Surecomp

RIVO Platform Security
Version – 07/2022

Surecomp

CONTENTS

OBJECTIVE

The purpose of this document is to present an overview of how RIVO solution tracks and guarantees the security of its customers' sensitive information on AWS.

RIVO SECURITY BASICS

Authenticate Users

Authentication means preventing unauthorized access to the organization or its data by making sure each logged in user is who they say they are. RIVO supports password authentication including Multi Factor authentication (MFA) via e-mail.

When customers Single Sign On is integrated, additional customer supported methods can be used.

Passwords

RIVO ensures each user will have a unique username and enforces a strong password policy. A Password is required on any login and MFA is enforced every 3rd login. When SSO is integrated, RIVO will follow the organizational password relevant policies.

Cookies

RIVO issues a session cookie to record encrypted authentication information for the duration of a specific session.

Multi-Factor Authentication

Multi-Factor Authentication method grants users access to the RIVO application only after successfully presenting two pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows "Password"), possession (something only the user has "Email").

Network-Based Security

Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use network-based security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

Surecomp is using the tools below to attempt prevention of cyber-attacks, these tools are implemented in addition to AWS best-practice tools, to detect and mitigate possible attacks as soon as they happen.

Endpoint Detection and Response (EDR) protecting the Cloud servers:

The EDR tool records and stores endpoint-system-level behaviours. EDR uses a variety of data analytics tools to aid in the detection and prevention of possibly suspicious behaviours within the system. EDR also provides

relevant contextual information, blocks malicious behaviours, and provides mitigation and remediation suggestions to restore affected systems.

Real-Time Cyber Threat Intelligence:

Cyber intelligence service that analyses and monitors the deep web and dark web for threat intelligence related to the specific cloud service.

Third-Party Penetration Tests:

Surecomp performs gray/black box Penetration tests by third-party security experts to ensure adherence to industry best and latest practices, and compliance/resilience in relation to the latest OWSAP known CVEs.

Security Incident Response:

In case of a system alert, events are escalated to our 24/7 teams providing operations, network engineering, and security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

Session Security

After logging in, a user establishes a session with the platform. The platform is using session security features to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session.

Custom Login Flows

Use a login flow to introduce business processes during login, such as to prompt for a second factor of authentication, accept terms of services, or collect information from users. After users complete the login flow, they are logged in to RIVO.

Single Sign-On

Single sign-on (SSO) lets users access authorized network resources with one login. The user is requested to validate its existing organizational username and password against your corporate user database or other client app rather than RIVO managing separate passwords for each resource.

Data Encryption

RIVO Encryption gives data a whole new layer of security while preserving critical platform functionality. It enables encrypting sensitive data at rest, and not just when transmitted over a network, so the company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling confidential data. Data is kept encrypted using AES256 encryption via AWS Disk Encryption.

What is the platform? AWS

What cloud deployment model is used? Private

Data At Rest

We are using AWS S3 storage encryption & AWS TLS key encryption.

Data At Transit

Data transfer is done using secure protocols in addition to the authentication process. HTTPS protocol will be used when transferring data using the web portal

Monitoring Organization's Security

Track login and field history, monitor setup changes, and take actions based on events. Review the following sections for instructions on monitoring the security of RIVO organization.

Field History Tracking

Audit trail of transactional field values. The field history includes the applying user, time, associated transaction, previous and new values. Data is retained for an unlimited period.

RIVO PLATFORM DATA ACCESS SECURITY MODEL

Overview

RIVO provides several layers of security with lots of flexibility to accommodate virtually any business needs.

Object-level-security

Before allowing a user access, RIVO first verifies that the user has permissions to see the data to specific (organization level or unit level).

Profiles

In RIVO, profiles control access to RIVO functionality-level and additional features like apps, tabs, and so on.

Record-level security (Record Sharing Rules)

RIVO provides some ways to share records with others and access others' records.

Role Hierarchies

Virtually all companies have an organization structure where groups of people may be segregated between units with different rights of access, such as Processor, Approver or Administrator, forming a tree-like org chart, where an admin must first assign each user with a role granting the required access.

Manual Sharing

The sharing feature enables a party to invite others to collaborate over a deal, for reading only or to actively engage with the counterparts.

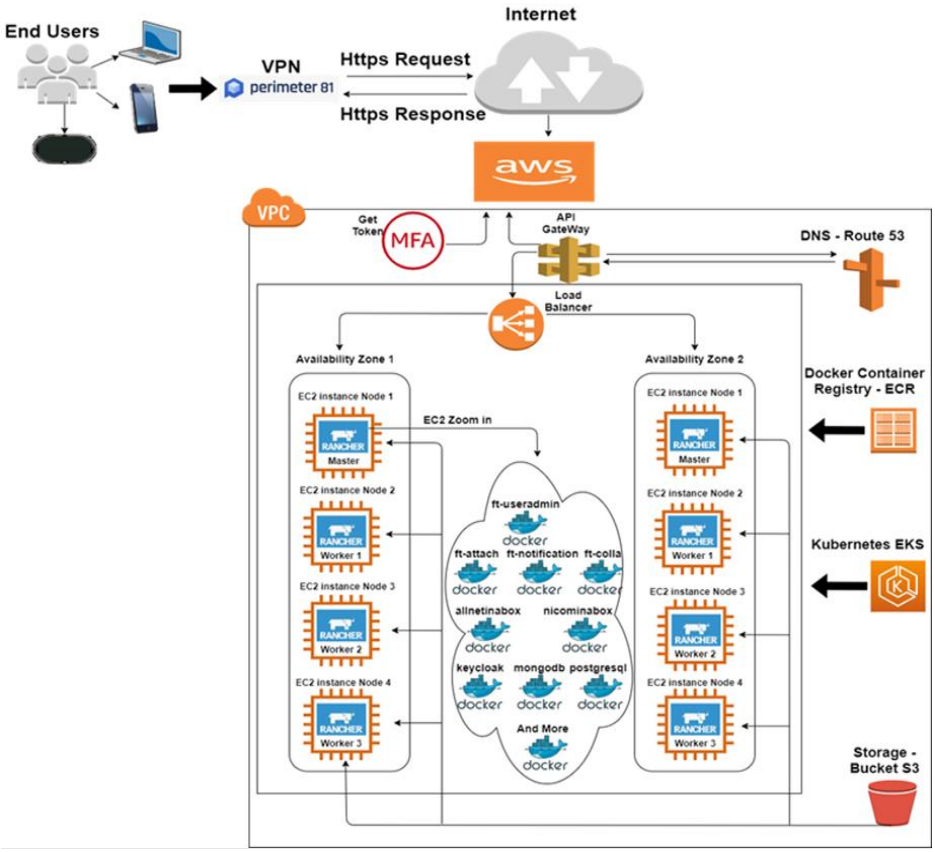
RIVO PLATFORM DATA MANAGEMENT

Overview

RIVO helps Financiers and Corporates to efficiently manage all of their trade finance business in one place. RIVO is the only trade finance platform that provides a comprehensive solution with seamless collaboration among all trade counterparts by connecting an ever-growing ecosystem, digitizing trade finance instruments, and enabling efficient collaboration.

RIVO Diagram

Surecomp follows best practices and industry standards to comply with industry common practices, security, and privacy frameworks, to ensure we meet our customer's compliance standards. All Customer data is protected behind the Firewall and access to the data is audited and monitored. RIVO Platform is natively built and 100% hosted on AWS – below a macro-diagram with the main components of the RIVO platform:



Main Data-related-objects

In order to secure different trade finance transactions and collaboration data inside the platform, RIVO distributes the information in some main components.

Participants

Participants are all trade counterparts (people and/or entities) registered in the RIVO Platform. Participants are at the core of the platform and interact with it by means of Transactions and Collaboration Data.

Transactions

Transactions can be the result of processing a set of data or they even may start the processing itself.

Data Management

Surecomp data security policies and procedures for security handling data are GDPR compliant, as well as reviewed internally and externally audited on a yearly basis.

Data Residency

Surecomp hosts the application data primarily in AWS data centers that have been certified as ISO 27001, PCI DSS Service Provider Level 1, and is SOC 2 compliant. RIVO was launched on May 18th, 2022, using AWS Data Center located in Germany.

Data Backup

Production application backups take a daily snapshot of the production machines, including:

1. All system files
2. Configuration files
3. Database information
4. Database Archiving.
5. Attachments files.

The database server is configured as a database in archiving mode, such that it can be restored to the latest commitment point. Backups, i.e., snapshot files are stored directly in the different data centres, for a minimum of one month. Surecomp monitors the backup process and ensures the backups are successfully completed. AWS Data Centre can be changed related to the user's location.

Disaster Recovery

For European customers Surecomp uses AWS data centre for Disaster Recovery. In the event of a serious failure, Surecomp ensures that the production system is restored to the last known fully functional state, as expeditiously as possible. This may involve a restoration from backups in the event of any data loss or corruption.

Multi-Tenant Data Management

All tenant related data is stamped with the tenant organizational ID which is included in the token granted upon authentication. All data accesses are using the tokens post authentication to ensure data segregation.

Surecomp

RIVO DATA INTEGRATION

In general, there are several different ways to integrate separate but related application systems at the data layer. For example, any number of apps can access a single shared database and efficiently manage data in real time. In contrast, when each app must maintain its own database, or when you want to import or export large amounts of data, mechanizing the transfer of data among pertinent systems helps preserve the consistency and quality of data across the entire organization.

OPEN APIS

At the core level, the RIVO Platform has open APIs (based on industry-standards such as REST/JSON) that you can use to integrate RIVO endpoints with external endpoints such as apps or enterprise integration hubs.

General purpose data integration APIs support applications that need to work with the core data managed by RIVO.

Data integrations via REST/JSON APIs

Special purpose data integration APIs support applications that need to work with

peripheral data models in RIVO, or data managed by other Surecomp's platforms such as DOKA-NG and IMEX.