Security Commitment to Our Clients

Ensuring your organization's data and client privacy are protected and secure has always been a top priority at eCIO. We incorporate security measures into every level of our eVestech platform, from the servers that hold your data safe to user-level access security.

We Keep Your Data Safe and Secure With Enterprise-Level Infrastructure and Bank-Level Data Encryption

Throughout our infrastructure, API, and application-level systems, security is always front and center.

AWS Hosted Infrastructure

- All services, databases, file storage, and web applications are hosted on AWS.
- All files are maintained within Virtual Private Cloud (VPC).
- External Access is Blocked - Database connections are only accessible to services within the VPC.
- Database is encrypted at rest.
- Exposed services are accessed via a Security Group and Load Balancer to prevent malicious access.
- File/Blob storage (via AWS's S3 service) is only accessible inside the VPC or externally via a signed request with timeout.

API and Service Security

- All access to services must be validated with a certificate signed user identity token (JWT).
- Any incoming requests for data are analyzed by the service to determine if user identifier has access to a resource and what actions the user can perform before any action on a resource is permitted.
- Data on AWS S3 storage is partitioned by organization ensuring only an organization's users can access that organization's bucket. All processes on the services are logged to AWS Cloudwatch and are free of sensitive data.

Application

- All requests between application and server are encrypted with TLS.
- Signed access tokens are maintained locally with expiration to prevent malicious access.
- All actions on the application are logged to ElasticSearch and are maintained indefinitely.

We're Committed to Keeping Your Client's Privacy and Data Secure

Our security practices extend to your client servicing. Keep online conversations private, share files with clients seamlessly, and drive engagement virtually with confidence your communications will remain private.

- All interactions, messages, and files are secured with bank-level encryption technology.
- Never lose a file. All data is stored and backed up remotely in our private S3 encrypted storage buckets. Or, use your own S3 bucket for additional privacy.
- A uniform, single login process saves users the hassles of remembering multiple logins to various platforms. Multi-factor authentication or single sign-on services (OKTA, Google, Apple) are available

for your users.
- Files remain secure on client portals rather than sitting in people's email inboxes. Ensure members always have access to up-to-date documents.
- Utilize Secure Sockets Layer (SSL/TLS) certification which encrypts all browser data.
- Bank-level infrastructure security is modeled after Payment Card Industry Data Security Standard (PCI DSS).
- Secure audit logging to multiple sources for all application activity.

Bank-Level Storage and Access Control for You and Your Clients

Your data is stored and accessed with the same trusted vendors that banks and government agencies use. Amazon Web Services (AWS) is used by the Department of Defense, NASA, and the Financial Industry Regulatory Authority (FINRA).

Have questions regarding eVestech's abilities or security-related concerns? Talk with an eVestech representative, today!