Nesos vs Zoom

Why Meetis is a safer, more transparent platform for your meetings.

Introduction

Nesos is the first Italian Cybersecure Management Online Platform for video conference meetings, webinars, online courses, live chat, e-commerce, streaming and podcasting which provides a fully integrated, encrypted, untraceable, protected and threat free video communications ecosystem for Institutions, corporate and any other Organisation.

With the majority of communications taking place over long distance and mediated by technology, the increasing awareness of the importance of interception issues, a secure online video conference platform represents one of the most compelling factors of trust for firms and an obligatory requirement in Government bodies.

What is Meetis

The Nesos Ecosystem allows you to manage every aspect of an e-learning experience in one single platform with additional webinar and video conferencing capabilities. Create, Schedule, Sell, Deliver and Analyse your Courses, Meetings or webinar with ease in our online cloud based software.

As part of this ecosystem, to facilitate communication and collaboration while avoiding needing the use of another software and a possible compromise in security, we developed Meetis.

Meetis is our online learning and video conferencing environment and it is an integral part of the wider Nesos ecosystem. Unlike most other video conferencing software, Meetis has been designed from the ground up to ensure absolute privacy and security whether it is to protect users' privacy, children/pupils identities or corporate secrets.

Even though it has a slightly different focus than Zoom, it remains a competitor and for that reason it makes sense to compare the two and that's what this document sets out to do.

What is Zoom

Zoom is a cloud-based SaaS application that allows private individuals as well as businesses to virtually interact with each other. Communication can occur via text, audio, video, or a combination of the three.

Zoom is owned by Eric Yuan, a Chinese-American billionaire who acts as its CEO.

Feature Comparison

	Meetis	**Zoom**
HD Video	✔	✔
HD Audio	✔	✔
Camera Feed	✔	✔
Audio Only	✔	✔
Live Chat	✔	✔
Scheduling	✔	✔

Calendar Scheduling	✔	✔
Waiting Rooms	X	✔
Recordings	✔	✔
Custom Background	✔	✔
Comprehensive Branding	✔	X
File Sharing	✔	✔
File Editing	✔	X
Shared Notes	✔	X
Whiteboard	✔	✔
Closed Captions	✔	✔
Polls	✔	✔
Breakout Rooms	✔	✔
Users moderation	✔	✔
Non Verbal Comms	✔	✔
Screen sharing	✔	✔
Screen Audio sharing	✔	✔
Private Deployment	✔	X
Lan protection	✔	X
Custom Domain	✔	X
Custom Firewall	✔	X
Cross Platform	✔	✔
No Download Required	✔	X
No App required	✔	X
Works in browser	✔	X
PWA	✔	X

Concerns about Zoom’s Business Model

On the surface, Zoom operates on a freemium subscription model, which means it offers various plans with prices based on users and usage.
On top of the subscriptions for meetings, Zoom offers workspaces, webinar functionality and voIP features.

Zoom is a multinational company with an impressive revenue and unlike many other tech companies, it seems to be profitable.

So, we have a profitable multinational tech company with impressive growth, everything sounds great if not for a couple of developments that have cast a shadow of doubt over what Zoom's actual business model is.

The first one is the introduction of ads in their platform, which would not be necessarily a concern per se, if not for the fact that any advertising platform, to be profitable, needs reliable profiles of their users. Therefore it would be legitimate to suspect that Zoom could be tempted to harness the power of their userbase’s data to profile and identify potential customers to serve ads to.

If one considers that to be far fetched or improbable, I would point out that Zoom is being sued for illegally selling data to Facebook (Meta).
The lawsuit alleges that Zoom's software reported to Facebook whenever a Zoom user logged on for a conference call, a lawsuit filed Monday stated. After a user logged on, Zoom gave Facebook the person's customer information, including what device a person used to access Zoom, the device's model and the device's unique advertising identifier regardless of whether the user even had a Facebook account.

With the introduction of speech recognition AI, centralised database, alleged lawsuit about data sales, is it ungenerous to wonder whether your meetings, especially if on the free plan, are being listened to, transcribed and used for commercial purposes?
To add to all this Zoom reportedly violated it’s own terms of service to gain access to the Chinese market and actively censored its users per request of the Chinese government.

More details can be found here https://www.tomsguide.com/uk/news/zoom-china-blocking.

A quick google search on Zoom Censorship will yield many more results, some even concerning western countries.

Zoom Security Concerns

Zoom has had its fair share of problems, and rewriting them all here would be redundant, instead we want to highlight a few with links to more comprehensive resources. The aim here is not to condemn mistakes, those happen, but more to give an idea of scale, repercussions and allow the user to evaluate whether these are all mistakes as reported or if there was a more shady intention to work with user data, in a gray close to black area.

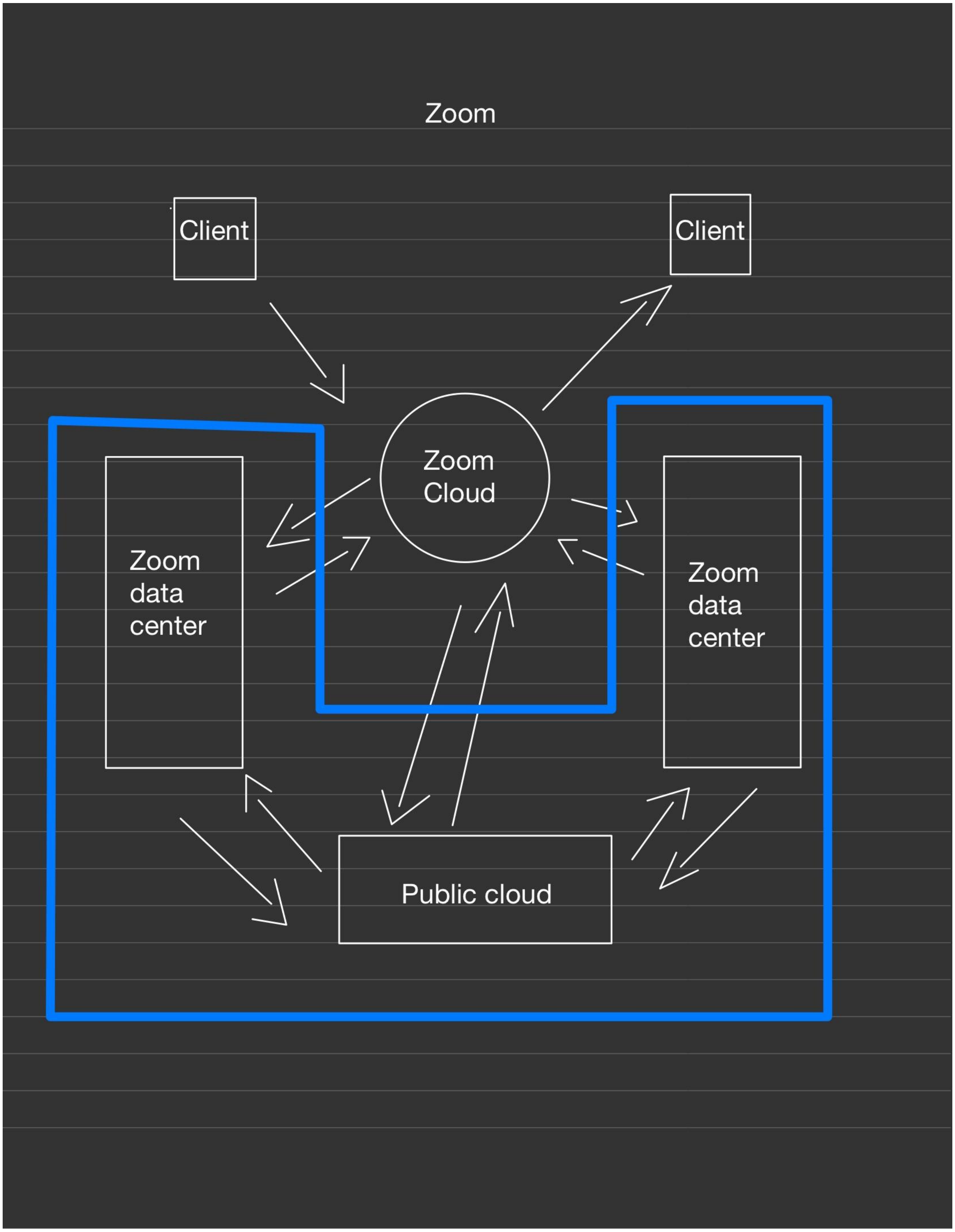
Zoom settles US class action privacy lawsuit for $86m
The lawsuit alleged that Zoom had invaded the privacy of millions of users by sharing personal data with Facebook, Google and LinkedIn.

It also accused Zoom of misstating that it offers end-to-end encryption and for failing to prevent hackers from "zoombombing" sessions.

Zoom even declared that their definition of End-To-End encryption is not the same as the common one used, most likely to get out of having to admit lying to their users about implementing it.

Here you can find a comprehensive list of Zoom blunders and whether the issues have been fixed, the list is long.

The Zoom Infrastructure



Zoom Vulnerabilities

By operating in a decentralised cloud infrastructure Zoom is able to serve with a single scaling deployment millions of users around the world.

This though, exposes Zoom to a wide variety of attacks, some of which are not even made by professionals (Zoombombing anyone?) due to faults in their design and inherent limitations of their infrastructure added to their notoriety and widespread use.

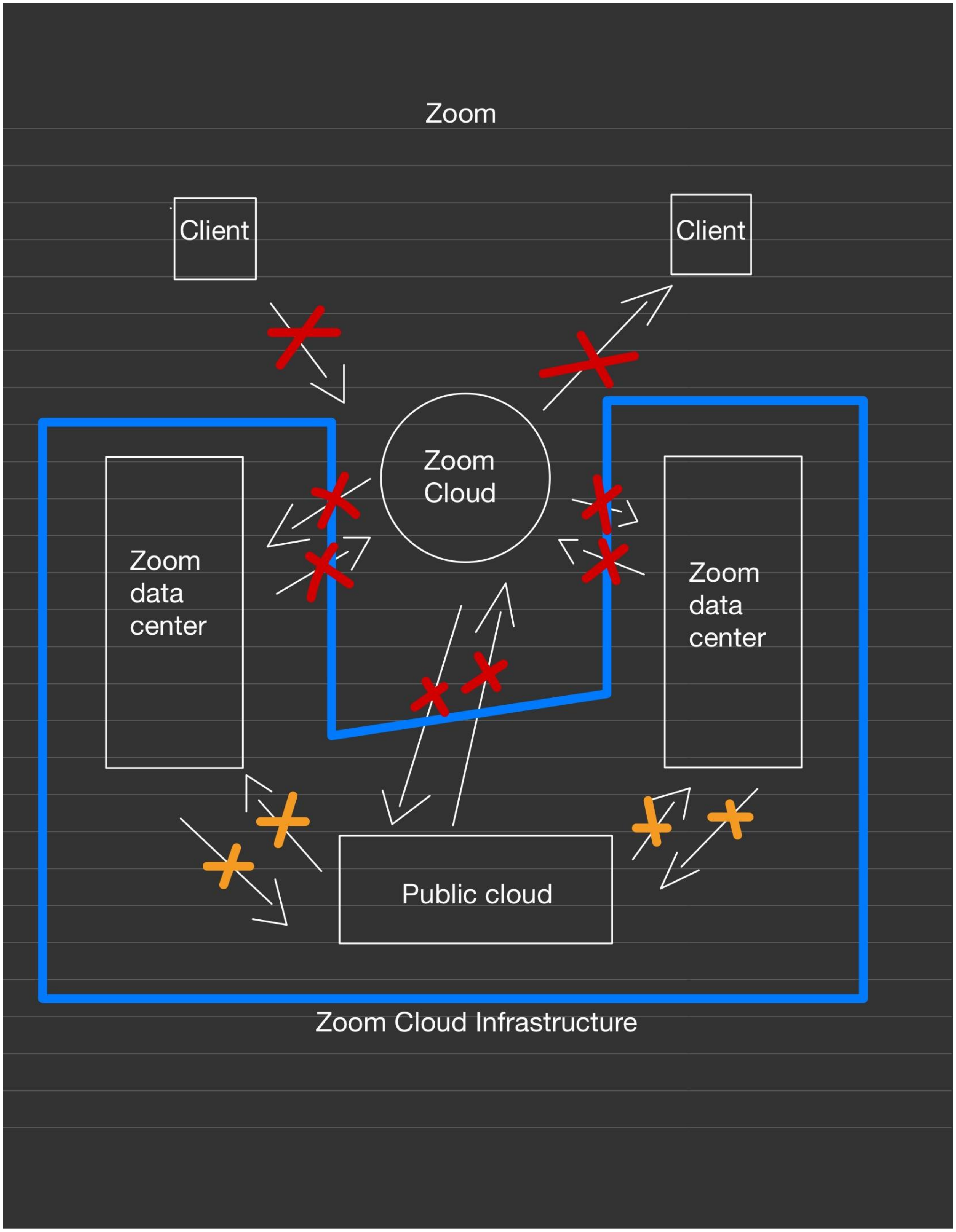
All communications from Zoom clients is collected centrally by the Zoom cloud and redistributed through their network of data centres and public cloud in various locations around the world. This makes the Zoom cloud a convenient target for attackers or interceptions.
The zoom client is installed as an app on the operating system, exposing it to inherent risks of the platform it operates on as shown in previous sections of this article.

Even inside the Zoom cloud infrastructure the communication happens between different geographical locations exposing the data to the wide area network and therefore making it more vulnerable to exploits.

As reported by Hackread the cybersecurity researchers at Positive Technologies identified three vulnerabilities in several critical apps part of the Zoom video conferencing platform (both apps and tools). These include Zoom Virtual Room Connector, Zoom Meeting Connector Controller, and Zoom Recording Connector.

These vulnerabilities could have allowed hackers to intercept your Zoom meetings and target customer infrastructure.

To top all of this off, the centralised nature and branding of the Zoom platform make it a prolific target of phishing and impersonation attacks via email or text.


Zoom
Client
Client
Zoom Cloud
Zoom data center
Zoom data center
Public cloud
Zoom Cloud Infrastructure

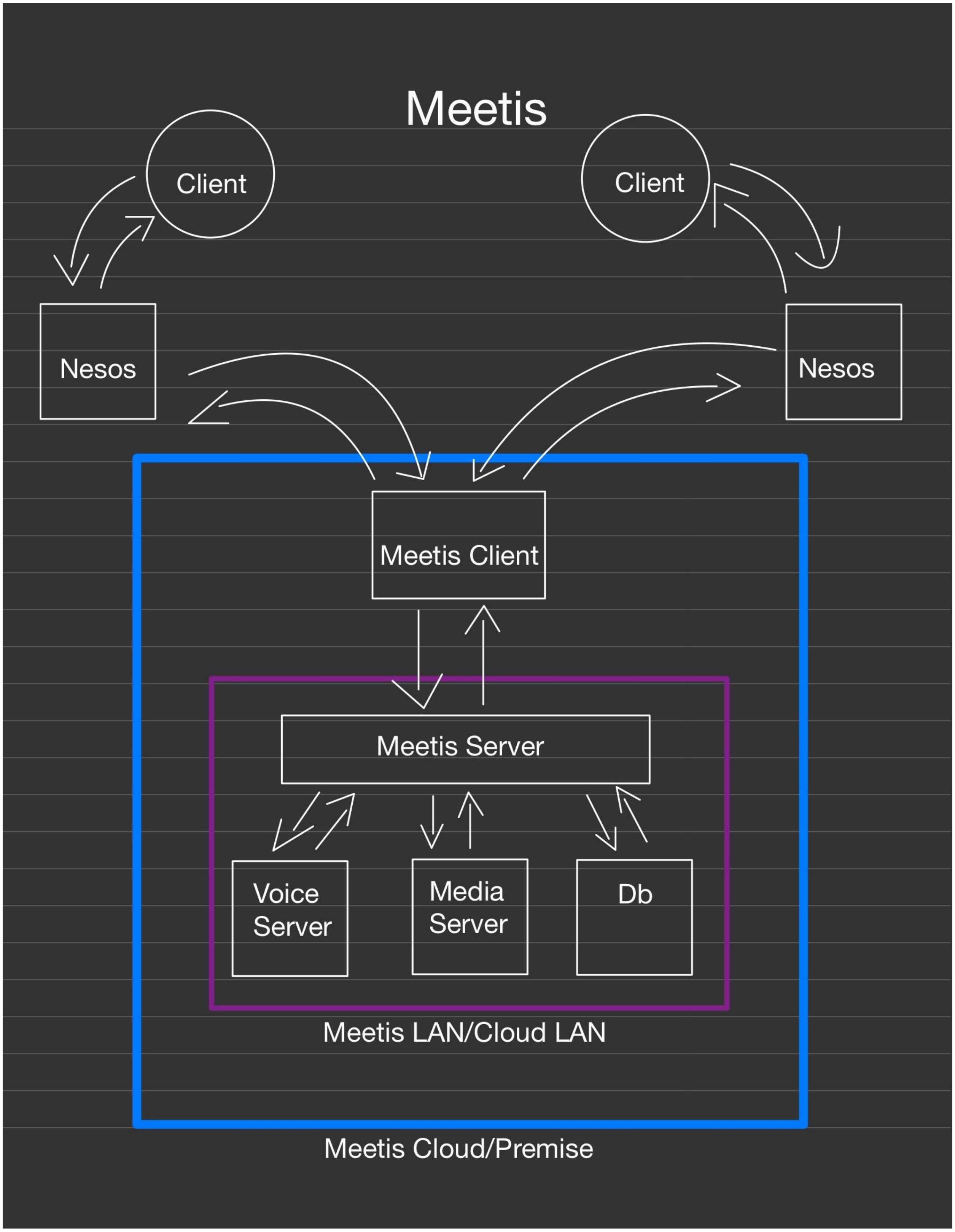
Meetis’ Transparency

Our company Cygnus Tech Solutions Ltd. does not gather, use, sell or disclose any of the data within Nesos or Meetis. It has never been our aim and it never will bel, it is not part of our business model and we are dubious about the ethics of it.

Each Nesos deployment has its own database so that each customer can have control over their data, where it is stored and who has access to it.

In this way the customer does not have to worry about compliance with GDPR like protocol nor worry about ever having their or their own clients data exposed.

Meetis’ Infrastructure



Meetis’ Vulnerabilities

From the diagram below we can see that the only communication that goes through the public internet infrastructure is the one from the user device to Nesos itself and then from Nesos to the Meetis installation in the Meetis Cloud or on premise.

We consider these channels secure though, as the communication from the user’s client to Nesos is encrypted and can be restricted to desired IPs, the specific MAC address of authorised devices and even set up to be accessible only through an Azure virtual client.

Nesos deployment is protected from attacks by Firewalls and by Azure Front Door, Microsoft’s modern cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications’ static and dynamic web content across the globe. This allows us to guarantee that Nesos is a secure application with built-in layer 3-4 DDoS protection supported by Threat Intelligence and access to its APIs is protected by a zero-trust access model.

The communication between Nesos and the Meetis environment is even more secure given the fact that each Nesos deployment has to match a specific Meetis deployment and everything can be setup on custom domains making it much harder to be found by automatic sniffing bots.

Even if the Meetis server was identified the attacker would have to discover the specific meeting id, have the Nesos credentials on top of the Nesos specific passwords that are automatically created with every meeting.

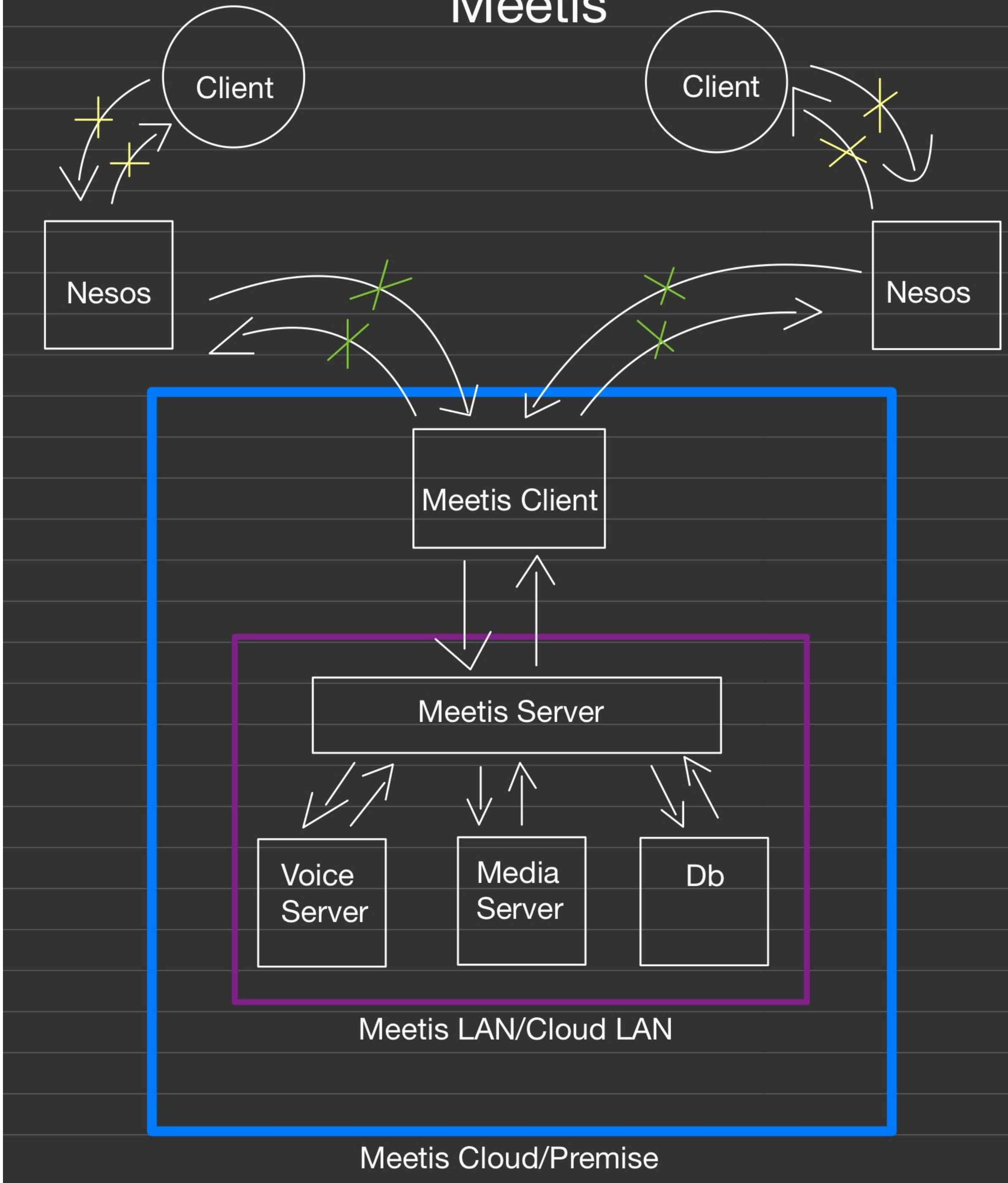
And this is assuming that any attacker could get past Sauron, the first Italian Artificial Cyber Security Operator able to simulate a Security Operation Center. Sauron deeply analyses the behaviour and intention of each process running in every connected device, in order to identify and block proactively, automatically and in real-time, for the smoothest possible business continuity any malware, hacker attacks and data theft while revealing the attackers’ identity.

Meetis fully integrates with Sauron to further protects its server and deployments leveraging the power of machine learning.

The rest of the communications happens inside a protected VLAN or LAN depending on the type of deployment which makes it extremely difficult to penetrate.

Without finding the deployments, finding the secret keys, compromising the user’s Nesos account, the device of the client and the meeting credentials, it is not possible to gain access to the content of a meeting happening on Meetis.

Meetis



Client

Client

Nesos

Nesos

Meetis Client

Meetis Server

Voice Server

Media Server

Db

Meetis LAN/Cloud LAN

Meetis Cloud/Premise

Conclusion

Despite the operational size difference, our divergent philosophies when it comes to how to approach security and privacy in online communication makes us believe that we can) offer the superior product to the security and privacy minded individuals or institutions.

Instead of getting a product companies need to adapt to, we offer to adapt our product around them and their use case. We can customise it and brand it for each company, deploy it where they want it and scale up security ad infinitum depending on the type of confidentiality needed.

Our clean record, company policy and technical infrastructure keeps us safe from centralised attacks whether those are political or technical. On the other end Zoom security concerns have prompted the US senate to issue a memo telling members to avoid Zoom.

If you want to know more about our Nesos secure ecosystem head to nesos.app and get in touch with us.