macchina.io

How to Evaluate Products for Secure IoT Remote Access?

Save time and money by evaluating secure remote access products for IoT devices effectively.

A 4 STEP WORKBOOK

A 4 step workbook for the successful selection of a remote access solution for IoT devices

STEP 1 INTERNAL COMPANY ANALYSIS

STEP 2 REMOTE ACCESS TECHNOLOGY

STEP 3 AVAILABLE SOLUTIONS

STEP 4 BUY OR DIY

INTERNAL COMPANY ANALYSIS

Why it is important to strategically set a technology pathway?

Before choosing or implementing a remote access solution, you should have a clear idea of why you need a remote access solution, and what you want to achieve.

You need to define your goals, needs, options and steps for choosing a remote access solution to ensure that you end up with a solution that fits your requirements perfectly and stays within your budget.

INTERNAL COMPANY ANALYSIS

By answering following questions, you will be able to clarify your business goal with remote access and choose the best solution for your situation

CRITICAL QUESTIONS - PART 1

Who should be able to remotely access devices?

- End users of the device
- Sales and service partners supporting customers in setting up and maintaining devices
- Internal staff

What do you want to access remotely?

- Access the to the device's web user interface or REST APIs
- Access to the devices screen and graphical user interface via screen-sharing (VNC or RDP)
- Access to the device's command-line shell via SSH for troubleshooting
- Access to the device via industrial protocols (e.g., Modbus TCP, OPC UA) or custom protocols (e.g., engineering tool to PLC)

Is fine-grained access control required?

- Should every user be able to access all devices?
- Does access to devices need to be controlled in detail (e.g., specifically for each user which devices or ports can be accessed)?

How many devices will have to be connected?

- 10s to 100s
- A few 1000s
- 100.000s or millions

INTERNAL COMPANY ANALYSIS

CRITICAL QUESTIONS - PART 2

Where should the solution be hosted?

- Is a cloud-based SaaS solution preferred?
- Is an on-premises/self-hosted solution preferred?

Does the remote access solution need to be integrated with existing applications or infrastructure, e.g., directory services (LDAP) or single sign-on (SSO) services?

Do I want an off-the-shelf solution or build everything myself?

Do my employees have the necessary skills to run/operate the solution?

What are the initial implementation/license/set-up costs?

What are the ongoing running costs (including license subscription fees, cloud hosting fees, operation and maintenance costs)?

What is the expected time-to-deployment? How much time do I have available for implementation?

Where is the data stored?

What are the legal requirements (EU GDPR, EU Cyber Resilience Act)?

What are the availability requirements?

Which cloud or hosting provider should be selected?

Is the use of open-source software possible?

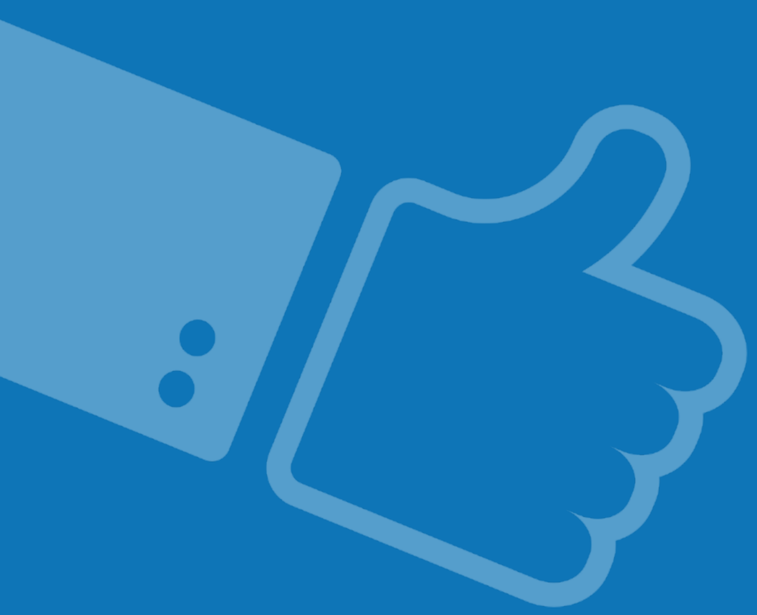
REMOTE ACCESS TECHNOLOGIES

Selecting the remote access technology

Your internal company analysis, carried out in step one, will guide you to the technology that best meets your requirements.

There are several types of remote access technologies available to companies, each with its own advantages and disadvantages.

The following is a comparison table of the most common remote access technologies, such as Secure Tunneling (macchina.io REMOTE), Port Forwarding and VPN (Virtual Private Network).



REMOTE ACCESS TECHNOLOGIES

The following is a comparison table of the most common remote access technologies: Secure Tunneling, Port Forwarding and VPN.

Secure Tunneling (macchina.io REMOTE)

When to use

Access to specific remote devices and ports (services) is required. No changes to existing network configuration at remote site are possible. Fine-grained access control for different user groups is needed. Must scale to 100.000s or millions of devices.

Port Forwarding

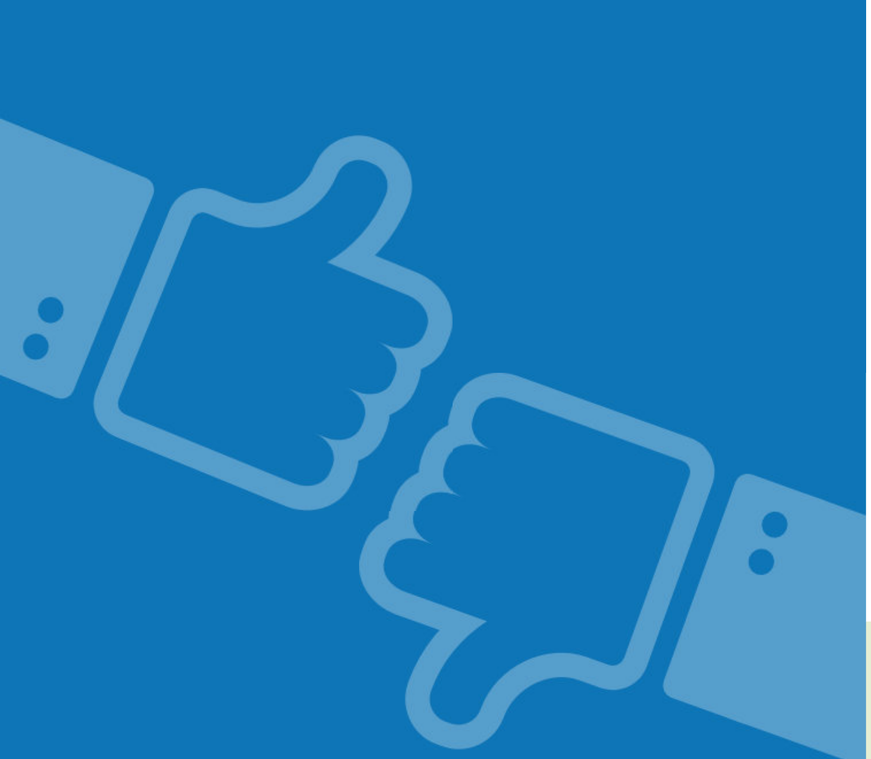
When to use

Access to a single device (or a very small number of devices) behind a router when security does not matter.

VPN (Virtual Private Network)

When to use

Access to an entire remote network is required.



REMOTE ACCESS TECHNOLOGIES

Secure Tunneling
(macchina.io REMOTE)

ADVANTAGES

- No changes to network infrastructure required.
- Secure, encrypted TLS connections.
- Supports most TCP-based protocols, including HTTP(S), SSH, VNC, RDP, Modbus/TCP, as well as custom protocols.
- Highly scalable, can support 100.000s to millions of devices.
- Integrated users and permissions management.
- Detailed role-based access control, allowing fine-grained control of the devices (and even services/ports) a specific user may access.
- Can be used to provide remote access via mobile apps.

DISADVANTAGES

- Device agent software needs to be integrated into the device itself, or another device (router) in the same network.
- Not all protocols can be supported (e.g., FTP).
- Not compatible with UDP-based protocols.

REMOTE ACCESS TECHNOLOGIES

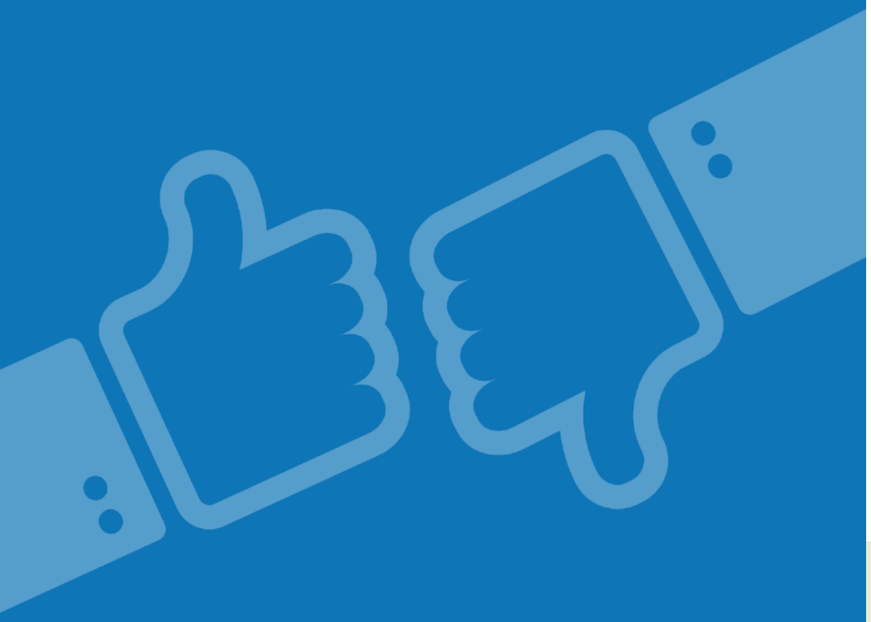
Port Forwarding

ADVANTAGES

- Supported by almost every router on the market.
- Gives access to any TCP or UDP port on a device.

DISADVANTAGES

- The device is directly exposed to the internet. Extremely high risk of attacks.
- NAT router configuration is complex, especially non IT experts.
- A dynamic DNS solution is needed if no public static IP address is available.
- Public IPv4 addresses are becoming increasingly rare and IPv6 is not yet available universally.



REMOTE ACCESS TECHNOLOGIES

VPN (Virtual Private Network)

ADVANTAGES

- Secure and encrypted connection to remote networks.
- Proven and standardized technology.

DISADVANTAGES

- VPNs may be blocked or restricted.
- VPN infrastructure is difficult to setup and maintain, especially with many devices.
- A VPN client must be installed and configured by all users requiring access to devices. Not suitable for end user remote access.
- It's hard or even impossible to limit access to specific devices for specific users. A VPN always gives access to an entire network or subnetwork.

AVAILABLE SOLUTIONS

How do you choose the best solution for your needs and preferences?

To help you with this decision, we have prepared a table that gives you a list of criteria to compare the different solutions against each other.

The table covers various aspects of remote access, such as licensing and delivery, technology, features, security, infrastructure, documentation, branding, and integration.

The table also includes one of the leading solutions in the market, macchina.io REMOTE, as an example.

DOWNLOAD SOLUTION EVALUATION CHECKLIST (Excel)

AVAILABLE SOLUTIONS

To help you with this decision, we have prepared a table that gives you a list of criteria to compare the different solutions against each other.

SOLUTIONS CHECK - PART 1

Solution	macchina.io REMOTE	
Licensing and Delivery	Combined proprietary (server) and open source (device agent, SDK)	
Technology	WebTunnel (secure tunnel over WebSocket/HTTPS/TLS)	
Self-hosted/on-prem	✓	
SaaS	Optional, through partners	
Software-only Solution	Independent from hardware providers	
Free plan	✓ up to 10 connections are free of charge	
Professional Support	✓	
Scalability	10s to millions of devices (load-balancing and server clustering)	

AVAILABLE SOLUTIONS

SOLUTIONS CHECK - PART 2

Security	Encrypted connections (TLS), device authentication via secrets or certificates	
Role-Based Access Control	✓	
Find-Grained Access Control to Devices	✓ (single device and port/service level per user)	
Two-Factor Authentication	✓ (TOTP)	
Required Infrastructure	Linux MySQL or PostgreSQL Docker	
Documentation and Examples	User guide, code and configuration examples, white papers, video guides	
White-Labelling/ Branding	✓	
Extensibility and Integration (customer-specific features)	REST APIs, webhooks and custom plug-ins upon request	
Time for initial setup	2 - 4 hours	

BUY OR DO-IT-YOURSELF

After completing the previous steps, you should have a clear idea of

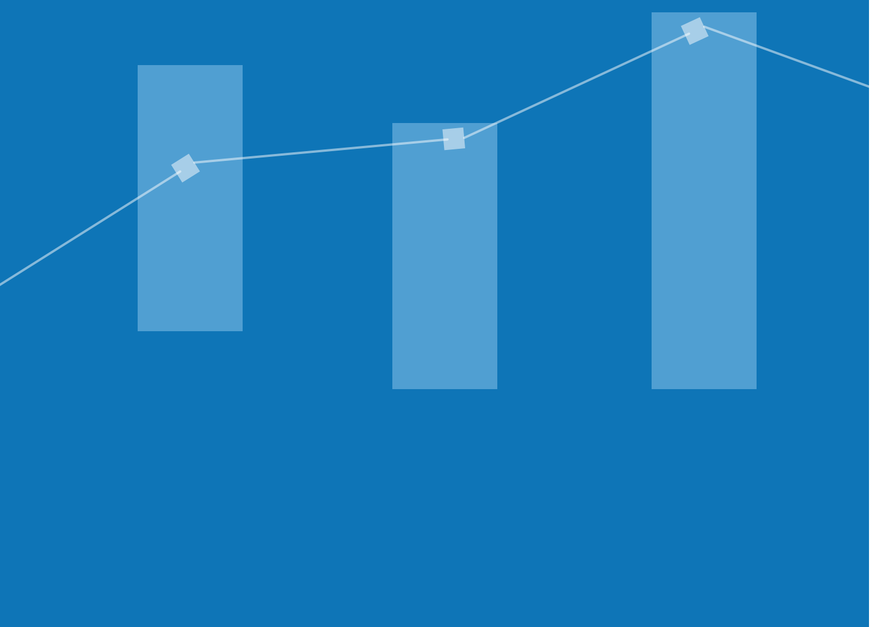
- your internal requirements and capabilities
- the appropriate remote access technology and
- the available solutions on the market.

Before you decide, whether to

- use an off-the-shelf one or
- build your own solution

let us discuss the following forms for licensing and delivery:

- Proprietary Software
- Software as a Service (SaaS)
- Open Source Software (OSS)
- Dual-licensed Open Source Software
- In-House / Do-It-Yourself



BUY OR DO-IT-YOURSELF

Proprietary Software: Proprietary, commercially licensed software products are generally predictable and reliable. You can get a full understanding of the features and costs before you buy, and you can get support and updates from the vendor. Commercially licensed software products are suitable for long-term or large-scale projects, but they may have licensing restrictions and dependencies. Vendor lock-in may be a disadvantage.

Some vendors like macchina.io offer some parts of their software under an open source license. For example, the macchina.io REMOTE server is commercially-licensed, but the device agent software is provided under an open source license.

Software as a Service (SaaS): SaaS solutions are easy to use and scalable, but they limit your flexibility, control and depending on the size of the project can get very pricey.
For example:

- You may not be able to access or customize the code.
- You may be locked in with long term contracts.
- SaaS solutions are good for short-term or experimental projects, but risky for long-term or large-scale projects.

Open Source Software (OSS): Open Source Software can save you time and money, but it depends on the interest and direction of the community maintaining the project.

For example: You may face challenges in maintaining and updating the software if the project loses popularity or forks.
Tip: Most open source projects can be found on GitHub.

BUY OR DO-IT-YOURSELF

Dual-Licensed Open-Source Software: This is a combination of open-source and commercially licensed software. Software under a dual licensing model combines reliability of commercial software with all the open-source advantages, offering full control over the software, access to the source code, the option of self-hosting, and customization.

Different variants are possible:

- Open-source licensed basic version. The open source version has limited features and limited support. The commercially licensed version comes with a full feature set (specifically features important for use in enterprise environments) and professional support. Tip: Good for quick prototyping!

- Restrictive open-source license - such as the GNU General Public License (GPL) with a commercial-license. This means derived works of such GPL-licensed software must be made available under the same license. Paying for a commercial license avoids the GPL restrictions. Tip: Good for inhouse projects!

In-House/Do-It-Yourself (DIY): Building your own solution gives you the most flexibility and control, but requires lots of resources and expertise that may not be readily available.
Generally, people tend to heavily underestimate the effort required to build software and very few software projects have been done in time and within initial cost estimations.
Unless your requirements are very special and specific for your company, and no available off-the-shelf solution fits the requirements, or can be adapted to fit the requirements, DIY is not a good strategy.
Other aspects to consider are time-to-market and ongoing software maintenance after the initial product has been built.

BUY OR DO-IT-YOURSELF

We have compared all forms of licensing and delivery based on the most important factors that affect your project budget, implementation time and risks.

	TIME	UPFRONT COSTS	RECURRING COSTS	RISKS
Proprietary Software	*	**	*	*
Software as a Service (SaaS)	*	*	**	*
Open Source Software (OSS)	**	**	*	***
Dual-Licensed Open-Source Software	*	**	*	*
In-House/Do-It-Yourself (DIY)	***	***	***	**

Agenda: * low, ** intermediate, *** high

SUMMARY

Selecting the right pathway is crucial for your project's success!

Remember, selecting the right pathway is crucial for your project's success. Evaluate your requirements, resources and the products on the market carefully to make the best decisions for your project.

These are the ways we can help you further:

🚀 Try for Free our products!

📝 Book a free online call with our experts!

➡ Read more on https://macchina.io/remote and sign-up for our free remote access demo.