SynergyXR ApS
Silkeborgvej 261-263
8230 Åbyhøj
Danmark

+45 86 17 18 33
contact@synergyxr.com

CVR 31177626

SynergyXR – IT Security Whitepaper

1. Introduction
   1.1. Background of the Solution

   In an era where immersive learning experiences blend seamlessly with cutting-edge technology, our no-code tool stands at the forefront, enabling users to create captivating multi-user journeys in Augmented Reality (AR) and Virtual Reality (VR). The platform's versatility extends across iOS, Mac, PC, and stand-alone VR headsets, providing a seamless and accessible environment for multi-user engagement.

   1.2. Purpose of the Whitepaper

   This document serves as a comprehensive overview of the robust IT-security infrastructure underpinning our platform. As the landscape of AR and VR learning experiences evolves, security becomes paramount. This document aims to enlighten stakeholders, including users, administrators, and partners, about the proactive security initiatives undertaken to safeguard data integrity, user privacy, and the overall reliability of our platform. This whitepaper clearly shows our unwavering commitment to providing a secure, innovative, and sustainable AR and VR learning platform.

   1.3. Audience

   1.3.1. Users

   Individuals leveraging our platform for content creation will gain insights into how their data is protected, ensuring confidence in sharing and collaborating within the immersive environment.

   1.3.2. Authors

Those engaged in creating and authoring experiences will understand the security measures in place to foster a secure and distraction-free learning atmosphere for users of the created content.

1.3.3. IT Administrators

Professionals responsible for managing the deployment and security of the platform within their organizations will find detailed information on the architecture and measures implemented.

2. Cloud-Based Content Backend Security

2.1. Overview of the Cloud Infrastructure

Our cloud-based content backend is the cornerstone of the SynergyXR platform, providing a scalable and secure environment for storing and managing user-generated content. The infrastructure is hosted in Microsoft Azure, a reputable cloud service provider, ensuring reliability and adherence to industry-leading security standards.

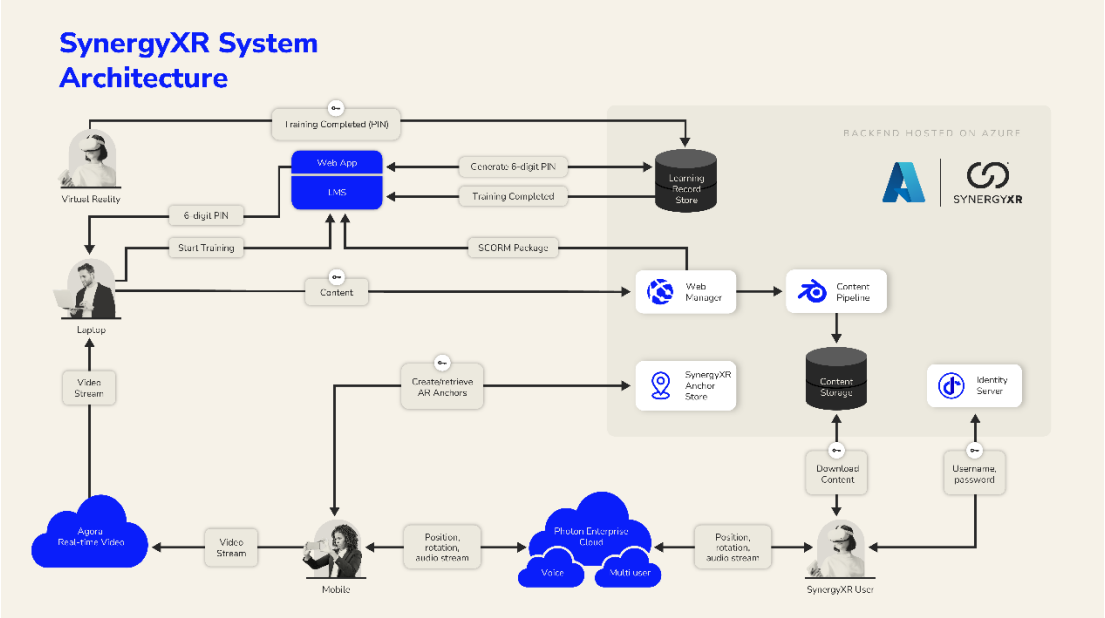

Figure 1: SynergyXR System Architecture

The SynergyXR backend is a fully hosted service deployed in Microsoft Azure - specifically in EU-West located in the Netherlands. We do not use dedicated servers, we manage ourselves. We rely on many of the security features offered by Microsoft Azure. This includes features like DDoS protection, network isolation, and traffic encryption through HTTPS.

Each customer gets their own instance of the SynergyXR content backend – these instances are called Workspaces. This means that data stored in one Workspace is stored in a separate Blob Storage, ensuring complete data

segregation of customer data in SynergyXR. User access is also segregated through Workspace access.

The Microsoft Azure Blob Storage and the associated Content Delivery Network (CDN) are where the raw files of the content are stored. Outbound traffic needs to be allowed for the following types of network traffic:

Hostname/IP	Protocol	Port	Description
cdne-sxr-synergysharedstorage.azureedge.net		443	HTTPS
synergysharedstorage.blob.core.windows.net	TCP	443	HTTPS
stsxrtips.z6.web.core.windows.net	TCP	443	HTTPS
stcachecontainer.blob.core.windows.net	TCP	443	HTTPS

To manage content, users, spaces and to plan online sessions, users will use the SynergyXR Web Manager. This is a Single-Page Application (SPA) hosted in Microsoft Azure. The Web Manager is written in Java Script using the Quasar Vue.js framework.

To store training results, as part of the Learning Management System (LMS) integration, SynergyXR hosts a Learning Record Store (LRS). This is a CosmosDB mapping of the LMS user ID, the SynergyXR user ID, the 6-digit PIN code generated by the system, and the results obtained during the training. This data is only stored until the training completion has been reported back to the LMS at which point the data is deleted.

In addition to the content backend, SynergyXR makes use of two external services: Photon Enterprise Cloud and Agora Real-Time Video Streaming Service. Read more about these in Section 2.4.

2.2. Access Controls and Authentication for Cloud Services

2.2.1. Access Controls:

2.2.1.1. Role-Based Access Control (RBAC)

Access to cloud services is governed by RBAC, ensuring that only authorized users have the necessary permissions to configure and manage the Workspace.

In SynergyXR, users can have one of four roles:

- Guest: time-limited user with read-only access. Cannot modify, add, or remove company assets. Can only join existing live sessions.

- Viewer: user with read-only access. Cannot modify, add, or remove company assets. Can create new sessions.
- Author: user with write access. Authors can upload new content, delete content, and save modifications to assets.
- Admin: can manage users - add new user, delete user, and change user access levels.

The customer can use all these roles to best suit their needs regarding RBAC.

2.2.2. Authentication Mechanisms

2.2.2.1. Token-Based Authentication

Users and services connecting to the cloud backend authenticate through token-based mechanisms, adding an extra layer of security during communication.

All API endpoints are fully authoritative requiring a valid access token. When our services connect to Microsoft Azure resources, the connection stays within Microsoft Azure and doesn't cross any network boundaries. However, the connection goes through the shared networking in Microsoft Azure, and to ensure proper security, communication between Blob Storage and our CosmosDB is also HTTPS encrypted.

2.2.2.2. Secure Identity Management

Integration with secure identity management systems ensures that only valid and authenticated users can access the cloud services.

The synergy backend handles secure user authentication via Duende IdentityServer4 which is an OpenID Connect and OAuth 2.0 framework for ASP.NET Core.

All communication between apps and backend is fully authoritative requiring a valid access token. HTTPS is used for all communication secured through TLS.

Outbound traffic needs to be allowed for the following types of network traffic as listed here:

Hostname/IP	Protocol	Port	Description
login.synergyxr.com	TCP	443	HTTPS
storage.synergyxr.com	TCP	443	HTTPS
portal.synergyxr.com	TCP	443	HTTPS

2.3. Data Storage Security

2.3.1. Encryption of Stored Content

2.3.1.1. Data-at-Rest Encryption

User-generated content, including 3D models, images, PDFs, and videos, is encrypted at rest, preventing unauthorized access to stored data. Microsoft Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Microsoft Azure Storage encryption protects your data and helps you to meet your organizational security and compliance commitments. Read more here: https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption

2.3.1.2. Key Management

Robust key management practices are employed to safeguard encryption keys, ensuring the confidentiality of user content. We configure all our services to retrieve their sensitive data (connection strings, API keys) from Microsoft Azure Key Vault for additional security.

2.3.2. Backup and Recovery Processes

2.3.2.1. Regular Backups

Microsoft Azure Backup provides a simple, secure, cost-effective, and cloud-based backup solution to protect your data stored in SynergyXR. Read more here: https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview

2.3.2.2. Soft Delete

SynergyXR utilizes Soft Delete to protect customer data from accidental deletes or overwrites. This is done by maintaining the deleted data in the system for 30 days. During the retention period, we can help the customer restore a soft-deleted object to its state at the time it was deleted. After the retention period has expired, the object is permanently deleted.

2.4. Third-party Services

2.4.1. Photon Enterprise Cloud

Photon (https://www.photonengine.com/) is an industry leader in providing fully hosted real-time multi-user services. In SynergyXR we use their “Enterprise Cloud” service ensuring that the service is hosted

on dedicated hardware with static IP enabling users of SynergyXR to whitelist these IP-addresses.

Outbound traffic needs to be allowed for the following types of network traffic:

Hostname	IP	Protocol	Port	Description
pi_unitystudios-eu-ns.exitgames.com	52.157.184.50	TCP	4533	Client to Nameserver
azeu704-master.exitgames.com	52.157.78.135	TCP	4530	Client to Master Server
azeu704-game.exitgames.com	52.157.74.166	TCP	4531	Client to Game Server
	52.157.184.42	TCP	4531	IP of VM

(see more here: https://doc.photonengine.com/en-us/realtime/current/connection-and-authentication/tcp-and-udp-port-numbers)

Photon hosts their service in Microsoft Azure, in the EU-West region, located in the Netherlands.

2.4.2. Agora Real-Time Video Streaming

Agora is a global leader in Real-Time Engagement, providing developers with simple, flexible, and powerful APIs, to embed real-time voice, video, interactive streaming, chat, and artificial intelligence capabilities into their applications.

SynergyXR makes use of their video streaming capabilities to ensure all users see the exact same view of the SynergyXR web browser.

Agora maintains a document describing the firewall requirements: https://docs.agora.io/en/video-calling/reference/firewall?platform=unity. All communication happens over port 443 using TCP, so this rarely causes any issues.

3. Device and Client Application Security

3.1. Security Measures on Devices

3.1.1. Data caching

To optimize the data traffic, all data is automatically cached on the device. Every time a Space is loaded, the system automatically detects if a new version of data is available on the content backend, or if the cached data can be used.

Every time a user logs out of SynergyXR, all cached data is automatically deleted from the device. If a user switches to another Workspace, all cached data is also deleted.

3.1.2. Regular Security Updates

We aim to provide new updates to SynergyXR every three months. New versions of SynergyXR are made available on one of several platforms:

- iOS and iPadOS: iOS app store
- visionOS: Vision app store
- PC: Microsoft Store
- Meta Quest VR devices: Meta Quest Store (App Lab), ManageXR Instant App, ArborXR content sharing, Quest for Business app sharing
- HTC VR devices: HTC VIVE Business App Store, ManageXR Instant App, ArborXR content sharing
- Pico VR devices: Pico Business Store, ManageXR Instant App, ArborXR content sharing
- For manual distribution: The SynergyXR download page: https://portal.synergyxr.com/download

To ensure proper compatibility, we only allow users to use the latest version of SynergyXR. Once a new version has been released, users on older versions are prompted to install the new version before being able to proceed.

3.2. Secure Communication Between Devices

3.2.1. Multi-user Security

All users engaged in multi-user collaborative sessions in SynergyXR download the necessary content directly from the SynergyXR content backend. No customer data is ever transferred over the Photon Enterprise Cloud – only simple data that is necessary to synchronize the experience for all users. This includes 3D positions of users, their rotation in 3D space, as well a remote procedure calls (RPC) for the actions they are performing.

3.2.2. Voice Communication Security

SynergyXR uses Photon Voice hosted on the Photon Enterprise Cloud as Voice over IP (VoIP) technology solution. All voice communication is encrypted – read more here: https://doc.photonengine.com/voice/current/reference/encryption

4. User Data Protection
    4.1. Data Protection Officer

        We recognize the paramount importance of safeguarding user data and ensuring compliance with data protection regulations. To further strengthen our commitment to data privacy, we have appointed Sune Wolff, our CTO, as the dedicated Data Protection Officer (DPO).

        In this role, Sune Wolff assumes the following key responsibilities: regulatory compliance; policy development; data subject rights; monitoring and auditing; and privacy impact assessments.

    4.2. Privacy policy and data handling practices

        4.2.1. GDPR Compliance

            Given the international user base, we are committed to GDPR compliance. User consent mechanisms, data access requests, and data erasure policies are integral components of our solution.

            Please see our Data Processing Agreement which is part of our general Terms & Conditions (see Schedule 1 of: https://synergyxr.com/terms-and-conditions/)

5. Real-Time Monitoring and Logging
    5.1. Continuous Monitoring

        5.1.1. System and Application Monitoring

            We use Microsoft Azure Security Center which provides unified security management and advanced threat protection across cloud workloads. Microsoft Azure Security Center continually monitors and enhances our security posture. This tool keeps us informed about compliance, provides security recommendations, identifies potential attack paths, and highlights areas for improvement. It's a crucial component in our commitment to maintaining a secure environment.

6. Company Security Initiatives
    6.1. Security Officer

        We recognize the critical importance of a dedicated leadership role in ensuring the ongoing effectiveness of our security initiatives. Sune Wolff, our Chief Technology Officer, has been appointed to the position of Company Security Officer. In his role, Sune Wolff undertakes strategic oversight; policy development; incident response leadership; technology evaluation; and user education and awareness.

    6.2. Company User Access Management

As a company, SynergyXR uses Microsoft Entra (previously known as Azure Active Directory (AAD)) as a cloud-based identity and access management service that helps your secure access to your applications and data. All employees use Multi-Factor Authentication (MFA - rolled out via policies) and only a selected few colleagues have access to the Microsoft Azure portal (managed through security groups).

We follow the Principle of Least Privilege regarding user access to ensure employees only have the necessary access rights to fulfill their job. We also perform a periodic user access review, ensuring Principle of Least Privilege is respected.

Part of our offboarding process also ensures that user accounts are deleted/disabled ensuring leaving employees do not have access to any systems, services or tools.

6.3. Development Environment

All source code is version-controlled, and under a 3-2-1 backup scheme (3 separate backups, located at least 2 different physical locations, at least 1 of which is off-site).

During development, we have development, test and production environments. Customer data is only stored in the production environment.

6.4. Compliance and Certifications

At SynergyXR we are in the process of obtaining the internationally recognized ISAE 3402 attestation. The audit is performed by Grant Thornton and the audit report is expected to be obtained in Q1 2025.

As part of this process, we have built our Information Security Management System (ISMS) following the guidelines defined in ISO 27002.

7. Future Security Roadmap

7.1. Planned security enhancements and updates

7.1.1. Single Sign-On Support

We do currently not support SSO. The obvious technical option would be to use MSAL (Microsoft Authentication Library) - unfortunately, MSAL is not supported by Unity which is the underlying engine of SynergyXR.

We are currently actively investigating using OAuth using a MSAL-like flow for SSO. We are initially targeting Microsoft Entra ID (Azure AD) as

the underlying authentication service, but OAuth should be flexible enough to be used for other authentication systems as well.

7.1.2. Security Assessment

Every two (2) months, we perform various security scans of SynergyXR. This results in a Security Assessment Report – find the latest here: https://knowledge.synergyxr.com/security-assessment-report.

7.1.3. Penetration Test

We are discussing partnership with Cobalt (https://www.cobalt.io/), utilizing their Pentest as a Service (PtaaS) platform for 3rd party penetration tests. Please, reach out for further inquiries.

7.1.4. Microsoft Azure Security Certification

Several of our backend engineers are currently working on their Microsoft Azure Security Engineering certification. Read more here: https://learn.microsoft.com/en-us/credentials/certifications/azure-security-engineer/

8. References

8.1. General Terms & Conditions

You can find the SynergyXR General Terms and Conditions here: https://synergyxr.com/terms-and-conditions/.

8.2. Data Processing Agreement

Included in the T&C as “Schedule 1” you can find our DPA.

8.3. Service Level Agreement

Included in the T&C as “Schedule 2” you can find our SLA.

8.4. Privacy Policy

You can find the SynergyXR Privacy Policy here: https://synergyxr.com/privacy-policy/.

Appendix A: Network Specification

The following IP/ports must be accessible to run SynergyXR – either through proxy settings or firewall whitelisting.

Hostnames and IPs

We don't always use dedicated IPs. For some scenarios we know the hostnames, and they are always the same not subject to change like "login.synergyxr.com" and "portal.synergyxr.com" but the IPs may be dynamic.

Fundamentals (DNS)

The client will need to be able to make DNS queries to function properly (UDP and TCP port 53).

SynergyXR Backend Hosted by Microsoft Azure

Outbound traffic needs to be allowed for the following types of network traffic as listed here. As this is regular HTTPS traffic it should be possible to do this via proxy.

Hostname/IP	Protocol	Port	Description
cdne-sxr-synergysharedstorage.azureedge.net		443	HTTPS
synergysharedstorage.blob.core.windows.net	TCP	443	HTTPS
stsxrtips.z6.web.core.windows.net	TCP	443	HTTPS
stcachecontainer.blob.core.windows.net	TCP	443	HTTPS

CDN and Azure Blob Storage

Outbound traffic needs to be allowed for the following types of network traffic as listed here. As this is regular HTTPS traffic it should be possible to do this via proxy

Hostname/IP	Protocol	Port	Description
login.synergyxr.com	TCP	443	HTTPS
storage.synergyxr.com	TCP	443	HTTPS
portal.synergyxr.com	TCP	443	HTTPS

Photon Engine

Outbound traffic needs to be allowed for the following types of network traffic as listed here.

Hostname	IP	Protocol	Port	Description
pi_unitystudios-eu-ns.exitgames.com	52.157.184.50	TCP	4533	Client to Nameserver
azeu704-master.exitgames.com	52.157.78.135	TCP	4530	Client to Master Server
azeu704-game.exitgames.com	52.157.74.166	TCP	4531	Client to Game Server
	52.157.184.42	TCP	4531	IP of VM