RESCUE LIVE GUIDE

SECURITY AND PRIVACY OPERATIONAL CONTROLS

V1

February 4, 2020

LogMeIn Rescue Live Guide
Security and Privacy Operational Controls

Publication Date: 2/4/2020

1 Products and Services

This document describes the security and privacy controls for LogMeIn Rescue Live Guide.

Rescue Live Guide is a web-based support tool used by customer care professionals to provide remote visual guidance in the browser, without the need for adding a script to the supported website or downloading any software. With the permissions of the end-user, Rescue Live Guide allows a customer care professional to co-browse websites with the end-user in a secure way and provides guiding tools to the agent.

2 Product Architecture

LogMeIn Rescue Live Guide is a Software-as-a-Service (SaaS)-based visual engagement solution that connects that end-user and the agent in a cloud based secure browser.

Both the Agent and the end-user applications are web applications running in the users' supported browser of choice. The backends serving these applications are hosted in LogMeIn's Amazon Web Services (AWS) cloud, providing the peers with the means to connect with one another in a co-browsing session.

The session is created when an end-user initiates a shared browsing session. A session PIN is generated and displayed for the end-user at the start of the session. The end-user can let the Agent join the session by sharing the session PIN. Once a co-browse session is established between end-user and Agent, the supported website is loaded in an isolated headless browser in the LogMeIn cloud.

The actual web browsing, and all communication with the supported website, takes place in the cloud browser. The image is streamed to both users' web applications and the user actions are sent to back to be performed in the cloud browser.

The cloud browser instances are completely isolated and other than reporting data, recording (if enabled) and session information, data is purged after the conclusion of a co-browsing session.

You can learn more about the security measures of the solution in the next (Technical Security Controls) chapter of this document.

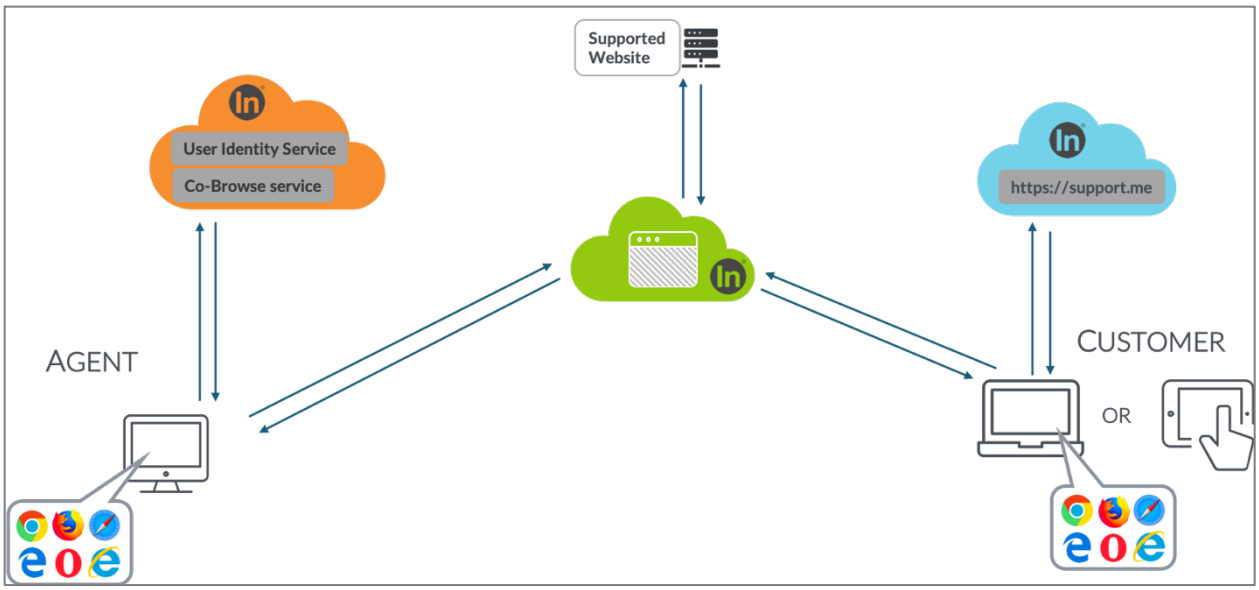

Figure 1- Rescue Live Guide Infrastructure

3 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.

3.1 Logical Access Control

Logical access controls are in place, designed to prevent or mitigate the threat 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.

Agents in Rescue Live Guide are tied to company accounts and are required to authenticate themselves using their username and a strong password. As an optional additional security measure, the account administrator can set up mandatory two-factor authentication for all agents under its account. The Agent Console can only be accessed after successful authentication.

The availability of additional services (such as reporting, recordings, account administration) for authenticated Agents/Admins can be controlled and limited with assigned roles.

3.2 End-user Protection

The privacy of end-users of Rescue Live Guide was kept in mind when creating this Service: the session PIN is owned by the end-user and a support agent can only join a session if the end-user has shared their session PIN with them. Additionally, the session PIN is company specific: a session initiated on a given website can only be joined by Agents who are part of the account assigned to the given supported website.

LogMeIn does not store the end-user content that is generated during the support session – as mentioned earlier, the cloud browser instances are completely isolated and other than reporting data, recording (if enabled) and session information, data is purged after the conclusion of a co-browsing session..

A *Stop* button is also available for the end-user during the whole support session -- the end-user can terminate the support session anytime by clicking this button.

3.3 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.

3.4 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.

3.5 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 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 datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.6 Data Backup, Disaster Recovery, Availability

The production datacenters utilize redundant high-speed network connections. There are pools of web and gateway servers across geographically distant datacenters. Load balancers distribute network traffic and maintain the availability of these servers in the event of server or datacenter failures.

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.

3.7 Malware Protection

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

3.8 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.

In-Transit Encryption

All network traffic flowing in and out of LogMeIn datacenters, including all Customer Content, is encrypted in transit. To provide protection against eavesdropping, modification or replay attacks, IETF-standard Transport Layer Security protocols are used to protect all communication between endpoints and our services. Our services support up to the following or better encryption protocols (as applicable): TLS 1.2, 2048-bit RSA, AES-256 strong encryption ciphers with 384-bit SHA-2 algorithm.

At-Rest Encryption

Rescue Live Guide configurations, session data and recording files are encrypted at rest with 256-bit AES encryption.

3.9 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.

3.10 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 Rescue Live Guide.

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 certifications and external audit reports:

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type 2 attestation report for the LogMeIn Rescue Service
- 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 Rescue Live Guide. 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

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 Services are 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 Rescue Live Guide 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 Rescue Live Guide for certain types of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded or generated to Rescue Live Guide:

- 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 Rescue Live Guide.
- 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 [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 party's 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," LogMeIn, Inc., June 2019. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[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., September 2019. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.