Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Ai Producer
Powered by LiveArena

Ai Producer Technical & Security Overview

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Introduction

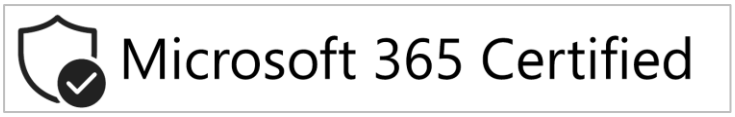
AI Producer is a cloud-based service from LiveArena Technologies AB ("LiveArena"), that provides automated productions for live events. It is developed for Microsoft Teams and requires no other software. It can be used on any device that supports Microsoft Teams.

We take pride in security and data privacy. How we built the service and process data is governed by LiveArena's privacy policy, industry best practices and certain legislation, which within the European Union mainly covers the General Data Protection Regulation ("GDPR"). LiveArena Technologies AB naturally complies with GDPR and any other data protection legislation that applies to LiveArena Technologies AB and its operations.

The service is available through Microsoft's online marketplaces Teams Store, AppSource and Azure Marketplace. Each marketplace has an approval process that validates both the publisher and the app to meet Microsoft's compliance, security, and usability requirements.

Microsoft provides more details regarding the Teams Store, AppSource and Azure Marketplace approval process and requirements.

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman



The Microsoft 365 Certification logo represents that this app has achieved Microsoft 365 Certification. In addition to app security, this program reviews the practices and procedures the app publisher employs. While customer data is under control of the app publisher, you can rest assured that Microsoft has validated that the app will handle it in a safe and secure manner.

Microsoft 365 App Compliance Program

AI Producer is a Microsoft 365 Certified app, which as part of the Microsoft 365 App Compliance Program, verifies that AI Producer and its supporting infrastructure, operational security, data handling processes and governance adhere to industry standard frameworks.

AI Producer has been audited by a third-party auditor on behalf of Microsoft, against a series of security controls and criteria derived from leading industry frameworks such as SOC 2, PCI DSS, and ISO 27001.

A Microsoft 365 Certification security audit includes internal and external penetration testing, of which any found vulnerability hinders certification.

AI Producer users will recognize the Microsoft 365 Certification badge icon in the Teams App Store and app consent screens.

Microsoft 365 Certification results: Application Information for AI Producer by LiveArena Technologies AB - Microsoft 365 App Certification | Microsoft Learn

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Data Processing

AI Producer only accesses the minimum data needed to be able to create a production out of meetings. AI Producer does access some personal information about participants in meetings that it has been added to. The data is only needed until the meeting and/or broadcast is over. However, the data can be stored for up to 90 days after the broadcast. The reason for storing it for a brief period after the broadcast is to be able to handle any support request(s) from the customer and improving the service.

The following information about the participants is accessed and temporarily stored by AI Producer:

- Name. Used to present a speaker name overlay in the broadcast.
- Email of the meeting organizer. Used to send a confirmation email to the organizer.
- User Principal name. Used to refer to the user in other API calls. User Principal Name (UPN) is the name of a user in an email address format. A UPN (User Principal Name) is not the same as an email address. Sometimes, a UPN can match a user's email address, but this is not a general rule.

The system also temporarily stores the scheduled meeting start & end time.

During a broadcast, AI Producer is processing text, audio, and video from the meeting. This data is processed in memory and is never written to a persistent storage.

Video

Playing video in a broadcast or into a meeting is part of the feature set. It is also possible to record a production. Both these features rely on Azure Storage accounts.

Record Production

It is possible to use a feature to record a production. This feature must first be enabled by an administrator of AI Producer before it can be used. If this optional feature is used, the production will temporarily be recorded to disk. When the production is over, the recording is moved to an Azure Storage Account (temporarily upload storage). After the file is moved, the recording is deleted from disk. In fact, the entire server environment hosting the software that produces the production is destroyed.

The recording is then sent as a file attachment - in a Microsoft Teams message - to the meeting producer who activated the recording. Once the producer has downloaded the recording, the file is deleted from the Azure Storage Account. In case the producer does not act on the Teams message attachment, the recording is automatically deleted after 30 days.

The customer may use their own Azure Storage Account for this temporary upload storage.

Video Playout

AI Producer offers a feature to play video in high quality in Teams Meetings and in broadcasts. The videos must first be uploaded to an Azure Storage Account to be available in the AI Producer Playout Library. It is recommended that a customer uses their own Storage Account to be in full control of the stored videos. LiveArena can also offer a Storage Account on behalf of the customer if needed.

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

User Consent & Microsoft Graph Permissions

As part of the installation process, AI Producer requires the following access to Microsoft Graph which is granted through permission consent.

AI Producer uses two types of permissions; "Delegated" and "Resource Specific Consent".

For "Delegated" permissions, the app will use the permissions of the current user of the app to gain momentary access on the same level as the user.

For "Resource Specific Consent" - RSC - permissions, the app only gains access to a specific instance of a data type, for example a single meeting.

Here follows a complete list of the permissions that AI Producer uses. None of these require admin consent.

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Microsoft Graph API / Permission name	Type	Description	Explanation
Calls.JoinGroupCalls.Chat	RSC	Join calls associated with this chat or meeting	Allows the app to join calls and scheduled meetings that it has been added to, as a bot.
Calls.AccessMedia.Chat	RSC	Access media streams in calls associated with this chat or meeting	Allows the app to get direct access to media streams in a call, as a bot. The bot can only access media in meetings that it has been able to join – see permission above.
User.Read	Delegated	Sign in and read user profile	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
openid	Delegated	Sign users in	Allows users to sign into the app with their work or school accounts and allows the app to see basic user profile information.
OnlineMeetings.Read	Delegated	Read Online Meeting	Allows an app to read online meeting details on behalf of the signed-in user.
ChatSettings.Read.Chat	RSC	Read this chat's settings	Allows the app to read chat settings of meetings associated with this chat.
ChatMember.Read.Chat	RSC	Read this chat's members	Allows the app to read chat members associated with this chat. This permission is used together with the permission below to keep an up-to-date list of the meeting participants.
OnlineMeetingParticipant. Read.Chat	RSC	Read information about participants in a meeting	Allows the app to read participant information, including name, role, ID, joined and left times, of meetings associated with this chat.
OnlineMeeting.ReadBasic. Chat	RSC	Read basic information about the associated meeting	Allows the app to read basic properties of meetings associated with this chat, such as name, schedule, organizer, join link, and start or end notifications.

How AI Producer uses these permissions

Calls.JoinGroupCalls.Chat - Join calls that the app has been added to

This permission is required to allow AI Producer to join calls. AI Producer will join the meeting as a participant. It must be able to join calls to be able to extract audio and video from the call to be able to create a production from the meeting,

Calls.AccessMedia.Chat - Access media streams in the call

When AI Producer joins the meeting, it will read the audio and video from the participants that have been selected to participate in the production. The app cannot read media from meetings it has not joined.

User.Read - Sign in and read user profile

This permission is used to check which Active Directory Groups that the user belongs to. Licenses and profile settings are dependent on these groups.

openid - Sign users in

Used for single-sign-on purpose so that the user can use their Microsoft account to log into the AI Producer app.

The token from this permission can be used to ask for on-behalf-of permissions, known as Delegated permissions.

OnlineMeetings.Read - Read Online Meeting

The app uses this permission when the app is added to a meeting to read information about who is invited to the meeting and when it starts and ends.

The app uses the information about the meeting and its participants to be able to collect the correct video and audio sources.

With this permission the app only gains access to the Online Meetings it has been added to. It cannot list all meetings in a users' calendar. For more details regarding this permission, see Microsoft documentation here:

https://learn.microsoft.com/en-us/graph/api/onlinemeeting-get?view=graph-rest-1.0&tabs=http

NOTE: AI Producer will work without this permission, but with the following limitation:

- External participants cannot be selected as presenters before they join the production meeting.

If this permission is not granted, the following four RSC permissions are used instead to fetch information about the meeting and its participants. These permissions can be considered a subset of the OnlineMeetings.Read permission:

- **ChatSettings.Read.Chat**
- **ChatMember.Read.Chat**
- **OnlineMeeting.ReadBasic.Chat**
- **OnlineMeeting.ReadBasic.Chat**

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

AI Producer bot, screen share & video

The AI Producer bot can display video to meeting attendees. It can either be by playing high quality video in a Teams meeting or by streaming a produced broadcast into a Teams meeting.

The bot can play this via its camera source using the permissions listed above. The bot can also play video via its screen share, but that requires an additional permission – *Calls.AccessMedia.All*, which is an *Application* permission. Contact LiveArena if this is of interest.

AI Producer Admin portal permissions

In addition to the Teams App, the AI Producer solution also offers an admin portal where administrators can configure settings for AI Producer, such as default branding, assign licenses to users, etc. This portal is not something a regular AI Producer user needs to access.

The admin portal requires access to the users in the Active Directory. These permissions are used for listing the users to be able to assign licenses to them.

All permissions are “Delegated”.

Microsoft Graph API / Permission name	Type	Description	Admin consent required	Details
User.Read	Delegated	Sign in and read user profile	No	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
User.ReadBasic.All	Delegated	Read all users’ basic profiles	No	Allows the app to read a basic set of profile properties of other users in your organization on behalf of the signed-in user. This includes display name, first and last name, email address, open extensions, and photo. Also allows the app to read the full profile of the signed-in user.
GroupMember.Read.All	Delegated	Read group memberships	Yes	Allows the app to list groups, read basic group properties and read membership of all groups the signed-in user has access to.
openid	Delegated	Sign users in	No	By using this permission, an app can receive a unique identifier for the user in the form of the sub claim. The permission also gives the app access to the UserInfo endpoint. The openid scope can be used at the Microsoft

				identity platform token endpoint to acquire ID tokens. The app can use these tokens for authentication.

How AI Producer uses these permissions

User.Read - Sign in and read user profile

Used to get the organization name of the logged in user.

User.ReadBasic.All - Read all users' basic profiles

Used for searching and listing users in the organization so that the administrator can assign AI Producer licenses to them. AI Producer does not store information about users that is listed in the admin portal. If a license is assigned to a user, only the users' ID is stored.

GroupMember.Read.All - Read group memberships

Used for searching and listing Active Directory groups and their members so that the administrator can configure specific AI Producer settings for separate groups. It is also possible to assign AI Producer licenses to whole AD groups. If an AD group is used for configuring AI Producer settings, the name of the AD group is stored by AI Producer. AI Producer does not store the members of AD groups.

openid - Sign users in

Used for single-sign-on purpose so that the user can use their Microsoft account to log into the AI Producer admin portal.

Limit the scope of the AI Producer app

There are a couple of ways you can limit the scope of AI Producer, meaning who can access the application in Teams.

Teams profile configuration: It is possible in the Teams Admin Center to setup profiles that determines who can see and access which app. More information about app permission policies can be found here:

https://learn.microsoft.com/en-us/microsoftteams/teams-app-permission-policies

AI Producer licenses: Even if a user can see the app, they will not be able to add it to a meeting without having a license to AI Producer. In the AI Producer Admin portal, you can configure who should be assigned a license. Licenses can be assigned to individual users or group of users, such as an Azure Active Directory Group.

Both can be combined, for example by enabling the app via Teams profiles to an entire region or department, and then restrict who can use the app using AI Producer licenses.

Data Sovereignty

All data resides within the EU (European Union) in datacenters managed by Microsoft.

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Data Security

LiveArena encrypts all data that is stored in the service according to NIST (National Institute of Standards and Technology) recommendations which meets EDBP's encryption recommendations for data at rest. The encryption is performed using symmetric encryption 256-bit AES with Microsoft platform managed key.

Data is only accessible over encrypted channels and is always authenticated.

Network Security

LiveArena encrypts all data in transit to and from the service according to Mozilla Intermediate compatibility or better which meets EDPB's encryption recommendations for data in transit. TLS (Transport Layer Security) is terminated between public and private networks meaning LiveArena's private network for SaaS or Customer's private network for Managed Application.

Private networks are both segmented and multi-layered with firewalls and proxies at the edge and additional network security controls between the different layers (I.e., applications and databases).

Administrative Access

All privileged accounts are protected with TOTP or Push Multi-factor Authentication. For additional security most administrative endpoints are also protected with VPN (Virtual Private Network).

All administrative access and operations are logged and shipped to a non-repudiable storage for 13 months.

SaaS vs. Managed Application

AI Producer is available as an Azure Managed Application as a deployment option to using the multi-tenant SaaS (Software as a Service) solution. There are a couple of distinct differences between SaaS and Managed Application:

1. The Managed Application is single tenant. Meaning it is not shared with any other customer.
2. The Managed Application is deployed into the customers Azure subscription. Meaning the customer is responsible for providing an Azure Subscription and managing capacity quotas and the cost for the Azure capacity. Thus, only paying LiveArena for the actual software licenses.

By design, some aspects are the same in both options:

1. AI Producer Microsoft Teams App. Meaning all customers use the same Teams App.
2. AI Producer Management API & Media Processor applications.
3. LiveArena has administrative access to AI Producer Management API & Media Processor to be able to deliver the service and ensure availability, reliability, and compliance. This means that LiveArena operates, monitors, patches, and upgrades the service.
4. AI Producer License Management & App Configuration service.

5. The customer does not see nor can access the underlying Azure resources that hosts the service.

Independent of which deployment option of AI Producer is used the customer is always responsible for approving the Teams App for use throughout their organization, manage consent and provide an RTMP target.

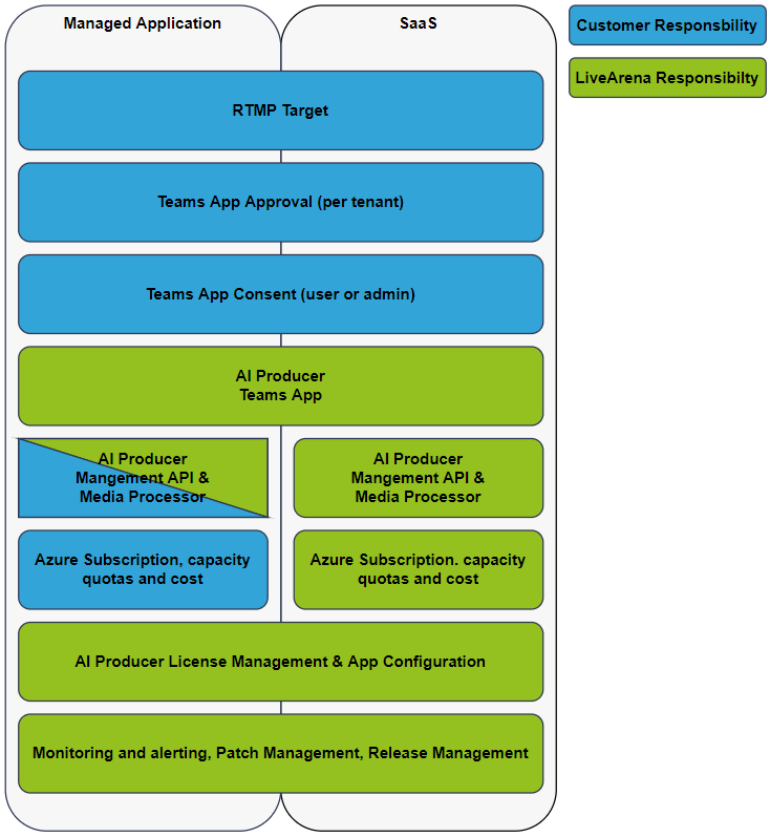
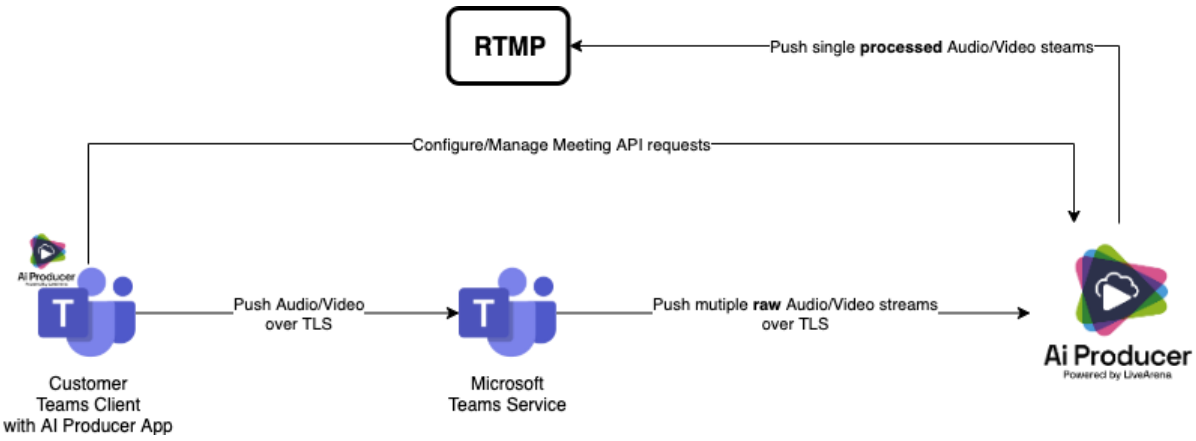


Figure: Responsibility Matrix

Published: 9/20/2023
Author: Daniel Grenemark
Revised by: Angus Dorrington
Approver: Andreas Björkman

Architecture



The AI Producer consists of 3 major components.

1. The AI Producer Microsoft Teams App (“Teams App”)
2. The AI Producer Management API (“Management API”)
3. The AI Producer media processing backend (“Meeting Stack”)

All components are built and maintained by LiveArena and hosted on Microsoft Azure.

The Teams App needs to be approved by the customer to their tenant before it is available for its users. Before using the application, it will ask for consent from the user (if allowed by the customer tenant) or it will need to be allowed by admin consent.

All requests between the Teams App and Management API are secured with TLS and authenticated with the user’s token from Teams. This token is also used for OBO requests to customer’s Graph API tenant.

The Management API will provision a dedicated and isolated compute unit for each individual meeting. The meeting stack receives the text, audio, and video stream from Microsoft Teams over TLS, which is always initiated by an authorized user, usually the meeting organizer. When the authorized user starts the broadcast, all media is processed, made available on the preview interface, and pushed to the configured RTMP target. After each meeting has ended the meeting stack is deleted.