Technical and Organizational Measures
GoTo Contact Center

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoTo Contact Center. 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:** GoTo Contact Center holds 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/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 Contact 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 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 Contact is a Contact Center as a Service (CCaaS) solution built on top of the GoTo Connect platform that enables organizations to improve the outcomes of their customer and prospect communications over multiple communication channels, such as voice, text, web chat, and social media. This solution is good for organizations of all sizes but is particularly useful in small to medium sized businesses.

This document describes the Technical and Organizational Measures (TOMs) of GoTo Contact and some of GoTo Connect, on which GoTo Contact is built.

The following are features and offerings within the GoTo Contact service (the Service):

- GoTo Contact is designed to help users manage call queues and incoming customer calls through interactive voice responses, automatic call distribution and customer relationship management integrations.
- Chat Queues allow people to send a message to a queue and have that message delivered to a company representative (rep) as if the external number were the rep's direct number. Chat queue messages can be sent through different communication channels: Text, Web Chat, Facebook, and other social media channels.
- Other channels can aid customer communication, such as voice to video and chat to video.
- GoTo Contact analytics provides real-time and historical reporting enabling supervisors and managers to improve customer interactions, optimize customer experience, optimize rep time to service customers and to coach representatives on their communication skills.

2 Product Architecture

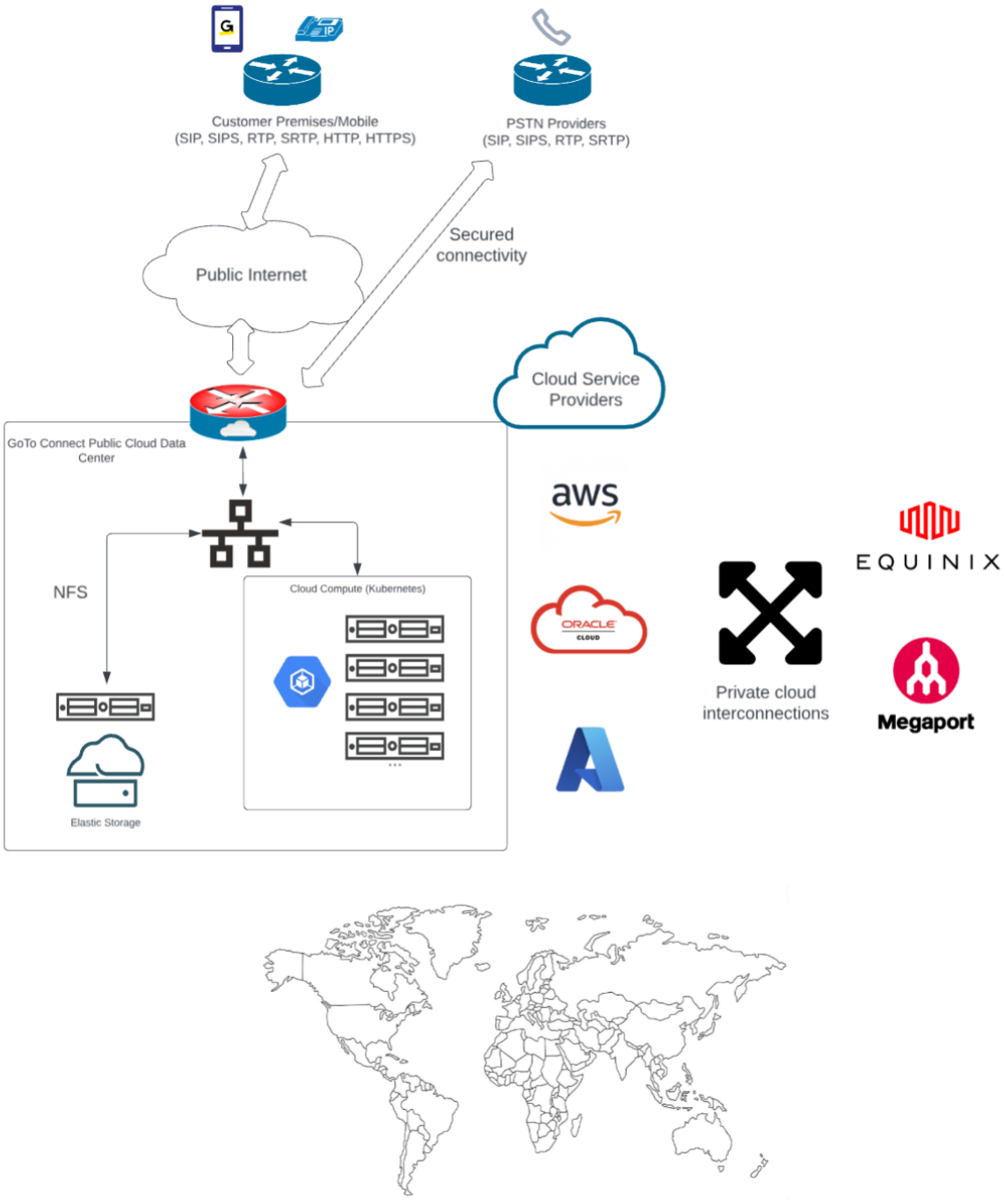

Figure 1- GoTo contact Infrastructure

3 GoTo Contact Technical Security Controls

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

3.1 Malware Protection

Anomalous activity alerting capabilities are actively deployed and monitored on the Service. Alerts indicating potential malicious activity are sent to appropriate response teams for resolution or mitigation.

3.2 Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

3.2.1 In-Transit Encryption

The Service provides end-to-end data security measures. The Service is designed to ensure that communication data is not exposed in unencrypted form with communication servers or during transmission across public or private networks. Internet Engineering Task Force (IETF) standard Transport Layer Security (version 1.2 or higher) protocols are used to protect communication between endpoints. All network traffic flowing in and out of GoTo datacenters, including all Customer Content, is encrypted in transit. See the Terms of Service for more information.

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.

When TLS connections are established GoTo servers authenticate themselves to clients using public key certificates. TLS is also supported for signaling between physical phones and the Service infrastructure to secure the traffic and communication when supported by Customer equipment. Media is transmitted using Secure Real-time Transport Protocol (sRTP) utilizing shared keys transmitted over Session Initiation Protocol Secure (SIPS) to secure audio traffic. Provisioning information containing the physical phones credentials from the Service's infrastructure to the phones are also secured using TLS.

3.2.2 At-Rest Encryption

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

3.3 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing

results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

4 Data Backup, Disaster Recovery and Availability

In order to provide redundancy, call failover, scalability, and high availability, the Service uses a containerized microservice mesh which allows for rapid deployment and scaling of services to satisfy the needs of GoTo's customers. This full-mesh design allows for microservices to self-discover and self-recover in the event of an outage at any specific datacenter or in the event of an issue localized geographically on the public Internet. Services are designed to fail-over between datacenters automatically.

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 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 GoTo Contact Center 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 and OCI). Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls/
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

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.

6 Logical Access Control

Users authorized to access GoTo Contact Center product components may include GoTo's authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. On-premises production servers are only available from jump hosts or through the Operations virtual private network (VPN). Cloud-based production components are available through SSU (Self Service Unix) authentication.

The GoTo Contact Integrated Service offering utilizes GoTo's proprietary identity management platform for customer provisioning, offers Single sign-on (SSO) using Security Assertion Markup Language (SAML), and integrates directly with the platform via API. This permits robust administrative controls, including allowing Customer account administrators to configure password policies, force password resets, and require utilization of SAML for login.

Service PBX administrators (Super Administrators) can grant or deny specific permissions in the PBX Administration Portal and grant GoTo Contact Admin role permissions to users of the GoTo. These group permissions include the ability to configure the PBX, edit E911 addresses/locations, view reports and pay invoices, as well as create, update, and delete settings and accounts for:

- Users;

- User Groups ;

- Extensions ;

- Devices;

- Hardware.

- Sites; and

- Phone Numbers (delete and create managed through number ordering).

User level permissions are not directly configured as they are derived from the user, device, and line relationships.

For more details on group permissions, please reference the GoTo Connect Administrator PBX Guide.

7 Customer Content Retention Schedule

Session recordings will be deleted on an ongoing 90-day rolling basis.[1] Additionally, unless otherwise required by applicable law, Customer Content shall automatically be deleted: 1) for paid accounts, ninety (90) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription; or 2) for free accounts, after one (1) year of inactivity (e.g., no logins).

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

8 Revision History

Version	Month/Year	Description
Version 1.3	July 2024	Updated and published by Legal
Version 1.4	August 2025	Standardized the document to include only Product Specific sections.

[1] 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.