Technology Specifications

Table of Contents

1. OVERVIEW

Rethink is a HIPAA-compliant system specifically designed for behavioral health service providers/agencies to streamline treatment planning and insurance reporting, collect behavioral data, train therapeutic staff, involve parents and practice management. The below is a resource providing technical overviews and specifications for the Rethink platform. Specifications are grouped by Technology and Infrastructure, Hardware and Operating System Recommendations, Web Browsers, Connectivity, Network Configurations and Security.

2. TECHNOLOGY AND INFRASTRUCTURE

2.1 Technologies

The Rethink solution is delivered over the Internet using virtual machines (VMs) for web and database servers, Azure web apps to host web applications, and Azure blob storage for content storage. Our applications combine both dynamically generated application features and statically published educational content. Rethink web applications are developed using the latest development practices and technologies. Customer-facing solutions are developed in ASP.NET, MVC Framework, C#, AngularJS, and SQL technologies using sophisticated design principles and some of the best Web 2.0 functionality available.

2.2 Facility

The Rethink solution is hosted in the cloud, using a Microsoft-managed datacenter in East US 2 region, state of Virginia.

2.3 Server Technology

Rethink hosts its applications and services on Intel cloud-hosted server hardware on Windows Server 2012 R2 machines. Rethink videos are hosted by iMediaSee and BrightCove.

2.4 High Availability

All servers are set up in a high-availability fashion to ensure ultimate up-time for our customers. An active server takes in all the traffic and a warm backup server is on stand-by with continuous synchronization. Should one server go down at any one point in time, the second server automatically kicks in without any manual intervention.

2.5 Load Balancing

Hardware-based load balancing distributes end-user connections across a "farm" of servers. This enables balanced load, fault tolerance and redundancy of the applications. The Rethink load balancing solution is provided by Microsoft Azure.

2.6 Content Delivery Network

Rethink hosts our educational content in Azure blob storage. Azure storage automatically replicates data to help guard against unexpected hardware failures and make sure it's available when you need it. Content is triple-redundant with an option of geo-redundant storage across hundreds of countries.

2.7 Data Back-up

Rethink employs multiple levels of backups to ensure your data is safe. Full backups of data are created on a nightly basis with transactional backups taken every hour throughout the day. Back-ups are stored in blob storage which is triple-redundant, creating 3 copies of each backup taken. Copies of backups are also rotated to off-site facilities to ensure the highest level of protection for customer data.

2.8 Monitoring

Rethink hardware and software is continuously monitored on a number of levels. Microsoft facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. Automatic web-tests are employed running every 30 seconds, to check on site

availability and the user load- and application-response times. Our monitoring systems are connected to an automated alerting system, which notifies Rethink operations staff of any noted issues.

3. Hardware and Operating System Recommendations

The Rethink solution functions on a wide variety of computer platforms, including dedicated desktop or laptop computers, thin client installations and mobile devices. This section describes the basic hardware and operating system recommendations for customers accessing the Rethink platform.

3.1 Mac OS X

OS Version	10.5, 10.6, 10.7, 10.9, 10.10, 10.11
Memory	256 MB or greater

3.2 Windows XP, 7, 8

OS Version	Windows XP Service Pack 2, Windows 7/8
Processor Speed	500 MHz or greater
Memory	256 MB or greater

3.3 Windows Vista

OS Version	Windows Vista
Processor Speed	750 MHz or greater
Memory	512 MB or greater

3.3.1 Use of Older System Configurations ad Software

The system recommendations listed in this document reflect the software and computer system configurations that Rethink actively supports. Please be aware that older browsers with older operating systems do not recognize the security certificate installed. As such, for any schools still using Windows XP or below, Internet Explorer is not an option. As an alternative clients with Windows XP can use any other browser like Chrome or Firefox. For Windows Vista or above (i.e. Windows Vista, 7, or 8) Internet Explorer can continue to be used. This is only a problem with very old operating systems and Internet Explorer as a browser.

3.4 Mobile

iPhone	All: iPhone 6+, iPhone 6, iPhone 5s, iPhone 5, iPhone 4s, iPhone 4, iPhone 3gs
iPad	All: iPad Air, iPad mini2, iPad 3, iPad 2
Windows phone	Nokia Lumia
Android phone	Samsung Galaxy (all phones): Galaxy s5, Galaxy s4, Galaxy s3, Galaxy s2, Galaxy s, Galaxy Note3, Galaxy Note2, Galaxy Note, Motorola Razr and Droid Razr, Google Nexus (all)
Android tablets	Amazon Kidle Fire (all), Google Nexus, Samsung Galaxy tab, Samsung Galaxy Note

3.5 Display

Rethink solution supports various resolutions and many screen sizes.

3.6 Sound

Sound is an important part of the Rethink solution to be able to view our videos. Hardware support for sound playback is required for lesson videos. We recommend the availability of headphones for use in public computing scenarios.

4. WEB BROWSERS

Rethink fully support a wide variety of properly configured modern browsers. Older generation browsers will also very likely function properly with our service if the browser supports CSS, JavaScript, Java and the Flash plug-in. This section lists the supported and recommended browser for users of the Rethink platform.

4.1 Recommended Browsers

The latest version of web browser software includes the most comprehensive security, usability and web site rendering functionality. Rethink routinely tests the latest release of the major browsers offered for the Windows and Mac OS X operating systems. Consequently, we recommend these browsers as the best option for customers looking for a secure, successful experience with the Internet generally and the Rethink solution in particular. As of the release of this document, these are the recommended browsers for use of the Rethink solution.

For customers using the Microsoft Windows operating system:

- Firefox 30 and subsequent versions
- Chrome 35 and subsequent versions
- Internet Explorer 11, 10

For customers using the Mac OS X operating system:

- Safari 8, 7
- Chrome 35 and subsequent versions
- Firefox 30 and subsequent versions

4.2 Supported Browsers

Most browser software released in the last 3-4 years is fully supported by the Rethink platform. Supported browsers represent software known to function properly with the Rethink solution. We strongly recommend that customers deploy more recent versions of these browsers as subsequent releases typically contain security fixes that preclude potential compromise of computing systems.

For customers using the Microsoft Windows operating system:

- Firefox 10 and subsequent versions
- Chrome 15 and subsequent versions
- Internet Explorer 9
- Opera 15 and subsequent versions
- Safari 4 and subsequent versions

For customers using the Mac OS X operating system:

- Safari 6.1, 6
- Chrome 15 and subsequent versions
- Firefox 10 and subsequent versions
- Opera 15 and subsequent versions

Notes on supported browsers:

Please be aware that older browsers with older operating systems do not recognize the security certificate installed. As such, for any clients using Windows XP or below, Internet Explorer is not an option. As an alternative clients with Windows XP can use any other browser like Chrome or Firefox. For Windows Vista or above (i.e. Windows Vista, 7, or 8) Internet Explorer can continue to be used. This is only a problem with very old operating systems and Internet Explorer as a browser.

4.3 Browser Configuration

All web browsers must have the following functionality enabled to properly access the Rethink platform.

- JavaScript enabled

- Cookies enabled
- Pop-up blockers turned off for Rethink domains

4.4 Browser Plug-Ins

The Adobe Flash Player plug-in is needed on desktops for lesson videos to stream. This plugin is not needed for mobile devices, as RTSP based streaming is used. Adobe Flash Player is freely available for download from the Adobe website at http://www.adobe.com/products/flashplayer/. This site will validate the currently installed plug-in version and enable users to upgrade their Flash Player to the latest release version of the software.

5. CONNECTIVITY

A high-speed connection to the Internet is recommended for better the user experience. However, Rethink platform can still be used via a dial-up connection. We engineer our systems to minimize the required bandwidth for client users making extensive use of caching, compression and HTTP protocol technologies. Whether dedicated or shared, the connection must be stable with minimal packet loss and latency, and no route flapping.

6. NETWORK CONFIGURATIONS

6.1 Rethink Domains

Access to the following domains and network address blocks should be unrestricted for your user population.

- Rethinkfirst.com
- Rethinkautism.com
- Rethinkbenefits.com
- Rethinkbehavioralhealth.com
- Rethinkbh.com

6.2 Third-party Domains

Rethink lesson videos are currently hosted by iMediaSee. Training videos are hosted on BrightCove servers. Accordingly, the following domains will need to be whitelisted:

- *.brightcove.com
- fstream.imedisee.com

6.3 Network Ports

Allow content from our servers to arrive on your client computers through your router, firewall, and/or proxy server over the following ports:

- 80 (for HTTP traffic from our Web servers)
- 443 (optional - for SSL traffic from our secure Web servers)
- 1935 (for iMediaSee video stream)

The following diagnostics page - http://www.imediasee.com/support/flash-diagnostics - can help determine which firewall ports need to be opened in order for the videos to stream.

7. SECURITY

All Rethink domains are protected by SNI SSL certificate to ensure encryption for data in motion. Database level encryption using Symmetric Key AES 256 algorithm encryption is in place as well for securing data at rest. SNI certificates are updated regularly for all Rethink domains as well as for API. Multiple security steps have been taken to ensure a secure service to our clients.

7.1 Remote Access

Securing access to Rethink Virtual Machines are maintained on multiple levels. Remote connection to Rethink servers is tightly secured by using tunneling and encryption protocols. In addition, the following best practices are followed to reduce exposure to attacks.

7.1.1 Username / Password

Complex usernames and passwords are set up for all servers, with a requirements of a minimum 8 character long with 3 of the following: a lowercase character, an uppercase character, a number, a special character.

7.1.2 Endpoints

Endpoints are only added on a need basis and eliminated when no longer in use. For Remote Desktop, the default port of 3389 is not used, but rather changed to help reduce exposure. All servers are set to automatically generate a random public port, which holds true for all existing servers, as well as for any new ones spun up.

7.2 Internal Load Balancing

Internal load balancing (ILB) enables Rethink to run highly available services behind a private IP address which is accessible only within a cloud service or Virtual Network (VNet), giving additional security on that endpoint. As a security enhancement, Rethink application tier and backend databases are run behind an ILB so that they are not exposed to public Internet, but still offer high availability through load balancing.

7.3. Separate development / testing / production environment

Development and testing of web applications is done on servers isolated from the internet, and do not use or connect to real life data and databases. This stands true for both server/applications and any data sources used.

7.4 Web Application Content

The web application and website files and scripts are on a separate partition from that of the operating system, logs and any other system files to provide for additional security. Public available content is stored in blob storage. Writing to blob storage, however, is restricted to Rethink IT team only.

7.5 Permissions, Privileges and Network Controls

File and network service permissions are limited to authorized Rethink IT staff only and controlled via Windows Azure Subscriptions. The following network vulnerabilities and controls are in place:

7.5.1. Interception Controls

- Physical access controls at data centers is limited to Microsoft personnel only
- Central office machines of IT staff are password-protected
- Upon termination of employees, all passwords are updated

7.5.2 Availability Controls

Redundant paths are currently set up for every resource as well as an access point and automatic routing to switch traffic to the available path without loss of data or time. This ensure optimal up-time to Rethink clients. This includes:

- Fault-tolerant production environment with multiple servers set for the application tier (currently served by a farm of 10 web servers) and backend databases (serviced by 2 Always-On servers)
- Automatic routing to switch the traffic upon failure of any web or database server.

7.5.3 Access / Entry Point Controls

See Section 7.1.2 – Endpoints. Additional security measures include:

- Firewall
- Physical separation of back-end servers from public-facing interfaces
- Antivirus software installed on all servers and workstations
- Electronic sessions are terminated after 50 minutes of inactivity

7.6 Monitoring/Logging

All Rethink applications and virtual machines are deployed in Azure, and are enabled with a set of operating system security events. Azure logs administrative operations, including system access, to create an audit trail in case unauthorized or accidental changes are made. Audit logs can be retrieved for view access and usage reports. Automatic email alerts are set up for head IT staff based on predetermined rules.

7.7 Data Encryption

7.7.1 Data-At-Rest

- Database level encryption using Symmetric Key AES 256 algorithm encryption, encrypting all PHI data and prevents database level attacks
- Protection of sensitive data in backup media and when interacting with raw database tables/objects

7.7.2 Data-In-Motion

- TLS 1.2 certificate with SHA-256 (SHA-2) hash algorithm that provides encryption for data in motion and includes built-in controls to prevent tampering with any portion of the encrypted data
- Protection of web application data from unauthorized use and modification utilizing secure channels during transmission of data between client and server
- Sensitive data is never transmitted via URL arguments. It is stored in a server-side repository or within a user's session
- All requests to the domain are sent over HTTPS using IIS redirects
- Sensitive data is never cached or persisted, preventing potential data leakage issues at the client or intermediary proxies