StarLeaf Standby Security Information

Contents

Introduction

StarLeaf Standby provides continuity for business-critical communications and collaboration.

The StarLeaf Standby suite of applications includes real-time communication tools for incident failover, seamless failover for video meetings, messaging and telephony, and a mass notification system for incident response, business continuity, and compliance.

The infrastructure on which this communications network is based is entirely owned and developed by StarLeaf. It provides a powerful and reliable platform for the provision of business-critical communications failover tools as a service to businesses globally, without reliance on any third-party infrastructure for the core service. As a result of this, StarLeaf is in a unique position to rapidly respond to customers and continuously evolve the service to meet their demands.

Underpinning the StarLeaf solution is a commitment to security in the software, infrastructure and processes. This security document outlines these key policies and processes.

Further information is available on request.

Architecture

The StarLeaf Standby platform runs on dedicated hardware, owned and maintained by StarLeaf. StarLeaf maintains defence-in-depth security controls over this hardware. Custom configured units acting as firewalls are implemented in all StarLeaf locations; border controllers then protect all platform nodes, which themselves validate all incoming traffic.

Each data centre has network connections which are fully redundant for live traffic in addition to a separate management connection. This allows StarLeaf to access equipment and enable recovery, even in the event of a critical error with the live connections. Furthermore, each virtual and physical machine can only communicate on a restricted virtual local area network to ensure isolation of traffic, and all non-public virtual machines are hosted on internal addresses only.

The StarLeaf Standby platform runs solely on internally developed code. There are no user-created applications within the StarLeaf Standby platform, and all code is owned and maintained by StarLeaf, limiting the scope for instances of malicious code/malware.

Each physical server only runs StarLeaf software within open source Linux operating systems. We do not share our physical servers with any other software. This means no other software could access any data via vulnerabilities such as Spectre or Meltdown.

Where StarLeaf works with third-party services, these services are constantly monitored, and any issues or outages are flagged to the StarLeaf operations team. In addition, ticket escalation and failover mechanisms are ready to be used if an extended outage is detected.

The following sections discuss details of the key areas which constitute the global network architecture, followed by the methods StarLeaf employs with regard to upgrading and reliability.

Networking

All StarLeaf Standby services are protected by a gateway that restricts which addresses and ports are accessible. This acts as a firewall and router. Furthermore, the core StarLeaf real-time communication services are accessed through a StarLeaf border controller for real-time communications. These act as proxies for inbound connections on the public IP address, blocking spurious data and transferring valid commands to the core. The StarLeaf core is accessible on private addresses only, routable only through the firewall and relevant border controller.

Dedicated data centres

StarLeaf has data centres around the world, selected for their physical security and strict access requirements. Details of the physical sites' ISO/IEC 27001, SOC2 and ISO/IEC 9001 certifications can be provided on request.

Physical access to the data centres is limited to those who have been authorised by StarLeaf. There is no physical access to StarLeaf infrastructure by third parties, other than data centre staff, and there is no network access for third parties. Servers are located in locked cages which have multiple barriers to entry. These are located within buildings with full CCTV coverage and monitoring.

Remote access is accessible exclusively using VPN, available only to the relevant and approved members of the StarLeaf operations team.

Data jurisdiction

The StarLeaf architecture design ensures customer data can be isolated to nominated locations, thereby retaining data within appropriate regional boundaries. Multiple data centres within each jurisdiction ensure data is stored with geographical redundancy. Where possible, StarLeaf offers the option to redundantly store data within individual countries. Details are available on request.

The StarLeaf user directory is hosted in Europe. This is the main directory that contains a small subset of personally identifiable information (PII) in order to direct users to their organisation's node, which will be in one of the data centres around the world. Customers are always hosted in their designated jurisdiction, where all their PII is stored. In the event of a major outage, customers are migrated to an alternative data centre within the same jurisdiction.

Upgrades

Upgrades are deployed across the StarLeaf global network in a consistent and controlled manner.

StarLeaf continually upgrades its platform to provide new features, fixes and security improvements. This upgrade management process covers all layers of the delivery technologies, including:

- Network (infrastructure components, routers and switches, etc.)
- Server and chassis management software
- Server operating systems
- Virtualisation software
- Applications
- Security subsystems (firewalls, etc.)

All code changes are initially tested in an isolated environment to ensure reliability and that full coverage regression tests are passed.

The StarLeaf infrastructure enables rapid upgrades and critical bug fixes, often within minutes.

Non-critical upgrades are deployed automatically every four weeks and do not require input from organisation administrators or users. Firmware upgrades to StarLeaf hardware, and software upgrades to the StarLeaf software client are handled in the same manner. To avoid disruption, these upgrades are scheduled out of hours in an organisation’s time zone.

Redundancy

Capacity

The StarLeaf platform has the capacity to support all StarLeaf Standby customers failing-over to the StarLeaf Standby service concurrently. Platform status is monitored 24/7/365 and usage patterns are carefully analysed.

Proprietary load-balancing algorithms are used to manage capacity across the various hardware layers within the network. Capacity planning is conducted far in advance, and there is a constant program of expansion.

Any issues relating to performance are prioritised by the Information Security Officer and the operations team.

Disaster recovery

The StarLeaf 'Service Level Agreement' guarantees to provide at least 99.999% availability. In addition, StarLeaf has implemented and maintains robust resiliency mechanisms. These mechanisms cover a variety of failure scenarios such as:

- Failure of any network connection
- Failure of any cable
- Failure of any switch
- Failure of any power supply
- Failure of any communications node
- Failure of any computing blade
- Failure of any data centre

Backups

StarLeaf maintains static daily backups for disaster recovery and real-time streaming backups for failover.

Static daily backups

Daily backups store the state of the platform nodes. This allows the system to roll back to a previous state in the event of data corruption or loss.

Real-time streaming

The real-time streaming backup maintains an up-to-date backup (see RPO, below) of the current configured state, including instant messages, call logs and management settings. This allows for a full recovery to the current state in the event of a major outage.

Backup targets

Recovery Point Objective (RPO)

The RPO defines the target age of the most recent backup at the moment the outage begins. The target at StarLeaf is to ensure the backup is correct to within seconds of the start of the outage. This is achieved with the real-time streaming backups (depending on the exact failure mode).

Recovery Time Objective (RTO)

The RTO defines the target duration from the start of the outage to the data being restored. The target at StarLeaf is to have service recovery within hours of the outage being identified. Restoration from backups is always tested as part of every new release of the StarLeaf platform.

StarLeaf clients

Firewall and connecting to StarLeaf

Dedicated StarLeaf clients connect to the StarLeaf platform through a tunnel connection. This means only a single port (TCP:443) is required to connect to the platform for all calling functions. This port is typically already open in organisations, reducing the requirement for additional firewall configuration.

In addition, one of the following UDP ports should be opened for a better experience in challenging network conditions:

[24704, 3478, 1194, 500, 123]

Standby data backed up from Microsoft

StarLeaf standby must be connected to a customer's Microsoft account to read data. StarLeaf Standby only requires read-only permissions for a global admin user in a customer's Microsoft account. When customers first connect it will ask for the following permissions:

Permission	Reason
Sign in and read user profile	Allow Standby to sign into the customer's Microsoft organisation.
Read all users' full profiles	Read users' telephone numbers so Standby can send them SMS messages when failing over meetings or use the broadcast message functionality.
Read all chat messages	For future use. To allow Standby to back up chat messages.
Read all channel messages	For future use. To allow Standby to back up chat messages.
Read contacts in all mailboxes	For future use. To allow Standby to record mobile numbers for a user's contacts to be able to send them SMS message meeting invites when meetings fail over.

Read all groups	Allows Standby to store group membership so the customer fail over or send messages to specific groups.
Read calendars in all mailboxes	Allows Standby to back up calendar items so that it can re-create the meetings in StarLeaf upon failover.
Read all call records	For future use. This allows standby to see the amount of usage, to assist StarLeaf with capacity planning.

Data security

Access

Access to live platform data is restricted to certain groups within StarLeaf. It is limited to those who perform a specific relevant action and therefore require access:

Group	Notes	Purpose
StarLeaf sales engineering team	Per StarLeaf's Access Control Policy sales engineers can only access their own customers' accounts.	Onboarding and customer support.
StarLeaf support team	Per StarLeaf's Data Privacy Principles only appropriate logs or information would be accessed for the support case at hand.	Advanced customer support
StarLeaf logistics and sales operations teams	Per StarLeaf's Guidelines and Procedures for Access Management only appropriate account settings would be accessed for account creation and customer onboarding.	Initial setup and customer onboarding.
StarLeaf operations team, including selected developers	Per StarLeaf's Data Privacy Principles only appropriate logs or information would be accessed for the support case or issue at hand.	Platform maintenance and development

All data access requires a personal login. Only users who are members of the above groups have logins which grant access to the platform and user data, all other access is denied.

Encryption keys

Encryption keys are stored exclusively within the StarLeaf secure network. Access to this network is restricted to authorised employees only.

Customer data segregation

Each organisation's data is physically stored on a server which may host several StarLeaf nodes, each of which may host several hundred organisations. Data for each organisation is isolated through the multi-tenant architecture of the platform service. All data related to one organisation is marked as such, and access to this data is restricted to authorised users and applications for that specific organisation. Backups are held in the same format, (real-time streaming backups and static backups) which ensures the same level of data isolation.

Encryption of data in transit

Data in transit refers to the scenarios where data is being transmitted between physically separate machines over a network.

StarLeaf client control messages

All control messages are encrypted using AES 256 in Galois/Counter Mode (GCM).

Audio/Video

Media streams are always encrypted using AES 128, including any transit between StarLeaf servers as well as between StarLeaf endpoints and the global network. For calls between users in different data centres, media will be sent between StarLeaf data centres and is also encrypted.

Messaging

All instant messages are encrypted in transit using AES 128 in Counter Mode (CTR).

Recordings

All recorded meetings are encrypted in transit using AES 128 in Counter Mode (CTR).

Encryption of data at rest

Data at rest refers to inactive data that is stored physically.

Meeting backup data

Meeting backup data is encrypted at rest with XTS-AES-256

Active Directory backup data

Active Directory backup data is encrypted at rest with XTS-AES-256

Audio/Video

Media streams are not stored.

Messaging

All instant messages are encrypted at rest using AES128 in Counter Mode.

Recordings

For Europe, Middle Eastern and African customers, meeting recordings are stored in the EU. For the rest of the world, meeting recordings are stored in the US. All recordings are encrypted at rest using AES 256.

Personally identifiable information (PII)

General data protection regulations (GDPR)

StarLeaf welcomes the increased profile attributed to information security under the GDPR. The requirements are significant, and our global team works consistently to ensure StarLeaf services and commitments are compliant, can continue to be trusted, and include reference to both the UK GDPR and the European GDPR.

Actions taken include the following:

- Appointment of a Chief Information Security Officer (CISO)
- Appointment of an expert regulatory compliance company for advisory assistance
- Increased investment in our security infrastructure
- Updated contractual terms and privacy notice
- Execution of Data Processing Agreements with relevant data controllers.

StarLeaf is committed to the highest forms of data protection. StarLeaf can specifically confirm the following:

- Sharing of information with third parties is done according to the terms and for the purposes defined within the Data Processing Agreement. This is limited to what is required for the operation of the platform
- The Data Processing Agreement defines the data retention policy for customer data. PII for which we are acting as a Data Processor will normally be deleted within 90 days of termination of a customer contract. Customers may request earlier deletion if required
- StarLeaf confirms that at no cost to the customer, specific records may be destroyed.

StarLeaf has completed a gap analysis against Data Protection law and has integrated policy and procedures into its ISO/IEC 27001 Information Security Management System to ensure adoption and practice by necessary employees.

StarLeaf has opted to employ an external Data Protection Officer as is permissible where “his/her function can be exercised based on a service contract concluded with an individual or an organization” (Article 29 Data Protection Working Party 2017, 22).

StarLeaf subprocessors

Subprocessors used by the StarLeaf Standby service can be found here: https://support.starleaf.com/legal-information/starleaf-subprocessors

Data retention policy

All data is kept for as long as the customer’s StarLeaf Standby account is active and deleted 90 days after deactivation or upon request from the customer. Exceptions are call records, connection events and detailed call diagnostics, which are deleted after 397 days.

Connection history stores the last connected time for as long as the StarLeaf account is active.

Anonymisation

Anonymisation is performed on call detail records so StarLeaf can run statistical analysis on past trends. This is done without recording the PII of users involved in all calls. While each Call Detail Record is being written we also write an anonymised summary. After 397 days the original Call Detail Record is deleted and only the anonymised summary remains.

Third-party endpoints

All communication between StarLeaf endpoints is encrypted as standard. Where possible, we also encrypt communications to third-party devices. The H.323 standard does not allow for call signalling to be encrypted, but StarLeaf always offers encryption on all media channels when the endpoint is capable of it.

To avoid these limitations of H.323 endpoints, StarLeaf recommends the use of StarLeaf endpoints or endpoints running the StarLeaf client.

Organisation level security

Authentication - Admins

StarLeaf Standby admin passwords are stored and protected with AES-256 encryption.

Authentication - Users

During end-user registration, StarLeaf leverages the security of the user's email account or mobile phone number to authenticate the user. It does this by sending a time-limited, one-time password by email or SMS (as chosen by their StarLeaf Standby admin). Upon successful sign-up, StarLeaf issues each app instance with a cryptographically secure token which is then used for all future authentication. All StarLeaf user passwords are securely stored and hashed using the PBKDF2 algorithm.

This token is also used by StarLeaf plugins to enable a single sign-on experience for users.

Account management and role-based access control (RBAC)

StarLeaf Standby admin dashboard

The StarLeaf portal is a web management tool that requires https access.

All management actions and settings are contained within the StarLeaf Standby administration dashboard. There are no settings located in user software that could affect the connection to the platform.

StarLeaf end-user portal

For StarLeaf Standby customers who choose to use the StarLeaf application for one or more of calendar, meeting, calling or messaging failover, each user can manage their individual StarLeaf account using the StarLeaf portal and see information currently stored for them, including all PII such as usernames, email addresses, meetings and recordings.

By default, all web sessions in the portal use a token from the installed StarLeaf app for authentication. If this is not available then the portal will require a username and password to log in, protected by an inactivity timeout. On request, passwords can be required to meet strict complexity requirements. There is also a password reset mechanism available to all users, which sends a link for password recovery to the user's email address.

All management actions and settings are contained within the StarLeaf portal. There are no settings located on user software that can affect the connection to the platform. The minimal settings located on the StarLeaf endpoints (e.g. IP address settings) can be locked using a PIN code from the online portal.

Provisioning and deprovisioning

User provisioning integration

The ability to deprovision users is critical to preventing unauthorized access to enterprise data by former employees. Real-time user synchronisation with StarLeaf Standby enables

the power of centralized user management. StarLeaf integrates with major user provisioning providers including Azure/on-prem Active Directory, OneLogin, and Okta.

StarLeaf security team and procedures

StarLeaf is committed to security in every aspect of the business. This is further demonstrated by StarLeaf achieving ISO/IEC 27001 certification. To maintain the ISO/IEC27001 certification, StarLeaf is audited each year by an external auditor. The following sections discuss the security procedures in place for the staff and processes at StarLeaf.

Employee onboarding

Before starting at StarLeaf, an external agency performs background checks on new employees who may have some level of access to customer data or software development. All new StarLeaf employees in any department are required to complete a comprehensive Trust & Confidence Agreement and Information Security Policy which formally documents their security and confidentiality obligations.

Policies are communicated to all new employees as part of their onboarding process and are prominently available on intranet resources.

The CISO is responsible for identifying and prioritising new threats, as well as responding to incidents. The development and operations teams are then responsible for implementing fixes and improvements.

All new employees are made aware of the security lead and are extensively trained in the importance of information security and with the procedures for safe working practices and identifying and responding to incidents.

Vulnerability monitoring

As part of ISO/IEC 27001 certification, StarLeaf has defined a security incident monitoring and reporting process. Access rights are strictly defined and restricted, and the development team is trained in a standardised method of reporting any observed deviations. In addition, there is ongoing functional monitoring which reports unusual operation or issues to the platform operations team.

StarLeaf runs highly automated systems which require regular internal training and re-training. A detailed Knowledge Center is maintained to ensure continuity in the event of staff turnover. Furthermore, StarLeaf runs multiple redundant offices and networks. Failure at any one office can be covered using other offices and remote working.

StarLeaf monitors potential vulnerabilities in several mutually reinforcing ways:

- Constant monitoring of performance and access permissions
- Regular testing by the in-house security team on all new software and hardware releases
- External penetration testing commissioned by StarLeaf and carried out by industry experts for every major release, at least twice per year
- Automated monitoring of open ports and network bandwidth
- StarLeaf operates an active bug bounty program to assist in the identification and timely removal of any possible security vulnerabilities.

Audit logging

Every action performed on the platform, by being logged into a machine, management console, or the portal is identifiable and can be traced to the user who performed the action.

StarLeaf maintains detailed events for at most 397 days as described in the data retention policy.

Employee access rights

StarLeaf maintains an independent information security team, led by the CISO within the development and operations team. This team is responsible for the discovery, prioritisation, and resolution of all security issues. They work closely with other teams in research and development in order to drive any required changes, and to deploy these to the global network.

Each StarLeaf employee has a specified set of roles, and each role has designated rights which are configured across all systems. Examples include the networks they have access to, the servers they can reach, and which customers they are authorised to view. These rights are continually reviewed against the HR system and updated.

The development and operations team provides expert input for the emergency response team in the event of a security incident.

Vulnerability and penetration testing

StarLeaf runs third-party penetration testing at least twice per year. The output of these tests is a detailed penetration test report.

Any issues highlighted in this report are triaged and prioritised according to severity. This process is managed by the Information Security Officer and the operations team.

StarLeaf operates an active bug bounty program to assist in the identification and timely removal of any possible security vulnerabilities.

Details of these results and reports are available on request.

ISO/IEC 27001

StarLeaf is ISO/IEC 27001 compliant.

ISO/IEC 27001 is the only auditable international standard which defines the requirements of an information security management system (ISMS). An ISMS is a set of policies, procedures, processes and systems which manage information risks such as cyber-attacks, hacks, data leaks and theft.

“Information security is a business problem, not an IT problem.

Risk-based approaches are vital for modern information security effectiveness. There are many ways to achieve security risk management, so a good standard like ISO/IEC 27001 puts formalities in place to ensure the right thought processes were followed and captured when the inevitable breach is realized.” - PwC

By completing the independent ISO/IEC 27001 certification process, StarLeaf has:

- Lowered risks by implementing a methodology for identifying threats and vulnerabilities
- Strengthened assurance in the supply chain
- Promoted customer satisfaction by investing in exemplary practice to safeguard information
- Improved processes through a framework of policies and procedures which are consistent, repeatable and maintainable.

Certification to ISO/IEC 27001 demonstrates StarLeaf has defined and put in place best-practice information security processes.

Legal information

Third-party software acknowledgments

Acknowledgments of third-party software are available at:

https://support.starleaf.com/legal-information/

Disclaimers and notices

This guide may not be copied, photocopied, translated, reproduced, or converted into any electronic or machine-readable form in whole or in part without prior written approval of StarLeaf Limited.

StarLeaf Limited reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of StarLeaf Limited to provide notification of such revision or change.

StarLeaf Limited provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose.

StarLeaf Limited may make improvements or changes to the product(s) and/or the program(s) described in this documentation at any time. All other product and company names herein may be trademarks of their respective owners.