Technical FAQ

Last updated by | Erik Ralston | Aug 12, 2021 at 6:30 AM PDT

This document answers frequently asked questions. This is intended to be a list of canned responses for user inquiries and each entry should be ready for customer eyes. Furthermore, they should be written such that they progressively disclose more information, providing more detail by simply copying more of the entry to the customer. Assume the first sentence is for management then by the last you're talking to a Principal Security Architect:

Does Soundbite have secure datacenters, geo-redundancy, physical security at sites handling data, or similar hosting hardware questions?

Soundbite uses the secure and global network of data centers provided by Microsoft Azure for all hosting.

Does Soundbite use automated soft management solutions and/or change management tools in hosting environments to provide OS patching, upgrades for virtual machines, etc?

Soundbite does not use automated orchestration of Virtual Machines (VMs) or similar technology because Soundbite uses Platform-as-a-Service (PaaS) or serverless/managed technologies that do not require such low-level management.

For example, for hosting the application itself we use a combination of Azure Web App and Azure Functions, both of which provide a zero-touch hosting environment. Persistence centers on Azure SQL Database and Azure Storage, which are self-contained fully managed services that do not require such active maintenance by the owner.

Does Soundbite use secure encryption?

Soundbite uses Microsoft Azure technologies to securely encrypt in transit and at rest.

In Transit encryption when data is moving to and from the Soundbite platform:

- App to API – TLS 1.2 provided via Azure Front Door, Azure-managed using a SHA256 cert
- App to content – TLS 1.2 provider via Azure Storage, Azure-managed using a SHA256 cert

At Rest encryption when data is held within the Soundbite platform:

- Database – Transparent Data Encryption (TDE) in Azure SQL Database, Azure-managed using AES256
- Content and NoSQL Storage – Storage Service Encryption (SSE), Azure-managed using AES256

Does Soundbite support Single Sign-On (SSO)?

We support SSO, enabling a user to log reuse their org account whenever they interact with Soundbite.

We offer SSO via Azure Active Directory (AAD) and Okta (for additional cost), integrating with your existing directory provider for user & group synchronization, plus user authentication and authorization.

On the front-end, we use OAuth 2.0 plus OpenID Connect. This allows for AAD or Okta to authenticate the user in its own flow - potentially including your configured Multi-Factor Authentication (MFA) - then passing back a JSON Web Token (JWT) that can access related services (EG, AAD JWT Tokens can access Microsoft Graph). That token is then exchanged with the Soundbite platform for a Soundbite token that securely accesses our APIs in the context of the logged-in user.

For AAD, a complete introduction to the OAuth + OIDC front-end flow is described by the Microsoft Authentication Library (MSAL). For Okta, the Okta React SDK documentation describes not only the JavaScript coding approach but also the required app configuration.

What is the Soundbite identity management, password policy, Multi-Factor Authentication (MFA), and similar user access control support?

Thanks to Soundbite implementing integration with the client's directory, no client secrets (EG, customer organization employee passwords) are stored in Soundbite itself. The directory (EG, Azure Active Directory provided by your Office 365 subscription) provides all of the authentications as an intermediary, only passing back secure authentication tokens to the Soundbite application. Passwords are NEVER handled or stored by Soundbite.

User access to Soundbite hinges upon having an active account with the client organization, which means deactivating an employee's account (EG, deleting their O365 user) will result in them losing access to Soundbite for that account. This also means that the security policy of the customer's directory is inherited as the policy for Soundbite, enforcing password length, complexity, MFA, and other aspects per the directory's configured without regard to Soundbite's operation.

How does Soundbite sync audiences?

Soundbite shadows your existing organizational directory to provide your choice of users and groups to target your content.

For usability and performance reasons, Soundbite attaches to your organization's directory service - Azure Active Directory (AAD) and Okta (for additional cost). This is NOT used for security, it provides the key information to scope the audiences of Soundbite and power the user interface.

On the back-end, Soundbite uses an autonomous server-to-server integration to provide **read-only** directory sync, shadowing a configured subset of the users and groups in your organization. In AAD, this is provided by configuring the Soundbite AAD app and service principal to have access to the Org's information. In Okta, this means using the Okta server-side SDK accessing the directory via Okta Authentication Token.

Does Soundbite have a backup and recovery strategy?

Soundbite leverages Microsoft Azure to provide versioning of files and point-in-time restore of databases to provide rollback of changes at customer request.

Database data (Org structure, sessions, notifications, and analytics activity) is persisted in Azure SQL Database which provides Point-in-Time Restore (PITR), which allows for reverting the consequences of both application failure or data corruption. Furthermore, customer requested rewind of content changes due to unwanted actions by users can be enacted.

Audio content persisted in Azure Storage has Blob Versioning enabled, which means all changes over time remain accessible by customer request.

Does Soundbite have a failover and/or disaster recovery strategy in the event of a data center catastrophe?

Soundbite uses Microsoft Azure's geo-redundancy to protect against single data center or single region failover, configured for the customer's need.

Database data (Org structure, sessions, notifications, and analytics activity) is persisted in Azure SQL Database which supports Active Geo-Replication to provide one or more secondary regions for organization data.

For audio content in Azure Storage, data is persisted using the Geo-Redundant Zone (GRS), unless disabled by request out of data sovereignty concerns, which provides a fallback in the event of a single zone (data center) or even single region outage.

Zone redundancy in Azure provides for a single data center failure (EG, a fire breaks out in a building and burns all the hard drives). All customers benefit from Zone redundancy. Geo-redundancy features may hinge upon the availability of appropriate secondary regions, but provide added protection against catastrophes (EG, all internet connectivity fails for an entire Azure region due to multiple major infrastructure failures of some kind).

How does Soundbite handling Personally Identifiable Information (PII)?

Soundbite does capture PII concerning users, but only in a single place that is always encrypted and anonymized elsewhere throughout the system.

Unique user information (EG, Full name, home address, email address, social security number, passport number, driver’s license number, credit card number, date of birth, telephone number, login details, etc) may exist in Soundbite’s software or data, along with partially identifiable information (first or last name, country, state, city, postcode, gender, race, age range, job position, workplace, etc). This data will be handled using best practices, including not storing where possible, anonymizing where possible, encrypting always, and ensuring more than one component of the system must be compromised before the information would be human-readable.

In accordance with GDPR, owners will be notified of any known breach of PII data in the Soundbite platform within 72 hours.

Does Soundbite have consideration for Data Sovereignty (GDPR)?

Data persisted in Soundbite is captured in the chosen Azure region associated with a customer, which can be a single country of your choice with no replication outside of that country.

When organizations are onboarded into the platform, they select a region from Azure’s ever-growing list of locations, including a safe fallback location for geo-redundancy of their SQL Database. This ensures they are in control of the jurisdiction for their data.

In the event a customer has an overriding data sovereignty concern, such as General Data Protection Regulation (GDPR) or similar regulatory concerns about data leaving a country, geo-redundancy can be disabled for a customer to keep all data within a single country.

Does Soundbite use Open-Source Software?

Virtually all software is built with Open Source components that reflect community best practices and solve common problems. Common Open Source foundations in the product include Microsoft's ASP.Net Core, multiple first-party client libraries like the Microsoft Authentication Library for JavaScript (MSAL.js), and utilities like the ubiquitous Newtonsoft JSON.

All open-source software utilized by Soundbite is evaluated on the following criteria that it must:

1. Have sufficient adoption and documentation such that it can be supported into the future
2. Permissively licensed to prevent IP liability
3. Acquired via a reputable public package management system with active security scrutiny (NuGet or NPM only)
4. Audited by automatic security scan (GitHub Dependabot)