Protecting Customer Data in a Multi-Tenant Environment

Document Version: 1.0
March 2017
Introduction

As a leading SaaS provider with more than 18 years of experience in the industry, we realize that working in a cloud-based multi-tenant environment may raise concerns related to the confidentiality and protection of sensitive data.

We decided to turn this key issue into our core security offering in order to enable our customers to trust us with their most confidential data, while leveraging the benefits of our multi-tenant SaaS solution.

This document outlines the main elements that LivePerson has implemented in each layer of LiveEngage, in order to ensure the appropriate security when utilizing shared resources.

Key Elements of Segregation

Secure Infrastructure

In order to provide a secure platform and address key issues related to security, LivePerson has implemented robust controls throughout its infrastructure and architecture in multiple layers. The following concepts and elements represent the standard level of security that we believe should be part of any SaaS based solution. These controls are similar for any customer using LiveEngage.

The LiveEngage infrastructure was designed to provide best-of-breed security in every layer, regardless of each specific customer’s needs. The service components are protected with various layers of security, for example Firewalls, ACLs, Load Balancers, Network IDS, Web-tier ISAPI filters, DDoS protection, etc. The operating systems are hardened according to strict standards, and the entire infrastructure is regularly tested for potential vulnerabilities, both by an independent third party, and by internal LivePerson scans.
Unique Account Identifiers and Settings

The LiveEngage platform is designed with inherent controls that were included in each layer to help prevent cross-account access between different customers. Each LiveEngage customer is provisioned with a unique LiveEngage account (site ID), and each request to the LivePerson servers is based on that unique identifier.

The unique customer account provides robust controls for dedicated user management, and dedicated customized security settings to align with each customer’s security policy, as outlined below.

All visitor and agent interactions always go through the LiveEngage platform for control and validation, and to help ensure appropriate segregation and security.

LivePerson invests great efforts to ensure that the all segregation and security controls are effective, and function according to the security model design. Independent security vulnerability assessments and penetration tests are performed on a regular basis, with specific test cases and scenarios that focus on the effectiveness of customer segregation controls.

Dataflow and Platform Diagram

The diagram below outlines the main components of the LiveEngage platform, as well as the dataflow process for agents and visitors communicating with LiveEngage. The diagram helps provide a better understanding of how security controls are embedded in each layer.

Figure 1: Main components of the LiveEngage platform
PROTECTING CUSTOMER DATA

Figure 2: Dataflow process for agents and visitors

Network and Web Layer

The LiveEngage tag is hosted on the customer website, and loaded by the visitor browser from the customer website.

Each session is identified by 3 unique identifiers:

- Unique LiveEngage SiteID
- Unique Visitor ID
- Unique Session ID

This combination ensures all data collected from each session is directed only to the relevant customer account.
The communication between the visitor and the agent during the engagement session is established over 128bit TLS HTTPS communication.

Cookie Configuration

Similar to other internet based services, visitor sessions are based on cookies. The LiveEngage platform was designed to allow customers to define which cookie configuration will be utilized as part of its LiveEngage deployment. While the usage of third party cookies is safe and based on the same unique site ID segregation, the ability to use first party cookies provides an additional layer of security, as the cookies are associated with the customer’s own domain.

Customized Dedicated URL

LiveEngage offers its customers a customized, dedicated URL based on the customer domain and certificates (for example chat.customer.com). LiveEngage can host the customer issued certificate and associate the customer Site ID as the only Site ID that can be used by this certificate. In addition, a dedicated IP is assigned for that customized URL. The combination of Site ID validation with a dedicated URL adds an extra layer of protection that eliminates potential risks of cross-account access even when each server hosts more than one customer.

DB Layer

Visitors’ session information (metadata) and chat transcripts are stored on LivePerson’s DB servers. The data is stored in the DB based on the unique site ID of each LiveEngage customer. The DB tables contain customer site IDs, and each request from the application server to the DB is based on stored procedures which contain the site ID in each query.

Storage

Data is stored under the storage table-space and divided into partitions. Each partition may contain several accounts, or can be assigned to a dedicated account [by request]. Either way, the partitions are based on unique Session ID and are tied to the Site ID. If a dedicated sub-partition is allocated, the data retention period can be adjusted according to the specific customer policy (extended or shorter period), without impacting upon other customers who consume shared resources.

Masking and Encryption of Data at Rest

Prior to storing data in the DB servers, LiveEngage provides two additional layers of protection for data at rest:

- **Selective Data Masking for chat transcripts**: The LiveEngage platform provides customers with the ability to identify specific sensitive data patterns and remove them from the chat transcripts prior to storing the transcript in the DB. The masking is based on a RegEx mechanism that identifies the sensitive pattern as configured by the customer, and replaces them with xxxx or *****. See Appendix A for screenshots, or download the data-masking data-sheet by clicking here.

- **Data Encryption**: Chat transcripts and other session variables can be stored on the LivePerson DB servers in an encrypted format. The encryption is based on 192bit AES algorithm, and controlled by the application server and not by the DB. Each LiveEngage customer is assigned with a unique encryption key, and, additionally, each chat session is encrypted with a unique key for that session (for example, 2 chat sessions of the same customer will be encrypted with 2 different keys).
PROTECTING CUSTOMER DATA

Figure 4: Sample screenshot of DB with encrypted data

Application Layer

Account data can only be accessed through the web-based console.

In order to improve the security around user access to data, LiveEngage has an extensive user management and access control tool. From a Login Policy through user permissions and IP restriction, all can be managed and fully controlled.

Note: Some user management and access control options must be set by a LivePerson Account Manager or LivePerson Technical Support.

The inherent IP based restriction access list that is built into the platform ensures that access to data can only originate from trusted IP addresses or ranges, as configured by each customer. This means that even if the data is stored on a shared resource, the access per Site ID can only be established from within the trusted IP ranges.

Note: As the unique Site ID validation is utilized in each request, the configuration is unique per customer account. One customer’s account policy cannot impact upon another customer’s policy.

These controls are extensively tested by independent third party security experts on a regular basis as part of the LivePerson security vulnerability assessment and penetration testing processes.
Appendix A

Sensitive Data Masking Interface

Figure 5: Masking configuration interface