

THOMSON REUTERS DATA CENTER

CS PROFESSIONAL SUITE®

PHYSICAL SECURITY

When using any of the CS Professional Suite web-hosted products or services, you can rest assured that your software and data are in the most secure location available—the Class IV, IBM-certified Thomson Reuters data center. As one of the largest data centers in the world, comprised of two separate, state-of-the-art facilities totaling 175,000 square feet, it's extremely reliable. The high-availability infrastructure continuously ensures your data's integrity and the quality of services offered to you.

INFRASTRUCTURE

Built-in redundancy allows for maintenance without any service interruptions to end users.

- >> Redundant power feeds from separate utility substations.
- >> Ten diesel generators with 19 megawatts of power supply backup for the entire complex.
- >> Separate rotary uninterruptible power supply (UPS) systems containing multiple 500 kilovolt-amp (KVA) modules can sustain power for 30 minutes before switching to generator power.

OPERATIONS SUPPORT

- >> Highly trained operations staff onsite 24/7/365.
- >> Proactive monitoring and troubleshooting are provided using state-of-the-art tools and processes.
- >> Trouble ticketing and automated problem escalation are used to ensure high availability.

FIRE

- >> Advanced fire control systems enable the detection of heat and smoke and use either HALON or CO² fire suppression above and below the raised flooring.

COOLING

- >> Six 400-ton cooling towers and multiple 25-ton air conditioning units with closed-loop systems are constantly monitored.
- >> 117,000 square feet of raised floor to accommodate cable management and uniform cooling distribution.

BACKUP SYSTEMS

- >> Incremental backups of all data are performed regularly.
- >> Disk-based backup systems allow NetFirm CS™ administrators to restore their firms' data.

SECURITY

24/7/365 internal security monitoring with camera surveillance at all entry points.

- >> Applications accessed via 128-bit secure socket layer (SSL) connections.
- >> Multi-zoned, multi-level keycard access controls and monitors all access to the data center and internal areas.
- >> Picture ID is required for entrance into any building.
- >> Vehicle identification is required.

NETWORK SERVICES

- >> Internet access using multiple providers.
- >> Gigabit Ethernet local area networks (LANs).
- >> Internet access through four OC-12 connections fed from four different providers at speeds of up to 2,488 megabits per second.
- >> Large installed base of equipment from Cisco Systems, Incorporated.

SYSTEMS

The Thomson Reuters data center offers one of the largest systems environments in the United States.

- >> Large installed base of Microsoft® Windows® and UNIX® systems.
- >> Storage Area Network: multiple NetApp metro-clusters providing redundant network-attached storage (NAS).



The Thomson Reuters data center takes every precaution to ensure the safety of your data and computer equipment. Built-in redundancy allows for independent operation and business continuance.



DATA SECURITY

PHYSICAL ACCESS

- >> Keycard entry system admits only authorized personnel and is logged and monitored continuously.

LOCAL ACCESS

- >> Servers within the server farm are required to use “secure channel” for data transfer.
- >> Several layers of network switching devices, each configured with a complex Access Control List (ACL), ensure that only specific network traffic is allowed to move between different logical networks.

REMOTE ACCESS

- >> Data moving over the public Internet is encrypted using Secure Socket Layer (SSL) protocol.
- >> Citrix Secure ICA (128-bit) encryption software encrypts the Citrix ICA datastream for Virtual Office CS™.
- >> Load-balancing devices provide port forwarding and proxy with built-in safeguards to prevent “Denial of Service” (DoS) attacks.
- >> Multiple levels of security allow elevated levels of control for maintenance personnel without compromising security—including private network circuits for Thomson Reuters management of data. Connections are secured at both ends with a firewall and a WAN router configured with an ACL (see Local Access above).

