

GoToMyPC®

GoToMyPC Technology Security White Paper

Security is essential when accessing home and office computers remotely. Learn how GoToMyPC provides reliable, industry-leading security to safeguard your files, applications and information.

• www.gotomypc.com

Introduction

GoToMyPC® enables secure browser-based access to any Internet-connected Mac® or PC. Keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream, yielding an experience that's like being there. GoToMyPC's capabilities include:

- **Screen Sharing:** Launch a resizable Viewer from any browser to enable interactive access to any desktop application (even those that are not Web based).
- **Drag-and-Drop File Transfer:** Move files, folders and directories – including file shares – between computers.
- **Remote Printing:** Print from your computer to a printer wherever you are.

GoToMyPC is a hosted service composed of four components:

- **Host Computer:** A small footprint server is installed on the computer to be accessed: Typically, this is a home or office computer with always-on Internet access. We call it the host computer. This server registers and authenticates itself with Citrix Online's GoToMyPC broker.
- **Browser:** From the remote, or client, computer, the user launches a Web browser, visits the secure GoToMyPC Web site, enters a user name and password and clicks a connect button for the desired computer, sending an SSL-authenticated, encrypted request to the broker.
- **Broker:** The broker is a matchmaker that listens for connection requests and maps them to registered computers. When a match occurs, the broker assigns the session to a communication server. Next, the client Viewer – a tiny session-specific executable – is automatically loaded by the browser's Java Virtual Machine. The GoToMyPC Viewer runs on any computer with a Java-enabled browser, including many wireless devices.
- **Communication Server:** The communication server is an intermediate system that relays an opaque and highly compressed encrypted stream from client to server for the duration of each GoToMyPC session.

Protecting the integrity of users' data and the privacy of sensitive information is of utmost concern to anyone. Whether you're using GoToMyPC for business or personal use, security is essential.

GoToMyPC Communication Architecture

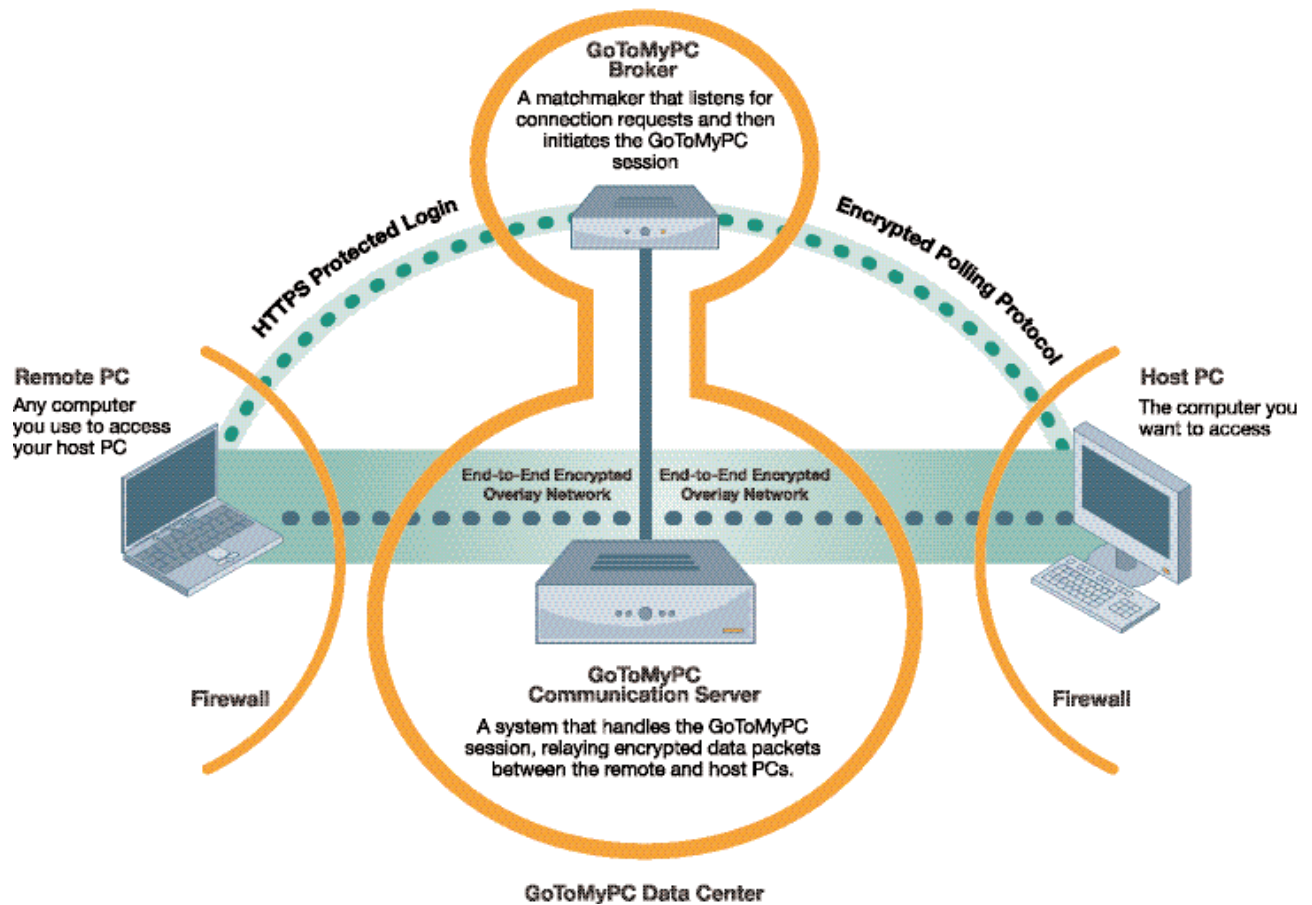


Figure 1: GoToMyPC's security architecture

Security from the ground up

Citrix Online delivers GoToMyPC using an SAAS model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

Secure facility

All GoToMyPC Web, application, communication and database servers are hosted in 5 highly secured data centers worldwide. Physical access to servers is restricted. Citrix Online's network operations center (NOC) in Santa Barbara, California, is protected with strict security measures.

Secure network

Citrix Online's access routers are configured to watch for denial of service (DoS) attacks and to log denied connections. Multi-layer perimeter security

is provided by a pair of firewalls: one between the Internet and Web servers, another between the GoToMyPC broker and back-end databases.

Secure platform

Citrix Online servers run on hardened Linux servers with the latest security patches installed. Servers have been penetration tested, and system logs are continuously audited for suspicious activity.

Citrix Online servers are administered over a private T1 linking the secure data center to Citrix Online's NOC in Santa Barbara. Secure Shell (SSH) supports authenticated and encrypted remote log-in access by Citrix Online's NOC staff. An intermediate server handles and authenticates all SSH connections, thereby avoiding open ports and ensuring very tight access control.

Scalable and reliable infrastructure

The Citrix Online infrastructure is both robust and secure. Redundant routers, switches, server clusters and backup systems are used to ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among Citrix Online Web servers. For optimal performance, the GoToMyPC broker load balances the client/server sessions across geographically distributed communication servers.

Protecting customer privacy

Citrix Online understands about the importance of privacy. Citrix Online has a strong privacy policy that prohibits unauthorized disclosure of personal or business information to any third party.

Published privacy policy

Citrix Online's published privacy policy is included in every GoToMyPC service agreement. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information. Citrix Online is a TRUSTe licensee, adheres to established TRUSTe privacy principles and has agreed to comply with the TRUSTe oversight and consumer resolution process.

Disclosure of customer information

To deliver service, Citrix Online must collect certain user information, including first and last name, email address and account-level passwords for GoToMyPC. Unless expressly authorized, Citrix Online will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed upon services. With its users' express consent, Citrix Online sends service update messages to its users at the email addresses they provided when requesting the service.

Even when GoToMyPC is accessed from a public computer, data left behind poses no privacy threat. GoToMyPC uses an optional cookie to track traffic patterns and retrieve registration information. This cookie holds a unique number generated at the time of registration, but does not contain any personally identifiable information or passwords. Users can block this cookie if desired. After a session ends, browser history indicates that GoToMyPC was accessed

– but information in the history cannot be used to access the account or any computer without a complete set of credentials, including the user's login and password, the computer's access code and (optionally) a One-Time Password.

Access to customer information

Citrix Online NOC staff are the only individuals with access to Citrix Online servers – limited access is granted on a need-to-know basis for the express purpose of customer support. Citrix Online developers do not have access to Citrix Online's production servers.

GoToMyPC session logs are used by Citrix Online to maintain quality of service and assist in performance analysis. GoToMyPC tracks domain names, browser types and MIME types for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user or company account.

Ensuring traffic and credential privacy

Although GoToMyPC communication servers relay traffic between the client browser and host computer, these packets are encrypted. Citrix Online cannot decipher this traffic because it does not possess the access code used to generate encryption keys. Even if a hacker were to gain access to Citrix Online's servers, computer access codes are not stored there and individual session traffic is not recorded, so live-session traffic cannot be compromised.

Digitally signed applications

Software is installed by visiting the GoToMyPC Web site and launching a signed Java applet. If your company prefers to block Java or prohibits installing software, you can launch the server or client software from a file instead. The server software is permanently installed on the host computer, but the client does not require any permanently installed Viewer software.

Most security parameters are pre-set and do not need to be configured by end users. Users can also enable additional security measures, such as blanking the computer screen and locking the keyboard during or after sessions, or generating One-Time Passwords to prevent keystroke capture attacks. Users are always responsible for setting their own passwords and computer access codes, thereby ensuring end-user privacy.

Firewall compatibility

GoToMyPC is firewall friendly. It generates only outgoing HTTP/TCP to ports 80, 443 and/or 8200. Because most firewalls are already configured to permit outgoing Web traffic, you do not have to bypass or compromise your corporate or branch office firewall or your remote worker's firewall to implement secure remote access with GoToMyPC.

Many other solutions require servers to receive incoming packets at a public IP address. The GoToMyPC host establishes a persistent TCP connection to the GoToMyPC broker (poll.gotomypc.com) that allows it to be notified if any connect requests have been received.

The host will attempt to keep the connection open by sending TCP “keep alive” packets approximately every 60 seconds. This makes GoToMyPC completely compatible with application proxy firewalls, dynamic IP addresses and network/port address translation (NAT/PAT).

Also, because GoToMyPC is firewall friendly, you can use it with computers at your company without creating a headache for your IT team. Companies can control GoToMyPC traffic by simply blocking traffic sent to the GoToMyPC broker’s IP address. Upon request, Citrix Online will filter GoToMyPC connections made to a company’s network address block, ensuring that only company-authorized computers can be accessed by company-authorized users. This permits a company’s visitors to use GoToMyPC to reach their own offsite computers while preventing unauthorized use of GoToMyPC to access a company’s own computers.

Guarding computer access

To be accessed remotely, your computers must have the GoToMyPC software installed and running on them. Installing GoToMyPC requires physical access to the computer. It is not possible to remotely activate GoToMyPC or use a Trojan to “plant” it on a computer.

Computers are added by visiting the GoToMyPC Web site from each computer. The user – the computer’s owner – must enter his or her user name, account password and a computer access code that only he or she knows. It is impossible for someone to reset the computer access code without supplying the user name and account password used to register the computer. Optional One-Time

Passwords can be generated to provide a third level of authentication. This eliminates compromise due to keystroke logging, which can be an issue when using GoToMyPC on a public computer.

Protecting confidential information

GoToMyPC uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the GoToMyPC browser client and host computer, including screen images, file transfers, copy/paste operations, keyboard/mouse input and chat text, is protected with end-to-end 128-bit Advanced Encryption Standard (AES) encryption.

Advanced encryption

GoToMyPC uses 128-bit Advanced Encryption Standard (AES) in Cipher Feedback Mode (CFB). In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected AES as a successor to DES. Originally known as Rijndael, AES was selected because of its computational efficiency, modest memory requirements, flexibility, simplicity and, of course, security.

Strong encryption keys

Even a strong cipher is vulnerable if it does not use strong, confidential encryption keys. GoToMyPC generates unique secret keys for each connection. These are derived using a zero-knowledge, public-key-based protocol

called SRP. (See below.) The access code verifier resides on the computer in encrypted format and is never transmitted to or stored on Citrix Online servers. Would-be hackers cannot intercept or generate the keys necessary to decode encrypted data.

Protection against message replay and modification

Screen sharing and file-transfer packets include a sequence number to prevent any attempted message replay attack. These packets carry highly compressed binary data that are framed in a proprietary protocol and encrypted with AES. An attacker cannot modify these packets without it being detected by the recipient.

Authenticated access

The GoToMyPC confidentiality between the browser client and host computer builds on the strong foundation provided by authentication. Authentication verifies the identity of every party from the GoToMyPC broker and communication server to the browser client and host computer. Access controls further ensure that only authenticated parties can gain access to authorized resources.

Strong passwords

GoToMyPC requires that every password be at least eight characters long and contain both letters and numbers. This requirement helps to prevent accounts from being configured with short, common passwords that are easily compromised with a dictionary attack. The longer and more complex the password is, the stronger the protection.

Limited number of log-in attempts

GoToMyPC limits the number of times any user can attempt to log in sequentially. This measure also helps to protect against password-guessing attacks. By default, after 3 authentication failures, access to the user's account and computer are temporarily deactivated for 5 minutes.

Multiple nested passwords

GoToMyPC uses multiple, nested passwords to keep outsiders away. Cryptographic techniques are used to ensure that sensitive data – user names and passwords – are never sent in plaintext. For an additional level of protection, users can generate One-Time Passwords.

The GoToMyPC broker authenticates itself to browser clients by supplying a digital certificate, issued by a trusted authority. Clients authenticate themselves to the GoToMyPC broker by supplying an account user name and password that is exchanged over SSL.

End-to-end authentication

Whenever a browser client connects to the host computer, they also authenticate each other, using a shared secret known only to the end user and the accessed computer. This access code is never seen or stored by Citrix Online. As long as the user keeps his or her access code secret, only he

or she can successfully launch a GoToMyPC connection to that computer. GoToMyPC uses the Secure Remote Password (SRP) protocol standard for end-to-end authenticated key agreement between the Viewer and host. This patented, well-reviewed protocol provides outstanding cryptographic strength, performance and resilience against a wide range of potential attacks. For more information, visit <http://srp.stanford.edu/>.

To enable One-Time Passwords authentication, the user clicks a button to generate a list of passwords from the computer to be accessed. When initiating future connections, a user who supplies the correct access code will be prompted for a numbered password from this list. Each password is used for just one connection, and the user can cancel or regenerate the list at any time. One-Time Passwords are an easy-to-use method to achieve stronger authentication without requiring added infrastructure.

Inactivity time-outs

Users walk away from public computers without logging out and leave home computers unattended. GoToMyPC addresses these threats by applying inactivity time-outs. Users are automatically logged out of the GoToMyPC Web site if their SSL connection is inactive for 15 minutes. Users can also configure the Viewer to time out after a set period of inactivity. Additionally, host security features allow users to blank the host screen and lock the host keyboard and mouse from accepting input.

OS-level access control

GoToMyPC leverages the OS-level access controls already in place on the corporate LAN. Simply leave the computer to be accessed in a screen-locked or logged-out state. When GoToMyPC connects, the remote user must enter a user name and password to access the computer and be granted file, host and domain-level permissions associated with his or her account. In other words, the remote user does not have tunneled access to the enterprise network – he or she only has access to a single computer's desktop, and is subject to access controls already in place for that computer.

Guest invitation

Users armed with GoToMyPC may choose to use desktop sharing for collaboration with colleagues, customers and clients. Guest access can be useful, but it must be implemented securely. The GoToMyPC user may grant a third party temporary access to any of his or her own GoToMyPC-enabled computers, without disclosing the account or computer password.

Limited invitation period

When permitted, users can invite others to access their computers using GoToMyPC. By right-clicking on the MYPC icon in the system tray, the user can issue an email invitation that expires after one, two or three hours. The user must supply his or her account login and password to satisfy a broker challenge/response and digitally sign the entire invitation. The broker then sends an email message to the guest's specified address containing a one-time access URL the guest will follow to get to the GoToMyPC Web site.

Granting access requires

Once at the Web site, the guest clicks on a button to download the GoToMyPC viewer. Because the URL contains a one-time token for dynamic login, the guest is not prompted for an access code or user password. Instead, a pop-up window is displayed on the computer to be accessed, requiring manual authorization by the user to complete the guest connection. Unauthorized invitations are further prevented by requiring the invitation to be generated from the computer itself, by someone with the account-level password and access code.

Shared control view-only option

Two guest access modes are supported: a view-only mode and a full-control mode. In view-only mode, the browser client can draw, but cannot initiate desktop actions or transfer files. Full-control mode offers the same access normally granted to the computer's owner. The local mouse always overrides remote control. The computer owner can end the GoToMyPC connection at any time by disconnecting the guest.

Access notifications

Whenever a client connects to a computer running GoToMyPC, a notice appears on the computer's screen. This notification makes sure that the computer's owner is always aware of the GoToMyPC connection, preventing a "lurker" from silently watching local desktop activity. In addition, the GoToMyPC Web site displays a session-in-use notification during an active connection. Upon each browser client login, the user is always notified of his or her last log-in attempt. This notification reassures the user that no unauthorized access has taken place during the interim. In addition, users can view their own connection histories, including the number of failed log-in attempts, to confirm that there has been no suspicious activity.

Conclusion

Citrix Online's recipe is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Protect remote-access connections with multi-level authentication and state-of-the-art encryption to keep users' information safe. The end result: GoToMyPC offers robust, secure remote access that's fast, reliable and simple to use.

Excerpted from a white paper prepared by:

Lisa Phifer
Core Competence, Inc.
lisa@corecom.com

About Lisa Phifer: Lisa A. Phifer, vice president and co-owner of Core Competence, has been involved in the design, implementation and evaluation of data communications, internetworking, security and network-management products for over 20 years. At Core Competence, she has advised companies large and small regarding security needs, product assessment and the use of emerging technologies and best practices.



Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117
U.S.A.
T 1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

**Citrix Online Europe
Middle East & Africa**
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europa@citrixonline.com

Citrix Online Asia Pacific
Suite 3201
32nd Floor
One International Finance Center
1 Harbour View Street
Central, Hong Kong SAR
T +852 100 5000
asiapac@citrixonline.com

About Citrix Online
Citrix Online solutions enable people to work from anywhere. Our products include GoToAssist® for remote support, GoToManage™ for IT management, GoToMeeting® for online meetings, GoToMyPC® for remote access, GoToTraining™ for interactive online training and GoToWebinar® for larger Web events.

©2010 Citrix Online, LLC. All rights reserved. Citrix® is a registered trademark of Citrix Systems, Inc., in the United States and other countries. GoToAssist®, GoToManage™, GoToMeeting®, GoToMyPC®, GoToTraining™ and GoToWebinar® are trademarks or registered trademarks of Citrix Online, LLC, in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.