



## GoToMeeting Security White Paper

*GoToMeeting provides true end-to-end data security measures that address both passive and active attacks against confidentiality, integrity and availability.*

CONTENTS

- 1 Introduction**
- 2 Business Needs for Secure Collaboration**
- 2 Role-Based Security Features**
  - 2 Organizer Privileges
  - 3 Presenter Privileges
  - 3 Attendee Privileges
- 3 Account and Meeting Authentication Features**
  - 3 Web Site Account Login
  - 4 Meeting Information Disclosure
  - 4 Authentication of Meeting Attendees
  - 4 Administration-Site Security
- 5 Communications Security Features**
  - 6 Communications Confidentiality and Integrity
  - 6 TCP Layer Security
  - 6 Multicast Layer Security
  - 7 Firewall and Proxy Compatibility
- 7 Endpoint System Security Features**
  - 7 Signed Endpoint Software
  - 7 Cryptographic Subsystem Implementation
- 8 Hosted Infrastructure Security Features**
  - 8 Scalable and Reliable Infrastructure
  - 8 Physical Security
  - 8 Network Security
  - 8 Customer Privacy
- 9 Conclusion**
- 9 Appendix: Security Standards Compliance**

FIGURES

- 1 Figure 1: GoToMeeting Service Architecture
- 5 Figure 2: Communications Security Features

## INTRODUCTION

GoToMeeting™ is the most secure online meeting product available. Standards-based cryptography with true end-to-end encryption, a high-availability hosted service infrastructure, and an intuitive user interface combine to maximize confidentiality, integrity, and availability.

This document provides a technical description of the security features built into GoToMeeting. It has been written for technical evaluators and security specialists who are responsible for ensuring the safety of their company's network and the privacy and integrity of business communications.

GoToMeeting is a Web-based online meeting service that allows multiple PC users to interact using desktop screen sharing, remote keyboard/mouse control, text chat and other features. GoToMeeting is ideal for Web conferencing, customer demos, sales presentations, staff meetings and project management.

GoToMeeting is a hosted service, delivered via Web browsers, downloadable client executables and a network of multicast communication servers operated by Citrix Online. Meetings are scheduled, convened and moderated using the Citrix Online Web site and client software. GoToMeeting automatically integrates with such existing business communication tools as instant messaging, Microsoft® Outlook® email and voice conferencing for ease of use and solution completeness.

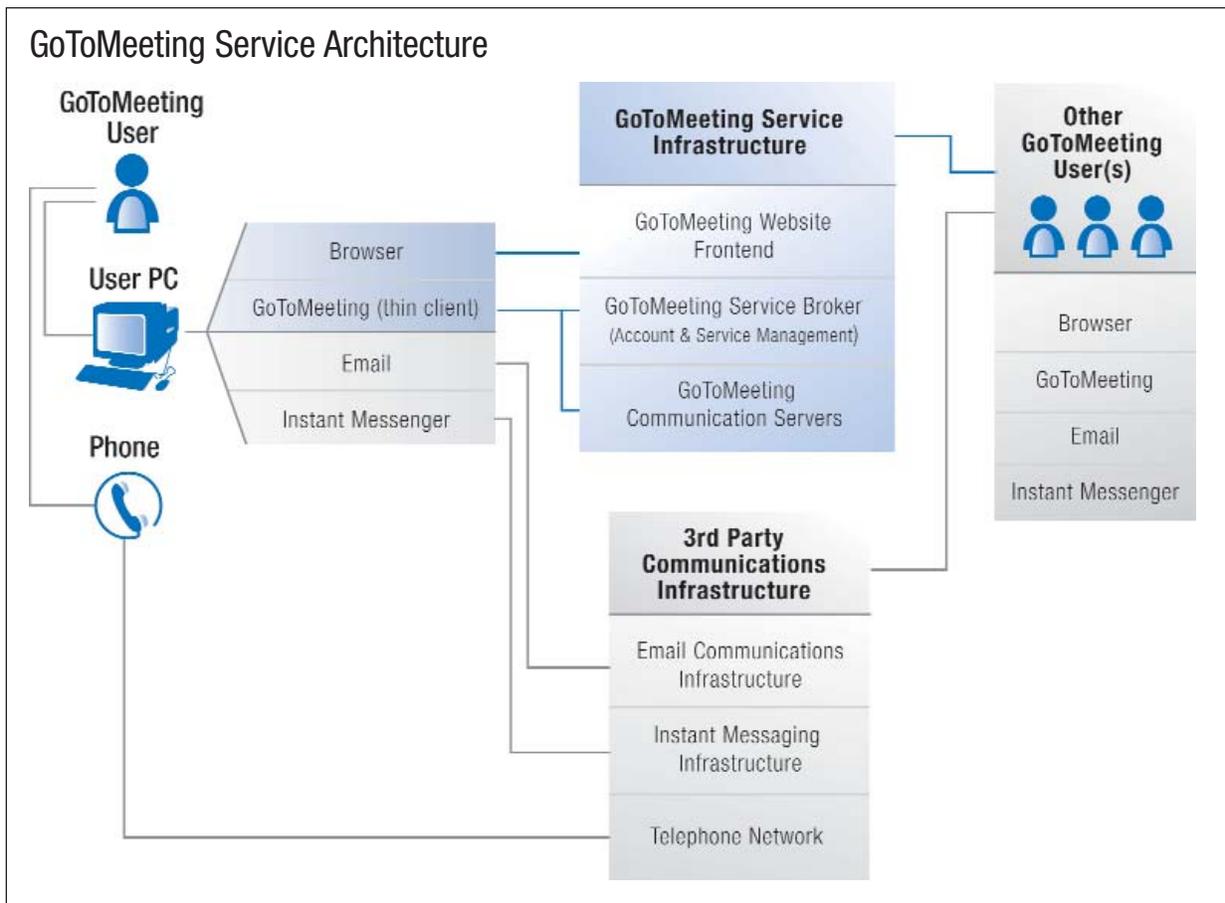


FIGURE 1

## BUSINESS NEEDS FOR SECURE COLLABORATION

Easy-to-use online business collaboration tools like GoToMeeting can help companies increase productivity by enabling them to communicate and interact more effectively with coworkers, business partners and customers. But such tools vary greatly when it comes to embedded security features. Moreover, it is essential to understand the security implications of online collaboration and comply with safe usage guidelines.

Using any online meeting service requires careful consideration of potential threats and resulting business risks. Business security needs that must typically be addressed when adopting an online meeting service include:

- Preventing unauthorized use of the service and its features so that only legitimate users and invited participants can schedule and participate in online meetings
- Avoiding any compromise of company assets, including client computers and the private networks to which they are attached
- Protecting the privacy and integrity of confidential communication, including screen sharing, text messages, email and voice interaction
- Ensuring availability and reliability of the service itself, so that business communications cannot be denied or disrupted
- Integrating seamlessly with other network/computer security measures, so that meeting services can leverage (not degrade) an organization's existing safeguards

GoToMeeting was developed from the ground up to satisfy these common business security needs. By incorporating security features and making them easy to administer and use, GoToMeeting enables effective and safe online business collaboration.

## ROLE-BASED SECURITY FEATURES

To enable account owners to enforce company access policies related to service and feature use, every GoToMeeting user is assigned one of several application-defined roles.

- *Organizers* are authorized to schedule meetings. An Organizer sets up each GoToMeeting session, invites other users to participate, initiates and ends the session, and designates the current Presenter.
- *Attendees* are authorized to participate in GoToMeeting sessions. Attendees can view the Presenter's screen, chat with other Attendees or view the Attendee list.
- *Presenters* are Attendees who are able to share their computer screens with other Attendees. Presenters also decide which other Attendees, if any, are permitted to control the keyboard and mouse of the Presenters' computers.
- *Internal Administrators* are Citrix Online staff members authorized to manage GoToMeeting services and accounts.
- *External Administrators* are individuals from a customer site authorized to manage multi-user GoToMeeting Corporate accounts. External Administrators can configure account features, authorize Organizers and access a variety of service usage reporting tools.

The GoToMeeting user interface provides intuitive session controls and status indicators that facilitate productive and safe online meetings. Controls and privileges available to each user depend on the currently assigned role: Organizer, active Presenter, or general Attendee.

## ORGANIZER PRIVILEGES

Organizers have the most control in a meeting and the ability to grant and revoke various privileges for the other participants. GoToMeeting Organizers can specify the respective roles and privileges of other participants.

Specific Organizer privileges include:

- The ability to invite Attendees, before or during the meeting, so that only authorized participants can join a given meeting
- The ability to see the complete list of Attendees and their current roles and privileges, so the Organizer remains aware of those present at all times
- The ability to start and end the meeting, which prevents others from disrupting the meeting accidentally or otherwise

- The ability to make any Attendee the active Presenter, controlling which desktop can be viewed at any point in time throughout the meeting
- The ability to disallow the use of Chat by one or more Attendees, and permitting "sidebar" discussions only when appropriate
- The ability to disconnect attendees
- The ability to transfer the Organizer role to another Attendee so the meeting can continue if the Organizer must leave early. (Once another Attendee becomes an Organizer this privilege cannot be revoked.)

## PRESENTER PRIVILEGES

A Presenter is the user actively sharing his or her desktop screen with other Attendees. Only one Attendee at a time within a meeting may be granted the active Presenter role. Presenters have the following controls available to them:

- The ability to enable, disable or pause screen sharing, which can be helpful to avoid displaying confidential data that might otherwise appear on the Presenter's desktop (e.g., while searching files or folders)
- The ability to grant/revoke remote keyboard and mouse control to another Attendee, which facilitates efficient communication through desktop interaction
- The ability to make another Attendee the Presenter, providing for a flexible, dynamic flow during meetings

Whenever a Presenter is sharing his or her screen with other Attendees, an "On Air" indicator is displayed on the Presenter's GoToMeeting Control Panel. To share his or her screen, the Presenter must click the "Show My Screen" button on the Control Panel. These features ensure that Presenters always know when desktop sharing is active so that desktop screens are never shared accidentally.

## ATTENDEE PRIVILEGES

Users with the basic Attendee role have the following privileges:

- The ability to join any meeting to which they have been invited at or after the meeting's start time
- The ability to view the Presenter's screen unless the Presenter has paused or disabled screen sharing
- If granted, the ability to remotely control the Presenter's keyboard and mouse. (Remote control privileges are automatically revoked whenever the active Presenter role is changed.)
- The ability to use Chat to send text messages to all other Attendees or to one specific Attendee. (Chat may be disabled for one or more Attendees by an Organizer.)
- The ability to leave a meeting at any time

Basing access rights and privileges on assigned roles allows flexible meetings that facilitate highly dynamic interaction between Attendees, without sacrificing either control or visibility. Organizers can easily add Attendees or change the Presenter as needed throughout the meeting. Presenters remain in complete control of their own desktops, and Organizers have everything required to manage the meeting effectively.

## ACCOUNT AND MEETING AUTHENTICATION FEATURES

Role-based authorization depends upon the ability to correctly identify and authenticate each and every user. To ensure that each Organizer, Presenter and Attendee is in fact who he or she claims to be, GoToMeeting incorporates robust account and meeting authentication features.

### WEB SITE ACCOUNT LOGIN

To access a user account on the GoToMeeting Web site, users must supply a valid email address and corresponding user account password. To make them hard to guess, all passwords must be at least eight characters and contain both letters and numbers. Too many failed log-in attempts cause the Web-site account to be temporarily locked to protect against password guessing. Passwords stored in the service database are encrypted and checked using a cryptographically secured verifier that is highly resilient to offline dictionary attacks.

## MEETING INFORMATION DISCLOSURE

Unlike some competing solutions, information describing scheduled GoToMeeting sessions is only available to the Organizer and invited participants. Because meeting descriptions are only displayed after users have successfully authenticated, and then only to those users authorized to view it, potentially sensitive information such as the meeting subject, Organizer name and meeting time are never exposed for casual perusal by hackers, curious Web surfers or your competition.

## AUTHENTICATION OF MEETING ATTENDEES

Because most organizations hold many meetings with restricted attendance, it is not enough to let any user associated with a given GoToMeeting account view meeting descriptions or attend meetings. Instead, authorization to join each meeting is based on a unique Meeting ID and an optional Meeting Password.

Whenever a meeting is scheduled, a unique nine-digit Meeting ID, created by the GoToMeeting service broker using a pseudorandom number generator, is returned to the Organizer. The Meeting ID is then communicated to all invited Attendees using email, instant messaging, a telephone or other communication methods.

To join the meeting, each Attendee must present the Meeting ID to the service broker by either clicking on a URL that contains the Meeting ID or by manually entering the value into a form presented by the downloaded GoToMeeting client.

Whenever a valid Meeting ID is presented, the service broker returns a set of unique session credentials to the GoToMeeting client. These session credentials are never seen by the Attendee, but are used by the software to connect to one or more GoToMeeting communication servers. Credentials include a 64-bit Session ID, a short Role ID and an optional 64-bit Role Token. These are used to identify the appropriate meeting and transparently authenticate the user as either an Organizer or Attendee. All sensitive communications take place over SSL-protected connections to prevent disclosure of session credentials.

In addition, Attendees must authenticate “end-to-end” with the meeting's Organizer. This is based on a secret random value provided by the service broker and an optional Meeting Password that the Organizer chooses and communicates to Attendees. To provide maximum assurance against unauthorized access and ensure meeting confidentiality, Citrix Online strongly encourages the use of the Meeting Password feature.

It is important to note that the optional Meeting Password is never transmitted to Citrix Online at any time. This provides added assurance that no unauthorized parties, including Citrix Online operations personnel, can join and participate in the meeting.

“End-to-end” authentication is accomplished using the Secure Remote Password (SRP) protocol. SRP is a well-established, robust, secure password-based authentication and key exchange method. SRP is resilient against a wide variety of attacks, including both passive eavesdropping and active password cracking. (More information on SRP may be found at <http://srp.stanford.edu>.)

By providing two levels of Attendee authentication, GoToMeeting ensures that only authorized Attendees can join meetings to which they have been invited, and that each user is granted privileges in accordance with his or her assigned role.

## ADMINISTRATION-SITE SECURITY

Like all connections to the GoToMeeting Web site, connections to the GoToMeeting administration portal are protected using SSL/TLS. Administrative functions are protected using strong passwords, activity logging, regular audits and a variety of internal physical and network security controls.

## COMMUNICATIONS SECURITY FEATURES

Communications between participants in a GoToMeeting session occurs via an overlay multicast networking stack that logically sits on top of the conventional TCP/IP stack within each user's PC. This network is realized by a collection of Multicast Communications Servers (MCS) operated by Citrix Online. This communications architecture is summarized in the figure below.

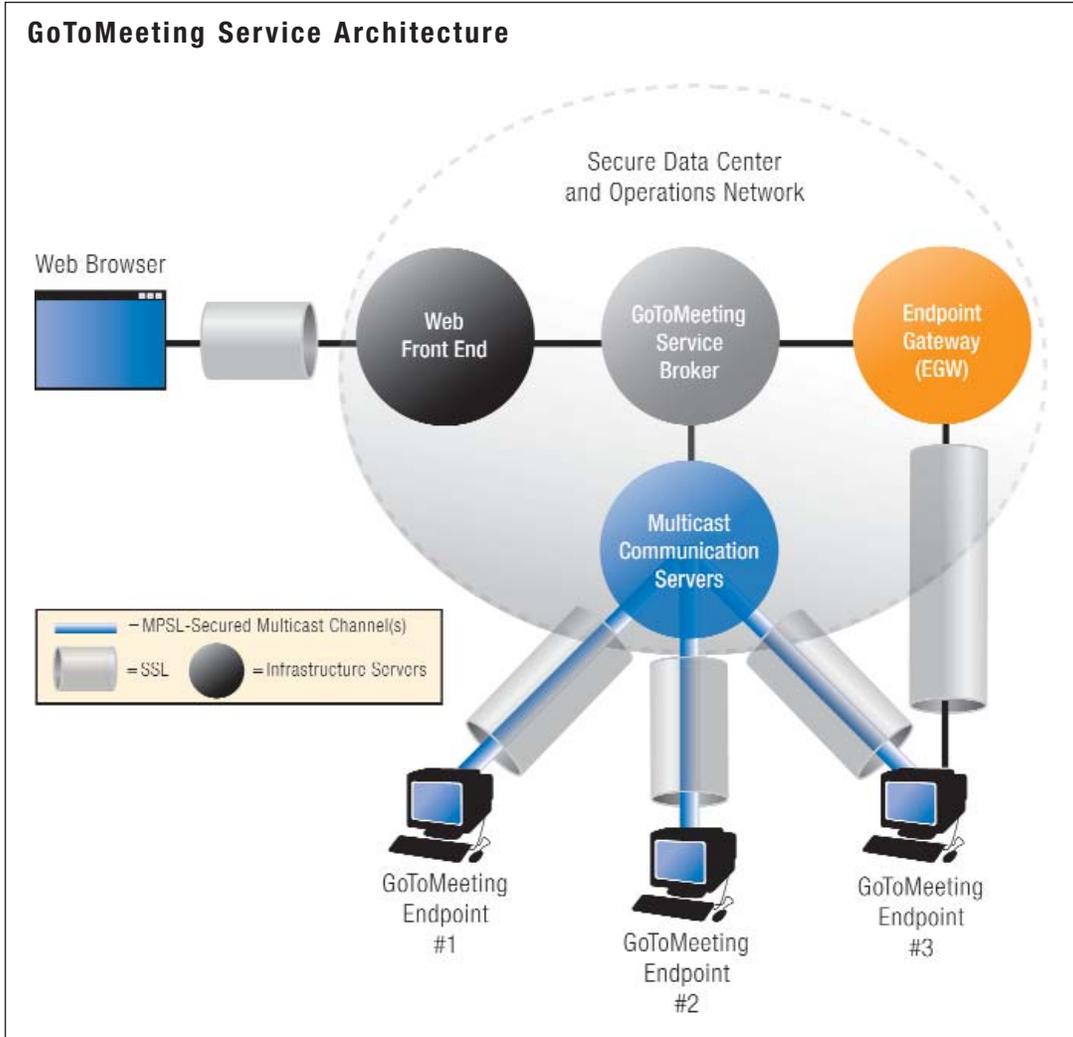


FIGURE 2

GoToMeeting participants (meeting endpoints) communicate with Citrix Online infrastructure communication servers and gateways using outbound TCP/IP connections on ports 8200, 443 and 80. Because GoToMeeting is a hosted Web-based service, participants can be located anywhere on the Internet—at a remote office, at home, at a business center or connected to another company's network. Anytime-anywhere access to the GoToMeeting service provides maximum flexibility and connectivity. However, to preserve the confidentiality and integrity of private business communication, GoToMeeting also incorporates robust communication security features.

## COMMUNICATIONS CONFIDENTIALITY AND INTEGRITY

GoToMeeting provides true “end-to-end” data security measures that address both passive and active attacks against confidentiality, integrity, and availability. All GoToMeeting connections are “end-to-end” encrypted and accessible only by authorized meeting participants. Screen-sharing data, keyboard/mouse control data and text chat information are never exposed in unencrypted form while temporarily resident within Citrix Online communication servers or during transmission across public or private networks.

Communications security controls based on strong cryptography are implemented at two layers: the “TCP layer” and the “Multicast Packet Security Layer” (MPSL).

### TCP LAYER SECURITY

IETF-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to protect all communication between endpoints. To provide maximum protection against eavesdropping, modification, or replay attacks, the only SSL cipher suite supported for non-Web-site TCP connections is 1024-bit RSA with 128-bit AES-CBC and HMAC-SHA1. However, for maximum compatibility with nearly any Web browser on any user’s desktop, the GoToMeeting Web site supports in-bound connections using most supported SSL ciphersuites.

For the customers’ own protection, Citrix Online recommends that customers configure their browsers to use strong cryptography by default whenever possible and to always install the latest operating system and browser security patches.

When SSL/TLS connections are established to the GoToMeeting Web site and between GoToMeeting components, Citrix Online servers authenticate themselves to clients using VeriSign/Thawte public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., MCS-to-MCS, MCS-to-Broker). These strong authentication measures prevent would-be attackers from masquerading as infrastructure servers or inserting themselves into the middle of meeting communications.

### MULTICAST LAYER SECURITY

Additional features provide complete “end-to-end” security for multicast packet data, independent of those provided by SSL/TLS. Specifically, all multicast session data is protected by “end-to-end” encryption and integrity mechanisms that prevent anyone with access to our communications servers (whether friendly or hostile) from eavesdropping on a GoToMeeting session or manipulating data without detection. This added level of communication confidentiality and integrity is unique to GoToMeeting. Company communications are never visible to any third party, including both users who are not invited to a given meeting and Citrix Online itself.

MPSL key establishment is accomplished using public-key-based SRP-6 authenticated key agreement, using a 1024-bit modulus to establish a wrapping key. This wrapping key is then used for group symmetric key distribution using the 128-bit AES-CTR algorithm (see <http://srp.stanford.edu/design.html>). All keying material is generated using a FIPS-compliant pseudorandom number generator seeded with entropy data collected at run-time from multiple sources on the host machine. These robust, dynamic key generation and exchange methods offer strong protection against key guessing and key cracking.

MPSL further protects multicast packet data from eavesdropping using 128-bit AES encryption in Counter Mode. Plaintext data is typically compressed before encryption using proprietary, high performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value generated with the HMAC-SHA-1 algorithm. Because GoToMeeting uses very strong, industry-standard cryptographic measures, customers can have a high degree of confidence that multicast meeting data is protected against unauthorized disclosure or undetected modification.

Furthermore, there is no additional cost, performance degradation or usability burden associated with these essential communication security features. High performance and standards-based data security is a “built-in” feature of every GoToMeeting session.

## FIREWALL AND PROXY COMPATIBILITY

Like other Citrix Online products, GoToMeeting includes built-in proxy detection and connection management logic that helps automate software installation, avoid the need for complex network (re)configuration, and maximize user productivity. Firewalls and proxies already present in your network generally do not need any special configuration to enable use of GoToMeeting.

When GoToMeeting endpoint software is started, it attempts to contact the GoToMeeting service broker via the Endpoint Gateway (EGW) by initiating one or more outbound SSL-protected TCP connections on ports 8200, 443, and/or 80. Whichever connection responds first will be used and the others will be dropped. This connection provides the foundation for participating in all future meetings by enabling communication between hosted servers and the user's desktop.

When the user attempts to join a meeting, GoToMeeting endpoint software establishes one or more additional connections to Citrix Online communications servers, again using SSL-protected TCP connections on ports 8200, 443 and/or 80. These connections carry meeting session data during an active meeting.

In addition, for connectivity optimization tasks, the endpoint software initiates one or more short-lived TCP connections on ports 8200, 442 or 80 that are not SSL protected. These network "probes" do not contain any sensitive or exploitable information and present no risk of sensitive information disclosure.

By automatically adjusting the local network conditions using only outbound connections and choosing a port that is already open in most firewalls and proxies, GoToMeeting provides a high degree of compatibility with existing network security measures. Unlike some other products, GoToMeeting does not require companies to disable existing security measures to allow online meeting communication. These features maximize both compatibility and overall network security.

## ENDPOINT SYSTEM SECURITY FEATURES

Online meeting software must be compatible with a wide variety of desktop environments, yet create a secure endpoint on each user's desktop. GoToMeeting accomplishes this using Web-downloadable executables that employ strong cryptographic measures.

### SIGNED ENDPOINT SOFTWARE

The GoToMeeting client endpoint software is a Win32 executable that is downloaded to users' PCs. A digitally signed Java applet is used to mediate the download and verify the integrity of the GoToMeeting endpoint software from Citrix Online servers. This protects the user from inadvertently installing a trojan or other malware posing as GoToMeeting software.

The endpoint software is composed of several Win32 executables and dynamically linked libraries. Strict quality control and configuration management procedures are followed by Citrix Online during development and deployment to ensure software safety. The endpoint software exposes no externally available network interfaces and cannot be used by malware or viruses to exploit or infect remote systems. This protects other desktops participating in a meeting from being infected by a compromised host used by another Attendee.

## CRYPTOGRAPHIC SUBSYSTEM IMPLEMENTATION

All cryptographic functions and security protocols employed by GoToMeeting client endpoint software are implemented using state-of-the-art **Certicom Security Builder® Crypto™** and **Certicom Security Builder® SSL™** libraries for assurance and high performance.

Use of the cryptographic libraries is restricted to the GoToMeeting endpoint application; no external APIs are exposed for access by other software running on that desktop. All encryption and integrity algorithms, key size, and other cryptographic policy parameters are statically encoded when the application is compiled. Because there are no end-user-configurable cryptographic settings, it is impossible for users to weaken GoToMeeting's security through accidental or intentional misconfiguration. A company that uses GoToMeeting can be certain that the same level of online meeting security is present on all participating endpoints, regardless of who owns or operates each desktop.

## HOSTED INFRASTRUCTURE SECURITY FEATURES

Citrix Online delivers GoToMeeting using an application service provider (ASP) model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

### SCALABLE AND RELIABLE INFRASTRUCTURE

Citrix Online's service architecture has been designed for maximum performance, reliability and scalability. The GoToMeeting service is driven by industry-standard, high-capacity servers and network equipment with the latest security patches in place. Redundant switches and routers are built into the architecture to ensure that there is never one single point of failure. Clustered servers and backup systems help guarantee a seamless flow of application processes—even in the event of heavy load or system failure. For optimal performance, the GoToMeeting broker load balances the client/server sessions across geographically distributed communication servers.

### PHYSICAL SECURITY

All GoToMeeting Web, application, communication and database servers are housed in secure co-location data centers. Physical access to servers is tightly restricted and continuously monitored. All facilities have redundant power and environmental controls.

### NETWORK SECURITY

Citrix Online employs firewall, router and VPN-based access controls to secure our private-service networks and backend servers. Infrastructure security is continuously monitored and vulnerability testing is conducted regularly by internal staff and outside third-party auditors.

Citrix Online is SiteSecure Certified by TruSecure Corporation. The SiteSecure audit and certification involves a series of evaluations of Citrix Online's network architecture, devices, configurations, and policies. Each of these areas is measured against potential threats to critical systems and data across major areas of risk including electronic threats, malicious code, downtime, privacy, physical security and human factors. The results determined that Citrix Online provides customers with enterprise-class protection against threats to critical systems and data.

TruSecure Corporation certifies the continual security of critical systems and information for thousands of companies. Its rigorous SiteSecure Certification process is validated regularly with quarterly audits. Through these measures and our comprehensive, state-of-the-art communications security architecture, you can be assured that your data and local systems remain secure when you use GoToMeeting.

### CUSTOMER PRIVACY

Because maintaining the trust of our users is a priority for us, Citrix Online is committed to respecting your privacy. A link to a copy of the current Citrix GoToMeeting privacy policy can be found on the service Web site at [www.gotomeeting.com](http://www.gotomeeting.com).

## CONCLUSION

With GoToMeeting, it's easy to conduct meetings, present information and demonstrate products online to improve business communication. This service's intuitive and secure interface and feature set make it the most effective solution for conducting and attending online meetings.

Behind the scenes, Citrix Online's hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment. As this paper shows, GoToMeeting promotes ease of use and flexibility without compromising the integrity, privacy or administrative control of business communication or assets.

## APPENDIX: SECURITY STANDARDS COMPLIANCE

GoToMeeting is compliant with the following industry and US government standards for cryptographic algorithms and security protocols:

- The TLS/SSL Protocol, Version 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
  - (FIPS Validated Implementation, NIST Certificate #175)
- AES Ciphersuites for TLS, IETF RFC 3268
- RSA, PKCS #1
- SHA-1, FIPS 180-1
  - (FIPS Validated Implementation, NIST Certificate #89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2



Citrix Online, a division of Citrix Systems, Inc. (Nasdaq: CTXS), is a leading provider of easy-to-use, on-demand applications for remote desktop access, Web conferencing and collaboration. Its "Simpler Is Better" approach to empowering business productivity online offers small and mid-sized businesses, consumers and professionals an easier, more cost-effective and secure way to access and interact with information, customers, partners and employees in real time. Citrix Online's award-winning services, which are used by more than 20,000 businesses and hundreds of thousands of individual subscribers, include: Citrix® GoToMyPC® for easy, secure remote PC access from anywhere; Citrix® GoToAssist™ for live, easy remote support; Citrix® GoToMeeting® for online meetings made easy; and Citrix® GoToWebinar™, the industry's first do-it-yourself solution for Web events. Based in Santa Barbara, California, Citrix Online has satellite offices and data centers distributed around the world. For more information, please visit [www.citrixonline.com](http://www.citrixonline.com).

©2006 Citrix Online, LLC. All rights reserved. Citrix® is a registered trademark of Citrix Systems, Inc., in the United States and other countries. GoToMyPC®, GoToAssist™, GoToMeeting® 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.

#11616/1.2.07/PDF

For more information on GoToMeeting, please visit [www.gotomeeting.com](http://www.gotomeeting.com)

## Citrix Online

**A Division of Citrix Systems, Inc.**  
5385 Hollister Avenue  
Santa Barbara, CA 93111 USA

**Product Information:**  
[www.gotomeeting.com](http://www.gotomeeting.com)

**Sales Inquiries:**  
[gotomeeting@citrixonline.com](mailto:gotomeeting@citrixonline.com)  
Phone: (800) 372-6207

**Channel Partners:**  
[resellers@citrixonline.com](mailto:resellers@citrixonline.com)  
Phone: (805) 690-5711

**Media Inquiries:**  
[pr@citrixonline.com](mailto:pr@citrixonline.com)  
Phone: (805) 690-2961

[www.citrix.com](http://www.citrix.com)