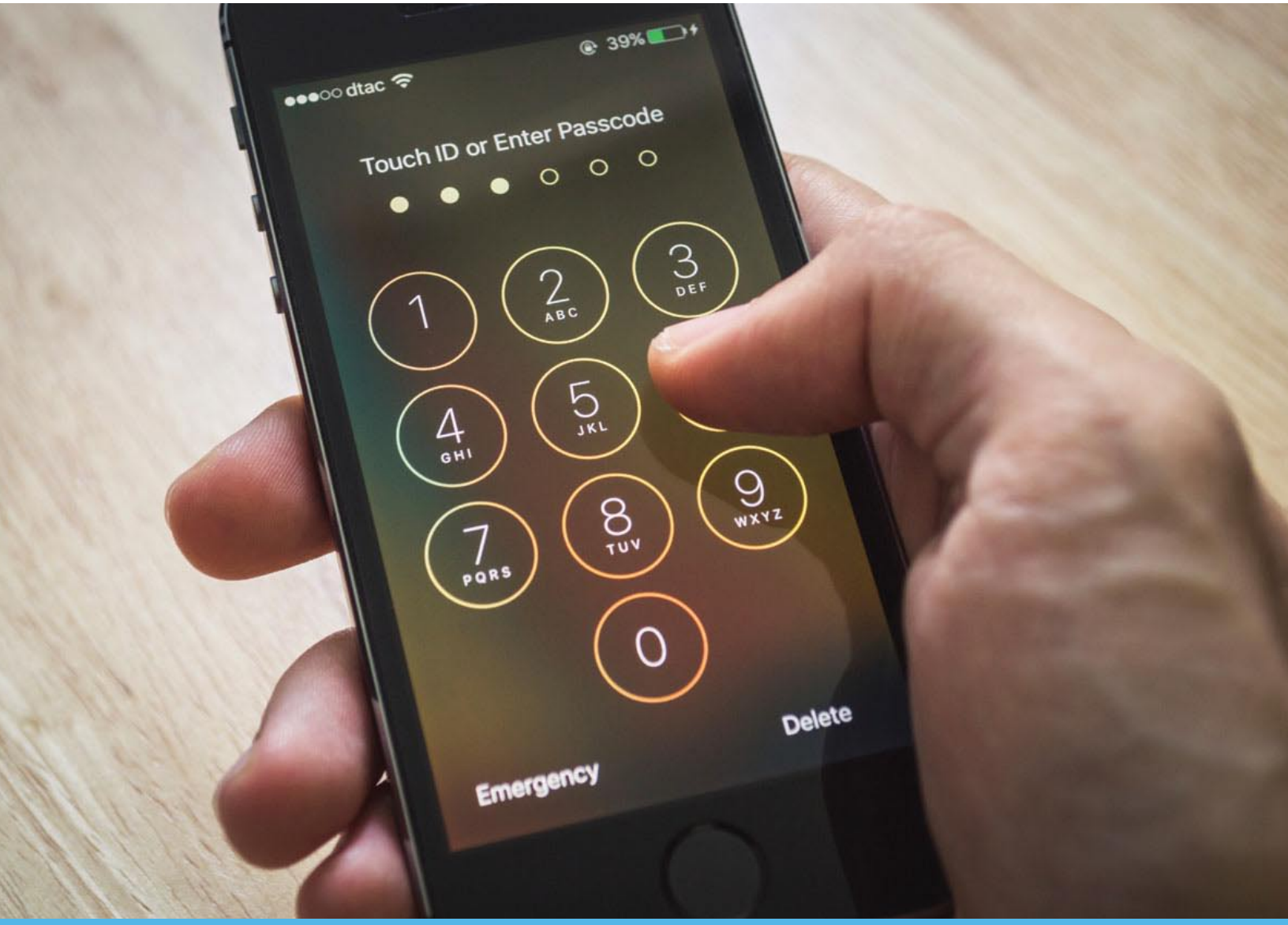
BOLDCHAT by LogMeIn

BOLDCHAT ARCHITECTURE & APPLICATION CONTROL

A technical overview of BoldChat's security.



WHITE PAPER

BOLDCHAT by LogMeIn

Key Benefits of BoldChat Security

- BoldChat service is hosted in two carrier-grade, geographically diverse datacenters designed to host entire service load independently
- Automatic load balancing ensures your application stays up and running
- All data transmissions are encrypted using 256-bit SSL
- Digital replacement within chat transcripts replaces sensitive data like credit card and social security numbers with stored generic characters

For More Information:
www.BoldChat.com
(866) 753 – 9933
info@boldchat.com

BOLDCHAT ARCHITECTURE

A technical overview of BoldChat's security.

Introduction

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

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

- Network, data flow, and system access and restrictions surrounding the infrastructure including threat detection, data encryption and security breach protocols
- Brief overview of the physical security of the datacenter including the environmental framework and security procedures
- Application controls including login and password configurations, permissions and data obfuscation
- The internal policies and controls for all employees and contractors including confidentiality agreements, privacy policies, background checks and training
- The BoldChat Business Continuity plan and Disaster Recovery process

Network, Data Flow and System Access Restrictions

The BoldChat infrastructure enables LogMeIn to provide a highly scalable and reliable live chat service to customers all over the world. In fiscal 2013, the BoldChat infrastructure handled more than 16 million chats.

Reliability and Scale

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

- The BoldChat service is hosted in two carrier-grade, geographically-diverse datacenters, located approximately 1,000 miles apart. Each site is designed to be capable of hosting the entire BoldChat 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
- The MS SQL database is configured as a centralized database with multiple servers and a standalone storage array
  - Data is replicated in near real time between the two geographic locations, across a secure VPN

Monitoring/Alerting

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.

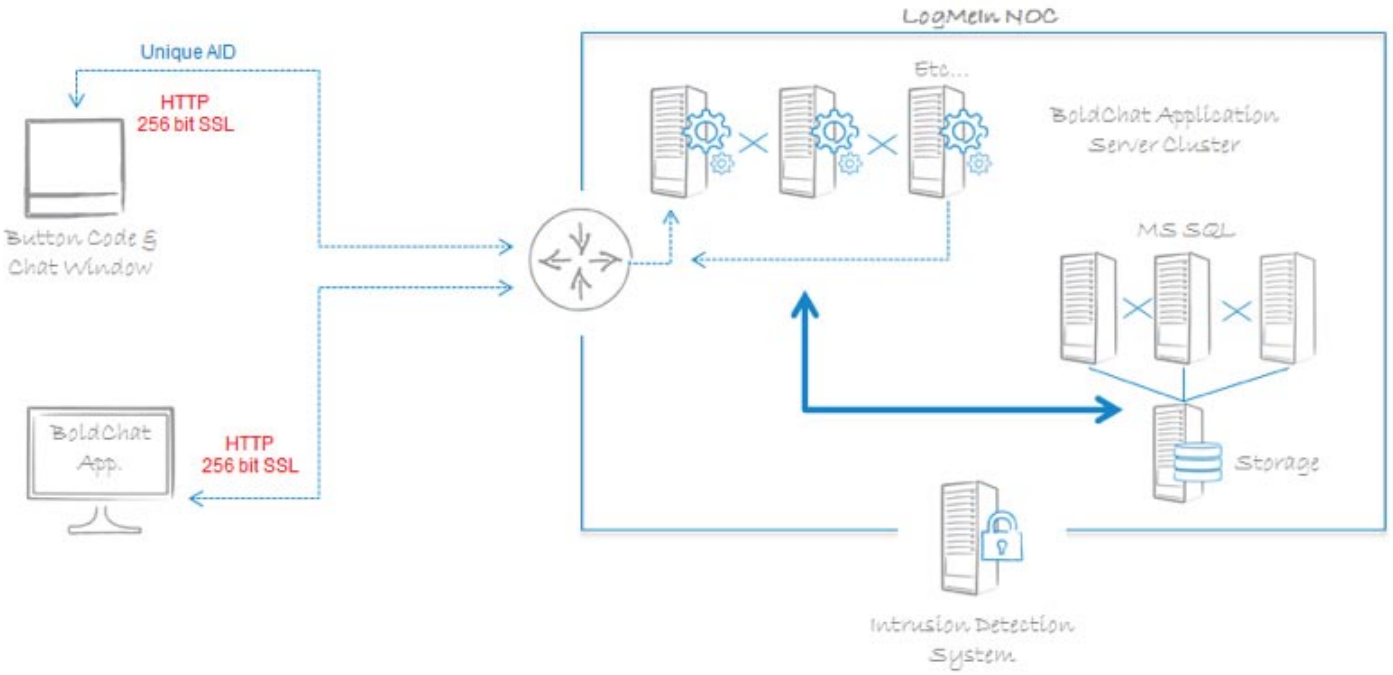
Additionally:

- We use a combination of internal and external (third party) monitoring
- Internal monitoring watches a variety of operational health metrics of our application server and database systems
- We use Alertra for external monitoring of global accessibility and uptime of the service
- Support staff is notified of issues via email, call and/or text message so they can immediately investigate and remediate

Flow of Data and Encryption

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

1. An agent logs in with a unique username and password combination into a BoldChat client application, establishing a persistent connection to the BoldChat servers in the LogMeIn NOC.
2. A website visitor launches a chat window, which sends an https request to the BoldChat service and establishes a separate persistent connection to the BoldChat 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 NOC and are handled by the BoldChat application servers.
4. Application servers bridge the agent and the visitor together. The BoldChat application does not open ports on local PCs and does not create a peer-to-peer connection.
5. Data is processed on MS SQL 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.



Data Centers

BoldChat is hosted in state-of-the-art, secure datacenters 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
- 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 BoldChat service may be made available from LogMeIn, Inc. under a Non-Disclosure Agreement.

Application Controls

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

- Changes of user login statuses are recorded each time a user logs into BoldChat. 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 a database using an SHA-512 hash 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 access to reset 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 operator has access to. This can restrict or limit operators from accessing actions, setups, 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.

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

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

Training

- LogMeIn conducts initial training, annual refresh sessions and ongoing education on all internal security policies and programs for those employees that have access to customer data
- Organized and documented security procedures, standards and expectations are reviewed periodically and updated as needed or required

Data Management/Deletion

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

Prevention of Security Breach

All public-facing elements of the BoldChat infrastructure are protected by firewalls configured to only allow http/https traffic on ports 80 and 443. Configuration access to these devices is limited to critical operations personnel.

Business Continuity

The BoldChat infrastructure has been designed to ensure that the BoldChat 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 occur to a backup server, which is housed inside the infrastructure
  - Backups are distributed across datacenters to provide off-site backup protection

Disaster Recovery

In the event that a disaster occurs at one of LogMeIn's datacenter facilities, operations can quickly be failed over to the other datacenter, which is designed to handle the full operational load.

Industry Standards

HIPAA/PHI/BAA

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

Safe Harbor Status

LogMeIn annually certifies to the U.S. Department of Commerce that it adheres to the Safe Harbor framework developed by the U.S. Department of Commerce and the European Union.

FOR MORE INFORMATION, VISIT BOLDCHAT.COM