ACCELERATED by DASA

ORTHOS

Securing *All* Operational Technology

DATASHEET

SYSTEMS OVERVIEW

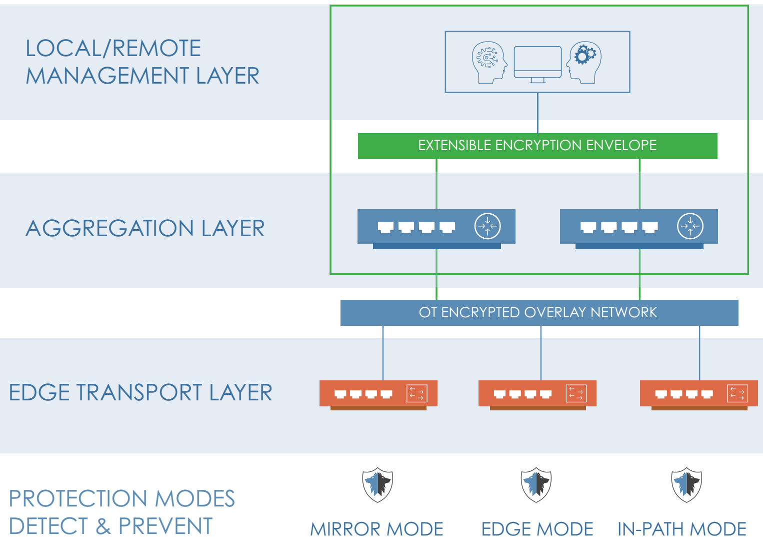
Project Orthos is an IT and Operational Technology (OT) cybersecurity solution. Built specifically to meet the government's call to reduce the cyber attack surface (RCAS), it protects critical infrastructure, static defence and mobile assets from a wide range of cyber threats.

Effortlessly scalable and secure by design, Orthos combines standards-based encryption with a cyber-physical security suite to shield operational technology and communications from vulnerabilities that may be exploited by threat actors.

Providing both detection and protection, it provides long-term, future-proof security through the incorporation of quantum-resilient encryption.

Orthos is a software-based solution, so it can be deployed on a wide variety of hardware and for the most challenging of applications, including high temperature, high humidity, and dirty environments.

SECURE REMOTE ACCESS, FROM ANYWHERE, DIRECTLY TO YOUR OPERATIONAL INFRASTRUCTURE



LOCAL/REMOTE MANAGEMENT LAYER

EXTENSIBLE ENCRYPTION ENVELOPE

AGGREGATION LAYER

OT ENCRYPTED OVERLAY NETWORK

EDGE TRANSPORT LAYER

PROTECTION MODES DETECT & PREVENT

MIRROR MODE

EDGE MODE

IN-PATH MODE

Project Orthos provides dual encryption security. First, a secure link from the management layer (wherever it is located) to the remote asset. Second, an encrypted overlay to the operational technology network infrastructure.

Secure remote access is available down to an individual component level, with rich media (images, voice and chat) to support operational staff with threat monitoring and assessment.

Orthos provides vulnerability shielding for operational technology within an encrypted overlay network. The network is highly scalable and features built-in redundancy for greater resilience. Since most legacy OT devices do not have built-in cryptographic capabilities, Orthos handles the cryptography and key management for every device on the network.

Communication between OT devices on the same network remains intact, no matter how isolated the system. Integration points with IT systems, such as SCADA, big data analytics, ERP, or cloud services sit within the overlay network.

KEY FEATURES

- Highly scalable and configurable
- OT vendor equipment agnostic
- Support for a wide range of industrial control protocols
- Compatible with IT and OT converged networks
- Provides encryption at Layers 2, 3 and 4
- Built-in asset management functionality
- Performs passive asset and protocol discovery
- Leverages machine learning and artificial intelligence

Orthos' approach to OT security and communication utilises certified encryption and key management processes to deliver a secure overlay that eliminates attack paths to vulnerable assets within the OT network. It has three deployment modes:

Although protective mode (in-path) is the recommended deployment, it is possible to run the system in mirror mode for observation and monitoring, or edge mode. In this case, the full in-path capability is still available as a contingency in case of a cyberattack.

FLEXIBLE MANAGEMENT

Orthos architecture allows for secure remote monitoring of an asset (EG a naval vessel) from a centralised command and control or cyber-physical operations centre (C-POC). The C-POC can be used to provide both security monitoring and remote engineering support, reducing the need to deploy maintenance staff to remote assets.

Orthos can also operate as a discrete, autonomous solution within a single asset (EG on-board a vessel during active engagement). In this scenario, command and control of the system is available through a single, non-technical dashboard and visualisation engine.

Contact Senetas

Senetas Europe Limited, Worting House,
Church Lane, Basingstoke, Hampshire RG23 8PX

E: info@senetas.com

SENETAS