For example, support authorization could be granted to 'support_engineer@runmyprocess.com' from xx/xx/xxxx to yy/yy/yyyy. In this example, the support engineer would be able to access the customer account – with the same privileges as the user that granted the access – for the defined period. If necessary the account administrator can also revoke access at any time.

Access to Customer Data Logs

All logs containing customer data are only accessible to designated "Operations Engineers" on a needs basis via VPN and certificate. Local control / access to all data is deactivated.

Operational Policies

Patch Policy

The RunMyProcess security team closely follows a list of security and vulnerability information sources such as the US CERT security bulletin. Based on information from such sources a triage process is undertaken and necessary updates are applied. Depending on the severity level of the threat such updates may be applied immediately or during a regular platform update.

Change Policy

All changes to the platform are assessed and where practical assigned to a specific release. All necessary tests to validate the functionality and security of the enhancement must be written as part of the development and release cycle. These tests must ensure that the feature is behaving as expected and that it will not introduce any instabilities or vulnerabilities.

When signed off as part of a release new features are rolled out as part of the formal update process.

Testing Policy

The Fujitsu RunMyProcess platform is tested daily through the application of over 5000 functional and security tests. These tests simulate a wide range of unitary and complex scenarios. This testing is continually evolving as we add new features to the platform.

Development Policies

At RunMyProcess we operate an agile development lifecycle focused on early testing and resolution of issues. We follow an iterative lifecycle of multiple design, develop and test loops for each platform release and have a range of security questions and patterns that are applied and reviewed at each stage. As part of our effort to reduce attack surface these reviews include the relevance of the new feature, its applicability to our full set of customers and the way in which it fits into our security models. Once validated, the change will be assigned to a new version of the platform and all necessary tests prepared. Finally we use state of the art tools to automatically check for quality and security issues within source code.

New features are made available during a platform update as per the release process.

Physical and Environmental Security

In this section we summarize the systems that our chosen infrastructure provider – Amazon Web Services (AWS) – has put in place to secure the physical locations powering our cloud platform.

Access Controls

AWS data centers are housed in nondescript facilities at a number of locations around the world and provide stringent controls over access and information for employees and contractors both at the perimeter and at building ingress points.

Environmental Controls

Climate control systems within AWS facilities maintain a constant operating temperature for hardware to prevent overheating and reduce the possibility of outages. Automatic fire detection and suppression equipment is deployed in all areas.

Power Controls

Electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Access Management and Control

In this section we discuss the ways in which we manage customer usage and protect systems and data from unauthorized and inappropriate external access.

Authentication

RunMyProcess offers several methods for user authentication:

- RunMyProcess login and password
- OAuth2 with Google Apps
- SSO via SAML V2

For server-to-server communication RunMyProcess supports the following schemes for calling external APIs:

- Login/password with RunMyProcess secure lockbox for credential storage
- OAuth2
- Java Keystore
- Windows Azure authentication
- AWS digest
- Fujitsu SOPOS

Authorizing Access to Resources

Once a principal is authenticated all subsequent requests are submitted to strict authorization mechanisms. These mechanisms are based on the role based authorization features in RunMyProcess.

These authorization features enable organizations to create a hierarchy of entities and roles which reflect the structure of their operating model. Using this model we guarantee the fulfillment of authorization requirements at four separate levels (Platform level, Project/application level, Process level, Step/Task level). More information on roles and access profiles can be found at https://docs.runmyprocess.com.

Transaction Security

Communication between the browser and the RunMyProcess platform is done via HTTPS and secured using 128-bit Transport Layer Security (TLS) with support for SNI extension. All connections require authentication and authorization and all user operations are recorded including IP addresses and other session details.

For server-to-server communication, the following secure communication protocols are supported: HTTPS, SMTPS, POPS, SFTP, FTPS and COAPS. All communication is made through TLS – key size 2048. For security reasons, Secure Sockets Layer (SSL) has not been accepted for platform connections since September 2014.

Logs

All user authentication is logged and available to account administrators for audit and security purposes. The information captured includes user login, timestamp, location and a description of any action undertaken.

Preventing Abuse

Depending on customer policies RunMyProcess can block accounts in response to a configurable number of failed authentication attempts. Once blocked, only an account administrator can restore access.

Secure Access to On-Premise Systems

RunMyProcess supports secure access to enterprise environments using the Secure Enterprise Connector.

The Secure Enterprise Connector creates a secure tunnel between the RunMyProcess platform and an organization's local network.

For this tunnel to work, an agent – named the Data Connector agent – is installed inside the firewall. This digitally signed agent creates an encrypted outbound tunnel to the RunMyProcess platform, providing a secure link based on TLS. Originally developed by Google the technology is now maintained by RunMyProcess.

When a connector configured to use the Secure Enterprise Connector tunnel is called, the request is sent to the agent through the encrypted tunnel and then dispatched locally to the relevant system.

Data Management

In this section we discuss the ways in which we ensure that the data & applications of our customers remain separate, private and available.

Data Encryption

In order to ensure high protection of our customers' data, the following encryption mechanisms are in place:

- All data at rest (Uploaded files, On-demand database...) is encrypted with asymmetric 256 bits keys which use the AES/CBC/PKCS5Padding algorithm.
- Application configurations, process definitions and the data of processes at rest are encrypted with customer-specific, asymmetric 256 bits keys which use the AES/CBC/PKCS5Padding algorithm.
- Passwords are encrypted with the SHA256 hash function.

In addition to these foundational capabilities platform APIs are provided which enable customers to implement own encryption on data they handle within the platform.

Data Segregation

RunMyProcess is a multi-tenant cloud platform built from the ground up to keep customer data private while enabling the benefits of a shared technical and operational environment. As such, customer data is segregated.

Configuration data is segregated by the software. Since all access is authenticated and authorized, customers cannot access data that does not belong to their account.

Customer and process data are segregated by both the software and the storage engine. This means that data is stored using different physical databases (for customer defined collections) or different S3 folders (for application and process definitions plus raw process execution data). All accesses are strictly authorized, preventing information visibility between customers.

Specifically, the segregation is carried out using a range of techniques dependent on the data in question.

- Account Configuration data
  - MySQL logical partition.
- On-Demand Database (accessible to developers to store business objects for their applications)
  - MongoDB physical partition (for every customer account).
- Application & process definitions / Raw process execution data
  - AWS S3 folder per customer.
- Uploaded files
  - AWS S3 folder per customer.

Data Retention

Production data is kept without any time limit so long as the contract between RunMyProcess and the customer remains in force.

Instant access to production data is guaranteed for a period of 48 months. Data that are older than 48 months may be archived and made available to the customer upon request. Instant access to test/acceptance data is guaranteed for a period of 2 months. Data that are older than 2 months may be deleted by RunMyProcess without any notice.

Data Extraction / Portability

All of the data stored within RunMyProcess – e.g. configuration data, process execution data, business objects, reports, etc.- are accessible via REST APIs which provide a JSON-format response for business object data and an XML-format response for everything else. In the case of a contract termination, customers can always extract all of their data.

Business Continuity

In this section we discuss the ways in which we ensure continuous platform access in the face of unforeseen events.

Multiple Availability Zones

In order to maximize business continuity, platform components are installed on different AWS availability zones. This ensures that the platform will still perform correctly in the case of an AWS zone deficiency. As of today, all application servers and databases (configuration data, collection data) are distributed across different zones.

Disaster Recovery

In the case of a total failure within a platform component, action will be taken to recover normal operations according to identified recovery procedures.

Data storage is replicated and distributed across several zones but in the worst case scenario, data recovery will be possible using backups. Collection and configuration data are backed up on a daily basis and can be restored for any given time in the last 7 days (Point in Time Recovery).

Storage Engines

As previously discussed, RunMyProcess uses multiple databases to store different kinds of data. Each of these data stores is configured in different ways to ensure continuity of service:

- MySQL
  - Master-slave over 2 availability zones,
  - Daily complete Snapshots, PITR to the minute for up to 7 days.
- MongoDB
  - Replicated over 3 Amazon servers on 2 different availability zones,
  - 1 daily snapshot, 7 days history
- AWS S3
  - 99,999999% data durability guaranteed by AWS

Service Availability

In this section we discuss the ways in which we ensure the security & availability of our customers' data & applications.

Supervision and Incident Management

Platform operations are monitored 24 hours a day, 7 days a week and supported by a range of best in class technical support tools. Identified issues are distributed for human action across a range of alert channels, with operations teams taking all necessary actions to solve the issue via predefined incident management & escalation procedures.

Operational Transparency

RunMyProcess is committed to building customer trust through transparency of operations. To support this goal regular service updates, incident information and resolution estimates are published via the @runmyprocess_ops twitter account.

Summary

In this document we have examined a range of security topics in order to give a broad understanding of the way in which RunMyProcess protects the interests of our customers. Specifically we have considered a range of different perspectives to give a rounded view of our approach, covering: