TECHNICAL AND ORGANIZATIONAL MEASURES FOR CENTRAL/PRO

SECURITY AND PRIVACY OPERATIONAL CONTROLS

Publication date: February 2022

1 Products and Services

This Technical and Organizational (TOMs) document covers the security and privacy controls for Central/Pro.

Central is a web-based management console that helps IT professionals access, manage and monitor remote computers, deploy software updates and patches, automate IT tasks and run hundreds of versions of antivirus software. Central is offered as a premium service with multiple pricing tiers based on the number of computers supported and features desired.

Pro is a remote access service that provides secure access to a remote computer or other internet-enabled device from any other internet-connected computer, as well as most smartphones and tablets. Once a Pro host is installed on a device, the service is designed to enable a user to quickly and easily access that device's desktop, files, applications and network resources remotely from the user's other internet-enabled devices. Pro can be rapidly deployed and installed without the need for IT expertise.

2 Product Architecture

Central/Pro is a SaaS-based application featuring a multi-tier architecture hosted in secure, reliable, geographically distributed data centers in geographically diverse locations. Security measures at all levels, from the physical layer through the application layer, provide defense in depth.

The Central/Pro application is composed of three key components that enable a successful remote access session: the client, the host and the GoTo gateway. The Central/Pro host is designed to maintain a constant Transport Layer Security (TLS)-secured connection with a GoTo gateway server located in one of the GoTo datacenters. After it establishes a secure connection to Central/Pro, the client is authenticated and authorized by the host to access the computer, and the remote access session begins. The gateway server mediates the encrypted traffic between the two entities but does not require that the host implicitly trust the client. The Central/Pro gateway allows either the client or host (or both) to be firewalled, relieving users of the need to configure firewalls.

GoTo's proprietary key exchange forwarding protocol is designed to provide security against interception or eavesdropping on our own infrastructure. Specifically, the connection between the client and the host is facilitated by the gateway in order to ensure that the client can connect to the host independently of the network setup.

With the host already having established a TLS connection to the gateway, the gateway forwards the client's TLS key exchange to the host via a proprietary key renegotiation request.

This results in the client and the host exchanging TLS keys without the gateway learning the key.

To learn more about Central/Pro architecture and security features, please see the Security Whitepaper.

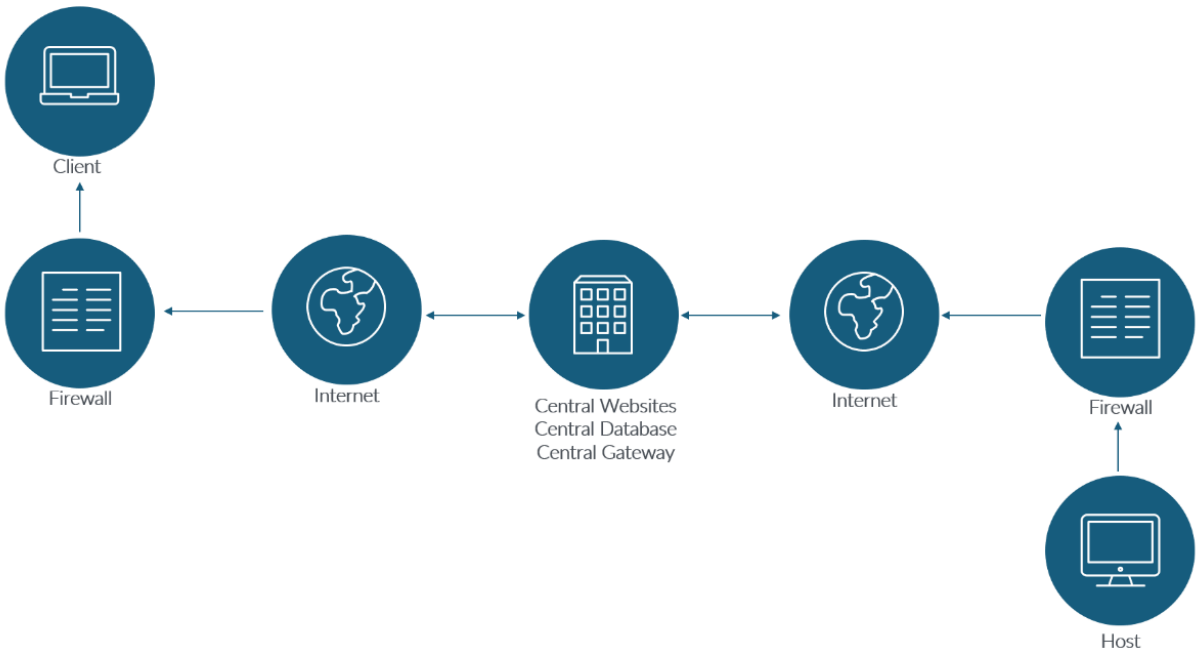

Figure 1. Central architecture

3 Central/Pro Technical 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. Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in both the corporate and production environment. 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.

3.2. Perimeter Defense and Intrusion Detection

The GoTo on-premise network architecture is segmented into public, private, and Integrated Lights-Out (iLO) management network zones. The public zone contains internet-facing servers, and all traffic that enters this network must transit a firewall. Only required network traffic is

allowed; all other network traffic is denied, and no network access is permitted from the public zone to either the private or iLO management network zones.

The private network zone hosts application-level administrative and monitoring systems, and the iLO management network zone is for hardware and network administration and monitoring. Access to these networks is restricted to authorized employees via two-factor authentication.

GoTo employs perimeter protection measures, including a third party, cloud-based, distributed denial of service (DDoS) prevention service, designed to prevent unauthorized network traffic from entering our product infrastructure.

3.3. 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.

3.4. Physical Security

GoTo contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- 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 datacenter
- 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 Technical Operations. GoTo management reviews physical access logs to data centers and server rooms on at least a quarterly basis. Additionally, physical access to data centers is removed upon termination of previously authorized personnel.

3.5. Data Backup, Disaster Recovery and Availability

Central/Pro has near instantaneous fail-over capabilities for most failure scenarios. The production data centers utilize redundant high-speed network connections. There are pools of web and gateway servers across geographically distant data centers. Load balancers distribute network traffic and are intended to maintain the availability of these servers in the event of server or datacenter failures.

The infrastructure is built with fully redundant datacenters, intended to reduce the risk of downtime. Central/Pro operates in three active-active datacenters in the United States and another pair of active-active datacenters in Europe. Each datacenter is designed to be capable of handling all user traffic.

Customer Content backup is done within the same datacenter in 24-hour and seven-day intervals. In addition, a corresponding backup is made in a geographically distant data center every seven days and is retained for four weeks.

3.6. Malware Protection

Malware protection software with audit logging is deployed on all Central/Pro servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.7. Encryption

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

3.7.1. In-Transit Encryption

All network traffic flowing in and out of Central/Pro data centers, including Customer Content, is encrypted in transit.

3.8. 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, remediation action is taken.

GoTo communicates and manages vulnerabilities by providing monthly reports to development teams and management.

3.9. 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 designed to protect the security and privacy posture of Central/Pro.

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 maintains compliance with the following certifications and external audit reports:

- 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.
- American Institute of Certified Public Accountants' (AICPA) Service Organization Control (SOC) 2 Type 2 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. These policies and procedures are designed to manage, identify and resolve suspected or identified security events across GoTo systems and Services, including Central/Pro. 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, when deemed appropriate. Employees can report security incidents via email, phone and/or ticket, according to 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, 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 onboarding 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, the subscribers to the 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. Central/Pro 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 coming into force, 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 Frameworks

GoTo has a robust global data protection program which takes into account applicable law 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

At any time, Customers may request the return or deletion of their Content through standardized interfaces. 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. Customer's Central/Pro Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Upon written request, GoTo will certify to such Content deletion.

5.6. Sensitive Data

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

- 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 or receive payment for Central/Pro.
- 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 the internal assessment and processes related to vendors and third parties, 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. The legal and procurement teams 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 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

In order 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 parties' 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.