BOLDCHAT / BOLD360 / BOLD360AI
SECURITY AND PRIVACY OPERATIONAL CONTROLS

V2 October 2020

LogMeIn BoldChat/Bold360/Bold360ai Security and Privacy Operational Controls

Publication Date: October 2020

1 Products and Services

This document covers the security and privacy controls for LogMeIn BoldChat/Bold360/Bold360ai. These products are live chat, omni-channel and ai bot engagement services that help customer service staff directly engage with and assist visitors to their organization's website. Key features include bot conversation, real-time visitor monitoring, co-browsing, detailed reporting on chat activity and its overall effectiveness, the ability to define rules that automatically trigger the initiation of a chat window, the ability to route and distribute chats to improve efficiency, and the ability to monitor and manage customer conversations on various social channels, email and via SMS messages. BoldChat, Bold360 and Bold360ai offer multiple service tiers based on the number of engagements, users and features desired. Further, Bold360 provides valuable built-in integrations and open APIs to allow customers to streamline operations with all of their systems working together.

2 Product Architecture

BoldChat/Bold360/Bold360ai (collectively or individually, “Bold”) is a SaaS-based application delivered via a chat client and internet-based application server that writes to a database. The chat client functions inside the visitor's browser making https calls and maintaining a web socket connection to the application server. Agents connect using a .NET or web client over authenticated https to the same servers. Bold Customer Content (as the term is defined in LogMeIn’s Terms of Service [1]) is processed on database servers and stored in an encrypted form. See the Bold360 Architecture & Application Control whitepaper [2] for more information.

3 BoldChat/Bold360/Bold360ai 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 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.

Administrative controls set or restrict agent/user access to certain actions, setup areas, departments and folders.

The Bold operational system is only accessible with an authorized username (or email) and password combination. Usernames (and emails) must be unique throughout the entire Bold system, and minimum password length and complexity requirements are enforced. Enhanced password controls, including initial login reset, rotation, aging, non-reuse and incorrect password lockout, are available to administrators in the user configuration settings. Single Sign-On (SSO) integration is available to Enterprise subscribers using SAML 2.0-compliant user management systems.

User logins to Bold are logged and reported within the application. Access to these reports can be restricted using permission settings.

3.2 Perimeter Defense and Intrusion Detection

The LogMeIn on-premises and Bold components and services running on third-party cloud providers' network architecture is segmented into public, private, and Integrated Lights Out (iLO) management network zones. The public zone contains internet- facing servers. 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 Bold account. Only authenticated parties are granted access to relevant accounts.

New Bold customers can use the Data Residency Option to choose whether their Content will be stored in LogMeIn's on-premise United States or European data centers and third-party cloud providers' United States, European and Indian regions hosted and replicated in separate regions to meet cross-border data privacy and residency requirements.

3.4 Physical Security

Datacenter Physical Security

LogMeIn contracts with datacenters and third-party cloud providers 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 and third-party providers limits physical access to production data centers 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 on-premise 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

Bold has near instantaneous fail-over capabilities for most failure scenarios. The production datacenters utilize redundant high-speed network connections. There are pools of redundant servers across geographically distant data centers. Load balancers distribute network traffic among these servers and maintain the availability of these servers in the event of server or datacenter failures.

The Bold database is synchronized every five minutes to another data center. In addition, a differential back-up is completed nightly, and full backups are conducted every weekend. The backup database is stored with the same encryption as the original. Backups are retained on-premises for one week. In the event of a complete failure of the data center hosting the primary database, Bold is designed to be restored within fifteen minutes.

3.6 Malware Protection

Malware protection software with audit logging is deployed on all Bold 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. 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.

In-Transit Encryption

All network traffic flowing in and out of LogMeIn data centers, including all Customer Content, is encrypted in transit with 256-bit AES encryption.

At-Rest Encryption

Bold encrypts all Customer Content at rest with 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 operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of Bold.

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

LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certifications and external audit reports:

- International Organization for Standardization – ISO/IEC 27001:2013 Information Security Management System (ISMS) Certification
- 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 Bold. 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 expectations 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 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 [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 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. [4]
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[4]. Execution of the SCCs helps ensure that LogMeIn customers can freely move data from the EEA to the rest of the world.[4]

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.[4]

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 Bold 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 Bold for certain kind of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded or generated to Bold:

- 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 by LogMeIn to collect payment for Bold. Another exception is that LogMeIn allows customers to maintain PCI-DSS compliance, while using

Bold to process payments, through a third-party gateway, contingent on Customer's appropriate configuration of their Bold environment.

- Any information especially protected by applicable laws and regulation, specifically 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 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 http://support.logmeininc.com/ for general inquiries or privacy@logmein.comfor 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., "Bold360 Architecture & Application Control," 2017. [Online]. Available: https://www.bold360.com/it/resources/articles/datasheets/boldchat-architecture-and-application-control. [Accessed 5 March 2018].

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

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