



advenica

Remote Access Device

Advenica Remote Access Device

- **Portable:** Small form factor and built-in battery allow users to easily move remote access to a single endpoint or a network of endpoints.
- **Secure:** Built on Zero Trust principles, ensuring Least Privileges, Access Control, and Audit Log.
- **Versatile:** A wide variety of I/O options enabling connections to an extensive range of devices.
- **Clientless:** Plug-and-play solution requiring no software installation on the endpoint, network, or technician's computer.
- **Out-of-Band:** Built-in LTE connection ensures remote access is isolated from the network.
- **Offline:** Whether utilizing LTE, WiFi, or LAN, the internet connection is not shared with the endpoint and will remain offline during remote access.



Attended or Unattended access

Attended access

one time access opened from site

Requires a physical press on the hardware device to generate a secure authorization code (OTP). This guarantees that only on-site personnel can authorize remote connections.

Unattended access

establish the connection remotely

Unattended Access through the Cloud Service Manager, utilising default multi-factor authentication and a mobile app for user identity verification. No on-site personnel required.



Remote Access Device: Specifications

General info

Data channel

Encrypted WebRTC via MQTT

OS

Minimal, hardened Linux version

Humidity and temperature

Max. 85% non-condensing relative humidity
41 °-104 °F (5 °-40 °C)

Connectivity

LAN, WIFI, LTE (3G and 4G)

Battery

Type

Industrial RRC1120 - 1S1P (UL2054 certified)

Power

3.70V / 2,000mAh / 7.4Wh

9-watt max power consumption

≈ 2 hours battery time

I/O

USB-C

Video input, keyboard/mouse output and charging

Bluetooth 4.0

Keyboard/mouse input

Micro-USB

Keyboard/mouse output and charging

Ethernet RJ45

Network (POE) and charging

RS232

Terminal session

SPDT

Power relay

HDMI

Video input up to 1080p @60Hz

SIM tray

Nano-SIM

Dimensions

Case size

L-124mm W-87mm H-27mm

Weight

250 g

LCD Display

2" TFT



Facility Owners

Manage 3rd party access with ease

Typical challenges for facility owners and manufacturers

Is any of the below familiar?

- Equipment where remote access is not an option today due to:
 - Equipment being offline
 - Equipment requires special connectivity (USB, serial)
- Legacy equipment (Windows XP and similar) that are connected and shouldn't be
- Lack of session control
(To what, when, who and how long 3rd party can connect)
- Non-compliant workarounds invisible to IT & cyber
- Delayed 3rd party support due to complex approvals

Our solution:

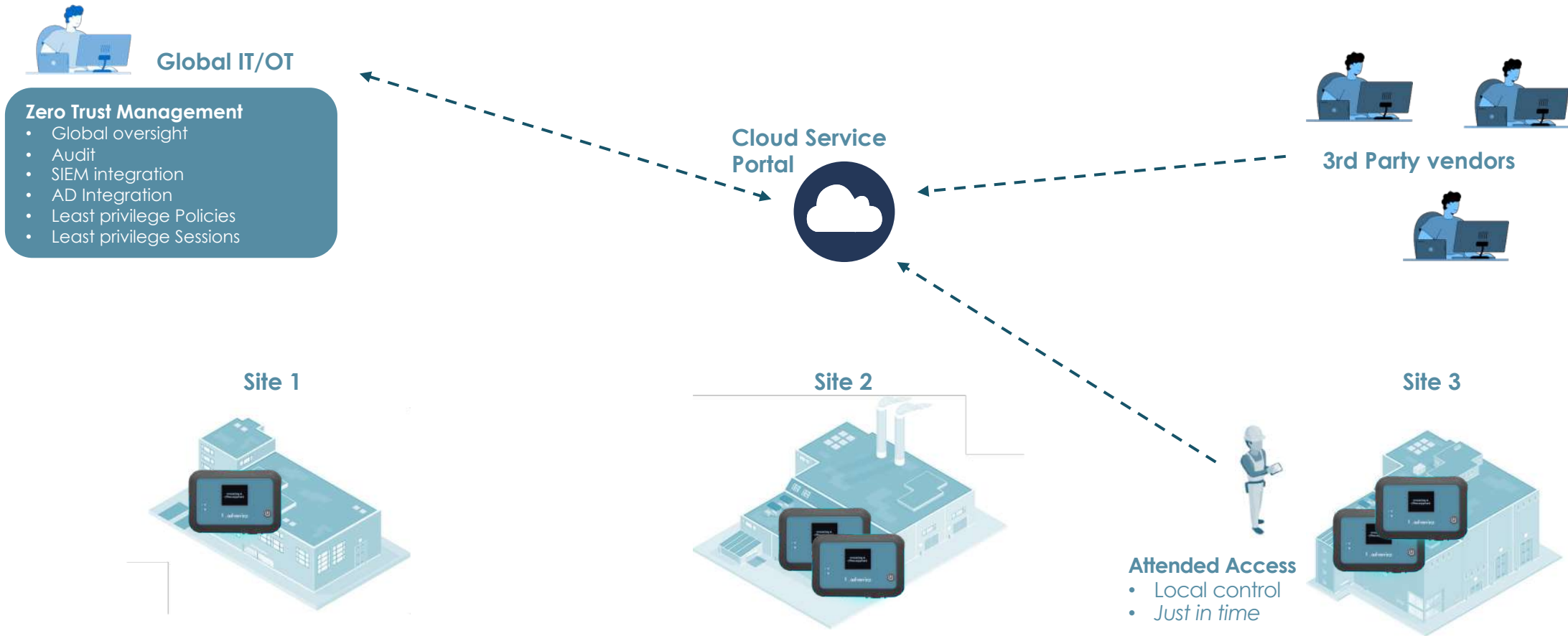
Put an **instant layer of secure control** around your site.

- Ad-Hoc Remote Access – Where it is needed when it is needed
- Support 3rd party needs whether they need tunnelling, IP/USB/Serial or even KVM access.
- Hassle free user administration
- No need to change your OT/IT infrastructure at your sites.



Ad-hoc Remote Access: Multiple sites

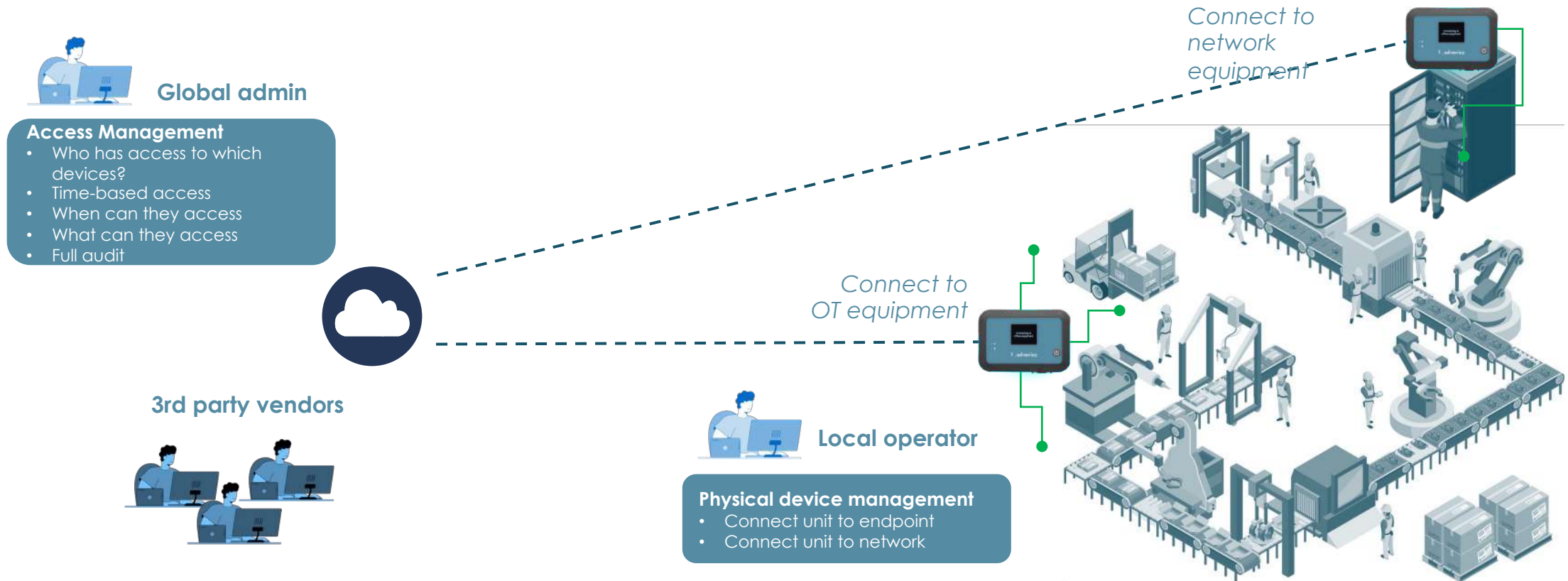
Protect your infrastructure with PAM* and Zero Trust principles instantly



*Privileged Access Management

Ad-hoc Remote Access: At a specific site

Protect your infrastructure with PAM* and Zero Trust principles instantly



*Privileged Access Management

Ad-hoc Remote Access: User handling

Global admin



3rd party vendors



Local operator



No need to maintain 3rd party users, you invite users during a timebased period.

The user interface makes it easy and simple to manage.

Who - Select who should assist you
If they are not a user, an invite is sent

What - Select what they should access
Access Device, connectivity service

When - Timebase the period
When should the access slot be available and for how long

Instant Access

With the OTP (One Time Password) feature an instant session can be established between a 3rd party user and a Remote Access Device

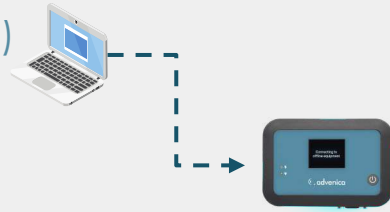
All events and session data are logged in the audit log



Connectivity overview

Clientless access (in-browser)

- KVM Access (Keyboard Video Mouse)
- Terminal Access (USB/Serial)
- SSH Access
- File transfer



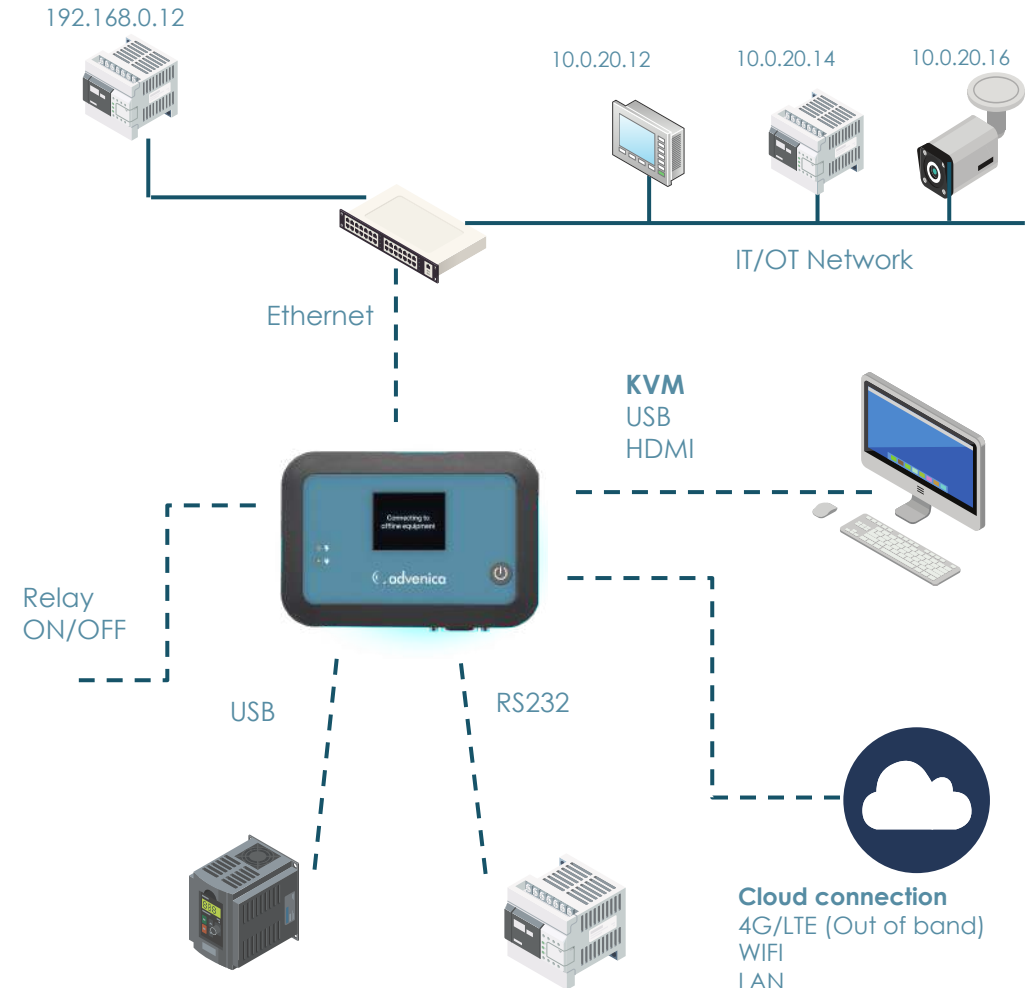
Clientless tunnelling

- IP tunnel between 2 HW devices
- USB tunnel between 2 HW devices
- Serial tunnel between 2 HW devices



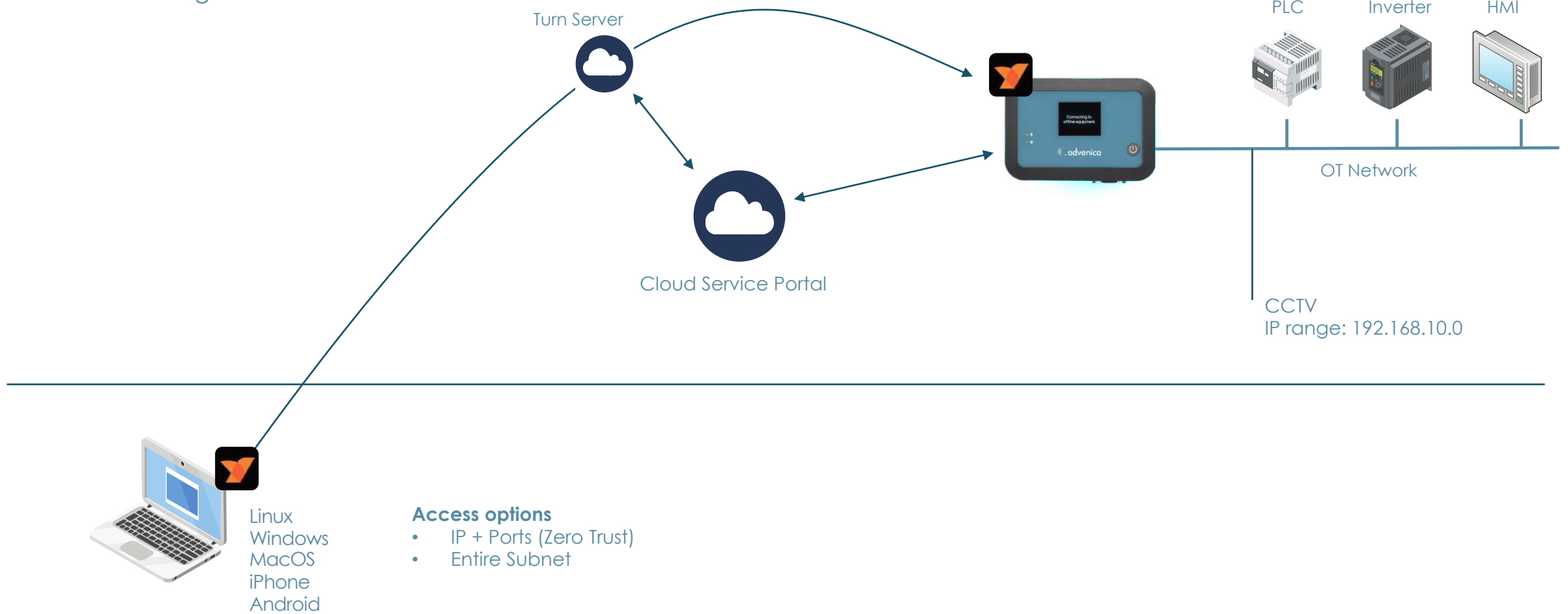
Direct Tunnelling

- Tunnelling with client
- Connect to one or multiple endpoints
- Subnet access



Direct Tunnelling with 1 HW device

Direct Tunnelling



OEM / machine builders

Convenient and secure remote
access to site

Key features for OEM / machine builders

- Several **connection types** supported to fit your equipment's interface
- Only connected when needed – **minimised cyber attack surface**
- **Out-of-band 4G/LTE** connectivity - No need to use the sites Internet connection
- Have **eyes on the site** during remote support – simply connect a USB camera or smartphone to the device



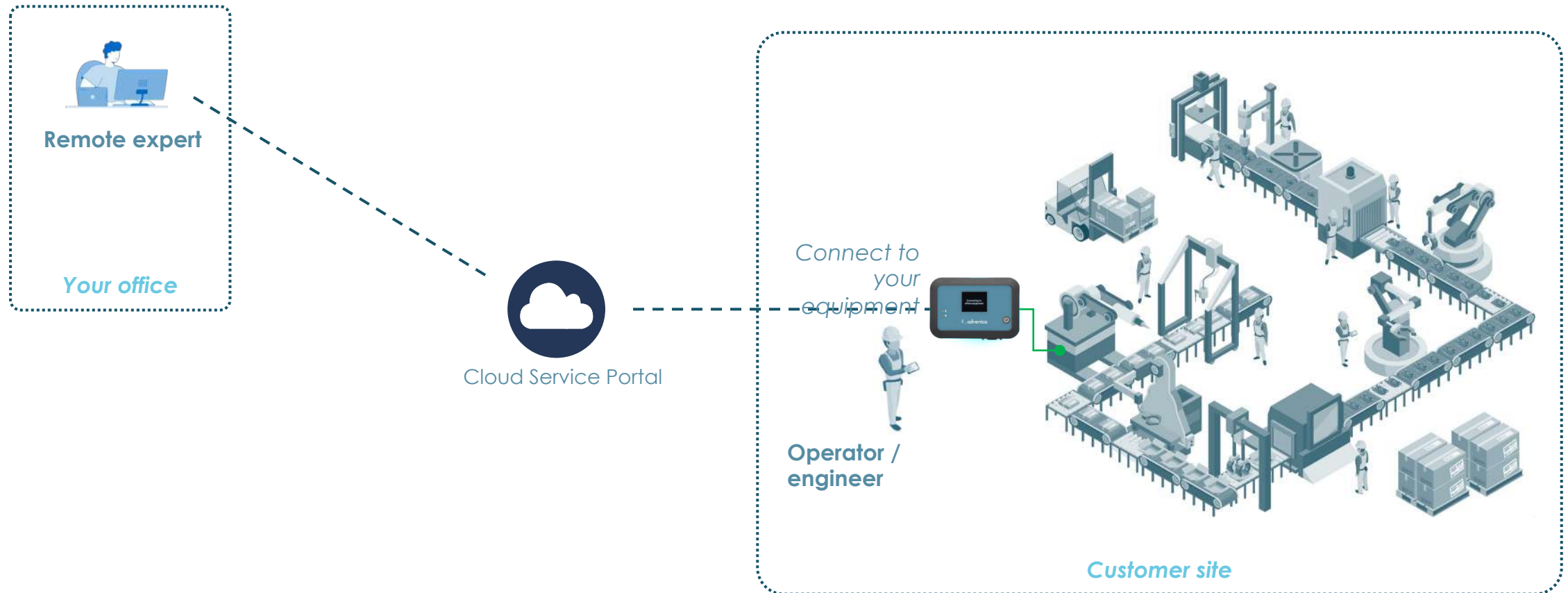
Key benefits for OEM / machine builders

- Access the equipment securely **even if** the manufacturing **site is taken offline** – fx during a cyberattack
- **Support on-site staff** by providing an instant lifeline to specialists back home
- **Update equipment remotely/offline** – no network connection needed at site and no present service technician needed
 - Use the built-in storage for firmware installs
 - Simple file transfer of logs and similar



Convenient and secure access to your equipment on site

Efficient remote support for both your customer's operators and your service engineers



Different ways to utilise the Remote Access Device

1. Sell it as a part of your machine equipment for increased customer satisfaction and control - *attended access* (one time password generation) for site owner
2. Use it to increase your own service organisation's efficiency and support your colleagues better

Or

Use as part of Advenica's **Secure Machine Connection** solution for even higher security with a hardware enforced impenetrable one-way data connection with continuous data flow for your digital services and production analysis work.

