



Technical compliance information

Security, infrastructure, and network requirements for IT and security teams

Company and contact



Software and company

Software: InvolveXR
Company: Lumeto



Contact

Ben Unsworth
793 Pharmacy Ave, Toronto ON, M1L 3K2



Data center

Cloud, provisioned by a third-party vendor.
Microsoft Azure, East US region, Richmond, Virginia.



Backups

Azure automatically backs up database and storage on hourly intervals, plus daily, weekly, and monthly cycles.



Server environment (Azure)

All cloud infrastructure is provided by Azure. Key services include:
Azure SQL Database • Azure Blob Storage • Azure App Service • Azure Active Directory B2C

Encryption at rest and in transit

Azure services meet or exceed industry standards, including NIST recommendations. Microsoft continuously monitors and updates these practices.



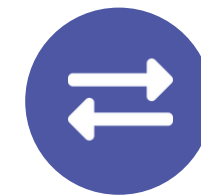
Data at rest

AES-256 encryption across all storage.

App Services: Transparent Data Encryption (TDE); underlying Azure Storage uses AES-256.

SQL Database: TDE encrypts database files, backups, and transaction logs using AES-256.

Blob Storage: AES-256, encrypted before persisting to Azure Managed Disks and decrypted transparently on retrieval.



Data in transit

TLS 1.2 and 1.3 with strong cipher suites.

App Services: TLS with strong cipher suites; supports TLS 1.2 and 1.3.

SQL Database: TLS protects data between the database and client applications; supports TLS 1.2 and 1.3.

Blob Storage: HTTPS with TLS protects data moving between storage and clients.

Compliance posture



Certifications

SOC 2 and ISO 27001 currently under preparation. Working toward SOC 2 Type 2, expected completion Q2 2025.



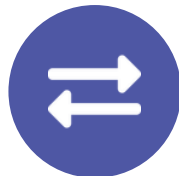
Auditing

Internal and external auditing performed annually. SOC 2 audit will be annual, starting Q2 2025.



Backup retention and restore

Lumeto DevOps staff can restore backups of cloud data when needed. SOC 1/SSAE, SOC 2, and SOC 3 reports available on request.



Exit policy

At the end of a contract, customer data is removed by request via email.



PII / PHI

No PII/PHI stored other than name, email, and some lesson session metrics.



Background checks

Full-time employees are subject to background checks as per Lumeto security policies.

Three applications



Admin Portal

Web application

Access: healthcare.lumeto.com

Security: SSL

API: GraphQL (Azure web service)

Use: Operation and content management for the platform.



Instructor App

Windows application

Format: .EXE, published under Microsoft License

Delivery: Installer file, manual install on any Windows PC. .EXE available on request for large orgs.

API: gRPC (Azure web service)

Updates: Approx. every 3 months

Mode: Instructor Led Training (ILT). Used by teachers to control a live simulation.



VR App

Oculus application

Format: APK

Delivery: Mostly the Oculus Store; also Meta for Business, ArborXR, or manual.

API: gRPC (Azure web service)

Updates: Approx. every 3 months

Mode: ILT and Self Directed Learning (SDL). Used by students to access the simulation.

Firewall and network requirements



Connection

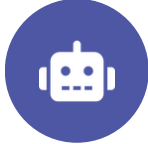
The Admin Portal communicates with the backend over a secure GraphQL API. Permit the connections below.
Note: the security team excluded healthcare-prod-client-api.lumeto.com from SSL inspection.

Setting	Requirement
IP addresses (in/out)	20.119.0.11, 20.42.5.0/24, 20.21.6.0/23
Port	Outbound TCP 443 (secure HTTPS)
Protocols	TCP and TLS v1.3 must be allowed through the firewall

These are the server addresses the application uses for all operations. Allowing TCP 443 is essential for the secure HTTPS communication the platform relies on.

Real-time components in our applications

Components used in real time by the Admin Portal, Instructor App, or VR App. Server-side services that need no customer security action are not listed. Full IP allowlists are in the appendix.

	Vivox	Real-time voice between learners and instructors in VR.	TCP 80/443, UDP 12000-52000
	Azure cloud services	GraphQL and gRPC APIs, blob storage, CDN, and speech-to-text.	HTTPS over TCP 443
	Cognitive3D	XR analytics used only to improve platform experience.	SSL / TCP 443
	PlayFab	Multiplayer interaction, session and player management.	UDP 30000-31000
	Conversation AI (OpenAI)	Dynamic patient conversations and NPCs, OnScreen learners.	HTTPS via api.openai.com

Vivox firewall guidance



What Vivox does

A communication platform for real-time voice between participants (learner and instructor) in VR. Ports: TCP 80 and 443 (HTTP/HTTPS), UDP 12000-52000 (voice media, RTP).



Important: apply exceptions carefully

Subnet masks matter. Most subnets end in /23 or /24. Entering one for the other can leave out the second half of a subnet.

Watch SSL interception. Some firewalls intercept web SSL traffic and block XMPP as not permitted, so exceptions must be made.

Test every device type. If one machine type works (console or PC), it does not mean firewall restrictions are not blocking the others.

Allowlist current as of May 21, 2024. See the appendix for the full subnet and domain list.

Solution components

The InvolveXR platform spans client applications, Azure services, and external service vendors. The full diagram follows on the next slide.



InvolveXR clients

- VR Game Client
- PC Game Client
- Web Portal



InvolveXR Azure services

- GraphQL Web Client API
- gRPC Game Client API
- Web Portal NextJS App
- Speech to Text Model VMs
- Text to Speech Azure Services
- Azure SQL
- Azure B2C
- Azure Function Text to Speech



External service vendors

- OpenAI
- Vivox VoIP
- PlayFab Game Server VM Containers

InvolveXR solution architecture

InvolveXR Solution Architecture

InvolveXR Clients

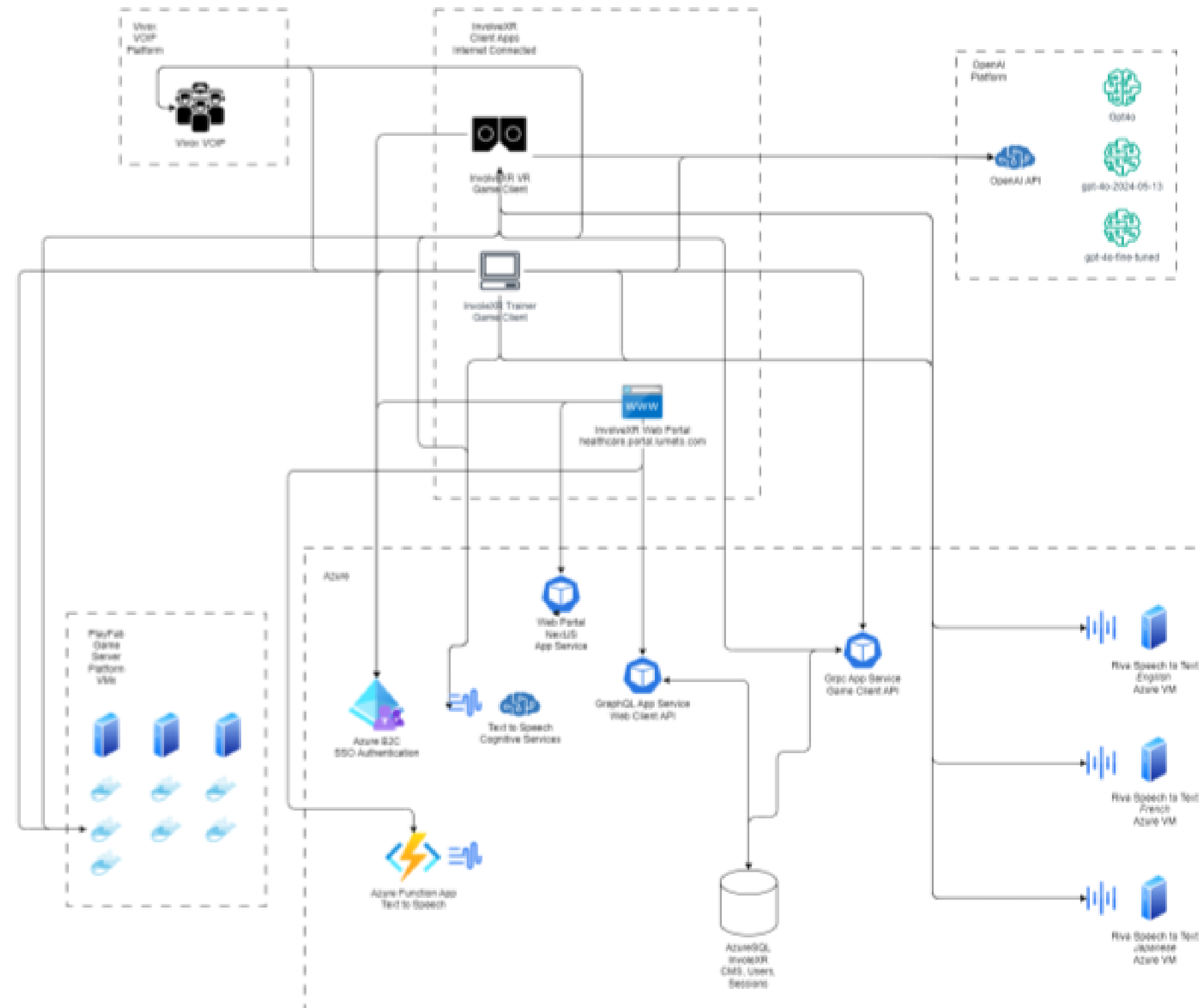
- VR Game Client
- PC Game Client
- Web Portal

InvolveXR Azure Services

- GraphQL Web Client API
- GRPC Game Client API
- Web Portal NextJS App
- Speech to Text Model VMs
- Text to Speech Azure Services
- Azure SQL
- Azure B2C
- Azure Function Text to Speech

External Service Vendors

- Open AI
- Vivox Voip
- Playfab Game Server VM Containers



APPENDIX

Full IP allowlists and endpoints

Vivox • Cognitive3D • PlayFab • Conversation AI (OpenAI)

Vivox subnets and domains

Current as of May 21, 2024. Ports: TCP 80/443 (HTTP/HTTPS), UDP 12000-52000 (voice media, RTP).

IP subnets	
63.251.140.0/24	74.201.105.108/30
69.25.124.0/23	85.236.96.0/21
70.42.8.0/24	188.42.95.0/24
70.42.198.0/23	188.42.147.0/24
74.201.102.0/23	216.52.53.0/24
74.201.106.0/23	

Domains
vivox.com
mt2p.vivox.com
mt2p.www.vivox.com

Analytics and AI endpoints

Cognitive3D XR analytics, SSL (TCP 443). Docs: docs.cognitive3d.com/firewall

Endpoint	Host	Addresses
Data collector	data.cognitive3d.com	54.83.239.136, 52.3.93.141, 50.16.188.224
API	api.cognitive3d.com	34.224.171.23, 52.54.161.208, 54.221.211.219

Conversation AI (OpenAI) Powers patient conversations, interaction tracking, and non-patient characters for OnScreen learners.

Host	Addresses	Status pages
api.openai.com	172.66.0.243, 162.159.140.245	status.openai.com, openai-status.llm-utils.org

Note: OpenAI addresses are a non-authoritative DNS answer and may change.

PlayFab multiplayer networking



How it works

PlayFab is a suite of cloud solutions for multiplayer interaction, session management, and player management. The headset initiates communication to the Azure PlayFab server. Object positional replication for Unreal Engine multiplayer runs over UDP on the PlayFab port ranges, synchronizing game objects and data across VR and desktop clients.

Setting	Requirement
Port range	30000-31000 for game traffic (inbound and outbound), all VMs
Location	Azure, East US, Richmond, Virginia
IP list	Azure virtual network service tags; ServiceTags_Public JSON (dated 12 Nov 2024)

Clients connect to game servers via Azure virtual network service tags. The full Microsoft ServiceTags_Public JSON (change number 332, dated 12 Nov 2024) is embedded below (double-click the file icon to open or save it).

ServiceTags_Public_20241111.json
Embedded file, change number 332. Double-click to open or save.