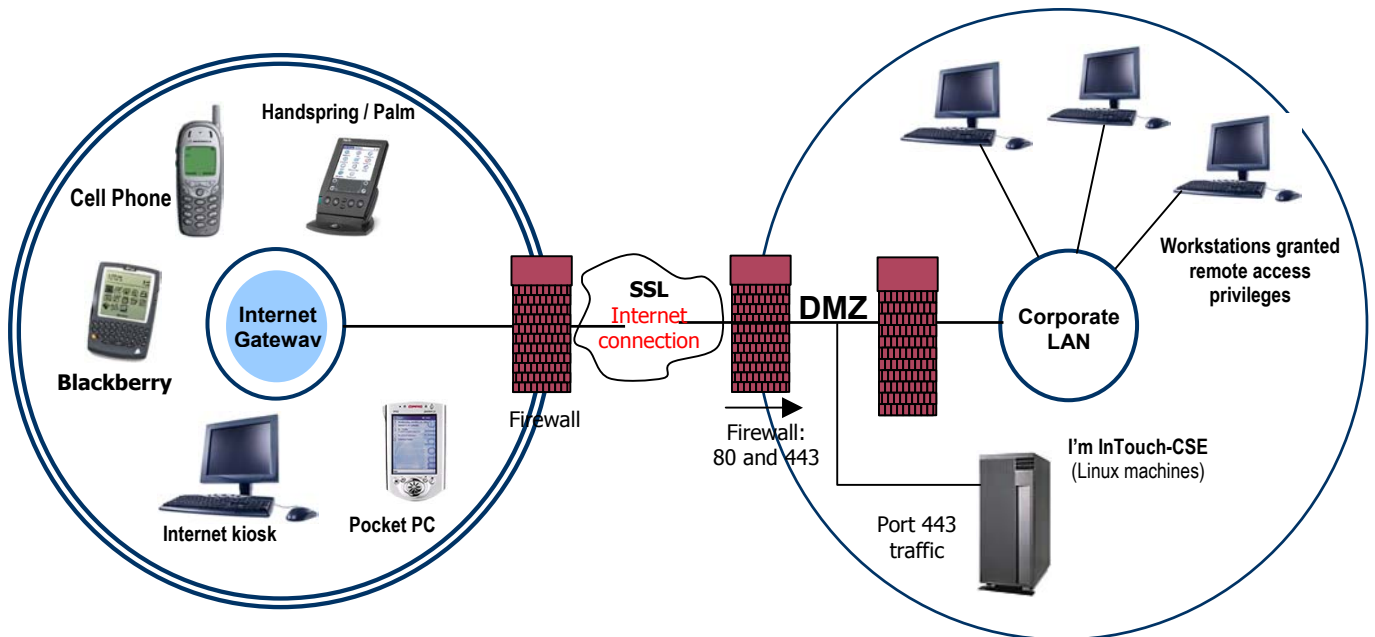




Security Whitepaper

Introduction to I'm InTouch Corporate Server Edition (CSE) Architecture

I'm InTouch – Corporate Server Edition (CSE) – (US Patent #6,928,479) 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 on the corporate network. 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.

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. The Server, upon receiving an authenticated browser Client request, will manage and forward the encrypted data request to the user's Host workstation. The request will be processed by the Host workstation and returned to the Server gateway for delivery back to 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.

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 and eliminate the need for pre-configured software on the local device (typical of traditional IP Sec VPN solutions) making I'm InTouch a versatile and easy-to-use service for end-users. 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.

I'm InTouch (CSE) Server 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 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 that assures that all data exchange is safe and encrypted.