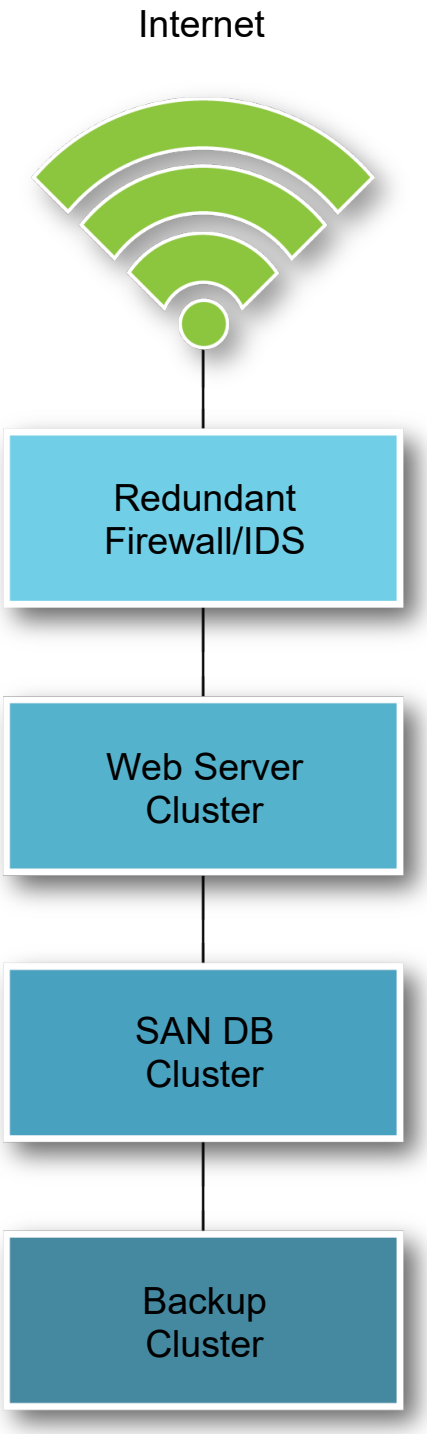
PTAEZ SECURITY AND ENCRYPTION DOCUMENTATION

Does PTAEZ have an off-site data backup and disaster recovery plan that restores both at the DB level or the object level?	PTAEZ offers a daily database backup and recovery plan that restores at the database level.
Does PTAEZ support intrusion detection systems and anti-virus/anti-malware controls? If yes, which systems and controls are supported.	PTAEZ is protected by a state-of-the-art firewall and intrusion detection system. This system automatically blocks IPs from any possible bad actors.
Does PTAEZ have an incident response protocol with a defined SLA for notifications? Do these notifications include notification of breaches? Are access logs retained for at least 2 weeks?	PTAEZ has incident protocol with a defined SLA for notifications including notification of breaches. If a breach is detected, the user will become notified immediately with detailed events/potential breaches that have occurred. All staff are properly trained in data security to identify areas of potential breaches. Access logs are retained for at least 2 weeks.
Is PTAEZ able to use encryption for password authentication, storage, and reset processes?	PTAEZ provides each site with a role that is then capable of creating roles of the same level of access or lower at the site for access needed. Once access is provided, if a user logs in with more than 3 incorrect password attempts, the user is then locked out and must call into our software support for reset.
Can search results be restricted by permission and security controls?	PTAEZ operates using predefined roles. Search results are restricted based upon the role of the user.
Can an individual's data be deleted when no longer required, or as required by document retention laws?	PTAEZ upholds document retention laws. All individuals can be inactivated, not "deleted". Once inactivated, the individual is invisible to the user in terms of pulling onto a receipt or having the ability to register for the web store; however, this individual can always be reactivated at any time. In addition to this, all records and reports are intact and continue to hold the individual's name as a record.

PTAEZ®

SYSTEM ARCHITECTURE



COLOCATION SECURITY

This diagram provides a high-level view of our system architecture that is secured in our data center. PTAEZ/Gray Step Software, Inc.'s data center is located in Los Angeles, California, and equipped with the finest physical and electronical security, fully redundant, and uninterruptible power and connectivity. Our state-of-the-art facility provides superior colocation and disaster recovery options.

Building entrances require card key access; data center and secured areas also require card key entry along with two-factor biometric authentication and a "man-trap" entrance. Guards are onsite 24x7 and active patrols are located inside and outside of the facility. Our Data center is equipped with a multitude of pan and tilt cameras to monitor the interior and exterior access points. Monitors display all the cameras at the front guard desk and in the Network Operations Center.

PTAEZ/Gray Step Software, Inc.'s engineering department selected a well secured location to store the sensitive information collected by our software.