Technical and Organizational Measures

Central and Pro

Executive Summary

This Technical and Organizational Measures (“TOMs”) document sets out GoTo’s privacy, security and accountability commitments for Central and Pro. 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 or higher.
  - *At Rest* - Transparent Data Encryption (TDE) and Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Cloud Provider regions:** Germany, Australia, the United Kingdom, the United States, the Netherlands and Ireland hosting locations to support redundancy and stability.
- **Compliance Audits:** SOC 2 / SOC 3 Type II, BSI C5, PCI DSS, TRUSTe Enterprise Privacy 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 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 designed and implemented to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: GoTo employees 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**:
  - Central and Pro 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 ninety (90) days after expiration of a customer’s then-final subscription term.

Contents

1 Product Introduction

Central is a web-based management console that enables IT professionals to access, manage and monitor remote devices, 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 devices 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 device, as well as most smartphones and tablets. Once a Pro host is installed on a device, the service is designed to enable an individual with a sub-account within a Customer account ("User") to 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.

Central and Pro are designed to allow secure remote access to critical resources over an untrusted network and security is a key consideration during product development.

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

2 Product Architecture

Central and Pro are SaaS-based applications featuring a multi-tier architecture hosted in geographically distributed data centers. Security measures at all levels, from the physical layer through the application layer, are designed to provide defense in depth.

The Central and Pro applications are composed of three key components that enable a successful remote access session:

- **Client**: the software (e.g., browser, native app, mobile app) accessing a remote resource;
- **Host or server**: the device being accessed, or the product's host software on this device; and
- **Central/Pro gateway**: the service that mediates traffic between the client and the host.

The Central/Pro host is designed to maintain a constant Transport Layer Security (TLS)-secured connection with a gateway server located in one of the GoTo data centers. After it establishes a secure connection to Central or Pro, the client is authenticated and authorized by the host to access the device, 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 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. As such, the client and the host exchange TLS keys without the gateway learning the key.

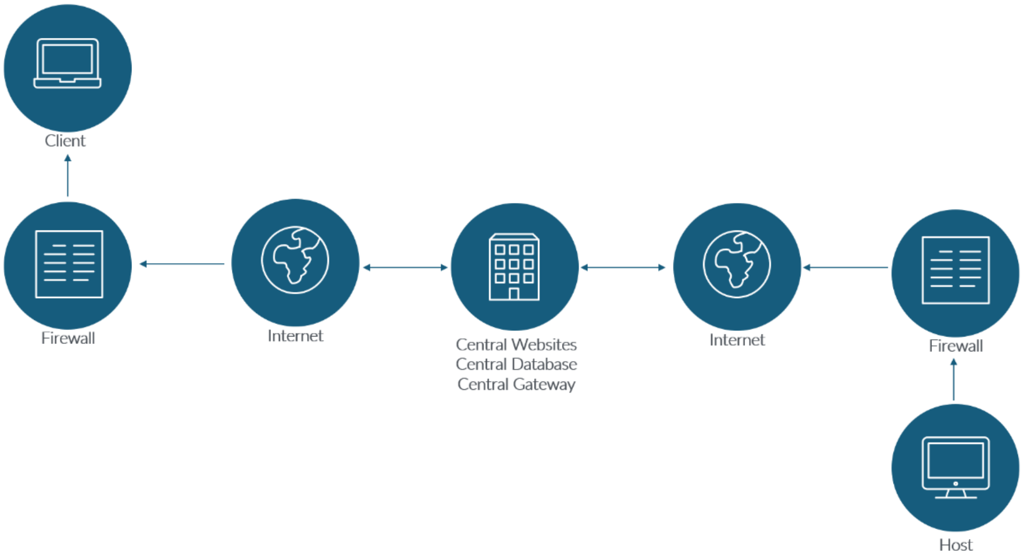

Figure 1: Central Architecture

3 Central Pro Technical Security Controls

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

3.1 Encryption

GoTo periodically 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 to continuously improve its practices and encryption methods.

Central and Pro services support the following encryption protocols (as applicable): TLS 1.2, 2048-bit RSA and AES256 encryption ciphers with 384-bit SHA-2 algorithm.

Central and Pro support both AES 128 and 256-bit keys, and the client and the server will agree on the strongest compatible and available cipher between those two key lengths. The client sends the server a list of ciphers it is willing to use, and the server chooses the one it prefers. In Central and Pro, the server selects the strongest shared cipher suite that the client has offered.

3.2 Encryption In Transit

All network traffic flowing in and out of Central/Pro data centers, including Customer Content, is encrypted in transit with TLS 1.2 or, where supported, TLS 1.3.

3.3 Encryption At Rest

All Central/Pro Customer Content is stored in MSSQL with Transparent Data Encryption (TDE) and encrypted at rest with AES-256.

3.4 User Authentication

Central/Pro uses a proprietary Common Login Service (“CLS”) for User authentication. CLS employs custom heuristics designed to prevent suspicious User access. For accounts that have a linked GoTo Common Identity Platform (“CIP”) account, the login is further protected by a third-party risk assessment service.

3.5 Multifactor Authentication

Multifactor authentication (also referred to as two-step verification or two-factor authentication) adds a second layer of protection to an account by requiring two distinct forms of identification to log in. After setting up multifactor authentication, Users will enter their credentials and then be prompted to verify their identity through a security code.

Central subscribers can enforce a login policy that forces all Users in their account to use multifactor authentication. For step-by-step instructions, visit support.logmeininc.com/central.

3.6 Printed Security Codes

Customers can opt to use printed security codes as an additional layer of protection. When the User enables this feature, they are required to print out a list of nine-character random passwords generated by the gateway. Each time the User logs in to their account at logmein.com, they will be prompted to enter one of the security codes from the list to gain access to their account. Each code can be used only once. Before the User runs out of printed security codes, they will be required to print another sheet. This invalidates any previously unused security codes.

3.7 Emailed Security Codes

When this feature is turned on and the User authenticates successfully with their email address and password to the Central/Pro gateway, a passcode is generated and sent to the email address. The User receives this passcode in an email and enters the code into the form provided by the gateway. The password expires either upon use or within a few minutes of generation, whichever comes first.

3.8 Authentication of the Gateway to the Client

Central and Pro utilize TLS 1.2 or 1.3 certificate-based authentication (with 1.3 used where supported and not explicitly disabled) to verify server identities and ensure that when a User connects to a Central or Pro server via a gateway, they are connecting with the intended device. When a connection is made, the server’s certificate is verified. A warning is presented if an untrusted certifying authority issued the certificate. A different warning is presented if the hostname in the URL does not match the hostname in the certificate, even if issued by a trusted authority.

If the server passes these verifications, the User's client generates a pre-master secret (PMS), encrypts it with the server's public key contained within its certificate, and sends it to the server. Public key cryptography is used so that only the server that holds the corresponding private key can decrypt the PMS. The PMS is then used by both the User and the server to derive the master secret, which is then used to derive initialization vectors and session keys for the duration of the secure session.

3.9 One2Many – Authentication and Encryption (Central Only)

The One2Many feature allows advanced scripting and deployment capabilities that enable Central Users to perform mass functions across managed organizations. With this tool, Users can execute, manage, and monitor administrative tasks on multiple Windows and Mac devices directly from Central.

Multifactor authentication is required for One2Many. One2Many stores multifactor authentication credentials in two different ways: when executing a task in real-time, it stores the credentials in the browser; when the task is scheduled to be executed later, the credentials are stored in the database of the product.

Credentials used in One2Many are encrypted with the host's public key first, and then further encrypted by the website. The first layer of encryption ensures that only the host can decrypt the credentials with its private key; and the second layer of encryption enables the option to wipe data from the website, even if the host is offline.

3.10 Authentication of Users to the Gateway

Users must be authenticated by both the gateway and the host. A User's email address and password is verified whenever they log on to Central/Pro.

NOTE: Central Customers can enforce a strong password policy. Visit support.logmeininc.com/central for details.

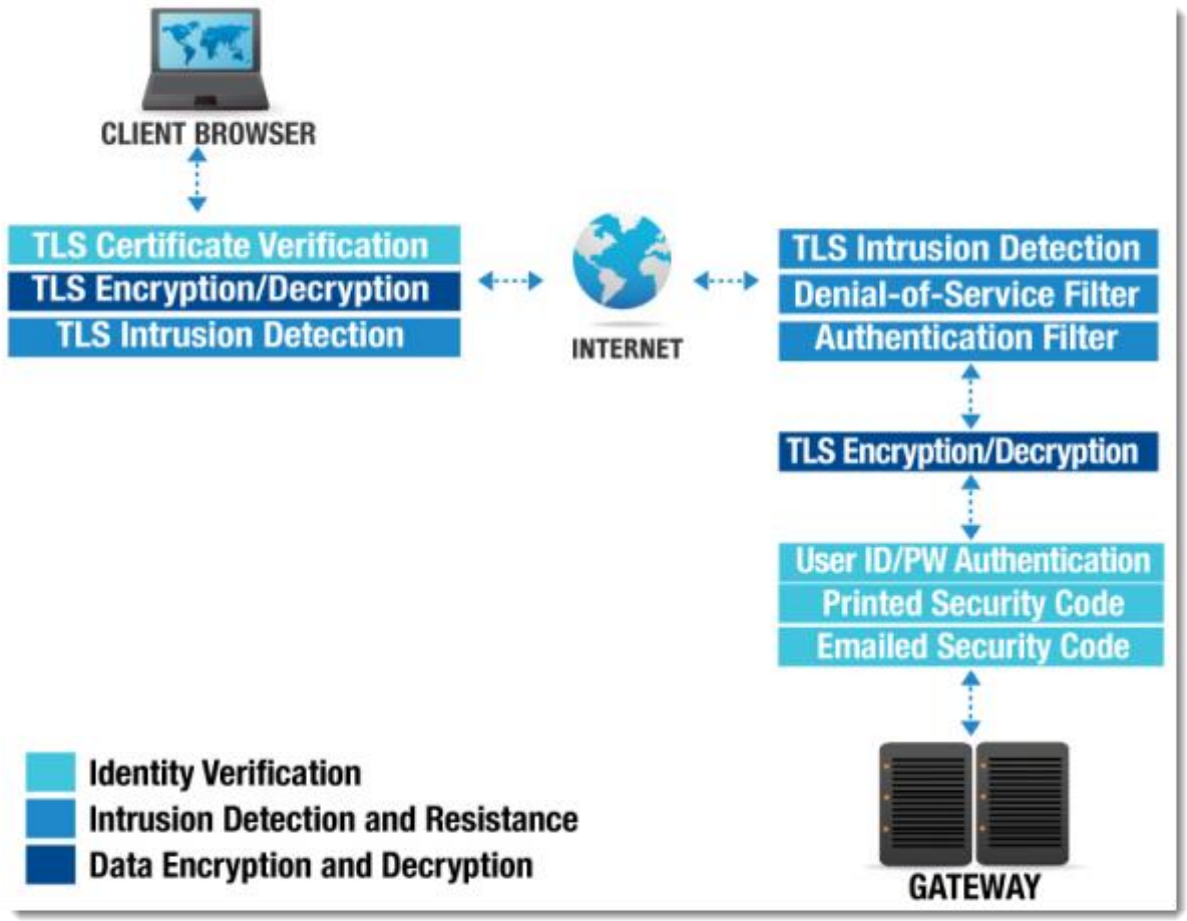

Figure 2: Authentication between Users and the Gateway

3.11 Account Audit

Customers can keep track of activity in their Central/Pro account through email notifications. In addition to default events, Customers can select events about which to be notified such as login attempt failure or password changes.

3.12 Authentication of the Gateway to the Host

The gateway must prove its identity to the host before it is trusted with access codes. The host, when making a connection to the gateway, checks the certificate transported during the TLS "handshake" to make sure it is connecting to one of the GoTo gateway servers.

3.13 Authentication of the Host to the Gateway

The gateway verifies the host's identity using a long unique identifier string. This string is a shared secret between the two entities and is issued by the gateway when the host is installed. Once the host identifies the unique identifier string, it communicates the string back to the gateway over a TLS-secured channel. Figure 3 illustrates how the host and the gateway authenticate each other before a host is made accessible to the client. To ensure further security, the host can change its shared secret with a request from the gateway via the secure connection.

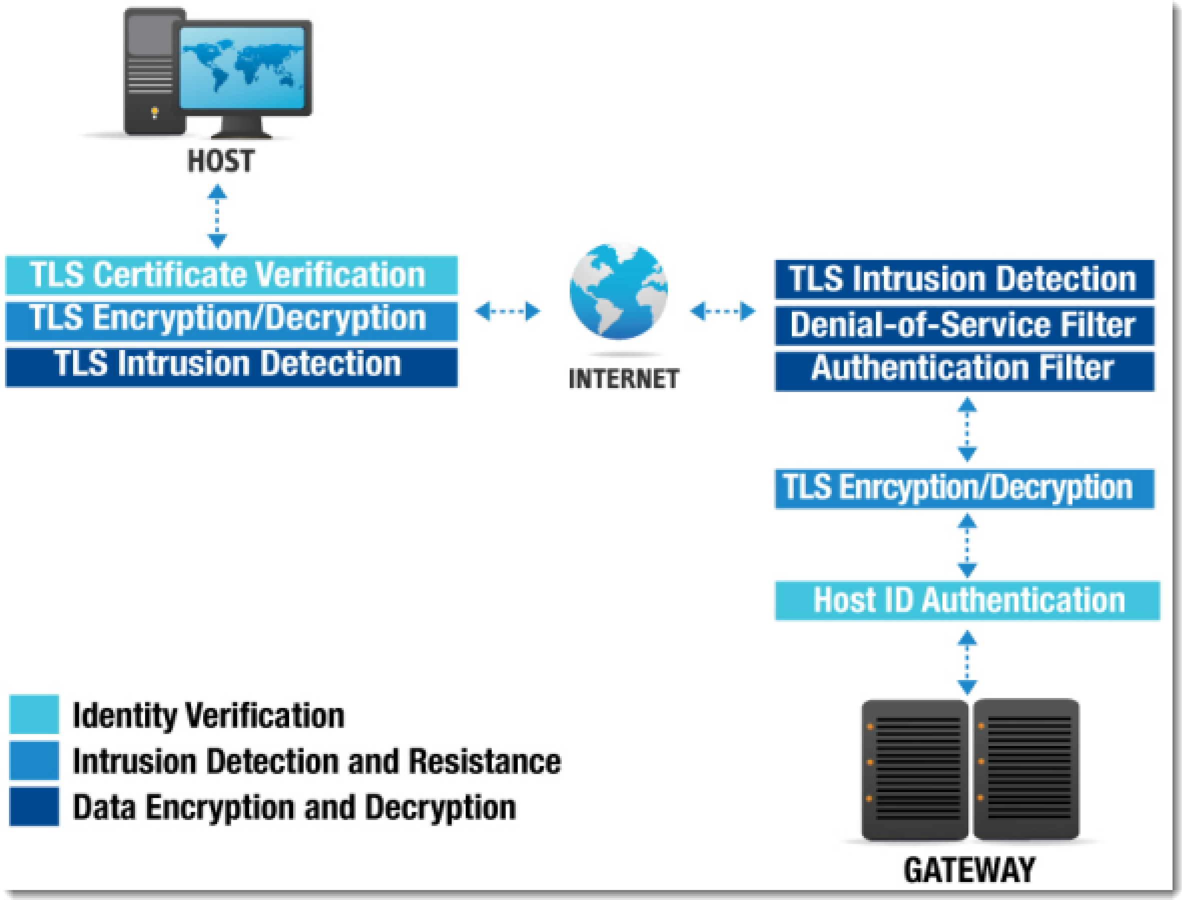

Figure 3: Host and Gateway Authentication

3.14 Intrusion Detection

Central and Pro have two layers of security which are designed to detect intrusion attempts: TLS and GoTo intrusion filters.

3.15 TLS

For the first layer of intrusion detection, Central/Pro utilizes TLS 1.2 or 1.3 certificate-based authentication (with 1.3 used where supported and not explicitly disabled) to ensure that the data has not changed in transit. This is achieved by the following techniques:

Record Sequence Numbering	Record sequence numbering means that TLS records are numbered by the sender and the order is checked by the receiver. This ensures that an attacker cannot remove or insert arbitrary records into the data stream.

Message Authentication Codes	Message authentication codes (MACs) are appended to every TLS record. This is derived from the session key (known only to the two communicating parties) and the data contained within the record. If MAC verification fails, it is assumed that the data were modified in transit.

3.16 Central/Pro Intrusion Filters

The second layer is provided by GoTo itself and is comprised of three intrusion filters:

3.17 IP Address Filter

When Central/Pro receives a connection request from a client, it first checks its list of trusted and untrusted IP addresses and may deny the connection if it is untrusted. An administrator can set up a list of IP addresses within Central/Pro that will be either allowed (trusted) or denied (untrusted) a connection to the selected host (for example, an administrator can designate the company's internal network and another administrator's home IP address as allowed).

3.18 Denial of Service Filter

A Denial-of-Service Filter rejects connections if the requesting IP address has made an excessive number of requests without authentication within the observation time window to protect the host device from being overloaded.

3.19 Authentication Filter

If the User made an excessive number of failed login attempts, the Authentication Filter rejects the connection. The Authentication Filter is in place to prevent a potential intruder from gaining access to an account by guessing an account name and password.

3.20 Authentication and Authorization of Users to the Host

After being granted access by the previous layers, the User must prove their identity to the host. This is achieved by a mandatory OS-level authentication step: the User is authenticated to the host using their device (e.g., Windows or Mac) username and password. Where relevant, the domain controller will receive this request which validates the User's identity and ensures that network administrators can control who is able to log in to a specific host.

3.21 Personal Password

A personal password is another optional security measure that can be set up on the Central/Pro host. The User can assign a personal password to the host, which, like the OS-level password, is not stored or verified by the gateway. Unlike with the operating system password, the host never asks for the complete personal password, so the User never enters it in its entirety in any single authentication session. The User is usually prompted for three random characters of the personal password for example, the first, the fourth and the seventh) by the host after OS-level authentication has succeeded. If the User enters the correct characters, they are granted access.

3.22 GoTo and RSA SecurID

To add an extra layer of security over the username/password authentication, Users can configure Central/Pro to require RSA SecurID authentication. For information on setting up this feature on a Central/Pro host, visit https://support.logmeininc.com/pro.

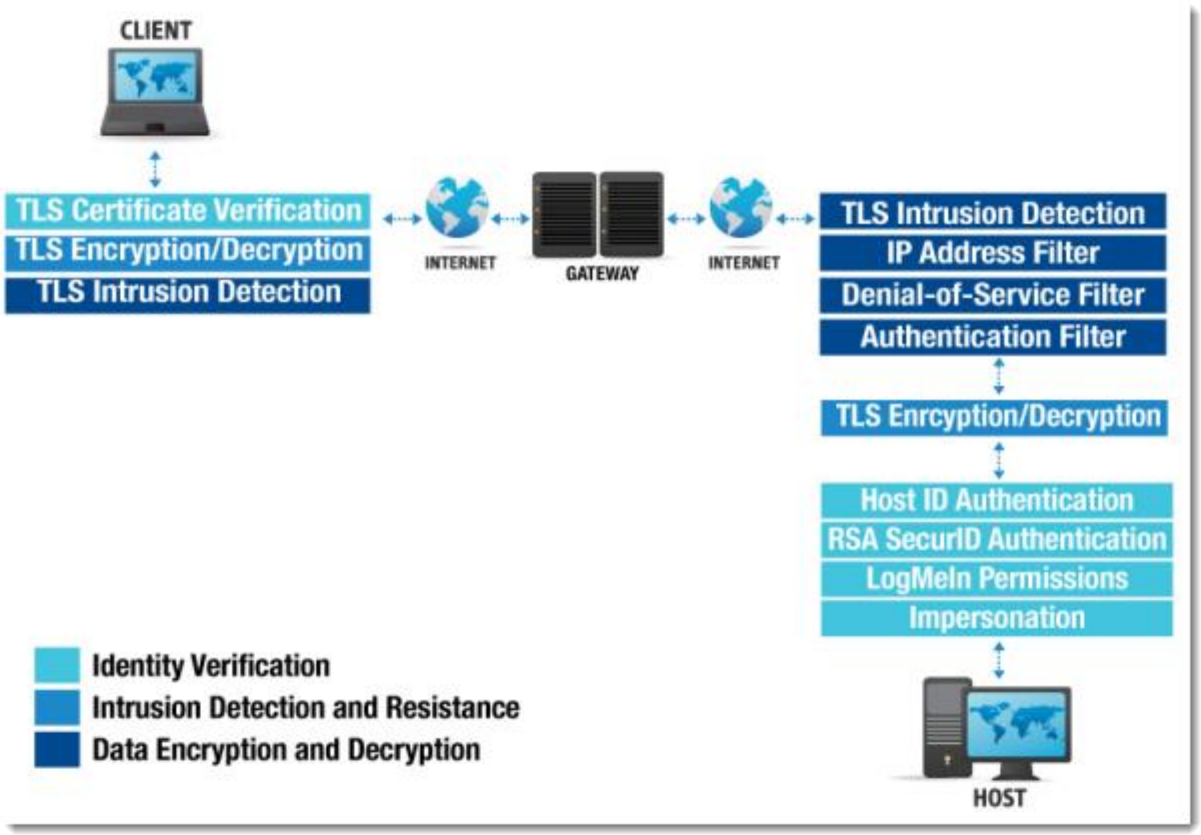

Figure 4: Authentication between Users and the Host

3.23 Authentication and Authorization of Users within the Host

Once Central/Pro has verified the User's identity using the above methods, it checks its own internal User database to see which internal modules the User is allowed to access.

System administrators can configure Central/Pro so that Users with certain roles have access only to a subset of tools offered by GoTo; for example, the Helpdesk department can be granted access to only view a device's screen and performance data, but not actually take over the mouse and the keyboard or make any changes to the system configuration. Alternatively, the Sales department could be given full remote-control access to their respective devices, but not to features such as performance monitoring and remote administration.

Using the operating system access token obtained when the User was authenticated, Central/Pro impersonates the User to the operating system while performing actions on the User's behalf. This ensures that Central/Pro adheres to the operating system's security model, and Users have access to the same files and network resources as if they were sitting in front of their device. Resources unavailable to Users in Windows or OS X also remain unavailable via Central/Pro.

See “Controlling Who Can Access Your Host Computers” on the Central or Pro support site for details.

3.24 Auditing and Logging

Central and Pro provide extensive logging capabilities. A detailed log of the events that occur within the software is kept in the Central/Pro data log directory. Certain important events are also placed in the Windows or OS X application event log, including logon and logoff actions. The detailed log can also be sent to a custom SYSLOG server of the Customer's choice.

See “How to View Host Event Log Files” on the Pro support site for details. For SYSLOG, see “Define Syslog Settings for the Host” on the Central support site.

3.25 Data Forwarding

The gateway provides end-to-end encryption by forwarding encrypted data between the host and the client.

To enable this, the first part of the TLS negotiation is performed between the gateway and the client. The gateway then passes the exchange on to the host, which re-negotiates the TLS session and agrees on a new session key with the client, thereby providing true end-to-end encryption.

When the traffic is relayed through the gateway, the client establishes a TLS session with the gateway using the gateway's certificate. The gateway transfers this TLS session's state (including the Pre-Master Secret) to the host. After agreeing on a new session key, the host uses this session state to handle the rest of the TLS session directly with the client. The gateway's certificate secures the session, leaving the client communicating directly with the host without the need for the gateway to decrypt and re-encrypt traffic.

3.26 UDP NAT Traversal

User datagram protocol (UDP) is used at the network layer, as defined by the ISO/OSI Network Model, with a transmission control protocol (TCP)-like transport layer built on top of it, complete with flow control, dynamic bandwidth scaling and packet sequence numbering. Logmein.com uses UDP instead of TCP packets (thereby effectively re-implementing a TCP-like transport layer). After a reliable TCP-like stream is constructed from unreliable UDP packets, the stream is further protected by a TLS layer, providing full encryption, integrity protection and endpoint verification capabilities.

To set up a UDP NAT Traversal connection, both the client and the host send several encrypted UDP packets to the gateway. These packets are encrypted using a secret key shared by the gateway and the respective peer and are communicated over the pre-existing TLS connection.

The gateway uses these packets to determine the external (Internet) IP addresses of the two entities. It also tries to predict which firewall port will be used for communication when a new UDP packet is sent. It passes its findings down to the peers, which then attempt to set up a direct connection. If the gateway can determine the port in use, the connection succeeds. The peers verify each other using another shared secret obtained from the gateway. A TLS session is established. The peers then communicate directly.

If a direct connection cannot be set up, the peers will connect back to the gateway over TCP and request that a forwarded, end-to-end encrypted session be used. This process takes only a few seconds, is transparent to the User, improves performance and reduces latency when a direct connection is in use.[1]

3.27 Software Updates and Gateway Security

The Central/Pro host, based on User preferences, can semi-automatically or automatically update itself on the User's device. The host software periodically checks the logmein.com website for newer versions of the software. If a new version is found, it is automatically downloaded, and a message is displayed to the User who can allow the update to take place. The download process uses at most 50% of the available bandwidth, therefore keeping interference with other networking applications to a minimum.

These software updates are digitally signed by logmein.com with a private key that is not found on any of our Internet-connected systems.

Central/Pro passwords are not stored in our database: Central and Pro use a one-way cryptographic key derivation function and a per-account salt value.

4 Data Backup, Disaster Recovery and Availability

Customer Content backup is done within the same data center 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.

RTO: The timeframe for recovery back to running state for the product services (DB) in case of a disaster is 60 minutes

RPO: The maximum acceptable amount of data loss in case of a disaster is 15 minutes, meaning data can be recovered up to 15 minutes prior to the incident

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 redundant, active-active infrastructure in cloud hosting provider data centers.

[1] For further details see US Patent no. 7,558,862

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the Central Pro 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://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
- https://aws.amazon.com/compliance/data-center/controls/

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

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.

7 Customer Content Retention Schedule

Unless otherwise required by applicable law, Customer Content shall automatically be deleted ninety (90) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer’s then-final subscription. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

8 Revision History

Version	Month/Year	Description
Version 1.8	July 2024	Updated and published by Legal

Version 1.9	July 2025	Standardized the document only includes Product Specific sections.