
JANUARY 2008

LivePerson: Security Model and Policy

This document is for informational purposes only. LIVEPERSON, INC. PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of LivePerson, Inc., except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. Actual savings or results achieved may be different than those outlined in the document. This document could include technical inaccuracies or typographical errors.

Timpani, SmartBar and LiveCall are trademarks or registered trademarks of LivePerson, Inc. in the United States and/or other countries. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Table of Contents

Introduction	1
Application Security	2
Chat Session Security	2
Web Vulnerabilities Resistance	3
Chat Agent Security	4
Privacy	5
Encrypted storage	6
Infrastructure security	7
Secure and trusted service providers	7
Physical / Environmental security	7
Network security	7
Personnel security	8
Operations	8
Disaster Recovery	8

This document is for informational purposes only. LIVEPERSON, INC. PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of LivePerson, Inc., except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. Actual savings or results achieved may be different than those outlined in the document. This document could include technical inaccuracies or typographical errors.

Timpani, SmartBar and LiveCall are trademarks or registered trademarks of LivePerson, Inc. in the United States and/or other countries All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Introduction

Security is top of mind to all parties who buy or do business on the Web. In order for the online marketplace to thrive, visitors need to be assured that their sensitive data is well protected. To help provide peace of mind, LivePerson offers a secure, reliable and trusted service through which retailers, banks, and other online entities can communicate with their customers.

Because breaches of security can pose major risks to contemporary e-businesses, LivePerson has implemented a multi-tiered approach to securing our services. Our policy is driven by the following core principles:

- There are no silver bullets for eliminating security vulnerabilities. Excellent security can only be achieved through multiple layers that protect the application, the physical infrastructure, and provide for disaster recovery
- Technology solutions are only effective when coupled with strong internal security processes and well-trained personnel to complete them
- Security solutions must be robust and flexible in order to support our clients' evolving needs

LivePerson's security model revolves around three main axes:

1. Application Security
2. Infrastructure Security
3. Policy & Operation Security

This document describes LivePerson's implementation of these mechanisms to maintain a highest possible level of security in all layers.

1 Application Security

1.1 Chat Session Security

The main service we protect is LivePerson's live chat. This process includes monitoring visitors on any Web page that is tagged with 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 click on 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.

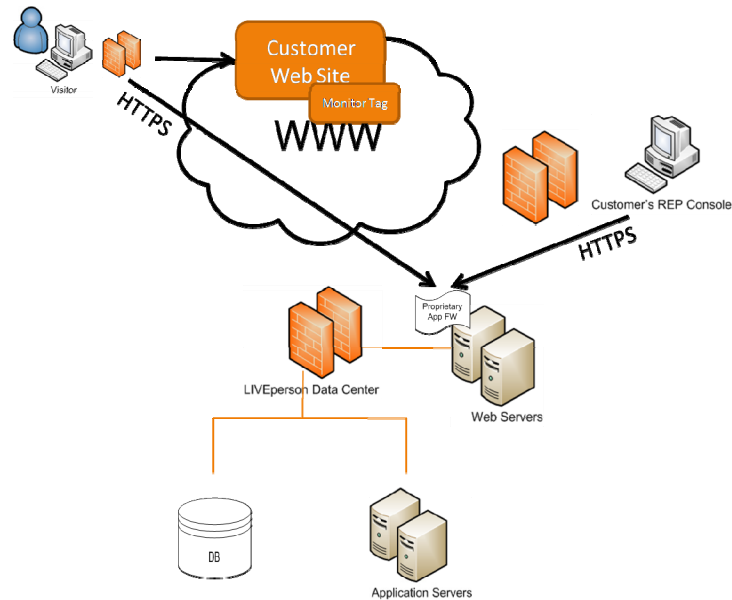
Data is transferred from the visitor's browser to our Web server using the protocol of the Web page itself (HTTP or HTTPS). Meanwhile, the Agent Console software deployed on your chat agents' PCs continuously communicates with LivePerson's Web server, notifying it of each agent's availability to accept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

When visitors request a chat via a click-to-chat button, the Web server forwards the request to the appropriate (i.e. correct skill group) application server. Part of this process is accomplished through LivePerson's proprietary application known as FW ©. 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 then initiate a parallel chat session 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 uses standard HTTP and HTTPS protocols using the standard ports 80 and 443. Visitors have no need to download or use any special protocols
- All sessions are encrypted with SSL V3 using a VeriSign certificate to ensure the authenticity of LivePerson's server to both parties
- Visitors have no need to install any software on their PCs; all communication is handled via common browsers
- No direct connections between your LAN and your visitor are required; all communication is handled by LivePerson's Web servers
- Because the FW© proprietary application filters all communication prior to establishing a chat session, the risk of an external security attack is greatly reduced



1.2 Web Vulnerabilities Resistance

Convenience, familiarity, and broad availability make the Web an ideal platform for hosting applications. The ASP model provides 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 describes the main security mechanisms embedded within LivePerson's application.

- **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 list 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-redirect, LivePerson customers can create a "white list" of approved sites for redirection. The white list 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-based application can expose visitors to Web-based vulnerabilities such as Cross Site Scripting, 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 script or any other content from running 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 may access your LivePerson application.

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 by the application server whenever a chat agent accesses the application.

1.3 Chat Agent Security

User management is fundamental to any security strategy. User authentication, user permission levels, and activity audits are all vital tools for maintaining excellent security. The LivePerson application enables our customers to define the level of security within the application so that it meets with the standards set by their own internal security policy.

This section defines the user management features that are available within the LivePerson application.

Password and Login Policy

- **User authentication and authorization**

Direct users of LivePerson's application are the chat agents and chat administrators who will access your system. Each user is assigned a unique user account and authorization level.

Users log in to the application using a username and password. The password policy for users is configurable, and can be customized to match your company's corporate password policy. Features available for configuration include:

- Password length
- Password complexity
- Password history
- Password expiration time
- Failed password entries allowed

All client-server data is exchanged via the SSL VS encrypted protocol, and all passwords that are subsequently stored are encrypted with Hash algorithm in the database.

Each user's authorization level can be configured to match his or her business requirements (i.e. chat agent, chat administrator, supervisor, etc.). And all users are associated to the specific LivePerson client by whom they're employed, thereby restricting access to chat sessions and data belonging to their company only.

- **Password/Operator lock-out**

To prevent brute force attacks, LivePerson customers can opt to lock an account after multiple failed entry attempts. Customers can choose the number of failed entries as well as the interval at which the lock out is reversed according to their internal policies.

The LivePerson application supports a session lockout mechanism to prevent unauthorized use of the application whenever a legitimate user has stepped away from his or her computer. Customers can configure the lock-out time to adhere to their own security and password requirements.

- **User activity auditing**

The activity of all users (chat agent, chat administrator, supervisor, etc.) is monitored and logged, enabling all configuration and security-related activity within the application to be traced and attributed to a specific user, date and time.

The activity log allows LivePerson customers to extend their control and auditing policies to the LivePerson application. Security events are monitored by LivePerson's operations center (see section 2.5 for complete discussion).

1.4 Privacy

- **Data collected by the application**

Customers can choose to deploy a pre-chat and exit survey; both are optional. If deployed, the LivePerson application prompts visitors to provide information about themselves via a pre-chat survey and an exit survey. All data collected on your visitors may 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.

If deployed, the pre-chat survey prompts visitors to enter their names. Visitors may enter their names in whatever format or detail they like (e.g. "Rick," "Jones, Rick" or "Rick Jones of XYZ Corporation). Additionally, LivePerson customers can configure their LivePerson application to prompt for detailed information regarding the nature of the visitor's concern or need to chat.

At the conclusion of the chat, the application requests 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.

The LivePerson application also logs the visitor's browser information (e.g., IP addresses and browser types).

- **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 first party cookies, meaning that your visitor's browser will recognize the cookies as belonging to your site, not LivePerson's.

You can opt to set your cookies to third party, meaning that the visitor's browser will recognize it as a LivePerson cookie. 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 if you set the LivePerson cookie to third party.

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 companies, however, have security policies that disallow persistent cookies. If that is the case with your company, you can request that your cookies be set to session-only. When session-only cookies are used, all data about your visitors will be removed from the LivePerson database once those visitors end their sessions (i.e. leave your site).

LivePerson cookies can be marked as "secured" upon your request. Securing the mark ensures that cookies will be sent only on an encrypted connection (HTTPS).

- **Masking non-public information**

All information handled by LivePerson is considered private and subjected to the highest level of security. As a service to our customers, we will support your company's security and privacy requirements (e.g. Gramm-Leach-Bliley or PCI).

LivePerson does not store non-public information in our databases. If your chat application collects private information from your visitors, it will be masked prior to transfer to our databases.

To accomplish this goal, LivePerson has developed a masking mechanism that will change every string of information defined by you as non-public (such as credit card or social security numbers) to characters that have no special meaning (i.e. ###, **).

For example, you can opt to define every string of numbers that's formatted as a credit card number 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 ****_****_****_****.

Once the non-public data is transferred to the LivePerson database it will no longer be available in its original format (in other words, you will not be able to retrieve a visitor's credit card information from the LivePerson database).

Note: many of LivePerson's clients within the financial sector are using the masking feature to comply with the PCI act.

All chat transcripts and visitor information gathered from the monitor tag on your website are kept within LivePerson's database and are available for your needs only.

1.5 Encrypted storage

Encryption is the final layer of protection. It is used to stop attackers who may have gained access to your information from actually using it.

LivePerson has built an encryption mechanism directly into our application. We have embedded cipher mechanics within the application code, enabling our customers to encrypt all data stored in the database (including transcripts and visitor information) and to manage re-generations of the key to align with their security standards.

- **What do we encrypt?**

LivePerson has the ability to encrypt the following types of information:

1. Chat transcripts – enables encryption of all chat transcripts
2. Custom variables – enables encryption of all or some of the information gathered on a visitor who enters a monitored Web page
3. Survey answers – enables encryption of survey information provided by your visitors

LivePerson uses Triple DES (TDES) as the encryption algorithm, 3 64-bit binary digits combined by mathematical algorithm to one 192 binary digits 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:

1. Secured key generation and storage
2. Limited and controlled access to stored keys
3. Segregation of duties between encryption and decryption permissions
4. Re-generation of keys in compliance with your company's security requirements

Infrastructure security

1.6 Secure and trusted service providers

The LivePerson application runs in a hosted environment. LivePerson has selected geographically-dispersed hosting facilities, located in Virginia, Texas and the UK. Our hosting service providers are NTT/Verio and Rackspace.

All of LivePerson's hosting providers undergo SAS-70 testing and certification, and are considered the best in their fields. Their standard of service, availability and physical security is outstanding, allowing LivePerson to provide a steady, reliable and secure application to its clients.

By storing its application and data in multiple locations, LivePerson is able to provide continuous service in the event of power disruptions or natural disasters that may occur in a specific state or region.

1.7 Physical / Environmental security

As stated above, LivePerson's application and data are hosted in multiple hosting facilities throughout the world. These facilities provide:

- Excellent perimeter security
- Physical intrusion and tamper prevention
- Protection against power outages, fire and natural disasters

Specifications for each of these security aspects can be found in the SAS 70 type II report for each of the hosting service providers.

1.8 Network security

LivePerson maintains the highest level of security and control over our network and communications infrastructure.

All communications with the outside world pass through access-list enabled routers. This feature 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 firewall, ensuring that only legitimate protocols are used, and that session integrity is maintained.

Only the HTTP and HTTPS protocols are allowed into or out of LivePerson's network. The firewalls direct acceptable protocols to the servers, and block all others. They also protect against Denial of Service and flooding attacks, thereby eliminating unnecessary stress from the Web and application servers.

LivePerson provides an additional layer of security: a proprietary application, installed on the Web server, checks every HTTPS request entering our Web server prior to forwarding the request to the application server.

By maintaining multiple layers of communication-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.

1.9 Personnel security

LivePerson employees are an essential component to the security of the network, the application, and all customer data. LivePerson depends on our employees to develop, operate and maintain our application and systems.

LivePerson conducts reference and background checks for every employee, regardless of the position for which they are hired. Our Ethical Conduct Policy 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 all employee contracts to ensure that all intellectual property and internal operational information remain within the company.

1.10 Operations

▪ Network Operation Center

LivePerson's security plan includes provisions that enable us to identify and act upon any potential breaches in security. Our Network Operations Center (NOC) monitors all network and application 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.

All security logs and alerts from all systems are collected and displayed by predefined scenarios.

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

▪ Penetration testing

LivePerson's security program includes considerable testing for security vulnerabilities by independent security experts. These experts perform an array of penetration tests on the network and application on a regular basis, as well as the application prior to all major releases.

1.11 Disaster Recovery

LivePerson's Disaster Recovery plan ensures that our customers experience no interruption of service in the event of a loss of data occurring at our main data center.

LivePerson's main data center is located in Washington, DC. We maintain a complete back-up of the data in a separate location. Encrypted channels (VPN) connect the two systems, ensuring that all data is

backed-up on regular basis. All of the hardware elements and software configurations are state-of-the-art.

Our disaster recovery plan and systems are tested on a monthly basis to ensure that all systems and personal are ready to perform in case of a crisis.

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