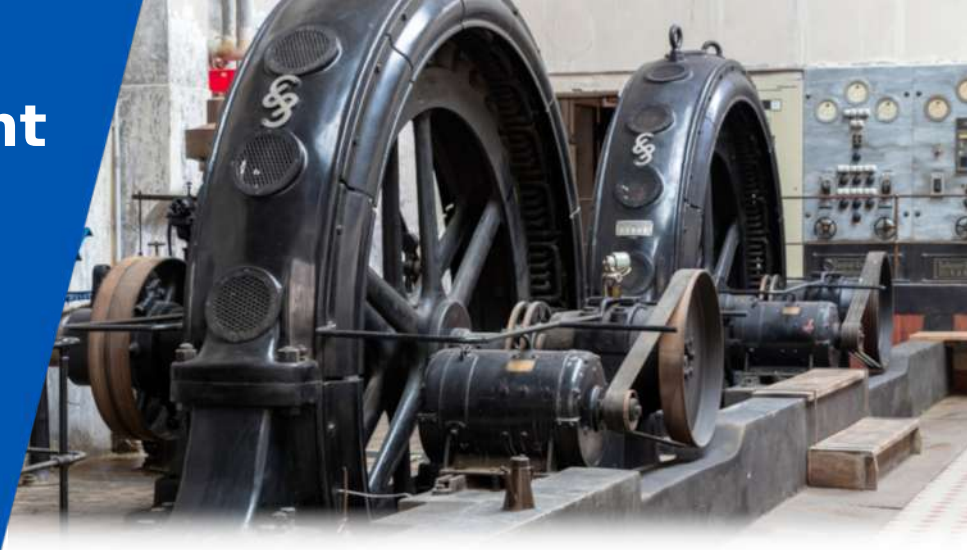
Legacy equipment maintenance



Fijoport enables our customers to remotely access key equipment in order to monitor and manage it on a 24/7 basis.

Authenticated users may establish instant VPN access, via the Portal Server, eliminating exposure to cyber threats.

BENEFITS

- **Secure bi-directional encrypted connectivity between user and remote site.**
- **Maintenance and management of devices on a 24/7 basis without user intervention at remote site.**
- **Any access is limited to authorised personnel only and all remote sessions are logged and auditable.**
- **No software installations required on remote devices being accessed.**

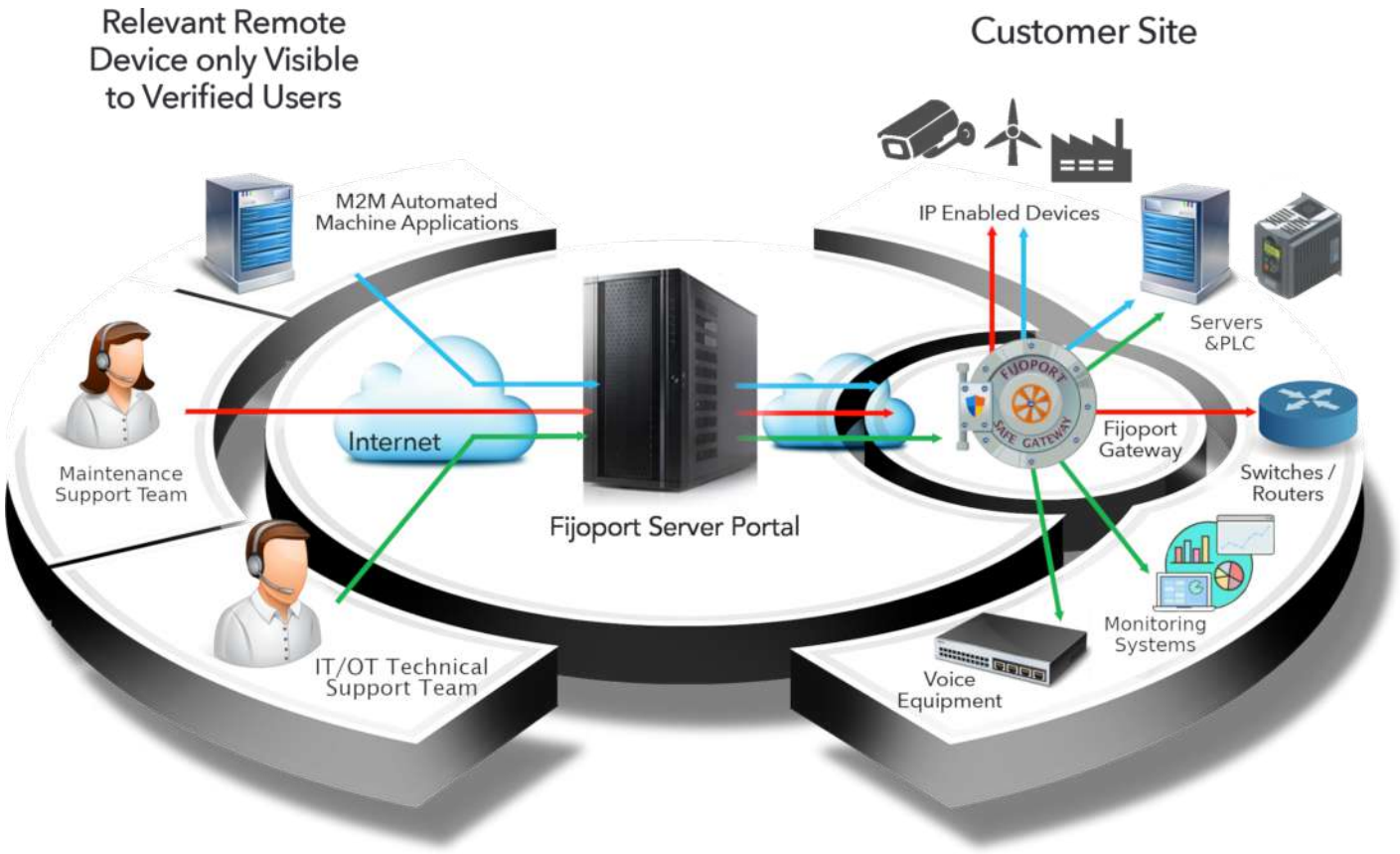
USE CASE
Direct & indirect Maintenance

Legacy equipment usually works with software that is no longer supported with security updates (for example, Windows 2000, Windows XP and Windows 7). For that reason, this equipment could be vulnerable to hackers. Companies that wish to avoid that risk, may deploy Fijoport as a layer of protection in front of this legacy equipment and eliminate any risk of cyber-attack.

Fijowave

How it works:

- **Legacy equipment running insecure software is especially vulnerable whenever they are connected to internet. When this equipment needs to be updated or connected to internet, Fijoport can act as a shield against malware and hackers.**
- **Remote maintenance activities can be carried out by either internal or external technical support teams.**
- **When needed, the authorized technicians are able to connect to the remote equipment to monitor, maintain and update. For example, Fijoport can be used to restart the systems in case of software malfunction.**
- **In case the problem cannot be resolved online and needs an onsite technician, the person in the operations centre can send one, reducing the downtime. Fijoport also allows an on-site and remote technicians to work together on the same equipment at the same time.**



sales@fijowave.com
www.fijowave.com

Fijowave