LiveAgent Security Policy

More than 17,000 customers trust LiveAgent with their data. Data security is of utmost importance for us. We combine multiple security features to ensure customer, employee and business data is always protected so our customers can rest easy knowing their data is safe, their communication is secure, and their businesses are protected.

Product Security

Two-factor authentication
2-Step Verification (/features/2-step-verification/) adds more security to your LiveAgent account. When you have 2-Factor Authentication enabled, any attempt to log into your account must be accompanied by the code that you generated in Google Authenticator app. 2-Step Verification can help keep unknown people out, even if they have your password.

HTTPS Encryption
All LiveAgent hosted accounts run over a secure connection using the HTTPS (/features/https-encryption/) protocol. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. It means all communication between your browser and LiveAgent is encrypted, including your chat and email communication.

Secure credential storage
We follow latest best practices to store and protect user login credentials and passwords in the cloud.

IP & network restrictions
Your LiveAgent Agent panel can be configured to only allow access from specific IP address ranges.

API Security
LiveAgent REST API (https://support.ladesk.com/840770-Complete-API-reference) is restricted to accredited users based on username and password or username and API tokens.

SPAM filtering
LiveAgent has an intelligent built in SPAM filter that learns and improves its filtering capabilities continuously.

Data Center Security

We ensure the confidentiality and integrity of your data with industry best practices. LiveAgent servers are hosted at Tier IV or III+, PCI DSS, SSAE-16, or ISO 27001 compliant facilities. Our Security Team constantly pushes security updates and actively responds to security alerts and events.

Physical security

	Server environment
Facilities	LiveAgent servers are hosted at Tier III+ or IV or PCI DSS, SSAE-16, or ISO 27001 compliant facilities. Data center facilities are powered by redundant power, each with UPS and backup generators.
	Security zones
On-site Security	Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.
	Server & Device monitoring
Monitoring	All Production Network systems, networked devices, and circuits are constantly monitored and logically administered by LiveAgent administrators. Physical security, power, and internet connectivity beyond co-location cage doors or Amazon/Linode services are monitored by the facilities providers.
	Datacenters in United States, Europe & Asia

Location	LiveAgent hosts data in multiple data centers based on your preference or geographical location in the United States, Europe, and Asia. Customers can choose to locate their Service Data in the US-only or Europe-only.

Network security

Our network is protected by redundant firewalls, best-in-class router technology, secure HTTPS transport over public networks, and network Intrusion Detection and/or Prevention technologies (IDS/IPS) which monitor and/or block malicious traffic and network attacks.

Network security

Architecture	**Security zones in our architecture** Our network security architecture consists of multiple security zones. More sensitive systems, like application servers and database servers, are protected in our most trusted zones. Other systems like loadbalancers are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk.
3rd-party Penetration Tests	**Third-Party Security Research** In addition to our extensive internal scanning and testing program, LiveAgent alsow works with third-party security experts and researchers to perform security checks and broad penetration tests.
Network Vulnerability Scanning	**Vulnerability scanning** Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.
DDoS Mitigation	**DDoS Mitigation** Industry-leading infrastructure is in place to protect against and mitigate the impact of denial of service attacks.
	Communication Encryption

Encryption	Communications between you and LiveAgent servers are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS) over public networks.

Disaster Recovery, Backup & Redundancy

We operate a multi-level backup and disaster recovery strategy. Backups and near real-time snapshots are taken at various intervals and multiple copies are securely stored on different servers. Our disaster recovery program ensures that our services remain available or are easily recoverable in the case of a disaster.

Our redundancy architecture eliminates a single point of failure. Combined with comprehensive backups, we ensure customer data is replicated and available across production systems.

EU GDPR

We are actively preparing for the General Data Protection Regulation (GDPR) that becomes enforceable on May 25th, 2018. A team of security experts and developers are working on strengthening our security policies and raising awareness about data protection and what is required of our employees to comply with rules that GDPR puts in place. We will also make sure that our customers would be informed about recent development in a timely manner. As the deadline for GDPR gets closer, we accelerate our effort to provide a seamless and effortless transition to the new regulation requirements. For more information about GDPR and LiveAgent, please contact our support via email support@ladesk.com