ReporterBase

Business management software for court reporting agencies, videographers, interpreting companies, & other legal support businesses

RB9

Security, Privacy, & Architecture

OMTI's latest version of ReporterBase employs the latest software innovation, ensuring its safety and data integrity.

Revised: 2/17/2021

OMTI

Office Management Technologies

Contents

The content of this white paper is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by OMTI Inc. OMTI assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

ReporterBase, RB9, RB Connect and the associated logos and design, are trademarks of OMTI Inc. in the United States and other countries. Microsoft, Azure, and Excel are trademarks of Microsoft Corporation registered in the United States and other countries. For current information on ReporterBase software and services, visit www.omti.com/rb.

OMTI • 1440 N. Harbor Blvd., Suite 108, Fullerton, CA 92835

OMTI's Corporate Trust Commitment

OMTI is committed to achieving and maintaining the trust of our clients. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of data submitted by clients to our services ("Customer Data").

Customer Data includes:

- **RB9 data:** Unique information clients input into their RB9 or that is automatically generated by their RB9 system, such as client information and scheduled depositions.
- **Repository files:** Non-RB9 data files that clients upload to their RB9, such as transcripts, notices, and exhibits.

Services Covered

This documentation describes the architecture of and the security and privacy-related administrative, technical, and physical controls applicable to the software services branded as ReporterBase 9 (RB9) and RB Connect (together, the "RB9 Services").

RB9 Infrastructure

OMTI leases the Azure cloud platform infrastructure from Microsoft where RB9 Services and Customer Data submitted to the RB9 Services reside. OMTI chose Azure, which has been available since 2010 and is continually being augmented and improved, for many reasons, particularly reliability and security.

RB9 Services and Customer Data are duplicated on multiple servers. For example, each client's RB9 data in a primary data center has an exact copy in a secondary data center. If something should happen to the first set of data, the version in the secondary data center would come online with no loss of data.

The RB9 Application Server is set up somewhat similarly, running simultaneously on multiple servers. This redundant setup is for load balance so your RB9 application won't slow down when multiple users access it at the same time. Azure Load Balancer handles any increased web requests by distributing the traffic load among these shared servers. And like the duplicated Customer Data on multiple servers, if one application server goes down, it doesn't affect our clients because the second application server takes over. Traffic monitoring and dispersing will continue as well. OMTI and our clients' have no role in maintaining, patching, or providing security in this process. It is all handled by Azure.

The SQL Servers where Customer Data resides cannot be accessed from outside. And the RB9 Application Server is designed to be accessed using the RB9 application only, so access to Customer Data is not possible without the application. Similarly, client repository files cannot be accessed from outside. They can only be accessed through the RB9 application.

In addition to Azure's safety and security protocols, OMTI adds one more layer of data protection with a several-day backup of all RB9 data. This data is encrypted and stored separately, and would be used in the case of the 0.001% chance that all our servers on the Azure platform crashed at the same time. Also clients' backup media are stored in isolated areas that no one can access.

Audits and Certifications

OMTI takes the security and privacy of our clients' records seriously, and so for RB9 Services, we chose the cloud platform with the highest level of compliance certification: Microsoft Azure.

Microsoft is a leader in cloud security and data privacy. They were the first cloud provider recognized by the European Union's data protection authorities for their commitment to EU privacy laws, and the first major cloud provider to adopt the international cloud privacy standard, ISO/IEC 27018. It is audited annually by a third-party certification body for its ISO/IEC 27018 compliance. Azure maintains the largest compliance portfolio in the industry, complying with numerous other national and international data privacy acts, including HIPAA/HITECH.

The complete list of compliance certifications can be found on the Azure compliance page: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

In addition, OMTI uses open source security tools to self-audit and make sure we receive A or A+ grade from OWASP (Open Web Application Security Project).

Security Controls

RB9 Services include a variety of configurable security controls that allow clients to tailor the security of RB9 Services for their own use. These controls are set forth in the RB9 User Guide, and include security groups, which restrict group members' access and usage of RB9, and password protocols.

Security Procedures, Policies and Logging

RB9 Services are operated in accordance with the following procedures to enhance security:

- RB9 only accepts TLS encrypted requests. It blocks TLS 1.0 and lower requests, which have been deprecated, and accepts only 1.1 and higher requests.
- User passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, URL executed on, operation performed (created, updated, deleted) and client IP address. Note that client IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by client or its ISP.
- If there is suspicion of inappropriate access, OMTI can provide clients log entry records to assist in forensic analysis. This service will be provided to clients on a time and materials basis, and is only for special cases where usual protocols fail.
- Logs will be kept for a minimum of 90 days in a secure area to prevent tampering.
- Passwords are not logged under any circumstances.
- OMTI personnel will not set a defined password for a user. Users can set or reset their passwords at any time. Passwords are not accessible to system administrators or OMTI personnel. System administrators can set password requirements, such as complexity and duration.

Threat Detection, Additional Logging, Security Patches, Viruses

The Azure cloud platform monitors RB9 Services for unauthorized intrusions using network-based intrusion detection mechanisms. OMTI may analyze data collected by users' web browsers (e.g., time zone, browser type and version, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that RB9 Services function properly.

All Azure cloud platform systems used in the provision of RB9 Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Azure maintains security incident management policies and procedures. OMTI promptly notifies impacted clients of any actual or reasonably suspected unauthorized disclosure of their respective Customer Data by OMTI or its agents of which OMTI becomes aware to the extent permitted by law.

Azure provides OMTI with 24/7 tech support and service health monitoring. When OMTI receives an alert from Azure's monitoring or our own internal tools, our development team starts to work immediately on remediation.

When Microsoft announces a critical/security patch, OMTI applies it immediately. Other patches that are not deemed critical or related to security are applied at our discretion.

Azure handles all firewall maintenance and patching, requiring no effort on OMTI's or our clients' part.

RB9 Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into RB9 Services by a client. Uploaded files, however, are not executed in RB9 Services and therefore will not damage or compromise RB9 Services by virtue of containing a virus.

User Authentication

Access to RB9 Services requires authentication via user ID/password, or optionally in the case of RB Connect, via social media sign-in (Facebook, Google, LinkedIn) as determined and controlled by the client. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used by Microsoft Azure to provide RB9 Services have access control systems. These systems permit only authorized personnel to have access to secure areas. Also, these facilities are designed to withstand adverse weather and other reasonably predictable natural conditions.

Reliability and Backup

All networking components, SSL, load balancers, web servers, and application servers are configured in a redundant configuration. All Customer Data submitted to RB9 Services is stored on a primary database server with multiple active clusters for higher availability and on redundant devices to ensure reliability and performance. All Customer Data submitted to RB9 Services, up to the last committed transaction, is automatically replicated on a near real-time basis to secondary servers.

Clients don't have to deal with backing up data or repository files with RB9 because everything is duplicated on multiple servers in real time. If the active server should go down, another server takes over with no loss of data. Microsoft Azure manages this process, not OMTI or our clients.

This is better than a backup system which only saves data up to a certain time, so anything entered since the last backup is lost. Microsoft SQL Server AlwaysOn Availability also eliminates the downtime involved in restoring data from the backup.

Repository files are equally secure. Copies of each file are stored on different servers. Azure Locally Redundant Storage replicates each file three times on different servers to prevent file loss.

Azure's enterprise-grade SLA guarantees RB9 99.95% uptime, which works out to at most 44 minutes of downtime/month.Another downtime cause can be network connection problems. If an agency's network connections are not stable, their remote users might encounter problems logging into RB9. RB9 solves this problem because it's just an internet connection, not a connection to an in-house network.

Data Encryption

RB9 Services use industry-accepted 256-bit AES (Advanced Encryption Standard) encryption to protect sensitive Customer Data in storage and communications during transmissions between a client's network and RB9 Services, including signatures and up to 256-encryption SSL certificate. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Return of Customer Data

Within 30 days post contract termination, clients may request return of their respective Customer Data submitted to RB9 Services. Client can download their own data in Excel or comma separated value (.csv) format directly from RB9. If client prefers, OMTI can provide raw SQL data file as well upon client request.

Deletion of Customer Data

After contract termination, client's RB9 service is deleted and the Customer Data submitted to RB9 Services is stored for 60 days, after which it is securely overwritten or deleted. Physical media on which Customer Data is stored during the contract term is not removed from the Azure data centers that OMTI uses to store Customer Data.

Without limiting the ability for clients to request return of their Customer Data submitted to RB9 Services, OMTI reserves the right to reduce the number of days it retains such data after contract termination. OMTI will update this RB9 Security, Privacy, and Architecture Documentation in the event of such a change.

Interoperation with Other OMTI Services

RB9 Services may interoperate with other OMTI services, including ReporterBase.com, an opt-in service for applying reporters' digital signatures to RB-PDF Transcripts. For information on these services, contact RB Support.

omti

OFFICE MANAGEMENT TECHNOLOGIES

Who is OMTI?

OMTI is a privately held company, founded in 1985, that develops business management software, web services and mobile apps for record retrieval companies, court reporting agencies, and other litigation support businesses. Hundred of legal support companies, mainly in the US and Canada, use OMTI's products and services on a daily basis. Clients of our ReporterBase and ReporterBase software range from national syndicates to one-person shops.

OMTI's products and services are available by subscription only. We know that our business management software is vitally important to our clients' businesses, so we must continue to support our clients and develop new products. Subscriptions provide OMTI with stable income and pay for all of our product development and support. All of our development costs are paid for by our clients. Desirable features like PDF transcripts, case repositories, mobile apps, and e-commerce were made possible by our clients' subscriptions.

We continue to develop and implement new technologies that benefit this unique industry. For example, RB Connect makes it easy for your clients and third parties to interact with your office online, including ordering depositions and paying invoices for access to transcripts and files (so even C.O.D. clients pay on time).

RB9 is the latest innovation from OMTI, simplifying court reporting business management while saving on overhead and increasing data security. Cloud-based solutions are the latest evolution of software, allowing us to quickly deploy new features and bug fixes to all of our clients. And by hosting our clients' systems on the best cloud services available, we can better ensure their systems' safety and integrity.

The success of OMTI's business model can be measured in both the continued significant growth in installed systems and add-on services, and the long-term loyalty of OMTI's customers — many have grown with the company since its beginnings, and companies that start using OMTI products overwhelmingly stay with OMTI products. OMTI values its customers, actively seeking their input on new solutions to their business problems and providing forums for information sharing and networking, such as our customer portal and user conferences.

OMTI is financially stable and has no debt. It is headquartered in Southern California, with a Korean office for product development and an Oakland, California office which handles marketing. All of the principals in the organization have been with OMTI for more than ten years.

Contact info

Corporate headquarters

OMTI Inc.

1440 N. Harbor Blvd., Suite 108

Fullerton, CA 92835

650-396-2105

fax: 650-560-6550

Website with Live Chat

www.omti.com

Product inquiries direct line

650-396-2111

Product inquiries email

sales@omti.com