Link-Live™ Cloud Service Security Overview

NetAlly takes a multi-layered approach to ensuring customer satisfaction and trust. Secure data centers, disaster recovery, data backups, security assessments, strong encryption, around the clock monitoring, third party assessments, and industry best practices are all parts of Link-Live Cloud Service. Here are the security and encryption details:

- Browser connections are via TLS1.3 ensuring a secure connection between the customers and Link-Live.
- Multifactor authentication is supported by Link-Live and enforceable across the entire organization.
- At rest, all customer data is stored in the Amazon AWS secure, highly available, multi-zoned cloud infrastructure, and is replicated to prevent data loss. It achieved ISO 27001 certification and validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS).
- Link-Live data is only removed through customer action. Deleting an organization will delete all data associated with the organization, including test results, screen shots, reports, etc. Personal identifiable information (PII) is deleted when a customer deletes his/her account.
- High-entropy password security using SHA-512 and HMAC hashing algorithms are used along with large, secure, randomly generated salts. Added computational complexity in hashing makes it cost prohibitive to breach even a single password.
- NetAlly regularly conducts vulnerability scans of Link-Live using Invicti Web App Security scanning
- NetAlly has a privacy policy: https://www.netally.com/privacy/. Users are requested to accept the policy when they log-in to Link-Live.
- Link-Live allows users to never store or display selective IP addresses of concern such as routers, switches, and network servers.

For more details on security at Amazon AWS please refer https://aws.amazon.com/security/