Technical and Organizational Measures

GoToMyPC

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoToMyPC. GoTo upholds comprehensive global privacy and security programs, along with organizational, administrative, and technical safeguards designed to:

- Ensure the confidentiality, integrity, and availability of Customer Content.
- Protect against threats and hazards to the security of Customer Content.
- Prevent any loss, misuse, unauthorized access, disclosure, alteration, and destruction of Customer Content.
- Maintain compliance with applicable laws and regulations, including data protection and privacy laws.

These measures include:

- **Encryption**:
  - *In-Transit* - Transport Layer Security (TLS) v1.2 or higher.
  - *At Rest* - Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Compliance Audits:** GoToMyPC holds SOC 2 / SOC 3 Type II, BSI C5, PCI DSS, TRUSTe Enterprise Privacy certifications, Internal controls assessment as required under a PCAOB annual financial statements audit, Global CBPR and PRP certifications, and APEC CBPR and PRP certifications.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA/CPRA and LGPD.
- **Penetration Testing**: In addition to in-house testing, GoTo contracts with external firms to conduct regular security assessments and/or penetration testing.
- **Logical Access Controls:** Logical access controls are implemented and designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: GoTo employes a multi-tenant architecture and logically separates Customer accounts at the database level.
- **Perimeter Defense and Intrusion Detection**: GoTo employs advanced perimeter protection tools, techniques, and services to prevent unauthorized network traffic from accessing its product infrastructure. The GoTo network is safeguarded by externally facing firewalls and internal network segmentation to ensure robust security.
- **Retention**:
  - GoToMyPC Customers may request the return or deletion of Customer Content at any time, which will be fulfilled within thirty (30) days of Customer's request.
  - Customer Content will automatically be deleted: (a) ninety (90) days after expiration of a Customer's then-final paid subscription term; or (b) for free accounts, ninety (90) days after expiration.

Contents

1 Product Introduction

This document covers the Technical and Organizational Measures (TOMs) for GoToMyPC, a cloud hosted service that enables secure remote access to an internet-connected Windows-based or Mac host computer from any remote computer, iPad, iPhone or Android device. Features include a screen-sharing viewer, drag-and-drop file transfer, remote printing, guest invite, use with multiple monitors, mobile apps and chat. There are two versions of GoToMyPC available in order to meet the needs of individuals, professional teams and corporations.

GoToMyPC provides two connection options:

- **GoToMyPC Classic:** The traditional application-based remote access solution
- **Connect-in-Browser (New GoToMyPC):** A browser-based solution built on the Resolve platform, accessible via the "Connect-in-Browser" button or through the New GoToMyPC console at https://console.gotomypc.com/

2 Product Architecture

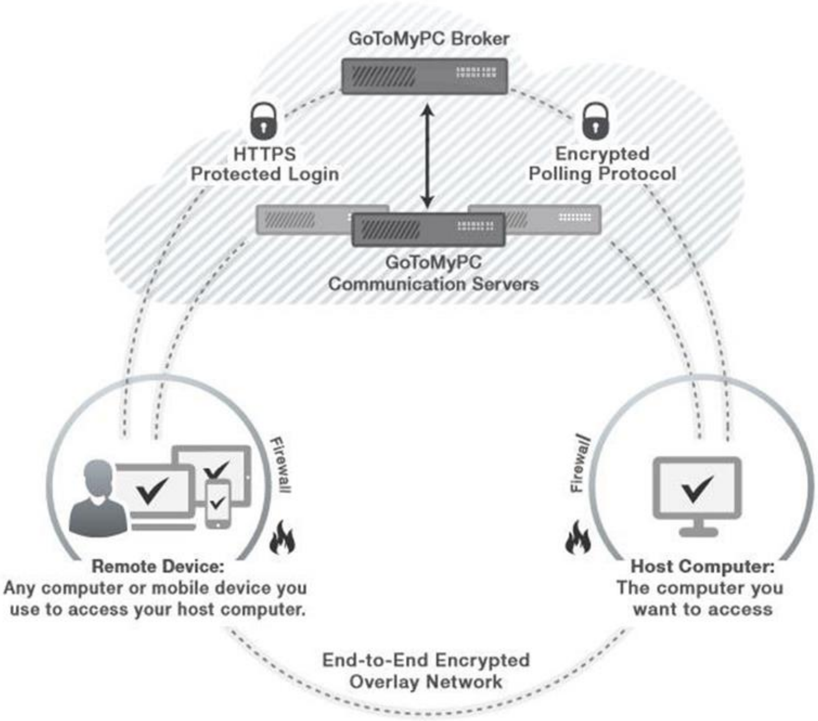
GoToMyPC offers two distinct connection methods; each built on different technical architectures:

2.1 GoToMyPC Classic

GoToMyPC is a hosted service comprised of five components:

- **Host Computer**: Typically, a home or office computer with always-on internet access on which a small footprint server is installed. This server registers and authenticates itself with the GoToMyPC broker.
- **Browser**: From the remote computer, called the client, the user launches a web browser, visits the secure GoToMyPC website, enters their username and password, and clicks “Connect” to send the broker an authenticated, encrypted request for access to the desired host computer. Alternatively, the user can install the GoToMyPC app on a supported tablet or smartphone or GoToMyPC Clientapp (windows only), enter their account details and click “Connect” to initiate the request.
- **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 session-specific executable applet — is automatically loaded by our automatic launcher tool.
- **Communication Server**: The communication server is an intermediate system that relays an opaque and highly compressed encrypted stream between the client and host computers for the duration of each GoToMyPC session.
- **Direct Connections**: Once the user is authenticated and connected, GoToMyPC attempts to establish a direct connection between the client and host, bypassing the GoToMyPC communication server whenever possible to increase the connection speed and improve in-session performance. The Direct Connections feature instructs both the

client and host to listen for a limited time for incoming connections and to attempt outgoing connections to each other; whichever signal arrives first establishes the connection. The client and host then proceed to execute a Secure Remote Password (SRP) protocol-based authenticated key agreement and establish a secure connection that is designed in a manner intended to reduce or eliminate susceptibility to “man-in the-middle” attacks. Should the direct connection be blocked or interrupted, the connection previously established through the communication server maintains remote access service. The Direct Connections feature is always enabled for GoToMyPC and GoToMyPC Pro accounts and is optional for GoToMyPC Corporate.


GoToMyPC Broker
HTTPS Protected Login
Encrypted Polling Protocol
GoToMyPC Communication Servers
Firewall
Firewall
Remote Device: Any computer or mobile device you use to access your host computer.
Host Computer: The computer you want to access
End-to-End Encrypted Overlay Network

The infrastructure is designed in a manner intended to be both robust and secure. Redundant routers, switches, server clusters and backup systems are designed and employed to ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among web servers. For the purposes of ensuring optimal performance, the GoToMyPC broker load balances the client/server sessions across geographically distributed communication servers.

GoTo’s proprietary key exchange forwarding protocol is designed to provide security against interception or eavesdropping on our own infrastructure. Specifically, the connection between the client and the host is facilitated by the gateway in order to ensure that the client can connect to the host independently of the network setup.

With the host already having established a TLS connection to the gateway, the gateway forwards the client's TLS key exchange to the host via a proprietary key renegotiation request. This results in the client and the host exchanging TLS keys without the gateway learning the key.

2.2 GoToMyPC Connect-in-Browser (New GoToMyPC)

GoToMyPC Connect-in-Browser provides an alternative browser-based connection method that leverages the LogMeIn Resolve platform as its underlying technical foundation. This solution enables remote access directly through web browsers without requiring additional software installation.

Access Methods:

- Via the "Connect-in-Browser" button on the traditional GoToMyPC interface
- Via the primary "Connect" button when using the New GoToMyPC console at https://console.gotomypc.com/

Both access methods utilize the same Resolve-based architecture and provide identical remote access functionality and user experience. For detailed technical and organizational measures specific to the Resolve platform architecture, please refer to the LogMeIn Resolve Technical and Organizational Measures document .

3 Technical Security Controls

GoTo employs industry standard technical security controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service) designed to safeguard the Service infrastructure and data residing therein.

3.1 Malware Protection

Malware protection software with audit logging is deployed on all GoToMyPC servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.2 Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications and other relevant standards groups. The cryptographic standard is periodically reviewed and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

3.3 In-Transit Encryption

GoToMyPC uses TLS 1.2 to establish a secure tunnel and perform a mutually authenticated key exchange, which generates unique, secret encryption keys for each session. These keys are then used by AES-256 to encrypt the actual remote desktop data transmitted through the tunnel. Together, TLS 1.2 and AES-256 provide strong, session-specific in-transit encryption for all traffic between the browser client and host computer.

3.4 Encryption at Rest

GoToMyPC configurations, all session data, and recording files are encrypted at rest with 256-bit AES encryption.

4 Hosting Workloads

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using cloud hosting data centers.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the GoToMyPC Sub-Processor Disclosure available in the Product Resources section of the GoTo Trust and Privacy Center.

4.1 Cloud hosted workloads

Physical security is the responsibility of the Cloud provider. Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls/
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

Other than physical security, all cloud providers operate with some form of a shared responsibility model where the cloud provider is responsible for protecting the infrastructure (hardware, software, networking) that runs all the services the provider offers. GoTo is responsible for the configuration of the services they are using.

5 Logical Access Control

Users authorized to access GoToMyPC product components may include GoTo's authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. Cloud-based production components are managed through a restricted Software-Defined Perimeter solution.

For Connect-in-Browser sessions utilizing the Resolve platform, access controls follow the measures outlined in the GoTo Resolve TOMs document.

6 Customer Content Retention Schedule

Session recordings will be deleted on an ongoing 90-day rolling basis.[1] Additionally, unless otherwise required by applicable law, Customer Content shall automatically be deleted: 1) for paid

[1] Customers with other retention requirements can elect to locally save recordings to a storage location of their choosing outside of GoTo environments. For more information, see the "Playing Session Recordings" section here.

accounts, ninety (90) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription; or 2) for free accounts, after one (1) year of inactivity (e.g., no logins).

Upon written request, GoTo may provide written confirmation/certification of Content deletion.

7 Revision History

Version	Month/Year	Description
Version 1.3	September 2024	Updated and published by Legal
Version 1.4	August 2025	Standardized the document to include Product Specific sections only.
Version 1.5	November 2025	Added GoToMyPC Connect-in-Browser architecture details and restructured Product Architecture section to distinguish between Classic and Connect-in-Browser connection methods. Updated Product Introduction to acknowledge dual connection options. Added cross-references to GoTo Resolve TOMs document for platform-specific technical details.