

Why host with CU*Answers?

Because CU*Answers is already providing data center services for hundreds of clients and a million credit union members every day.

Data Center Information

WESCO Net Web Services leverages CU*Answers' extensive network experience and facilities to provide a scalable high-availability-ready platform. Our hosting servers are located in CU*Answers' secure SAS-70 Level II data centers. These data centers offer redundant power including generators and multiple Internet connections to increase availability of all services. Also, the hosting servers are backed up daily using a 3 stage disk-to-disk-to-tape backup scheme providing both quick restore flexibility and longer term archival protection.

WESCO Net Staff Information

WESCO Net keeps the CU*Answers Data Centers operational every day through regular maintenance, security patching and performance monitoring. In addition to wide-ranging experience, many WESCO Net employees maintain industry recognized certifications. At a minimum, WESCO Net staff members receive security training quarterly.

WESCO Net Network and Systems Teams members hold the following industry certifications:

- Cisco Certified Network Associate (CCNA)
- Cisco Certified Design Associate (CCDA)
- Certified SonicWall Security Administrator (CSSA)
- CompTIA Network+
- CompTIA A+
- CompTIA Server+
- CompTIA Security+
- Interactive Intelligence Interaction Center Certified Engineer
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Professional (MCP)
- Microsoft Certified Trainer (MCT)
- Zend Certified Engineer (ZCE)

Independent Auditing

Our networks, systems, and security procedures and policies are regularly audited by independent auditors, and CU*BASE and supporting network infrastructure is SAS-70 Level II approved. Our disaster recovery plans

have been independently audited and approved by an industry-leading disaster recovery and business continuity firm.¹ Additionally, regular spot audits using industry standard tools are performed against systems, networks, and personnel to ensure established security procedures are being followed.

Data Center Details

Redundant, SSL-Accelerated and Load-Balanced Web Network

Web Servers are housed on a separate, fully redundant network that includes

- Redundant DS-3 Internet connections
- Multiple ISPs provide multiple routes to the Internet
- Redundant routers utilizing BGP 4 technology
- Redundant Checkpoint border gateway firewalls
- Redundant F5 load balancing devices provide
 - High availability
 - Real-time failover
 - Traffic load spread over multiple servers
 - Custom traffic directing rules for custom load balancing algorithms
 - Additional firewalling capabilities via port filtering and NAT
 - Facilitates daytime security patching
- SSL (Secure Sockets Layer) accelerator hardware
 - Over 600 SSL session tear-down and rebuilds per second

Two-Stage Network Backups Using NAS Devices and Tape

Daily backups are automated and run from a centralized backup server. Most devices are backed up in two steps:

- Data is backed up across the local network to a secure shared NAS device. Data is maintained on disk for up to 10 days. Disk backups offer short backup windows and fast restores.
- Data on the NAS is then archived to DLT tape weekdays for offsite storage. Standard data retention is 21 days.

Network Security, Audits, and Intrusion Detection

Because no single step can make a network secure, CU*Answers subscribes to the layered security methodology for securing data systems. These steps include at least the following:

- Secure network architecture designed by security experts
- Systems segregated by task
- Controlled physical access to the data center and systems
- Controlled network access to all systems by enterprise-grade firewall and router systems
- Technical filters control all outgoing and incoming network traffic to help prevent unauthorized use

- Securing of the underlying operating system against known attack by using the manufacturer's best practice recommendations
- Disabling or removing all unnecessary applications and services
- Security review of applications for known vulnerabilities and configuration errors
- Host-based intrusion detection; all access to the host system is logged and reviewed daily
- Systems are regularly patched and kept up to date with the latest software updates
- Network-based intrusion detection alerts administrators to attacks
- Network-based intrusion prevention thwarts certain known attacks
- Anti-virus systems scan network, host, and PC traffic and content in real time for virus activity. Pattern files are updated hourly.
- A proactively trained and alert staff on the latest security vulnerabilities and responses.

Physical Datacenter Security

CU*Answers employs multi-level building access controls including:

- All guests must sign-in, wear visitor badges and be escorted at all times
- Employees must use electronic security keys to enter main building, and various secure areas throughout the center, entrance activities are centrally logged and monitored
- Video surveillance is used throughout the facility to monitor activity
 - Security tapes are stored in a secure off-site location
- Access to computer room is controlled through key code panels or electronic security keys
 - Operators staff the production datacenter 24x7 and monitor secondary access
 - Only authorized employees are permitted access
 - Employees who do not work in the datacenter are required to sign in and wear I.D. badges while in the facility

Power Protection and Continuance

- Liebert UPS uninterruptible battery backups maintain clean power to all servers even in the event of power loss.
- Natural-gas generator systems with auto-transfer switch backs up the UPS systems.
 - Generators are tested weekly

1 Retailer Direct is not considered a business critical function.