LITERA

Litera Transact
(Single-Tenant)

Security White Paper

August 2023

Litera
550 West Jackson Blvd.
Suite 200
Chicago, IL 60661
US: +1 630 598 1100 UK: +44 (0)20 3890 2860

On the Web: https://www.litera.com/

Contents

Introduction

Our Approach to Security

Keeping customer data safe and secure is of fundamental importance to Litera and one of our most critical responsibilities. This white paper outlines our approach to security and data privacy for Litera Transact hosted as a single tenant instance. This is where the software and data is run on infrastructure that's dedicated to a single customer — without sharing frontend, backend, storage, or database resources.

Overview of Security

Infrastructure

- Litera Transact application is hosted in Amazon Web Services (AWS).
- Data and files are hosted in AWS S3 buckets dedicated to the customer.
- Data in transit is encrypted with TLS 1.2 or above and at rest with AES 256.
- The platform resides in remote AWS data centers with industry-leading resiliency to prevent data destruction and access disruptions, while promoting rapid scalability and recovery.

Information Security Accreditation

- Litera Transact is included in the scope of our ISO 27001:2013 certification and controls.
- AWS, as the infrastructure provider, has the highest levels of infrastructure and information security certifications.

Access Controls

- Customers access Litera Transact through an authenticated user account.
- Native multifactor authentication is provided.
- Corporate logins and passwords are under the control of the customer Account Administrator with options for integration with other Identity Providers like Azure Active Directory and Okta.

Organizational Security

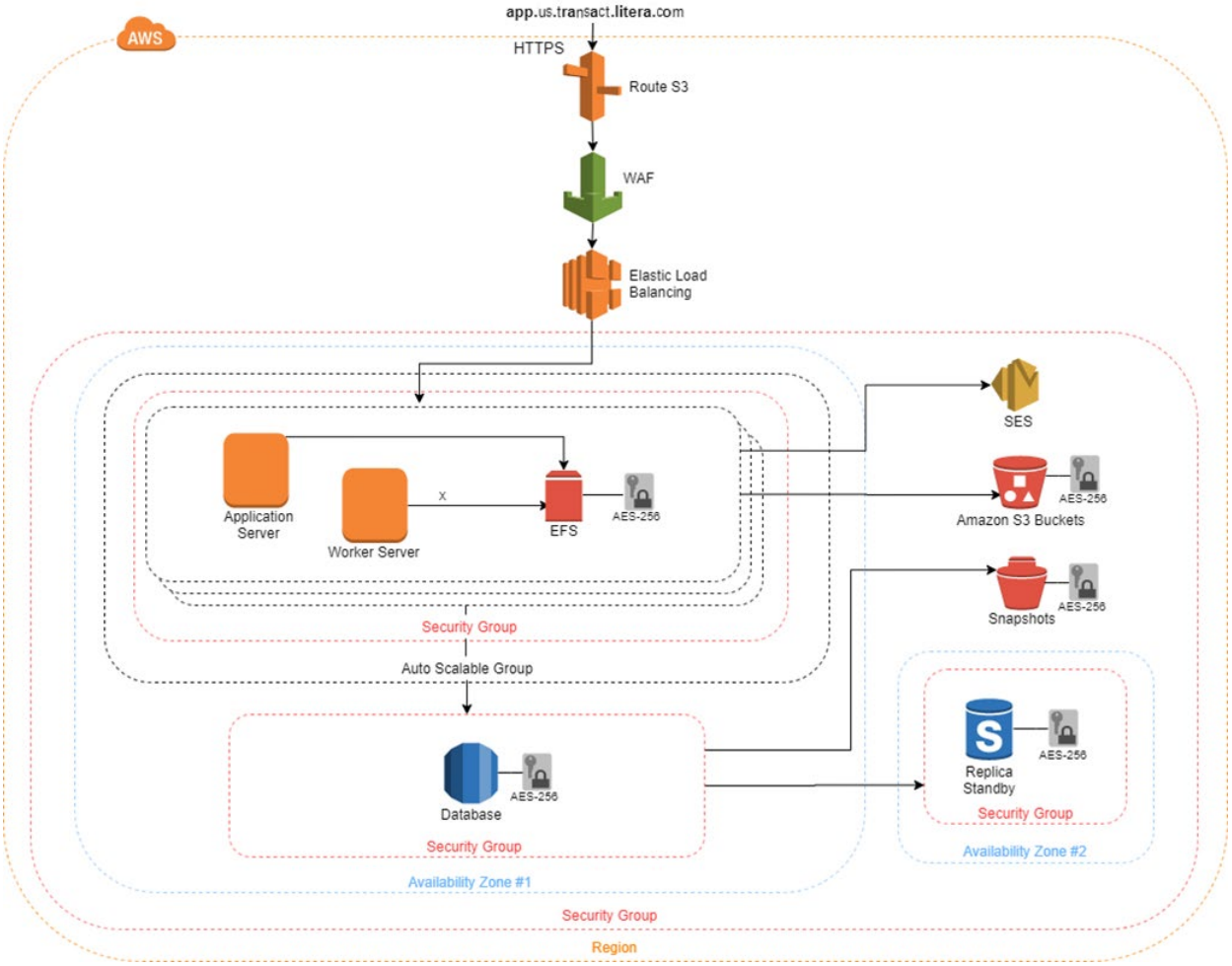
- Litera staff and our data center partners' personnel are screened, bound by strict confidentiality agreements, and have reference and background checks, where applicable.

Application Platform Security

Application Architecture and Hosting

- Litera Transact is a cloud-hosted SaaS application.
- The service itself and all customer data are hosted in AWS data centers maintained by industry-leading service providers that offer the highest levels of security for the servers and related infrastructure (For more information: AWS Security Whitepaper).
- Litera Transact can be hosted in a multitude of geographic regions to support data sovereignty requirements.
- Each customer's dedicated cluster is protected by an AWS security group and a web application firewall, which provides ingress network filtering from the broader Internet.
- The application is multi-tiered, consisting of an application front-end, worker backend, database, and storage repository; each tier is further isolated by security group and made resilient with availability zones.
- Our service agreement with AWS ensure the safeguarding, confidentiality, integrity, and availability of Litera's customer data and guarantee controlled access of their own employees. (For more information: AWS Physical Security).

Application Diagram



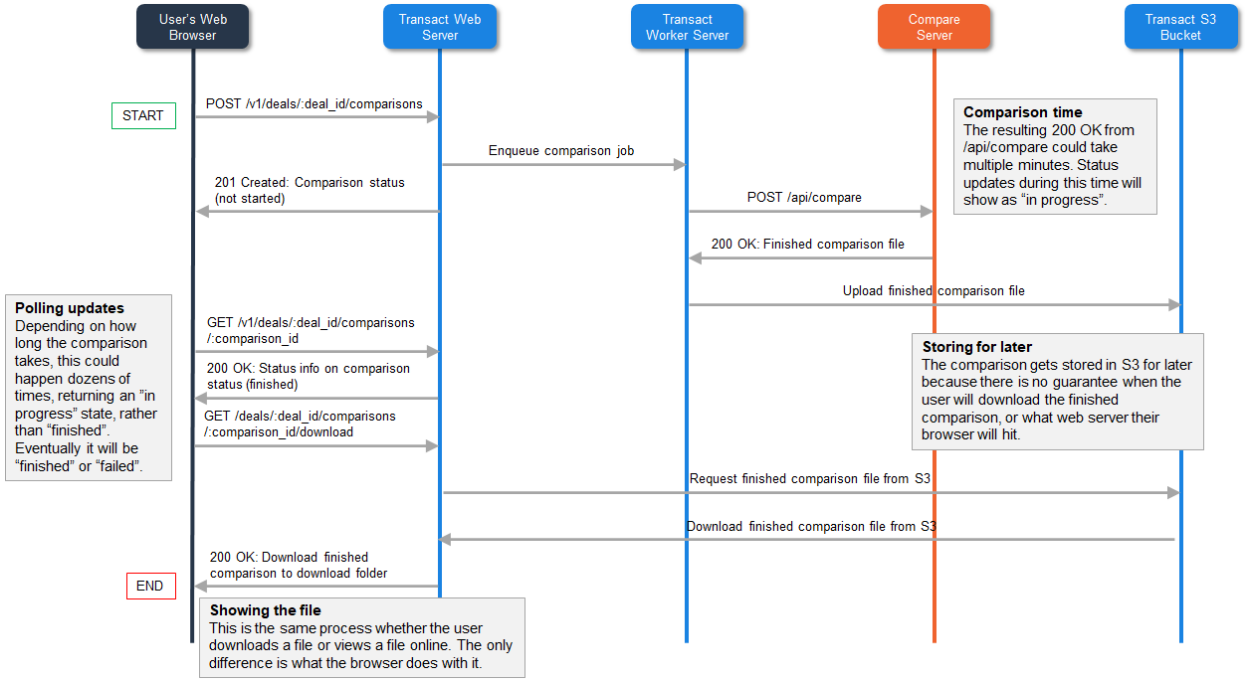
Data Encryption

Data processed and stored by Litera Transact is encrypted and protected when at rest and in transit. AWS provides the encryption infrastructure.

- **Encryption in Transit**: Only TLS 1.2 and above is authorized. Certificates are generated and maintained by Amazon Certificate Manager (ACM) using RSA keys with a 2048-bit modulus and SHA-256. All data access requires the use of HTTPS. HTTP connections are disabled. Inside the platform, all data is transmitted using HTTPS.
- **Encryption at Rest**: The Litera Transact database and customer data stored in AWS S3 buckets are encrypted with AES-256. User account passwords are stored inside the database using an asymmetric non-reversable algorithm.

Litera Product Integrations

Litera Transact makes use of Litera's Compare-as-a-Service (CaaS) to provide comparison of document versions in the checklist. The compare server performs the comparison and provides the redline but does not retain any documents or data at all. The data flow and system actions are shown in the following diagram:



System Monitoring, Penetration, and Vulnerability Scanning

Several systems are used to monitor the performance and security of the Litera Transact application.

- **Performance:** Application Performance Monitoring (APM) is enabled. Monitoring allows the Litera team to track overall application load and the performance of application and worker servers, while planning for future server capacity for the customer's dedicated instance.
- **AWS Security**: CloudWatch event logs are monitored. Alerts are sent to the security team channel by email and SMS for immediate resolution. CloudWatch alarms are setup for database and disk space to alert for capacity planning.
- **Application Errors**: Rollbar is used to monitor the web, worker, and API systems for any errors. Alerts are sent by email and to the Litera team to resolve.

- **Server Security**: AWS GuardDuty is used to monitor the servers and other infrastructure in AWS for intrusions and threats. Alerts are configured to send email and SMS alerts to the security team.
- **Vulnerability Scanning**: Internal configuration vulnerability scanning is run every 36 hours to identify points of weakness, and to subsequently ensure all AWS configurations and systems are configured correctly.
- **Code Security**: Litera Transact code is continuously evaluated for flaws and security vulnerabilities using automated static, dynamic, and software composition analysis scans.
- **Penetration Testing**: Penetration testing is conducted annually to safely identify any vulnerabilities in the Litera Transact application, systems, network, configurations, or services.
- **Intrusion Detection Scanning**: Litera Transact has implemented real-time monitoring of the application servers for any exploits and inspects all packets before they reach the server.
- **File Integrity Monitoring**: Each server is equipped with an antivirus agent that monitors the file system for any outside modifications.
- **Event Logs:** Event logs are collected and maintained for 12 months.

Organizational Security

Policies and Standards

Litera maintains a comprehensive set of policies that guide our procedures and practices for ensuring compliance with our information security obligations and requirements. Our policies align directly with the relevant ISO 27001:2013 framework of controls.

Personnel Security and Screening

At onboarding and annually thereafter, all Litera employees must agree to confidentiality terms, participate in annual security awareness training, and must abide by internal policies and standards. Security training covers privacy and security topics including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting.

Security Incident Response

Litera has established policies and procedures for reporting and responding to potential security incidents. All incidents are managed by our Incident Response Team (IRT). Our policies provide for notification to customers in the event of a security incident involving the unauthorized use or disclosure of confidential or personal information.

Business Continuity and Disaster Recovery

Litera Transact is deployed with a fully mirrored recovery site with data stored in separate availability zones to provide data center and geographic resiliency. Litera maintains a robust business continuity and disaster recovery plan that is tested annually. Litera has established runbooks that aid the business continuity team with quick resolution of an event.

Data Privacy

Litera Transact is designed with data privacy in mind. All data stored or processed by the system from a customer or their collaborators is never inventoried, scraped, or classified. Data is always encrypted, and can be stored in specific geographic regions to comply with privacy laws and regulations.