

Systems and Data Security

Leading Edge Security Infrastructure

Rethink Solutions Inc. (RSI) utilizes the latest in state-of-the-art physical and data security to ensure that your data management systems are never compromised. We devote extensive resources to continually develop our leading edge security infrastructure; thereby delivering unsurpassed security and privacy to our clients' data and information.

When deploying an RSI solution, in addition to our standard security measures, we provide:

- A multi-disciplined team of experienced, professional security specialists dedicated to 24/7 protection of data and systems.
- Constant deployment and implementation of proven, up to date firewall protection and SSL encryption.
- Ongoing evaluation of emerging security developments and threats.

Security Details

RSI applications are as secure as the leading online financial institutions and service companies. Configured by expert professionals and rigorously tested before going into production, our security infrastructure includes current, proven firewall protection, intrusion detection systems, SSL encryption, and other security technologies.

Data Hosting Facility

RSI hosts its servers and applications at a state-of-the-art hosting facility in the United States. The highly secure, redundant infrastructure of the data center protects our servers and web environment, and ensures we are up and running 24 hours a day, 7 days a week. The data center space, conditioned power, network access and internet bandwidth are each covered by service level agreements assuring 100% uptime.

Regulated Climate Control:

The HVAC (Heating Ventilation Air Conditioning) systems have full particle filtering and humidity control. The environment within the data center is maintained at a cool 68 degrees to ensure that our servers are functioning at their best in an optimal environment.

Backup Power Systems:

The data center's on-site diesel-powered generators and centralized uninterruptable power systems provide power conditioning and ensure uninterrupted dedicated hosting data center operation. The generators are regularly tested to make certain that they will function as needed in the event of an emergency.

Data Center Security:

The data center is physically isolated from everyone but senior technicians and authorized personnel. Monitored closed circuit television and 24/7 onsite security personnel guard the facility while military grade pass card access and biometric handscan units provide further layers of security.

Perimeter Defense

The network perimeter is protected by a multi-layered firewall and monitored by intrusion detection systems. Furthermore, firewall logs are monitored and analyzed regularly to proactively identify security threats.

Data Encryption

RSI leverages the strongest encryption products available to protect client data and communications using SSL certification. The lock icon in the browser window indicates that data is fully shielded from access while in transit.

Authentication & Application Security

Clients/Users access their organization's data systems only with a valid username and password combination. RSI's comprehensive application security permission model prevents one customer from accessing another's data. This security permission model is reapplied with every request and enforced for the entire duration of a session.

Internal Systems Security

Inside of the perimeter firewalls, all systems are safeguarded by network address translation, port forwarding, IP masquerading, non-routable IP addressing schemes, and more. Exact details of these features are restricted.

Operating System Security

RSI enforces strict operating system-level security by using a minimal amount of access points to all production servers. All operating system accounts are protected with strong passwords, and production servers do not share a master password database. All operating systems are maintained at each vendor's recommended patch levels for security and are further protected by disabling and/or removing any unnecessary users, protocols, and processes.

Database Security

Wherever possible, database access is controlled at database connection levels for additional security. Access to production databases is limited to only a small, required number of access points.

Server Management Security

All data entered into any of RSI's applications by a client is owned by that client. RSI and affiliated employees do not have direct access to the RSI production equipment and databases, except where necessary for system management, maintenance, monitoring, and backups.

Reliability and Backup

All networking components, web servers, database servers, and application servers are configured in a redundant configuration. All client data, up to the last committed transaction, is automatically backed up nightly.