Secure Being

Data & Security Best Practices at Litify

Below are the results of an audit performed by Secure Being to test Litify's security approach and protocols.

About the Litify Platform

Litify is built on two of the largest cloud based platforms used by nearly every technology provider in the world, Salesforce and Amazon Web Service (AWS). This unique mix of technologies let's Litify provide the most intuitive and flexible set of capabilities that are built specifically for the legal industry, while also taking advantage of the robust security measures implemented by two of the largest technology companies to exist.

Litify Data Management on Salesforce

Salesforce provides a strict data security protocol trusted by some of the most security conscious organizations in the world including the Department of Defense and Coca-Cola. Read more about their stories by following the links.

All Litify customer data is stored within the Salesforce platform directly on Salesforce servers. Litify does not maintain any servers or retain any direct access to a customer database. Data stored within Litify can only be accessed by authorized employees of the company with the express permission of the client. To ensure that only authorized personnel are able to login to a customer's specific environment of Litify, Salesforce implements highly secured login practices including multi-factor authentication and encryption. All Litify customers have exclusive control over how their information is accessed and shared. No third party is able to access customer information in Litify, including Litify employees, investors, shareholders, and board members.

Litify Support users may request Login Access to your database when it is necessary to log in to Litify applications to replicate, isolate, troubleshoot, and ultimately resolve issues stemming from customer initiated support inquiries when support is not possible with existing access to a customer's organization settings, setup tree, or other customer metadata.

No one within Litify Support may log in to your organization to resolve issues without this explicit permission and duration for the access. After explicit approval by the customer, the Litify support team can temporarily access the customer database for only the amount of time allotted by the customer. Any access by a Litify support employee is tracked in audit logs that the customer can reference at any point.

In order for Litify Support users to use Login Access to log in to a customer's organization, the customer themselves (i.e. the individual user) must first use the process outlined in "Grant Litify Support Team Access" to explicitly approve Litify Support's request to log in with their user profile. Litify Support users then follow an explicit internal process to document that their use of Login Access is permitted in a Support case. Other Litify employees are explicitly blocked and do not gain any additional access through this support mechanism.

Litify File Management on Amazon Web Services

Litify manages the storage of documents on Amazon Web Service(AWS). The AWS platform is fully secured using an automated system of monitoring and alerts. Access is highly restricted on an individual basis so only the right people, internal and external to the customer's organization, are able to access key documents and information. Access for Litify employees is also highly limited and follows a strict approval process. More information regarding AWS data privacy and security can be found here.

Leveraging industry standard tools and techniques, Litify continually runs security testing on it's product hosted on the AWS platform. Additionally, independent third party industry experts conduct routine penetration testing to validate the security of Litify's product.

Security and Privacy Controls

Litify, Salesforce, and Amazon Web Services all follow industry best practices to ensure Litify customer data is stored in a secure and private environment.

A key aspect of ensuring Data Security is login attempt tracking. All successful and failed login attempts by any party including internal users, administrators and any 3rd party are tracked in audit logs that the customer can reference at any point. The audit logs include, at a minimum, the username, timestamp, and originating IP address.

Additional best practices include the following:

Written policies and procedures following industry best practices on security and privacy

Completely inaccessible by competitors

Highly restricted access by third parties unless under a direct legal obligation

Internal security testing and Penetration testing by third party industry experts

Secure software development tools and practices

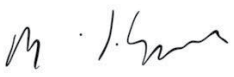
Active monitoring of environments for security vulnerabilities and threats

Secure access to environments through stringent credential protocols including Multi-Factor Authentication

Strong encryption standards for data in transit and at rest

About the Audit

Mike Sheward is a Chief Information Security Officer with 16 years experience in the information security sector, specializing in ethical hacking techniques that uncover vulnerabilities in application source code and network infrastructure. Mike carries the following certifications CISSP, CISM, CCFP-US, CISA, HCISPP, CEH, OSCP, CHFI and has performed penetration testing for a wide range of public and private sector clients. He took a look under the hood at LItify's complete security protocol which consisted of a 4-phased testing methodology including initial discovery, policy review, Salesforce.com configuration review and lastly, an AWS configuration review. After completing the tests he has verified that Litify, Salesforce and AWS are currently practicing the security measures outlined above.



Secure Being

Mike Sheward, Secure Being

CISSP, CISM, CCFP-US, CISA, HCISPP, CEH, OSCP, CHFI