LIVEPERSON

LiveEngage Security White Paper

Table of Contents

LiveEngage is a cloud-based platform designed to deliver secure digital interactions between brands and consumers, wherever they are — on the web, mobile applications, messaging applications, or SMS/text messages.

With more than 20 years of experience in the real-time chat and messaging industry, we consider security a core guiding principle for all aspects of our business. The LiveEngage platform was specifically designed for enterprises and, as such, complies with the highest security standards.

While there are no truly bulletproof solutions, we do our best to follow best practices and keep service secure.

Security organization and program

We strive to implement security processes and practices across all business units. To help with that, we have a full-time chief security officer in house as well as a dedicated security team of professionals that manages LivePerson's security. Our practices are based on industry-leading standards, on which we are audited annually, like SSAE 16, an SOC framework, ISO 27001, and PCI DSS.

The framework includes policies and procedures, asset management, access management, physical security, people security, product security, cloud and network infrastructure security, third-party security, and vulnerability management as well as security monitoring and incident response.

Information security policies and standards are approved by management and available to all LivePerson employees.

People Security

The people behind LivePerson products are an essential part in protecting the service, as the human factor has a key role in and influence on our organizational level of security. Some of the controls we put in place include a pre-employment screening process, which includes the following.

Background Checks	The screening process is based on background checks and personal interviews with recruitment/HR manager and a prospective employee's direct manager. Where applicable, background checks include criminal record check, credit check, education check, references and identity, and verification of CV claims. Additional checks may be performed in accordance with the local law.
InfoSec training	New employees go through an on-boarding process that include communication of security guidelines, expectations, and code of conduct. In addition, all LivePerson employees undergo an annual security awareness training.
Continuous communication	The LivePerson security team provides continuous communication on emerging threats, performs phishing awareness campaigns, and communicates with the company regularly.
Ethics hotline	LivePerson utilizes a confidential internet- and phone-based hotline service 24/7, which enables concerned parties to anonymously inform the legal and HR teams of any unethical behavior.

Product Security

The LivePerson security development lifecycle (SDLC) standard helps ensure the delivery of a highly secure platform and activities.

The following activities help us achieve this mission.

Penetration testing	LivePerson regularly performs testing for security vulnerabilities both in house and by independent security-assessment service providers. Penetration tests are performed on an annual basis by a third party.
Change management	LivePerson follows a strict change management process. Changes are tracked, reviewed, and approved to ensure operational changes are aligned with LivePerson's business objectives and compliance requirements. A change is reviewed before being moved into a staging environment, where it is further tested before finally being deployed to production.
Encryption in transit	LivePerson supports TLS1.1 or above with minimum key length of 128 bit to encrypt network traffic between the customer application and LivePerson.
Encryption at rest	LivePerson offers customers the option to encrypt chat transcripts and other session variables that are stored on the LivePerson DB servers in an encrypted format. The encryption is based on a 192-bit AES algorithm.
Account security	LivePerson offers robust security controls that the customer can choose to enable or use in the application and add more layers of protection to the account, such as masking, IP restriction, audit trail, log-in policy password complexity, and more. We encourage customers to work with their account managers and use these controls.

Private cloud infrastructure

The security of our infrastructure and networks is critical. Creating a safe platform for LivePerson applications and customer innovation is the mission of our cloud security.

Top-tier infrastructure	We use multilayered controls to help protect our infrastructure, constantly monitoring and improving our applications, systems, and processes to meet the growing demands and challenges of security.
Asset management and ownership	All assets are assigned with a defined owner and accountability.
Access control	Access to production infrastructure is limited to the minimal number of individuals based on least-privilege concept and need-to-work basis.
Monitoring	LivePerson utilizes a wide range of tools to monitor its environment across all data centers from both the server and application level. Parameters are collected from devices on the network and aggregated at a central location with redundancy for the sake of detecting anomalies, trends, threshold crossing, etc. In addition, logs are collected into a SIEM platform that is monitored by a dedicated security operations center (SOC) to help ensure rapid detection and mitigation of risks.
Distributed denial-of-service (DDoS) prevention	As part of the multilayered-protection approach, a dedicated DDoS mitigation ecosystem has been put in place. On a high level, this includes ACLs on the border routers, multiple layers of firewalls, including specific configuration for DDoS mitigation, traffic reputation service, and a dedicated equipment for DDoS mitigation. On top of that, DDoS scrubbing-center service is available.

Physical Security

Physical security of LivePerson facilities is an important part of our security strategy.

Data center security	LivePerson's production environment is hosted in data centers across the APAC, United States, and Europe. Our servers are locked in private cages and are privately owned by LivePerson for our dedicated use and service delivery. The facilities comply with the highest industry standards for physical, environmental, and hosting controls. For example, this includes 24/7 security officers, facility access, biometric hand reader, exterior security, interior security, annual audits, cages, alarm monitoring/intrusion protection, video imaging, CCTV, audio intercom and two-way radio subsystem, ID requirements, intrusion testing, security personnel hiring/training, security policies, asset tracking, and video surveillance.

Business continuity plan and disaster recovery

LivePerson maintains a full-scale, one-to-one ratio disaster recovery facility, which guarantees consistent service performance and minimal data loss in the event of a regional disaster.

Recovery planning	LivePerson maintains formal business continuity and disaster recovery plans that are regularly reviewed and updated.
Global resiliency	LivePerson operates out of two data centers in the US, serving mainly US-based customers: one in Virginia and one in California. Within Europe, it also operates out of two data centers — one in the UK and one in the Netherlands — serving its Europe-based customers. LivePerson additionally has two servers in Australia for its APAC customers: one in Sydney and one in Melbourne. LivePerson has established a business continuity plan (BCP) that enables the company to respond quickly and remain resilient in the event of most failure modes, including natural disasters and system failures.
Customer data backups	LivePerson conducts backups in two tiers: 1. In the central storage tier, we take daily snapshots of the local storage, mirror all the data to another storage unit, and, in real time, also mirror the data to a DR site. 2. Another tier is a standard backup-to-disk backup done with NetBackup. We back up everything, including DBs, file systems, and virtual servers (VMware).

Third-party security

In today's interconnected business environment, maintaining visibility into the software supply chain is of utmost importance. LivePerson has implemented the following procedures.

Vetting process	Third parties used by LivePerson are checked before employment to validate that prospective third parties meet LivePerson's security standards. Customers' data will not be accessible to third parties or subcontractors.
Ongoing monitoring	Once a relationship has been established, the LivePerson security team will conduct an annual review to the vendors. The annual review can be done by LivePerson's security team or by getting a third-party report (e.g., SSAE 16 SOC2 report, ISO27001). The procedure takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

Security compliance

LivePerson is committed to mitigating risk and ensuring LivePerson services meet regulatory and security compliance requirements.

Regulatory environment	LivePerson complies with applicable legal, industry, and regulatory requirements as well as industry best practices.
SSAE16 SOC2	LivePerson has obtained SOC2 certification, providing our customer validation on the security controls and the confidence in our security program.
PCI-DSS 3.2	LivePerson has obtained PCI-DSS certification for the secure chat widget, allowing our customers to receive CCD from the visitor in a secure manner.
ISO 27000 series	LivePerson has obtained ISO 27001 certification, showing our maturity within the information security space. Security is a top priority for LivePerson, and this achievement demonstrates our commitment to information security, data protection, and continuous improvement.
EU - US privacy shield framework	LivePerson has been working in the European Union for many years. Our operations are certified under the EU privacy regulations through Privacy Shield provisions as a part of our commitment to comply with EU data protection requirements in case of a need to process or store EU data outside of the EU.
GDPR May 2018	As mentioned, LivePerson has been active in the EU for a long time, including compliance with the EU privacy requirements. As such, LivePerson is actively working to meet the new GDPR requirement by May 2018.

Continuous monitoring and vulnerability tests

At LivePerson, the security and resiliency of our products and infrastructure is a top priority.

As part of the ongoing work of the security team, continues monitoring is being done as part of the compliance and regulation program and the risk assessment. The Vulnerability tests establish how we identify, respond, and triage vulnerabilities against the LivePerson platform. To ensure security of our platform, LivePerson continues to mature the following capabilities:

Continuous monitoring program	Our SOC (Security Operations Team) team monitors security using centralized SIEM system to collect logs from the different security tools and other components, for any new vulnerabilities, incidents, and threats that LivePerson need to respond and mitigate accordingly.
Distributed denial-of-service (DDoS) prevention	LivePerson infrastructure is protected with multiple layers of defense systems, including a dedicated, near real-time best of breed DDoS mitigation technology. LivePerson's Border Routers contain ACLs to deny traffic that is not approved by LivePerson. On top of that, multiple layers of F5 Firewalls are deployed and include advanced protection controls such as Reverse Proxy for all traffic, Packet Filter rules and stateful inspection. In addition, LivePerson uses GeoBlock and Reputation Service to block traffic from known malicious sources and large ranges of IPs. LivePerson using the services of scrubbing center in case of DDoS attack.

Summary

As a leading SaaS provider with more than 20 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. Security mechanisms to protect physical, network and application components of the platform, coupled with transparency about our security policies and processes, let brands trust us with their most confidential data, while leveraging the benefits of our multi-tenant SaaS solution.

For further details and steps to secure your LivePerson account, check out the documents on the security page. Lastly, if you have more questions, or need more detailed answers, feel free to get in touch with our Security Team via the Support Team or your Account Manager.