GoToAssist Corporate
Security and Privacy Operational Controls

V1

February 4, 2020

LogMeIn GoToAssist Corporate Security and Privacy Operational Controls

Publication Date: 02/04/2020

1 Products and Services

This document covers the security and privacy controls for LogMeIn GoToAssist Corporate, a hosted service designed to enable multi-agent support teams to deliver live remote technical assistance to corporate users of Windows-based and Mac computers. GoToAssist Corporate is customizable to a company's unique environment and features advanced administrative, collaborative, and customer-queuing features, including team collaboration, session transfer, customer surveys, and session recording.

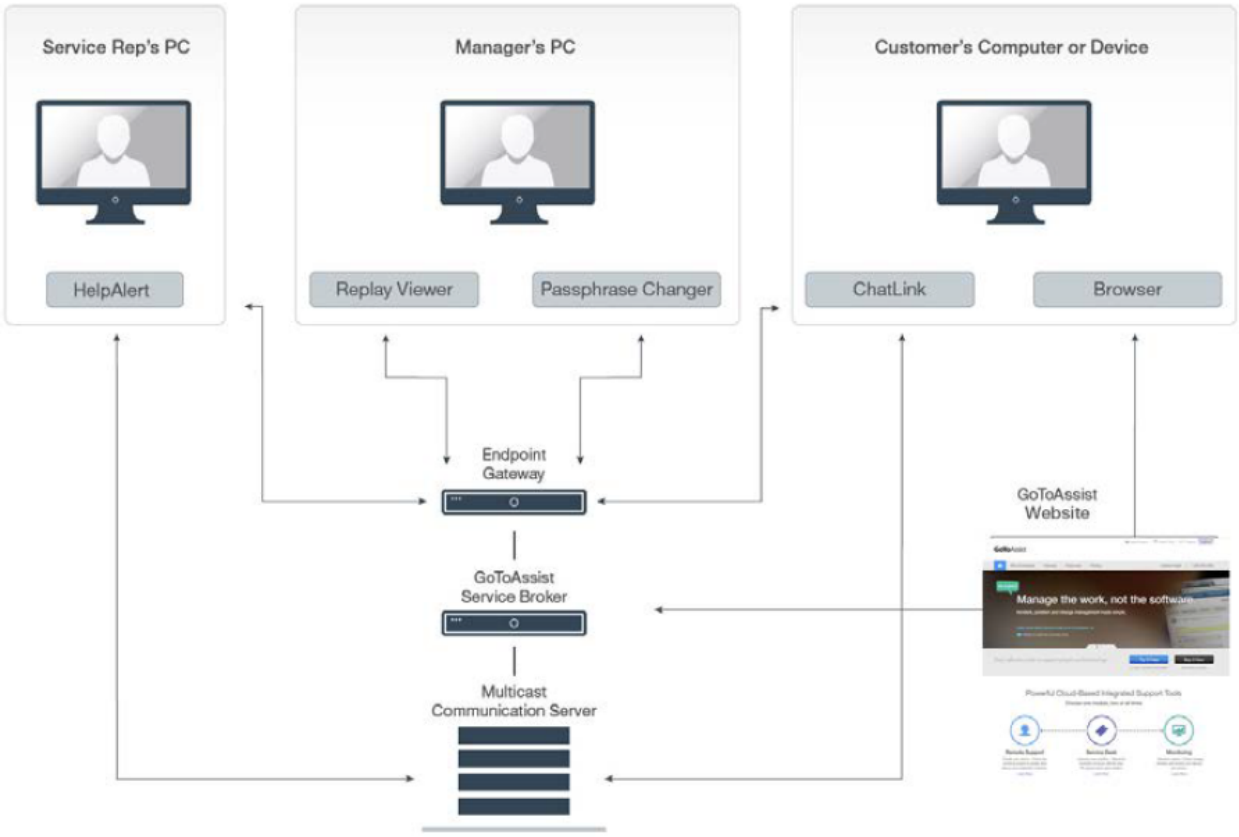
2 Product Architecture

GoToAssist Corporate 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 for performance, reliability and scalability. Redundant switches and routers are built into the architecture which is designed to ensure that there is no single point of failure. High-capacity, clustered servers and backup systems are intended to ensure application processes in the event of a heavy load or system failure. Service brokers load balance the client/server sessions across geographically distributed communication servers in order to ensure performance.

The web, application, communication and database servers are housed in secure co-location datacenters featuring redundant power and environmental controls. Physical access to servers is tightly restricted and continuously monitored. Firewall, router and VPN-based access controls are employed to secure our private-service networks and backend servers. Infrastructure security is continuously monitored, and vulnerability testing is conducted regularly by internal staff and outside third-party auditors.

3 LogMeIn GoToAssist Corporate Technical Security Controls

LogMeIn 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 [1]) in order to safeguard the Service infrastructure and data residing therein.



GoToAssist Website - Web application that provides access to the GoToAssist website and web-based internal and external administration portals. The websites are hosted in Tier 1 co-location data centers.

GoToAssist Service Broker - Web application that realizes GoToAssist Corporate account and service management, persistent storage and reporting functions. Brokers are hosted in Tier 1 co-location data centers.

Endpoint Gateway (EGW) - A special-purpose gateway used by various endpoint applications to securely access the GoToAssist Service Broker for a variety of purposes using remote procedure calls. EGW are hosted on Amazon Web Services.

Multicast Communication Servers (MCS) - A fleet of globally distributed servers used to realize a variety of high-availability unicast and multicast communication services. MCS are hosted in Tier 1 co-location data centers.

3.1 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or "least privilege") access to specified LogMeIn systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

Users authorized to access LogMeIn GotoAssist Corporate product components may include LogMeIn's 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 Ops VPN and both are protected by multi-factor authentication (MFA). Cloud-based production components are available through SSU (Self Service Unix) authentication.

3.2 Perimeter Defense and Intrusion Detection

LogMeIn employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering our product infrastructure. The LogMeIn network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls. In addition, a third party, cloud-based distributed denial of service (DDoS) prevention service is used to protect against volumetric DDoS attacks; this service is tested at least once per year. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

LogMeIn leverages a multi-tenant architecture which is logically separated at the database level based on the organization's LogMeIn account. Only authenticated parties are granted access.

3.4 Physical Security

LogMeIn 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 data center
- Scheduled maintenance and validation of all critical security and environmental controls

LogMeIn limits physical access to production datacenters to authorized individuals only. Access to an on-premises 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. LogMeIn management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.5 Data Backup, Disaster Recovery, Availability

LogMeIn's architecture is generally designed to perform replication in near-real-time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. 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 the system is tested periodically.

3.6 Malware Protection

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

3.7 Encryption

LogMeIn maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable 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.

Key points regarding encryption in GoToAssist Corporate include:

- Public-key-based Secure Remote Password (SRP) protocol authentication provides authentication and key establishment between endpoints
- 128-bit AES encryption is used to safeguard session data
- Session keys are generated by endpoints, and are never known to LogMeIn or its systems
- Communication servers route only encrypted packets and do not have the session encryption key

3.7.1 In-Transit Encryption

To further safeguard Customer Content while in transit, LogMeIn uses current Transport Layer Security (TLS) protocols and associated cipher suites to protect many internet protocols. In addition, LogMeIn uses the latest version of Secure Shell (SSH) for certain administrative functions. Connectivity to internal networks is protected through appropriate Virtual Private Network (VPN) technologies, intended to ensure the confidentiality and integrity of LogMeIn internal traffic.

Communication security features

Communication between participants in a GoToAssist Corporate session occurs via an overlay multicast networking stack that logically sits on top of the conventional TCP/IP stack within each user's computer. This network is realized by a collection of Multicast Communication Servers (MCS).

Communication confidentiality and integrity

GoToAssist Corporate provides end-to-end encryption and data security measures that are designed to address both passive and active attacks against confidentiality, integrity and availability. Screen-sharing data, keyboard/mouse control data and text chat information are

never exposed in unencrypted form while temporarily resident within communication servers or during transmission across public or private networks.

When recording is disabled, the GoToAssist Corporate session key is not kept on the servers in any form. Thus, for example, breaking into a server would not reveal the key for any encrypted stream that a malicious actor may have captured. When recording is enabled, chat, screen-sharing and screen-viewing data is stored in encrypted form. The session key is also stored, but it is protected with 1024-bit RSA public/private key encryption. A portal-specific public key is used to encrypt the session key before storage. As a measure to safeguard session data, session replays require the following: access to the session recording, the encrypted session key and the portal's private key. Communications security controls based on strong cryptography are implemented at two layers: the "TCP layer" and the "Multicast Packet Security Layer" (MPSL).

TCP layer security

Internet Engineering Task Force (IETF)-standard TLS protocols are used in order to protect communication between endpoints.

For their own protection, LogMeIn 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 to the website and between GoToAssist Corporate components, LogMeIn servers authenticate themselves to clients using public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., MCS-to-MCS or MCS-to-Broker).

Multicast packet security layer

Additional features provide complete end-to end security for multicast packet data, independent of that provided by TLS. Specifically, all multicast session data is protected by end-to-end encryption and integrity mechanisms designed to prevent anyone with access to the communications servers (whether friendly or hostile) from eavesdropping on a session or manipulating data without detection. Unique to LogMeIn products, the MPSL provides an added level of communication confidentiality and integrity.

MPSL key establishment is accomplished by using a randomly generated 128-bit seed value selected by the GoToAssist Corporate service broker, that is distributed to all endpoints over TLS and used as the input to a NIST-compatible HMAC-SHA1 key-derivation function. The seed value is erased from the GoToAssist Corporate service broker's memory when the session ends.

MPSL further protects multicast packet data from eavesdropping using 128-bit AES encryption in counter mode. Plain-text data is typically compressed before encryption using proprietary, high-performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value.

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 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.

3.9. Logging and Alerting

LogMeIn collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

LogMeIn maintains a comprehensive set of organizational and administrative controls to protect the security and privacy posture of GoToAssist Corporate.

4.1 Security Policies and Procedures

LogMeIn 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

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certification(s) and external audit report(s):

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LogMeIn's eCommerce and payment environments
- TRUSTe Enterprise Privacy Certification

4.3 Security Operations and Incident Management

LogMeIn'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 LogMeIn's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating

procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including the GoToAssist Services. 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 appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the LogMeIn intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

LogMeIn'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 LogMeIn 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.

LogMeIn employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding 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

LogMeIn takes the privacy of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Privacy Policy

LogMeIn discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website [2]. 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.

5.2 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. The Service is compliant with the applicable provisions of the GDPR. For more information, please visit www.logmeininc.com/trust.

5.3 CCPA

LogMeIn hereby represents and warrants that it will be in compliance with the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA no later than January 1, 2020. For more information, please visit www.logmeininc.com/trust.

5.4 EU-U.S. and Swiss Privacy Shield

LogMeIn, Inc. and its US affiliates participate in the EU-U.S. Privacy Shield Framework and Swiss Privacy Shield regarding the collection, use and retention of personal information from European Union member countries and Switzerland [3]. Certification is reviewed annually by TRUSTe and any findings are promptly addressed by LogMeIn.

5.5 Return and Deletion of Customer Content

At any time, GoToAssist Corporate Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available or LogMeIn is otherwise unable to complete the request, LogMeIn 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. Customers' GoToAssist Corporate Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Upon written request, LogMeIn will certify to such Content deletion.

5.6 Sensitive Data

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

- 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) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related 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 LogMeIn to collect payment for GoToAssist Corporate

- 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

LogMeIn is continuously improving its websites and products using various third-party web analytics tools, which help LogMeIn understand how visitors use its websites, desktop tools, and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy [2].

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. Legal and Procurement 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 that are granted access to sensitive or confidential data by LogMeIn 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

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, LogMeIn reviews relevant third parties' terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7. Contacting LogMeIn

Customers can contact LogMeIn at https://support.logmeininc.com/ for general inquiries or privacy@logmein.com for privacy-related questions.

8. References

[1] LogMeIn, Inc., "Terms of Service for LogMeIn and Goto Services," LogMeIn, Inc., June 2019. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[2] LogMeIn, Inc, "LogMeIn Privacy Policy," [Online]. Available: https://secure.logmein.com/policies/privacy.aspx. [Accessed 2 April 2018].

[3] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., September 2019. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.