THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2007078 August 2, 2007

Collaboration with Security — Imera's *TeamLinks*

Analyst: Anne MacFarland

Management Summary

The recent championing of collaboration's role in business – as contrasted, perhaps, with *death by cubicle* – brings needed re-emphasis on the human side of business. The preceding hyper-focus on technology as the basis of success, like the emphasis on the mechanical reaper and, later, the efficiency of factory floors, was justified, but missed the point. Technology lays the table for a feast of profitability, but the quality of the feast depends on good planning and a great kitchen staff – all human activities. This is more than a reprise of the era of teaming – for **the Internet and many software developments give far more options for collaboration, but with them come risks.**

When the collaboration happens over external networks, and it will, some organizations start to get worried. They want to collaborate, but they do not want to lose control of the process, or to add new sources of risk to their corporate environment. For many organizations with large research and development initiatives, savage competition, very sensitive information to protect – or all of the above – this is more than a chronic worry. It is a matter of corporate survival. They realize that, without good collaboration, they lose critical time to market and cannot thrive. With the wrong kind of collaboration, they may empower their enemies, alienate their customers, and squander all they have built.

A company named Imera, based in San Jose, CA, has developed collaborative software that comes with a link of highly-proprietary, non-reverse-engineerable transport protocol. It was co-founded by ex-Cisco folks, who felt that many networking approaches glossed over some substantial networking issues. **By creating an unhackable, very-not-open network protocol, they secure collaboration without demanding changes to either data center or to network security. Their approach allows authenticated individuals to have full access – not to enterprise networks, but to the specific applications they need.** Within the context of theses applications, Imera provides the collaboration software to share desktops, annotate, and trade desktop control back and forth.

This process is fully auditable and meets the standards of the payment card industry and the US Department of Defense. As the one-way valves that make our bodies' systems of veins recirculate our blood properly, Imera's team spaces have the regulation and security that surpasses some other approaches. If paranoia seems a healthy attitude in your line of work, you will want to read on for details.

IN THIS ISSUE

Collaboration Accelerates the Pace of Business

Pre-scheduled meetings are great for imposing a cadence on business, but they are insufficient for increasing its pace. They shortchange the value of participation by making it an obtrusive exception rather than an inherent part of process. E-Mail's civility, as opposed to phone tag, started building the pace of working together. A more peremptory Instant Messaging, often tempered these days by presence awareness, lets the immediacy of collaboration be negotiable.

Collaboration software can recreate the collegiality that happens when co-workers are co-located. It can extend it opportunistically to more people and more places as the need arises – something that you can't do if closeness comes in cubicles.

As more and more business processes are supported by technology, the focus of collaboration is frequently some kind of digital artifact in an application. Sharing an application session must be a managed process. Sharing it across security boundaries must also be carefully managed. And, if the opportunism of collaboration results in a litany of tweaks to application and data center security, it is difficult to support.

While the users want the ability to work from home and the ability to share applications with team colleagues, the Data Center must secure the applications and their data, secure the business process, secure the data center environment. In many key applications in sensitive industry, IT is charged with maintaining an audit trail.

Other approaches to collaboration security

For these higher-security situations, VPN[1]s, even with SSL, offer inadequate documentation. They document what IP address is talking to what IP address, but not who is doing what and in what order. In these same situations, distributed servers may pose an unacceptable risk, as well as a costly management headache. The good news it that the Imera *TeamLinks* can address the challenge of secure management of remote equipment as well as the need for off-site collaboration.

Imera TeamLinks

Imera TeamLinks is deployed in an appliance that sits in the DMZ on the edge of corporate networks. It can inherit with LDAP or Active Directory access control lists. The Imera protocol is carried on a SSL session out to remote participants beyond the firewall. Those participants download an Imera TeamLinks agent.

In the ISO Stack, Imera's protocol sits beneath the application and over the physical infrastructure. Administrators can specify what IP addresses can connect to which application without interfering with existing application or infrastructure security. Because the protocol is proprietary and purpose-built to foil reverse engineering, *nothing can take data out of the data center.* This is not true with other thin or managed client approaches, and they all require adjustments to existing security.

A session initiator can drag and drop his name to join Joe Smith to a session, or you can set up a separate session and merge them together. The initiator of a session can cede control to another participant who asks for it. The participant can then annotate. The initiator can always take back control.

TeamLinks has all the expected team features. All keystrokes can be captured, and a transcript of the collaboration generated. The full audit trail allows actions to be captured as a part of the development process.

While participants can see, they cannot write, print, or save. If permitted, they can take snapshots, but this is of a bitmap, not of data. Where even this risk (small, among known participants) is a problem, snapshots can be disabled.

TeamLinks includes IPVoice, which cuts telecommunications expenses for people working at home. Applications like CAD can be shared over distance, as an alternative to expensive duplicate deployments. In such cases, email is not an adequate option.

[1] Virtual Private Networks.

Imera TeamLinks collaboration also offers an alternative to the use of Web Conferencing. Agents can be used by external participants, and then rendered invalid. In both cases, the Imera link is fully secure and does not conflict with data center security.

The policies that administrators can set are very flexible. Collaboration policies can be granular to the individual. They can be asymmetrical. The owner of the Imera appliance has rights to full audits. If multiple organizations wish to collaborate as peer (each with audit rights), Imera appliances will federate (in the manner of e-mail servers) to provide audits to all owners.

TeamLinks supports not only collaboration, but also remote management of IT environments, monitoring of outsourced IT resources, and customer support. To be used for remote support, the customer with ailing technology can point to a URL and join a session where a technician can take control and safely look at exactly what is going on. It can be used in IT outsourcing situations to monitor operations without touching any security. Imera was named a recognized innovator in 2006 by the SSPA[2] technical service and support industry association.

Because Imera is a closed loop environment, it can be compliant with security at both the data center and a remote location. Therefore, it provides a good way to manage unattended computers. In this mode, Imera adds an additional level of visibility and security that may be useful to many organizations. In addition to the access controls provided by active directory or LDAP, Imera maintains an access control list for resources of the unattended computer resources, with a separate password.

Building on all the capabilities described above, Imera can be used as a multi-user gateway to allow multiple users to share multiple resources. Because the secure Imera link is separate from and not integrated with site security, complex user collaborations are both secure and easy to set up and maintain.

Pricing

Pricing includes a nominal base price[3] for the appliance, and a per user fee that depends on multiple factors. It depends on the number of logged-in users, the number of concurrent, screen-sharing sessions (IM alone does not count), and the number of total participants. For comparison with traditional Web conferencing, the price per logged-in user, over three years, comes to under $20/user/month for ten users and a maximum of two concurrent sessions, and just 60 cents/user/month for 100,000 logged in users and 2000 concurrent sessions.

For many organizations, the power collaborators who use heavy-duty applications and sensitive information represent a small fraction of the total workforce. In such situations where security is key (think of activities like product design, medical collaboration, or supply chain negotiations) and where time to market is just as important, Imera offers many interesting capabilities. Think of them for those times where "openness" is a really, really bad idea.

Conclusion

Imera gives remote access without using traditional network access. It facilitates viewing information without transporting information. It is not an anti-information solution, but an information control system. It dances between end users and enterprise data systems like an aquatic water-strider that skitters atop the surface tension of the water in a pond in its own peculiar (in this case, proprietary) way and plays on both sides of the boundary. If you want a richer degree of collaboration with a high degree of security and a low impact on the status quo, take a look at Imera.

[2] Service and Support Professionals Association.

[3] $1,000, $3,000, or $4,000 depending on the number of users and concurrent sessions (U.S. pricing).

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**, **Clipper Notes**, 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.