

A Comparison of I'm InTouch Corporate Server Edition (CSE) and VPN's for Accessing Distant PC Information

The advent of the internet and Virtual Private Networks (**VPN's**) have attracted the attention of many organizations looking to expand their networking capabilities and reduce their traditional wide area networking costs. They are found in workplaces and homes, where they allow employees to safely log into company networks over the public internet and provide a convenient way to stay "plugged in" to the corporate intranet. But is a VPN necessarily the best technology solution today for allowing mobile individuals to remain connected and productive while away from the office? While VPN's cater well to individuals requiring access from a particular physical location or device, does it serve the needs of an emerging mobile society that is constantly in different places and that wants to travel with ease and flexibility?

The **I'm InTouch** Corporate Server Edition (CSE) remote access solution represents a new cost-effective remote access solution that not only saves money when compared to the cost of deploying and maintaining a VPN, but is quick to deploy and provides the versatility for mobile individuals to get access to the information they need on a distant PC, when they need it. I'm InTouch also provides the flexibility to choose virtually any device connected to the internet to safely access a distant PC, with reliable performance and existing corporate security policy adherence.

What makes these two technologies that deliver mobile access to data located on a distant computer or server different? The following chart provides a framework for comparison.

| Characteristic | I'm InTouch Corporate Server Edition (CSE) | VPN |
|------------------------------|--|---|
| Security | <ul style="list-style-type: none"> • Adopts to existing security policies of the organization and utilizes those existing security settings of the desktop host PC that the I'm InTouch enabling software is installed on • The CSE server is installed behind the firewall or within the DMZ and utilizes ports 80 & 443, eliminating the need to open new ports on the firewall or port-forward to internal IP's • End-to-end user authentication and dual passwords required for login • Passwords are stored on the host PC, not on the CSE gateway server • All session data is encrypted, using SSL 128-bit encryption • Remote access session time-out after defined period of inactivity | <ul style="list-style-type: none"> • Requires the articulation and implementation of additional security policies at the time of its initial implementation • Authentication allows VPN clients and servers to correctly establish the identity of people on the network <ul style="list-style-type: none"> ○ potential security flaw if implemented in such a manner that only client authentication is required to the server with no human input of passwords – a lost device with the VPN client could mean unrestricted access • Encryption allows potentially sensitive data to be hidden from the general public. |
| Performance | <ul style="list-style-type: none"> • Screen sharing technology, only emitting desktop screen changes, reduces overhead, allowing for improved performance • CSE server does not run applications/programs on it | <ul style="list-style-type: none"> • Intensive applications/programs may perform slowly |
| Software Requirements | <ul style="list-style-type: none"> • No client required on the remote access device • Enabling software is installed only on the host PC by the end-user, after the system administrator has configured the user's account on the CSE server. • Service update notices delivered directly to the host PC from the CSE system | <ul style="list-style-type: none"> • Deployment and configuration of the client software required on each device to be used for remote access <ul style="list-style-type: none"> ○ typically requires the support of an IT person ○ requires co-ordination with employee to schedule a time for access to the device and results in unproductive time for employees • Ongoing need to update/manage the clients installed on each remote access device <ul style="list-style-type: none"> ○ Need for employee to give-up device for a period of time if changes required and related unproductive time |
| Hardware Requirements | <ul style="list-style-type: none"> • CSE server software can be installed on any server machine <ul style="list-style-type: none"> ○ Optimized Linux OS included • I'm InTouch enabling software is installed on existing Windows PC's • No specific hardware required for the remote device, just a device connected to the internet | <ul style="list-style-type: none"> • Typically requires installation of a VPN server • Technologies from different vendors may not work well together due to immature standards <ul style="list-style-type: none"> ○ Employees may be required to standardize on a particular remote access device and a particular manufacturer leaving little flexibility and choice of remote device for the employee |

| Characteristic | I'm InTouch Corporate Server Edition (CSE) | VPN |
|---|---|---|
| User Mobility | <ul style="list-style-type: none"> • Any device with an internet browser provides access – home PC, internet kiosk, cellphone, wireless PDA, hotel PC, laptop • Ability to travel light <ul style="list-style-type: none"> ○ during the day using a wireless PDA, at night using a home PC ○ eliminates the need to lug a laptop home at the end of a day, can use a home PC | <ul style="list-style-type: none"> • Limited to devices with pre-installed client – typically a particular device like a laptop |
| Implementation Timeline | <ul style="list-style-type: none"> • Approximately one hour for CSE server installation and to create user accounts • Approximately 5 minutes for a user to install the I'm InTouch enabling software onto their PC that they wish to be able to reach | <ul style="list-style-type: none"> • Several hours to weeks or months depending on the number of remote employees • Requires significant co-ordination <ul style="list-style-type: none"> ○ Qualified personnel required to configure the network, including VPN server placement, firewall configuration and network addressing ○ Require scheduling time with each user to configure each remote access device |
| Total Cost of Ownership (TCO) | <ul style="list-style-type: none"> • Low – minimal server hardware requirements and labor to deploy and manage | <ul style="list-style-type: none"> • High – VP server hardware, clients, resource time to implement and manage, lost productivity for remote employees as devices are configured and managed |
| Ongoing Management | <ul style="list-style-type: none"> • Service updates installed at CSE server and may require user PC's to run an update file | <ul style="list-style-type: none"> • Management of the VPN network, including servers and clients • Resource time required to assess possible compatible new remote access devices |
| Remote Access Device Flexibility | <ul style="list-style-type: none"> • Any device with an internet browser provides access allowing access from virtually anywhere, anytime | <ul style="list-style-type: none"> • Limited to devices with pre-installed client – typically a particular device like a laptop – without this device, no remote access |
| Ability to provide access to the tools that the remote person requires | <ul style="list-style-type: none"> • Access to any program already on the users desktop PC | <ul style="list-style-type: none"> • VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology. |

Conclusion

I'm InTouch Corporate Server Edition (CSE) is a versatile and flexible remote access service that addresses the current and emerging needs of a business world that is becoming increasingly mobile and in need of access to information from anywhere, anytime. Any business considering a remote access solution that will boost employee productivity while out of the office, will find that I'm InTouch's low cost of ownership and adherence to their existing implemented security policies is good news for the bottom line when compared to the operational expense and impact on existing network configuration and security policies that VPN solutions represent. I'm InTouch can be implemented quickly, by end-users, and with no more than five minutes of lost employee productivity. Secure access to all the business tools found at the office are made available, from email to business programs and applications. The flexibility to utilize any device connected to the Internet - a home PC, a wireless PDA, an internet kiosk - allows a mobile employee to travel and work comfortably, confident that regardless of where they are, they can easily access the information they need to remain productive. I'm InTouch's unique device-agnostic access approach, embraces the need for flexibility and choice that each business and its individual employees require in choosing an appropriate remote access device depending on the time of day that they are working and individual preferences.