TECHNICAL AND ORGANIZATIONAL MEASURES FOR GOTO RESOLVE

SECURITY AND PRIVACY OPERATIONAL CONTROLS

Publication date: February 2022

1 Products and Services

This document highlights the technical and organizational measures (TOMs) to ensure privacy and security of the GoTo Resolve infrastructure and communications channels.

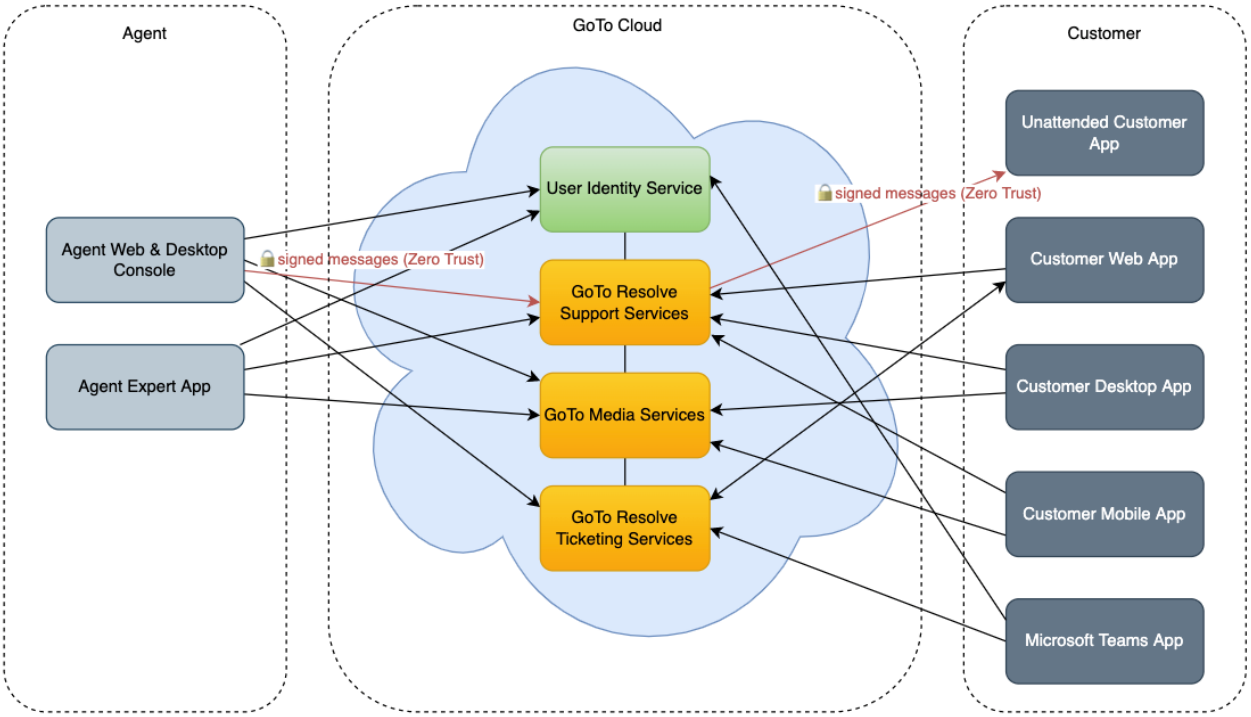
GoTo Resolve enables IT and support professionals to deliver remote support to computers, servers and mobile devices with remote view, remote control or camera share from a web-based or desktop agent console. GoTo Resolve employs robust data security measures to defend against both passive and active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

2 Product Architecture

GoTo 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 for optimal performance, reliability and scalability. GoTo Resolve leverages Amazon Web Services and Microsoft Azure cloud resources to provide scalable, highly available solution with no single point of failure. GoTo Resolve uses backup systems hosted in multiple regions to ensure continued operation of application processes in the event of a heavy load or system failure.

2.1 Communications Architecture

The GoTo Resolve communications architecture is summarized in the figure below.



Agent authentication utilizes the GoTo User Identity Service. Communication between participants in a GoTo Resolve session occurs via an overlay networking stack that logically sits on top of the conventional UDP and TCP/IP. This network is provided by the GoTo Resolve Service and Media Service hosted by Amazon Web Services and Microsoft Azure.
GoTo Resolve session participants (Agent Web Console, Agent Desktop Console and Customer Endpoints) communicate with GoTo Resolve Service and Media Service using outbound TCP connections on port 443 or UDP port 15000, depending on availability. Because GoTo Resolve is a web-based service, participants can be located nearly anywhere on the Internet — at a remote office, at home, at a business center or connected to another company's network.

2.2 Agent Desktop Console

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

3 GoTo Resolve Technical Controls

GoTo employs industry standard technical controls appropriate to the nature and scope of the Services (as defined in the Terms of Service) designed to safeguard the Service infrastructure and Customer Content residing therein. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

3.1 Authentication

GoTo Resolve Agents and Account Administrators are identified by their email address and authenticated using a password. During authorized authentication, the password is never transferred in an unencrypted state.

Authentication procedures are governed by the following policies:

Strong passwords: A strong password must be a minimum of 8 characters in length with sufficient complexity requirements (i.e., must contain both letters and numbers). Passwords are checked for strength when established or changed.

Two-Factor Authentication: As an additional security measure, optional two-factor authentication is available for every GoTo Resolve company account. If enabled, two-factor authentication requires every user to authorize access via two separate methods.

Account lockout: After five consecutive failed log in attempts, the user account is put into a mandatory soft lockout state. This means that the user account holder will not be able to log in for five minutes. After the lockout period expires, the user account holder will be able to attempt to log in to their account again.

3.2 Logical Access Control

Logical access control procedures are in place and designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments.

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.

Users authorized to access GoTo Resolve product components may include GoTo’s authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators or end-users of the product. Production servers are only available through the Operations virtual private network (VPN). Furthermore, the production servers are protected by Role-Based Access Control to prevent unauthorized access. Cloud-based production components are available through SSU (Self Service Unix) authentication.

3.2.1 Zero-Trust Access Control

In this model, the GoTo Resolve Services are not trusted, they serve only as a channel to forward Commands to Customer Endpoints. Authorization is based on industry standard cryptography. Each Agent has an asymmetric private-public key pair, where the private key is used to sign Commands, and is only known by the Agent (not known by GoTo Resolve Services or Customer Endpoint). The public key is deployed to each Customer Endpoint and used to verify the signature of each Command, received from the Agent. Therefore, the Customer Endpoints do not trust GoTo Resolve Services, but trust only the Agent.

All cryptography operations use industry standard and secure algorithms (for example EC-DSA, SHA-256/512, HMAC-SHA-256, AES-256-GCM, PBKDF2). These cryptosystems and ciphers are handled by the operating system or the OpenSSL library. In the case of the Web Console, the browser of the end user provides native functions to generate or manipulate data securely.

3.3 Permission-Based Access Control

3.3.1 Attended Session

An essential part of GoTo Resolve’s security is its permission-based access control model designed to protect access to the Customer’s computer and data. During customer-attended live support sessions, the customer is prompted for permission before initiation of any screen sharing, remote control or transfer of files.

Once remote control and screen sharing have been authorized during an Attended Session, the Customer can watch everything the Agent does. Further, the service is designed to allow the Customer to easily take back control or terminate the session at any time.

3.3.2 Unattended Session

Unattended support requires the Unattended Customer App to be installed on the Customer’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 Customer approval.

In-Session Setup: once the Customer and Agent have entered an Attended Session, the Agent may request extra permission to install the Unattended Customer App. The Customer is prompted for approval and must give explicit authorization.

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

3.3.3 In-Session Security

GoTo Resolve is not designed to override local security controls on the Customer's computer. Specifically, if the Customer returns to the machine while an Unattended Session is in progress, they may end the session at any time and can permanently revoke the Agent 's unattended support privileges.

3.4 Role-Based Access Control

GoTo Resolve provides access to a variety of resources and services using a role-based access control system that is enforced by the various service delivery components. The following roles are defined:

Account Administrator: GoTo 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: GoTo Resolve user. The agent can initiate GoTo Resolve Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

Customer: Unauthenticated person requesting support from the Agent. The Customer can close sessions and must grant permissions for the Agent to access their device.

3.5 Perimeter Defense and Intrusion Detection

GoTo employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls.

3.6 Data Segregation

GoTo leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's GoTo account. Only authenticated parties are granted access to relevant accounts.

3.7 Physical Security

Since the whole infrastructure is deployed to public cloud providers, physical security is not a concern for GoTo.

3.8 Data Backup, Disaster Recovery, Availability

GoTo's architecture is designed to perform replication in near-real-time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. In the event of a disaster or total site failure in any one of the multiple active locations, the remaining locations are designed to balance the application load. Disaster recovery related to these systems is tested periodically.

3.9 Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable 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.
Key points regarding encryption in GoTo Resolve include:

- GoTo Resolve Session data is protected with Transport Layer Security (TLS) 1.2 and 256-bit AES encryption in transit.
- Session keys are generated server-side by the agent and remain there to be able to connect the customer to the agent. The service is designed to ensure that these keys are never exposed or visible to the public.
- Encrypted media communication between the customer and the agent in GoTo Resolve occurs via a custom media service solution.
- Endpoints within the public GoTo Resolve infrastructure use TLS connections.

3.9.1 In-Transit Encryption

To further safeguard Customer Content (as the term is defined in the Terms of Service) while in transit, GoTo uses current TLS protocols and associated cipher suites. Customer Endpoint and backend communication are encrypted via the OpenSSL library. Communications security controls based on strong cryptography are implemented on the TCP layer via TLS standard solutions.

Strong authentication measures are utilized in order to help reduce the likelihood of would-be attackers masquerading as infrastructure servers or inserting themselves into the middle of support session communications.

To provide protection against eavesdropping, modification or replay attacks, IETF-standard TLS protocols are used to protect all communication between endpoints and our services. 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, AES-256 strong ciphers for data encryption with 384-bit SHA-2 HMAC algorithm).

In order to ensure appropriate compatibility and security balance, the GoTo Resolve service also supports inbound connections using most supported TLS cipher suites in TLS 1.2.

GoTo also advises that agents configure their browsers to use strong cryptography by default whenever possible, in order to increase technical safeguards on the agent's machine, and to always install the latest operating system and browser security patches.

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

3.9.2 TCP Layer Security

Internet Engineering Task Force (IETF)-standard TLS protocols are used to protect communication between public endpoints.

For their own protection, GoTo recommends that customers configure their browsers to use strong cryptography by default whenever possible, and to ensure that operating system and browser security patches are kept up to date.

3.9.3 Customer Endpoint Protection

Customer Desktop Apps and Unattended Customer Apps must be compatible with a wide variety of desktop environments. GoTo Resolve accomplishes this using an executable download that employs strong cryptographic measures.

The Customer Desktop Apps and Unattended Customer Apps are downloaded to the Customer PC as a digitally signed installer. This helps protect the Customer from inadvertently installing a Trojan or other malware posing as GoTo Resolve software. The endpoint softwares are composed of several digitally signed executables and dynamically linked libraries. GoTo follows appropriate quality control and configuration management procedures during development and deployment to enhance software safety.

3.10 Vulnerability Management

Ensuring the safety and protection of GoTo's customer's Content and systems is top priority. GoTo implements various security measures throughout the lifecycle of all its products. Security aspects are considered and taken into account during development and operations of GoTo Resolve.

Dynamic and static application vulnerability testing, as well as Security assessment testing activities for targeted environments, are also performed periodically. Relevant vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams and management.

3.10.1 Security Team

GoTo's Security team continuously monitors product development and operations in close collaboration with the product engineers in order to keep GoTo Resolve secure and prevent or reduce the likelihood for possible risks.

3.10.2 Internal and External Audits

GoTo's internal audit process includes regular security assessments at both the infrastructure and software level. Our internal audits are complemented by various independent external assessments to ensure that we maintain industry standards.

3.11 Logging and Alerting

GoTo collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

GoTo maintains a comprehensive set of organizational and administrative controls to protect the security and privacy posture of the GoTo Resolve product.

4.1 Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

GoTo complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certification(s) and external audit report(s):

- TRUSTe Enterprise Privacy & Data Governance Practices Certification to address operational privacy and data protection controls that are aligned with key privacy laws and recognized privacy frameworks. To learn more, please visit our blog post.
- International Organization for Standardization – ISO/IEC 27001:2013 Information Security Management System (ISMS) Certification
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Payment Card Industry Data Security Standard (PCI DSS) compliance for GoTo's eCommerce and payment environments
- Internal controls assessment as required under a Public Company Accounting Oversight Board (PCAOB) annual financial statements audit

4.3 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with GoTo's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating

procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including GoTo Resolve. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management, where appropriate. Employees can report security incidents via email, phone and/or ticket in accordance with the process documented on the GoTo intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

GoTo's application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis against running applications and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the GoTo Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

GoTo employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

GoTo takes the privacy of its Customers (which for the purposes of this Section are the subscribers to GoTo Services), and end-users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. GoTo Resolve is compliant with the applicable provisions of GDPR. For more information, please visit https://www.goto.com/company/trust/privacy.

5.2 CCPA

GoTo hereby represents and warrants that it is in compliance with the California Consumer Privacy Act (CCPA). For more information, please visit https://www.goto.com/company/trust/privacy.

5.3 Data Protection and Privacy Policy

GoTo is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs GoTo's processing of Personal Data.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of GoTo's technical and organizational measures. Additionally, to account for CCPA, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that GoTo will not sell our users' 'personal information.'

For visitors to our webpages, GoTo discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on the public website. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.4 Transfer

GoTo has a robust global data protection program which takes into account applicable laws and supports lawful international transfers under the following frameworks:

5.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the European Economic Area ("EEA") will be transferred in compliance with EU data-protection law. GoTo has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. GoTo offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope GoTo services as part of its global DPA. Execution of the SCCs helps ensure that GoTo customers can freely move data from the EEA to the rest of the world.

Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created the following FAQ designed to outline its supplemental measures utilized to support lawful transfers under Chapter 5 of the GDPR and address and guide any "case-by-case" analyses recommended by the European Court of Justice in conjunction with the SCCs.

5.4.2 APEC CBPR and PRP Certifications

GoTo has additionally obtained Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP") certifications. The APEC CBPR and PRP frameworks are the first data regulation frameworks approved for the transfer of personal data across APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance.

5.5 Return and Deletion of Customer Content

Customers may request the return or deletion of their Content through standardized interfaces at any time. If these interfaces are not available or GoTo is otherwise unable to complete the request, GoTo will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request. Upon expiration or termination of a Customer's account, Customer's Content shall automatically be deleted thirty (30) days after the effective date of the account expiration or termination. Upon written request, GoTo will certify to such Content deletion.

5.6 Sensitive Data

While GoTo aims to protect and safeguard all Customer Content, regulatory and contractual limitations require us to restrict the use of GoTo Resolve for certain types of information. Unless Customer has written permission from GoTo, the following data must not be uploaded or generated to GoTo Resolve:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) as identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as other relevant applicable laws and regulations.
- Information related to financial accounts and payment instruments, including – but not limited to – credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by GoTo to collect payment for the Service.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics

GoTo is continuously improving its websites and products using third-party web analytics tools which help GoTo understand how visitors use its websites, desktop tools, and mobile applications, as well as user preferences and problems. For further details please reference the Privacy Policy.

6 Third Parties

6.1 Use of Third Parties

As part of GoTo's internal assessment and processes related to vendor and third-party management, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by GoTo are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, GoTo reviews relevant third party's terms and conditions and either utilizes GoTo-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting GoTo

Customers can contact GoTo at https://support.goto.com for general inquiries or privacy@goto.com for privacy-related questions.

8 Appendix—Terminology

Agent: GoTo Resolve user, who creates GoTo Resolve Sessions to provide technical assistance to Customers via remote view, remote control or camera share.

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

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

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

Customer: person receiving technical support from the Agent via a GoTo Resolve Session.

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

Customer Endpoint: collective term referring to any customer endpoint: Customer Web App, Customer Desktop App, Customer Mobile App, Unattended Customer App.

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

Customer Web App: web application that runs in any supported browser on the Customer's computer/mobile device and connects to a GoTo Resolve Session through the GoTo 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 Customer Desktop App or installing the Customer 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.

GoTo Resolve Sessions: attended chat, remote view, remote control or camera share and unattended remote control.

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

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

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

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