NEXALTA®

Decentralized. Secure. Yours.

The self-hosted zero-knowledge private cloud that protects your organisation's most sensitive data.

We deliver the infrastructure components needed to achieve Data Sovereignty for any kind of organisations.
Our self-hosted zero-knowledge cloud solution, based on our cloud software components for data sharing, messaging and backup, and on our disruptive cloud appliance, allows to share highly sensitive data within your organisation, without relying on the public cloud and without ever exposing the raw data to cybersecurity threats.

We are combining Smart SD-WAN with safe End-2-End-Encryption and with local Edge Computing in order to deliver a credible answer to the rising costs and risks of the public cloud.

Our private cloud solution is addressing the huge gaps in digital resilience affecting SMEs and distributed organisations.
We deliver an on-premise cloud solution that can scale up from stand-alone to a Web3.0 decentralized data space infrastructure.
With military-grade security, local encryption processing, upgradable to Post-Quantum Encryption.
But as effortless and easy to use as a “good old” fax machine.

- At the Edge and decentralized, we do not rely on any public cloud, thus avoiding rising recurring costs, connectivity outages, vendor lock-in, zero-day cyber exploits.
- Trustless, data confidentiality and integrity are not just on paper, but guaranteed by mathematics.
- Both hardware and software have been in-house developed.
- Our full suite of cloud services includes data sharing, instant messaging, immutable backup for disaster recovery, local AI LLM.

THE PROBLEM

The CLOUD Act, a US law passed in 2018, allows US authorities to access data stored by American technology companies – even if the data is physically located outside the US, for example in European data centres.

Over the past two decades, we have witnessed **the rise of the public cloud**, i.e. the increasing prevalence and acceptance of public cloud services, as they support individuals and businesses through improved scalability, apparent cost savings, and permits the users to basically ignore the underlying IT. Access your data from everywhere, and no need for procurement and maintenance of a noisy and energy-consuming PC server, these were the promises.

In 2025, however, organisations are becoming aware both of the actual increasing costs and of the *risks* of the public cloud, that include geopolitical issues, data breaches, misconfigurations, data loss, account hijacking, denial of service attacks, compliance issues, and vendor lock-in. Other threats involve insecure APIs, insider threats, ransomware.

All these risks are only exacerbated by the rise of AI and LLM, where big corporations, often supported by governments, want to finally gain full access to your data, and train for free their LLM, in an effort to monetize your data in the long term. It's the so-called “surveillance capitalism”.

THE SOLUTION

The global cloud market is a massive and rapidly growing sector, projected to surpass USD 1 trillion in 2025 and reach over USD 2 trillion by the end of the decade.

The only solution to all these problems is prioritizing data sovereignty, by bringing your data back under your control. Since data privacy and integrity are no more just a compliance issue – they are now a core priority for businesses.

An **effortless "private cloud"** is needed. The increasing availability of quick and reliable FTTH connectivity makes it finally possible.

However, in order to become widely available and to gain general adoption, it has to provide convincing answers to several challenges, too:

- delivering the utmost "zero-knowledge" security with native end-2-end encryption
- standardizing the service suite, in order to be able to easily source support services
- being energy efficient and possibly noise-less, in order to make SOHO deployments possible
- supporting local AI
- giving the user the choice of being operated either in fully stand-alone private mode or in „Web3.0" federated mode, enabling point-to-point data sharing with other entities.

Our solution meets all these requirements.

MEET THE TRUSTLESS CLOUD MACHINE

Converging connectivity, edge computing and encryption in a single device is game-changing

Public cloud services have been increasingly adopted, making us totally reliant from external actors, that aim to store our complete private and business data.

Giving up the complexity of internal IT has been the natural choice, for many small businesses, but in 2025 risks are slowly becoming apparent.

Exposing raw data to cybersecurity threats is a huge business risk, that no one can afford any more.

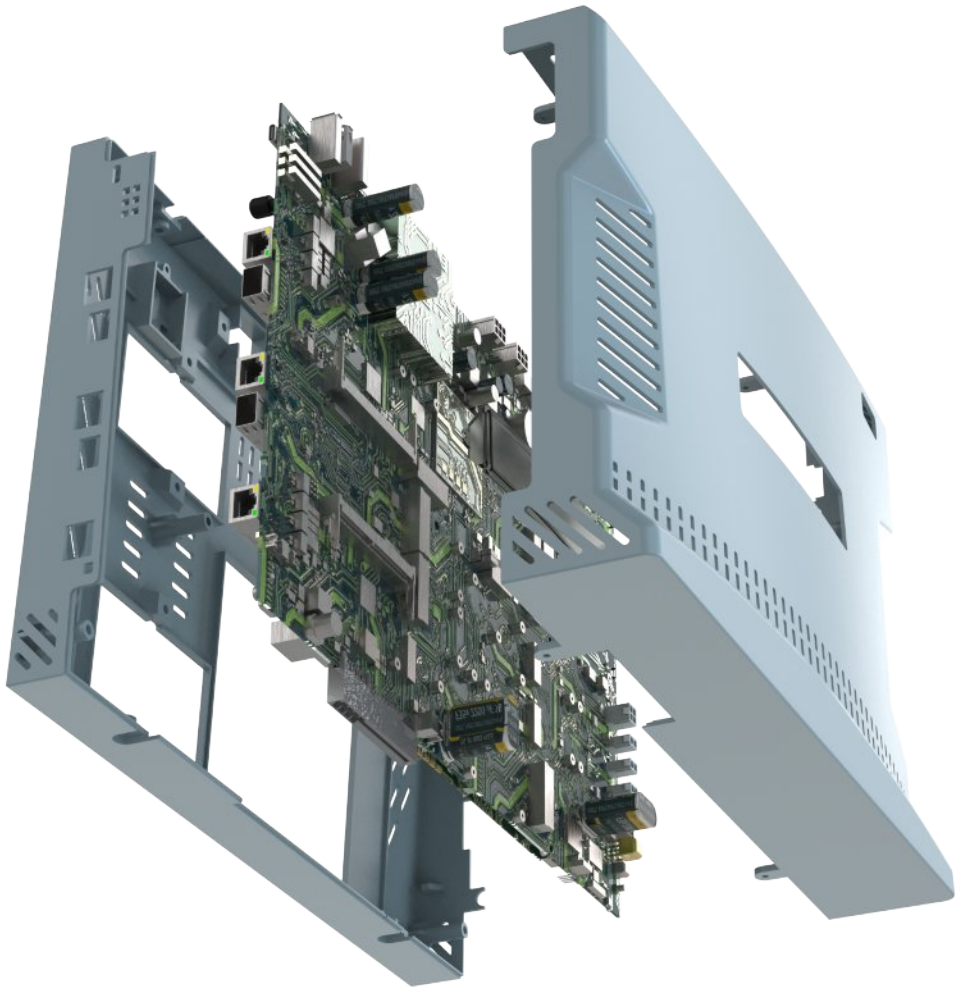
“Back to self-hosting” is gaining momentum, but small businesses and SOHO users often lack the required IT staff. We recognized the need to develop a purpose-built appliance in order to achieve user-friendly sovereign cloud computing.

Meet **Nexalta Guardian**, our trustless secure communications appliance. In terms of performance, convenience, cybersecurity we are delivering what would otherwise need a whole set of different devices connected by a lot of cables, that could not be deployed on-the-fly. Our all-in-a-box solution enables automated error-free deployment, without the need of a local IT staff.

The full suite of cloud services includes data sharing, instant messaging, immutable backup for disaster recovery, local AI LLM. Supporting Clients with Windows, MacOS, Linux, iOS, Android.

LINK
https://youtu.be/P6DT9xrRFUc?si=F8s6wC_HGPsf8nQ1

Picture: NEXALTA Guardian appliance



USE CASES

SMALL MEDIUM ENTERPRISES

Our core mission is to make small and medium-size businesses safer, with our cloud and messaging platform that is natively secured by end-to-end Encryption (E2EE), in order to deliver your RESILIENT PRIVATE CLOUD.

We support companies that are ready to reduce their excessive dependence on the public cloud in order to gain data sovereignty.

NEXALTA Guardian is the gatekeeper to your secure "private cloud", that gives you back full control over your data.
It offers secure data sharing, collaboration, instant messaging, backup and can even train a local AI with your local data (if you add an AI Edge accelerator in a free slot).

MOBILITY AND MASS TRANSIT

We have partnered with world-class OEM partners with the purpose of enhancing internet connectivity for the public transportation industries and of getting ready for autonomous driving vehicles.

Through this use case we are bootstrapping our venture, as well achieving the needed MOQ to start mass production of our hardware.

HEALTHCARE DATA SECURITY

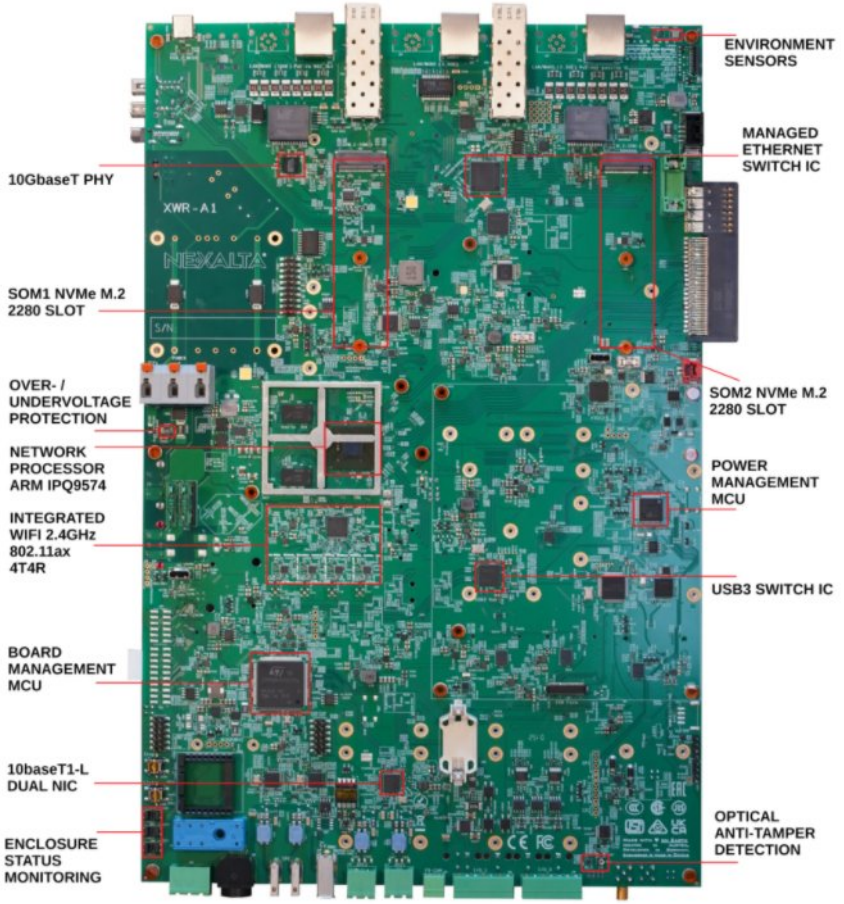
It is estimated that 7% of the world population is suffering from very complex diseases. There are only very few researchers in each country, so cross-border connections are crucial for both patients and researchers. Our decentralized sealed cloud, interconnecting regions with different regulatory frameworks, as GDPR and HIPAA, links together all healthcare stakeholders.

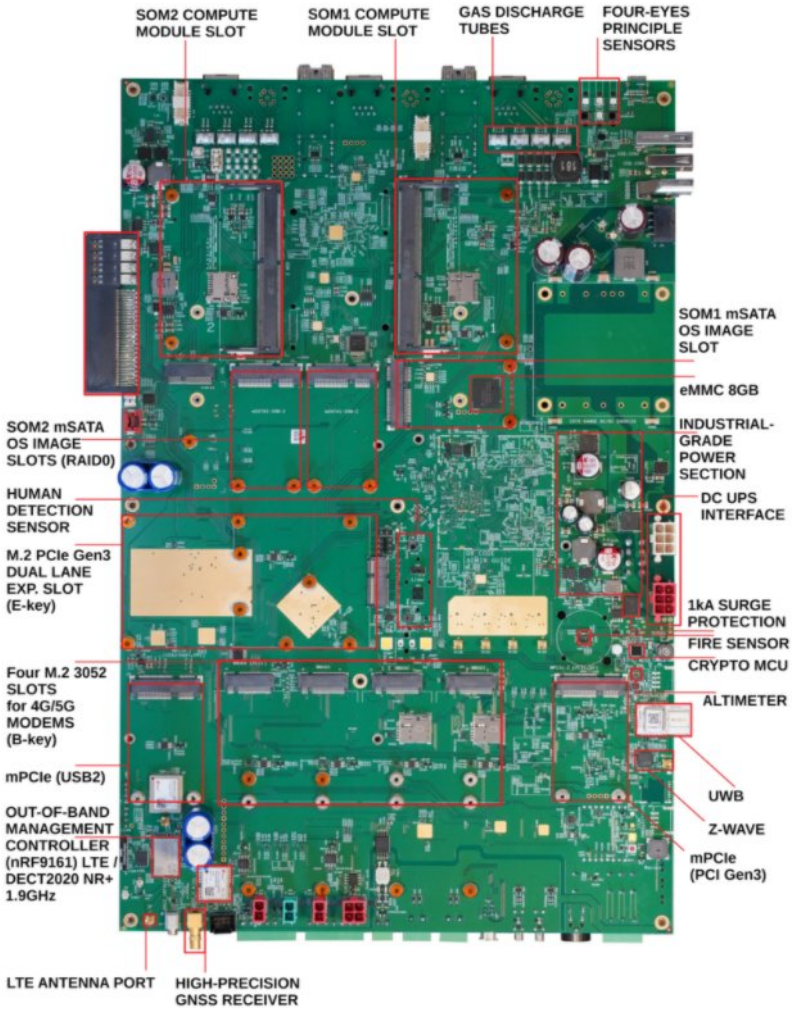
THE HARDWARE MAKING DECENTRALIZED PRIVATE CLOUDS AS RELIABLE AS DATACENTERS

As Alan Kay said ... "People who are really serious about software should make their own hardware"

A resilient private cloud is not science-fiction, but can be achieved with the right software as well the right set of computing and networking components.

To achieve datacenter-grade availability, we needed to think out of the box, and to develop our own cloud appliance, choosing carefully each of its 4700 components, including the cryptographic silicon.





OUR SOFTWARE: CRYPTOGRAPHIC LAYER MAKING BUSINESS COMMUNICATIONS SAFE AND USER-FRIENDLY

Meet ***EncryptedMessaging***, our open-source software library that makes the safest cloud and messaging possible.

NEXALTA's EncryptedMessaging is a project born with a clear mission: to provide a secure, flexible, and adaptable communication platform that breaks free from the constraints of conventional messaging systems.

Unlike for example the Signal app — which has established itself as a solution for private, internet-based conversations — EncryptedMessaging was not designed as a messaging app, but rather as a universal cryptographic layer.

Signal relies on a central server for user registration, message routing, and key management—each account tied to a phone number, creating a centralized point of vulnerability. Though encrypted, Signal's infrastructure stores metadata and user associations, making it susceptible to data breaches, outages, or government access requests.

EncryptedMessaging eliminates this risk by adopting a completely serverless model. It quickly went viral and was downloaded 33,000 times.

There are no backend servers, no databases, and no enforced user identifiers. Each participant in the network owns a cryptographic identity based on public/private keys, and every transmitted packet is digitally signed by the sender. This guarantees the integrity and origin of data without relying on third parties.

Our system is trustless by design: messages are simply propagated through routers or proxies that act as stateless repeaters, unable to decrypt, analyze, or retain any sensitive information.

NATO Compliance
☑ **STANAG alignment** (4774/4778, 4609) ☑ **Interoperability** (TCP/IP, GSM, serial RS232/485)
☑ **Secure key storage** (SecureStorage library) ☑ **Open-source** for auditability (procurement-friendly)
"Designed for the cybersecurity triple pillar: Integrity, Authenticity, Confidentiality."

EncryptedMessaging is not only practical—it's technically robust. Built with cryptographic algorithms such as AES-256 and SHA-256, and compatible with NATO standards like STANAG 4774/4778, the library delivers military-grade security. Every message is signed and independently verifiable, offering a level of accountability and resilience not present in Signal's architecture. Its decentralized, trustless structure ensures that sensitive communication is not just secure in transit, but shielded from systemic vulnerabilities.

LINKS:
https://www.nuget.org/packages/EncryptedMessaging/
https://github.com/Andrea-Bruno/EncryptedMessaging/

Furthermore, we are delivering tailor-made cloud and connectivity solutions to two specific industries:
Mobility and Healthcare.

NEXALTA®

for MOBILITY

Nexalta for Mobility redefines secure industrial-grade connectivity standards. Through OEM partnership we address for example rail/bus/truck fleet operators, first responders and critical infrastructures.

NEXALTA®

for HEALTHCARE

Our long-term mission is to deliver a HealthTech communication platform that protects personally identifiable clinical data and makes privacy-protected AI and cross-border collaboration finally possible in healthcare and medical research, linking world regions with different compliance frameworks.

THE MINDS BEHIND

ANNA NAUMENKO

Co-CEO

FRANCESCO BONAFE

Co-CEO
Chief Strategy Officer

OLEG NAGAITSEV

Chief Operations Officer

ANDREA BRUNO

CTO

We have been working in our spare time from 2022 to the beginning of 2025 to start building our platform. We've developed open-source software libraries to manage encrypted information exchange, including the EncryptedMessaging library, which quickly went viral and was downloaded 33,000 times.

We also started early to develop our own hardware, a rugged PCB optimized for decentralized data exchange infrastructures, using up to 3 ARM-based microprocessors and 4 microcontrollers. Our hardware appliance has been first shown to the world on April 2025, when our project officially launched at GITEX 2025 in Singapore.

The founding team comes from Italy and Ukraine, and consists of Anna (co-CEO), Francesco (founder and co-CEO), Oleg (COO) and Andrea (CTO), supported by further co-founders who are ready to join the team gradually as we scale up.

OUR EXPERTS

More information about our complete team is available online:

JUSTIN TORIBIO

Head of AI and ML

ELY SILABAN

Chief Compliance Officer

LUCA FELICE

Chief Marketing Officer

...and more


NEXALTA
GUARDIAN

OUR SILENT AND EFFICIENT CLOUD HARDWARE

Nexalta Guardian is a disruptive noise-free cloud appliance built for 365/7/24 operations. The appliance can be either operated desktop, or wall mounted.

NEXALTA „GUARDIAN“ GATEWAY BUNDLES UP TO 8 WAN LINKS, INCLUDING FTTH, 5G, SATCOM

We made it: an energy-efficient, noise-free, always-on cloud SD-WAN-powered appliance with maximum availability and reliability.

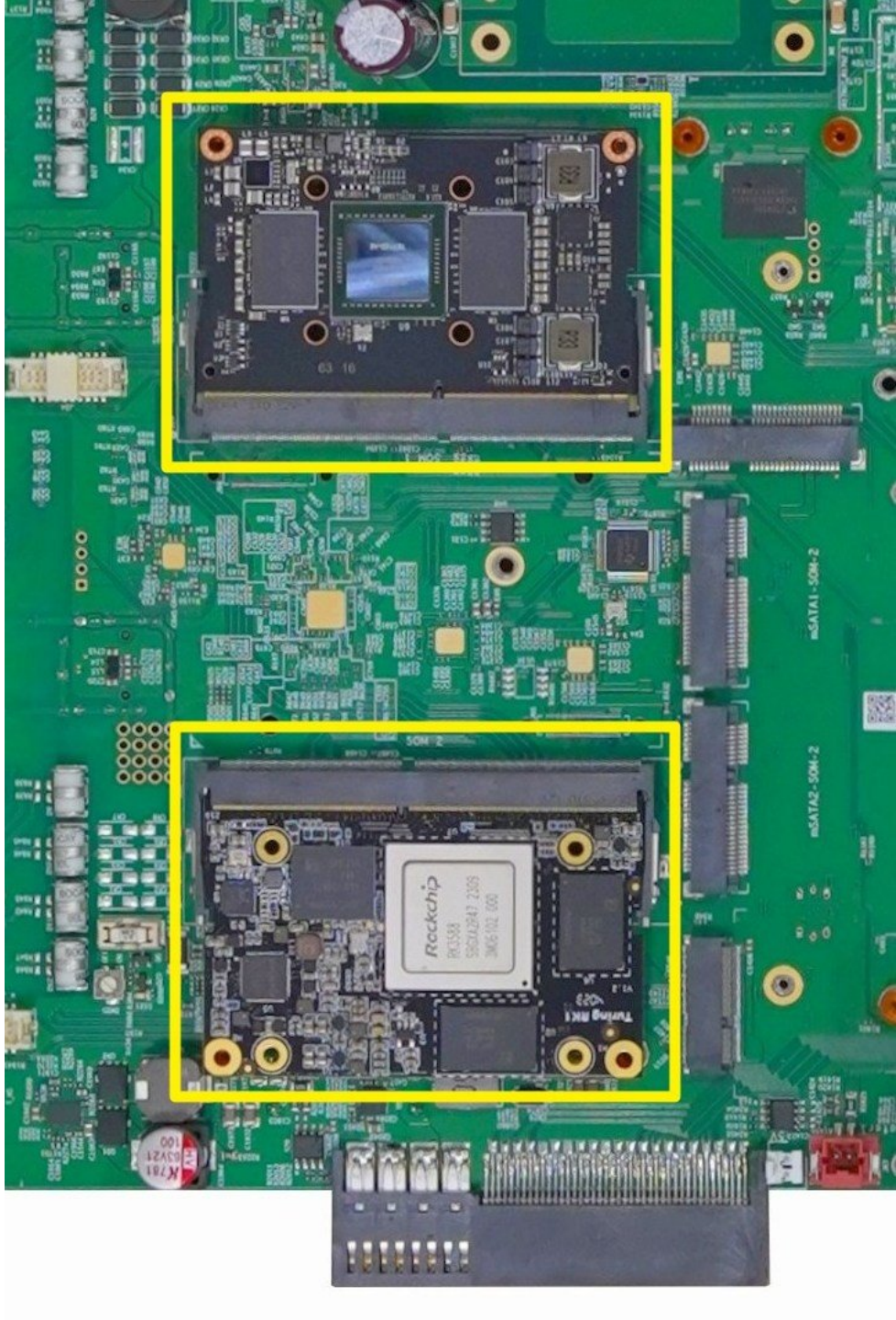
- **SD-WAN gateway and firewall are built-in**
- **Rich connectivity. Dynamic WAN bundling of the FTTH/5G uplinks increases reliability, reduces latency, and permits to continue operations even when a WAN outage occurs**
- **Built-in 5G with (e)SIM, up to 4/7 modems and up to 52 SIM/eSIM profiles (for railway applications)**
- **10GE SFP+ LAN, dual 2.5GE LAN/WAN and WiFi7 triple-band for connecting PCs, notebooks, phones, as well as IoT transceivers for Z-Wave 900MHz, DECT2020 1900 MHz, UWB for wearables and sensors, GPIO inputs/outputs, Modbus/RS485 for integration of legacy devices**
- **GPS/GNSS receiver for geo-fencing**
- **Powered by 24/48V DC. Integrated management of an optional DC/DC UPS. Our PCB in its Heavy-Duty + Railway version has rugged M12 connectors instead of the RJ45 connectors of the Standard Duty version**

DUAL COMPUTE MODULES, INFINITE POSSIBILITIES

Dual Computing modules with ARM architectures enable sovereign computing on the go, with such a high efficiency that a 24V battery can supply the needed power

By supporting one or two computing modules, we adapt to changing needs and can deploy:

- Single module mode (e.g. ARM server with 8/16/32 GB RAM)
- Dual modules, same type, in order to deliver high-availability, using DRDB software for HA cluster
- Dual modules, different types (as in right picture: one ARM-powered 32GB RAM cloud server and one NVIDIA AI accelerator)



CLOUD SOLUTIONS' COMPETITIVE MARKET ANALISYS

When comparing to existing SECURE CLOUD solutions for businesses, we immediately notice that they always involve some compromises.

NEXALTA's CLOUD SOLUTION MERGES THE BEST TECHNOLOGIES IN A UNIQUE PROPOSITION

Let's take popular self-hosted cloud solutions: **NextCloud** and its forks are widely-adopted solutions that enable on-premises cloud.

Unfortunately, their End-2-End Encryption is always optional, not permitting to easily understand if and when it's really active. Furthermore, it's not working reliably, severe bugs are present, therefore it's not a viable solution.

Let's take popular end-2-end encrypted cloud solutions: **MEGA.io** is the best known solution that enables end-2-end encryption.
Unfortunately, it's not possible to self-host it and install it on your own hardware.

- **NEXALTA's cloud is always end-2-end encrypted**
- **NEXALTA's cloud software can be installed on your Guardian appliance, on your own generic hardware, as well on the public cloud**


INVESTING
IN NEXALTA

OUR BUSINESS MODEL.

SMALL BUSINESSES

Provisioning and delivery of our private cloud service, running on our rugged appliance («Nexalta Guardian») combining True SD-WAN with E2E Encryption and Omni-Channel LAN. Safely connecting all clients and devices in any organisation.

INDUSTRIAL CONNECTIVITY

Smart factories make extensive use of IoT sensors and robots, which must be connected in a secure workflow with software applications, ICS systems, human operators and AI agents. Ensuring the security of these connections and protection from malicious external agents is our goal. Pricing on demand and projects only through channel sales.

HEALTHCARE

We deliver a decentralized encrypted platform that enables cross-border sharing of both EHR and patient-generated data from wearables, respecting the GDPR and HIPAA regulation. Medical doctors, AI agents and researchers, labs, hospitals are self-hosting our appliances and paying a monthly fee.

MOBILITY & TRANSPORTATION

To enhance the “internet on board” passengers wifi experience, we are offering to railway operators a complete ecosystem of revolutionary devices able to deliver higher speeds with a lower TCO.
Our offering consists of rail SD-WAN mobile routers, rail Access Points, rail inter-carriage-bridges, back-end systems.
Delivery through OEM partners.

INVESTING IN NEXALTA

2022-2024
BUILDING

330 000 €

Q4 2025
SEED

To complete the technical development and launch the full solution, we are looking for seed stage investors willing to take a stake of up to 10%, feel free to reach out to know more.

420 000 €

Q2 2026
SEED++

To scale up and start mass production we plan to offer a further stake up to 10% for seed capital for a total of 3,5 million Euro.

3 500 000 €

NEXALTA®

CONTACT

NEXALTA NETWORKS GmbH
Plantagenweg 1, D-85354 Freising
Max-Planck-Str. 17, D-85716 Unterschleißheim

Web https://www.nexalta.com
Phone +49 151 15811441
E-Mail office@nexalta.com