# Technical Overview

Management Console, Mobile Auditor

And Enterprise Intelligence

Q1 2020

rizepoint

2890 East Cottonwood Parkway, Suite 250
Salt Lake City, UT 84121
(801) 285-9810

# Contents



# 1 Executive Summary

This document summarizes the technical architecture of RizePoint Technology Group's cloud-based software and mobile device applications. It provides an overview of its physical infrastructure, security safeguards, backup strategy, and disaster recovery plan. This document assumes a relatively high level of technological expertise and is provided to answer questions from vendors or prospective RizePoint customers.

# 2 Application Design

## 2.1 Three Components

The RizePoint product suite consists of three components:

- Management Console
- Mobile Auditor
- Enterprise Intelligence

### 2.1.1 Management Console

Management Console is a cloud-based application accessible from any browser with Internet connectivity. It communicates with our in-house database and a data warehouse hosted on RizePoint's internal Data Center servers. *See 3.1 Data Center*.

Management Console is built using Microsoft technologies including:

- Windows Server
- SQL Server
- Active Directory
- Internet Information Server (IIS)
- SharePoint
- .NET Framework

### 2.1.2 Mobile Auditor (MA)

Mobile Auditor is developed in HTML5 using a hybrid application technology which yields native implementations for iOS, Android, Windows App, and Web devices. The iOS, Android, and Windows App versions are designed to run in a

disconnected state. Supported devices and corresponding system requirements are regularly updated in the RizePoint Online Help file—accessible from within the Management Console.

#### 2.1.3 Enterprise Intelligence

Enterprise Intelligence uses the MicroStrategy® Business Intelligence suite. It is built on an industry standard data warehouse on top of which RizePoint also allows access through an Application Program Interface (API).

### 2.2 Customer Sites

Each RizePoint customer receives a web site and database separate from those of all other customers:

- A Production site with a customer-specific URL.
- An optional "Staging" site with its own URL that allows for the testing of configuration modifications, and previewing of new features prior to changes being introduced into production. Upon request, a production site's database may be duplicated to the staging environment. This is known as a "Staging Site Refresh" and results in the staging site being a point-in-time mirror of the production site.

#### 2.2.1 Domain Names

RizePoint customers receive a subdomain name configuration ending in *.RizePoint.com*. Example: *abccompany.RizePoint.com*. Custom domain names are also available.

### 2.3 Customizable Configuration Options

RizePoint applications use a single code base that provides configuration options to meet the needs of each customer's implementation. Configurations include security settings, management structures, account fields, audit forms, scheduling, and others.

### 2.4 Integration of Corporate Systems and Data

Data is generally loaded into the RizePoint system via web browsers, mobile devices, and data feeds. Once data is in the system, it is processed and prepared for reporting. *See Section 3.2* for a logical network diagram that illustrates data flow.

### 2.4.1 REST API

RizePoint provides a feature rich REST (Representational State Transfer) API for use in integrating various technologies and systems. This API provides support for configuration, User management, Data Import and more. Documentation for the REST API is available at demo3.rizepoint.com/rizepointapi/ui/index. Customers can use a version of the documentation with a built-in sandbox at their personalized URL (http://'yourcompanyname'.rizepoint.com/rizepointapi/ui/index)

### 2.4.2 Importing and Exporting Files

RizePoint supports the integration of corporate systems and data by importing and exporting XML or CSV files via an FTP site. This process synchronizes the most common forms of corporate data including:

- Users and Security
- Locations and Management
- Audit Results and Corrective Actions

# 3 Enterprise Architecture

## 3.1 Data Center

RizePoint production infrastructure is hosted at a third party, enterprise class data center in Salt Lake City, Utah which meets the SSAE 16 Auditing Standard. The hosting facility is secured and protected using best in class, physical, operational and technical safeguards. More details about the RizePoint data center can be found in the document *"Security Policies and Practices"* available at trust.rizepoint.com or by request from RizePoint Customer Support.

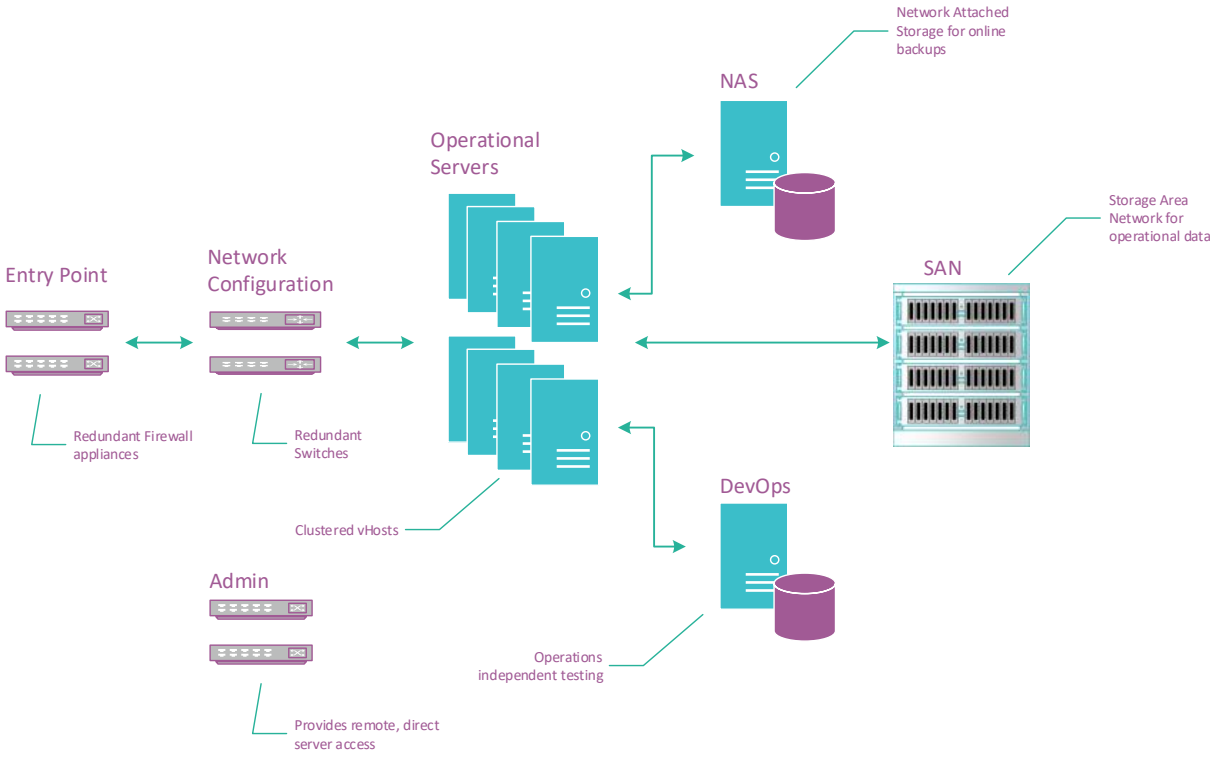


*Figure 3.1 Data Center – Physical Configuration*

### 3.1.1 Virtual Environment – Customer-Facing Operations

Figure 3.1.1 illustrates the high-level overview of the RizePoint virtual environment and customer-facing operations. The virtual manager determines where in the data center a given virtual server is running at any point in time.

- Web applications, database manager instances and utilities execute in this environment, but store their data on a SAN.
- Web applications use a transactional database. MicroStrategy (MSTR) and Management Dashboards (Tableau) use a reporting database.


*Figure 3.1.1 Virtual Environment – Customer-Facing Operations*

### 3.1.2 Virtual Testing Environment

Figure 3.1.2 provides a high-level diagram of the virtual testing environment. This environment provides the following:

- An application build server. It is not clustered with any customer-facing server.
- Separate web applications and the database manager instances which provide support for development and test execute in this environment, and store their data here.
- This environment allows for the testing of customer-specific implementations without impact on the operational environment.
- Deployments are tested in this virtual environment prior to customer updates.

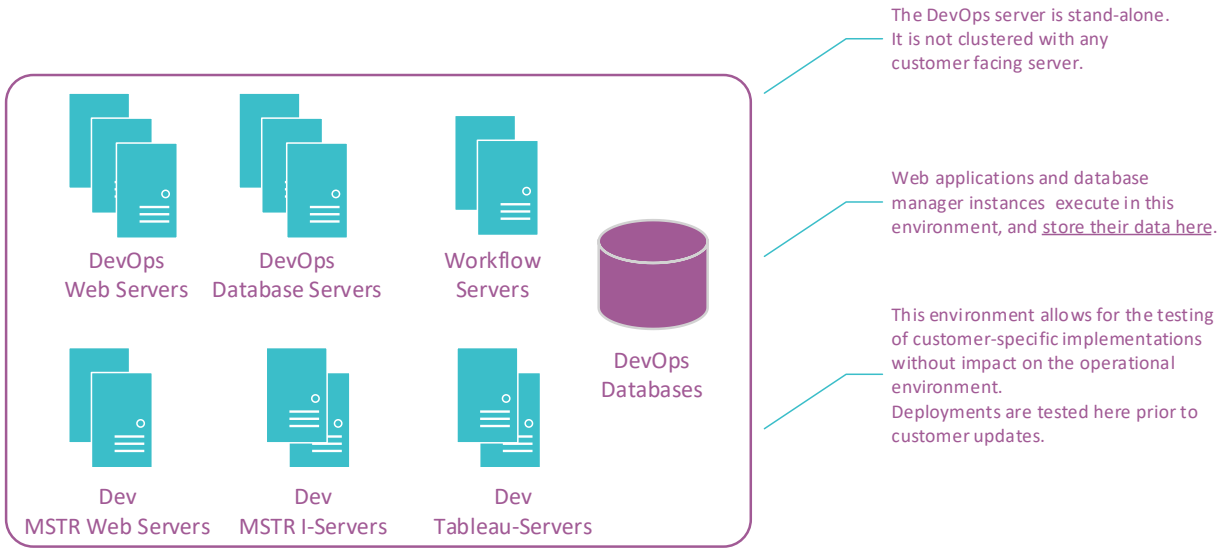


*Figure 3.1.2 DevOps – Virtual Testing Environment*

## 3.2 Logical Network Diagram and Data Flow

Figure 3.2 illustrates the data flow within the RizePoint cloud-based system including areas where customer data is transitory vs. persistent.

RizePoint applications require access to IP ports 80 and 443 over customer networks to establish communications with the hosted portions of the application. RizePoint supports use of its applications over Virtual Private Network (VPN)

connections.

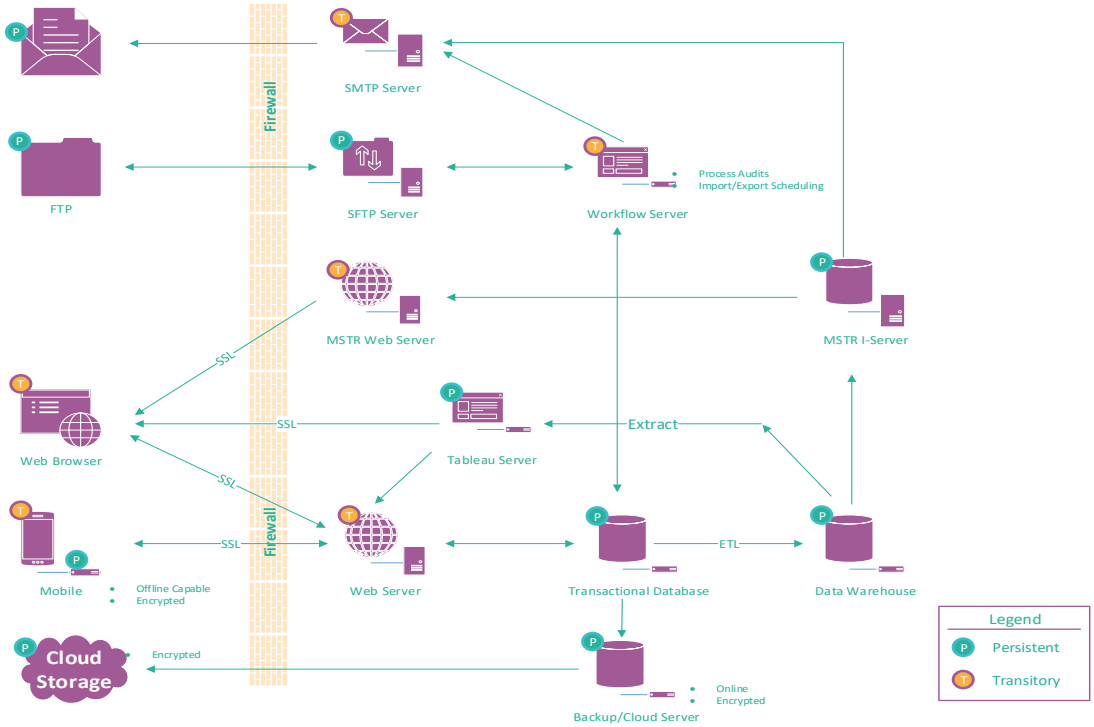


*Figure 3.2 Logical network diagram including data flow*

# 4 Software Development Lifecycle (SDLC)

RizePoint ascribes to the principles of the "Agile Manifesto", which highlights the importance of delivering reliable working software to customers on an ongoing basis. In particular, the organizational design of the engineering group is built around adaptability and responsiveness. Engineers are responsible for both developing and maintaining RizePoint functionality, to build pride-of-ownership and a commitment to quality.

Development engineers, product managers and designers are organized into teams which work in two week iterations. An iteration is a set period of time during which RizePoint develops new features, addresses issues and tests changes. Development and testing systems are isolated from production systems.

## 4.1 Version Control

Source code and development work items are managed using Microsoft Team Foundation Server (TFS) allowing a direct alignment of specifications, source code changes, and application builds.

All application code is reviewed by at least one additional engineer, and a Change Control Board authorizes all deployments of new code to production environments.

## 4.2 Release Schedule

RizePoint releases major new features and capabilities three times per year (Generally in February, June and October). Service packs for customer-specific enhancements as well as emergency issue updates are released monthly.

Release Notes providing the details of each release are distributed through the published Release Notes topic in the RizePoint Online Help—accessible through the RizePoint Management Console.

Updates are released first to the optional staging sites, then to production sites. Most features are optioned on or off giving customers control over when and how they choose to introduce new functionality.

### 4.2.1 Releases of Mobile Auditor for iOS, Android and Windows Apps

The iOS, Android and Windows App versions of Mobile Auditor are distributed via the Apple App Store, Google Play and the Windows App Store respectively. These apps are updated on an as-needed basis. While we attempt to align them with our monthly release schedule, they are not dependent on the general release schedule and will be deployed through the respective app stores as needed.

### 4.2.2 Release of Mobile Auditor for Web

The Web version of Mobile Auditor is updated as needed and is released in sync with Management Console.

# 5 Security

## 5.1 Enterprise Security Office

The RizePoint Enterprise Security Office (ESO) is chaired by the CTO (Chief Technology Officer) and consists of the Director of Information Technology and Principal Architect. Under the authority of the ESO, RizePoint maintains administrative, physical and technical safeguards to endeavor to protect its network and systems from security risks. RizePoint data protection policies and procedures are then managed by the RizePoint IT team and Data team.

## 5.2 Compliance Environment

The data held at the RizePoint hosted data center does not contain Payment Card Industry (PCI), Personal Health Information (PHI), or Personally Identifiable Information (PII) data. Instead, the data consists of configurations, account (location) data such as property addresses, names of staff associated with accounts, and the results of audits of those accounts.

The data stored in RizePoint systems is confidential business information where the primary concern is isolation of one customer's data from another's and protection from external threats.

## 5.3 Security Documentation

RizePoint publishes an exhaustive review of all enterprise safeguards in the document *"Security Practices and Policies"*, available at trust.rizepoint.com or by request from RizePoint Customer Support.

# 6 Backups and Data Recovery

The RizePoint backup strategy combines complete and incremental backups ensuring a high level of fidelity in backup options. System backups are not customer-specific. Backup and recovery software verifies and validates every backup and sends alerts if a problem is detected during the process.

## 6.1 Backup Frequency

Full production and staging file (database and content storage) backups of every RizePoint customer site are created to disk on a weekly basis. Daily differentials from the complete backup date to 15 minutes. Transaction logs are backed up every 15 minutes.

## 6.2 Backup Retention

RizePoint maintains data at both onsite and offsite locations. All database backups are encrypted. Figure 5.3 below shows the level of fidelity of data kept onsite and offsite by date range:

| | Previous 2 Weeks | Previous 3 Weeks | Previous 6 Weeks | Previous 6 Months | 2 Years |
|---|---|---|---|---|---|
| Onsite | 15 minutes | Daily | Weekly | --- | --- |
| Offsite | Daily | Daily | Monthly | Monthly | Monthly |

*Figure 5.3: Level of fidelity by date range*

## 6.3 Data Recovery

If service must be restored to a customer site, the process can be initiated in two ways:

### 6.3.1 RizePoint-Initiated Restoration:

In the unlikely event that RizePoint redundant systems fail and a customer experiences data corruption or loss, RizePoint will restore customer data to the most recent backup. The Account Manager will periodically update the customer during the restoration process.

### 6.3.2 Customer-Requested Restoration

At the request of the customer, RizePoint can initiate a restoration of customer data to a previous state. The Account Manager will periodically update the customer throughout the process.

### 6.4 Data Recovery Testing

RizePoint backup and recovery software verifies and validates every backup. Additional tests are performed in conjunction with the RizePoint Disaster Recovery testing policy, detailed in the RizePoint published document *"RizePoint Disaster Recovery Plan"*, Section 5, available at trust.rizepoint.com or by request from RizePoint Customer Support.

# 7 Disaster Recovery

RizePoint has developed and maintains a robust Disaster Recovery plan in the event of simultaneous loss of operations at both the Primary Data Center and corporate facilities. This recovery plan uses encrypted offsite data storage, copies of all virtual machines, as well as process and inventory documentation to restore service from a public cloud hosting location. Full details of this plan are published and available in the document *"RizePoint Disaster Recovery Plan"*. This plan can be viewed at trust.rizepoint.com or by request from RizePoint Customer Support.

### 7.1 Disaster Recovery Overview

- The RizePoint Disaster Recovery Plan is reviewed and revised quarterly by key RizePoint personnel. During a disaster recovery scenario, RizePoint will use cloud backups to restore customer data to a temporary environment. Limited functionality will be available to RizePoint customers while full restoration of services is established.
- Customers will lose all connectivity to their site while the data center is offline. Depending on the severity and magnitude of the disaster, time to restore full operations will vary. The greatest potential data loss for any given customer is one day's worth of data.
- Offsite backups are stored in the cloud mitigating the effects of a regional disaster. Because temporary environments are hosted in the cloud, a disaster recovery period will not be affected by one individual geographic disaster.
- RizePoint phone and email services are hosted in the cloud; thus, allowing a customer's Account Manager to provide status updates as needed.

# 8 Conclusion

This document is reviewed quarterly and updates made to provide an up to date window into the operations of the RizePoint platform. RizePoint operates an enterprise grade facility and regularly drills on best practices to ensure the highest quality of service for customers. This document and all other efforts by the RizePoint technology group represent our ongoing commitment support customers in keeping the promise of their brand.

## 8.1 Further Information

Additional information about the RizePoint Disaster Recovery approach can be found in the document "*RizePoint Disaster Recovery Plan*".

A more comprehensive description of RizePoint security controls can be found in the document "*RizePoint Security Policy and Procedures*".

For further information about this Technical Overview, or to request additional documentation, please visit trust.rizepoint.com or contact your RizePoint Sales Representative.

# 9 Appendix A – Single Sign-On Requirements

This section details the RizePoint Single Sign-On implementation and data requirements for customers integrating an external identity provider to RizePoint hosted services.

Using the public key provided by your identity provider, the RizePoint Single Sign-On provider will validate the message integrity and configure conditions before checking the supplied username against the RizePoint identity repository for access to RizePoint hosted services.

## 9.1 Supported Protocols

RizePoint utilizes the SAML protocol to validate identity assertions made by external identity providers.

## 9.2 Required Message Properties and Attributes

| Attribute | Description |
|---|---|
| Destination | The page destination within the RizePoint hosted service used to authenticate and authorize access to the system (e.g. https://hosted.RizePoint.com/WebApp/Common/SfLoginMenu.aspx?sso=true)<br><br>This attribute value must be included within the Response element of the SAML message. |
| NameID | The value of this assertion must be the same as the RizePoint user's unique username. It can be up to 50 alpha numeric characters.<br><br>This value must be included within the Attribute Statement identity claim of the SAML message. |
| NotBefore | A UTC timestamp (e.g. 2015-01-01T01:00:00Z) used to establish the period for which the identity claim will remain valid.<br><br>This value must be included within the Conditions statement of the SAML message. |
| NotOnOrAfter | A UTC timestamp (e.g. 2015-01-01T01:00:00Z) used to establish the period for which the identity claim will remain valid.<br><br>This value must be included within the Conditions statement of the SAML message. |

*The following table outlines the specific SAML 2.0 message properties and attributes required for integration with the RizePoint Single Sign-On provider.*

## 9.3 Authentication and Authorization Process

The RizePoint Single Sign-On provider is triggered through the designation of the "sso" attribute upon access to the site login page. The request is then examined for posted content that includes the SAML message asserting the identity.

If the message is present and the site has a public key configured to validate the assertion, the message is validated prior to resolving the message expiration. If the message is valid and has not expired, the identity is then used to resolve an account within the RizePoint hosted services by username. If the account has appropriate permissions and configuration to access the system, the system will redirect the user to the system configured landing page for the user to begin utilization of the RizePoint solution. If the account cannot be resolved, has insufficient permission or configuration, the user will be redirected to the standard log-in page.