Technical and Organizational Measures
Rescue Live Guide

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for Rescue Live Guide. 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.
- **Cloud Provider Regions:**[1] United States, Germany, and Japan hosting locations to support redundancy.
- **Compliance Audits:** 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 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 offensive security testing, GoTo contracts with external firms to conduct 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 employs 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**:
  - Rescue Live Guide 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.

[1] Hosting locations may vary (i.e., depending on data residency election), consult the applicable Rescue Live Guide Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

- 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 **Rescue Live Guide.** Rescue Live Guide is a web-based support tool used by customer care professionals to provide remote visual guidance in the browser, without the need for adding a script to the supported website or downloading any software. With the permissions of the end-user, Rescue Live Guide allows a customer care professional to co-browse websites with the end-user in a secure way and provides guiding tools to the agent.

2 Product Architecture

GoTo Rescue Live Guide is a Software-as-a-Service (SaaS)-based visual engagement solution that connects that end-user and the agent in a cloud based secure browser.

Both the Agent and the end-user applications are web applications running in the users' supported browser of choice. The backends serving these applications are hosted in GoTo's Amazon Web Services (AWS) cloud, providing the peers with the means to connect with one another in a co-browsing session.

The session is created when an end-user initiates a shared browsing session. A session PIN is generated and displayed for the end-user at the start of the session. The end-user can let the Agent join the session by sharing the session PIN. Once a co-browse session is established between end-user and Agent, the supported website is loaded in an isolated headless browser in the GoTo cloud.

The actual web browsing, and all communication with the supported website, takes place in the cloud browser. The image is streamed to both users' web applications and the user actions are sent back to be performed in the cloud browser.

The cloud browser instances are completely isolated and other than reporting data, recording (if enabled) and session information, data is purged after the conclusion of a co-browsing session.

You can learn more about the security measures of the solution in the Technical Security Controls section.

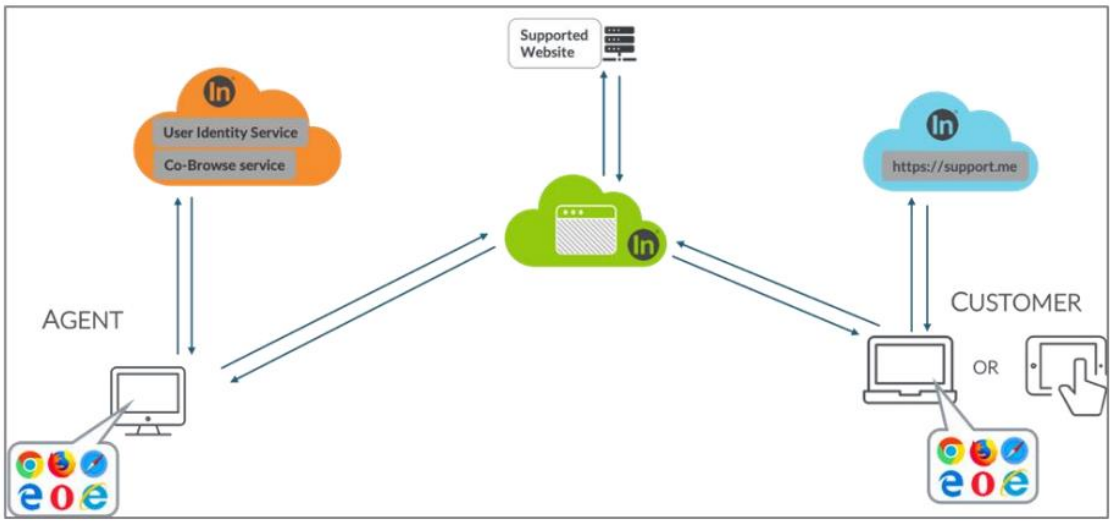

Figure 1- Rescue Live Guide Infrastructure

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.

4.1. Malware Protection

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

4.2 End-user Protection

The privacy of end-users of Rescue Live Guide was considered when creating this Service: the session PIN is owned by the end-user and a support agent can only join a session if the end-user has shared their session PIN with them. Additionally, the session PIN is company specific: A session initiated on a given website can only be joined by Agents who are part of the account assigned to the given supported website.

GoTo does not store the end-user content that is generated during the support session – as mentioned earlier, the cloud browser instances are completely isolated and other than reporting data, recording (if enabled) and session information, data is purged after the conclusion of a co-browsing session.

A Stop button is also available for the end-user during the whole support session -- the end-user can terminate the support session anytime by clicking this button.

4.3. 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.

4.3.1. In-Transit Encryption

All network traffic flowing in and out of GoTo datacenters, including all Customer Content, is encrypted in transit. To provide protection against eavesdropping, modification or replay attacks, IETF-standard Transport Layer Security protocols are used to protect all communication between endpoints and our services. Our services support the following encryption protocols (as applicable): TLS 1.2, 2048-bit RSA, AES-256 strong encryption ciphers with 384-bit SHA-2 algorithm.

4.3.2. At-Rest Encryption

Rescue Live Guide configurations, session data and recording files are encrypted at rest with 256-bit AES encryption.

4.4. Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities 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 Data Backup, Disaster Recovery and Availability

RPO and RTO times are measured during the annual disaster recovery test. During the last testing, we measured **30 minutes of RTO**. Since we have Point in Time recovery enabled on the database, the **RPO is less than 1 second**.

5 Hosting Workloads

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using:

a) redundant, active-active design; and
b) cloud hosting provider data centers.

Upon account creation, Rescue Live Guide Customers may elect to utilize either GoTo's European Union or Global data infrastructure to store their Customer Content. Hosting locations are specified below[2]:

- **European Union:** Germany
- **Global:** United States, Germany, Japan.

5.1 Cloud hosted workloads

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

- https://aws.amazon.com/compliance/data-center/controls/

Other than physical security, all cloud provider operates 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 used.

6 Logical Access Control

Users authorized to access Rescue Live Guide 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 available through Azure Entra authentication.

7 Customer Content Retention Schedule

Session recordings will be deleted on an ongoing 90-day rolling basis.[3] Additionally, unless otherwise required by applicable law, Customer Content shall automatically be deleted: 1) for paid 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.

[2] Hosting locations may vary (i.e., depending on data residency election), consult the applicable Rescue Live Guide Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

[3] 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.