Technical and Organizational Measures
LogMeIn Resolve

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for LogMeIn Resolve. 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:** LogMeIn Resolve holds ISO/IEC 27001:2022, 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 and LGPD.
- **Penetration Testing**: In addition to in-house 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**:
  - LogMeIn Resolve 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).

Contents

1 Product Introduction

LogMeIn Resolve enables IT and supports professionals to deliver remote support to computers, servers and mobile devices with remote view, remote control and camera share functionality from a web-based or desktop agent console. LogMeIn Resolve employs data security measures designed to defend against both passive and active attacks.

Capitalized terms in this document that are not defined within the text are defined in the Terms of Service.

2 Product Architecture

LogMeIn Resolve uses an application service provider (ASP) model designed to provide secure operations while integrating with a company's existing network and security infrastructure. Its architecture is designed to provide optimal performance, reliability and scalability. LogMeIn Resolve leverages Amazon Web Services and Microsoft Azure cloud resources to provide a scalable, highly available solution with no single point of failure. LogMeIn Resolve uses backup systems hosted in multiple regions to support continued operation of application processes in the event of a heavy load or system failure.

2.1 Communications Architecture

The LogMeIn Resolve communications architecture is summarized in the figure below:

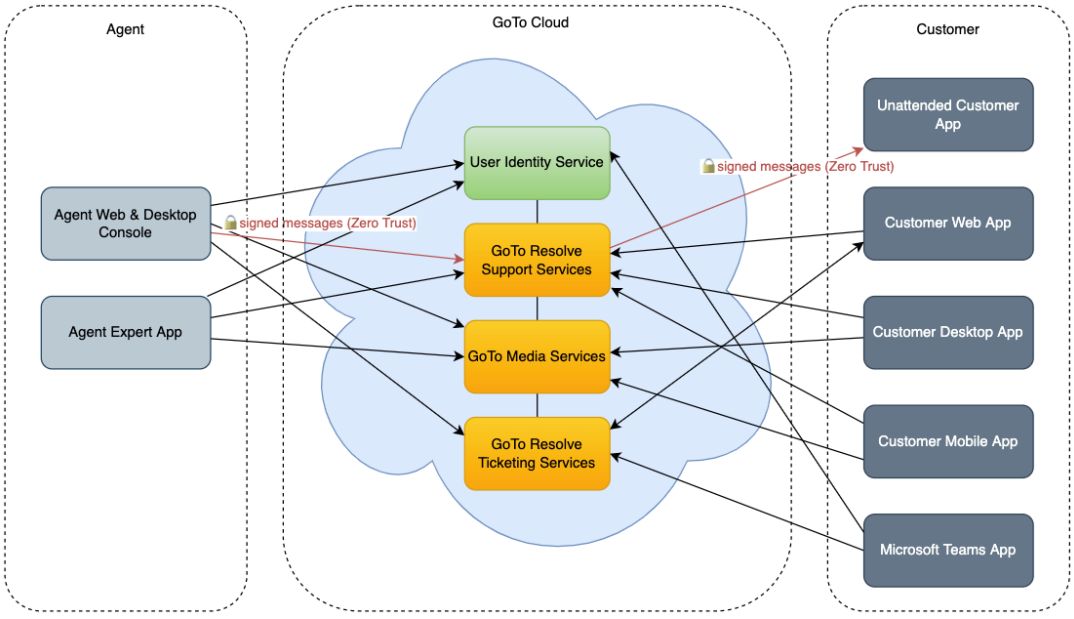

Figure 1: LogMeIn Resolve Communications Architecture

Agent authentication utilizes GoTo's proprietary User Identity Service. Communication between participants in a LogMeIn Resolve screen sharing session occurs via an overlay networking stack that logically sits on top of the conventional User Datagram Protocol (UDP) and Transmission Control Protocol/Internet Protocol (TCP/IP). This network is provided by LogMeIn Resolve and GoTo Media Services hosted on Amazon Web Services and Microsoft Azure.

LogMeIn Resolve session participants (Agent Web Console, Agent Desktop Console, Agent Expert App and End User Endpoints (shown in Figure 1 as "Customer" Endpoints)) communicate with LogMeIn Resolve and the GoTo Media Service using outbound TCP connections on port 443 or UDP port 15000, based on availability. Because LogMeIn Resolve is a web-based service, participants can access it from nearly anywhere if they are connected to the Internet—at a remote office, at home, at a business center or connected to another company's network.

2.2 Agent Desktop Console

Agents can use Agent Web Console or an installable Agent Desktop Console to connect to LogMeIn Resolve. The Desktop Console uses the cross-platform Qt toolkit to run on MacOS and Windows and leverages the open-source Chromium web browser to support components of the Web Console.

2.3 Zero Trust Model

2.3.1 Architecture

LogMeIn Resolve employs a zero trust architecture wherein agents using LogMeIn Resolve create a private signature key that is a required, additional form of verification used when performing sensitive tasks.

The key uniquely identifies the agent. When deploying the LogMeIn Resolve application on a remote device, the key creates a link between the agent and the device. The key is used to sign commands sent to the remote device so the remote device can verify the origin.

For this authorization, cryptographic key pairs are used. The private key, that is used to sign commands is only known by the agent (i.e., not known by LogMeIn Resolve Services or Customer endpoints). The public key is deployed to each remote device and used to verify the signature of each command received from the agent. In this model, the remote devices do not "trust" LogMeIn Resolve Services – they trust the commands coming from an agent with an authorized key

2.3.2 Signature Key Types

The core of the signature key is a private-public key pair: the public key is stored in the backend and shared with each device while the private key never leaves the agent's machine/browser in unencrypted form. The key pair is randomly generated on the P-384 elliptic curve in the agent's browser, using native methods.

The cryptographic key pairs are encrypted using a password and then stored in the backend so that the agents can access their keys from any browser. The encryption key is derived from the password and is different for each company and agent.

2.3.3 Cipher Suites

The zero trust architecture uses the following cryptographic algorithms:

- ECDSA on elliptic curve P-384 (used for private-public key generation)
- SHA-256/512 hashing algorithm
- HMAC-SHA-256 (used for message authentication)
- AES256 with GCM cipher mode of operation (used for key encryption)
- PBKDF2 key derivation function

These cryptosystems and ciphers are handled by the operating system or the OpenSSL library. They are either provided by the operating system or by the OpenSSL library.

2.4 Zero Trust Example

The following diagrams (Figures 2, 3 and 4 below) demonstrate how LogMeIn Resolve's zero trust architecture is designed to protect your devices. Figure 2 shows a hypothetical scenario that could unfold if a backend is compromised in architecture without zero trust, where an attacker is able to deploy malicious content to the runner instances by creating jobs.

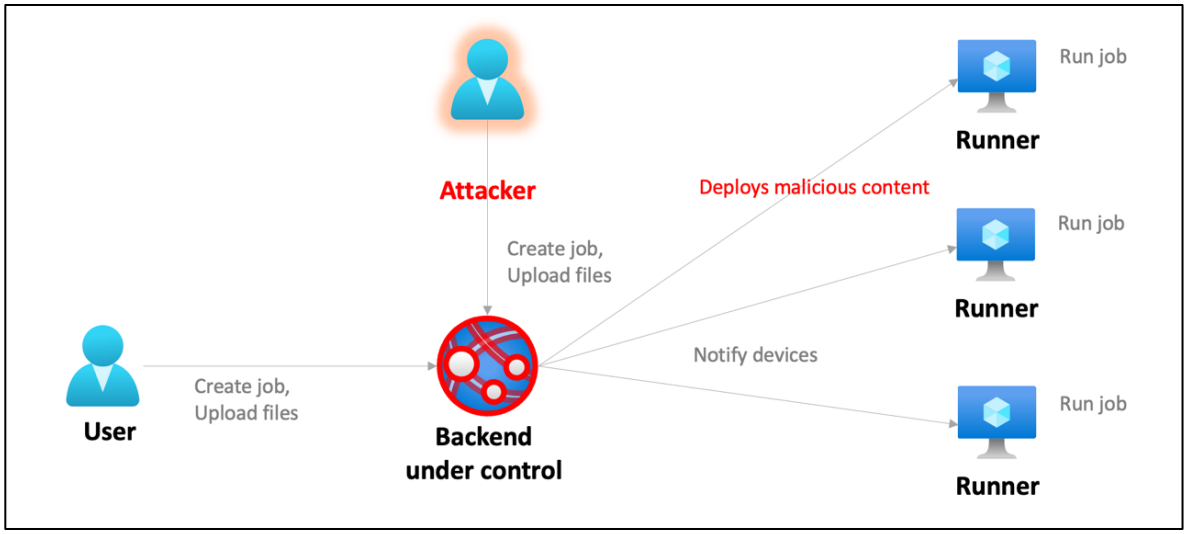

Figure 2. Compromised Backend System without Zero Trust

Figures 3 and 4 show the advantages of the zero-trust model, where every job is signed with the User's signature (private) key before being sent to the backend. Signed jobs are forwarded to the runner instances, which can then verify them using the public key. The jobs are only executed once the signature verification is successful. Figure 3 shows how zero trust works to avoid some of these potential risks.

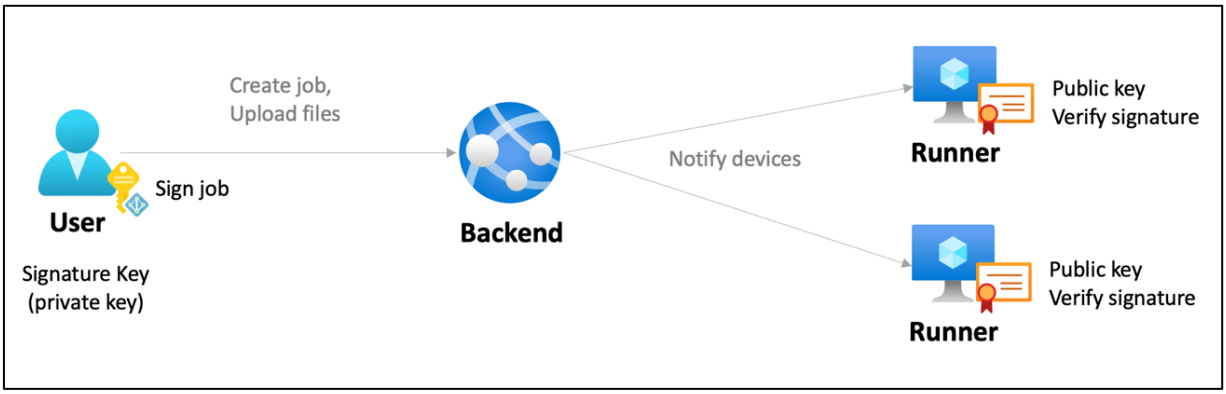

Figure 3. Job Signing and Signature Verification in Zero Trust Environment

Figure 4 represents a hypothetical scenario that could unfold if a backend is compromised in a zero-trust environment. In this scenario, the attacker would be unable to access the signature key and therefore would not be able to deploy malicious content or interact with the runner instances. In this scenario, the private-public key verification would fail, and the runner would discard the job or command. The private key cannot be derived from the public key.

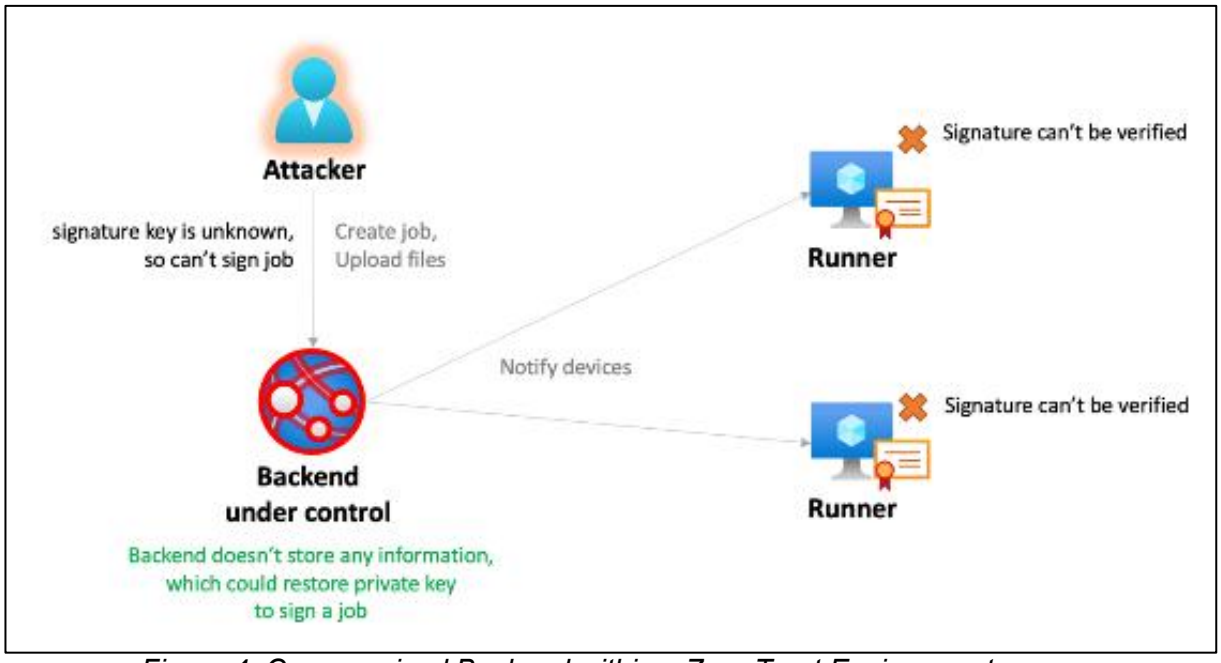

Figure 4. Compromised Backend within a Zero Trust Environment

2.5 Media Services Infrastructure

The media infrastructure consists of the following servers/protocols:

- Signaling server
- **Session Traversal Utilities for NAT (**STUN) and **Traversal Using Relay around NAT Secure** (TURN(S)) server

The signaling server uses secure WebSockets (full-duplex communication channels) to communicate with the End User and the agent at the same time and to share metadata and control information needed for setting up the peer-to-peer connection. After upgrading the HTTPS connection, the client and the server communicate over that same TCP connection and use TLS 1.2+ to secure the connection.

WebRTC is used to provide Real-Time Communication (RTC) to web browsers and remote support applications. All WebRTC sessions employ Secure Real-Time Transport Protocol (SRTP) encryption. WebRTC encrypts information (specifically data channels) using Datagram Transport Layer Security (DTLS) 1.2+ in case of UDP and TLS 1.2+ in case of TCP connections. All data sent over RTC data channel is secured using DTLS.

DTLS-SRTP is used as a secure encryption key exchange protocol and requires encryption keys to be transmitted from peer to peer on the media plane. The TURNS server uses TLS 1.2+ over TCP to relay data between the peers.

3 Technical Security Controls

GoTo employs technical security controls that are designed to safeguard the Service infrastructure and data residing therein.

3.1 Encryption

GoTo regularly reviews its encryption standards and may update the ciphers and/or technologies used in accordance with the assessed risk and market acceptance of new standards.

3.1.1 Encryption In Transit

GoTo uses TLS protocols and associated cipher suites to safeguard Customer Content while in transit.

End User endpoint and backend communications are encrypted via the OpenSSL library. Communications security controls are implemented on the TCP layer via TLS solutions.

Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are encrypted in transit with TLS 1.2 (ECDHE, DHE and RSA for key exchange, RSA for authentication, AES256 for data encryption with 384 or 256-bit SHA-2 HMAC algorithm) or TLS 1.3. Session keys are generated server-side and remain there to enable the connection with the End User.

GoTo servers authenticate themselves to clients using public key certificates signed by DigiCert or GlobalSign Global Root CA when connections are established to the LogMeIn Resolve website and between LogMeIn Resolve components. Server-to-server APIs are accessible only within GoTo's firewall-protected private network.

3.1.2 Encryption At Rest

At the server-side, Customer Content is encrypted at rest with AES256, using Galois Counter Mode (GCM) or similar modern block cipher modes of operation. On the client side, GoTo has configured the client application to store and secure credentials that enable connection to the Service using the operating system's cryptographic APIs. Customer Content is not stored on the client side.

3.2 End User Endpoint Protection

End User desktop apps and unattended End User apps are downloaded and installed via a digitally signed installer.

The installer uses an executable download that employs strong cryptographic measures to help protect the End User from inadvertently installing a Trojan or other malware posing as LogMeIn Resolve software.

LogMeIn Resolve's endpoint software is composed of several digitally signed executables and dynamically linked libraries. GoTo has implemented quality control and configuration management procedures during software development and deployment.

3.3 User Authentication

Agents and account administrators are identified by their email address and authenticated using a password. During authorized authentication, the password is encrypted in transit.

Authentication procedures are governed by the following policies:

- **Strong password requirements:** Passwords must be a minimum of 8 characters in length and must contain both letters and numbers. Passwords must meet these minimums when they are created or changed.
- **Two-Factor Authentication:** Optional two-factor authentication can be enabled at the account level. If enabled, two-factor authentication requires every User or End User within the account to authorize access via two separate methods.
- **Account lockout:** A User or End User account is put into a mandatory soft lockout state after five consecutive failed login attempts. The soft lockout prevents account access for five minutes. After the lockout period expires, the User or End User will be able to attempt to login to their account again.

3.4 In-Session Security

A User may end an unattended session at any time while it is in progress and can permanently revoke the agent's unattended support privileges.

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 provider data centers.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the LogMeIn Resolve 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). Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/control/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- Mongo DB, Inc. – database hosting provider for specific product features.

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. The customer is responsible for the configuration of the services they are using.

5 Logical Access Control

Logical access control procedures are in place to reduce the risk of unauthorized application access and data loss in corporate and production environments. Employees are granted access to specified GoTo systems, applications, networks and devices based on the principle of least privilege. User privileges are segregated based on functional role (role-based access control) and environment using segregation of duties controls, processes and/or procedures.

Production servers are only available using a virtual private network (VPN). Authentication through Self Service Unix (SSU) is required to access cloud-based production components.

5.1 Permission-Based Access Control

5.1.1 Attended Session

An essential part of LogMeIn Resolve's security is its permission-based access control model designed to protect access to the End User's system and data. During End User-attended live support sessions, the End User is prompted for permission before any screen sharing, remote control or transfer of files is initiated.

Once remote control and screen sharing have been authorized during an attended session, the End User can watch everything the agent does. The End User can take back control or terminate the session at any time.

5.1.2 Unattended Session

Unattended support requires the Unattended End User app to be installed on the End User's device. It can be set up in one of two ways: in-session setup (during an attended session) or using an out-of-session installer, both of which require End User approval.

In-Session Setup: Once the End User and agent have entered an attended session, the agent may request specific permission to install the Unattended End User app. The End User is prompted for approval and must give explicit authorization.

Out-of-Session Installer: After securely logging in to the LogMeIn Resolve website or desktop application, the agent can download an installer, which allows installation of the Unattended End User app on any Windows PC or Mac for which the agent has administrator access.

5.1.3 Role-Based Access Control

LogMeIn Resolve provides access to a variety of resources and services using a role-based access control system. The following roles are defined:

- **Account Administrator**: LogMeIn Resolve User with full administrator privileges to perform administrative functions pertaining to agents. Account administrators can create, modify and delete agent accounts and modify subscription data.
- **Agent**: LogMeIn Resolve User that can initiate LogMeIn Resolve sessions to provide technical assistance to End Users via remote view, remote control or camera share.
- **End User**: sensis and other individuals who use GoTo services (e.g., unauthenticated person requesting support from the agent). The End User can close sessions and must grant permissions for the agent to access their device.

6 Customer Content Retention Schedule

Unless otherwise required by applicable law, Customer Content shall automatically be deleted.

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

7 Terminology

Agent Web Console: A web application that runs on the Agent's PC, Mac, Android or iOS Tablet or Chromebook devices in any of the supported browsers (Chrome, Firefox, Safari) and connects to the LogMeIn Resolve Service. It enables the Agent to create and conduct LogMeIn Resolve sessions as well as various account management, service management and reporting functions.

Agent Desktop Console: A desktop application that runs on MacOS and Windows computers and connects to the LogMeIn Resolve Service and leverages the LogMeIn Resolve Agent Web Console technology, Qt and the Chromium web engine. It provides the same functionality as the Agent Web Console but in a native look and feel.

Attended Session: A support session where the End User is present during the session and can participate in it.

End User Desktop App: A desktop application that runs on the End User's computer (Windows or Mac) and connects to a LogMeIn Resolve Session through the LogMeIn Resolve Service. It provides remote control capability as well as other advanced functionalities and the ability to install Unattended App on the End User's computer.

End User Endpoint: A collective term referring to any End User endpoint: End User Web App, End User Desktop App, End User Mobile App, Unattended End User App.

End User Mobile App: A mobile application (Android and iOS) that runs on the End User's mobile/tablet device and can connect to a LogMeIn Resolve Session through the LogMeIn Resolve Service. It provides remote view (Android and iOS) and remote control (Android only) capabilities.

End User Web App: A web application that runs in any supported browser on the End User's computer/mobile device and connects to a LogMeIn Resolve Session through the LogMeIn Resolve Service. It can provide chat, remote view and camera share capabilities as well as the possibility to elevate the session anytime to remote control by downloading the End User Desktop App or installing the End User Mobile App.

Media Service: A fleet of load-balanced, globally distributed servers providing a variety of high-availability unicast and multicast communication services based on WebRTC protocols.

LogMeIn Resolve Sessions: Attended chat, remote view, remote control or camera share and unattended remote control.

LogMeIn Resolve Service: A fleet of load-balanced, globally distributed servers providing secure access for the Agent Web Console and End User Endpoints through encrypted web-socket connection and API calls.

Unattended End User App: An installable desktop application (Windows and iOS) that runs in the background on the End User's computer. It can download and execute an End User Desktop App to connect to an authorized Unattended Session.

Unattended Session: A support session where the End User is not present. The session is initiated and established by the Agent without End User involvement through an authorized Unattended End User App.

User: Individuals with sub-accounts within a customer account (e.g., employees, administrators).

LogMeIn Resolve Ticketing Services: A backend application which supports Helpdesk feature of LogMeIn Resolve. It also facilitates communication between MS Teams app and LogMeIn Resolve.

8 Revision History

Version	Month/Year	Description
Version 1.2	July 2024	Updated and published by Legal
Version 1.3	June 2025	Standardized the document to only include Product Specific sections.
Version 1.4	August 2025	Added verbiage to Compliance audits section under "Executive Summary" to include "Global CBPR and PRP certifications,"
Version 1.5	December 2025	Updated TLS versions from 1.2 to 1.2+. and updated verbiage in Section 2.3.1.