THOMSON REUTERS LEGAL TRACKER SAAS SECURITY

WHAT YOU NEED TO KNOW WHEN EVALUATING MATTER MANAGEMENT SOLUTIONS

The benefits of cloud computing—such as collaboration, reduced IT costs, and nonstop availability—are prompting many companies to adopt cloud solutions to meet their business needs. As the adoption rate of cloud solutions increases, so does the emphasis on data security. Not all cloud solutions are created equal, which is why it is important to partner with a provider that not only emphasizes the importance of security, but also has a demonstrated commitment to data security through certifications and continuous improvement.

We have a demonstrated history of implementing data-security best practices combined with independent third party assessments to validate that the security controls are both appropriate and operating effectively. The security and availability of your data is our priority. In the preceding 12 months, Thomson Reuters Legal Tracker™ (formerly Serengeti Tracker™) has maintained 99.9% uptime.

CERTIFICATIONS AND AUDITS

In 2009, Legal Tracker was the first matter management and e-billing solution to be certified under the SAS 70 Type II. Tracker has successfully passed each annual SAS 70 Type II audit since receiving the initial certification.

In late 2011, the governing agency, AICPA, deprecated the SAS 70 report and replaced it with the SSAE 16 Service Organization Controls (SOC) reports. Of the new SOC reports, the SOC 2 and SOC 3 are directly applicable to cloud providers in that they directly audit the providers' controls around critical areas such as security, confidentiality, availability, and processing integrity. In April 2012, Tracker underwent its first audit under the new SSAE 16 controls to receive a SOC 2 Type II certification, which tests that the controls are appropriate for the relevant criteria and that the controls are operating effectively.

Because it is not enough for only the application provider to be certified, we have partnered with Tier 1 colocation providers that are also SOC 2 Type II-certified. Combining our security practices with our partner colocation facilities, we are able to address data security from end to end.

In addition to the SOC 2 certification, we have had independent third party Vulnerability Threat Assessments (VTA) performed annually since 2006. These third party VTAs include both network and Web application testing in which the testers attempt to find any flaws in both perimeter and application security.

The combined SOC 2 and VTA reports are available upon request and completion of a fully executed NDA.

DATA CENTER SECURITY

We have partnered with top-tier facilities in Seattle and Chicago to provide primary and disaster recovery sites. Both facilities are SOC 2-certified for their physical and environmental controls. Each site includes environmental features like backup generators, state-of-the-art fire suppression and water-detection systems, 24/7 security guards on staff, and video surveillance and biometric access controls, to name a few.

NETWORK SECURITY

We subscribe to the principle of defense-in-depth. The network is protected on several levels through the combined use of firewalls, multiple layered networks, authentication requirements, intrusion detection systems (IDS), and encryption.

Both the production and disaster recovery networks are physically and logically separate from our corporate networks. Access to the network is limited to a select group of senior IT administrators who each have specific roles, and thus enforces separation of duties.

QUICK FACTS

- 99.9% uptime in the preceding 12 months
- Defense-in-depth security provides a multifaceted approach to data security
- Tracker is SOC 2 Type II and SOC 3-certified
- Annual third party vulnerability threat assessments are performed on both the network and application
- Data is encrypted in transit and at rest

the answer company™
THOMSON REUTERS®

SERVER SECURITY

Servers are hardened prior to deployment through the use of best practices (i.e., disabling unnecessary services) and applying approved patches. All servers are monitored programmatically for changes, and all changes are reconciled against the record of approved change requests. All changes to systems adhere to our Change Management policy to ensure that changes are tested, reviewed, and approved prior to application to production systems.

Servers are segmented into roles, with each role having a specific network that it resides on and limited or no access beyond its assigned network.

APPLICATION SECURITY

To ensure against co-mingling of client data, Tracker provisions each client into physically separated databases and file structures. Data stored in the databases is encrypted at-rest to further protect customer data against loss.

The Tracker application is built upon the principle of permissions. User accounts are created and administered by the customer. New accounts receive an email with a one-time-use link that will require the user to set a password upon using the link. User accounts are provisioned access to matters by a customer account with appropriate permissions. Users can only see the data to which they have been granted access. Tracker enables customers to configure password requirements to mirror their own corporate password policies.

From a supported Web browser, customers connect to Tracker via an HTTPS session that is secured with 256-bit encryption certification, thereby enforcing encryption of data in transit. At the customer’s request, we can enable IP restrictions that limit the ability of customer users to log in to Tracker only from their corporate network or through their corporate VPN.

MONITORING

Multiple monitoring strategies have been implemented to allow us to monitor the entire infrastructure from a variety of different angles to enable a full view into the performance of the environment. Automated monitoring is configured to programmatically page the on-call personnel in the event certain thresholds are reached and to enable prompt resolution.

DISASTER RECOVERY

We use a multi-phased approach to enable the recovery of customer data in the event of a disaster. Disk-to-disk backups are utilized to eliminate the need for tape backups. Both data and backups are replicated to the disaster recovery site to offer the maximum flexibility for recovery in the event of a disaster. Failover testing at the disaster recovery site is performed at least twice a year.

To learn more, please contact your representative at **1-888-736-9587** or visit **legaltracker.com**.