Technical Overview, Network Topology and Management of ImageShare

Revised March 2018

Definitions

- Vigilant Medical Web Application Network: The ImageShare web application is hosted in a virtual private cloud (VPC) on Amazon Web Services.
- Registered Web Users: Any users including customers (i.e. healthcare users) and Vigilant Medical employees with private credentials provide access to the ImageShare web application.
- Vigilant Medical IT System Administrator: Vigilant Medical staff member authorized to access the VPN tunnel between our local Vigilant Medical office network to the Amazon hosted Vigilant Medical VPC.

System Design

This concise list enumerates components utilized in ImageShare.

Physical Layer

Amazon Web Services Elastic Compute Cloud
Amazon Web Services Elastic Block Storage
Amazon Web Services Simple Storage Service
Amazon Web Services Load Balancer

Data Layer

10gen MongoDB
Postgresql

Application Layer

Microsoft Windows Server 2012 R2
Microsoft .NET Framework 4.6.2
Microsoft ASP.NET 4.6.2
Microsoft ASP .NET MVC version 5.2.4 Framework
Microsoft Internet Information Services 8.5
Neologica RELite Dicom web based viewer

Client Layer

Oracle Java 8.0 Update 155
Microsoft Internet Explorer 10+
Microsoft Edge 40+
Mozilla Firefox 4.0+
Google Chrome 55+

Application Configuration & Deployment

ImageShare Application

ImageShare is a web-based application utilizing Microsoft .Net Framework hosted using Internet Information Services (IIS) 8.5 on a cluster of Windows Server 2012 R2 virtual machines. The ImageShare application communicates with a Mongo server database cluster hosted on a Linux virtual machine with Mongo Server 3.6 edition installed.

Neologica web-based DICOM viewer

ImageShare also uses Neologica RELite as a DICOM web-based viewer server running also on a Linux virtual machine. This application securely retrieves DICOM encrypted files from AWS S3 using a rotating public/private key for each file request. Any access attempt will cause RELite viewer to validate user request with ImageShare web api for appropriate permissions.

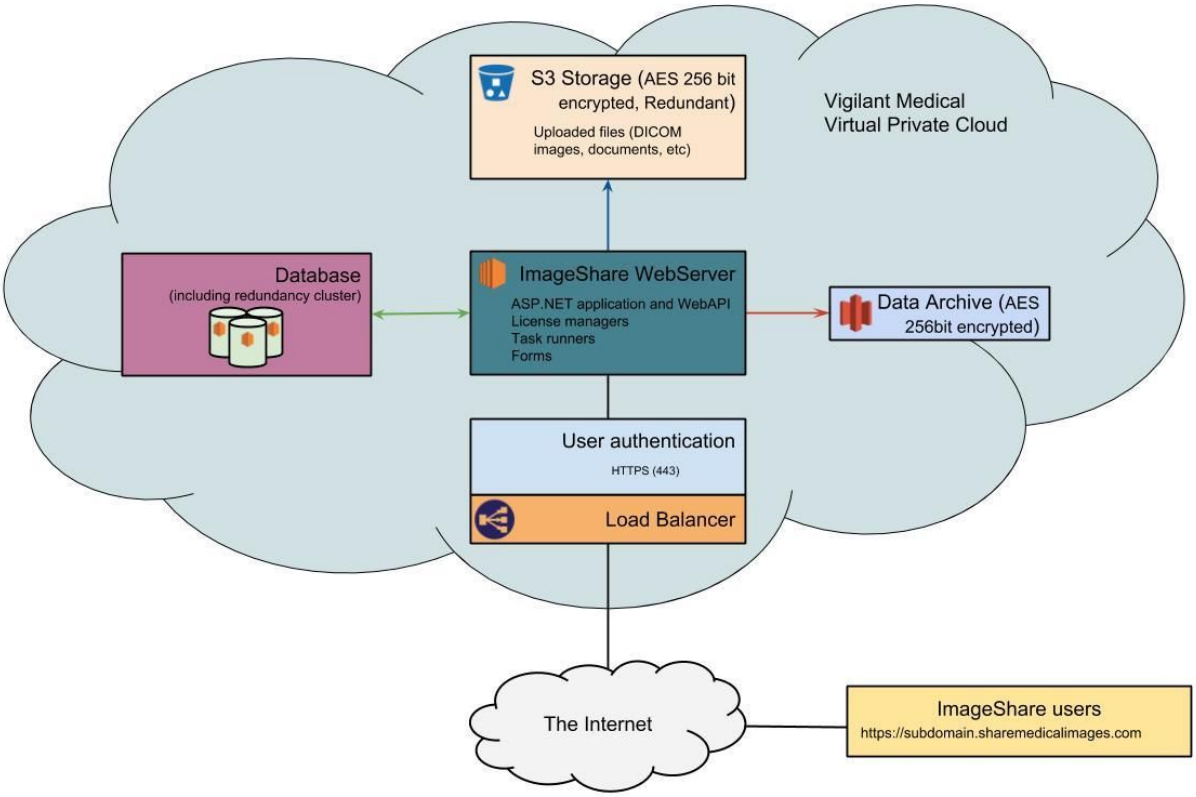
Network restrictions for above applications

The ImageShare application server and Neologica RELite are the only network resources that can be reached from the internet without going through a VPN tunnel. It is configured on a network segment with a security group allowing:

- HTTP (80) only for redirection to the HTTPS endpoint;
- HTTPS (443) to access both web applications

Our cloud environment is setup using AWS Virtual Private Cloud (VPC). It is a secured network zone restricted to public API services and VPN access only. The hardware and physical location is maintained and secured by Amazon through a signed BAA agreement. Our office is secured using a standard firewall and communicates with our cloud environment exclusively through a VPN tunnel for which is restricted to a set of computers which only the Vigilant Medical IT System Administrator can access. Through that encrypted tunnel, only a few ports are open for maintenance purpose.

Application Network Topology Diagram



Security Practices

Firewall management & network segmentation policy

We use AWS Application Load Balancers with the minimal set of open ports required to make our applications work. All firewall load balancer rules are implemented through the use of AWS Security Policies managed by Vigilant Medical IT system administrator.

Our Virtual Private Cloud is segmented into multiple zones (subnets) in order to isolate database cluster from web server cluster. Our database cluster is not directly accessible from the internet and can only access internet on maintenance schedule through a secured gateway to apply applications updates and security patches.

Our web server cluster can only communicate with the database cluster subnet on designated database port on which encrypted data is transported. Any other access, such as SSH for system administration needs to be done from our VPN only subnet which is only accessible from authorized computers.

Public access to our web infrastructure is limited in our firewall to the usage of port 80 for HTTP (to enable redirection to HTTPS) and 443 for HTTPS itself. It is not possible to access our public services through any other way.

Anti-malware

All Vigilant Medical staff member runs an anti-malware and antivirus on their workstation. We currently do not scan our customer data. However, we never execute any of the executable files uploaded as part of our customer data.

Vulnerability management & Patching

All our client application deployed softwares encrypt sensitive data.

We actively monitor publicly known vulnerabilities and address them accordingly when relevant. Windows and Linux machines are patched as often patches are released, sometimes more than once per week if necessary, most of the time the day the patch has become available.

We monitor the security alerts and web page documentation updates for all the software and application software development kits (SDKs) that we used to either provided service and build our own software.

Network scanning and testing

We perform internal network penetration testing using Kali Linux and OpenVAS 8.0 Vulnerability Scanning[1] on our clouded environment on a regular basis multiple times per year.
We also stress-test our application on a weekly basis and ensure it can sustain a high load of requests and resists denial-of-service attacks on key part of our applications.

Access control & Authentication mechanism

Vigilant Medical employee account management

All Vigilant Medical employees workstations and Vigilant Medical admin only services are managed under Active Directory with enforced account and password policies. Our Active Directory infrastructure is hosted in Azure as an HIPAA compliant service.

[1] https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/

Vigilant Medical ImageShare user account management

Our ImageShare users' passwords are transferred using TLS channels only and stored salted encrypted hashes. We do not store unencrypted passwords at rest. SSL has been deprecated for security vulnerabilities.

Our users are required to comply with a certain level of password complexity and length in order to avoid weak passwords.

Management console & privileged credential control

All management is done by authorized users on authorized computers with a vlan tagged connection to our encrypted VPN tunnel to our cloud infrastructure. Users have roles enabling or restricting them into some action or sensitive information.

Auditing, logging & monitoring

Every data access, views and downloads are audited and stored in database. We actively monitor our services for data inconsistencies, analysis tasks completion and customer technical support.

Web application firewall

We are in the process of implementing a AWS Web App Firewall according to their documented best practices.

Data protection/integrity monitoring

Data, both medical imagery and metadata stored in database, is encrypted at rest.
Database cluster is actively monitored with health check at less than a minute interval.
Data files are stored on a redundant Amazon S3 AES-256 server-side encrypted storage.

Database files are stored on a logical stripped array of disks (Raid1) over backed up physical array of disks (Raid5). Database cluster member are replicating across multiple AWS Availability Zones in order to increase resilience in case of outage.

Risk Assessment by Layer

Physical Layer Risks

Physical risks arise only when a threat arises to the hardware acting as the server. In a traditional hosting scenario, there would be a well-defined piece of hardware housed in an office or data center.

ImageShare utilizes a modern virtualized server model provided by a third party, Amazon Web Services [AWS]. AWS secures the virtualizing environment, as well as the hardware processing and storing the virtualization. AWS provides a security policy and auditing documents on their website.

Physical access, here, relates directly to datacenter access. ImageShare virtualized instances are hosted in the EC2 – EAST datacenter in Virginia. AWS strictly restricts access to the physical hardware in their data centers. AWS defines their datacenter physical security policy in their security documents. In addition to security from unauthorized access, AWS provides extensive protections from environmental disasters, to provide uninterrupted data integrity at or beyond the industry standard for datacenter protections

In this case, then, physical access also refers to the ability to access the virtualized instance in the Elastic Compute Cloud [EC2]. This access is restricted by a 2048-bit RSA key pair with the private certifying key maintained on the AWS server and public access keys are generated and assigned only to select members of the Vigilant Development and Support staff. These keys are managed and may be revoked at any time, should one become compromised. AWS strictly restricts their own employees' access to virtualized instances as described in their security document.

Data Layer Risks

The system Data Layer refers to the persistent storage of the virtualized server instance [VSI] as well as the run-time state of the random access memory [RAM]. Persistent storage is a combination of the file storage (the actual file contents) and the database (metadata and file system references). As data is accessed by the application layer, it is referenced in the database, and portions of the files are moved into RAM. The VSI, not AWS, is responsible for maintaining the integrity and security of the VSI's file system and database.

In a typical scenario, a patient's imaging data is uploaded to the VSI. Disregarding, for now, the protections afforded by the Client, Transport, and Application Layers, data is temporarily buffered in RAM and then recorded in two places within the Data Layer. File contents (in this case, imaging data) is stored to the file system and associated reference metadata is entered into the database. Database and file system access are thusly restricted to the application logic (required for the application to operate) and to the highest-ranking Vigilant system administrator assigned to maintenance on this VSI (required for maintenance and support). Access is restricted for all other purposes. No other VSI system user is authorized to view or edit objects in the Data Layer.

The Data Layer transport is further protected by using TLS protocol. The database access is encrypted with similar technology provided by a different part of the Application Layer .

Application Layer Risks

The security of the Application Layer is directly dependent upon the security of the VSI's operating system. Microsoft provides extensive security documentation of their Windows server software on their website.

Windows Server 2012 Release 2 (WS2012R2) provides an additional level of security by role-based authentication. This augments the 2048-bit RSA key pair with a high-entropy password, offering dual-layer security that first verifies the connecting machine and then the connecting user. WS2012R2 handles the file system utilized by the Data Layer and stores file contents using the common and high-data-integrity NTFS File System. WS2012R2 and NTFS are commonly used, enterprise-grade, server and data systems.

Vigilant has configured the ImageShare VSI's WS2012R2 software for a "Default Deny" approach to user-permissions. That is, by default, users are restricted from all activity, unless a particular activity is expected for that user. The Application Layer, for instance, must have read/write access to the file system and database in order to serve data to authorized users. The Application Layer is authorized to do this as well as execute code on the VSI processor. These are the only two actions that the Application Layer is required to perform and, as such, are the only two actions permitted. The Application Layer cannot, for example, create, modify, or query system information, cannot add, drop, or modify database tables, and cannot trigger any VSI system actions such as shutdowns or restarts.

Transport Layer Risks

The Transport Layer is secured by an Equifax certificate to validate the server identification. As with any web application, it is the responsibility of the user to verify that the server is validly identified. Most modern browsers will issue an alert to the user when an inaccurate identity certificate is encountered.

Once the server has been identified, the transport layer is further protected by the establishment of a Secure Socket Layer [SSL] connection with high-grade 128-bit AES encryption. It is imperative to note that this channel-level encryption is in addition to the 256-bit AES encryption active on the imaging data packets themselves. The SSL connection is established before any application data is exchanged between client and server, so no authorization information may be intercepted.

Users may verify the encryption level and server identification information through their browser's security panel.

Client Layer Risks

The Client Layer typically is the most difficult to secure. Web applications offer unique challenges in securing the Client Layer. Web applications, by their nature, are available on a variety of platforms with

varying degrees of client protections and vulnerabilities: outdated browsers still in use; compromised client systems logging keystrokes; and unclosed sessions can allow access to unauthorized users.

Vigilant mitigates as many of these risks as possible, but the vast majority of viable Client Layer protections must be taken by the individual users and enforced, where possible, by the Information Technology policies of the subscribing institution.

Vigilant attempts to enforce client security by implementing as many server-side controls as possible. For instance, users of an obsolete browser (e.g. Internet Explorer 6, Mozilla Firefox 2.x) are provided a reduced feature set while using the service. This helps to limit the information displayed in a potentially unsafe browser. However, since the server depends upon the client browser to identify itself, a wholly compromised browser could spoof the user-agent information in the request.

The key to strong Client Layer security is a complete and well enforced institutional information security policy. Vigilant's mitigation schemes for the Client Layer can be compromised (as can the schemes of nearly any software system) by insecure user activity. Users should choose, or be assigned, a high entropy password. Users should actively log out of the service when not using it. Although ImageShare will automatically log out idle sessions, users should not depend on this feature as the standard log out mechanism. High entropy passwords can be enforced by regular expression on the request of the institutional administrator.

Vigilant will work with the Information Technology administrator of the subscribing institution to devise ideal Client Layer security protocols for using the ImageShare service. Similarly, extraordinary user security rules of the subscribing institution (e.g. password entropy requirements, session timeout limits), that must be implemented server-side, can be implemented by Vigilant with due notice.