LogMeIn join.me Security and Privacy Organizational Controls

Publication Date: 3/28/2019

1 Products and Services

This document covers the security and privacy controls for join.me.

join.me is an online meeting and screen sharing service that gives users the ability to quickly and securely host an online meeting with other people. These services can be initiated through a visit to the https://join.me website, through a small downloadable desktop application or through mobile applications (iOS and Android). It is available in a free and Lite version, as well as a "Pro" premium version for individuals and small teams and a premium "Business" version for larger teams and company-wide use.

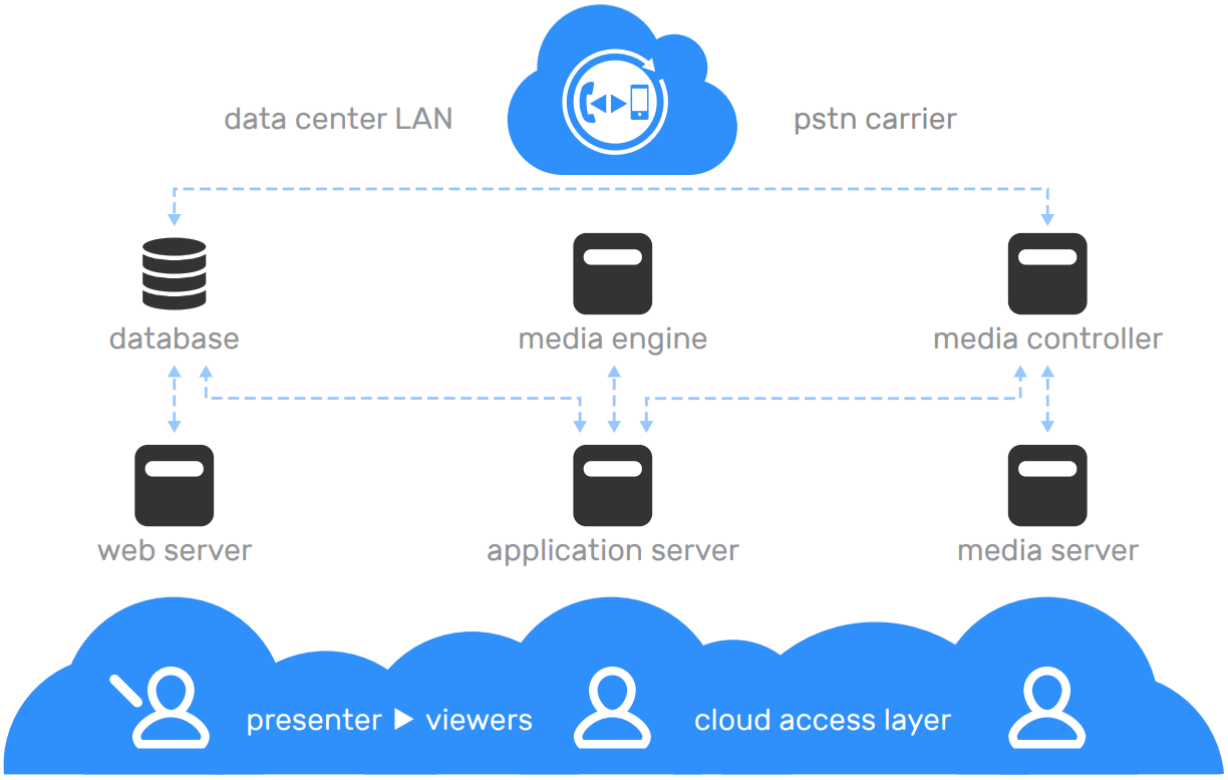
2 Product Architecture

LogMeIn join.me is a SaaS-based application hosted on multi-tier architecture located in secure and reliable data centers in key locations around the globe. A multi-layer security approach is utilized at all levels from the physical layer through the application layer.

The join.me architecture includes components such as web servers, application servers, media servers, databases, media controllers and media engines. The application has built-in redundancies, designed to increase the availability and reliability of the service, so that if an application server or data center goes off-line or become unreachable, the session should quickly migrate to a different application server. Load balancers are utilized in order to geographically maintain availability. Both access to the application website and the information that travels between components is encrypted in transit utilizing Transport Layer Security (TLS) protocol. Customers have the flexibility to elect specified types of data that are stored on their behalf -- session data, for example, such as screens, video, or chat logs, are not, by default stored on LogMeIn servers.

Services provided by join.me rely on third-party telecommunication companies to provide the audio-based conference infrastructure that allows audio participants to connect to each other regardless of which endpoint device they use to join. WebRTC technology is utilized to deliver video conferencing on platforms such as Windows, Mac OS X, HTML5, iOS and Android. The MP4 video format is used to save video recordings and can be stored in the Azure storage region closest to the presenter's location.

A typical **join.me** session involves at least the following components:



Web server – User registration, account and meeting settings, meeting launch

Application Server – Maintains meetings, distributes data among appropriate viewers

Media server – Distributes media streams among appropriate viewers

Database – Stores user profiles and meeting settings

Media controller – Controls media sessions and PSTN connections

Media engine – Post-processes media elements in order to provide recorded meeting video

3 join.me Service 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 [2]) 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

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, 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 co-location data centers 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 a 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 and 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 join.me Servers. Alerts indicating potential malicious activity are sent to the 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

At the protocol level, join.me uses TLS for communications security. The key exchange protocol is ECDHE, while data encryption in transit utilizes the Advanced Encryption Standard (AES) (preferably at AES256-SHA384). Every session is secured using the Application Server's TLS certificate. The Application Server terminates the SSL connections that are established by the viewer and the presenter -- while a single viewer/presenter pair could potentially employ end-to-end encryption and use the Application Server as a simple networking relay, this becomes unfeasible when multiple viewers are present. As designed, the system supports multiple viewers without placing bandwidth constraints on the presenter. All join.me communications are secured using TLS, including access to the website itself.

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 operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of join.me.

4.1 Security Policies and Procedures

LogMeIn maintains and implements 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 2 attestation report for the join.me services
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LogMeIn's eCommerce and payment environments
- TRUSTe Verified 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 join.me 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 [3]. 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

To the extent LogMeIn Processes Personal Data [as such terms are defined in the LogMeIn Data Processing Addendum (DPA) located at the Resource Center at www.logmeininc.com/gdpr] on behalf of Customer in providing join.me, it shall do so in accordance with the requirements of General Data Protection Regulation (GDPR) directly applicable to LogMeIn in the provision of its Services.

5.3 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 [4]. Certification is reviewed annually by TRUSTe and any findings are promptly addressed by LogMeIn.

5.4 Return and Deletion of Customer Content

At any time, join.me Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available, LogMeIn will otherwise make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Additionally, Customer Content will be deleted within thirty (30) days of Customer request.

Upon the expiration or termination of a paid subscription to join.me, Customer's accounts shall revert to a free account. Free join.me accounts shall automatically be deleted after two (2) years of user inactivity (e.g. no logins). Upon written request, LogMeIn will certify to relevant account and Content deletion.

5.5 Sensitive Data

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

- 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 join.me.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.6 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 [3]

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 where 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., "join.je Architecture Whitepaper," 2018. [Online]. Available: https://az766929.vo.msecnd.net/document-library/joinme/pdf/english/jm-guides-architecture-v1.pdf.

[2] LogMeIn, Inc., "Terms of Service for LogMeIn and Goto Services," LogMeIn, Inc., February 2018. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

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

[4] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., November 2017. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.