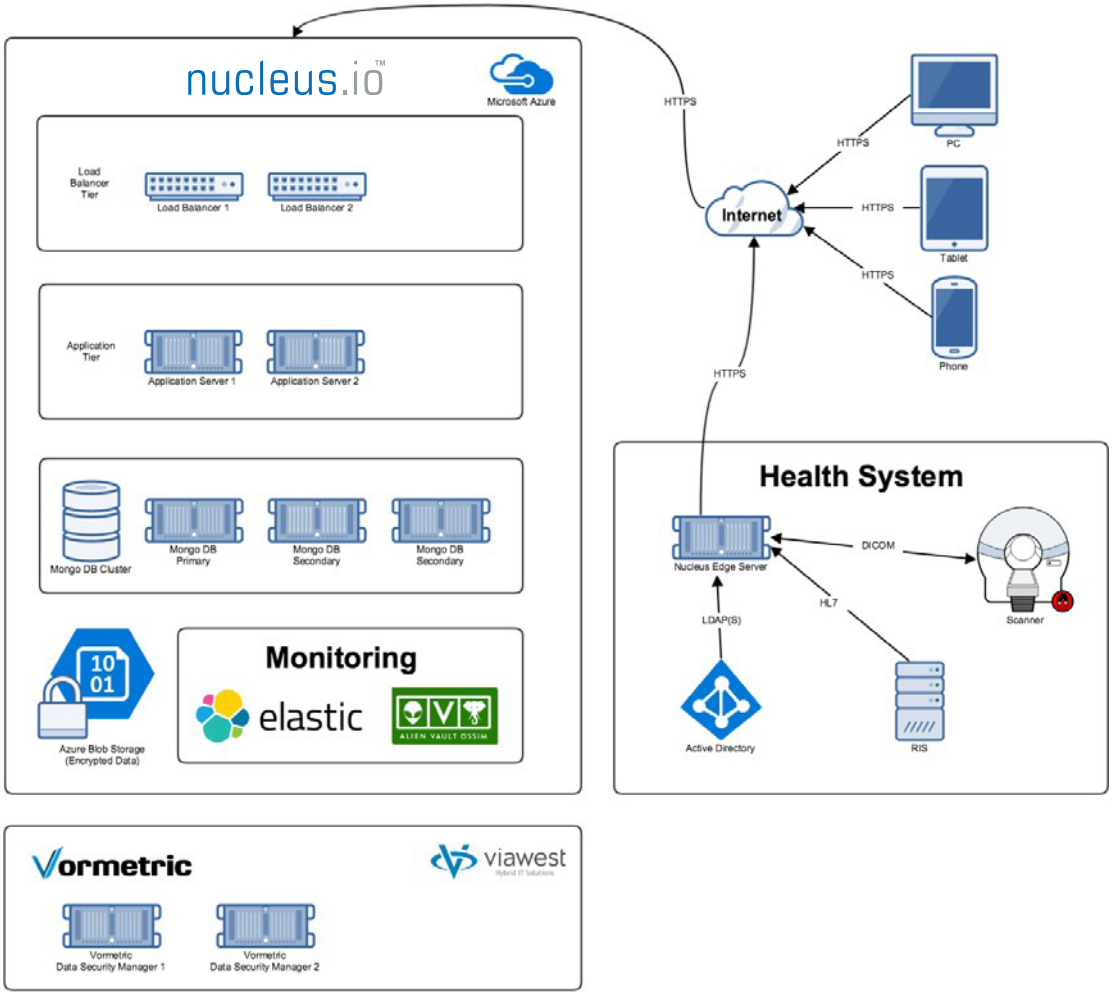
Nucleus.io Security Overview

Nucleus.io is a cloud based medical imaging infrastructure delivered via the public cloud in Microsoft Azure. Nucleus.io is deployed in a highly available configuration using Microsoft Azure Resource Manager.

A production deployment of Nucleus.io consists of two load balancers, a set of at least two (but often more) application servers, and a mongo cluster with three nodes.
These virtual machines comprise the data processing and service infrastructure. Azure Blob Storage is used to store data for the system, including the virtual hard disks (VHDs), DICOM metadata, and DICOM pixel data.



Clients access Nucleus.io over the internet using HTTPS; no VPN connection is used. Data transfer via unencrypted HTTP is not allowed.

All data in Azure Blob Storage is encrypted via AES 256 using cipher mode GCM. All data stored in the Nucleus.io processing infrastructure, including PHI (DICOM metadata) in MongoDB, is encrypted with AES 256 with keys stored FIPS 140-2 Level 2 compliant, externally to Azure in Vormetric Data Security Manager co-located in the NucleusHealth Data Center at Via West in Las Vegas Nevada.

Nucleus.io Security Technical Details

Nucleus.io is designed to prevent unauthorized access to PHI even by highly privileged members of the system administrator staff.

Ports and Protocols

Nucleus.io Cloud Deployment

The Nucleus.io deployment consists of two virtual networks – front and back. The front virtual network is for traffic flowing to and from the internet. The back virtual network is for traffic flowing internally inside of Azure.

Traffic on the front virtual network allows for incoming connections on port 80 (HTTP) and 443 (TLS) with all traffic on port 80 (HTTP) being automatically redirected to port 443 (TLS). [1] Nucleus.io never allows data to be transferred via an unencrypted channel.

The back virtual network is strictly limited to traffic originating from the front virtual network on well-known ports. Application servers have incoming ports 3000, 4000 – 4007, and 5000 open for application traffic. MongoDB servers have incoming port 27017 open for database traffic.

For administrative purposes, Nucleus.io is accessible via Azure Point to Site VPN connection. The VPN connection is secured via client certificate. Once a presence is established on the VPN gateway administrative access to machines is available via SSH over port 22 using SSH certificate authentication.

Edge Server

The Edge Server by default communicates with enterprise systems over well-known ports, however these are configurable where needed or appropriate. DICOM communication happens over port 104, HL7 communication happens over port 6661, and Active Directory LDAP communication happens over port 389 and 636 where LDAPS is available.

Encryption

Sensitive information on load balancers, application servers, and database servers are encrypted using the Vormetric Transparent Encryption agent. The Vormetric Data Security Manager contains security policy periodically retrieved by the machines where the Vormetric Transparent Encryption agent is running. This policy

[1] For comprehensive details on TLS configuration see Appendix A: Qualys SSL Report

controls the processes and users which can use the encryption keys to encrypt and decrypt data.

PHI Encryption and HIPAA Compliance

All PHI in transit between clients and Nucleus.io is transmitted via HTTPS. All PHI stored on the MongoDB servers is encrypted with AES 256 via the Vormetric Transparent Encryption agent. PHI stored in Azure Blob Storage is encrypted via AES 256 using cipher mode GCM.

Security Monitoring, Intrusion Detection and Prevention

Nucleus.io is actively monitored for intrusions, malware, and security issues via Alien Vault OSSIM SIEM. The SIEM in the Azure subscription actively monitors for unexpected traffic and provides alerts to Nucleus.io administration when abnormalities are encountered.

MongoDB Security

MongoDB is configured in a cluster to ensure high availability. The cluster uses X.509 certificates for cluster authentication amongst the replica set members. All access to MongoDB occurs over SSL. For clients connecting to the replica set, authentication is required.

Certificate Infrastructure

Nucleus.io uses Microsoft ADCS to issue certificates for MongoDB X.509 authentication and SSL configuration.

Nucleus.io uses ssh-keygen to create an RSA key with a bit length of 2048 for SSH administrative access to production systems.

Edge Server Authentication

Nucleus.io uses an API key for edge server authentication. This key is generated server side and provided via HTTP header to interactions with the Nucleus.io API. All interactions with the Nucleus.io system occur over HTTPS; as such this header is never transmitted in clear text.

Edge Server Administration

The Nucleus.io Edge Server supports Windows Server 2012 R2.
Nucleus.io administrative staff utilizes LogMeIn for access.