OPERANT NETWORKS

The leader in secure data transport & segmentation

Networks are complicated.
Securing your data doesn't have to be.

Scan to Access Digital Version

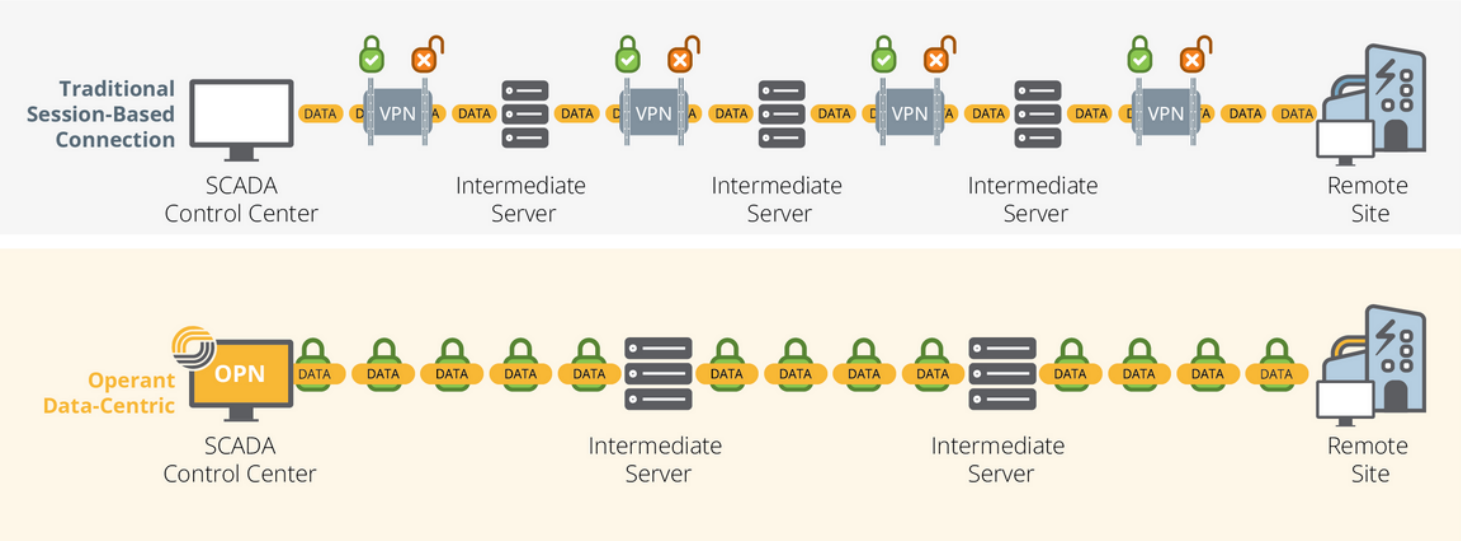
OPN Connect™

Secure-by-Design software layer for industrial networks.

Decentralization and digitalization trends are creating an increasingly unique set of challenges for Operational Technology (OT) teams. Implementing solutions developed for traditional IT use cases often results in overly costly and complex architectures. Ultimately, forcing customers to choose between **reliability, security, and cost.**

What is a Data-Centric Approach?

It's common to think of connections as point-to-point, but in the real world they seldom are. Data traverses multiple VPNs, servers, and firewalls as it moves from the field to an operations center. Likewise, most security tools were developed for securing point-to-point infrastructure and network perimeters. Thus, cyber solutions end up stitched together between handoffs requiring an intricate coordination of data decryption/re-encryption, ongoing configurations, and key management in a best-effort attempt to prevent breaches. The end result is often an entangled assortment of solutions with marginal effectiveness.



Instead, a data-centric approach offers a holistic solution with the ability to easily segment and encrypt data while at the same time authenticating each and every SCADA transaction. Thus, offering seamless end-to-end security for all communications, regardless of network topology or number of handoffs.

OPERANT NETWORKS

The leader in secure data transport & segmentation

Networks are complicated. Securing your data doesn't have to be.

OPN Connect is a secure-by-design software layer that can be added to existing network servers, virtual machines, or on edge gateways.

When deployed, it has the following advantages over traditional approaches:

- **Resilient**. Allows for multi-path communications without the need for complex fail-over controls as found in costly SD-WAN solutions. When packets pass across redundant links, such as private fiber and cellular, or to geographically redundant data centers, 'fastest packet wins' ensures both resiliency and lowest latency.

- **Secure**. All data flows are end-to-end encrypted. Key SCADA data is signed and authenticated, allowing for each transaction to be verified before being processed. Thwarting attempts by malicious actors who may have gotten past perimeter defenses.

- **Nano-segmentation.** All communications are encrypted, kept private, and only visible to trusted parties. Certificates are derived from a verified root of trust, assisting with IT/OT/IoT convergence, even across public networks.

- **Flexible.** Can connect over 'any link that can pass bit'. Additionally, can act as an overlay on existing networking infrastructure, making it easy to deploy, even in complex legacy systems.

- **Multi-Party Trust (MPT)**. MPT falls within the Zero-Trust framework and offers customers an easy way to deploy zero-trust capabilities within OT systems. Multi-Party Trust allows individual users and/or machines to be assigned granular access to remote network assets such as servers, PLCs, etc.

NERC-CIP

End-to-end encryption makes compliance easy, removing the need for intermediate sites and servers to be physically secured.

Multi-Party Trust (MPT) allows individual users and/or machines to be assigned granular access to remote network assets supporting CIP-003-9 compliance requirements.

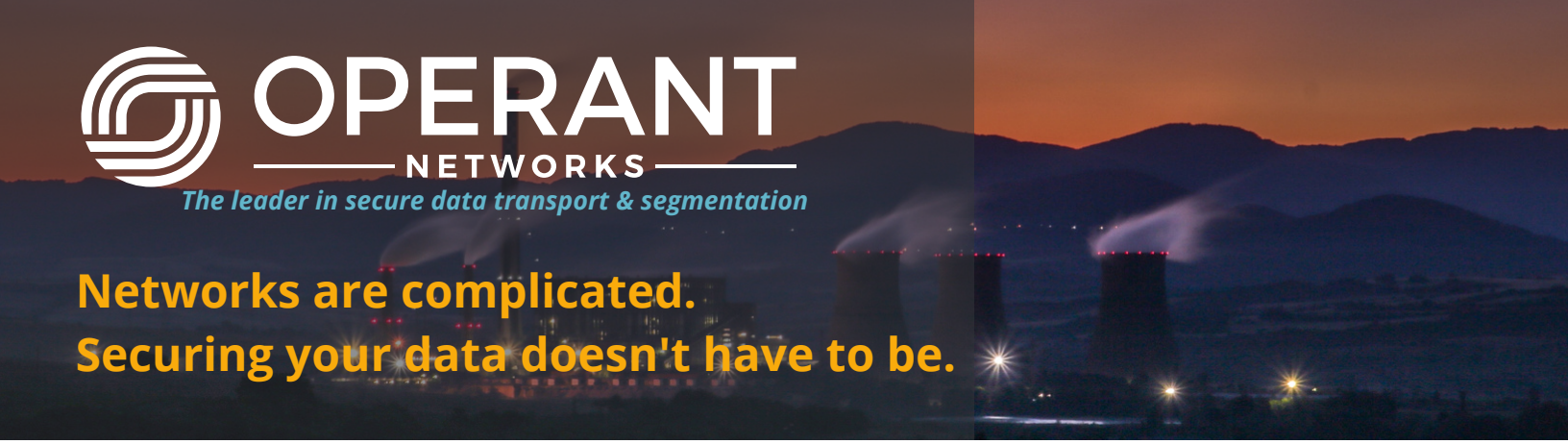
Secure-by-Design for OEMs and Developers

OPN Connect is available for integration with other technology providers. It has a modern publish/subscribe architecture that is broker-less and secure, making it inherently secure. It is compatible with MQTT use cases, but more appropriate for situations requiring reliability and cybersecurity.

Security Summary

Tested and/or backed by the following organizations:

- Dragos
- Exelon/Constellation
- Sandia National Labs
- DOE (U.S Department of Energy)
- NREL (National Renewable Energy Lab)
- Idaho National Labs



Security Summary

Publication/ Packet	Publication Signing	Publication Encryption	Response Publication Signing	Response Publication Encryption	Comments
Command	EdDSA Client software- based private key	AEAD-128	EdDSA Gateway software-based private signing key	AEAD-128	Full end-to-end security. Signing key and certificate updated every day and verified with TPM private key.
Transport	AEAD-128 authentication	AEAD-128	AEAD-128 authentication	AEAD-128	Each transport link is AEAD-128 encrypted with separatekey giving authentication.
AEAD key (default: updated every 4 hours)	EdDSA Server software instance private key	EdDSA public key from certificate collection	-	-	AEAD-128 contentkey encrypted in turn with each public key in certificate collection. Separate AEAD keys for end-end and transport link encryption and authentication.
X.509 Certificate	-	-	-	-	Certificate is signed by root CA and is public.
Signing Certificate	EdDSATPM-based private signing key	-	-	-	Software signing key used for speed with publiccertificate signed by TPM private key having X.509 certificate

OPERANT NETWORKS

The leader in secure data transport & segmentation

Networks are complicated.
Securing your data doesn't have to be.

OPN Connect™ Specifications

Platforms

- Microsoft Windows
- Ubuntu Linux
- RedHat Linux

Supported Protocols

- Industrial
  - Modbus
  - DNP3
  - IEEE 2030.5
  - IEC 61850*
  - FTP/ SFTP*
  - rsync*
- Generic
  - RDP
  - HTTP
  - HTTPS
  - SSH
  - SQL Queries*
  - SCP*

* Feature currently in development

Security

- See table on page 3
- 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

(Optional) Edge Gateway

OPN Connect™ is deployed in containerized VMs or on local servers, gateways, etc. Operant has several preconfigured plug-and-play edge gateways to choose from.