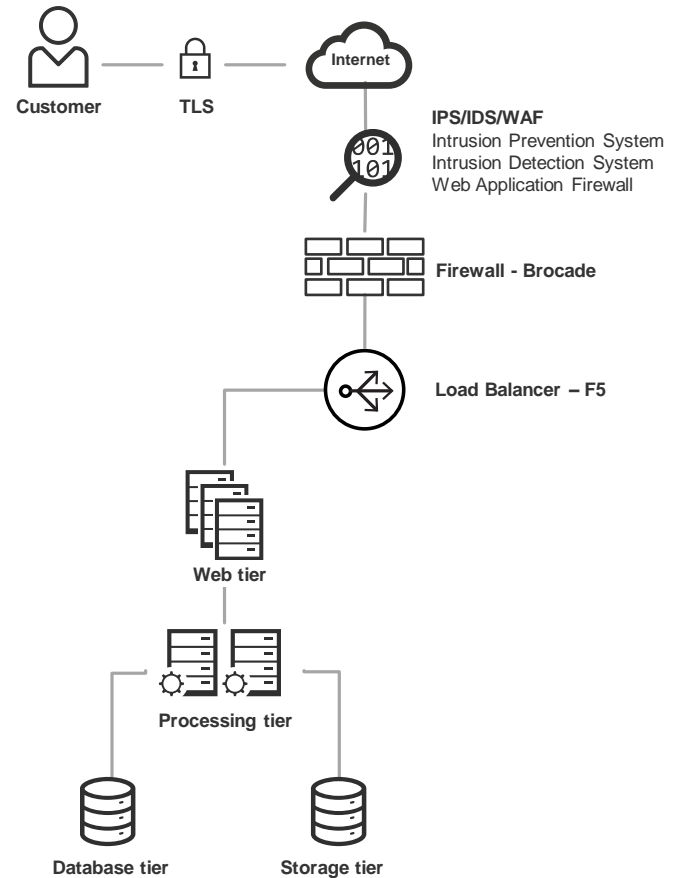


eScripton RH

Infrastructure and data flow diagram

Topic	Position
Segmentation	<ul style="list-style-type: none">3 -tier network segmentationData centers separated using firewalls and ACLs
Protection	<ul style="list-style-type: none">WAF (Web Application Firewall)IPS/IDS Firewall3rd Party Antivirus/Malware
Data and encryption	<ul style="list-style-type: none">In transit: https: and TLS 1.2At rest: All PHI and transcription data stored in an encrypted database. Audio stored on file system and either audio encrypted, or disk encrypted at all points.Local: Varies depending on system component
Data retention	<ul style="list-style-type: none">Retention of historical audio and data within the application will be stored for no more than 2 years by default, but can be changed according to customer's retention policy
Data usage	<ul style="list-style-type: none">Used to improve products and services as stated in customer contract
Access and administration	<ul style="list-style-type: none">All access to production environments are role-based, least privilege, and utilize jump hostsAccess by administrators is separate from the data center through multi-factor authentication and jump hostsUser auditing through centralized logging system



eScripture RH

Service recovery and business continuity

Topic	Position
Data centers	<ul style="list-style-type: none"> Primary and secondary locations Incorporates the industry's best practice standards and policies
Data backup and replication	<ul style="list-style-type: none"> Full image backups Stored on a separate encrypted device Replicated to secondary hot site
Redundancy and high availability	<ul style="list-style-type: none"> Multiple data centers with manual-failover Fully-redundant network infrastructure, including load balancers and switches Multiple, clustered application servers High-availability network storage with high speed connections Clustered database servers
RTO	<ul style="list-style-type: none"> 5 hours
RPO	<ul style="list-style-type: none"> 5 minutes
Critical Incident (CI) process	<ul style="list-style-type: none"> CI team activation Per product customer notification Updates every hour Updates at CI close
Disaster recovery testing	<ul style="list-style-type: none"> Nuance performs disaster recovery testing on an annual basis

