

GoToMyPC Security

Introduction

GoToMyPC enables secure browser-based access to any Internet-connected Windows PC. Keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream, yielding "good as there" experience over broadband and impressive performance over dial-up. Applications supported by GoToMyPC 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).

Guest Invite: Collaborate with colleagues by granting temporary access to a GoToMyPC-enabled desktop.

File Transfer: Drag and drop files, folders and directories - including fileshares - between the browser and computer.

Chat: Communicate with a guest by chatting while sharing full or view-only control of your PC.

Remote Printing: Print from the host Viewer to your local client printer.

GoToMyPC is a hosted service composed of four components:

Computer: A small footprint server is installed on the computer to be accessed: Typically, this is a home or office PC with always-on Internet access. This server registers and authenticates itself with Citrix Online's GoToMyPC broker.

Browser: On the client side, the remote or mobile worker launches a Web browser; visits the secure GoToMyPC Web site, enters a username/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 the corporate network and the privacy of sensitive data is of utmost concern to any enterprise. Security is essential when extending Internet-based remote access to remote and mobile employees. However, to ensure low total cost of ownership (TCO), secure remote-access solutions must integrate smoothly with each organization's existing security infrastructure and require little IT support or per-user configuration. Citrix Online's enterprise product, GoToMyPC Corporate, was developed with these key security issues in mind, as illustrated in Figure 1 and described throughout this paper.

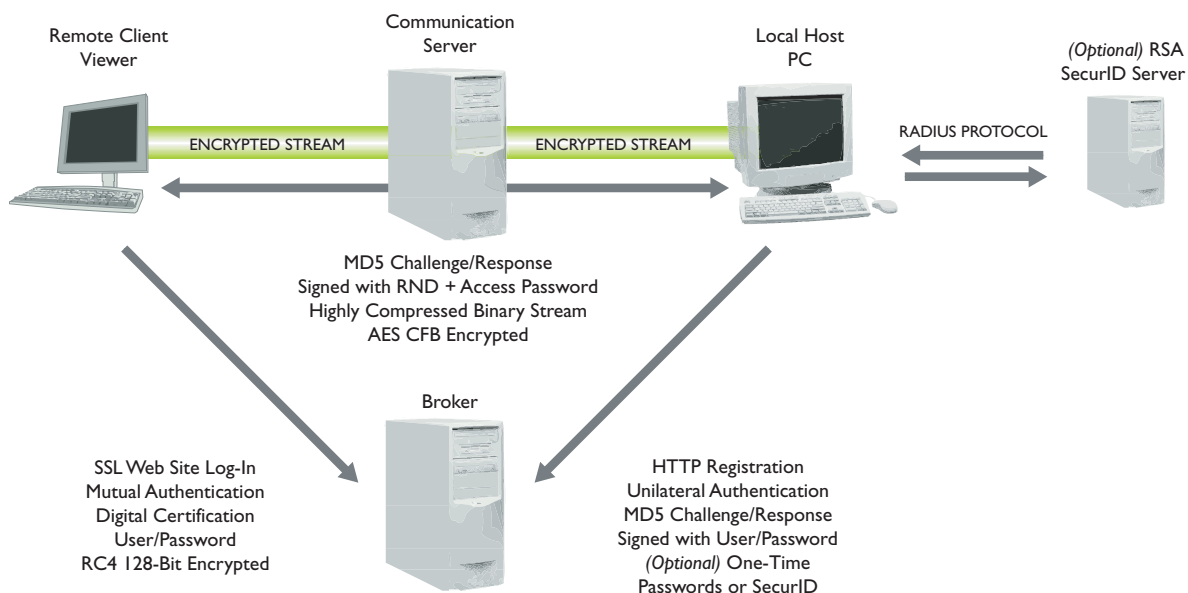


Figure 1: GoToMyPC's Security Architecture

Security from the Ground Up

Citrix Online delivers GoToMyPC using an ASP 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 a highly secured data center. Physical access to servers is restricted. The entire site sits in a locked cage that is monitored by cameras. Citrix Online's network operations center (NOC) in Santa Barbara, California, is similarly protected with strict security measures.

Secure Network

Citrix Online's access routers are configured to watch for denial of service (DoS) attacks and 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. The security of this architecture has been independently confirmed by penetration tests and vulnerability assessments conducted by TruSecure Corporation. Citrix Online has achieved TruSecure SiteSecure Certification, an industry-recognized security assurance program that certifies all aspects of information security, ranging from network and system analysis and assessment to physical and policy evaluation. Quarterly perimeter tests ensure that Citrix Online continues to meet all SiteSecure Certification requirements.

Secure Platform

Citrix Online servers run on hardened Solaris 8 with the latest security patches installed. The entire service delivery platform is SunToneSM certified for quality and reliability. Servers have been penetration tested, and system logs are continuously audited for suspicious activity.

Secure Administration

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 that all enterprises that outsource service delivery are concerned about privacy. Citrix Online has a strong privacy policy that prohibits unauthorized disclosure of personal or corporate 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/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 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. Upon request, Citrix Online will also enter into a formal non-disclosure agreement (NDA) with any customer.

Even when GoToMyPC is accessed from a public PC, 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/password, the computer's access code and (optionally) a One-Time Passwords or SecurID two-factor authentication token.

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

Citrix Online's enterprise solution, GoToMyPC Corporate, gives account administrators access to real-time and summary usage records associated with their companies' accounts, but not to the traffic exchanged during individual remote-access sessions, nor to the access codes or other credentials required to launch a connection.

In fact, 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.

Security Policy Administration

GoToMyPC Corporate provides a secure online Administration Center from which administrators can control the employees who are permitted remote access and can block unauthorized access or features.

Secure Management Interface

The Administration Center is accessible from any Web browser. To reduce unauthorized log-in attempts, the Administration Center URL is not published. Once an organization establishes a GoToMyPC Corporate account, the administrator is provided with access instructions. The GoToMyPC server is authenticated with an X.509 digital certificate. The administrator sub-authenticates by username/password. Thereafter, SSL with 128-bit RC4 encryption protects all management traffic from disclosure or modification in transit.

Inviting New Users

Only the administrator is authorized to create new user accounts and groups. The administrator simply logs into the Administration Center and supplies a list of email addresses. A customizable mail message containing instructions and a one-time self-activation URL is sent to each invited user. The new user visits this URL, defines his or her own password and then adds computers to his or her own account. The administrator can limit the number of computers available to each user and can require explicit administrative authorization of both host PCs and client viewer systems. This approach streamlines large-scale deployment while retaining enterprise control over remote-access authorization and end-user privacy and accountability.

Suspending or Canceling User Accounts and Connections

The Administration Center can also be used to check the activation status for individuals and groups. Controls are available to temporarily suspend or permanently cancel any user or group account. Email messages are sent to affected users, indicating the suspension or cancellation, and future client browser or computer log-in attempts with the user's account are denied. In addition, GoToMyPC Corporate administrators can view connection activity in real time and end connections immediately if necessary.

Managing User Accounts

GoToMyPC Corporate administrators can configure user account parameters to meet organizational needs, implement corporate security policies and support privacy mandates. Administrators can limit access by users or groups to specific services such as file transfer and remote printing. Administrators can also enforce password update frequency and reuse policies, limit time-out periods, lock accounts and computers after authentication failure and mandate use of One-Time Passwords or SecurID two-factor authentication. Fine control over these settings allows administrators to match corporate security policies, and customizable multi-level groups enable enterprisewide policy enforcement and rapid update, even in very large deployments.

Secure Service Installation

GoToMyPC software installation and update procedures were designed with enterprise security in mind.

Digitally Signed Applications

Software is installed by visiting the GoToMyPC Web site and launching a signed Java applet. Companies that prefer to block Java or prohibit users from installing software 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. This prevents misconfiguration, ensuring that company-specified secure remote-access policies are always enforced. At the administrator's discretion, users can 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 both end-user privacy and accountability.

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 server sends an outgoing HTTP "ping" to the GoToMyPC broker (poll.gotomypc.com) at regular intervals, checking to see if any connect requests have been received. This makes GoToMyPC completely compatible with application proxy firewalls, dynamic IP addresses and network/port address translation (NAT/PAT).

However, because GoToMyPC is firewall friendly, it does not mean that you will lose control over use of your company's remote-access services. 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 off-site computers while preventing unauthorized use of GoToMyPC to access a company's own computers.

Guarding Computer Access

To be accessed remotely, your network 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 install GoToMyPC or use a Trojan to "plant" it on a computer. With GoToMyPC Corporate, administrators can even require pre-authorization of client and/or server systems after installation but prior to a connection. By individually fingerprinting each system's hardware, GoToMyPC optionally gives the IT department fine-grained control over the specific computers that can be accessed and the location from which each computer can be accessed.

Computers are added by visiting the GoToMyPC Web site from each computer. The user - the computer's owner - must enter his or her login, 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 login and account password used to register the computer. At the administrator's discretion, 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 PC. The most robust version of GoToMyPC Corporate can be integrated with a corporation's existing RSA SecurID infrastructure. This option provides strong two-factor authentication by requiring users to have their own SecurID token in their possession in order to launch a session.

Protecting Confidential Data

GoToMyPC uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing

performance. All traffic between the GoToMyPC browser client and host PC, including screen images, file transfers, copy/paste operations, keyboard/mouse input and chat text, is protected with end-to-end 128-bit 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. AES is now the U.S. government's designated cipher for protecting sensitive information. Through industry-standard encryption methods, GoToMyPC can help an organization implement strong security policies and conform to such privacy mandates as the Health Insurance Portability and Accountability Act (HIPAA).

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 that are derived from the computer access code and a large, random bit sequence. The access code 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 an attempted message replay attack. These packets carry highly compressed binary data that are framed in a proprietary protocol and encrypted with AES. A hacker cannot modify these packets without corrupting them.

Chat packets carry text, which is also encrypted with AES. Because it is possible to modify encrypted text without corrupting it, chat packets also carry a signed MD5 hash to ensure message integrity.

Defeating Man-in-the-Middle Attacks

GoToMyPC implements AES in CFB mode. Any third party (man in the middle) attempting to inject or replay packets would have to know not only the session key, but also the current state of the AES engine. Compressed binary payloads make it exceedingly difficult to generate valid modified packets or "guess" the session key through traffic analysis.

Authenticated Access

The GoToMyPC confidentiality between the browser client and host PC 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 PC. Access controls further ensure that only authenticated parties can gain access to authorized resources.

Long, Complex 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, the stronger the protection. With GoToMyPC Corporate, administrators can set password expiration and update and reuse rules to align with the existing corporate password policies. As noted in the End-to-End Authentication section, passwords can also be combined with other stronger authentication methods.

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 dictionary attacks. By default, after three authentication failures, access to the user's account and computer are

temporarily deactivated for five minutes. In the most robust version of GoToMyPC Corporate, administrators can match existing security policies by customizing the lockout period and enabling hard lockout after a consecutive number of incorrect password entries. Hard lockouts require administrator intervention to unlock the user's account.

Multiple, Nested Passwords

GoToMyPC uses multiple, nested passwords to keep outsiders away. Cryptographic techniques are used to ensure that sensitive data - logins and passwords - are never sent in plaintext. For an additional level of protection, users can generate One-Time Passwords. With the most robust version of GoToMyPC Corporate, administrators can mandate the use of One-Time Passwords or RSA SecurID two-factor authentication..

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 login/password that is exchanged over SSL.

When a computer registers with the GoToMyPC broker, it relies on DNS resolution of the broker's hostname to reach the correct destination. The broker assigns the server a unique random number. The server initially authenticates itself by signing its unique number with MD5 and the account login/password. Thereafter, the broker and server exchange MD5 challenge/response messages, based on a sequence known only to the pair.

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. The browser client and host PC each generate a very large random number and digitally sign that number with the access code. This challenge/response provides end-to-end authentication without transmitting the access code. 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.

As previously noted, the administrator has the option to combine the access code with One-Time Passwords or SecurID two-factor authentication. 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.

Companies that have already deployed RSA SecurID two-factor authentication can easily use that added protection with GoToMyPC Corporate. To enable SecurID authentication, the computer must be configured with names of the company's own RSA Server(s). Thereafter, a user supplying the correct access code will be required to enter the value currently displayed by his or her SecurID token. That value changes constantly, preventing access by anyone who does not have the token in her or her physical possession. Two-factor authentication is a proven method, widely used to strengthen remote access to enterprise networks. GoToMyPC integrates seamlessly with a company's existing SecurID infrastructure, without requiring complex configuration or delegation of trust to Citrix Online servers.

The use of One-Time Passwords or SecurID authentication is optional, but GoToMyPC Corporate administrators can require their users to implement them. As previously noted, administrative authorization can also be required to add server computers or identify client viewer systems - in that case, if an unauthorized viewer attempts to access a computer, end-to-end authentication will fail.

Inactivity Time-Outs

Users walk away from public PCs without logging out and leave home PCs 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 several minutes. Users can also configure the Viewer to time out after a period of inactivity, subject to limits set by the administrator. Additionally, host security features allow users to blank the host screen and lock the host keyboard and mouse from accepting input. The most robust version of GoToMyPC Corporate enables

administrators to require use of these security features - for example, setting a maximum time-out or preventing user modification.

OS-Level Access Control

GoToMyPC leverages the OS-level access controls already in place on the corporate LAN. Simply leave the PC to be accessed in a screen-locked or logged-out state. When GoToMyPC connects, the remote user must enter a Windows login/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. In the most robust version of GoToMyPC Corporate, administrators can further secure access by defining the days of the week and time periods when users are allowed to remotely access their computers, thus ensuring that users connect to corporate resources only when remote access is appropriate.

Guest Invitation

Users armed with GoToMyPC may be tempted to use desktop sharing for collaboration with colleagues, customers and clients. Guest access can be useful, but it must be implemented securely. If the administrator has given the user permission to use GoToMyPC's Guest Invite feature, the 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 GoToMyPC launcher, 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 Required

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.

Share Control or 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.

Monitoring Access Within an Organization

The GoToMyPC Administration Center enables an organization to track all connections made by users, create detailed reports and maintain connection logs for security audit and accounting purposes.

Monitoring Usage

The GoToMyPC Corporate administrator can view connections for any given day, including those that are still active. Administrators can also use this tool to end active connections immediately if necessary. Each connection record displays details such as the first and last name of the user, the name of the host PC, the IP address of the client initiating the connection, the connection start and stop time, the connection duration and the type of session (normal or guest invite).

The Administration Center can also be used to generate reports for specific dates and date ranges that provide details on users, connection time and average connection duration. Administrators can also generate additional reports to

evaluate data such as the features enabled for each user/group, hours of access or the frequency of failed log-in attempts.

These standard reports can be analyzed to spot unusual access patterns, including exceptionally long connections and unexpected client IP addresses. They also serve as audit trails, making it possible to check to see who accessed a particular computer at a particular time.

Users can view their own connection histories when logged into the GoToMyPC Web site. Connection history can also be integrated an existing reporting infrastructure by sending records to the Windows Event Log on each computer.

Detailed Connection Logs

The GoToMyPC broker logs additional information for each connection, including the last user access time, type of browser (user agent), download status for the viewer, communication server ID, who closed the connection (server/client/broker/time-out), a close error code and the build number of the computer. This information is intended to aid problem diagnosis; access is limited to Citrix Online customer support on an as-needed basis.

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.

Upon each browser client log in, 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. Complement this foundation with secure enterprise-class configuration and monitoring tools to control remote access. Protect remote-access connections with multi-level authentication and state-of-the-art encryption to keep corporate traffic safe. Integrate this solution seamlessly with each company's existing network and security infrastructure. Provide flexible administrative controls to support and enforce a wide variety of security policies and hierarchical grouping to enable scalable management. The end result: GoToMyPC Corporate for robust, secure remote access with low total cost of ownership (TCO).

Prepared by:

Lisa Phifer

Core Competence, Inc.

lisa@corecom.com

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
