CENTRAL / PRO

SECURITY AND PRIVACY OPERATIONAL CONTROLS

Central/Pro Security and Privacy Operational Controls (SPOC)

Publication Date: 1/9/2020

1 Products and Services

This document covers the security and privacy controls for LogMeIn Central/Pro.

LogMeIn 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. LogMeIn Central is offered as a premium service with multiple pricing tiers based on the number of computers supported and features desired.

LogMeIn 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 LogMeIn 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. LogMeIn Pro can be rapidly deployed and installed without the need for IT expertise.

2 Product Architecture

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

The LogMeIn Central/Pro application is composed of three key components that enable a successful remote access session: the client, the host and the LogMeIn gateway. The LogMeIn Central/Pro host is designed to maintain a constant TLS-secured connection with a LogMeIn gateway server located in one of the LogMeIn datacenters. After it establishes a secure connection to LogMeIn 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 LogMeIn Central/Pro gateway allows either the client or host (or both) to be firewalled, relieving users of the need to configure firewalls.

To learn more about Central/Pro architecture and security features, please see the LogMeIn Security Whitepaper [1].

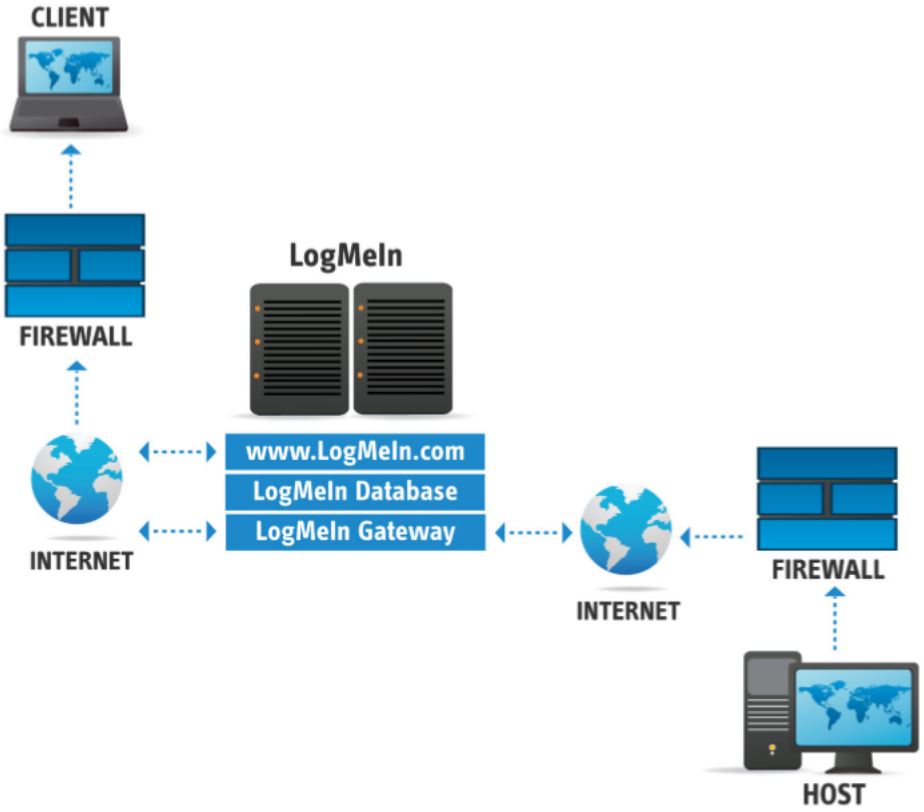

Figure 1. LogMeIn Architecture

3 LogMeIn Central/Pro Technical 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 [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 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 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

The LogMeIn 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.

Moreover, LogMeIn 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

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 datacenter
- Scheduled maintenance and validation of all critical security and environmental controls

LogMeIn 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. 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, Disaster Recovery, 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

LogMeIn 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 LogMeIn Central/Pro data centers, including Customer Content, is encrypted in transit. In addition, LogMeIn Central/Pro support sessions are protected with end-to-end 256-bit AES encryption.

3.7.2 At-Rest Encryption

LogMeIn Central/Pro encrypts all customer uploaded files (files, one-to-many) both using the underlying Azure blob storage technology and by a user specific key as well using 256-bit AES encryption.

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

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, and in order to ensure ongoing compliance.

4.2 Standards Compliance

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and maintains compliance with the following certifications and external audit reports:

- American Institute of Certified Public Accountants' (AICPA) Service Organization Control (SOC) 2 Type 2 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. These policies and procedures are designed to manage, identify and resolve suspected or identified security events across LogMeIn 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 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 on local applicable law, job responsibility, as well as 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. Further, mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team, on an on-going and annual basis.

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 expectations of its Customers and end-users very seriously and is committed to disclose its 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

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 [4]. 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, 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. 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, LogMeIn will certify to such Content deletion.

5.6 Sensitive Data

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

- Government issued identification numbers and image 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. One exception extends to explicitly identified payment forms and pages that are used my LogMeIn to collect payment for Central/Pro.
- Any information especially protected by applicable laws and regulation, which may include information about individual's race, ethnicity, religious or political believes, 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 [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 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

In order to ensure business continuity and that appropriate measures are in place which are 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.

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., “LogMeIn Security, An In-Depth Look”, LogMeIn, Inc., 2016. [Online]. Available: https://secure.logmein.com/welcome/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf.

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

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

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