Pragma Systems & Stay-Linked™: Remote SSH Connectivity Done Right

This paper is designed to serve as a primer for upgrading – or choosing and implementing – a highly effective, secure SSH connectivity solution. This document provides an overview of key regulatory and market developments driving the need to make remote computing systems more secure; takes a look at the origins of SSH and the factors that have led to its becoming the enterprise security protocol of choice; outlines key components of an optimal SSH-based security approach; and, then, examines the market's most trusted, effective, end-to-end, server and client SSH security solution, offered in partnership by Pragma Systems and Stay-Linked.

Contents

Pragma Systems & Stay-Linked™: Remote SSH Connectivity Done Right

Executive Summary

Over the last few years, more and more companies have opted to upgrade from Telnet to a more secure remote-computing solution. Driven either by regulatory compliance or irresistible advances in mobile-device capabilities, most firms have either taken steps to upgrade their network security or are in the process of evaluating an optimal approach – and, as they do, questions abound over the what, when, why and how of implementing a customized, fully functioning, end-to-end secure connectivity solution.

Where should remote security start and stop? Which approach works best in which environment? Is there really a solution that can handle security not just on the company servers, but on all of its remote clients, both inside and outside the four walls, and all the way back to the host?

This paper is designed to serve as a quick primer for either upgrading an existing – or choosing and implementing a new – system to create a highly effective, secure connectivity solution. We start by examining the recent trends underlying enterprise-level remote computing. Then, we take a look at key areas to consider when making the shift from FTP, Telnet and other system-administration methods to the implementation of SSH, enabling truly secure logins and command execution over unsecured networks and between hosts. Finally, we provide an overview of the end-to-end SSH solution provided by Pragma Systems and Stay-Linked, the market's most trusted and experienced SSH server and client solution.

Takin' it to the streets

It's not uncommon these days to see employees using handheld devices to check inventory at a warehouse; gather information from the field; track product across multiple checkpoints; and, then, transmit that data to a home office from a car or an airport lounge. In 2010, Forrester estimates that 75 million employees will have become "mobile" – and the firm projects that the demand by workers to access corporate networks remotely will, accordingly, increase exponentially in the years ahead.

Given the large amount of federal privacy and data-protection regulations, not to mention the increasing technical acumen now exhibited by garden-variety Internet criminals, allowing employees to have remote access to the network via Telnet protocol is increasingly untenable in an enterprise setting. Having stated that, we all know change-resistant users and companies who are reluctant to make the shift. But, as companies and their employees redefine the geographic sweep of the workplace, Telnet's inherent weaknesses underscore its status as a fundamentally insecure approach to mobile computing.

Clearly, it's time to leave clear text behind

Among the key issues that, left ignored, add up to either a costly security breach and/or being caught flat-footed not adhering to various federal or state data protection standards:

- **Clear-text transmission**: All communications done in clear text, including usernames and passwords
- **Weak client authentication:** Telnet authenticates users through usernames and passwords that, time and time again, have proven to be unreliable authentication methods, and offer no support for advanced methods such as public/private key, Kerberos or digital certificates
- **No server authentication:** Users have no way to confirm that they are communicating with their intended server instead of an attacker impersonating the server
- **Absence of data integrity:** Anyone can alter and corrupt data being transmitted between server and the client without detection

Regulatory rundown

Although most of us are well aware of the federal regulations put in place over the last decade to protect consumer and corporate privacy, it *is* worth keeping them "top of mind" when putting in place an optimal remote computing solution:

- **PCI-DSS (2004, updated January 2009):** This payment-card, industry data-security standard regulates how credit card information is processed, stored and transmitted. The lack of encryption, weak authentication, and the absence of data integrity render Telnet completely unsuitable for supporting the standard's requirements on a wireless network.
- **GLBA (1999):** The Gramm Leach Bliley Act requires the financial industry to adequately protect customer data information – again, an unrealistic expectation with Telnet or FTP.
- **Sarbox (2002):** Sarbanes Oxley requires the implementation of solid internal controls to guarantee that financial reports properly reflect the economic reality of any publicly traded company. Most auditors reviewing IT systems tend to require the shutdown of Telnet or FTP remote-computing activities.
- **HIPAA (1996):** Among other things, this healthcare industry regulation requires doctors to encrypt and protect their patients' information – again, not possible with Telnet or FTP.

CUSTOMER STORY:

Global Grocer Needs PCI-DDS Compliance from Pragma, PDQ…

The world's leading retailer of natural and organic foods, *with more than 200 retail outlets in North America and the United Kingdom, faced the need to effect compliance with the global Payment Card Industries (PCI) Data Security Standards (DSS).*

To effect its compliance with the PCI DSS, *the grocery concern urgently required a system that could work seamlessly with the IBM point-of-sale system it had already put in place to effectively secure its network connections. Key requirements: A way to remotely establish secure connections with its 265 stores, facilitating the secure transfer of files between all levels of its operations****. To fully comply with PCI, the grocer's technology team knew it needed to migrate its more than 300 users in seven regions toward a secure SSH and SFTP environment.***

The retailing giant turned to Pragma's market-leading FortressSSH ClientSuite, which gives organizations the ability to secure networks comprising desktop, laptop, industry-standard mobile and handheld devices. ***"Once we met with Pragma, our choice was clear,"*** *explains a company manager. "After reviewing our options, we knew Pragma Systems, with its Fortress suite, its deep experience in helping companies effect secured communications, and its ability to integrate seamlessly with our existing technology, would be the quickest path toward helping us meet the stringent requirements of the PCI DDS. Pragma's FortressSSH allowed us to effect complete compliance with the PCI.* ***After submitting evidence of our FortressSSH installations to external auditors, we were deemed to be PCI compliant. Problem solved."***

CUSTOMER STORY:

Marshfield Clinic & Pragma Systems: HIPAA, the SSH Way

The Marshfield Clinic system *is one of the largest private, comprehensive medical practices in the United States, with 792 physicians representing more than 80 different medical specialties and subspecialties, 6,474 support personnel, and more than 40 locations in 35 Wisconsin communities throughout northern, central and western Wisconsin.*

Faced with the ***need to comply with HIPAA requirements****, the Clinic needed a secure way to proffer secure access to its production servers, allowing its programmers to remotely examine logs and real-time status messages from custom-developed applications. Infrastructure Systems Manager Derek Dieringer said Marshfield Clinic also needed a secure way to grant select programmers concurrent access to deploy and execute programs. Making matters more complex, Marshfield Clinic development staff needed secure concurrent access to the development servers to deploy, run, and debug programs prior to deployment on production servers.*

"The challenge essentially was that our programmers needed remote access to our servers to be able to monitor logs and start and stop jobs they had written," explains Dieringer. Marshfield Clinic turned to Pragma Systems and its Fortress SSH Server technology – and a legacy relationship was born. ***"We turned to Pragma Fortress SSH Server, which afforded us secure access through SSH to all needed servers,"*** *Dieringer said. "All of our Marshfield Clinic custom-developed applications and tools are designed to run from the command line, making Pragma and SSH a perfect fit." Other potential solutions proved to be "overkill," reports Dieringer. "They provided too much access at too high a cost.* ***Pragma's Fortress SSH was built from the ground up to do exactly what we needed.****"*

Moving beyond the promulgation of straightforward regulation, the federal government also recently kicked off a six-month study of its data centers (2010), the findings of which will lay the groundwork for a sweeping, public data-center consolidation effort. In the wake of the federal announcement, the City of New York also began a similar initiative. As government agencies work to streamline data-center and storage capabilities and place more and more functions within the "cloud," many industry watchers expect these broadscale initiatives will usher in still further data and privacy protection regulation aimed at ensuring remote computing security.

Gaga for gadgets

Perhaps more compelling for companies still clinging to Telnet: it is increasingly tough to resist the never-ending parade of time and money saving remote devices. New mobile phones and handheld computing devices from the Motorola/Symbol MC9090 to LXE's MX7, Psion Teklogix's PTX7535 to Intermec's CK3 are incenting more and more companies to expand their mobile offerings and capabilities. With the help of companies like Datalogic and its Kyman, companies are hitting the road, boosting productivity and capturing the cost and efficiency dividends made possible by the real-time transmission of mission critical data.

So….adding it all up, it's time for a change…

According to a 2008 Forrester study, the total cost of a security breach runs $90-$305 per record breached. That means, for example, that a breach involving a simple text file containing 5,000 names, addresses and Social Security numbers or credit card numbers would end up costing the average company $450,000-$1,525,000. That's a price few businesses can stand to pay – particularly when an upgrade to an end-to-end SSH solution costs only a fraction of that amount. The bottom line? Upgrading to a more secure remote computing solution is about more than the sum total of the technicalities, it's about how much you put your business at risk – and what the end price you pay for continuing that risk will eventually be.

CUSTOMER STORY

An IT Director tells a friend about Stay-Linked...

Chuck:
I recall you mentioning ***some software you were very satisfied with for maintaining RF sessions on the I5.*** *I was in Elkhart yesterday and they were expressing frustration with shop floor connections dropping. Do you know what I'm talking about?*

Scott:
This is great stuff – stay-linked.com. *It moves the telnet session internal to the i5 and extends the session over the wire – similar to a Citrix protocol – UDP instead of TCP. The packets are small and fast back and forth to the i5.*

You can literally remove the RF battery and when the device revives itself and boots you are right back in the session waiting for the next keystroke. You can take control of a session or just watch it – great for support purposes. Or move it to another device.

The proprietary RF client installs on a wide range of devices and can be locked down and made automatic. I have the RF devices setup to boot to a sign on screen – or if they already are active in a session then they get that. It does it every time.

Server runs on windows or i5 – I have mine on the i5. There is a windows admin client I run on Vista to manage the i5 server program – sort of like ops nav. ***Service is*** *as* ***good*** *as TL Ashford****. Just call / email and they help.***

This is so much better than having to try to get the last 5 nines of reliability on your wireless coverage.

-IT Director for a Major Manufacturer

…but…to *what?*

If you're reading this paper, odds are you're either in the market for an upgrade or your company recently made the step up from Telnet or FTP. Telnet was easy, user friendly and, despite its lack of security, phenomenally flexible. Now that it's time to make a change, the field is flooded with companies selling competing, complex solutions, making it even tougher to figure out the right approach. Too many companies promise to solve it all – and the "all" hasn't been well identified.

If you've morphed to using IPSEC or other types of SSL-based solutions, you know firsthand how time consuming, complicated and unwieldy these types of solutions can be. You're also likely to have experienced multiple points of failure. End-users hungry for critical productivity enhancements can find themselves swept up in a sea of complexity, training and day-to-day challenges. The fact is, nothing is easier to use than Telnet, thus making the transition to an IPSEC or SSL-based approach even more painful.

If your organization is like most, your speed of implementation and ease of use is as important as the security benefits you seek in a move away from Telnet or other insecure protocols. When it comes to mitigating the pain of such an approach, more and more companies rank SSH (Secure Shell protocol) as one of the best ways to "check off the boxes" associated with network security.

> ***CUSTOMER STORY***
>
> ***Putting SSH in the Field for Motorola***
>
> *Motorola—known around the world as an innovator and leader in wireless and broadband communications—designs and delivers "must have" products and powerful networks, and offers a full complement of support services. A Fortune 100 company with global presence and impact, Motorola, which employs more than 66,000 in 30 locations worldwide, had sales of $22 billion in 2009.*
>
> *One of Motorola's cutting-edge biometric products, the Mobile Automated Fingerprint Identification System (Mobile AFIS), provides remote and timely access to fingerprints, facial images and criminal history. This widely deployed identification and verification tool provides governmental entities with immediate access to essential information, even in outlying and mobile locations. Simply put,* ***Motorola's Mobile AFIS gives law enforcement officers the ability to securely establish an individual's identity in real time, while they still have face-to-face contact in the field with potential suspects.***
>
> *In line with the integrated communication provider's commitment to maintaining the cutting-edge functionality, security, and overall value of its Mobile AFIS offering, Motorola conducted a detailed review of the market's leading data-in-motion security providers. The company's goal? To identify a technology partner that could significantly upgrade the security and feature set of the Mobile AFIS communications capabilities.*
>
> *Motorola's decision? A team that included Pragma****. "The combination of security, functionality and value that the Pragma team offered was particularly important for Mobile AFIS*** *because most state and local police forces have limited budgets for solutions like these," explains Anthony Esquivel, Manager, Marketing Communications and Mobile AFIS product line, Motorola Networks & Enterprise.*

SSH: The Once and Future Protocol

A network protocol that allows data to be exchanged using a secure channel between any two networked devices, SSH was, in fact, designed from the ground up specifically to serve as a replacement for Telnet and other insecure remote shells. Invented in 1995 to replace Telnet and FTP, SSH uses encryption to ensure the confidentiality and integrity of data transmitted over insecure networks. With the right SSH solution, a company is able to protect itself against:

- Eavesdropping of data transmitted over any network
- Data manipulation at intermediate elements in the network – i.e., routers
- IP address spoofing
- DNS spoofing of trusted host names/IP addresses; and
- IP source routing

Over the last 15 years, the role of SSH has expanded to become the *de facto* industry standard for secure remote access, secure file transfer, and secure tunnel connection. Perhaps more important, SSH has become the secure delivery transport of choice for delivering applications from servers to desktop and mobile clients. From Cisco routers to corporate production servers, SSH – an IEEE draft standard – can be used across platforms, including Microsoft Windows, UNIX, Apple Mac and Linux, for:

- Login to a shell on a remote host (replacing Telnet and rlogin)
- Executing a single command on a remote host (replacing rsh)
- Copying files from a local server to a remote host
- In combination with SFTP, as a secure alternative to FTP file transfer
- In combination with rsync to backup, copy and mirror files efficiently and securely
- Forwarding or tunneling a port
- Forwarding from a remote host (possible through multiple intermediate hosts)
- Browsing the web through an encrypted proxy connection with SSH clients that support the SOCKS protocol
- Securely mounting a directory on a remote server as a file system on a local computer using SSHFS
- Automated remote monitoring and management of servers through one or more of these mechanisms; and
- Secure collaboration of multiple SSH shell channel users where session transfer, swap, sharing, and recovery of disconnected sessions is possible

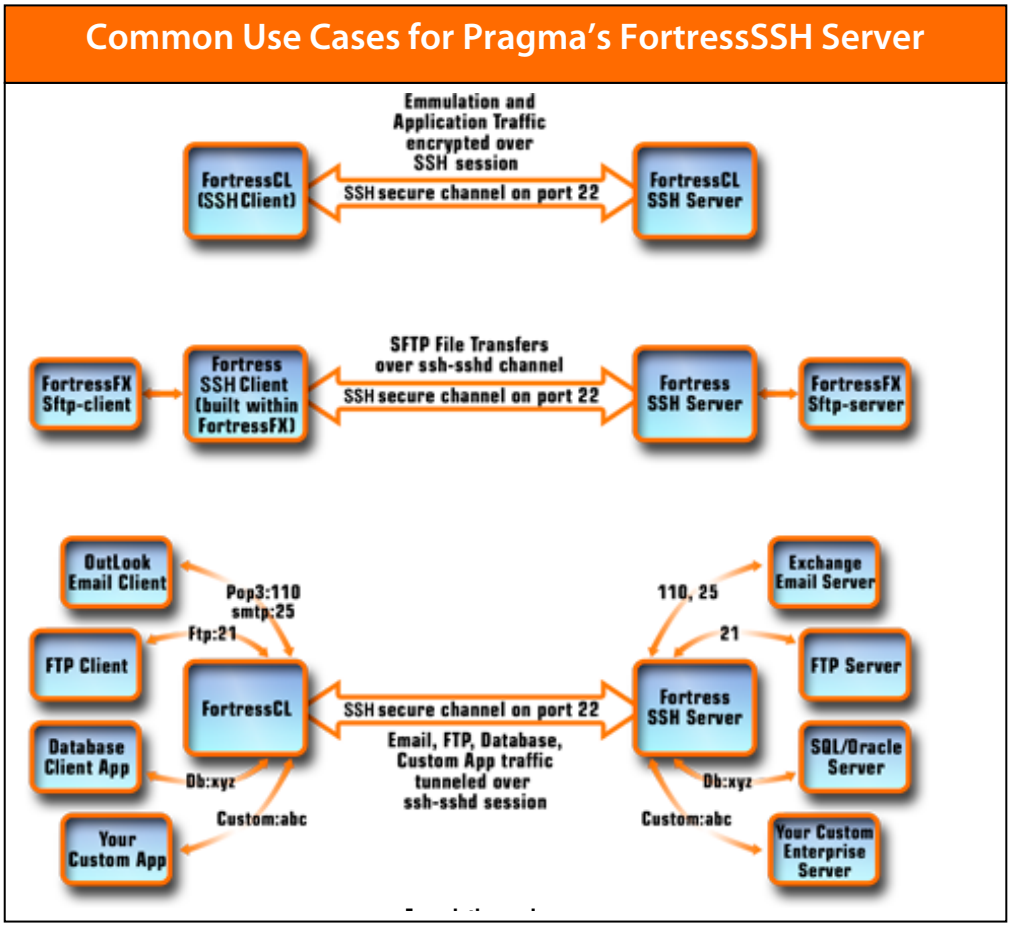
So, after weighing all of these considerations SSH seems like the right approach. But, when it comes to putting in place an easy to deploy, end-to-end remote computing solution that works with your legacy host computing, where do you turn? Who does SSH right? What works best with your Windows driven environment? And, is SSH alone enough to support everything your company needs and wants to do from the field?

Pragma Systems + Stay-Linked = Remote Network Security Done Right

If your company operates a Windows environment and uses Telnet for host application access, you owe it to yourself to look at the solution stack offered by Pragma Systems and Stay-Linked.

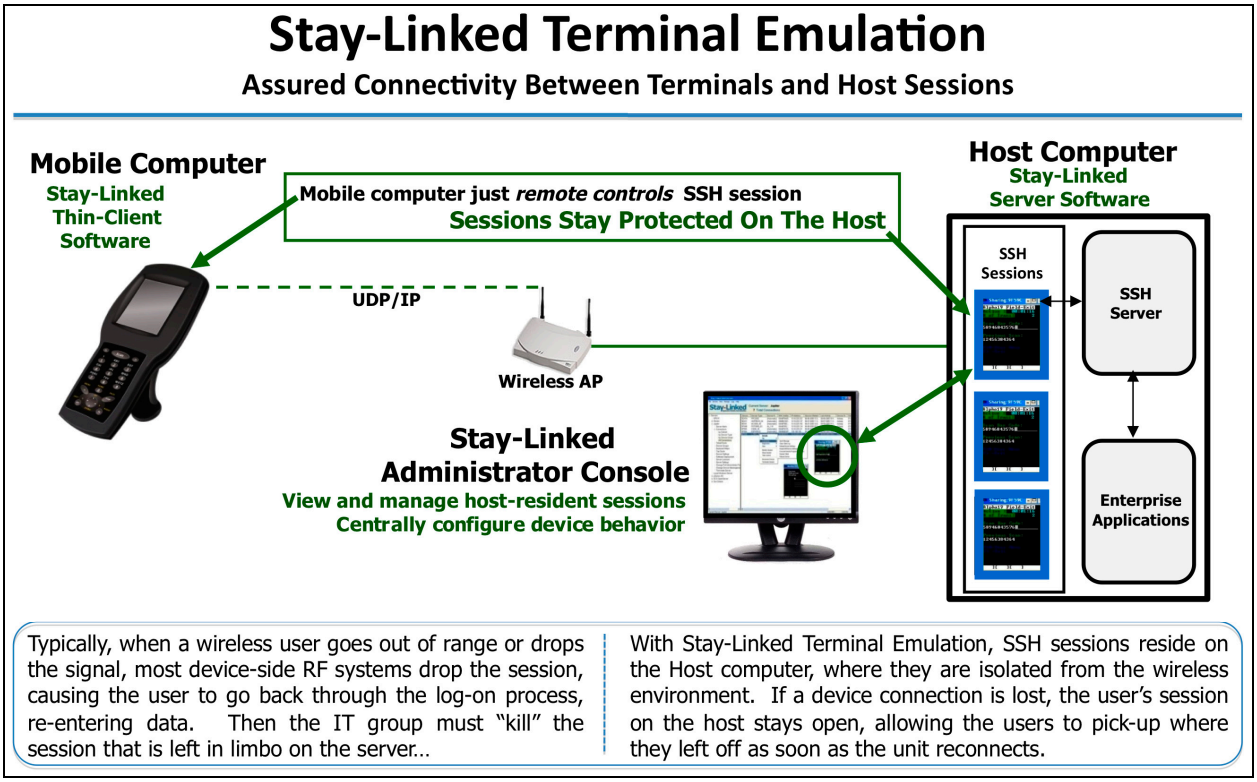
Pragma's Fortress SSH™ is the market's leading, most feature-complete SSH server product for the Windows Host platform, offering:

- Remote installation, management and configuration
- C++ application, 32-bit and 64-bit platform support across Windows Server 2008 R2/ Windows 2008/2003/2000 and Windows 7/Vista/XP
- Best-in-class scalability
- Support for more than 1,000 simultaneous sessions
- Ability to run console applications and allow history scroll back
- Capability to run any console/character mode applications remotely
- Accelerated SFTP and SCP file transfer
- End-to-end encryption to, from and within the network



Stay-Linked works hand-in-glove with Fortress SSH to add much needed flexibility to Pragma's built-in security offerings, giving companies:

- Firewall-friendly communications architecture (port restrictions and static NAT configuration for Servers; NAT-friendly connections for clients)
- Additional security with the Stay-Linked protocol:
  - Blowfish encryption, provides data-layer security to supplement network layer
  - Native, proprietary, end-to-end, application-layer encryption technology for use on older/slower devices and those that run only DOS
- Application lock-down mode for restricting access to other applications on Windows-based devices
- Compatibility with all popular network architectures and platforms, allowing "port-filtering" or "access list" definitions to be applied at the network switch or smart AP level to restrict host access from wireless devices to Stay-Linked UDP/IP transmissions on specific UDP ports



Pair Fortress SSH with Stay-Linked -- the industry-leader in host-based, thin-client wireless terminal emulation and device management – and you've built an optimal, end-to-end remote computing solution. In fact, Pragma and Stay-Linked have partnered specifically to ease the deployment of SSH in supply chain, retail, warehouse management, point-of-sale, healthcare and industrial manufacturing settings, giving companies an industrial grade, high performance solution.

This collaboration comes in the wake of the successful testing and validation of the companies' two flagship software offerings as a single, best-in-breed solution stack for accessing host-based business applications.

But Don't Take Our Word For It: Listen to Our Customers

Across application and vertical industry categories, companies are increasingly turning to the combined expertise of Pragma Systems and Stay-Linked.

> ***CUSTOMER STORY***
>
> ***Stay-Linked Puts Apparel Distributor's Remote Connectivity Over the Top***
>
> *"I knew when we put our remote system into place that I wanted some kind of centralized software to manage the devices, manage those sessions, manage our traffic in the network, and* ***Stay-Linked was our answer for all of that****," states a major US apparel distributor's Director of Distribution Systems. "We purchased* ***Stay-Linked*** *ahead of time as we were purchasing our devices, and we ran all of our session-management and device purchase through Stay-Linked. We love the fact that* ***if a user gets disconnected, that user can pick right back up where they left off****.* ***Stay-Linked's remote ghosting or monitoring of sessions is helpful as well.*** *We don't use it a ton but it's there when we need it.*
>
> *"Recently, we used some of the diagnostic tools built into* ***Stay-Linked*** *to analyze the problems we had with the wireless network in California, and they were really helpful as we tried to figure that out. Not only were their diagnostic tools really helpful, but I have felt – and my system administrator has told me many times –* ***that we get the best support from Stay-Linked of almost any of our vendors****. The support, technical support and expertise through their help desk is amazing****. I would unreservedly recommend Stay-Linked to anybody else who is looking for this kind of session-management and device-management solution."***

Other customers, resellers, and device manufacturers comment...

"It is coming up on our one first year of our implementation and I must say it is ***one of the best investments we have ever made.*** *The system is stable, reliable and both we like it a lot."*

"Working with Pragma and Stay-Linked has been great! Thanks to Pragma and Stay-Linked, we enjoyed a trouble-free installation… Pragma and Stay-Linked software continue to serve as a worry-free component within our new architecture."

"When it came time to find a highly secure solution to satisfy our clients' requirements, Pragma's Fortress more than met the challenge. The ease of configurability, high level of encryption and speed we get with Pragma more than satisfies our stringent requirements. We'll definitely be using the software for all our other clients who require similar, secure data-transfer processes. We have no hesitation in recommending Pragma and its products."

"The logging features you've built in enabled us to observe and track activity that we've just not had the capability to do before. ***The knowledge of the people we worked with, both about the product and the whole wireless network/device environment was incredible."***

"Your **excellent online guide** to downloading, installing and configuring the product **was all I needed to get the product up and running."**

"Thanks for all your help…the ease of doing this switch (downloads and installs, nothing to do on the handhelds) and your help getting it done is the reason these guys are going to keep Stay-Linked. Thanks again, and nice work keeping a customer on board ***with great customer service and an excellent product."***

"By extending application functionality to wireless devices on the same host platform as the applications themselves**, you provide benefits not only in reliability but also in cost of ownership and productivity**. In this tight economy, manufacturing and distribution companies need every employee to be efficient and mobile connections have not always been capable of delivering that in the past."

About Pragma Systems

Pragma Systems is the only company in the world that offers end-to-end secure shell (SSH) and telnet solutions for Windows servers, desktops and handheld devices. Pragma Systems' solutions deliver fast, comprehensive connectivity for IT administrators and users who need reliable and secure access to corporate data and networks. More than 4,000 customers around the world use Pragma's secure file transfer (SFTP), remote systems management, Telnet, and SSH products, which offer unparalleled performance and quality for secure remote access requirements. Visit www.pragmasys.com.

About Stay-Linked

Stay-Linked, with its thin-client Client2Host™ architecture, overcomes all of the typical challenges associated with deploying enterprise wireless terminals by providing:

- Reliable host-based preservation of wireless user application screens/sessions
- Centralized management of wireless emulation (SSH) sessions and mobile devices
- Secure, end-to-end data transmission between wireless users and host-resident applications
-

Stay-Linked is pre-loaded on all currently shipping Psion Teklogix, LXE, Janam, AML, and Paxar devices. Stay-Linked also supports devices by Motorola/Symbol, Intermec, Datalogic/PSC, Honeywell/HHP, BOSaNOVA, Citadel, SmarTerminal, Timbatec, and other popular DOS, MS Windows, Win CE, PocketPC™, and Windows Mobile devices – flawlessly. Visit www.stay-linked.com.