



Technology White Paper

Secure Remote Access To Operate Workstations On Your Corporate Network, From
Anywhere In The World



I'm InTouch Corporate Server Edition (CSE) (US Patent #6,928,479) is a versatile and flexible remote access solution 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. The solution was co-developed with Hitachi Business Solution Co., Ltd, of Japan.

Any business considering a remote access solution that will boost employee productivity while out of the office, will find I'm InTouch CSE to be a low cost and secure solution that adheres to existing implemented security policies and 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 typically represent. 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.

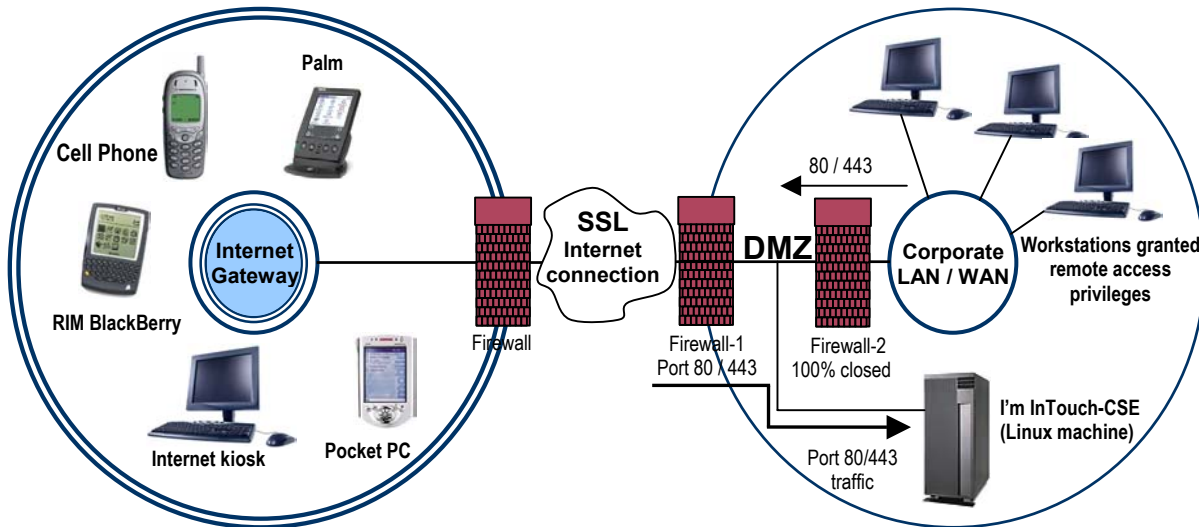
Highlights

- **Secure** - The I'm InTouch Corporate Server gateway securely deploys behind your firewall or within your DMZ and utilizes standard Internet ports 80 & 443 for all host Windows PC to server communications, eliminating the need for port forwarding to reach PCs on the internal network and dynamic DNS solutions. All sessions are encrypted using 128 bit SSL and OS level controls already in place on the user's PC are maintained.
- **Web based remote access** from any Internet browser, eliminating the need to pre-configure the local device that a user is logging in from with specific client software to be able to remotely access PCs at the office.
- **Centralized system administration**, allowing system administrators to easily add, remove and manage users, control user feature restrictions and view usage reports.
- **Highly scalable**. The I'm InTouch CSE server gateway brokers communication between the remote user and the host Windows desktop PC and provides all the required administrative functionality. Most processing is done at the host desktop. This unique "distributed processing" architecture means that a single server can handle from 500 to 2,000 users, depending on the specific server hardware configuration.
- **Easy Deployment**. Install the I'm InTouch CSE server within your network, then add user accounts. By entering your employee or customer's email address within their account profile, the system will automatically invite users to set up their computer for remote access. They simply download and run the I'm InTouch enabling software onto their Windows PC and within minutes can begin to use the system. Users login and see their PC as if they were sitting at it, using screen-sharing technology, essentially eliminating the need for training on your new remote access solution.
- **"Wake-up" server architecture** (patent-pending). With a patent-pending feature allowing employees to remotely power-up their PCs, employees can choose to "Shut Down" their PCs when leaving the office to conform to corporate security or environmental policy.



I'm InTouch Corporate Server Edition (CSE) Architecture

I'm InTouch – Corporate Server Edition (CSE) – provides businesses a secure and cost-effective way to implement remote access to employee workstations and business resources.



Browser Clients

Hosts (workstations on corporate network)

Note: Workstations off the LAN can also be registered with CSE.

Remote access is accomplished by allowing authorized users to remotely access their workstation on the network from virtually any device with an Internet browser and uses 128-bit Secure Socket Layer (SSL) to provide encrypted access to business resources.

The service is comprised of a Server deployed within the DMZ of the business that runs the I'm InTouch Linux operating system and components. This Server is the communication gateway between browser clients and workstations registered on the CSE gateway. I'm InTouch software installed on authorized user workstations, assists to enable the secure communication between the browser Client, Server and Host workstation, with all data exchange authenticated, encrypted and transported through Internet ports open on the firewall.

For larger organizations, scaling may be needed. A single I'm InTouch-CSE server can service up to 500 simultaneous sessions. If CSE server performance slows due to a consistently large number of simultaneous remote sessions being handled by the CSE gateway server, server farming can be implemented.



A workstation running the I'm InTouch software maintains a SSL session with the Server by polling the Server to see if any remote connection requests have been made, using outbound HTTPS through port 443 on the firewall. As no ports need to be opened through the firewall (other than the usual Internet ports) you do not have to bypass or compromise your firewall and existing security policies of the business are maintained.

A remote employee establishes a connection to the Server gateway using virtually any Internet browser, eliminating the need for permanent client software on the device being used to login. The login to the CSE system occurs through a company web page that the system administrator defines during the install of the system. The Server, upon receiving an authenticated browser Client request to login, will manage and forward the encrypted data request to the user's Host workstation. The login request will be processed by the Host workstation and returned to the Server gateway to dynamically generate all web pages required for remote viewing at the browser Client. The Host does not just implicitly trust the browser Client request during a session; the Client must specifically authenticate itself to the Host workstation by first logging in. Login passwords are stored only on the Host workstation. Upon successful authentication from a remote PC, a resizable Desktop Viewer is launched by the browser of this PC that provides a full view of the users desktop at the office and all programs running on it. Beyond screen-sharing control of the PC, a File Transfer feature can be used to transfer files between the PC's.

I'm InTouch maintains workstation OS-level access controls already provided to the end-user by the business. When a user logs in remotely, they only have access to their individual workstation and are subject to the access controls already in place for that workstation. They will be restricted to those domains, file drives, etc already assigned. I'm InTouch's design approach ensures that the introduction of a remote access solution does not allow employees to suddenly have access to all the resources of the business. Existing business security policies set at the employee or organizational level are maintained. Further restrictions, such as allowing remote access only at certain times of the day, can be defined by the system administrator when creating user accounts

Mobile workers benefit from the flexibility to use virtually any device with an Internet browser. This is unlike traditional IP Sec VPN solutions that require pre-configured software on the local device being used to login and specific network routing configurations to reach the business. I'm InTouch's flexible any device with a browser approach, makes remote access possible from anywhere, at any time and is both convenient and easy-to-use. Browser based remote access also provides the assurance that in most cases, the employee is able to get access through the firewall of the local network they are remotely logging in from. Productivity gains, improved customer response times and improved employee morale are just a few of the many possible outcomes from the implementation of I'm InTouch.



“Distributed Processing” Environment

The desktop PC of today is more powerful than a mainframe computer of 20 years ago and in today’s business environment the vast majority of office employees have one. It makes sense for a company to make use of this processing power and hence capitalize on their investment. I’m InTouch CSE was designed for this very reason, which is to capitalize on the processing power of a desktop PC and maximize a company’s return on their computing investment.

Given the computing power of the desktop PC today it is no longer necessary to concentrate remote computing into a central remote access server. I’m InTouch CSE’s “Distributed Processing” was designed to take advantage of the computing power of a desktop PC and provides several benefits over the traditional means of using a central remote access server.


- **Guaranteed performance.** By its definition, using a central remote access server means the user is accessing the server where the application is processed. Multiple remote users accessing the same server at the same time can result in a deterioration of performance. Distributed processing means the desktop PC is accessed directly, resulting in a one-to-one remote session and guaranteeing a higher level of performance regardless of how many users are conducting remote sessions. In addition, applications are running locally at the workstation when the user is not on the road. This ensures the best application performance for the user and eliminates the need to purchase extra application software licenses for a central server.

- **Easy access.** Any device with an Internet browser can be used to access and control the host PC. The user is using the remote device as a “dumb terminal” to control the host PC, where most session processing takes place. This allows for accessibility from virtually anywhere in the world, including the users home PC, an Internet kiosk, Internet café, cellular phone, PDA, Smartphone, etc.

- **Ease of use.** The remote user is accessing and controlling their desktop PC, which means there is no alteration to the way they see their desktop. They continue to view and control their PC as if they were sitting at it. This screen-sharing approach virtually eliminates any need for end-user training on their new remote access system



- **Lower total cost of ownership.** The I'm InTouch CSE server acts as the gateway to the host desktop PC from a remote device and provides all the required administrative functionality. Processing is done at the desktop. This architecture means that a single server can handle from 500 to 2,000 users, depending on the server configuration. There are no additional client side or server software licenses required. With other traditional central remote access server solutions such as IPsec or SSL VPNs there are additional costs to be considered when determining the total cost of ownership. These additional costs include more powerful servers to run the applications, application software licenses for the server and client side licenses. The table below gives a comparison of the total cost of ownership between I'm InTouch CSE and other vendors.

25-user licenses		Citrix Server	Microsoft Terminal Server	Microsoft IPsec VPN Server	Netscreen SSL VPN server	Symantec pcAnywhere via VPN
Hardware	¹ \$500	² \$3,000	² \$3,000	² \$3,000	³ \$4,000	² \$3,000
Licenses	\$5,235	\$15,000	\$3,500	\$2,500	³ Included	\$5,000
Other vendor's licenses (hidden costs)	\$0	⁴ Application software licenses + ... etc.	Microsoft server licenses + ⁴ Application software licenses + ... etc.	Client hardware deployment (e.g. notebook PC) + Client application software licenses + ... etc.	Client hardware deployment (e.g. notebook PC) + Client application software licenses + ... etc.	Microsoft server licenses
Total >	\$5,735	\$18,000 +	\$12,000 +	\$40,000 +	\$40,000 +	\$12,000 +

¹ Although server machines with good processing power (e.g. dual-CPU, 2G RAM, RAID hard drives, etc.) are always recommended for better performance and reliability, I'm InTouch CSE's "Distributed Processing" architecture does not require a powerful server machine. e.g. a plain PC with single-CPU, 512M RAM, 20G IDE drive, etc. can serve up to about 500 active users while a good server machine with dual CPU, 2G RAM, RAID drives, etc. can serve up to 2,000 active users or more. In other words, a single server machine can easily grow with the end-user's company.

² A "Concentrated Processing" server has to be a powerful server machine with dual-CPU, 2G RAM, RAID drives, etc. to serve only about 25 active users (depends on the actual volume of remote access usage and types of applications being used). Thereafter, additional server machines would be required.

³ This proprietary "Concentrated Processing" server may require a new server box for each 50 active users or less (depends on the actual volume of usage and types of applications being used).

⁴ End-user company may save on application software licenses by running everything on the remote access server locally and remotely; however performance will suffer by not running the application locally on their workstation when at the office.



I'm InTouch CSE Technical Requirements

Server Requirements

CPU:

Pentium 3 processor at 800MHz or higher – hard drive redundancy suggested

RAM:

512 MB RAM minimum for first 100 users, 64MB per 100 additional users

Operating System:

01 Communique optimized Linux OS supplied during install

Storage:

Minimum 9GB SCSI for 100 users. RAID class disk array recommended

Network:

Static TCP/IP LAN connection. Approx 7.5 kbps of bandwidth required per active remote session. Each 1MB T1 can accommodate an average of 130 simultaneous remote sessions

Workstation (Host) System Requirements

- Internet connected Windows 98 Second Edition, 2000 Professional, ME, XP, 2003 Server
- Minimum Pentium 233 with 32 MB of RAM
- Outlook Express 5.0 + or Outlook 98+ and POP3 or Exchange email client for wireless email access
- 30M free disk space





Security

Operating System

I'm InTouch (CSE) is deployed on a server within the DMZ and installs with a hardened Linux operating system. All recent security patches and an optimized kernel are applied. No ports need to be opened through the firewall (other than the usual Internet ports 80 & 443), maintaining existing security policies of the business.

The server runs Apache 2.0.50 HTTP as the web server.

Encrypted Transport using Secure Sockets Layer (SSL)

The protection of confidential business data is critical and ensured by the utilization of the 128-bit SSL HTTPS protocol. All traffic between the browser Client, Server gateway and Host workstation, including screen images and file transfer is protected with an end-to-end 128 SSL encryption.

“Wake-up” server architecture (patent-pending)

With a patent-pending feature allowing employees to remotely power-up their PCs, employees can choose to “Shut Down” their PCs when leaving the office to conform to corporate security or environmental policy.

Authentication

The purpose of authentication is to ensure that the identity of the Server gateway, browser Client and Host workstation is verified. I'm InTouch deploys a number of authentication processes to ensure that data exchange is between trusted sources.

During a remote session the Server gateway must first authenticate itself to the browser Client by supplying a digital certificate, issued by a trusted authority.

After knowing that the Server is a trusted source, browser Client authentication continues by the user inputting a user specified Computer Name (selected by the user during the installation of the Host workstation software) that can contain up to 64 characters of both letters and numbers. Long and complex Computer Names naturally provide stronger protection. The Server checks to see that this is a valid Computer Name and that this workstation is currently on and running the I'm InTouch software, thereby being “registered” or polling with the Server.

The Server gateway then passes a further authentication request to the Host workstation. Authentication is in the form of a login name and password that is stored only on the host workstation and managed by the workstation user. The login name can contain up to 254 characters and the password up to 12 case-sensitive alphanumeric characters. This login name and password is never seen on the Server gateway.



Ongoing authenticated browser Client and Host workstation data exchange is encrypted and managed through the Server gateway.

The system administrator can further enhance end-to-end authentication by forcing remote users to login only from browser clients that have installed a pre-assigned digital certificate, issued to the user by the administrator.

Security Features of the I'm InTouch Host Workstation Program

To be remotely accessed, authorized user's workstations must have the I'm InTouch software installed and running on them. After the system administrator assigns a user remote access rights, he/she will be provided with the location of the software download and the assigned serial number. Installation requires physical access to the PC, avoiding any inherent risks associated with attempted remote installs.

Authentication to the Host requires a User Login Name and Password that are stored only at the Host workstation, eliminating the possible risk of all system wide passwords being found at the Server gateway during a hacker attempt. Local management of the authentication passwords at the Host allows for regular and ongoing user password updates by end-users, a good security practice.

To help protect against dictionary attacks, I'm InTouch limits the number of times any user can attempt to login sequentially. By default, after three unsuccessful login attempts, access to the Host workstation is disabled for five minutes.

To minimize the risk associated with users leaving a remote session initiated at a public PC without first logging out, inactivity time-outs are applied. After several minutes of inactivity on the SSL session, the Host workstation will automatically terminate the session.

I'm InTouch maintains workstation OS-level access controls already provided to the end-user by the business. When a user logs in remotely, they only have access to their individual workstation and are subject to the access controls already in place for that workstation. They will be restricted to those domains, file drives, etc already assigned. I'm InTouch's design approach ensures that the introduction of a remote access solution does not allow employees to suddenly have access to all the resources of the business. Further restrictions, such as allowing remote access only at certain times of the day, can be defined by the system administrator when creating user accounts

To provide assurance to the workstation owner that nobody can be silently accessing his or her PC, a notice is displayed on the computer's screen whenever a browser Client establishes a remote connection with the Host workstation. Further, at the time of each remote access login, the user can view within the I'm InTouch viewer, the time of their last login. Both of these tools are useful in assuring end-users that I'm InTouch is safe.



System Administration and Authorization Controls

I'm InTouch has been designed to provide the system administrator with the required authorization tools to ensure he/she can control which employees of the business are granted remote access privileges, to set restrictions on how and when the user accesses the system and to control what features they will be able to utilize. Robust system reporting allows for full monitoring for both security auditing and accounting purposes.

I'm InTouch administration can be undertaken directly from the server and/or restricted to the URL defined by the administrator during the Server installation. The administrator will assign his/her own login name and password for the administrator account. Authentication with the Server while logging in from a browser Client will occur using an X509 digital certificate installed by the Administrator. Accordingly, all remote administration activities will be protected from disclosure with SSL 128 bit encryption.

Creation of new user accounts is restricted to the administrator. After creating a new user account and specific access rights for the user, the user will be provided with the location of the I'm InTouch program download and the assigned serial number to be used during the installation onto the user's workstation. During install, the user will set their personal login name and password to be used as authentication when starting a remote session. These are stored only on the host workstation. Installation requires physical access to the PC, avoiding any inherent risks associated with attempted remote installs.

At any time, the administrator has the ability to remove user accounts from the Server. Any attempts by a user to login to an inactive account are denied, as the host workstation will not be able to "register" or communicate with the Server gateway.

The ability to set remote access restrictions on each user account is particularly important in assisting to ensure business security policies already established at the employee or organizational level are maintained. Feature restrictions include allowing or disallowing file transfer, access to the complete desktop, access to email only, and whether a user has the right to invite guest users to their workstation to participate in online training or presentations. Refined file management restrictions allow the administrator to set access to all file system rights of the workstation or to limit file access to specific folders on the network. Day of week and time of day access restrictions can also be applied as part of remote access policy management. Mandating users to only login from browser Clients installed with a pre-assigned digital certificate is available to provide enhanced endpoint protection.



Remote Access Usage Monitoring and Auditing

Monitoring remote usage is important for two reasons, the need to monitor for security purposes and to measure return on investment of the I'm InTouch implementation. The I'm InTouch administration console provides monitoring of individual user accounts across a selected date range and also provides a quick list view of all users and their usage.

Account level monitoring displays details such as total remote sessions, total hours and minutes of usage, average session length, last login attempt and a view of what features are most often used. A list view of all accounts shows whether a user session is active, number of logins in the date range and average remote session length. These reports can be analyzed to spot unusual usage patterns.

Detailed connection logs are maintained at the Host workstation and can assist the system administrator to get specific details on remote sessions, including the ip address of the browser Client and the specific time of login and logout.

Conclusion

In conclusion, I'm InTouch is an affordable and secure remote access solution that easily integrates into a company's existing network and security architecture. It provides protective processes and the necessary tools to ensure that business resources are always safe. These include thorough authentication of all devices and users involved in a remote session. Extensive authorization controls manage who becomes a user of the system and what abilities the user will have during a remote session. Auditing tools ensure the business can stay on top of user activity for both security and return on investment purposes. All of this is delivered within a secure system architecture that does not require change to existing business network configurations and assures that all data exchange is safe and encrypted.