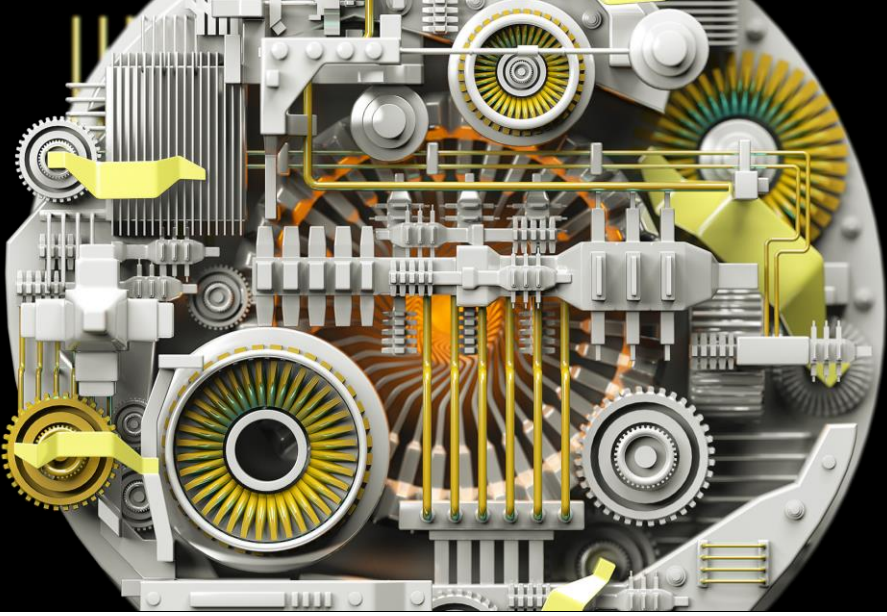



Industrial Networks Remote Access

The importance of remote access solutions for Industrial Networks




With **the increase of remote work**, it is crucial to invest in remote access solutions aligned with organizational needs to prevent the **risk of cyberattacks** and avoid huge **operational** and **financial** impacts.




Cyber attacks

Industrials companies are increasingly **more vulnerable for cyber security** related incidents as a result of **automation** and implementation of **Industry 4.0 use cases**.




Operational impact

A **cyber attack** on an industrial network can **stop the production of a company**. In this situation, the top priorities are safety and getting the system back online.




Financial impact


During unplanned downtime, every minute matters. The **more unplanned downtime**, the **higher your costs** and the greater the impact to your bottom line.



9 out of 10 OT organizations experienced **at least one system intrusion** in 2020, and **63% had 3 or more intrusions** ^[1]



A single **ransomware** causes on average **16 days** of unplanned **downtime** ^[1]




A minute of downtime in an industrial network costs on average **\$100,560** ^[2]

Sources: [1] Dispel, [2] Fortinet

How remote access misuse can lead to security challenges?

The remote access technology provides flexibility to work remotely from any location, for a successful implementation it's essential to recognize the different types of users, use cases, challenges and risks.

Types of remote access users



- Equipment support**
OT equipment/applications vendors that provide remote **maintenance**
- Remote workers**
Users that are **working remotely** from different locations
- Third-party contractors**
Outsource companies that specialize in **specific operational areas**

It is important to clearly **identify the remote access use cases** to avoid undesired **challenges** and **risks** such as:

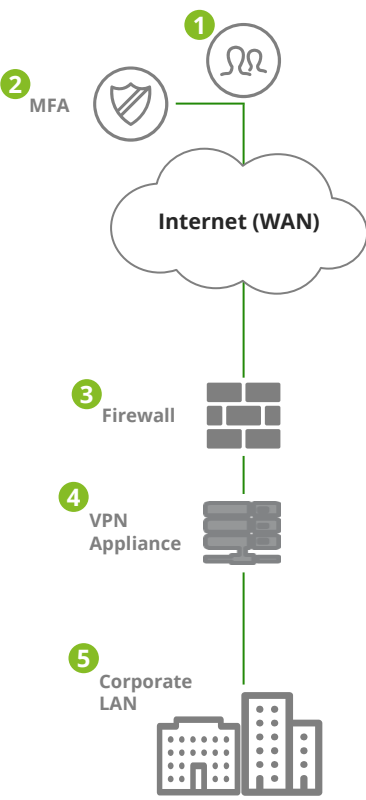
- Reduced cybersecurity knowledge**
- Reduced user visibility**
- Unsecure authentication methods**
- No regular software updates**

What are the main OT Remote Access solutions?

All companies have different operational needs, so the appropriate remote access solution for each OT network depends on the specific business requirements, network architecture and desired remote network control features.

Network-based remote access

Network-based remote access solutions enable privileged remote users to securely access the corporate LAN and OT systems, through a VPN connection.



Authentication steps

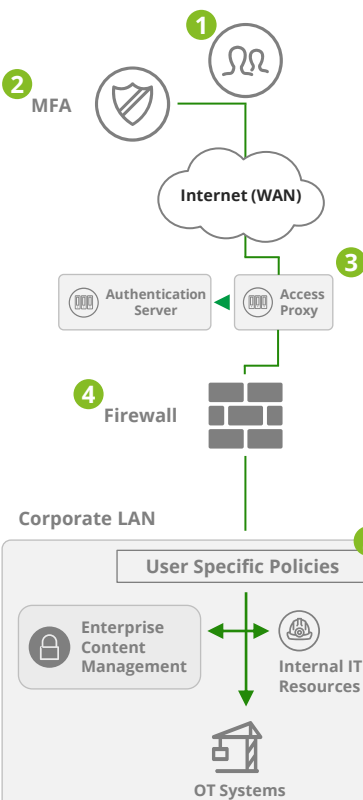
- Privileged user connects through a VPN Client app
- User identity authentication with multi-factor authentication
- Firewall filters traffic policies of privileged remote users
- Data goes through a private encrypted tunnel over the public internet
- Privileged users allowed to access the Corporate LAN

Use Cases & Implementation

- Small and medium-sized companies
- Non-complex nor critical OT networks
- Simple and affordable solution with effective security mechanisms

Application-based remote access

Application-based remote access solutions provide segmentation filtering of the remote connections, by validating the users' and providing access to only specific network sections.



Authentication steps

- Privileged user connects through an application software solution
- User identity authentication with multi-factor authentication
- Access proxy validates the user-specific access policies
- Application-level micro-segmentation prevents user's unauthorized access
- Users access only authorized systems within the corporate LAN restricted to user policies

Use Cases & Implementation

- Large enterprises and industrial companies
- Complex OT networks with a high number of users and OT systems
- Best possible security model despite being more expensive than other solutions

Regardless the remote access solution that best suits each company, there are a set of **best practices** ^[3] that should be considered when implementing the solution in order to reduce the successful attacks.

Establish user-specific authentication servers

Remote access users should have a **unique and non-transmissible account**. The authentication server should identify the user.

Implement multi-factor authentication

MFA should always be used in the connections. Also, each one should be a different kind of method.

Use dedicated hardware and software

A company owned **firewall** and **router** at the remote workstation should be provided.



Perform a risk and threat assessment

A threat and risk **assessment** enables to **understand the current situation** regarding endpoints, users and connections.


Eliminate direct connections to critical assets

Remote access that **circumvents the path through the DMZs** and **connects directly to ICS from the Internet** poses a much **greater**.

Define role-based authorization levels

Technicians should be granted access to jump hosts. Remote access users should only be **granted access only to the systems and applications**.

Sources: [3] Sans Institute



Remote access solutions for OT Networks vary in **features**, **operation** and **use cases** depending on the **size**, **characteristics** and **operational needs** of the target OT network. To successfully implement any kind of remote access **solution** within an OT network, it is always advisable to strictly follow the **standard** set of **best practices** described before, as this will reduce the likelihood of complex security **breaches** or application failure.

How can Deloitte help?

Our team combines technology and engineering expertise with business strategic skills that allow us to be a unique partner for the whole IT and OT transformation journey.

- Trust-worthy advisor for **every step of remote access solution**, with a proven methodology from assessment to design until implementation
- Unique technology and engineering offerings**, with a proven track record in network and tech transformation
- Multidisciplinary specialized teams, which combine the high technical expertise with **business and strategic consulting teams**

Contacts

Expert



Bruno Pires
gTEE - Global Telecom Engineering Excellence Manager
brunpires@deloitte.pt

Sponsor



Luís Abreu
gTEE - Global Telecom Engineering Excellence Partner
labreu@deloitte.pt

Acknowledgements
Special thanks to whom contributed to this publication in terms of researching, providing expertise, and coordinating:
David Andrade | Guilherme Castelo | Margarida Esteves | Filipe Costa