GoToMyPC

Security and Privacy Operational Controls

V2 October 2020

GoToMyPC Security and Privacy Operational Controls

Publication Date: October 2020

1 Products and Services

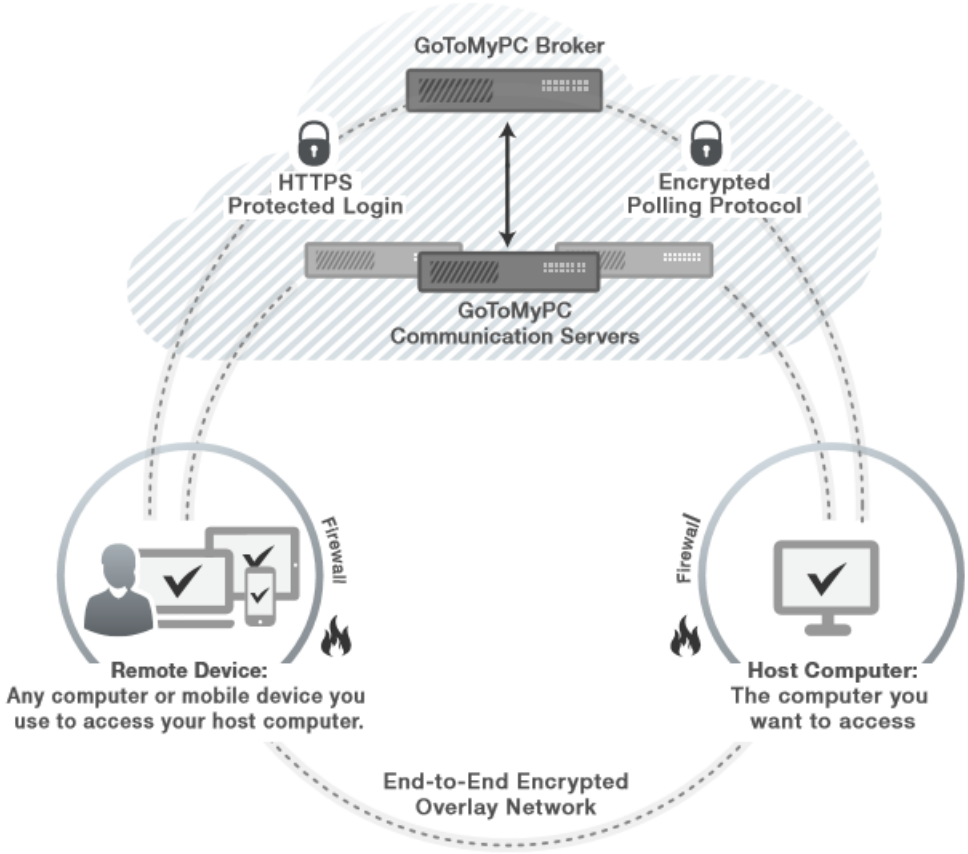
This document covers the security and privacy controls for GoToMyPC, a hosted service that enables secure remote access to an internet-connected Windows-based or Mac host computer from any remote computer, iPad, iPhone or Android device. Features include a screen-sharing viewer, drag-and-drop file transfer, remote printing, guest invite, use with multiple monitors, mobile apps and chat. There are three versions of GoToMyPC available in order to meet the needs of individual professionals, teams, and small and medium-sized businesses (SMB).

2 Product Architecture

GoToMyPC is a hosted service comprised of five components:

- *Host Computer:* Typically, a home or office computer with always-on internet access on which a small footprint server is installed. This server registers and authenticates itself with the GoToMyPC broker.
- *Browser*: From the remote computer, called the client, the user launches a web browser, visits the secure GoToMyPC website, enters his or her username and password, and clicks "Connect" to send the broker an authenticated, encrypted request for access to the desired host computer. Alternatively, the user can install the GoToMyPC app on a supported tablet or smartphone, enter his or her account details and click "Connect" to initiate the request.
- *Broker*: The broker is a matchmaker that listens for connection requests and maps them to registered computers. When a match occurs, the broker assigns the session to a communication server. Next, the client viewer — a session-specific executable applet — is automatically loaded by our automatic launcher tool.
- *Communication Server*: The communication server is an intermediate system that relays an opaque and highly compressed encrypted stream between the client and host computers for the duration of each GoToMyPC session.
- *Direct Connections*: Once the user is authenticated and connected, GoToMyPC attempts to establish a direct connection between the client and host, bypassing the GoToMyPC communication server whenever possible to increase the connection speed and improve in-session performance. The Direct Connections feature instructs both the client and host to listen for a limited time for incoming connections and to attempt outgoing connections to each other; whichever signal arrives first establishes the connection. The client and host then proceed to execute a Secure Remote Password (SRP) protocol-based authenticated key agreement and establish an end-to-end secure connection that is designed in a manner intended to reduce or eliminate susceptibility

to “man-in-the-middle” attacks. Should the direct connection be blocked or interrupted, the connection previously established through the communication server maintains remote access service. The Direct Connections feature is always enabled for GoToMyPC and GoToMyPC Pro accounts and is optional for GoToMyPC Corporate.



The infrastructure is designed in a manner intended to be both robust and secure. Redundant routers, switches, server clusters and backup systems are designed and employed to ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among web servers. For the purposes of ensuring optimal performance, the GoToMyPC broker load balances the client/server sessions across geographically distributed communication servers.

3 GoToMyPC Technical Security Controls

LogMeIn employs industry standard technical controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service [1]) designed to safeguard the Service infrastructure and data residing therein.

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.

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. Specifically, multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and web servers, and another between the GoToMyPC broker and back-end databases. Cloud resources also utilize host-based firewalls. Additionally, a third-party, distributed cloud-based distributed denial of service (DDoS) prevention solution is used in order to protect against volumetric DDoS attacks; this service is tested at least once per year. Critical system files are designed to be protected against malicious and unintended infection or destruction.

3.3 Data Segregation

LogMeIn leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's LogMeIn account. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Datacenter 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-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. LogMeIn 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 and Disaster Recovery

GoToMyPC performs database replication in near-real-time to a secondary site located in a geographically diverse location. 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 GoToMyPC 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 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.

3.7.1 In-Transit Encryption

GoToMyPC Corporate has end-to-end, 128-bit Advanced Encryption Standard (AES) encryption built in. All traffic between the GoToMyPC browser client and host computer is highly compressed and encrypted. GoToMyPC generates unique, secret encryption keys for each connection using a fully contributory and mutually authenticated key agreement.

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 in order to protect the security and privacy posture of GoToMyPC.

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

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

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 GoToMyPC. 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, which for the purposes of this Section 5 is the subscriber to the LogMeIn 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 Data Protection and Privacy Policy

LogMeIn 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 LogMeIn's processing of Personal Data as may be located within Customer Content.

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 LogMeIn'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 LogMeIn will not sell our users' 'personal information.'

For visitors to our webpages, 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. GoToAssist Remote Support v4 is compliant with the applicable provisions of GDPR. For more information, please visit http://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 Transfer Frameworks

LogMeIn is aware of the European Court of Justice's decision with respect to the EU-U.S. Privacy Shield Framework and is actively monitoring the situation. [3]
LogMeIn's privacy program and contracts have been designed to account for shifts in the regulatory landscape to avoid impacts to our ability to provide our services to you. The EU-U.S. Privacy Shield Framework was just one (of several) mechanisms that LogMeIn relied on to lawfully transfer personal data. Therefore, LogMeIn offer in the following Transfer 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 EEA will be transferred in compliance with EU data-protection law. LogMeIn has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. LogMeIn offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope LogMeIn services as part of its global DPA[3]. Execution of the SCCs helps ensure that LogMeIn customers can freely move data from the EEA to the rest of the world.[3]

5.4.2. APEC CBPR and PRP Certifications

LogMeIn 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 between APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance.[3]

5.5 Return and Deletion of Customer Content

At any time, GoToMyPC 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 after Customer's request. Additionally, Customer's GoToMyPC 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 GoToMyPC for certain types of information. Unless Customer has received written permission from LogMeIn, the following data must not be uploaded, generated, or input to GoToMyPC:

- 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 LogMeIn to collect or receive payment for GoToMyPC.
- 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 relevant identified 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 such third-party control environments are functioning adequately and that 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, such information (as applicable).

6.2 Contract Practices

In order to ensure business continuity and that appropriate measures are in place which are in each case, designed 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 and appropriate.

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," LogMeIn, Inc., March 2020 [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[2] LogMeIn, Inc, "LogMeIn Privacy Policy," LogMeIn, Inc., April 2020 [Online]. Available: https://www.logmeininc.com/legal/privacy

[3] LogMeIn, Inc., "LogMeIn Special Note on Privacy Shield," LogMeIn, Inc., August 2020 [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.