Technical and Organizational Measures
GoTo Connect

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoTo Connect. 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:** 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.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA/CPRA and LGPD.
- **Penetration Testing**: In addition to in-house testing, GoTo contracts with external firms to conduct 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**:
  - GoTo Connect 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.
  - Content will automatically be deleted thirty (30) days after expiration of a Customer's then-final subscription term. During the subscription term, call recordings and call reports are retained for thirteen (13) months from the date they are created.

Contents

1 Product Introduction

GoTo Connect is an all-in-one Unified Communications as a Service (UCaaS) solution for enterprises and businesses. It combines cloud-based Voice-over-Internet Protocol (VoIP) phone systems with the web, audio and video conferencing services of GoTo Meeting* in one simple, reliable and flexible collaboration solution (the "Service").

The Service includes the following features and offerings:

- GoTo Connect's cloud-based phone service is designed to replace traditional, on-premises Private Branch Exchange (PBX) phone equipment. The PBX administration portal allows Users with administrator permissions to view and make universal changes to system settings from any device with an internet connection.
- Public Switched Telephone Network (PSTN) replacement services (including phone numbers and minutes) are provided through partnerships with some of the world's leading telecommunications providers.
- Visual dial plan editor is a call flow editing tool that can direct calls to specific voicemail boxes, auto attendants or ring groups or set up wait times.
- GoTo Connect business continuity (formerly known as 'JBC') is an optional, premium service and hardware offering installed on the premises of an individual using the Service ("User") that provides local phone service via an independent third-party whose services are separately procured by a User in the event of a network outage.

*For more information about the GoTo Meeting Service and its technical and organizational measures, consult the GoTo Meeting TOMs available at https://www.goto.com/company/trust/resource-center.

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

2 Product Architecture

The diagram below (Figure 1) shows the GoTo Connect network architecture.

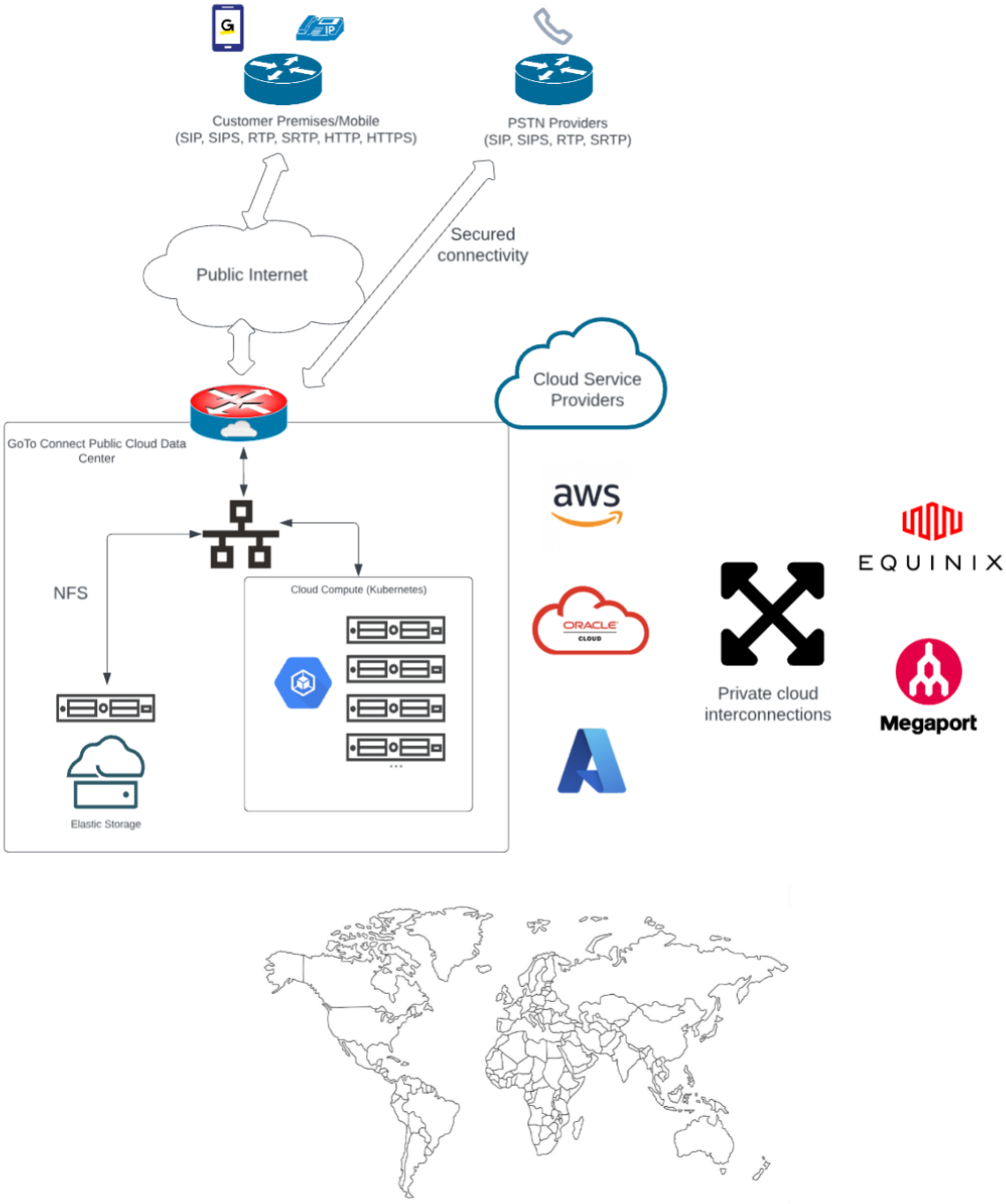

Figure 1: GoTo Connect Architecture

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.

3.2 Encryption In Transit

The Service is designed with end-to-end data security measures to ensure that communication data is not exposed in unencrypted form during transmission across public or private networks or to communication servers.

Internet Engineering Task Force (IETF) standard TLS protocols are used to protect communication between endpoints. All network traffic flowing in and out of data centers that hold GoTo data, including all Customer Content, is encrypted in transit.

When TLS connections are established, GoTo servers authenticate themselves to clients (i.e., workstations or devices), using public key certificates. When supported by User equipment, TLS is used to secure the traffic between User equipment and the Service's infrastructure. TLS also secures the transfer of provisioning information, which includes the physical phone's credentials, from the Service's infrastructure to the phones. Media is transmitted using Secure Real-time Transport Protocol (SRTP) while audio traffic is secured using shared keys transmitted over Session Initiation Protocol Secure (SIPS).

3.3 Encryption At Rest

Voicemail recordings, voicemail greetings, and call recordings are encrypted at rest using 256-bit AES encryption when stored in GoTo's cloud storage.

3.4 User Authentication

GoTo Connect provisions User access using GoTo's proprietary identity management platform, uses Security Assertion Markup Language (SAML) to offer single sign-on (SSO), and integrates directly with the GoTo platform via API. The identity management platform supports administrative controls related to User authentication including configuring password policies, forcing password resets and requiring utilization of SAML for login.

Service PBX administrators (super administrators) can grant or deny specific permissions in the PBX administration portal. These permissions include the ability to configure the PBX, edit E911 addresses/locations, view reports, view and pay invoices and update and delete settings and accounts for:

- Users;
- User Groups;
- Extensions;
- Devices;
- Hardware;
- Sites; and
- Phone Numbers (deletion and creation of phone numbers is managed through the phone number ordering process).

For more details on group permissions in PBX administration, visit the Getting Started Guide for Admins.

4 Data Backup, Disaster Recovery and Availability

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using cloud hosting data centers. Specifically, the Service uses a containerized microservice platform that allows for rapid deployment and scaling of services and provides redundancy, call failover, scalability, and high availability to Users. This full mesh design allows for microservices to self-discover and self-recover in the event of an outage at any specific location or in the event of an issue localized geographically on the public internet.

Goto product infrastructure is fully deployed in the public clouds, leveraging AWS, Oracle Cloud Infrastructure (OCI) and Microsoft Azure across multiple regions worldwide. Critical services are architected using cloud-native clustering and high-availability features, such as availability zones and multi-regions replication, to maximize redundancy and resilience. Interconnectivity between regions and public clouds takes place over private cloud networking, with dynamic failover mechanisms to ensure continuity if primary connections are interrupted.

Each cloud region maintains independent connectivity to the public Internet, enabling reliable external communication. All production environments are deployed in such a manner that internal applications can securely access required services across all regions, regardless of their deployment location. No workloads are hosted on-premises; all compute resources are provisioned and managed within the public cloud provider environments.

Connectivity to the Public Switched Telephone Network (PSTN) is established through redundant, secure and geographically distributed SIP trunks via the public Internet toward multiple telephony partners.

To ensure high availability and continuity of service, the cloud infrastructure operates with a minimum of N+1 capacity model, meaning the solution is designed to tolerate the loss of at least one entire cloud region's worth of capacity without impacting uptime. Client traffic can be automatically redirected to other operational regions to maintain service availability without any impact on service.

5 Data Centers and Hosting Workloads

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using cloud hosting data centers.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the GoTo Connect Sub-Processor Disclosure available in the Product Resources section of the GoTo Trust and Privacy Center.

5.1 Cloud hosted Workloads

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

- https://aws.amazon.com/compliance/data-center/controls/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

Other than physical security, all cloud providers operate with some form of a shared responsibility model where the cloud provider is responsible for protecting the infrastructure (hardware, software, networking) that runs all the services the provider offers. The customer is responsible for the configuration of the services they are using.

6 Customer Content Retention Schedule

Unless otherwise required by applicable law Customer Content shall automatically be deleted thirty (30) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription. During the Customer's subscription term, call recordings and call reports are deleted on a rolling basis and retained for thirteen (13) months from the date they are created. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

7 Revision History

Version	Month/Year	Description
Version 3.2	July 2024	Updated and published by Legal
Version 3.3	June 2025	Standardized the document to include Product Specific sections only.