OTORIO

remOT™

Safe Remote OT Access from OTORIO

A secured by design, governance solution providing a safe, single-point-of-entry for your production environment.

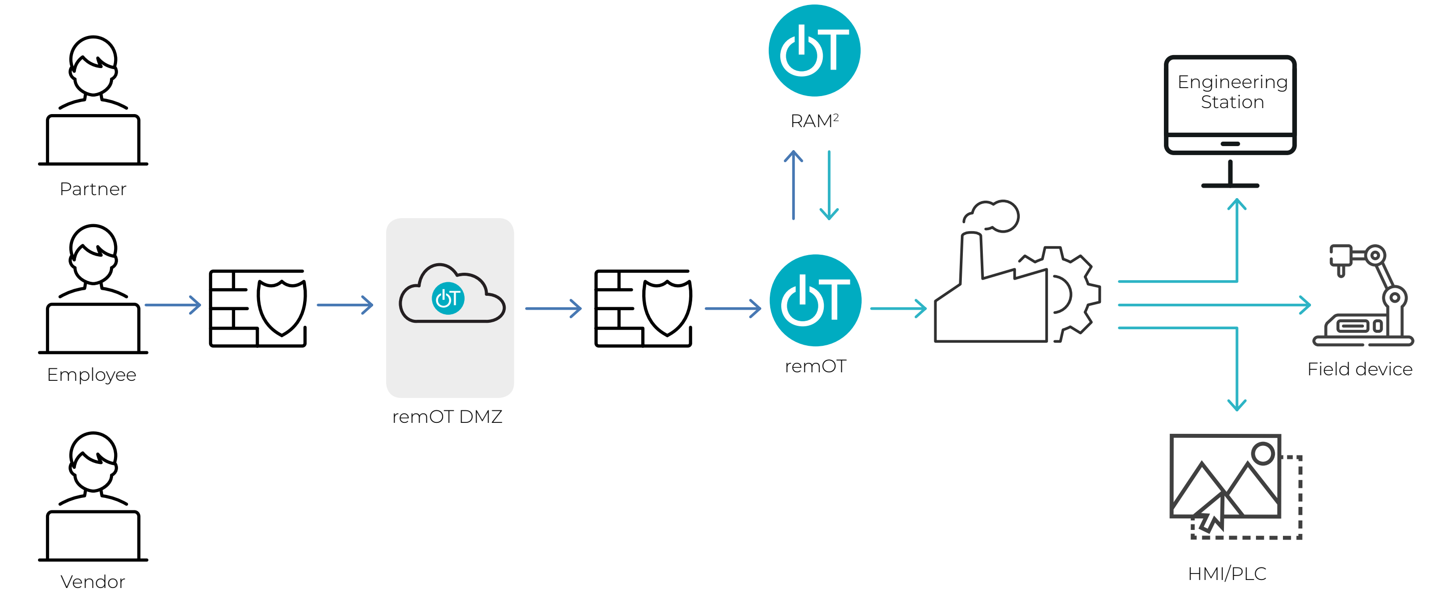
Solving Industrial Network Challenges

The need for remote access in industrial environments has solved many human resource and budget challenges and provided more business efficiency. At the same time, remote connectivity, which is often unsupervised, has brought about many business concerns and security risks.

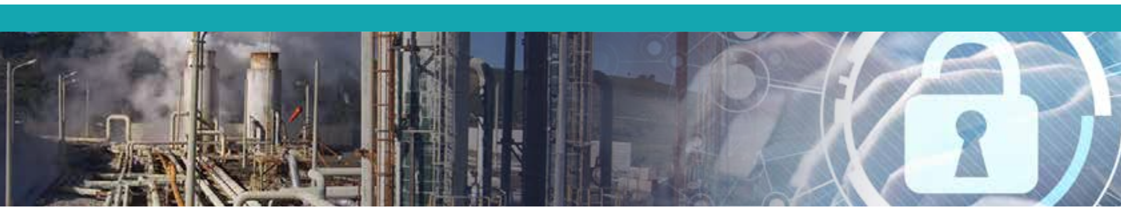
Simple to Deploy, Configure, and Maintain

OTORIO's remOT can be deployed quickly, requiring no changes in firewall rules or end-point configuration. Administrators can easily manage users' and groups' access permissions and introduce secure remote connectivity to an entire plant or multiple sites within hours. remOT's low latency design even allows connectivity to remote sites that have low-quality connectivity.

Designed by OTORIO's leading nation-state cyber defense team, reMOT provides enhanced governance in a resilient and safe solution making for a secure and transparent single-point-of-entry to the OT environment.



remOT Workflow



Remote access challenges and our solutions

Increasing Attack Surface

remOT provides monitoring and control of this expanded attack surface to keep your organization safe from vulnerabilities that can be exploited by hackers.

Traffic Monitoring Challenges

remOT provides secure and transparent single-point-of-entry to the OT environment. This makes it easier to manage risks and focus your security teams' attention on protecting your network from one location.

Direct Access to Production Floor Assets

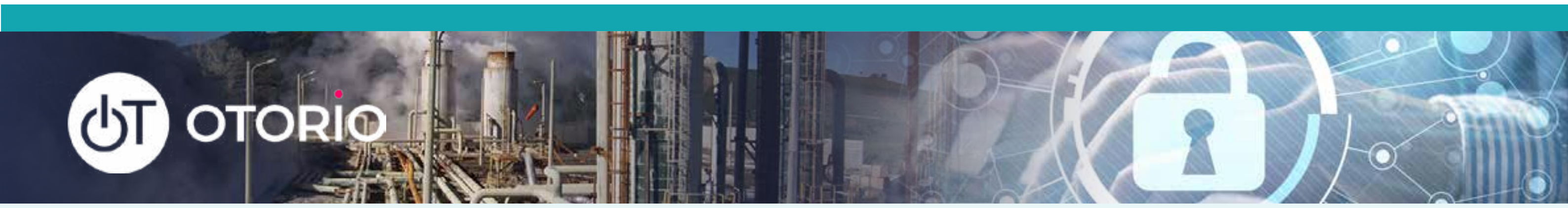
remOT enables your organization to focus on risk management by limiting remote access to specific assets and allowing authorized users to only access certain assets. remOT controls user access permissions and roles on the asset and protocol level. The tool allows no direct access to the OT network, thereby preventing hackers from leveraging and exploiting known CVEs.

Insufficient Access Gateways

reMOT restricts the scope of usage to authorized users and prevents unauthorized personnel from entering the network. With reMOT, administrators can easily manage users' and groups' access permissions and introduce secure remote connectivity.

Excessive Product Floor Access

reMOT limits access of third-parties and vendors to specific assets in the OT Network (e.g., PLCs, HMIs).



remOT Use Cases

Plant managers:

- Provide a secure, single-point-of-entry to the OT network for employees and third-party support and maintenance staff
- View and control remote access to every network segment and asset
- Limit access of third-parties and vendors to specific assets in the OT Network (e.g., PLCs, HMIs)
- Immediately terminate sessions that indicate suspicious activities by sending real-time alerts
- Monitor and control remote Human-to-Machine and Machine-to-Machine (H2M/M2M) communication

Service providers:

- Remotely connect to multiple customer sites without compromising security, safety, or operational integrity.
- Employ a unified central management system to reduce the complexity and cost of managing different remote access solutions

OT equipment and software vendors:

- Provide secure support and maintenance to multiple customers easily and with full transparency

Key Features

Security Features

- Encrypted tunnel
- Multi-factor authentication
- Secure file transfer
- Role-based access list
- No direct connection to the OT network

Administrator Features

- Permission & identity management
- Full visibility on every session & connection
- Control every activity and session
- Record and log every connection for auditing purposes
- Integration with user management password vault tools
- Central management portal and dashboard
- Enhance threat modeling and threat hunting – using OTORIO's RAM^2

About OTORIO

OTORIO delivers next-generation, OT-security and digital risk management solutions that ensure reliable, safe, and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial security experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. Visit our website at www.otorio.com.