Technical and Organizational Measures
Join.Me

Executive Summary

The Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for JoinMe. 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 and 1.3.
  - *At Rest* - Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Compliance Audits and Certifications:** JoinMe holds the TRUSTe Enterprise Privacy certification, Internal controls assessment as required under a PCAOB annual financial statements audit,.
- **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 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**:
  - JoinMe 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, after one (1) year of inactivity (e.g., no logins). Recordings are deleted on a rolling basis after ninety (90) days.

Contents

1 Product Introduction

This document covers the Technical and Organizational Measures (TOMs) for join.me.

Join.me is an online meeting and screen sharing service that gives users the ability to quickly and securely host an online meeting with other people. These services can be initiated through a visit to the https://join.me website, through a small downloadable desktop application or through mobile applications (iOS and Android). It is available in a “Lite” version as well as a “Pro” premium version for individuals and small teams and a premium “Business” version for larger teams and company-wide use.

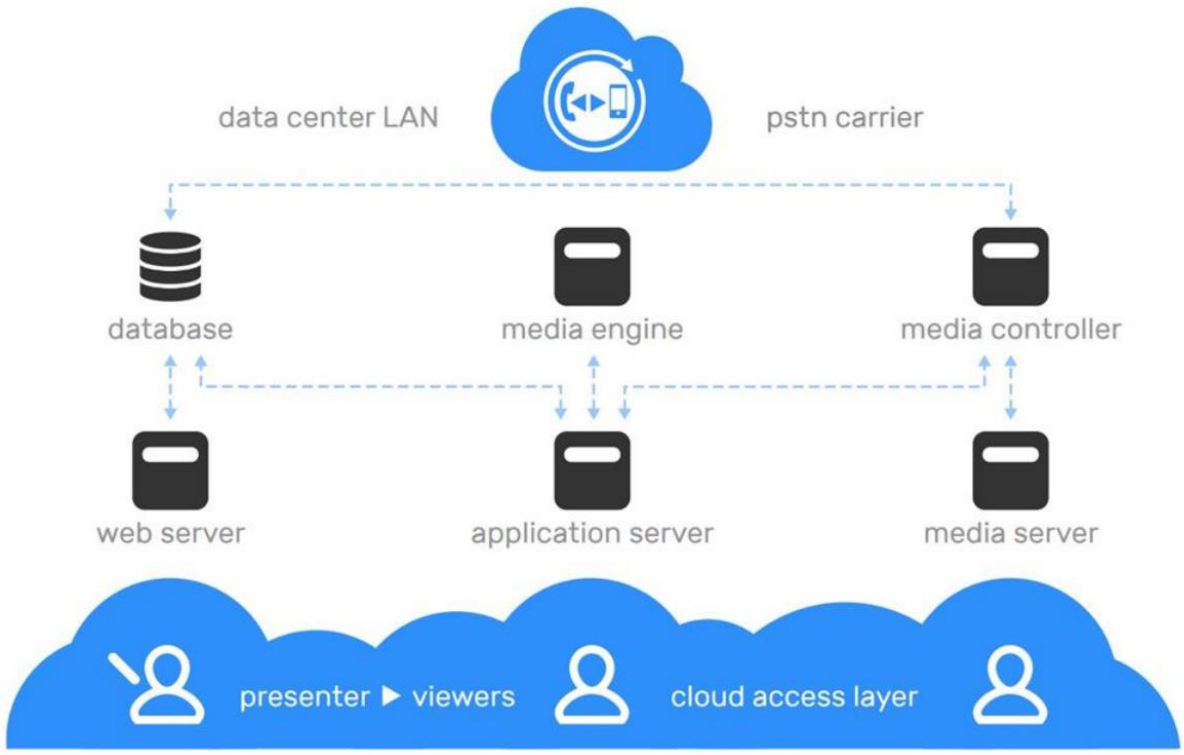
2 Product Architecture

Join.me is a SaaS-based application hosted on multi-tier architecture located in secure and reliable data centers in key locations around the globe. A multi-layer security approach is utilized at all levels from the physical layer through the application layer.

The join.me architecture includes components such as web servers, application servers, media servers, databases, media controllers and media engines. The application has built-in redundancies, designed to increase the availability and reliability of the service, so that if an application server or data center goes off-line or become unreachable, the session should quickly migrate to a different application server. Load balancers are utilized in order to geographically maintain availability. Both access to the application website and the information that travels between components is encrypted in transit utilizing Transport Layer Security (TLS) protocol. Customers have the flexibility to elect specified types of data that are stored on their behalf -- session data, for example, such as screens, video, audio or chat logs, are not, by default stored on GoTo servers. See the join.me architecture white paper for more information.

Services provided by join.me rely on third-party telecommunication companies to provide the audio-based conference infrastructure that allows audio participants to connect to each other regardless of which endpoint device they use to join. WebRTC technology is utilized to deliver video conferencing on platforms such as Windows, Mac OS X, HTML5, iOS and Android. The MP4 video format is used to save video recordings and can be stored in the Azure storage region closest to the presenter’s location.

A typical **join.me** session involves at least the following components:



Web server – User registration, account and meeting settings, meeting launch

Application Server – Maintains meetings, distributes data among appropriate viewers

Media server – Distributes media streams among appropriate viewers

Database – Stores user profiles and meeting settings

Media controller – Controls media sessions and PSTN connections

Media engine – Post-processes media elements to provide recorded meeting video

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. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

4.1 Malware Protection

Malware protection software with audit logging is deployed on all join.me Servers. Alerts indicating potential malicious activity are sent to the appropriate response team.

4.2 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.

4.2.1 In-Transit Encryption

At the protocol level, join.me uses TLS for communications security. The key exchange protocol is ECDHE, while data encryption in transit utilizes the Advanced Encryption Standard (AES) (preferably at AES256-SHA384). Every session is secured using the Application Server's TLS certificate. The Application Server terminates the SSL connections that are established by the viewer and the presenter -- while a single viewer/presenter pair could potentially employ encryption and use the Application Server as a simple networking relay, this becomes unfeasible when multiple viewers are present. As designed, the system supports multiple viewers without placing bandwidth constraints on the presenter. All join.me communications are secured using TLS, including access to the website itself.

4.3 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

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 JoinMe 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 (AWS, Azure, OCI). Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls
- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- 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. The customer is responsible for the configuration of the services they are using.

5 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in both the corporate and production environment. Employees are granted minimum (or "least privilege") access to specified GoTo systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

6 Customer Content Retention Schedule

Unless otherwise required by applicable law, Customer Content shall automatically be deleted: 1) for paid accounts, eighty (80) 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	July 2024	Updated and published by Legal
Version 1.4	September 2025	Standardized the document to include Product Specific sections only.