Technical and Organizational Measures
GoTo Resolve

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for GoTo Resolve. Specifically, GoTo maintains robust global privacy and security programs and organizational, administrative and technical safeguards designed to: (i) ensure the confidentiality, integrity and availability of Customer Content; (ii) protect against threats and hazards to the security of Customer Content; (iii) protect against any loss, misuse, unauthorized access, disclosure, alteration and destruction of Customer Content; and (iv) maintain compliance with applicable law and regulations, including data protection and privacy laws. Such 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.
- **Data Centers:**[1] United States, Germany, Ireland, Sweden, Singapore, India, Netherlands, and United Kingdom data center locations to support redundancy.
- **Compliance Audits:** GoTo Resolve holds ISO/IEC 27001:2013, SOC 2 Type II, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy 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.
- **Security Assessments**: 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 employs a multi-tenant architecture and logically separates Customer accounts at the database level.
- **Perimeter Defense and Intrusion Detection**: Perimeter protection tools, techniques and services are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation.
- **Retention**:
  - GoTo 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). Recordings are deleted on a rolling basis after ninety (90) days.

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

Contents

Click the page numbers below to go to the relevant TOMs section

1 Product Introduction

GoTo Resolve enables IT and support 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. GoTo 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 either defined in the Terms of Service or explained in Section 23.

2 Technical Measures

GoTo's products are designed to provide solutions that are secure, reliable and private. The technical measures defined below describe how GoTo implements that design and applies it in practice for GoTo Resolve.

2.1 Safeguards

GoTo's implementation of safeguards, features and practices involves:

I. Building products that take security and privacy by design and default into account, and including additional layers of security in order to protect Customer Content;

II. Maintaining organizational controls that operationalize internal policies and procedures related to standards compliance, incident management, application security, personnel security and regular training programs; and

III. Ensuring privacy practices are in place to govern data handling and management in accordance with applicable law, including the GDPR, CCPA, LGPD, as well as and our own Data Processing Addendum (DPA) and applicable GoTo policies and commitments.

By building security safeguards into the product, we strive to protect GoTo Customer Content from threats and ensure security controls are appropriate to the nature and scope of the Services. GoTo's configurable security features can help administrators minimize threats and risks to systems and networks posed by individuals who use GoTo services.

3 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 to provide optimal performance, reliability and scalability. GoTo Resolve leverages Amazon Web Services and Microsoft Azure cloud resources in order to provide a scalable, highly available solution with no single point of failure. GoTo 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.

3.1 Communications Architecture

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

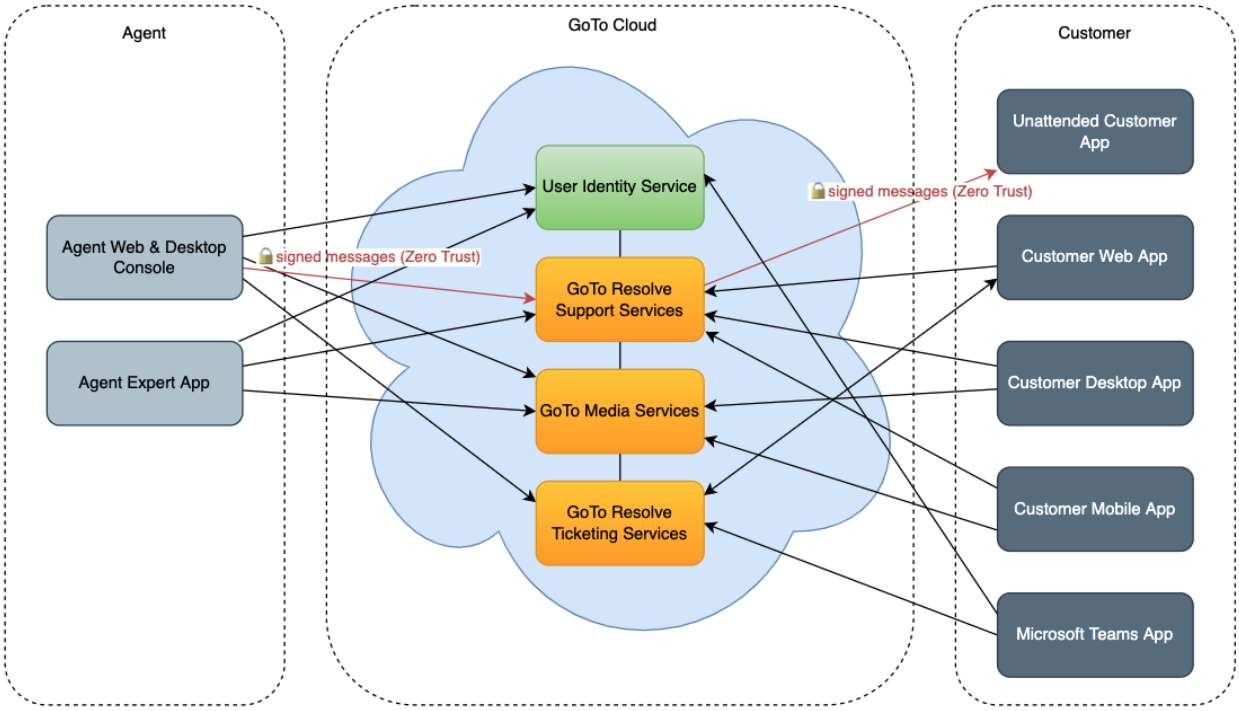

Figure 1: GoTo Resolve Communications Architecture

Agent authentication utilizes GoTo's proprietary User Identity Service. Communication between participants in a GoTo 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 GoTo Resolve and GoTo Media Services hosted on Amazon Web Services and Microsoft Azure.

GoTo 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 GoTo Resolve and the GoTo Media Service using outbound TCP connections on port 443 or UDP port 15000, based on availability. Because GoTo 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.

3.2 Agent Desktop Console

Agents can use Agent Web Console or an installable Agent Desktop Console to connect to GoTo 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.

3.3 Zero Trust Model

3.3.1 Architecture

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

When deploying the GoTo Resolve application on a remote device, the key creates a link between the agent and the device and uniquely identifies the agent. The key encrypts every command sent to the deployed remote device and shows who sends each command. Authorization of commands is based on asymmetric private-public key pairs, where the private key is used to sign commands and is only known by the agent (i.e., not known by GoTo Resolve Services or Customer endpoints). The public key is deployed to each End User endpoint and used to verify the signature of each command received from the agent. In this model, the End User endpoints do not “trust” GoTo Resolve Services – they trust the commands coming from an agent with an authorized key.

3.3.2 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 its 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 agent can access them from any browser. The encryption key is derived from the password and is different for each company and agent.

3.3.3 Cipher Suites

The zero trust architecture cryptography operations use the following 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.

3.4 Problem Definition

The following diagrams (Figures 2, 3 and 4 below) demonstrate how GoTo Resolve’s zero trust architecture is designed to protect individuals. 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.

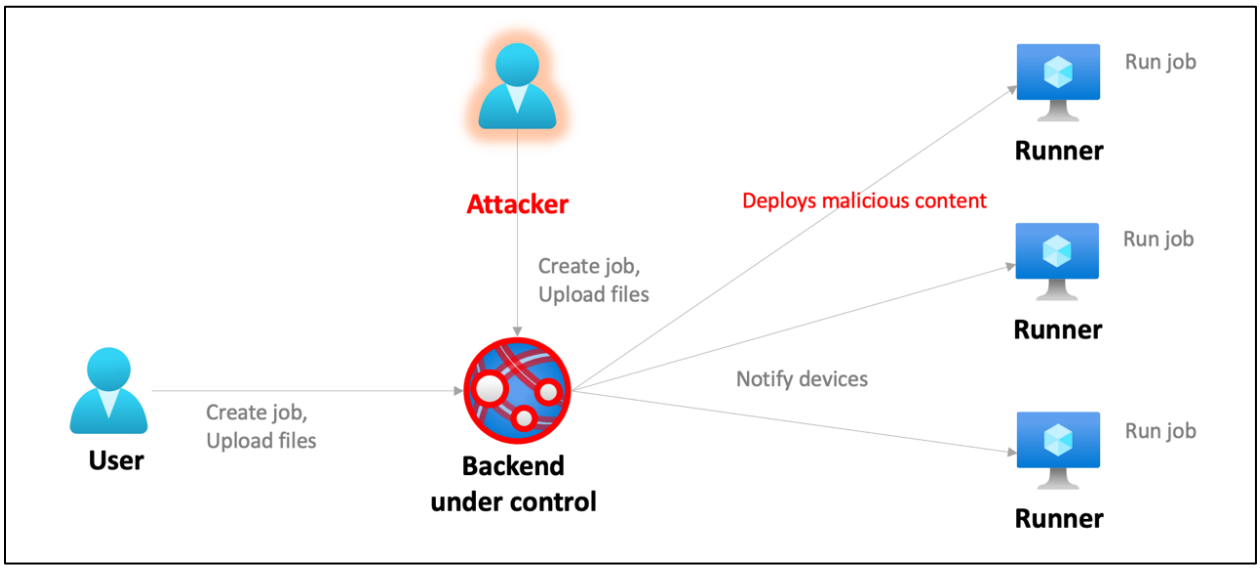

Figure 2. Compromised Backend System without Zero Trust

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 private-public key verification is successful. Figure 3 shows how zero trust works to avoid some of these potential risks.

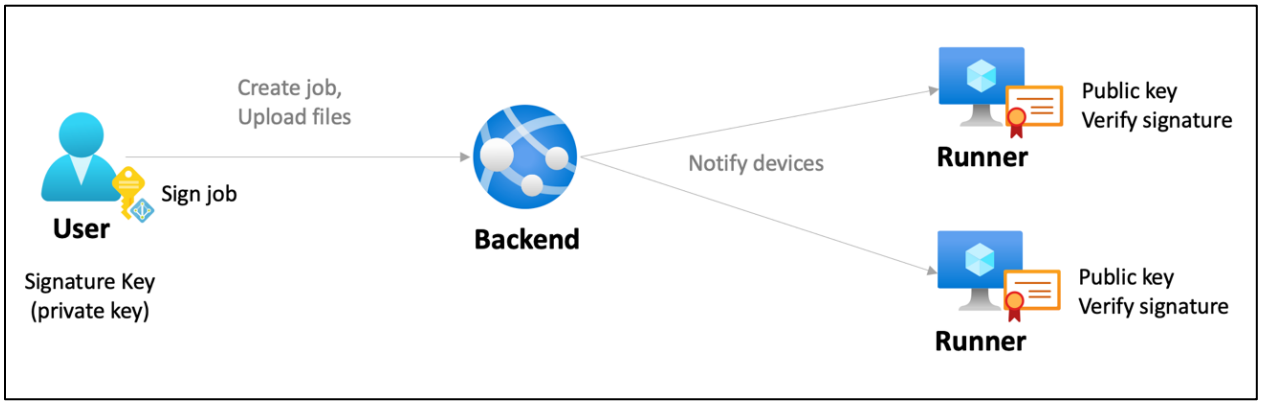

Figure 3. Job Signing and Signature Verification in Zero Trust Environment

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 signature key cannot be restored from the public key.

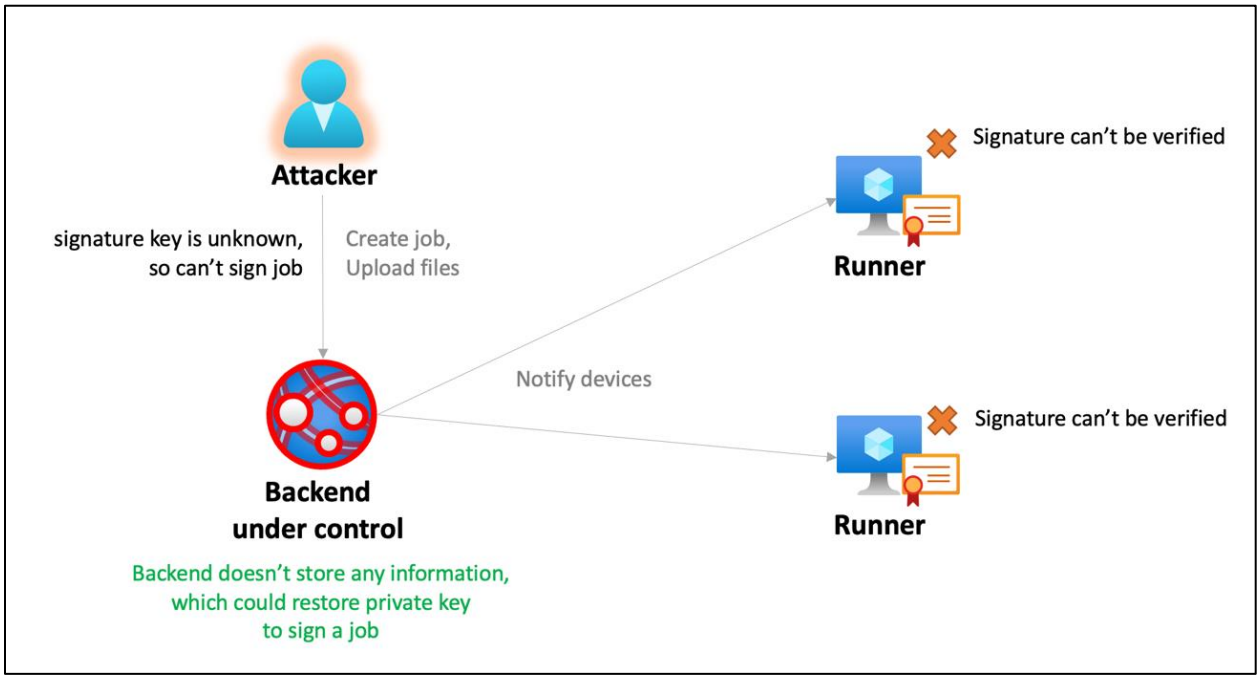

Figure 4. Compromised Backend within a Zero Trust Environment

3.5 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 RTCDataChannel 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.

4 Technical Security Controls

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

4.1 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.

4.1.1 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 GoTo Resolve website and between GoTo Resolve components. Server-to-server APIs are accessible only within GoTo's firewall-protected private network.

4.1.2 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. At 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 client side.

4.2 TCP Layer Security

TLS protocols are used to protect communication between public endpoints.

4.3 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 GoTo Resolve software.

GoTo 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.

4.4 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.

4.5 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.

5 Security Program Updates

GoTo reviews and updates its security program and engages independent third parties to assess its relevant security controls at least annually to ensure it evolves against the current threat landscape and to ensure compliance with relevant frameworks, industry standards, Customer commitments and, as applicable, changes in laws and regulations pertaining to the security of GoTo data.

6 Data Backup, Disaster Recovery and Availability

GoTo's architecture is designed to perform replication in near real time to geographically diverse locations. Databases are backed up using snapshots and point in-time recovery. 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.

7 Data Centers

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-passive data centers; or
b) cloud hosting provider data centers.

Upon account creation, GoTo Resolve 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, Ireland, Sweden and the Netherlands
- **Global:** United States, Germany, Singapore, India, United Kingdom and the Netherlands.

All data centers include monitoring of environmental conditions and have around-the-clock physical security measures addressed below.

7.1 Data Center Physical Security

GoTo contracts with data centers to provide physical security and environmental controls for systems and servers that contain Customer Content. These controls include the following:

- Video surveillance and recording
- Heating, ventilation and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters as required by the geography and location of the relevant data center
- Scheduled maintenance and validation of all critical security and environmental controls

GoTo limits physical access to production data centers to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by GoTo's technical operations team. All physical access to data centers and server rooms is logged and GoTo management reviews logs on at least a quarterly basis. Additionally, data center physical access authorization is removed promptly upon role change (where such access is no longer required) or upon termination of any

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

previously authorized personnel. Multi-factor access (e.g., biometrics, badge and keypad) is required for highly sensitive areas, which include data centers.

8 Standards Compliance

GoTo regularly assesses its compliance with applicable legal, security, financial, data privacy and regulatory requirements. GoTo's privacy and security programs have met rigorous and internationally recognized standards, been assessed in accordance with comprehensive external audit standards and achieved key certifications, including:

- **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, visit our blog post.
- **TRUSTe APEC CBPR and PRP Certifications** for the transfer of Customer Content between APEC-member countries obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance. To learn more about our APEC certifications, click here.
- 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)**.
- **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.
  (a)

9 Application Security

GoTo's application security program follows the Microsoft Security Development Lifecycle (SDL) to secure product code. The Microsoft SDL program includes manual code reviews, threat modeling, static code analysis, dynamic analysis and system hardening. GoTo teams also periodically perform dynamic and static application vulnerability testing and penetration testing activities for targeted environments.

10 Logging, Monitoring and Alerting

GoTo maintains policies and procedures around logging, monitoring and alerting, which set out the principles and controls that are implemented to bolster our ability to detect suspicious activity and respond to them on a timely basis. GoTo collects identified anomalous or suspicious traffic in relevant security logs in applicable production systems.

11 Endpoint Detection and Response

Endpoint Detection and Response software with audit logging is deployed on all GoTo servers to minimize disruption or impact on the performance of the Service. Security investigations will be initiated in accordance with our incident response procedures if suspicious activity is detected, as appropriate and necessary. See section 17 for more information on GoTo's Security Operations Center and incident response procedures.

12 Threat Management

GoTo's Cyber Security Incident Response Team ("CSIRT") is comprised of multiple teams and is responsible for cyber threat protection. Specifically, the Cyber Threat Intelligence team within the CSIRT collects, vets and disseminates information as it pertains to current and emerging threats. GoTo stays current with threat intelligence and mitigation through review of open and closed sources and participation in sharing groups and industry memberships (IT-ISAC, FIRST.org, etc.).

13 Security and Vulnerability Scanning and Patch Management

GoTo maintains a formal patch management program and, on at least a quarterly basis, performs patch management activities on all relevant systems, devices, firmware, operating systems, applications and other software that process Customer Content. GoTo assesses and scans for system-level, internal and external host/network ("Systems") vulnerabilities, on no less than a monthly basis, as well as after any material change to such Systems and remediates relevant discovered vulnerabilities in accordance with documented policies that prioritize remediation based on risk.

14 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.

14.1 Permission-Based Access Control

14.1.1 Attended Session

An essential part of GoTo 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.

14.1.2 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 GoTo 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.

14.1.3 Role-Based Access Control

GoTo Resolve provides access to a variety of resources and services using a role-based access control system. 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 that can initiate GoTo 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.

15 Data Segregation

GoTo has implemented controls to prevent Users from seeing the data of other Users. For instance, GoTo leverages a multi-tenant architecture, logically separated at the database level,

based on a User's or organization's GoTo account. Parties must be authenticated to gain access to an account.

16 Perimeter Defense and Intrusion Detection

GoTo uses perimeter protection tools, techniques and services to protect against unauthorized network traffic entering GoTo's product infrastructure. These include, but are not limited to:

- Intrusion detection systems that monitor systems, services, networks and applications for unauthorized access
- Critical system and configuration file monitoring
- Web application firewall (WAF) and application-layer DDoS prevention services that proxy GoTo traffic
- AWS security groups on GoTo web servers that filter inbound and outbound connections, including internal connections between GoTo systems
- Internal network segmentation.

17 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed incident response procedures, including a documented Incident Response Plan.

GoTo's Incident Response Plan is aligned with GoTo's critical communication processes, policies and standard operating procedures. It is designed to manage, identify and resolve relevant suspected or identified security events across its systems and services, including GoTo Resolve. The Incident Response Plan sets out mechanisms for employees to report suspected security events and escalation paths to follow when appropriate. Suspected events are documented and escalated as appropriate via standardized event tickets and triaged based upon criticality.

18 Deletion and Return of Content

Deletion and/or Return: Customers may request return and/or deletion of their Customer Content by submitting a request using GoTo's Individual Rights Management Portal ("IRM"), via support.goto.com, or by e-mailing privacy@goto.com. Requests shall be processed within thirty (30) days of receipt by GoTo, however, in the unlikely event we need more time, we will provide notice as soon as possible of any anticipated delayed and revised completion deadline.

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,

[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.

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.

19 Organizational Controls

19.1 Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures that are periodically reviewed and updated as necessary to support GoTo's security objectives, changes in applicable law, industry standards and compliance efforts.

19.2 Change Management

GoTo maintains a suitable change management process and changes to GoTo Systems are assessed, tested and approved before implementation to reduce the risk of disruption to GoTo services.

19.3 Security Awareness and Training Programs

GoTo's privacy and security awareness program involves training employees about the importance of handling Personal Data and confidential information ethically, responsibly, in compliance with applicable law, and with due care. Newly hired employees, contractors and interns are informed of security policies and the GoTo Code of Conduct and Business Ethics during onboarding. GoTo Employees complete privacy and security awareness training at least annually. Awareness activities take place throughout the year and can include campaigns for Data Privacy Day, Cybersecurity Awareness Month, webinars with the Chief Information Security Officer and a security champions program.

Where appropriate, employees may also be required to complete role-specific trainings. Additionally, all GoTo employees, contractors and subsidiaries must review and adhere to GoTo's policies related to security and data protection.

20 Privacy Practices

GoTo takes the privacy of our Customers, Users and End Users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

20.1 Privacy Program

GoTo maintains a comprehensive privacy program that involves coordination from multiple functions within the company, including Privacy, Security, Governance, Risk and Compliance (GRC), Legal, Product, Engineering and Marketing. This privacy program is centered around compliance efforts and involves the implementation and maintenance of internal and external policies, standards and addenda to govern the company's practices.

20.2 Regulatory Compliance

20.2.1 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law regarding data protection and privacy for individuals within the EU. GoTo maintains a comprehensive GDPR compliance program and to the extent GoTo engages in processing of Personal Data subject to the GDPR on behalf of the Customer, we will do so in accordance with the applicable requirements of the GDPR. For more information, visit https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively referred to as "CCPA") grants Californians additional rights and protections regarding how businesses may use their personal information. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the CCPA on behalf of the Customer, we will do so in accordance with the applicable requirements of the CCPA. For more information about our compliance with the CCPA, see GoTo's Privacy Policy and Supplemental California Consumer Privacy Act Disclosures.

20.2.3 LGPD

The Brazilian Data Protection Law (LGPD) regulates the processing of Personal Data in Brazil and/or of individuals located in Brazil at the time of collection. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the LGPD on behalf of the Customer, we will do so in accordance with the applicable requirements of the LGPD. For more information, visit https://www.goto.com/company/trust/privacy.

20.3 Data Processing Addendum

GoTo offers a global Data Processing Addendum (DPA), available in English and German. This DPA meets the requirements for GDPR, CCPA, LGPD and other applicable regulations and governs GoTo's processing of Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including:

(a) data processing details and sub-processor disclosures as required under Article 28;
(b) revised (2021) Standard Contractual Clauses (a.k.a. the EU Model Clauses); and
(c) GoTo's product-specific technical and organizational measures.

Additionally, to account for CCPA requirements, our global DPA includes:

(a) revised definitions mapped to the CCPA;
(b) access and deletion rights; and

(c) warranties that GoTo will not sell our Customer's, Users' and End Users' personal information.

Our global DPA also includes provisions to:

(a) address GoTo's compliance with the LGPD;
(b) support lawful transfers of Personal Data to/from Brazil; and
(c) ensure that our Users enjoy the same privacy benefits as our other global Users.

20.4 Transfer Frameworks

GoTo supports lawful international data transfers under the following frameworks:

20.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), sometimes referred to as EU Model Clauses, are standardized contractual terms, recognized and adopted by the European Commission, to ensure that any Personal Data leaving the European Economic Area (EEA) will be transferred in compliance with EU data protection law. The SCCs, revised and issued in 2021, are incorporated in GoTo's global DPA to enable GoTo Customers to transfer data out of the EEA in compliance with the GDPR.

20.4.2 Data Privacy Framework

The EU-U.S. and Swiss-U.S. Data Privacy Frameworks (DPF) and the UK Extension to the EU-U.S. DPF are voluntary frameworks that, respectively, provide mechanisms for companies to transfer personal data from the EU, Switzerland and the UK to the U.S. in compliance with the data protection regulations in these jurisdictions. GoTo complies with each of these frameworks regarding the collection, use, and retention of personal data from the EU, Switzerland, and the UK, respectively. To learn more about the DPF, and to view GoTo's certification, please visit the DPF website.

20.4.3 APEC CBPR and PRP Certifications

GoTo has 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 between APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party data protection compliance vendor.

20.4.4 Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created an FAQ designed to outline the supplemental measures implemented 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 use of the SCCs.

20.5 Data Requests

GoTo maintains comprehensive processes to facilitate receiving data protection and security-related requests, including the IRM portal, Privacy email address (privacy@goto.com) and Customer support at https://support.goto.com.

20.6 Sub-Processor and Data Center Disclosures

GoTo publishes Sub-Processor Disclosures on its Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). These disclosures show the names, locations and processing purposes of data hosting providers and other third parties that process Customer Content as a part of providing the Service to GoTo Customers.

20.7 Sensitive Data Processing Restrictions

Unless expressly requested by GoTo or Customer has otherwise received written permission from GoTo, the following types of sensitive data must not be uploaded to GoTo Resolve or otherwise provided to GoTo:

- 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.

20.8 Compliance in Regulated Environments

Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of GoTo Resolve to support devices in regulated environments.

21 Security and Privacy Third-Party Controls

Prior to engaging third-party vendors that process Customer Content or confidential, sensitive, or employee data, GoTo reviews and analyzes the vendor's security and privacy practices using the appropriate Procurement channels. As appropriate, GoTo may obtain and evaluate compliance documentation or reports from vendors periodically to ensure their control environment and standards continue to be sufficient.

GoTo enters into written agreements with all third-party vendors and either utilizes GoTo-approved procurement templates or negotiates such third parties' standard terms and conditions to meet GoTo-accepted privacy and security standards, where deemed necessary. The Finance, Legal, Privacy and Security teams are involved in the vendor review process and verify that

vendors meet specific mandatory data handling and contractual requirements, as necessary and/or appropriate. GoTo's third party risk policies govern privacy and security requirements of vendors on the basis of type and duration of data processing and level of access. Where appropriate (e.g., where Customer Content is processed or stored), agreements with vendors include "compliance with applicable law" requirements, a DPA or similar document that addresses topics such as GDPR, CCPA, LGPD and use and sale restrictions, as appropriate. For instance, GoTo's Supplier DPA has restrictions around data "selling" as defined under the CCPA. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors.

22 Contacting GoTo

Customers can contact GoTo at support.goto.com for general inquiries. For questions or requests related to Personal Data or privacy, please visit our IRM portal or send an email to privacy@goto.com.

23 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 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: A 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. 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 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 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 GoTo Resolve Session through the GoTo 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 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 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.

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 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).

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.