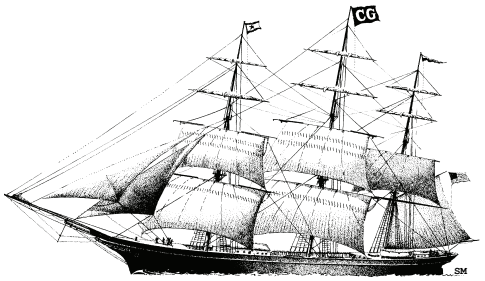
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006110 December 27, 2006

RedCannon — Answering the Needs of the Road Warrior and the DR Planner

Analyst: Dianne McAdam

Management Summary

Those of us that live in the Boston, New York City, or Washington, DC, metropolitan areas may find this story familiar. After completing a long workday in NYC, I took a taxi to the LaGuardia shuttle terminal for my return trip to Boston. It was 8 p.m. on a cold, rainy weekday night and the terminal was packed with tired, grumpy business travelers trying to get home to Boston or Washington as quickly as possible.

If you have traveled by air during the last few years, you are very familiar with the routine. Take your laptop out of the briefcase, take off your shoes, put everything on the conveyor belt, walk through the detection device, then gather all your belongings, and wait for the plane to be boarded.

While waiting for my plane to be boarded, an announcement was made – "could the person that took the wrong laptop please return it to the security desk?" The laptop was not returned that night. I wonder if the laptop ever got back into the hands of its rightful owner.

Imagine the poor owner of that laptop. He no longer has a laptop, he no longer has his data on the laptop (maybe he does have a backup copy somewhere), and, if he buys another laptop tomorrow, it may take him hours to get it properly configured with all of his software. If he is lucky, the laptop did not contain any sensitive or confidential data. If he wasn't so lucky, then he may have to disclose to his customers that their information is now in the hands of someone else.

Wouldn't it be nice if we could be productive on the road, without having to drag our laptop (and power cord and a host of other devices) with us? Not only would we have to carry around a lot less stuff, but also we would not have to worry about our laptop being stolen, being dropped, or accidentally left behind.

RedCannon has the answer for the road warrior – they transform a USB Flash drive into a secure thin client that contains everything you need to be productive on the road without dragging your laptop with you. Disaster recovery planners – take note. RedCannon's products can be very useful when a disaster occurs. Think about having all of the information that you need to be productive during extended outages in one very small portable device during extended outages. To learn more about RedCannon's products, read on.

First, the Weary Road Warrior

Many road warriors are IT consultants; their jobs require that they work onsite at different companies to install software, develop new applications, or tune existing applications. Some enterprises restrict consultants from bringing their own PCs onsite. Enterprises have many good reasons to restrict external PCs from their environment. They are concerned about virus infections being injected into their environment or unauthorized users downloading and removing confidential information.

Unfortunately, the consultant needs to periodically check his email or use his company's applications to report status information. This means the consultant has to leave the premises and find a coffee shop with wireless access to respond to

IN THIS ISSUE

emails and update status information. The enterprise that hired the consultant may not have a good impression about the consultant's work ethic – they may believe the consultant spends too much time drinking coffee and not enough time working at his assigned cubicle. Unfortunately, the consultant is just trying to keep two bosses happy – the company that needed his services and his company that gave him this assignment.

RedCannon solves this problem with *KeyPoint Access* that transforms a USB Flash drive into a secure thin client. KeyPoint Access integrates RSA *SoftID* with *Citrix*, email, VPN and web clients with anti-spyware and a data vault. Now the consultant can plug the RedCannon device into any Windows workstation to access his email and applications securely without having to leave his cubicle and find a wireless network and without leaving any traces on the "borrowed" workstation.

RedCannon KeyPoint Vault

Road warriors have many different jobs. You may be a product manager traveling around the country giving sales presentations that confidential information about new products to customers. You could drag your laptop into each new account, untangle the power cords, find an available outlet, power it up … wait a few minutes … and start your PowerPoint presentation, or you could simply use an existing PC or workstation, slip in the RedCannon KeyPoint Vault Flash Drive and bring up your PowerPoint presentation. KeyPoint Vault allows enterprises to distribute content to authorized personnel and store the content in an encrypted (and compressed) format preventing unauthorized people from accessing the contents of the flash drive. If the flash drive accidentally finds its way into the wrong hands, then the contents can be deleted remotely. Now, enterprises have a central way to distribute and manage sensitive information.

RedCannon's solutions are a boon for the traveling IT consultant or the high tech product manager but serve other professions as well. For example, corporate accounting professionals may be required to travel to regional offices or divisions to audit documentation and discuss accounting practices within that office. RedCannon allows these professionals to work at remote locations in a secure way. During the discovery phase, corporate attorneys may also be required to travel to different locations to gather evidence. Again, these professionals can accomplish their mission while maintaining the proper levels of security.

On to Disaster Recovery

KeyPoint Vault is not just for people who travel extensively but can be a valuable tool for those displaced by a disaster. Let's assume that a data center located in the southeastern part of the United States has been subjected to hurricanes over the last several years. Disaster recovery planners within this organization have compiled documentation that includes recovery plans and contact lists containing the home addresses and phone numbers of the executives. This information is important in case of a disaster; however, this information contains sensitive information that must be managed carefully and must always be current. Some organizations distribute printed copies of the DR documentation. These organizations have no assurances that the outdated reports are properly shredded. KeyPoint Vault can solve this problem. People that need to know can be assigned KeyPoint Vault Flash Drives. Whenever changes are made to the documentation, the updated content is distributed to the authorized people. This ensures that everyone is working from the correct version of the list. Other critical information, such as contingency plans, password lists, vendor support numbers, and any other documentation that is critical during and after the recovery operation can also be distributed. If the drive is accidentally misplaced, the content can be deleted remotely.

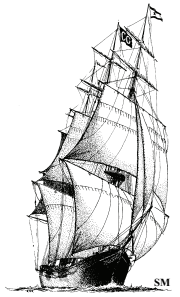
Recent events, such as the flooding in New Orleans from the effects of Hurricane Katrina, have forced disaster recovery planners to broaden their scope. No longer can DR planners be only concerned about a local event, such as the loss of electrical power to a building. They must also plan for a regional event that can cause outages that strength for miles. Regional disasters can force employees to work from remote locations for days or weeks. DR plans must accommodate employees that have to access systems remotely for an extended period of time. While natural disasters, such as flooding, can make buildings uninhabitable, the threat of diseases, such as Avian flu, can also make intact buildings unsafe for workers to enter. Again, RedCannon's KeyPoint Access can provide workers with a way to log on to email and other systems from any location without compromising security.

Conclusion

Laptops have given workers a great deal of mobility. It allows workers to access systems from any location that supports LAN or wireless connections. But this mobility comes at a price. The accidentally loss or theft of laptops that contain confidential information violates privacy laws and gives companies unwanted publicity that can take months, or even years, to overcome.

Distributing laptops to all employees that may have to travel can be an expensive proposition for any company. Laptops that are not lost or stolen need to be replaced periodically. They can break or must be replaced with more powerful machines to keep pace with compute-intensive applications. RedCannon can eliminate the need to purchase, fix, and upgrade laptops and that can save on capital and operating expenses.

Road warriors need a secure way to conduct business while "on the road". Employees relocated by natural (or unnatural) disasters also need a way to continue to work at remote locations. RedCannon's KeyPoint Access gives them the ability to access systems without requiring them to own a laptop – any workstation will do. The addition of KeyPoint Vault gives displaced workers access to key documents without requiring access to enterprise systems. Road warriors and DR planners should evaluate RedCannon's solutions. It can make their life simpler and more secure.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.