glassbeam™

CLinical Engineering ANalytics (CLEAN™)

IoT Blueprint for Healthcare Industry

Version 1.0, November 2017

TABLE OF CONTENTS

Blueprint Objective

If ever a sector of the economy needed smarter systems to enable optimization of business and operations processes, it's healthcare. The healthcare arena offers untold opportunities to apply IoT and Smart Systems technologies to increase awareness, knowledge, efficiencies and actions.

According to several sources, global healthcare expenditures expanded to over $8 trillion dollars in 2016; capital expenditures for machines, devices and equipment totaled over $350 billion. Healthcare delivery organizations are discovering the many and diverse opportunities that networks, sensors, intelligent machines and software create. The healthcare sector has put significant investment and resources into new technologies for automated diagnostics, remote patient monitoring, medical equipment monitoring and drug and supply chain tracking.

Today, the average 200+ bed hospital has over 250 brands of equipment and devices and the typical hospital patient comes into contact and interacts with over 75 devices per day. The speed and scale at which manufacturers are integrating automation and data analytics into healthcare equipment systems is staggering. These innovations are aimed at revolutionizing the quality, consistency and efficiency of equipment and devices in support of patient care.

But, are users realizing the maximum benefits from these new tools? We think not; but why?

We believe that the clinical engineering heads who are tasked with kinds of analytics are challenged with issues including:

- Lack of single pane glass view to view multi-modality multi-manufacturer solution view
- Poor visibility into operator utilization and benchmark data across operators & procedures
- Lack of analytics on asset utilization and procedures by facilities to justify Capex decisions
- Lack of ability to provide the industry benchmark of 99% or higher uptime availability

Enter Glassbeam CLEAN™ blueprint – Industry's first IoT blueprint focused on Clinical Engineering Analytics. The CLEAN™ blueprint is the industry's first Multi Modality Multi Manufacturer analytics application that allows companies to:

- **Aggregate ALL assets in single portal**
  - o View data from multiple data sources, modalities and frequencies
  - o Drill down to individual modalities
- **Track utilization and Uptime**
  - o Ensure inventory is being used optimally while bubbling up critical issues to maximize uptime
- **Analyze operator efficiency**
  - o View aggregated time taken per procedure type by operators to find gaps in training and effective machine utilization

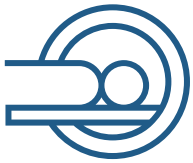
Benefits are several to clinical engineering groups, such as:

- **Assemble a single view** of all modalities and manufacturers such as GE and Siemens
- **Reduce unplanned downtime** and reclaim lost revenues with machine availability > 99.5%
- **Reduce support costs By 20-40%** and improve financial management across entire fleet
- **Make strategic decisions** with better visibility into asset & operator utilization

The Glassbeam CLEAN™ blueprint is a rapid implementation methodology delivered over the cloud in 4 weeks or less. The objective of this document is to provide an overview of the various architecture components required to process machine log data from medical devices such as CT and MRI machines. In addition, it lays the deployment specifics of the agent based architecture to send raw log data from your clinic or hospital to Glassbeam Analytics (hosted on a private or public cloud).

Deployment Architecture

The high level architecture comprises of 4 components:



Medical Modalities

Gateway Server (optional)

Glassbeam Agent

Glassbeam Analytics

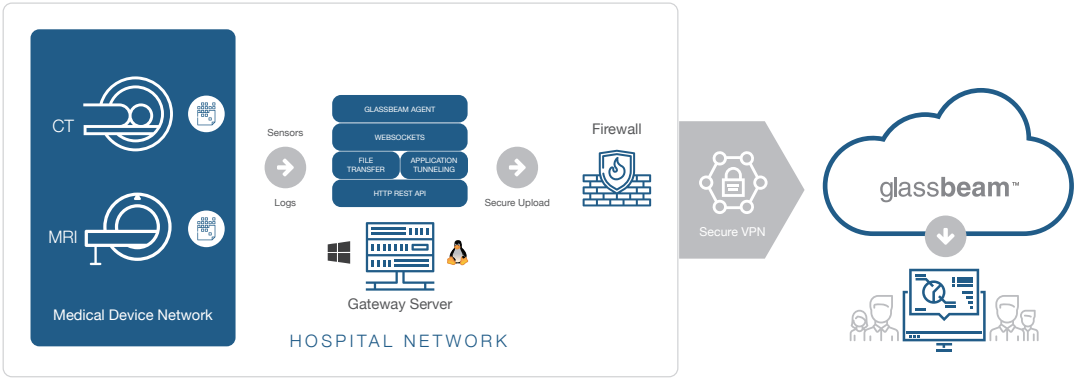
To enable data flow across the above components, the following considerations need to be taken into account.

Connectivity

Security and Compliance

Desensitization

Glassbeam works closely with the IT department of the clinic/hospital to enable each component in the architecture as well as satisfy all the requirements for documentation and compliance.



Medical Modalities

The medical devices, as illustrated above, reside within the hospital's firewall. Based on the device's capability and the hospital's IT policy, the device may or may not be connected to the internet.

The deployment options may change based on the available options at the site to secure internet connectivity. The medical device in this case is assumed to be imaging equipment connected to a Windows or Linux based operating system.

- ✓ SIEMENS Sensation CT
- ✓ SIEMENS Definition CT
- ✓ SIEMENS Somatom Force CT
- ✓ SIEMENS Emotion CT
- ✓ SIEMENS Aera MRI
- ✓ SIEMENS Espree MRI
- ✓ SIEMENS Avanto MRI

- ✓ Optima CT
- ✓ Brightspeed CT
- ✓ Revolution CT
- ✓ HDX Series MRI
- ✓ MR450/750 series MR
- ✓ Pioneer 3.0T MRI
- ✓ Excite 11x MRI
- ✓ DXI CT

Gateway Server

The gateway server is a dedicated Windows/Linux machine that is required in situations where the medical device does not have any access outside the site's firewall. The gateway server, in this case, acts as a proxy with a dedicated secured connection to the Internet via secure protocols or site-to-site VPN connection with Glassbeam Analytics.

A typical Gateway Server configuration would be:

- Intel 4 CPU 16 GB RAM
- Linux/Windows 64 bit OS
- 500 GB Hard disk/space
- JRE 1.7 or higher
- LAN connectivity
- Internet connectivity or VPN

Glassbeam Agent

The Glassbeam agent is a small Java-based program powered by PTC ThingWorx™ that enables data acquisition and secure data transfer to the Glassbeam Analytics cloud. This agent can run either on the gateway server or on the cloud. The agent is configured to watch the FTP directory and periodically picks up all the dropped files, groups them by the device identifier, and securely transfers the data to the Glassbeam Analytics cloud.

Glassbeam Analytics

Glassbeam Analytics is our cloud-based SaaS solution that collects, stores, transforms, and visualizes the data collected by our data collection agent. Glassbeam's key differentiators include:

- Ability to ingest, parse and analyze multi-structured machine log data; the solution goes beyond the simple value provided by analyzing sensor or historical data.
- Much faster time to deployment, which also leads to significantly reduced cost (rapid deployment and reduced man hours).
- Much more granular development of Rules & Alerts when compared to competitors; Complex rules logic allows machine learning model integration into the data workflow
- Overall, Glassbeam can deliver 10x the functionality in 1/10th the time at half the cost of other solutions.

Design Considerations

Connectivity

Internal connectivity within the client's firewall is required in case a gateway server is being setup to aggregate data from all the medical devices. In such cases, the gateway server acts as an FTP server for the medical devices to copy data from the local directories. The Siemens devices support this by allowing its autosupport feature to be redirected to the jump server destination. All GE imaging equipment are Linux machines that support FTP transfer with the requisite credentials.

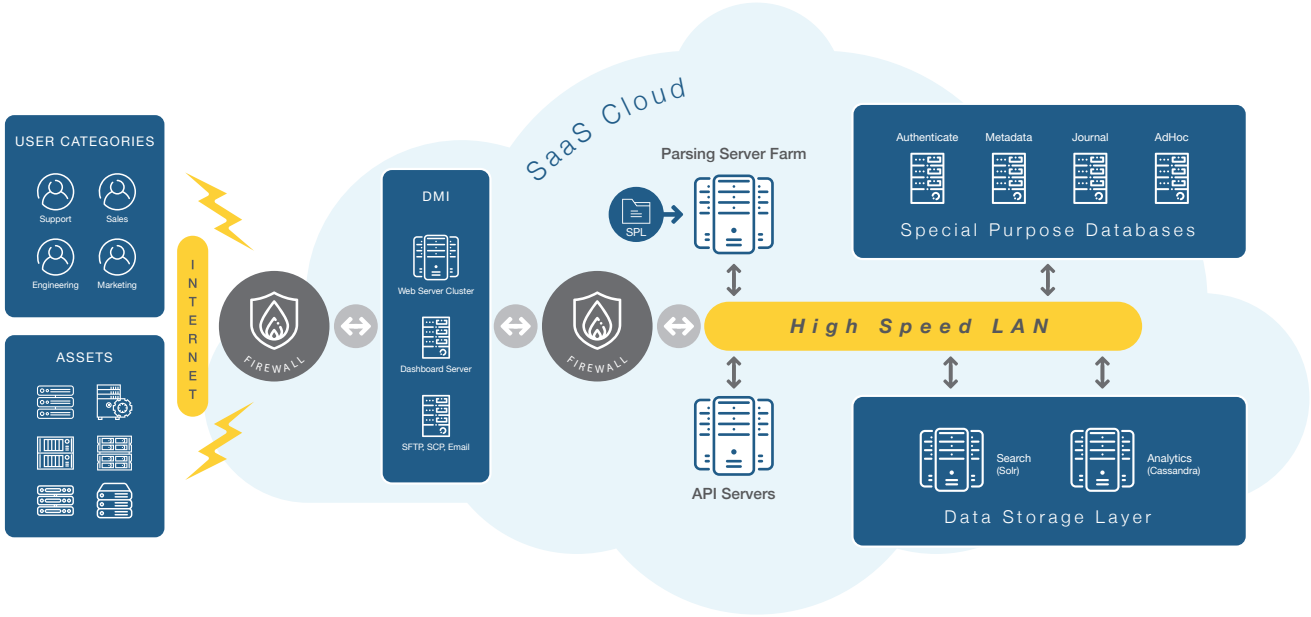
There are 2 broad approaches to achieving end-to-end connectivity:

Internet Connectivity

Possible in case either the individual medical devices or the jump server has access to the internet. In this case, a simple SFTP connection is established between the source and destination.

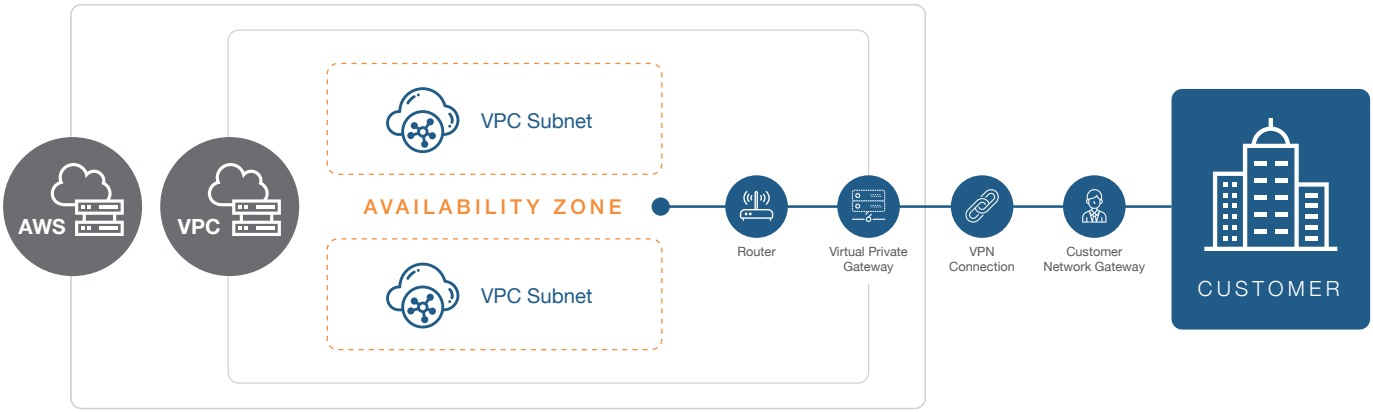
VPN Connectivity

In case there is no direct access to the internet, then a permanent site to the sites' VPN tunnel is established between each medical device or jump server and Glassbeam Analytics. The VPN setup is illustrated below.



Cloud Hosting

Glassbeam works with several leading PaaS/Cloud providers for all data and application hosting needs. Currently all healthcare customers are hosted on Amazon Web Services (AWS) Cloud. From a security perspective, all of our service providers are SAS 70 Type II, PCI DSS Level 1 and European Safe Harbor certified and have data centers and global operations.



Physical security, Data Encryption, Backups, Firewalls, Access Control, Security and Compliance, Data Desensitization

The physical data and infrastructure security is handled several ways:

- All areas within the facility are monitored 24x7x365 by closed-circuit cameras and onsite guards
- The datacenter space is physically isolated and accessible only by administrators of the PaaS provider
- Access is restricted by authorized personnel through biometric two-factor authentication
- CCTV digital cameras cover the entire center, including cages, with detailed 24x7 surveillance and audit logs.

Data Encryption, Backups and Firewalls

Data is stored with 256-bit encryption at rest and 128-bit SSL encryption in transit. In addition, Glassbeam supports configurable Virtual Private Clouds (or Virtual LANs) between servers.

We ensure that all data remains consistent and up-to-date even in the event of an unforeseen disaster. We have a comprehensive backup policy that covers raw log files, processed data, as well as installed software and operating system. Since your data is stored on the cloud, we have the capability to utilize geographically dispersed data centers for remote disaster recovery. Our combination of full and incremental automated backups with zero downtime ensures that the latest data is available at any point in time. Our support staff will regularly monitor the backup process and make sure that recovery is performed in a timely manner.

In addition, firewalls have the following security features:

- Fully-managed, hardened, stateful inspection firewall technology
- Fully-managed Intrusion Detection System (IDS)
- Edge-to-edge security, visibility and carrier-class threat management and remediation utilizing Arbor Networks Peakflow to compare real-time network traffic, immediately flagging anomalies such as:
  - o Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms or botnets
  - o Network issues such as traffic and routing instability, equipment failures, or misconfigurations
- 24x7x365 Firewall, VPN, and IDS support and maintenance
- Dedicated teams to handle reports of security incidents

Access Control

Access to servers is limited to dedicated production support/IT personnel, who can connect through a secure VPN (or SSH) with Endpoint Protection. Endpoint Protection ensures that no malicious software can be introduced through the VPN tunnel. Root access is not provided to anyone except the system administrator. All other authorized users are provided limited application level access.

Stringent security measures are in place at all stages of the employee lifecycle for granting and revoking access to the data. Roles are restricted such that no sensitive information can be copied without leaving a trace. Passwords are changed periodically and complexity levels are enforced. Monthly IT audits are conducted to ensure that the security policies have been enforced.

Security and Compliance

Security is ensured through proper usage of secure data transfer protocols such as SFTP and HTTPS. Compliance parameters are handled by adhering strictly to the current guidelines and polices enforced by the clinic/hospital. Following are some of the compliance artifacts that Glassbeam Inc. has worked with:

- Mutual non-disclosure agreements
- Business associate agreement (N/A for direct sale to hospital)
- Vendor scorecard / Solution compliance questionnaire
- Vendor design notebook
- Business Impact Analysis and IT service continuity
- VPN connectivity form

Data Desensitization

All logs collected from the medical equipment have no sensitive patient-related information, so this step has not been considered. In cases where sensitive information is present, a desensitization script will be executed by the agent that targets specific regions of the file and strips out the sensitive data. The two techniques that are used include:

- **Data masking:** Selected regions of the text are masked with generic string patterns such as '#' or '*'
- **Removal:** Sections containing sensitive data are removed entirely

Sample Application Snapshots