

CUDP Gets BakBone to Back Up CUSO's Client Systems, Secure Data

By MARC RAPPORT
*CU Times Technology
Correspondent*

FARMINGTON, Utah – Credit Union Data Processing Inc. (CUDP) was looking for an efficient way to back up data, and has ended up with a new, encrypted storage system to offer the 21 credit unions served by the Utah-based CUSO.

CUDP recently deployed the NetVault backup and recovery system from BakBone Software in San Diego, and has just added the company's encryption feature as a plug-in module.

Encrypting stored data, especially personal financial information, has become a hot-button issue in the financial services industry, as losses of unencrypted backup tapes drew headlines and attention from regulators.

That attention is reflected in sales at BakBone, the company says. "Last year we sold eight encryption plug-ins. So far this year, we've sold more than 125," says Dani Kenison, director of corporate communications at BakBone (www.bakbone.com).

The NetVault software directs the initial backup of data to disk. The data also then can be sent via VPN or other secured electronic transmission to offsite locations. Either way, that backup then serves as part of the organization's disaster recovery preparedness.

"Encryption then comes into play typically when you put that data on tape and send it somewhere else for

storage," says Charlie Keiper, NetVault senior product manager at BakBone. The NetVault system differs from much of the market in that the data is password-protected at the server level, instead of by a hardware device residing in the data path to storage somewhere else, Keiper says.

That eliminates the small window of vulnerability from server to hardware and also allows the data to easily be segregated and encrypted by areas internally, such as payroll, the company says.

At CUDP, the main concern is

making sure data are locked down as they move between the owner credit unions and the core processor's host servers for backup and storage, says Charlie Fulks, the CUSO's CEO.

"We were using it for network backups in our office and found that we could also do backups of remote servers, so now we can connect to all our credit union sites, including those with in-house systems, and do secure, offsite backups back to our data center here," he says.

Seventeen of the CUSO's credit unions – which range in size from about \$1.5 million to \$75 million in assets – have in-house systems, and five so far have begun using that service, Fulks says. The four service bureau users are protected that way automatically, he says.

"We wanted to guarantee that no personal data from

any of our credit unions' members would be vulnerable if a backup tape were lost or stolen, so we've gone to great lengths to make our VPN bulletproof and ensure that data are encrypted before traversing the networks," Fulks says.

BakBone says its software also aims to alleviate what it says is a dual concern of many managers charged with locking down local or far-flung storage networks and data paths: software-based systems can slow down a CPU, while hardware encryption devices that don't affect the network

or client/server performance can be very expensive, especially since they're typically installed in pairs for redundancy.

Fulks agrees.

"The fact that it's doing it through the client software on each server and leaves the network already encrypted, and is just a module plug-in, helps make this a very efficient, low-cost system, especially compared with what it would cost if we had to do it with hardware at each site," the CUDP CEO says.

CUDP (www.cudp.com) has to buy an encryption module for each site that's being backed up remotely. The software modules are priced at \$195 per server, the company says, while the NetVault backup and disaster recovery package ranges in entry price from \$1,195 for Solaris, Linux and Windows-based systems to \$2,995 for the UNIX Solaris 10 system.

"We're running UNIX in our office, with a Windows server, while all our credit unions are running an IBM AIX. It's been working great, and we haven't had any problems," Fulks says.

"We basically take snapshots of their whole systems every night and encrypt the whole thing,"

— mrapport@sc.rr.com



FULKS