white paper

GoToMyPC™

Like being there.

Remote-Access Technologies:

A Comparison of GoToMyPC™ and pcAnywhere™

CITRIX® | online

Summary

Companies are looking for ways to provide cost-effective network access to their remote and mobile employees. Remote-control solutions such as Citrix Online's GoToMyPC and Symantec's pcAnywhere™ 10.5 are one way to provide this access.

With the GoToMyPC Corporate product for enterprises, administrators can roll out and manage a remote-access solution in minutes. It is a highly secure and cost-effective way for employees to access their computers and network resources remotely. Employees simply access and work on their computers using any Web browser. This document demonstrates that GoToMyPC has significant advantages over Symantec's pcAnywhere™ 10.5.

GoToMyPC is significantly easier to implement, configure and administer than pcAnywhere™. GoToMyPC provides a cost-effective, easy-to-implement, fast and secure way to enable employees to remotely access corporate-network resources. Users find that GoToMyPC is convenient because it works from almost anywhere and requires no configuration.

Comparative Summary of GoToMyPC and pcAnywhere™

	GoToMyPC	pcAnywhere™
Software Installation	GoToMyPC does not require the installation of client software ahead of time, thus lowering the TCO. Users can access and control their host computers from virtually anywhere. The host software installation is Web-based and has a small footprint.	pcAnywhere™ requires pre-installation of the client software from a CD-ROM and the configuration of several settings. Its lack of intuitive wizards makes setup difficult for novice users.
Security	GoToMyPC is preconfigured for maximum security using industry-standard Advanced Encryption Standard (AES) 128-bit encryption. GoToMyPC connects through most firewalls so that a company's data and network remain secure. It is not possible to weaken security, and additional security features such as One-Time Passwords and RSA SecurID integration further secure remote connections. The administrator can enforce corporate policies by enabling additional password and security features. Industry-standard encryption and authentication methods help an organization conform to HIPAA privacy and security standards.	Although administrators can configure pcAnywhere™ with various encryption and authentication options, doing so may be too complex for many users, thus weakening network security. In addition, establishing a connection behind a firewall is complex, leading users to circumvent network security by using modem connections. It is not HIPAA compliant.
Firewall Configuration	GoToMyPC requires an outgoing connection only; as a result, users can access computers without modifying the firewall or network configuration.	Controlling a computer with pcAnywhere™ requires that a user configure an incoming connection to that computer. This may be difficult in corporate environments

		necessitating that the network and/or firewall be configured.
Configuring the Connection	GoToMyPC establishes the connection to the remote computer easily with no configuration. Users only need to know their email address and password.	pcAnywhere™ requires locating IP addresses and configuring multiple settings. Dynamic IP addresses further complicate a pcAnywhere™ configuration.
Connection Costs	GoToMyPC works securely across local Internet connections so no additional infrastructure or connection costs are necessary.	Because pcAnywhere™ users are more likely to connect using dial-up connections to get around firewalls, higher telecommunications costs may result.
Guest Invitation	GoToMyPC allows users to invite a second person to temporarily view or share control of the host computer without installing or configuring software. This feature is particularly useful for sales presentations, training and troubleshooting.	pcAnywhere™ allows users to access a host computer, but the pcAnywhere™ software must first be installed, and the host connection settings must be sent to the user.
Management Features	GoToMyPC has extensive management features through an online Administration Center. Administrators can set up users in a few minutes using the management tools. Additional features enable such comprehensive management capabilities as authorization of specific host and client computers.	An administrator must configure management features of pcAnywhere™ in advance. Managing a corporate rollout of pcAnywhere™ is complex and involves license management.
Platform Compatibility	GoToMyPC supports Windows-based host and multiplatform clients running a Java-enabled browser. It is accessible from certain wireless devices.	pcAnywhere™ supports Windows-based host and client computers only.

Remote Control Overview

One of the major issues confronting information systems managers is providing secure access to corporate resources to people who are physically located outside of the corporate network. In today's increasingly connected society, traveling salespeople, remote workers and work extenders all need real-time access to resources on corporate networks. For security reasons, these resources – such as databases, sales tools and email – are usually protected behind firewalls so that users outside the corporation cannot access them.

Remote Control Solutions

A common method for allowing remote access to protected computing resources is to use remote control software, such as Symantec's pcAnywhere™. Such solutions ship only the screen images and keyboard input between the host and client computers. This functionality affords remote users access to computers on the corporate LAN, allowing them to remotely access all applications while experiencing the same performance as

if they were on the LAN itself. However, traditional remote control solutions bring their own set of management and security challenges. This paper compares the management and security issues of one market-leading remote control product, pcAnywhere™, with GoToMyPC from Citrix Online. It should be noted that the issues applicable to pcAnywhere™ generally apply to other remote-control products.

Intended Application

pcAnywhere™ is a packaged, software-based remote control program. Although it can be customized for a variety of configurations, its setup may call for more knowledge than that of the average computer user. pcAnywhere™ is best used by server administrators, help desk personnel or others who have confidence configuring its many features to provide remote access between two fixed computers. Because of the intensive time necessary to configure the software, pcAnywhere™ is most appropriate for skilled administrators who require many configurable options.

GoToMyPC was developed exclusively for the remote and mobile workforce and others with remote-access needs. Because GoToMyPC is Web-based, these users can easily access their remote computers from almost any other Internet-connected computer with minimal setup and no configuration.

Revolutionary Solution: GoToMyPC from Citrix Online

GoToMyPC is Web-based screen-sharing software that allows users to access and use any of their computers through the https://www.gotomypc.com Web site. With GoToMyPC, users can see their computer screens and access all of their computers' programs, files and network resources as if they were sitting at and using their computers locally, even if they are a thousand miles away.

All communications between the computers are encrypted using AES 128-bit encryption. Only screen and keyboard updates are sent between the host computer and the client computer used to access it (unless the user initiates a file transfer), so bandwidth demands are minimal. Users can take advantage of almost any Internet-connected computer to control the host computer because there is no need to install special software. The client and host computers both initiate outward TCP connections on well-known ports, so firewall changes are usually not necessary.

GoToMyPC includes competitive remote-access features such as File Transfer, Remote Printing, Guest Invitation, Online Administration and Collaboration through text chat and draw. In addition to AES encryption, robust security features include dual passwords, end-to-end authentication, inactivity time-out, host screen blanking, host keyboard locking, One-Time-Passwords generation and automatic session logging.

Comparison of the Remote Control Capabilities of GoToMyPC and pcAnywhere™

Software Installation

pcAnywhere™: To connect to a host computer with pcAnywhere™, it is first necessary to install approximately 20MB of software on the computer acting as the host. In addition, a user must perform a similar software installation on the computer that will be controlling the remote host. For many users, this necessitates that they carry the pcAnywhere™ CD-ROM with them in the event they need to access their host computer while traveling. The required software installation makes it difficult to access the host computer from Internet cafes and other locations that may prohibit the installation of software on their computers.

pcAnywhere™ has many configurable options during setup. For users not familiar with IP addresses, connection settings and authentication types, setting up pcAnywhere™ can be challenging. Many of the latest versions of pcAnywhere™ (including Version 10.5) lack wizards for easy setup by novice users.

The installed software includes extra device drivers, which is significant in two respects. First, the presence of device drivers requires that the computer be rebooted before it can be used as a client computer. Although pcAnywhere™ 10.5 includes a rebootless host, this issue remains with the client computer and earlier

versions of pcAnywhere™. Second, these components can give rise to software conflicts with other device drivers that attempt to use the same system resources, in some cases rendering the system unusable.

These software-installation issues can lead to management and licensing issues and can compel mobile users to carry laptops simply to have access to the pcAnywhere™ client instead of relying on systems that may be available at their destinations.

GoToMyPC: No configuration is necessary on the host and client computers with GoToMyPC. Installing GoToMyPC on the host computer requires a one-time installation of a 1.4MB file. The file automatically downloads from the GoToMyPC site, and novice users not familiar with remote control software can easily install it. Using GoToMyPC, users can download, install and connect to a remote computer in 65 seconds. In fact, administrators can install and configure GoToMyPC four times faster than pcAnywhere™.[1] Because the software is downloaded from the Web site, there are no upgrades to buy.

Accessing the host computer from the client computer is straightforward. GoToMyPC allows users to control their remote machines from any Internet-connected machine using a Web browser and does not require any special software to be installed ahead of time. To access a host computer from a client computer, the user downloads a small (200KB) self-launching plug-in that does not require configuration. Because GoToMyPC connects to the host using a Web browser, you can access your host computer from virtually any operating system with a Java-enabled browser, including Windows, Linux, Solaris and Macintosh. Secure wireless remote access is also available for mobile devices running Microsoft Windows CE.4.x or Microsoft Windows Powered Pocket PC.

Security

pcAnywhere™: pcAnywhere™ supports a wide variety of security features. But most users will not know how to set them up appropriately for maximum security, typically leaving the settings at default values. After a pcAnywhere™ session is closed, the connection information is still on the client system. Although it is possible to password-protect the client information, users may not configure the computer for this added security. Additional password schemes are possible with pcAnywhere pcAnywhere™. However, it requires a complex series of steps to set up, generate and revoke single-use passwords.

The difficulty of establishing network-based pcAnywhere™ connections to hosts behind a firewall results in users opting to attach modems to their PCs so that they can establish pcAnywhere™ connections. But using a modem completely circumvents the corporate firewall and security policies and depends on the security of the PC to prevent unauthorized access. Frequently, hackers exploit such backdoor modem connections as a means to invade a corporate network.

Another common method of installing pcAnywhere™ is to set up a central system to accept remote connections with little or no security and to rely on the network operating system security to protect access. However, if malicious intruders can connect to a system, they can install keystroke loggers and other tools to circumvent the security. This is a much-discussed technique on hacker message boards. pcAnywhere™ is not compliant with industry privacy mandates such as the Health Insurance Portability and Accountability Act (HIPAA).

GoToMyPC: GoToMyPC traffic is encrypted with 128-bit AES encryption using a secure challenge-response password-authentication protocol. Dual passwords include an access code that resides on the host computer and is never transmitted or stored on GoToMyPC servers. A third level of password security through One-time Passwords can easily be generated by end users. It is not possible to inadvertently (or deliberately) configure a computer using GoToMyPC in a manner that will weaken security. Once a remote session is over, there is no way for a user to connect to the host computer without having to first re-authenticate. Through industry-standard authentication and encryption methods, GoToMyPC helps organizations conform to strong security policies and mandates such as HIPAA.

---

[1] Comparative study of GoToMyPC and pcAnywhere™ Version 10 conducted by National Software Testing Labs (NSTL), July 2001.

By making network-supported connections much more reliable and functional even in a secure environment with firewall protection, GoToMyPC removes the motivation for users to install non-secure modems on their PCs.

For novice users, GoToMyPC has several security features that are easy to enable such as Screen Blanking to prevent others from viewing the screen activity on the user's host computer and Keyboard Locking to prevent unauthorized access to the host computer while a user is connected. Although similar features are available on pcAnywhere™, setting these features may not be intuitive for novice users. GoToMyPC administrators can enable these and other security features without user intervention, and in the most robust version of GoToMyPC Corporate, they can restrict the features users can access, including File Transfer and Remote Printing.

Administrators who use GoToMyPC Corporate can further strengthen security for individual users or groups of users. Several security options give administrators a way to configure security options that integrate with their current security policies and infrastructure. For example, with the most robust version of GoToMyPC Corporate, administrators can define password expiration policies, account lockout policies, security time-out periods and specific times for remote-access availability. As an option, administrators can implement two-factor authentication through RSA SecurID Integration, a feature not available with pcAnywhere™.

To demonstrate the infrastructure security of GoToMyPC, Citrix Online has achieved Site Secure Certification n from TruSecure Corporation. This industry-recognized security-assurance program certifies all aspects of information security, ranging from network and system analysis and assessment to physical and policy evaluation.

Firewall Configuration

pcAnywhere™: To control a computer via pcAnywhere™, it is necessary to establish an incoming connection to that computer. The most convenient way to do this is over the network. This provides the best performance and quickest connection setup. But it also requires that the network allow the remote user to establish an incoming connection to the computer that is to be controlled. This is problematic in most corporate settings because the corporate firewall will almost certainly block incoming connections from outside.

Even if a company's security policy allows such incoming connections, providing this capability requires significant administrative overhead in firewall management. pcAnywhere™ by default will use both User Datagram Protocol (UDP) and TCP ports. Many companies will not allow UDP traffic across their firewalls. While this use of UDP can be disabled in pcAnywhere™ (resulting in more administrative overhead for every client), doing so comes at the cost of some functionality. (If the host is in use by another user, then users will appear to make a connection to the host but will see a black screen.)

Some firewalls will only allow one connection to an internal computer to use a specific IP port. In this case, not only must the firewall be configured specifically for every internal computer that will be accessed from outside, but the internal computer's pcAnywhere™ installation also must be changed from its default IP ports in coordination with the firewall. To further complicate things, different versions of pcAnywhere™ require different TCP/IP port configurations.

Even in a noncorporate setting, supporting incoming connections can be problematic. Many home computers use either personal firewall software or hardware. These must also be configured to allow incoming connections on the appropriate ports. If end users attempt this configuration, many will either inadvertently remove most or all the security the firewall provides or be unsuccessful in determining how the firewall needs to change.

Different versions of pcAnywhere™ also use different versions of Winsock, which can result in timing difficulties when attempting to connect through firewalls.

GoToMyPC: With GoToMyPC, both the controlled and controlling computers receive all communications through an outgoing TCP connection, using protocols and ports that can transparently transit almost all firewalls. Thus, no firewall changes are required, and all the problems with incoming network connections that are an issue with the use of pcAnywhere™ are effectively avoided.

Configuring the Connection

pcAnywhere™: pcAnywhere™ requires users to set up the connection manually. Unless the default ports happen to be configured for pcAnywhere™, users generally need to know the IP address or DNS name of the host computer and the specific IP ports on which that computer is listening. This may cause problems for many users who do not know or have difficulty obtaining this information. Users must also know this information if they are attempting to connect between different versions of pcAnywhere™.

If the target system is assigned an address dynamically (as are most DSL, modem and cable-modem-attached computers and many corporate LAN computers), then it is impossible to know the IP address of the remote computer unless the user determines it in advance or there is someone at the remote computer who can determine it.

If the computer to be accessed is behind a firewall, then, even assuming that the firewall has been configured to allow incoming pcAnywhere™ connections, users need to determine the outside interface of the firewall or an address with which the firewall has been specifically configured. Determining this address can be difficult, especially if the firewall is assigned a dynamic address, which is the case with a firewall protecting a DSL or cable-modem home network. If the target system has a dynamically assigned IP address and is behind a firewall, then the firewall is unlikely to know the dynamic address to which it should translate incoming connections. This scenario precludes the possibility of using pcAnywhere™ on the internal computers.

GoToMyPC: GoToMyPC is effectively self-configuring. Setting up the host computer involves registering the computer, installing the software, naming the host computer and creating an access code. From almost any client computer with an Internet connection and a Web browser, the user can log in to https://www.gotomypc.com and view a list of all registered computers. These host computers notify the GoToMyPC servers of their availability on a real-time basis through outgoing connections, thereby avoiding any possible firewall, Network Address Translation (NAT) or dynamic address problems. Users need only remember their email addresses and passwords and the access codes of the computers that they wish to access.

Organizations using the most robust version of GoToMyPC Corporate can optionally enforce the use of One-Time Passwords or RSA SecurID Integration to provide integration into their existing security infrastructure. Administrators may want to further secure their corporate infrastructure by using a feature that authorizes computers on each end of the remote connection before remote connections occur. This gives administrators a way to maintain control over the endpoints of the remote connection.

Connection Costs

pcAnywhere™: As noted previously, the difficulty of establishing network-based pcAnywhere™ connections to hosts behind a firewall results in many users and companies setting up modem pools so that dial-in users can establish pcAnywhere™ connections. In addition to the security implications of this approach, this technique can result in very high telecommunications costs because either the user is forced to pay for long-distance calls or the central site must establish a toll-free number and pay for incoming calls in addition to allocating administrative overhead for provisioning and maintaining the correct number of extra phone lines.

GoToMyPC: By making network-supported connections secure, reliable and functional even in an environment with firewall protection, GoToMyPC allows users to confidently connect from any local ISP. Thus, users can use a local call to establish their connections, and no extra infrastructure is required at the central office, affording significant cost savings.

Guest Invitation

pcAnywhere™: One feature requested by remote-access users is the ability to invite a guest to a computer for a product demonstration, training or other collaboration needs. Remote-access users also want the ability to grant remote access to a guest without changing settings or divulging sensitive information such as their passwords.

To allow guest access to a computer running pcAnywhere™, a user must configure the host connection settings and then provide this information to the guest. The guest must also install pcAnywhere™ before connecting to the host computer, thus precluding use for remote demonstrations to customers and other on-

the-fly uses. The user granting access to the host computer must also ensure that the guest cannot gain access to the host computer after the remote session is completed.

GoToMyPC: Inviting a guest to the host computer with GoToMyPC is straightforward and requires no configuration. A user sends an invitation by right-clicking on the GoToMyPC icon in the system tray and selecting Invite Guest to PC. The user then types the email address of the guest and next enters the GoToMyPC account email address and password.

The person who is connecting to the user's computer receives an email with a link that starts the screen-sharing connection for one time only. Users can optionally grant view-only access. Users never have to compromise security by giving out their passwords, nor are they required to change their passwords immediately after use.

Because GoToMyPC is firewall friendly and doesn't require any software pre-installation, the guest invitation feature can be extremely useful for corporate sales, training and troubleshooting.

Management Features

pcAnywhere™: An administrator must configure the management features of pcAnywhere™ in advance. For example, administrators may want to take advantage of the pcAnywhere™ Packager, which creates customized installation, sets to simplify deployment. Although pcAnywhere™ can provide enhanced logging to track activities during a remote session, this feature must also be set up in advance. Using pcAnywhere™ in a corporate rollout necessitates license management.

GoToMyPC: The management features of GoToMyPC are built in and accessible via the online Administration Center. Administrators can easily create and manage users and groups, check user status and statistics, disable features for certain users and enable optional security features. To gain information about the use of GoToMyPC in an organization, administrators can quickly generate a variety of reports. Administrators can perform a corporate rollout of GoToMyPC in minutes without the licensing issues inherent in packaged software.

Administrators can further configure end-user settings to conform to existing corporate policies. For example, the most robust version of GoToMyPC Corporate gives administrators the option to define the days and times when users are allowed to access their host computers, set the maximum number of host computers per user, define password expiration policies or set customized lockout rules.

Platform Compatibility

pcAnywhere™: pcAnywhere™ supports 32-bit Windows operating systems as the host and client computer.

GoToMyPC: GoToMyPC supports 32-bit Windows operating systems as the host computer. To ensure that users can access their host computers from anywhere, GoToMyPC enables them to use virtually any operating system with a Java-enabled browser, including Windows, Linux, Solaris and Macintosh. Users of mobile devices running Windows CE 4.x and Windows Powered Pocket PC devices can gain wireless access to their desktops using GoToMyPC.

Platforms Supported as Host Computer

Platform	GoToMyPC	pcAnywhere™ 10.5
Windows Server 2003	✓	
Windows XP Home Edition/Professional	✓	✓ (Not available with version 10.0 and earlier versions of pcAnywhere™)
Windows 2000 Professional/Server	✓	✓
Windows Millennium Edition	✓	✓
Windows 98/ Windows 95	✓	✓

Windows NT Workstation and Server 4.0	✓	✓

Platforms Supported as Client Computer

Platform	GoToMyPC	pcAnywhere™ 10.5
Windows Server 2003	✓	
Windows XP Home Edition/Professional	✓	✓
Windows 2000 Professional/Server	✓	✓
Windows Millennium Edition	✓	✓
Windows 98/ Windows 95	✓	✓
Windows NT Workstation and Server 4.0	✓	✓
Linux	✓	
Solaris	✓	
Macintosh	✓	
Windows CE 4.0 and higher	✓	
Windows Powered Pocket PC	✓	

Summary

In contrast to pcAnywhere™, GoToMyPC is a cost-effective solution for providing secure remote access to corporate computing resources without extra staff requirement, loss of security or loss of performance. GoToMyPC is also far more convenient for end users because it does not require any client software, is accessible from any Web browser and does not require prior knowledge of the remote resource. Administrators can easily deploy a remote-access solution with a minimum of effort. Additional security features can be deployed by administrators to meet existing corporate security policies. Overall, GoToMyPC provides lower total cost of ownership than pcAnywhere™.

Product Information: corp.gotomypc.com | www.gotomypc.com/security

Sales Inquiries: gotosales@citrixonline.com | Phone: (888) 646-0016

Alliance Partners: resellers@citrixonline.com | Phone: (805) 690-5711

Media Inquiries: pr@citrixonline.com | Phone: (805) 690-6448

CITRIX® | online

Citrix Online Division • 5385 Hollister Avenue • Santa Barbara, CA 93111