Secure Remote Control

Security Features for Enterprise Remote Access and Control

Good communication is vital to any company, large or small. Many departments within companies are utilizing different platforms and protocols. For example, most high-level graphic design is done on a Macintosh, Excel and Word are Windows based, CE devices are optimal for portable management, and Linux/Unix are long standing systems in corporate IT departments. Also, with the increasing Help Desk and Call Center Industrial outlets and more employees traveling and/or working from remote locations, the secure transmission of information is essential in the corporate world of today.

Contents

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
800-675-0729
www.CrossTecCorp.com/remotecontrol/

Secure Remote Control
Security Features for Enterprise Remote Access and Control

1. Overview
Remote Control Software has enabled IT administrators to efficiently manage networks for almost thirty years. By connecting directly to the desktop of end user computers, companies have saved invaluable amounts of time, money, and energy.

There are a large number of remote control applications and services available today that all claim to have different unique capabilities. The following white paper analyzes some of the current trends in the remote control industry and identifies useful features to seek that will not only allow administrators to control another computer, but enable them to securely manage an entire network as well.

2. The Problem
Good communication is vital to any company, large or small. Many departments within companies are utilizing different platforms and protocols. For example, most high-level graphic design is done on a Macintosh, Excel and Word are Windows based, CE devices are optimal for portable management, and Linux/Unix are long standing systems in corporate IT departments. Also, with the increasing Help Desk and Call Center Industrial outlets and more employees traveling and/or working from remote locations, securely transmitting information is essential in the corporate world of today.

However, more statistics indicate that 22% of companies in the United States are not meeting regulatory requirements for business continuity, information security, or electronic records retention. Furthermore, more than half (56 percent) of company boards rarely or never discuss policies regarding access to critical information, leaving the tasks to IT Security management teams to comply with Federal regulations.

Nearly 80 percent of managers in security and human resources reported that workplace violence is a bigger problem today than it was two years ago. A survey from Risk Control Strategies found that close to 70 percent of managers that were interviewed said many incidents go unreported. Disgruntled employees are also finding new ways to get even with companies after layoffs, pay cuts or outsourcing with the use of computer viruses or sabotaging company products.

3. Implications and Risks
Hackers have long enjoyed accessing and stealing valuable information and disgruntled employees who are not satisfied with their working conditions have sabotaged many computer networks. Other employees with access to certain information have faced legal consequences for manipulating financial records and funneling money to offshore bank accounts. Surveys show that 60 percent of security breaches are internal, but 70 percent of people are worried about hackers on the outside. Some companies even spend 90 percent of their security efforts on firewalls alone.

A recent study from a threat management and risk assessment firm found that the majority of 223 security and human resource executives said that workplace violence is a bigger problem now than it was two years ago. Twenty-three percent of them said that employees intentionally downloaded viruses over the past 12 months. Another study stated that 88 percent of outsourcers cited employee backlash as their primary concern. (http://www.csoonline.com/metrics/). This creates problems for everyone.

To battle this, the United States Government is armed with an arsenal of laws and regulations to protect the unauthorized flow of information, including the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act of 2002 (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and enforcement of Payment Card Industry (PCI) Data Security Requirements. Not adhering to these Federal regulations or securely protecting your network from malware will bring serious consequences, including:

- Excessive dollars spent to correct infiltration of network systems due to malware
- Regulatory fines & penalties levied by the Federal Government
- Increased expenses for labor, hardware maintenance and insurance

4. Examples of the Problem in Action

Victims of the 2004 & 2005 Hurricane Seasons, fires, and flooding across the country are all-too-aware of the business disruptions. Now the CDC and USDA are accelerating measures to protect against the Avian Influenza (H5N1) strain virus and urging businesses and schools to have a plan, as coping with these vulnerabilities can place additional financial and social burdens on corporations nationwide.

Upgrading software is a relatively quick and simple procedure on one machine. However, for the IT employee of a large organization responsible for upgrading hundreds of computers, it can take days or even weeks to bring the computers up-to-date.

Road warriors often fall victim to information being accessed by non-legitimate personnel, especially with the advancements in laptop and wireless technologies. This creates a lack of confidence in personnel for using their computers outside the office. Also, many companies are now utilizing the portable CE devices to keep everything organized and simple to use in any environment and with the international scope of corporations today, secure remote connections are needed more than ever before.

In a survey conducted by the Computer Security Institute (www.csoonline.com/metrics/), 639 respondents reported that the average loss from unauthorized data access grew from $51,545 in 2003 to $303,234 in 2004. Also, average losses from information theft rose to $355,552 from $168,529. Total losses for those two categories were about $62 million.

5. Benefits of Possible Solutions

Remote control software can expand the usability and centralize the security of their network.. Remote control software links your keyboard, mouse and screen to any PC you need to control, and administrators have the ability to monitor all computers on the network to ensure they are not using their time for personal use and/or illegal activities. IT personnel can fix problems and keep every computer running at maximum productivity and employees can get technical support in a matter of seconds.

It's important for a remote control program to support a variety of different operating systems, especially for large enterprises that have several platforms operating on the network. Some applications go way beyond passwords and encryptions to offer several different levels of security. Additional ports provide hackers with multiple back-door entry-points into a network to provide increased vulnerability to the network.

Software-Based Remote Control solutions are designed for a private network environment. These have more features and security and configuration options than web-based or ActiveX solutions.

Software-based remote control solutions usually have a set purchase price; once the software has been purchased it can be used as often as needed. With software-based remote control, a Control application and a Client application must be present on both ends of the connection in order for a remote session to be conducted. This enables a Control to securely connect directly to the desktop of a Client machine.

A Remote Command Prompt takes the interruptions out of remote control sessions. With a remote command prompt, an administrator can conduct remote maintenance without actually remote controlling the Client's desktop or interrupting the end user at the remote machine.

By standardizing in remote control software it is possible to deter hackers and minimize the threat of malicious actions to improve organization, communication and file sharing within a company allowing more productive and efficient work to be accomplished. However, hackers generally try to erase all activity logs in order to destroy any evidence or footprints that could blow their cover. A good security strategy will enable all Control and Client activity logs to be stored in a central, secure network location as well as the computer's system log such as Windows Event Viewer. This way, any intrusions or tampering with of company information is recorded and logged for the network administrator to investigate.

Some software solutions include Internet Gateway Servers. A gateway server functions like a traffic patrol officer, directing all in/out-bound data streams through a single port in a firewall such as HTTP or HTTPS. This assures that no additional ports are opened in a firewall each time a new remote control session is initiated.

Once the system administrator has assigned who can remote control the clients using Active Directory or basic NT authentication, every time a remote connection is attempted, the Control logging in can be identified by their Active Directory account. Another useful feature of a Remote Control Client is event logging. Every Client should have the ability to log to the Windows Event Log or a network location any activity done to the Client machine during a remote session, in the event of an intrusion by a hacker, or just for general auditing purposes, it is important that these logs be accurate and easy to understand. If an unrecognized or outside Control attempts to make a connection to a Client machine, the Client will automatically prevent them from establishing a connection and log the event accordingly.

There are many software solutions available for Remote Control and Access. However, like a mechanic without the right tools, a network won't reach its potential return on investment and provide the necessary security without the proper software.

6. Our Solution

The Remote Control Software from CrossTec lets you securely control and support PCs or Windows CE devices anywhere on the network. CrossTec offers comprehensive cross-platform support for Windows, Linux, Solaris, Pocket PC and Mac* systems with TCP/IP, IPX, HTTP and NetBIOS protocols. The Internet Gateway delivers seamless Remote Control between multiple PCs that may be located behind different firewalls, and provides a stable and secure method for CrossTec enabled systems to locate and communicate over the Internet via an HTTP connection.

Full and comprehensive security is built in to all CrossTec modules. Everything from simple password protection to integration with Windows Security has been included. CrossTec supports AES

Encryption up to 256-bit and can allocate individual profiles for different types of users while providing settings for customized security levels, privileges, and capabilities.

Centralized management and support is provided by viewing the screens of numerous PCs as "Thumbnails", which simplifies identifying and resolving problems as they occur. You can even set up a virtual training room in real time for Distance Learning projects to conduct computer training sessions over the Internet or on the LAN.

Additional useful features include chat options, printer redirect, White boarding capabilities to mark and highlight screen, and recording abilities for later playback on either the control or client workstations. Administrators can launch applications, log out and then back in as an administrator, simple rebooting options with available help request messages and USB capabilities.

The file transfer, synchronization, and distribution utility enable you to copy files to multiple PCs simultaneously, and the "Delta File Transfer" speeds up redundant transfers by only copying the portions of files that are different on the different machines. Scripting and scheduling options let you perform these tasks at any time – even when you're not there.

See a real-time view of the hardware and software installed on the target workstation such as applications in memory, installed hot-fixes, processes running and installed services. The Linux client also now features full Hardware and Software Inventory reporting to maximize productivity across the network. CrossTec also integrates directly with IE explorer, to allow launch key functionality directly from your system without needing to first start CrossTec Remote Control.

7. Conclusion

Remote control technology has been around since DOS and OS/2 dominated the computer industry. However, since its inception in the 1980's, remote control software has come a long way - evolving into sophisticated, resourceful tools that provide much more than just simple remote control. Enterprises worldwide have saved thousands of dollars and countless hours of wasted time by enabling helpdesk employees to be in two places at once.

With a number of remote control products on the market, it is important to know what features are truly beneficial in order to separate the good from the bad. Usability, security, platform support, and speed should all be taken into consideration when purchasing remote control software.

A good remote control application will combine all these features to enable system administrators to monitor, address, and resolve all network related issues from a single desktop to provide superior network management. When deciding which application to purchase, a sufficient amount of research is needed to make sure the selected applications meet all of the technical needs of the company.

Testing a product for 30 days will usually give you an idea of how it will handle your network's demands for end user support. After researching and testing each candidate, then you will be ready to make an educated decision on which application will be best for your environment.

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
800-675-0729
www.CrossTecCorp.com/remotecontrol/