# Table of Contents

**INTRODUCTION** ......................................................... 1  
**APPLICATION SECURITY** ............................................. 2  
**CHAT AGENT SECURITY** ............................................... 2  
**WEB VULNERABILITIES RESISTANCE** .......................... 4  
**CHAT AGENT SECURITY** ............................................... 5  
**PRIVACY AND DATA RETENTION** ............................... 6  
**MASKING NON-PUBLIC INFORMATION** ......................... 7  
**SECURE STORAGE** .................................................... 7  
**ENCRYPTED STORAGE** ............................................... 7  
**COOKIES** ............................................................. 8  
**INFRASTRUCTURE SECURITY** ......................................... 9  
**NETWORK SECURITY** .................................................... 9  
**CONTENT FILTERING** ................................................ 9  
**LOGICAL SECURITY** .................................................. 9  
**MONITORING** ........................................................ 10  
**OPERATIONS** .......................................................... 10  
**UPTIME, BUSINESS CONTINUITY AND DISASTER RECOVERY** ......................................................... 11  
**DATACENTERS** ........................................................ 12  
**SECURE AND TRUSTED SERVICE PROVIDERS** ................ 12  
**PHYSICAL AND ENVIRONMENTAL SECURITY** .................. 12
Introduction

When it comes to doing business on the Web, security is always a top priority. In order for the online marketplace to thrive, businesses and consumers alike need to be assured that their sensitive data is well protected. LivePerson offers a secure, reliable and trusted service and platform through which online businesses can safely communicate with their customers.

Due to the fact that breaches of security can pose major risks to contemporary e-businesses, LivePerson has implemented a multi-tiered approach to securing its services, which are governed by the following core principles:

- First-rate security can only be achieved through multiple layers that protect the physical infrastructure, network, application and system components.
- Technology solutions are only effective when coupled with strong internal security processes and well-trained personnel to oversee them.
- Security solutions must be robust and flexible in order to support customers’ evolving needs.
- With respect to the above, security vulnerabilities cannot be totally eliminated.

This document provides a high-level overview of how LivePerson maintains the highest possible level of security in all areas.
APPLICATION LEVEL SECURITY

CHAT SESSION SECURITY

The main service that LivePerson protects is live chat. This process includes monitoring visitors on any Web page that has been “tagged” with the LivePerson monitoring code, as well all chat sessions between your chat agents and visitors. This section describes how LivePerson secures all data throughout the live chat process.

LivePerson routinely collects data on visitors who browse Web pages tagged with LivePerson monitoring code. This data is collected for the purposes of determining which visitors to engage, which of your chat agents (i.e. skill group) should engage them, and when.

Data is transferred from the visitor’s browser to LivePerson’s Web servers using the protocol of the Web page itself (HTTP or HTTPS). Meanwhile, the Agent Console software deployed on your chat agents’ PCs continuously communicates with LivePerson’s Web servers, notifying it of each agent’s availability to accept chats.

When visitors request a chat via a click-to-chat button, the Web server forwards the request to the appropriate application server. Part of this process is accomplished through LivePerson’s proprietary Firewall application. Only valid requests will result in the initiation a chat session between your visitor and LivePerson’s application server.

Once the application server receives a valid request for a chat, it will initiate a parallel request with an appropriate and available chat agent. Both sides (visitor and chat agent) will then communicate in a chat session, each pulling the other’s chat text from LivePerson’s application server.

This architecture offers the following security advantages:

- The entire system and communications are based on standard HTTP (80) and HTTPS (443) protocols and ports. Visitors have no need to download or use any special protocols.
- Visitors do not need to install any software on their PCs as all communications are browser-based.
- No direct connections between your LAN and your visitor are required; All communication is handled and intermediated by LivePerson’s Web servers.
- Sessions are encrypted with 128 bit SSL V3, using a trusted public certificate authority (CA) to ensure the authenticity of LivePerson’s server to both parties.
- LivePerson’s proprietary firewall application filters all communication prior to establishing a chat session; therefore the risk of an external security attack is greatly reduced.
A high level view of LivePerson's chat dataflow is outlined below:

A high level view of LivePerson's architecture is displayed in the following diagram:
WEB VULNERABILITIES RESISTANCE

Convenience, familiarity, and broad availability make the Web an ideal platform for hosting applications. The Application Service Provider (ASP) and Software as a Service (SaaS) models provide maximum flexibility for the broadest swath of potential customers worldwide.

The challenge faced by all ASP-based services is to build security features directly into the application itself rather than relying on third-party systems to protect its services. And while security must be tight, it cannot interfere with the usability and performance of the application itself.

This section shortly describes the main security mechanisms embedded within LivePerson’s applications.

**Trusted Domains**

The LivePerson application has the ability to distinguish between known (and therefore trusted) domains and unknown domains. Every LivePerson customer may opt to create a whitelist of trusted domains, thus restricting connections to those domains only. This feature is helpful to customers who need the ability to re-direct visitors to multiple domains (for instance, guide a visitor to a country-specific domain). It prevents visitors from being redirected to a non-trusted domain for nefarious purposes.

**Restricted Redirection**

Many LivePerson customers need the ability to re-direct their visitors to sister websites. To protect against the threat of phishing during a re-direct, LivePerson customers can create a “whitelist” of approved sites for redirection. The whitelist ensures that your visitors will not be sent to a malicious site while using the LivePerson application.

**Content Filtering**

Without proper precautions, use of a Web application can expose visitors to vulnerabilities such as Cross Site Scripting (XSS), a form of attack that injects malicious content into the visitors’ browsers. LivePerson prevents such attacks through content-filtering capabilities that are embedded directly into the application. LivePerson customers can enable this feature to block scripts and other potential malicious content from running on their chat agents’ consoles, as well as in their visitors’ browsers.

**IP Restrictions**

One of the simplest ways to stop unauthorized users from gaining access to your system is to create a predefined list of IP addresses that are authorized to access your LivePerson account. The LivePerson application enables customers to define a range of IP addresses from which a connection to the application is allowed. This restriction is enforced whenever a chat agent attempts to access the application.
CHAT AGENT SECURITY

User management is fundamental to any security strategy. User authentication, user permission levels, and activity audit trails are all vital tools for maintaining excellent security. The LivePerson application enables customers to define the level of security within the application so that it meets the standards set by the customer’s own internal security policy. This section describes the user management features that are available within the LivePerson application.

Login Policy

User Authentication and Authorization

Direct users of the LivePerson platform are the chat agents and administrators who access the system. Each user is assigned a unique user account and specific authorization & permission level, as controlled by the account administrator. Each user’s authorization level can be configured to match his or her business requirements (i.e. Chat agent, Chat administrator, Supervisor).

Password Policy

Operators and users authenticate to LivePerson with site ID, username and password. The password policy is configurable, and can be customized to match your organization’s corporate password policy.

Authentication is established over 128bit SSL V3 HTTPS encrypted protocol and passwords that are subsequently stored in the database are encrypted with a Hash algorithm.

The following attributes in the password policy are configurable:

- Password length
- Password complexity
- Password history
- Password expiration time
- Failed password entries allowed
- Restrict commonly used password

Password and Operator lock-out

To prevent brute force attacks, LivePerson customers can opt to lock an operator account after multiple failed login attempts. The number of failed logins and the interval at which the lock-out is reversed are both configurable according to the customer's organizational policies.

The LivePerson platform supports a session lock-out mechanism to prevent unauthorized use of the application whenever a legitimate user has stepped away from their workstation. Same as other login policy options, the lock-out time is configurable.
Audit Trail and Logs

Users’ activity within the LivePerson platform is monitored and logged, enabling configuration changes and security-related activity within the application to be traced and attributed to a specific user, date and time. The activity logs apply for all types of users (chat agents, chat administrators, supervisor, etc.) and allow LivePerson customers to extend their control and auditing policies to the LivePerson platform.

PRIVACY AND DATA RETENTION

Data collected by the application

As an Application Service Provider, LivePerson collects information from visitors on behalf of customers. Unless configured otherwise, LivePerson logs the visitor’s browsing information (e.g. IP addresses, browser types, referring page).

In addition, LivePerson customers can opt to deploy a pre-chat and exit survey; both are optional and configurable. If deployed, the survey prompts visitors to provide information about themselves as configured by the site admin (e.g. name, email, phone). Visitors may enter their names in whatever format or detail they like (e.g. “Rick,” “Jones, Rick” or “Rick Jones of XYZ Corporation”).

All data collected on your visitors can be encrypted using a Triple DES algorithm. You may encrypt all of the data, or just portions of it, such as the visitor’s name and email address.

At the conclusion of the chat, the application prompts the visitor to complete an exit survey in order to obtain his or her feedback regarding the experience. LivePerson customers may opt to ask for contact information (e.g., email address), demographic information (e.g., zip code, age or income level) and level of satisfaction. Visitors are not required to complete the survey; it is completely voluntary.

LivePerson customers who do not wish to present their visitors with an exit survey may request that the survey be removed.
MASKING NON-PUBLIC INFORMATION

All information handled by LivePerson is considered private and subjected to the highest level of security. LivePerson has the ability to support your organization’s security and privacy requirements, e.g. Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA).

For example, you can opt to define every string of numbers in credit-card format as data that requires masking. In such cases, the credit card number will be replaced with a string of characters when it is transferred to the LivePerson database. Thus, 1111-2222-3333-4444 will become ****-****-****-****. The masking process is irreversible and once executed, the data will no longer be available in its original format. Note: many of LivePerson’s customers are using the masking feature to help support PCI-DSS requirements.

SECURE STORAGE

All chat transcripts and visitor information gathered from the LivePerson monitor tag on your website are stored within LivePerson’s database servers for a 13 months period. Each Liveperson customer is assigned with a unique site ID, and the access control mechanisms embedded in the application and in the DB prevent unauthorized access. Although it may be stored on shared database servers, the data is logically protected and segregated in a way that ensures only authorized entities will be able to access it.

ENCRYPTED STORAGE

Encryption is the final layer of protection. It is implemented in order to prevent potential attackers who may have gained access to your information from actually using it.

LivePerson has built an encryption mechanism directly into the application. The embedded cipher mechanics within the application code enable our customers to encrypt the data stored in the database (including transcripts and visitor information). Encryption keys are unique for each customer, and the key management / generation is configurable to align with your organizational security standards. The encryption is done by the application and not by the DB.
What can be encrypted?
LivePerson has the ability to encrypt chat transcripts, survey answers and “custom variables” (all or some of the information gathered on visitors who enter a monitored Web page).

Encryption Algorithm:
LivePerson uses Triple DES (3DES) encryption. 3 64-bit binary digits combined by a mathematical algorithm into one 192 binary digit key. The Triple DES algorithm is a well-accepted encryption method used by leading companies. The advantage of using a well-known encryption algorithm is that it has been subjected to numerous penetration tests and improvement processes by the community of encryption experts.

Key Management
Management of the encryption keys is as important as the encryption itself. LivePerson’s key management strategy focuses on secured key generation and storage, utilization of a unique encryption key for each customer, limited and controlled access to stored keys, segregation of duties between encryption and decryption permissions and re-generation of keys in compliance with your security requirements.

COOKIES
As is the case with all other Web-based applications, the LivePerson application uses cookies to identify users and user sessions. Standard LivePerson deployments use third-party cookies, meaning that the visitor’s browser will recognize it as a LivePerson cookie. LivePerson can also support first-party cookies, meaning that your visitor’s browser will recognize the cookies as belonging to your site, not LivePerson’s. Note: some browsers allow the user to deny third-party cookies as a security precaution. In such cases, you will not be able to engage with those visitors.

LivePerson customers may choose the type of cookie to use: persistent or session-only. The advantage of persistent cookies is that they allow you to recognize repeat visitors and visitors who have chatted with your company in the past.

Some organizations, however, have security policies that prohibit persistent cookies and can request that cookies be set to session-only. When session-only cookies are used, all the data about your visitors will be removed once those visitors end their sessions (i.e. leave your site).

LivePerson cookies can be marked as “secured” upon your request, which would ensure that cookies are only sent on an encrypted connection (HTTPS).
INFRASTRUCTURE SECURITY
LivePerson’s network, infrastructure and architecture have multiple protection layers that ensure the highest levels of efficiency, security and control. These layers include:

- Network and communication security, including firewalls and access control lists
- Content filtering and validation via LivePerson’s proprietary application Firewall
- Logical security, including access control to all media and systems, server hardening, and patch management
- 24/7 network, infrastructure and service monitoring

NETWORK SECURITY
All communication with the outside world passes through access-list enabled routers. This configuration blocks the majority of nefarious or unwanted traffic, as well as network-based attacks. It also serves to protect the next layers of security mechanisms from overload.

Traffic that has been allowed to pass through the routers is screened by multiple sets of network firewalls ensuring that only legitimate protocols are used, and that session integrity is maintained. Only HTTP and HTTPS protocols are allowed into or out of LivePerson’s service network. The firewalls direct acceptable protocols to the servers, and block all others.

CONTENT FILTERING
As described earlier, LivePerson provides an additional layer of security via the application Firewall; a proprietary application installed on the Web server. This application checks every HTTPS request entering LivePerson’s Web server prior to forwarding the request to the application server.

By maintaining multiple layers of communications security and limiting the protocols that may be used for incoming and outgoing communication, LivePerson is able to sustain a high standard of security and service reliability.

LOGICAL SECURITY

Access Control:
LivePerson devotes a great deal of effort to ensuring that one customer cannot see or access another’s data. Customer data is logically protected and segregated in a way that ensures only authorized entities are able to access it. Access Control mechanisms have been implemented to efficiently support this goal, and are specifically tested as part of the standard penetration testing process.

Patch management and server hardening:
Because security vulnerabilities are inherent in many industry-standard software, systems and applications, LivePerson has implemented robust patch management and server hardening processes. Patches are rolled out following a strict approval and testing policy. LivePerson has established security policies for the servers within its network and application.
Anti-Virus
Where technically applicable, LivePerson uses a leading real-time anti-virus solution to protect its servers against viruses, worms, Trojan horses and other forms of malicious code that may cause damage.

MONITORING
LivePerson’s security plan includes provisions that enable us to identify and act upon potential security incidents. Our Network Operations Center (NOC) monitors network, application and server infrastructure elements on a 24/7 basis. In the event of a potential breach, the NOC immediately alerts the appropriate teams who can assess and address the situation without delay.

The combination of constant monitoring with the well-defined plans-of-action for potential security incidents enables LivePerson to ensure the security of the network, the application, and our customers’ data.

OPERATIONS

Organizational Security:
A full-time dedicated security team headed by a Chief Security Officer (CSO) is responsible for ensuring that all aspects of security adhere to the highest standards, and that effective security controls are embedded and enforced in relevant processes within LivePerson. Additionally, LivePerson has established and implemented a comprehensive set of Information Security policies and procedures. The operational controls are strictly audited for effectiveness by a third-party big-four audit firm on an annual basis, in a SSAE16 SOC 2 Type II audit.

Change Management:
Changes to LivePerson’s environment and service are only executed within a defined maintenance window, after a coordination process that includes obtaining the appropriate authorizations and approvals from various factors based on segregation of principle duties.

Penetration Testing:
LivePerson’s application and network are tested for security vulnerabilities by independent security experts as part of the secure development lifecycle. The tests include an array of penetration scenarios. In addition, the LivePerson platform and service are tested and scanned on a daily basis for thousands of common hacker vulnerabilities.

Secure Development Training:
LivePerson’s security awareness program includes a Secure Development training for R&D teams, based on the Open Web Application Security Project (OWASP) vulnerabilities.
Personnel and HR Security:
LivePerson employees are an essential component to the security of the network, application, and customer data. Reference and background checks are performed for every employee in compliance with applicable laws, regardless of the position for which they are hired. LivePerson’s Ethical Code of Conduct and mandatory compliance training ensure that all employees conduct themselves in a highly professional manner, particularly in regards to customer data.

LivePerson leverages confidentiality clauses and non-disclosure agreements in employee contracts to ensure that intellectual property and internal operational information remain within the company.

UPTIME, BUSINESS CONTINUITY AND DISASTER RECOVERY

Capacity and uptime
LivePerson’s multi layered infrastructure was designed with the appropriate capacity to manage large scale traffic and C.P.S (Connections per Second) to allow highly available service for our customers. Between the years 2008-2010 LivePerson achieved a yearly 99.95% uptime.

Disaster Recovery and BCP
LivePerson’s disaster recovery plan ensures that our customers experience almost no interruption of service in the event of a loss of data occurring at our main datacenter.

In case of complete failure of the primary datacenter, LivePerson will continue serving its customers from an alternate Disaster Recovery (DR) site. The transition will not require any changes on the part of our customers. Failure scenarios and activation of DR site are tested on regular basis in accordance with LivePerson’s Business Continuity Plan (BCP).

LivePerson maintains standby DB servers and backups of the data in a separate location. Encrypted channels (VPN) connect the two systems, ensuring that all data is backed up on a regular basis. No backup tapes or external media is utilized for backups. All hardware elements and software configurations are state-of-the-art and redundant.

Service Interruption Notifications Based on the account size, type of deployment and agreed services level agreements - Enterprise level customers are notified within 1 hour after internal LivePerson confirmation that a service disruption has occurred.

This level of readiness ensures that our customers are secure, while also being offered a high availability of service.

Service Interruption Notifications
Based on the account size, type of deployment and agreed services level agreements - Enterprise level customers are notified within 1 hour after internal LivePerson confirmation that a service disruption has occurred.

This level of readiness ensures our customers not only secure but also high availability of service.
DATACENTERS

SECURE AND TRUSTED SERVICE PROVIDERS

LivePerson’s services are hosted in advanced datacenters operated by recognized industry leaders (Equinix and Digital Realty Trust). LivePerson has a primary and backup datacenters in the United States and Europe. LivePerson selected these vendors based on their proven leadership in hosting services for high-capacity businesses. Our vendors adhere to the highest industry standards of quality, security and reliability. Their commitment to excellence enables LivePerson to deliver 24-hour service, 365 days a year to our customers.

The primary datacenter in the United States is located in Ashburn, Virginia. The Disaster Recovery site is located in Oakland, California. The primary datacenter in Europe is located in London, England and the Disaster Recovery site is located in Amsterdam, the Netherlands. By storing the application and the data in multiple locations, LivePerson is able to ensure continuous service in the event of power disruptions or natural disasters that may occur in a specific region.

PHYSICAL AND ENVIRONMENTAL SECURITY

LivePerson’s datacenters utilize an advanced array of security equipment, techniques and procedures to prevent unauthorized access to its facilities. LivePerson’s servers are located in a private, restricted cage with biometric access control system. Any access to the cage is monitored and recorded.

To protect the integrity of its systems, most of the security controls within the datacenters are confidential. Some of the more visible measures include:

- Excellent exterior & interior intrusion and tamper-prevention systems
- Advanced array of closed circuit TV camera and recording systems (CCTV)
- 24/7 security officers on site
- Comprehensive security audits and tests
- Strict security policies

Specifications for each of these security aspects can be found in LivePerson’s SAS 70 Type II audit report, as well as in the SAS 70 Type II reports of those hosting vendors that have undertaken these audits.

All LivePerson datacenters are built to effectively withstand natural disasters (e.g. fire, flood, earthquakes). In addition, to minimize potential service interruptions caused by power outages, power is delivered via distributed redundant UPS systems, backup batteries and independent diesel generators.