# Technology White Paper

Secure Remote Access To Operate Workstations On Your
Corporate Network, From Anywhere In The World
(US Patent #6928479, #6938076, #8234701)

I'm InTouch Server Edition (SE) is a versatile and flexible remote access solution that addresses the current and emerging needs of the business world that is becoming increasingly mobile and to access information from anywhere, anytime.
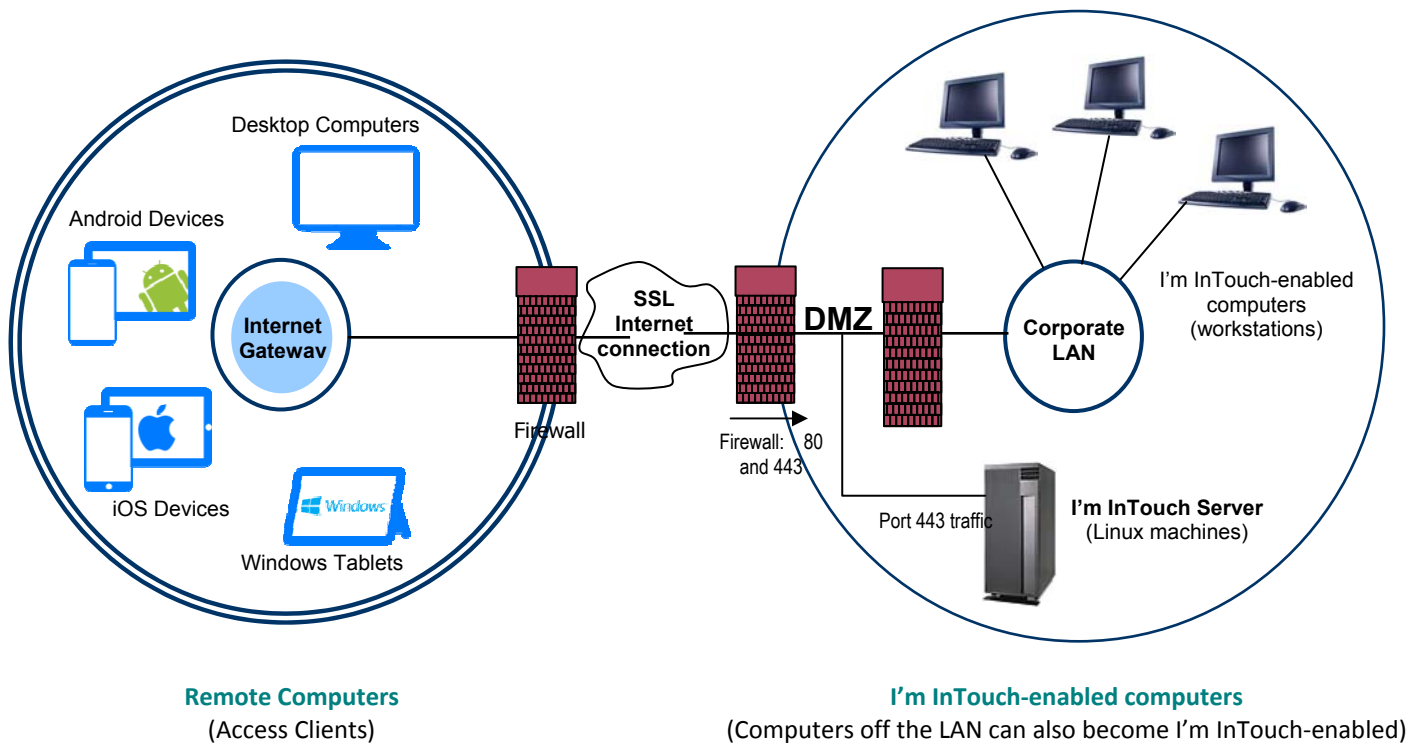
Any business considering a remote access solution that will boost employee productivity while out of the office will find I'm InTouch SE to be a low cost and secure solution that adheres to its existing implemented security policies.  This is good news for their bottom line when compared to the costly operational expense, the impact on their existing network configuration and security policies that VPN solutions typically brings.  I'm InTouch's unique device-agnostic access approach embraces the need for flexibility and choice that each business and its employees desire when selecting their remote access devices.

## Highlights

- **Secure** - The I'm InTouch server gateway securely deploys behind your firewall or within your DMZ and utilizes standard Internet ports 80 & 443 for all host Windows computer to server communications.  All sessions are encrypted using SSL and OS level controls that should be in place on the user's computer.

- **Web based remote access** from any Internet connected devices, eliminating the need to pre-configure the local device that will be used to login.  This is no need to pre-install any client software on the local device as well.

- **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 SE server gateway creates communication between the remote user and the I'm InTouch-enabled computer ("host") 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 between 500 to 2,000 users, depending on the specific server hardware configuration.

- **Easy Deployment**.  Install the I'm InTouch SE server within your network, then add user accounts.  By entering your employee, or customers' email addresses within their account profile, the system will automatically invite them to set up their computers for remote access.  They simply download and run the I'm InTouch enabling software onto their computers and within minutes they can begin to use the system.  Users login and see their computers as if they were sitting at them.  This screen-sharing technology is easy to understand thus little or no training is required to use this new remote access solution.

- **"Wake-up" server architecture**.  This patent-protected feature allows employees to remotely power-up their computers.  Employees can choose to "Shut Down" their computers when leaving the office to conform to their corporate security or environmental policy.

# I'm InTouch Server Edition (SE) Architecture

I'm InTouch – Server Edition (SE) – (US Patent #6928479, #6938176, #8234701) provides businesses a secure and cost-effective way to implement remote access for employees to work on their workstations anytime, anywhere.



**Remote Computers**
(Access Clients)

**I'm InTouch-enabled computers**
(Computers off the LAN can also become I'm InTouch-enabled)

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

The service is comprised of a Server (or server farm depending on the load requirement) 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 the remote computers and the I'm InTouch-enabled computers. All the data is exchange authenticated, encrypted and transported through the I'm InTouch server.

The I'm InTouch-enabled computer maintains a SSL session with the I'm InTouch server by polling the server to see if any remote connection request has been made, using outbound HTTPS through port 443 on the firewall. As no port needs 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.

An employee can establish a connection to the I'm InTouch server gateway remotely using virtually any Internet device.  The server gateway, upon receiving an authenticated client request, will manage and forward the encrypted data request to the user's I'm InTouch-enabled computer. The request will be processed by the I'm InTouch-enabled computer and returned to the server gateway for delivery back to the remote computer. The I'm InTouch-enabled computer does not just implicitly trust the remote computer request during a session.  The remote computer must specifically authenticate itself to the I'm InTouch-enabled computer via a password that is stored only on the I'm InTouch-enabled computer.

I'm InTouch maintains the workstation OS-level access controls which has already been setup by the business.  When a user logins remotely, the user only has access to the individual workstation and is subject to the access controls already configured for that workstation.  They will be restricted to those domains, file drives, etc. that have been assigned. I'm InTouch's design approach ensures that the introduction of a remote access solution does not change the access rights of the employees to the network.  Existing business security policies set up at the employee or organizational level are maintained.  Further restrictions, such as what time periods of the day will remote access be allowed, can be defined by the system administrator when creating the user accounts.

Mobile workers benefit from the flexibility to use virtually any device with an Internet connection and eliminate the need for pre-configured software on the local device (typical of a traditional IP Sec VPN solution) making I'm InTouch a versatile and easy-to-use service for end-users.  Remote access also provides the assurance that in most cases, employees are able to get access through the firewall of their local network to their own workstations.  Productivity gains, reduced customer response times and improved employee morale are just a few of the many benefits of implementing I'm InTouch.

# "Distributed Processing" Environment

The desktop computer of today is more powerful than a mainframe computer in the past.  In today's business environment the majority of office employees have a computer at work.  It makes sense for a company to make use of this processing power and hence capitalize on their computing investment.  I'm InTouch SE was designed for this very reason.

Given the computing power of the desktop computer today it is no longer necessary to centralize remote computing on a central remote access server.  I'm InTouch SE's "Distributed Processing" was designed to take advantage of the computing power of a desktop computer and it gives many benefits over the traditional means of using a central remote access server.

o **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 computer 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 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.

o **Easy access**.  Any device with an Internet browser can be used to access and control the host computer. The user is using the remote device as a "dumb terminal" to control the host computer, where most session processing takes place.  This allows for accessibility from virtually anywhere in the world, including the user's home computer, an Internet kiosk, Internet café, Smartphones, tablets, etc.

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

o **Lower total cost of ownership**.  The I'm InTouch SE server acts as the gateway to the host desktop computer 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 between 500 to 2,000 users, depending on the server configuration.  There are no additional clients or server software licenses required.  With other traditional central remote access server solutions such as 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 clients.

# I'm InTouch SE Technical Requirements

*Server Requirements:*

- Minimum Pentium 3 processor at 800MHz or higher
- 512 MB RAM minimum for first 100 users, 64MB per 100 additional users
- Linux (01 Communique optimized Linux OS supplied during installation)
- Minimum 9GB SCSI for 100 users. RAID disk array recommended
- Minimum T1 Internet (Static IP recommended - Approximately 7.5 kbps bandwidth required per active remote session.  Each 1MB T1 can accommodate an average of 130 simultaneous remote sessions)

*I'm InTouch-enabled Computer (Host) System Requirements:*

- Windows Server, XP, Vista, Windows 7, 8 (32 and 64-bit)
- "Always-on" Internet connection
- Minimum 40M+ free disk space and 128M RAM
- Outlook 2000+ (for Outlook integration features)
- Internet Explorer, Mozilla Firefox, Google Chrome, Mac (Leopard+ Safari)
- Mobile app access client: I'm InTouch Go for iOS, Android, and Windows Tablet

# I'm InTouch (SE) Server Security



*Operating System*

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

*Encrypted Transport using Secure Sockets Layer (SSL)*

Protection of the confidential business data is enforced by the utilization of the SSL HTTPS protocol. All traffic between the remote computer, server gateway, and the I'm InTouch-enabled computer, including screen images and file transfer are protected with the end-to-end SSL encryption.

*"Wake-up" server architecture (US Patent #8234701)*

This patent-protected feature allows employees to remotely power-up their computers. Employees can choose to "Shut Down" their computers when leaving the office to conform to their corporate security or environmental policy.

## Dual Authentication

The purpose of authentication is to ensure that the identities of the server gateway, the remote computer and the I'm InTouch-enabled computer are verified. I'm InTouch deploys a number of authentication processes to ensure that data exchange is permitted between trusted sources only.

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

After knowing that the server gateway is a trusted source, the user inputs the Computer Name (selected by the user during the installation of the I'm InTouch-enabling software) that can contain up to 64 characters of both letters and numbers. Long and complex Computer Names naturally provide stronger protection. The server gateway checks to see if 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 gateway.

The server gateway then passes a further authentication request to the I'm InTouch-enabled computer. Authentication is in the form of a login name and password that are stored only on the I'm InTouch-enabled computer and managed by its owner. The login name can contain up to 254 characters and the password can have up to 12 case-sensitive alphanumeric characters. This login name and password are encrypted and will not be seen on the server gateway.

Ongoing data exchange between the remote computer and the I'm InTouch-enabled computer is encrypted and is managed through the server gateway.

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


## Security Features of the I'm InTouch remote access system

To be remotely accessed, authorized computer must be I'm InTouch-enabled. After the system administrator creates a user account, the user will receive an activation email. Then use the computer that will become I'm InTouch-enabled to receive the activation email. Follow the simple instructions on the email to download and install the I'm InTouch enabling software. Installation requires physical access to the computer.

Authentication to the I'm InTouch-enabled computer requires a User Login Name and Password that are stored only at the I'm InTouch-enabled computer, eliminating the risk of passwords being stolen at the server gateway during an unlikely event of a system-wide hacker attack. Local management of the authentication passwords at the I'm InTouch-enabled computers allows frequent user password updates by end-users which is a good security practice.

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

To minimize the risk associated with users leaving a remote session on a public computer without first logging out, inactivity time-outs are applied.  After a user-defined time period of inactivity on the SSL session, the I'm InTouch-enabled computer will automatically terminate the session.

To provide assurance to the owner of the I'm InTouch-enabled computer that nobody can silently access his/her computer, a notice is displayed on the computer's screen whenever a remote computer establishes a connection to the I'm InTouch-enabled computer.  In addition, users can always check the log to view the history of their last login.  Both of these tools help to assure end-users that I'm InTouch is secure and safe to use.


## System Administration and Authorization Controls

I'm InTouch provides the system administrator with the required authorization tools to ensure the administrator can assign different remote access privileges to different employees.  The administrator can also set restrictions on how and when the user can access the system and what features they will be able to utilize.  The robust system reporting allows full monitoring for both security auditing and accounting purposes.

I'm InTouch administration can be undertaken directly at 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 remote computer is achieved by using an X509 digital certificate installed by the Administrator. Accordingly, all remote administration activities will be protected from disclosure by SSL encryption.

Only the administrator can create new user accounts.  After creating a new user account and its specific access rights, the user will be provided with an activation email with instructions to download/install the I'm InTouch enabling software. During installation, the user will set his/her personal login name and password to be used as authentication when starting a remote session. These are stored only on the I'm InTouch-enabled computer. Installation requires physical access to the computer.

 At any time, the administrator has the ability to remove user account from the server. Any attempt by a user to login to an inactive account will be denied, as the remote computer will not be able to "register" or communicate with the server gateway.

The ability to set remote access restrictions on each user account is crucial in ensuring the business security policies that have already been established at the employee or organization level are upheld.  Restrictions that can be configured 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 his/her I'm InTouch-enabled computer to participate an online training or presentation.  For file management restrictions, the administrator can allow access to all file system rights of the I'm InTouch-enabled computer or limit file access to specific folders on the network.  Day of week and time of day access restrictions can also be defined as part of the remote access policy management. Mandating users to login only from a remote computer that has been installed with a pre-assigned digital certificate is an optional feature which can provide enhanced endpoint protection.

## Remote Access Usage Monitoring and Auditing

There are always needs to monitor remote access usage for security purposes and to measure the return on investment of the I'm InTouch implementation.  The I'm InTouch administration console allows 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 the total number of 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 the average remote session length.  These reports provide analysis which can help to spot unusual usage patterns.

Detailed connection logs are maintained at the I'm InTouch-enabled computer.  They help the system administrator in obtaining specific details on the remote sessions, including the IP address of the remote computers and the specific time of logins and logouts.

## Conclusion

In conclusion, I'm InTouch is an affordable and secure remote access solution that can be easily integrated 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 administrative tools and options let the system administrator manage users and their access rights effectively.  Auditing tools ensure the business can stay on top of user activities for both security and measuring return on investment purposes.  All of these are delivered within a secure system architecture that does not require change to existing business network configurations.  And most importantly all data exchange is safe, secure and encrypted.