bold360

ARCHITECTURE AND APPLICATION CONTROL

A technical overview of Bold360's security

Table of Contents

INTRODUCTION

LogMeIn offers consistently reliable service to its Bold360 customers and is vigilant in efforts to provide services that are not only robust and scalable, but also secure.

This document describes how we achieve reliable scalability and the measures taken by LogMeIn to protect Bold360 customer data. It explores each of the following:

- Network, data flow, and system access and restrictions surrounding the infrastructure including threat detection, data encryption, and incident response.
- Brief overview of the physical security of the data center including the environmental framework and security procedures.
- Application controls including login and password configurations, permissions, and data obfuscation.
- The internal policies and controls for LogMeIn employees and contractors including confidentiality agreements, privacy policies, background checks and training.
- The Bold360 Business Continuity plan and Disaster Recovery process.
- Our compliance with industry standards.

Network, Data Flow And System Access Restrictions

The Bold360 infrastructure enables LogMeIn to provide a highly scalable and reliable live chat service to customers all over the world. In fiscal 2016, the Bold360 service handled over 100 million chat sessions, tracked over 5.5 billion website visitors and helped manage several million emails. All public-facing elements of the Bold360 infrastructure are protected by firewalls configured to only allow https traffic. Configuration access to such infrastructure is limited to critical operations personnel

Reliability and Scale

LogMeIn has taken multiple steps to ensure service reliability and scalability:

- The Bold360 service is hosted in two US and two European based carrier-grade, geographically-diverse datacenters, located approximately 1,000 miles apart.
- Customers can select their desired data residency region where Content (formerly known as Service Data) will be stored, hosted, and replicated to meet cross-border data privacy and residency requirements.
- Within each data residency region redundancy is provided via the dual sites, each is designed to be capable of hosting the entire Bold360 service load independently.
- Application server arrays load balance the work; if one server fails, another automatically assumes the load. The application server architecture remains easily scalable; new hardware can come online quickly, as needed, though we believe that the current configuration could handle more than double its current load.
- Similarly, multiple high availability database clusters allow for scale and reliability while remain flexible enough to handle volume spikes.
- Data is replicated in near real time between the two in-region geographic locations, across a secure VPN.

Detection & Response

The Bold360 service is safeguarded against Distributed Denial of Service (DDoS) attacks through industry leading protection services.

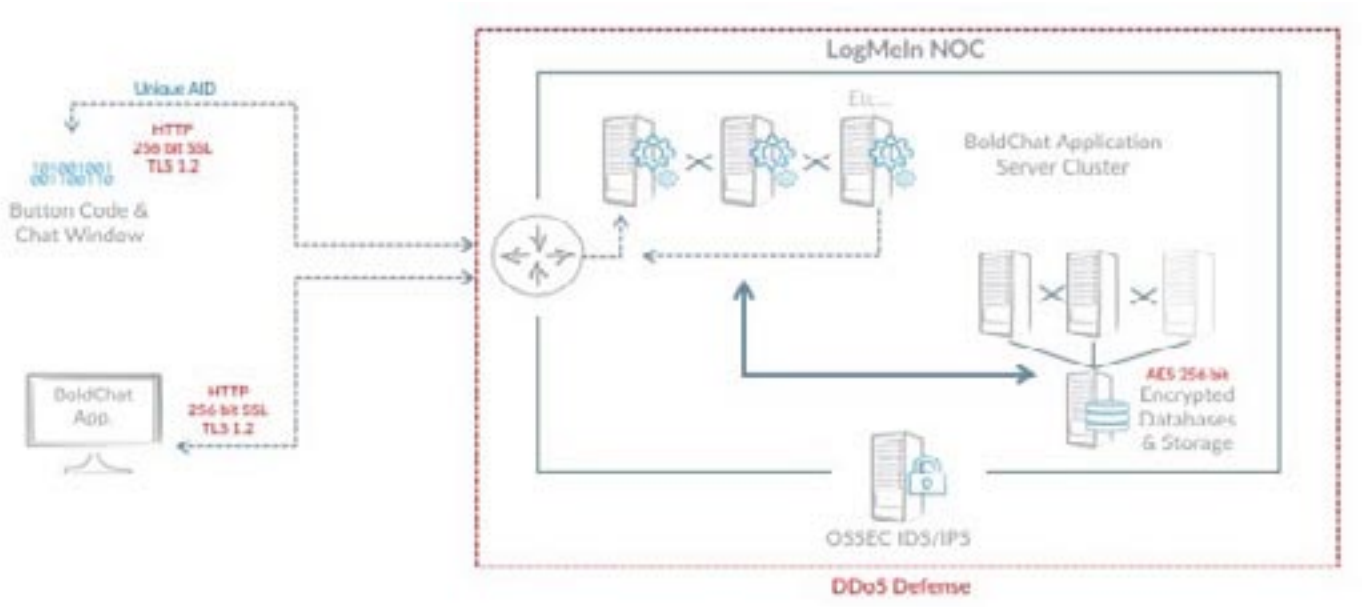
We utilize an omnipresent intrusion detection system (IDS), which is monitored by our Network Operations Center (NOC) team. Event monitoring is in place to detect when a fault condition is approaching or a service disruption occurs.

Additionally:

- A combination of internal and external (third party) monitoring services; Internal monitoring watches a variety of operational health metrics of our application server and database systems
- Dedicated tools for external monitoring of global accessibility and uptime of the service and;
- Support staff is notified of issues via email, call and/or text message so they can promptly investigate and initiate remediation.

Flow of Data and Encryption

Bold360's robust infrastructure facilitates fast data transmission without interruption while simultaneously ensuring data privacy; all data transmissions to and from Bold360 are encrypted using 256-bit TLS 1.2 (preferred). The chat service, for example, works as follows:



1. An agent logs in with a unique username and password combination into a Bold360 client application, establishing a persistent connection to the Bold360 servers in the LogMeIn data centers.

2. A website visitor launches a chat window, which sends an https request to the Bold360 service and establishes a separate persistent connection to the Bold360 servers.

3. Subsequent requests from visitor chat windows and agent client interfaces contain a unique Account ID (AID) and other relevant data; those requests go to the LogMeIn data centers and are handled by the Bold360 application servers.

4. Application servers bridge the agent and the visitor together. The Bold360 application does not open ports on local PCs and does not create a peer-to-peer connection.

5. Data is processed on databases running in an active/active/passive configuration and are bi-directionally connected to the application servers in real time. Data is stored on large storage devices and accessed when needed.

6. All customer data is also encrypted at rest via 256-bit AES encryption.

Data Centers

Bold360 is hosted in secure data centers that feature:

- Multilayer security control procedures, biometric entry systems and 24/7 closed-circuit video and alarm monitoring;
- Uninterruptible redundant AC and DC power, onsite backup power generators;
- HVAC redundant design with air distribution under raised flooring for maximum temperature control; and
- Smoke detection system above and below raised floor; double-interlock, pre-action, dry-pipe fire suppression.

Additional information about the data center facilities used to host the Bold360 service may be made available from LogMeIn, Inc. under a Non-Disclosure Agreement.

Application Controls

The Bold360 service itself includes user-configurable settings to help prevent unauthorized access to data. Many of these settings can be customized to better conform to a customer's workflow and security standards.

Login Policy

All Bold360 users are required to choose a username that is unique throughout the entire Bold360 universe. Bold360 is only accessible with an authorized username and a password combination.

- Changes of user login statuses are recorded each time a user logs into Bold360. These logs are reported and available within the application. Access to these reports can be restricted using the permission settings.
- Single Sign-On integration is available for Enterprise subscribers to simplify the login process. Any user management system that is SAML 2.0 compliant can be configured for Single Sign-On.

Password Policy

- Passwords must be at least eight characters long with alphabetic and numeric characters.
- Passwords are stored in database using a SHA-512 algorithm.
- This algorithm renders passwords invisible to everyone, including LogMeIn employees.
- Passwords can only be reset after logging in or utilizing a secure password reset routine.
- LogMeIn employees do not have direct access to customer passwords.

Enhanced password controls, including initial login reset, rotation, aging, non-reuse and incorrect password lockout, are available to administrators in the user configuration settings.

Permission-Based Controls

Administrative controls determine which features and folders an agent/user has access to. This can restrict or limit users from accessing certain actions, setup areas, departments and folders.

Data Obfuscation

Digital replacement within chat transcripts is available to replace potentially sensitive data, including digital strings like credit card numbers, social security numbers and telephone numbers with stored generic characters after a chat has been ended or in near real time. For example, a credit card number that looks like 1010-1010-1010-1010 will be replaced with: xxxx-xxxx-xxxx-xxxx within the chat transcript. If a customer's use of live chat may include disclosures (inadvertent or purposeful) of these types of digit strings which might jeopardize that customer's PCI compliance or may involve the disclosure of sensitive personally identifiable information, such as social security numbers, this capability should be enabled.

Internal Policies and Controls

Through attestation of documented policies, employee background checks and periodic training, the management and employees of LogMeIn understand the seriousness of, and their role in, securing the data of its customers.

Agreements and Policies

All LogMeIn employees and contractors are required to sign a Privacy and Confidentiality Agreement prior to hire. Additionally, all employees are required to agree to the following policies, among others:

- Internet Use Policy
- Email Use Policy
- Insider Trading Policy
- Code of Business Conduct & Ethics Policy
- Whistleblower Hotline Policy
- LMI Disclosure Policy
- Personal Information Disclosure

Background Checks and Access

All U.S. LogMeIn employees also undergo background checks prior to hire.

- All background checks include a Consumer Credit report, SSN trace, criminal check, education verification and sex offender search.
- LogMeIn reserves the right to periodically and randomly conduct additional background checks on their employees at any time.
- Restricted access to customer data is only given to

those employees that have a need to manage servers hosting customer data.

- Access is promptly revoked upon a LogMeIn employee or contractor departing from the company or reassignment to a different department.

In order to limit potential data disclosure, only a strictly limited and tightly controlled list of LogMeIn employees have root-level access to servers that host customer data. Accountability is designed for employees who have access to the systems that host customer data through:

- Documented username/password management
- Layers of audits via VPN account access logs

Security Software Development Life Cycle

The software development teams leverage an industry standard Security Development Lifecycle to ensure security by design. This includes among others: dynamic analysis, static analysis, threat modeling, and secure development training. As a leading SaaS company with security in our DNA, in addition to a dedicated Security team, each software development team also has a designated security champion responsible for executing on secure practices and rolls up to a broader organization-wide security chapter.

Data Management/Deletion

After a customer ends their Bold360 service, customer data is routinely purged. However, users also have the ability and control to delete their own data as they wish.

Security Review

LogMeIn's Security Team conducts monthly vulnerability assessments, and arranges for an annual thirty party penetration test of our systems.

Organized and documented security procedures, standards, and expectations are reviewed periodically and updated as needed or required.

Training

LogMeIn conducts initial training, annual refresher sessions, and ongoing education on all internal security policies and programs for employees.

An independent third party security assessment of the Bold360 service may be made available from LogMeIn, Inc. under a Non-Disclosure Agreement.

Business Continuity

The Bold360 infrastructure has been designed to ensure that the Bold360 service stays running in the face of a range of interruptions through the use of:

- A hardened and secured infrastructure
- Redundant hardware for both the application and database
- Geographic diversity
- Multiple routine backups
- Nightly backups are distributed across datacenters to provide off-site backup protection

Disaster Recovery

In the event a disaster occurs at one of LogMeIn's data center facilities, operations can quickly be failed over to redundant datacenters, which are designed to handle the full operational load.

Industry Standards

HIPAA/PHI/BAA

Bold360 users who work in the healthcare industry and/or provide healthcare-related services and who intend to utilize the Bold360 live chat service in a manner that may involve the disclosure and processing of certain Protected Health Information ("PHI") through the Bold360 service and the data centers used by LogMeIn to provide the Bold360 service should inquire further about executing a Business Associate Agreement with LogMeIn.

SOC 2

Bold360 is SOC 2 attested which assures clients we are using the proper controls to protect their important data. SOC 2, Service Organization Control 2 is extensive, based on multiple principles and criteria, testing the controls and processes that affect the security, availability of the systems used to process data and the confidentiality of the information processed by these systems. An annual review must be completed to maintain SOC 2 compliance.

As the "gold standard" for software companies that is widely recognized nationwide across industries, completing and maintaining the SOC 2 attestation is just one more way we demonstrate our commitment to security and privacy.

Safe Harbor Alternatives/Data Protection Laws

On October 6, 2015, the European Court of Justice issued a judgment declaring Safe Harbor as "invalid". So the EU Safe Harbor Framework is not a valid mechanism to comply with EU data protection requirements anymore. Regardless of the invalidation of Safe Harbor, LogMeIn offers many robust alternatives to Safe Harbor:

- Data Residency: Bold360 customers can leverage the Data Residency Option to choose whether their Content (formerly known as Service Data) will be stored in LogMeIn's United States or European data centers, hosted and replicated to meet cross-border data privacy and residency requirements.
- EU Model Clauses: please note that for some time we have offered our customers the EU Model Clauses for execution, by way of our Data Protection Addendum, to which the invalidation of Safe Harbor has no impact. The EU Model Clauses are time-tested and considered a superior legal mechanism for ensuring that any personal data leaving the EEA will be transferred in compliance with EU data-protection law and meet the requirements of EU Data Protection Directive 95/46/EC. More importantly, LogMeIn has invested in the operational processes necessary to meet the stringent requirements of the EU Model Clauses for the transfer of personal data to processors, which in turn allows us to provide our customers with contractual guarantees around the transfer of their personal data.
- Privacy Shield: LogMeIn strives to be a leading Software-as-a-Service company and has been working closely with a leading IT security and data privacy vendor to ensure that, to the strictest standards, we are internally compliant with Privacy Shield, certified by this vendor, and approved to list such certification by the US Department of Commerce. As such, while we are very close to finished with our work to certify for Privacy Shield, we believe that it will just be but one additional means for customers to utilize to ensure legal guarantees around their data and encourage our customers to utilize our Data Protection Addendum (that contains the EU Model Clauses), to which the invalidation of Safe Harbor and the introduction of Privacy Shield have had no impact.