OPERANT NETWORKS

The leader in secure data transport & segmentation

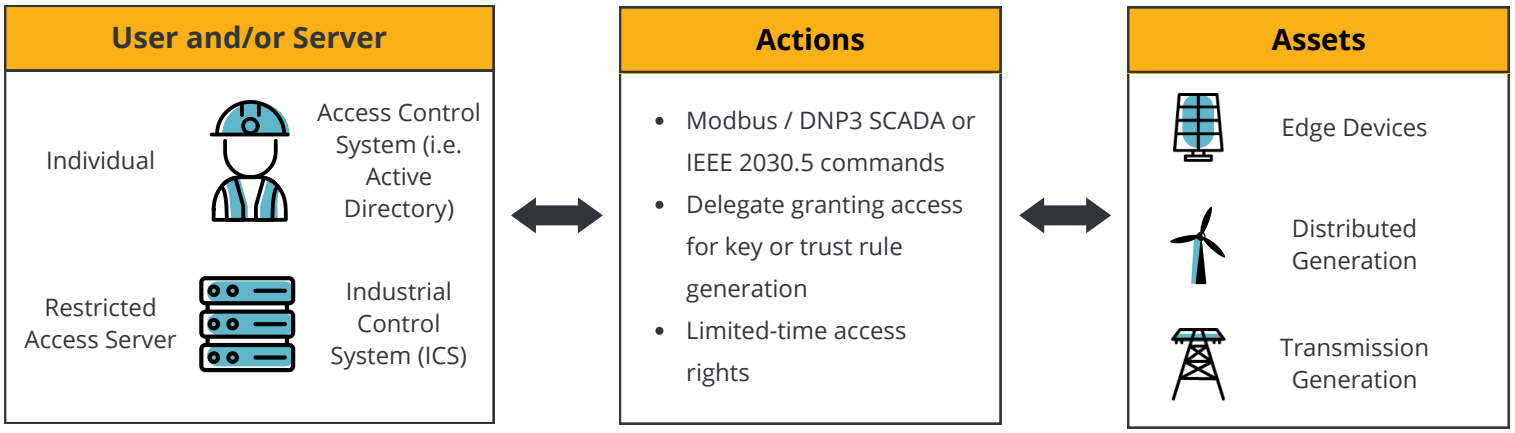
Networks are complicated.
Secure remote access doesn't have to be.

Scan to Access Digital Version

Multi-Party Trust (MPT)

Simplifying secure access controls between machines, systems, and people.

It's a common problem in Operational Technology (OT) networks: How do you give users the access they need easily to assets in the field, without giving them more access than they should have, and for longer than they should have it?



MPT uses a trust console to deploy user-defined policies out to assets in the field and to connect stakeholders while ensuring secure data segmentation.

Attributes

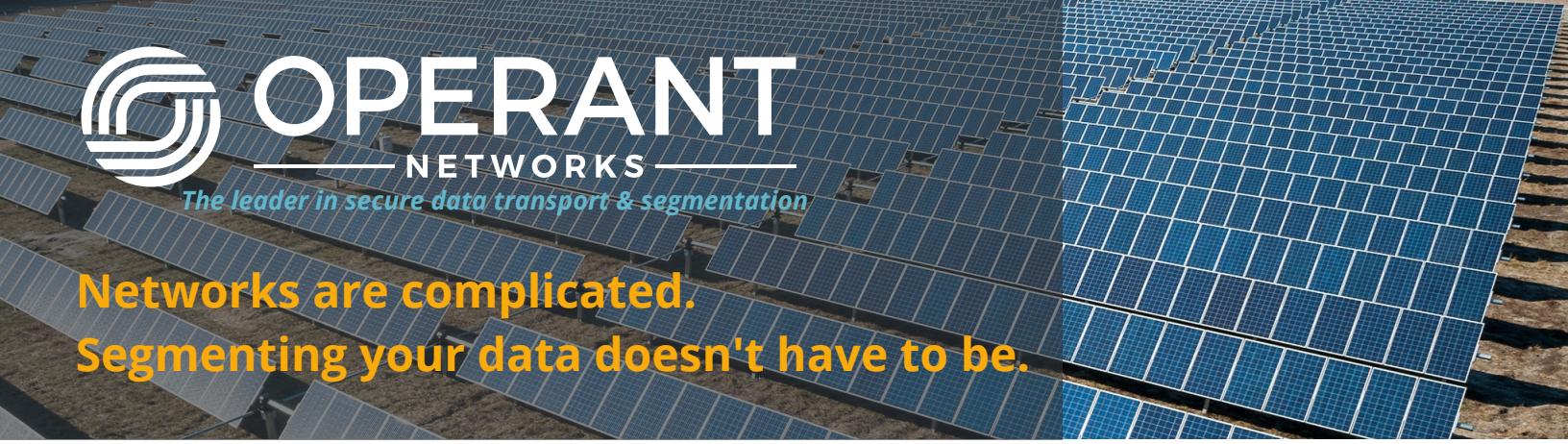
- **Governance** enables administrators' assignment of roles to users and attributes to equipment through identity management services such as Active Directory. Once assigned, these can be synchronized to local Active Directories, allowing secure access when connectivity is lost.

- **Multiple Stakeholder's** roles can be per job function across organizational departments, or even between organizations such as facility owners, third-party contractors, or OEMs.

- **Fine-grained** attributes can be site specific with access restricted down to individual pieces of equipment on-site such as SCADA servers, PLCs, weather stations, historians, etc. Access can be time-bounded for one-off access or restricted to particular maintenance windows on a periodic basis. Access can be further restricted to a list of allowable protocols.

Data-Centric Approach

Using a data-centric approach offers the ability to encrypt, authenticate, and validate each and every data flow's trust rules. This fundamental technology allows users to deliver fine-grained access controls across multiple internal and external stakeholders, while ensuring data is being segmented appropriately.



MTP Specifications

Identity Management

- Identity management based on Azure Active Directory (AAD)
- Simplified list of accessible sites and assets tailored per user
- Time-bounded access settable by the administrator
- Deny-by-default (Zero Trust)
- Role-based access control (RBAC) and Attribute- Based Access Control (ABAC):
- One-time
- Time-based
- Regularly scheduled
- Permanent
- Automatic synch between cloud and local Active Directory servers
- Local authentication for offline sites
- Centralized management in the cloud

Active Directories

- Can anchor into Azure Active Directory, Active Directory; AWS IAM*, Okta*

Platforms

- Microsoft Windows
- Ubuntu Linux
- RedHat Linux

Security

- NERC CIP-012 and CIP-003-9 compatible
- FIPS 140-2 compliant
- NIST compliant
- OpenVPN supported
- TLS 1.3 supported
- SHA 256 hashing supported
- X.509 certificates
- Post-quantum cryptography*

Supported Protocols

- User-to-machine
- RDP
- HTTP
- HTTPS
- SSH
- SQL Queries*
- SCP*
- Machine-to-machine
- Modbus
- DNP3
- IEEE 2030.5
- IEC 61850*
- FTP/ SFTP*
- rsync*

* Feature currently in development