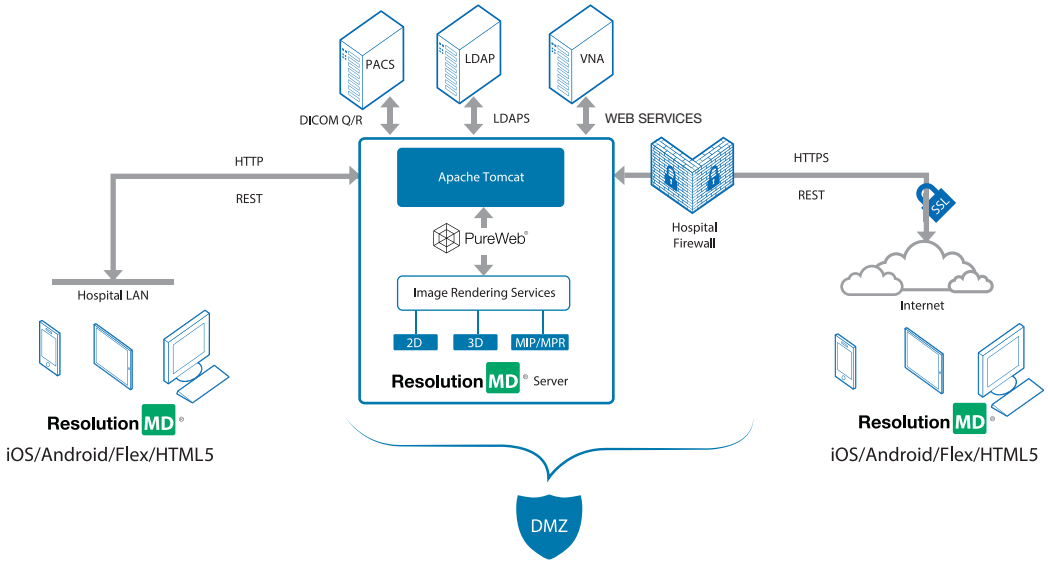
ResolutionMD® Security Overview

Ensuring the security of information and applications is a critical priority for all organizations, particularly those in the field of healthcare. When operating in an environment of thorough security practices, the architecture, features and services of the ResolutionMD® enterprise image-viewing platform enable medical images and information to be securely and conveniently accessible to users from anywhere in the world, without compromising network or information security.

1 Sample Architecture



Above is a high-level architecture of a single instance of the sample architecture with typical infrastructure components:

- *PureWeb® software is a platform by Calgary Scientific upon which ResolutionMD software is developed. PureWeb provides for the communication layer between the web server (Apache Tomcat) and the ResolutionMD services.*
- *The Picture Archiving & Communication System (PACS) is the back-end data store in DICOM format.*
- *The vendor neutral archive (VNA) is the back-end store for DICOM and NON-DICOM data.*
- *The iOS/Android/Flex/HTML5 areas represents the various client viewer applications that can access ResolutionMD software from within the hospital network or over the Internet.*

The ResolutionMD server is typically intended to be installed within a data center in close network proximity to the back-end data store (and that's generally true for the LDAP security systems as well). This to minimize the network distance over which data transfer takes place between ResolutionMD and the data source. ResolutionMD can also be fully deployed in private, public, and hybrid cloud architectures.

Additionally, the web server component and imaging components are ideally located on the same server to reduce performance issues related to latency. From a security perspective, the imaging processes on the ResolutionMD server are short lived. They are only initiated for each imaging session and have an inactivity timeout configuration to control the active life of these processes. The processes provide no means of writing or changing data locally and only facilitate a save request to the back-end data source in the case of a secondary capture. The imaging components make no request to alter data, either locally or in the back-end data source.

2 Server Security

Physical and Virtual Infrastructure

ResolutionMD® software is a server-based application which is accessible via a web browser running on a workstation, PC, laptop or notebook computer or via HTML5 or a native mobile iOS or Android application on a mobile device. Given that the ResolutionMD image viewer is server based, paying close attention to infrastructure is among the simplest facets of security that can be implemented to protect ResolutionMD resources from unwanted access.

Network

IT security best practices dictate that all network, servers and devices be deployed and configured in a manner which minimizes the opportunity for and the impact of external and internal attacks. Firewalls are typically a critical part of this security infrastructure. Depending on which user communities are accessing the ResolutionMD application and where they are located, the ResolutionMD server(s) can be deployed within the corporate network behind the firewall or within a DMZ, separated from both an internal network and the Internet.

ResolutionMD Server & OS

The hardware and operating system platform required for the most current version of ResolutionMD software is based on the support for two primary components: select NVIDIA Graphics Processing Units (GPU); and the operating system, Red Hat Enterprise Linux (RHEL) Enterprise Server (ES) or Windows Server. It is the operating system that in particular requires specific attention to ensure that it is secure. It is recommended that ResolutionMD and supporting applications be operated on a dedicated server platform. This greatly reduces performance and security risks from malware or viruses that maybe reside in other software applications.

ResolutionMD Server Application

There are three privilege levels or roles defined for secure access into the ResolutionMD software. The Server Admin role enables access to all application configuration and administration capabilities on the system. The Server Monitor role enables access to a subset of application monitoring and log capabilities and finally a User role enables viewing of images. Each level is protected and requires a valid user ID / password for access.

Server Application Administration

Administrative functions of ResolutionMD server are only accessible by those with the knowledge of the appropriate URL(s) to access those functions. Additionally, login credentials are required to permit further access to the administrative areas of the application.

The ResolutionMD system includes the ability to configure timeout and user session control parameters so that opportunities for misuse of the system via intentional acts or user carelessness are minimized.

User Account Authentication

The ResolutionMD software application does not include a database of users, but instead leverages a hospital's existing directories and databases for authentication. Standard LDAP and Secure LDAP authentication, as well as proprietary authentication mechanisms embedded into partner specific ResolutionMD plug-in modules, are supported.

Activity Logging

Once a user has successfully authenticated into the ResolutionMD system, all user activity is logged. Within the log, all sessions are actively recorded by user ID and details on what information has been accessed.

Data & Resources

Data is typically at the core of security concerns within system infrastructure and in the case of medical systems, Personal Health Information (PHI) data is of particular concern. However, no patient data is persistently stored either on the ResolutionMD server or on client devices which access the software. This greatly reduces potential PHI security concerns, eliminating the requirement to actively manage the security of data in these domains.

Instead of caching requested studies on the server, ResolutionMD software uses a real-time query mechanism to pull user-specified images into server memory only for the duration of the image-viewing session. This data is used by the server for the duration of the session to render 2D, 3D, and MIP/MPR images. Only rendered images (i.e., not DICOM data) are ever transferred to the client devices for viewing. Once a user ends their session or selects alternate images for viewing, the prior image data no longer persists on the server and rendered images no longer persist on the client.

3 Client Security

The Flex and HTML5 ResolutionMD client applications are dynamically loaded from the server at runtime through the use of a URL. The iOS and Android ResolutionMD clients are native applications that are both lightweight and offers high-end user performance.

Security has been part of the design of the ResolutionMD client since its inception:

1. No patient data is actually left persistent on the client mobile device or browser session. Once a session times out or is ended, the data in memory is deleted and no written data is persistent on the device. If a phone or tablet is lost or stolen there is no concern about patient data being left behind and accessible.
2. The ResolutionMD server is set up to require users to enter login credentials for production use.
3. The image data, delivered to an end user using HTTPS, cannot be read in transit and can only be interpreted once rendered on the screen of the device. Even study textual meta-data that may be superimposed on the displayed image is delivered in bit format that does not allow for easy interpretation until rendered on screen.
4. The ResolutionMD client is typically further secured with the use of SSL. SSL implemented in conjunction with the ResolutionMD Server ensures that all data transmission between the client device and the server are encrypted so as not to be interpreted while in transit from a network.
5. Optionally, a VPN can be added as a secure conduit through which the end user device can communicate with the ResolutionMD server.