THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2006026 April 19, 2006

RedCannon's *KeyPoint* — Secure Remote Access to Enterprise Systems

Analyst: Anne MacFarland

Convenience is the rallying cry of many markets these days. Of course, what defines convenience may vary. For some it is a matter of location, for others a matter of the expanse of inventory (or the precise focus of inventory), or the ease of doing business. Enterprises struggle to meet these demands for convenience, while, at the same time, meeting operational requirements for process efficiency and security. For, while enterprise operations may seem like mere extensions of the e-commerce with which we are all familiar, they have different requirements. The amount of critical data that must be given protection in a shopping transaction is limited. In business, the whole process, and evidence that it took place, must be routinely secured. While a commercial experience, once the seduction of marketing has secured the desire to buy, must be kept simple, business processes often need considerable local functionality to be effective.

There has always been a dynamic tension between the secure efficiency of back-end operations and the opportunism required by customer-facing operations. When you add in the *process transparency* demanded by the impatience of the modern marketplace, the tension is increased. More workers are dispatched off site, but they are often armed with minimal functionality because *out there* is seen as inherently insecure. Laptops can be stolen or lost. The information on them can be stolen or compromised. They are still too expensive to be used by the majority of the distributed work force and too big to be easily secured.

To further speed business processes, enterprises need to give their workers, wherever they are, more functionality without adding more risk. Ideally, the worker's environment would be contained in a secure shell and use local resources, rather than a dedicated laptop. RedCannon Security, based in Fremont, CA, offers just that, by separating the IT client environment from the device that connects it to the Internet. Their *KeyPoint Access* assesses the local *Windows* client computer for Trojan horses, key-loggers, and spyware. It creates a shell inside which a secure session of enterprise applications, delivered with the full functionality of the local workstation, can be safely supported. When the session is over, there is no evidence of the enterprise functionality left on the host computer.

The RedCannon approach has broad relevance for any enterprise with personnel who do substantive work on the road. Citrix is using RedCannon's KeyPoint Access as an option for their thin client delivery. Service enterprises and consultants, who don't want to leave their expertise behind unintentionally, could benefit from this approach. If the idea of safe use of local resources, and the way it could rewrite the economics of doing business sounds attractive, read on for more details.

IN THIS ISSUE

The Ideal Enterprise Client

For mobile business use, there are certain requirements for the ideal client. It should be *portable* and *protectable*, so productivity can be wherever the worker is. It should be potent enough to afford the worker a complete interactive environment wherever, irrespective of the availability of access to the Internet. But, most importantly, the client must be *secure*. Insecurity in the client obviates any benefits you get from its being easy to take with you and potent to use.

With RedCannon's KeyPoint Access thumb drives, enterprises can rethink how they provision their workers. Local and other people's equipment can be safely leveraged, for nothing is actually installed on the local or borrowed equipment, and, upon removal of the USB device, nothing is left behind.

The enterprise can customize the KeyPoint environment for a variety of roles. The KeyPoint Access device will synchronize with the KeyPoint Management Server when it is connected securely to the enterprise environment. New functionality also can be dispensed by a quick swap of KeyPoint Access thumb drives.

How RedCannon's KeyPoint Access Works

KeyPoint Access is an ultra-thin client that can attach to a client device via a USB port, but it is far more than a memory stick or an authentication token. It is, itself, encrypted and password protected. It can scan the environment to which it is connected for key-loggers, Trojan horses, and spyware before a SSL session is initiated. If the environment is clean, it will set up a shell environment that will allow applications to be used safely and privately. If the environment is infested, it can either clean up the environment or alert the user that he or she must seek another device to host a secure connection.

KeyPointAccess comes in capacities from 256 KB to 4 GB, generally enough to hold key enterprise application clients and data. It is meant to be used in a connected mode, but can also support some functionality when running on an isolated device. At present, KeyPoint Access uses *Windows* infrastructure to connect to the Internet. In the future, *Linux* may be supported.

Every RedCannon device is part of a larger, policy-managed system[1]. Enterprise IT sets policies covering how they are provisioned, how usage is tracked, and how functionality is restricted for certain users. Back end *KeyPoint Management* is provided by a server[2] that sits in the DMZ. This server centrally manages up to 10,000 mobile KeyPoint Access clients. It provisions users and recovers passwords, securely pushes data and applications, and generates regulatory compliance reports. KeyPoint management can remotely destroy data on a device if it is stolen. With the proper policy installed on the device, it can respond locally to brute force hijack attempts. KeyPoint Access devices can even "get around" PCs that "don't allow" downloads.

Every time the device is unplugged, it uploads (encrypted) usage information to a central site. Every time it is plugged in, it connects to the central site and gets downloads and policy updates. All usage logs are in standard XML format. At the central site, logs are analyzed and reports, including the reports needed to support regulatory compliance, are generated. The logs can also be used for business process analysis.

KeyPoint Access leaves no trace of user activity on the host computer. Cookies are stored locally on the KeyPoint Access device. It also encrypts the memory area of the PC processor it uses. Support for RSA, OATH, digital certificates, and two-factor authentication is built in. It has received FIPS 140-2 Certification.

Ramifications of the KeyPoint Approach

KeyPoint Access facilitates using a wide variety of edge devices in a wide variety of situations. With KeyPoint Access, a mobile worker can create a secure environment within a shell on any PC and get work done. KeyPoint Access could facilitate the portability and

[1] This differentiates KeyPoint Access from consumer-style devices that fall outside of, and area threat to, the effectiveness of business governance.

[2] *KeyPoint for Citrix* is completely compatible with *Citrix SecureAccess Gateway 4.0,* and can be used for internal temporary access and testing of new services as well as in remote locations without a Citrix-provisioned laptop. RedCannon is a Citrix Global Alliance Partner.

privacy of medical records (and the applications needed to present them) for a patient being shunted from one health care facility to another. Offices could have fewer workstations. As all the applications are on the device, full SOX compliance and business governance audit capabilities are built into the solution. Moreover, while the solution is confined at present to Citrix environments, it could work elsewhere.

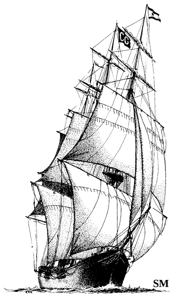
The aggregation of portals provides access to information for roving workers, but integrated functionality, delivered at the point of productivity, is also key. The software revolution of service-oriented architectures allows applications to be more easily integrated as complimentary services. An appropriately-sized, secure, and portable environment for these service aggregations will be increasingly important.

The KeyPoint Access solution presents a significant opportunity to value added resellers and service providers, particularly in industries like Financial Services, Government, Manufacturing, and Health Care, where extreme mobility with low overhead is beneficial to the business, and where there is sensitive information that must travel as well.[3]

Conclusion

The capabilities of technology have, in the past, often changed how you had to do business in ways that were unattractive. RedCannon gives you an opportunity to rethink how you do business to reduce business risk, increase worker mobility, and manage change effectively. It's a *win-win* opportunity for the business-on-the-go that should not be overlooked.

Uncontrolled usage of business information and processes is a risk waiting to become a calamity. The need to do business wherever it arises has always had security trade-offs – until now. Think of how you could do business with fewer constraints by using this approach to mobile enterprise functionality.



[3] RedCannon also offers *KeyPoint Vault*, an encrypted thumb drive for data only.

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

Anne MacFarland **is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" 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.