



Proven OT, IoT, IT and 5G protection.

Sectrio is an agentless, non-intrusive and multi-tenant cybersecurity solution for OT, IoT, IT, and 5G networks. Sectrio offers end-to-end OT/ICS and IoT security coverage on a single platform.



### DISCOVER

Discover all devices (managed and unmanaged) on your network to assess network vulnerabilities and underlying risk exposure.



### MITIGATE

Reduce internal attack surfaces, network gaps, and stop malicious network movements within the network.



### DETECT

Detect network threats in real-time using Sectrio's patented AI/ML based anomaly detection, heuristics and signatures



### REMEDiate

Respond to attacks using automated/manual actions and industry-standard frameworks.

## Why Sectrio ?



Maintains the world's largest honeypot network capturing over 22M attacks a day in over 75 countries.



Micro-segmentation built on a Zero Trust framework as a core component within our product.



Seamless implementation and deployment across facilities with complex and diverse set of technologies.



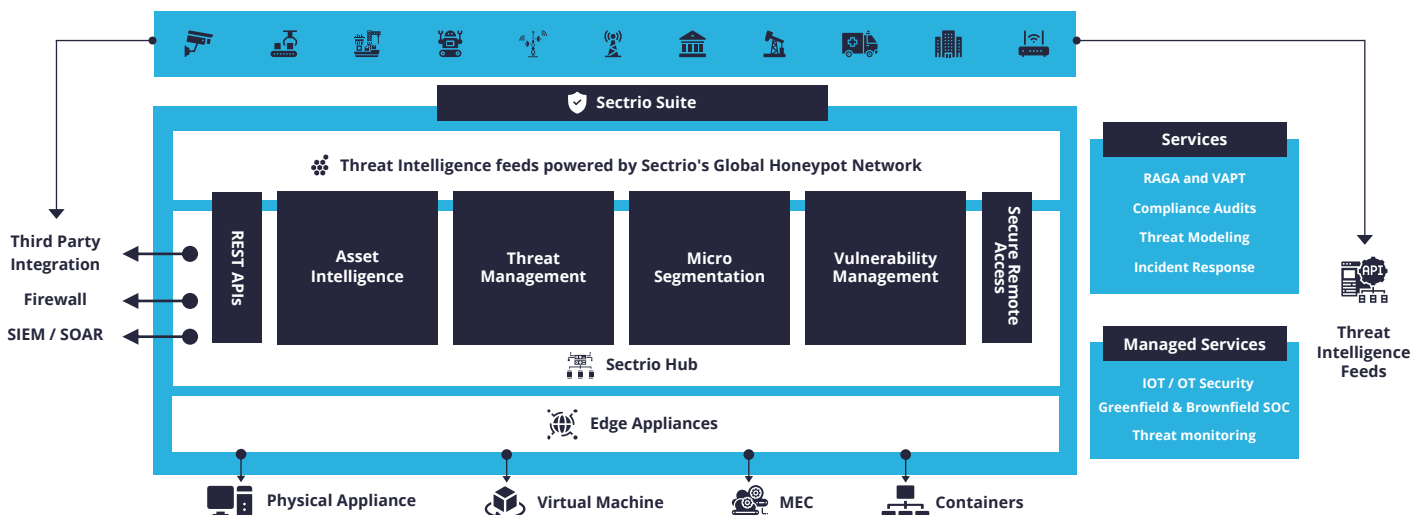
Comply with global standards and guidelines such as ISA/IEC 62443, NIST, NERC CIP, CEA, NIS2 and NCAs OTCC



24/7 Global SOC coverage with essential services from certified OT/ICS cybersecurity professionals



Our IoT/OT threat intelligence is industry leading with over 30% organic traffic generated.





## The Hub

Is the heart of the Sectrio deployment. The Hub is the central point for the Edgetech Appliances and gives the user an intuitive interface.



## Vulnerability Management

Module discovers devices within IT-OT and IoT networks, maps the vulnerabilities, and highlights risks.

### Highlights

- Continuous discovery and scanning in both active and passive modes giving a comprehensive risk assessment of your network.
- Allows discovery of all managed and unmanaged devices in network.



## Threat Management Module

Allows fully automated, agentless, and non-intrusive monitoring of all connected devices to discover threats in real-time.

### Highlights

- Real-time threat detection leveraging the most advanced IoT/OT-specific threat intelligence data in the market.
- Deter hackers using artificial intelligence, signatures, heuristics, and patented technology to continuously check for anomalies and rogue behavior within your network.
- Ensure compliance with the latest cybersecurity mandates.



## EdgeTech

Data Collectors are deployed in network segments that need to be monitored. An appliance can be physical, virtual, containerized or cloud based. Easily supporting any deployment type.



## Micro-segmentation Module

Helps manage east-west network access and enforces policies to limit access and control unwanted lateral network movement.

### Highlights

- Detect and prevent unauthorized access within the network by diving into workload level details.
- Track device behavior and improve east-west network security.
- Comply with zero-trust cybersecurity mandates.



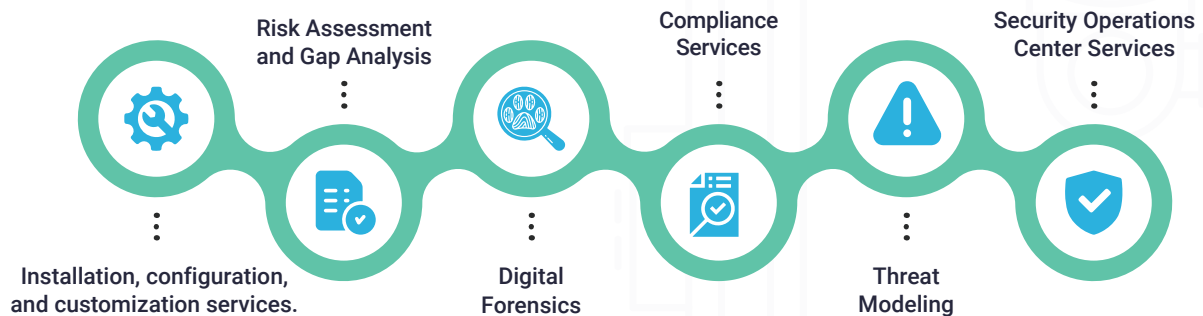
## Threat Intelligence

Is built into the core of our Threat Management Module but can be deployed as a standalone instance as a feed. Derived from the world's largest honeypot network focusing on IoT/OT exploits.

### Highlights

- Identify Indicators of Compromise, detect attack patterns and course of mitigation actions, and improve overall IoT/OT cyber resilience.
- Integrate into existing deployed solutions like SIEM, SOAR, and SOCs via APIs and STIX/TAXII.
- Mitigate risk with our zero-day attack data to ward off newly found threats.

## Professional Services



## About Us

Sectrio is a division of Subex Digital LLP, a wholly owned subsidiary of Subex Limited. Sectrio is a market and technology leader in the Internet of Things (IoT), Operational Technology (OT) and 5G Cybersecurity segments. We excel in securing the most critical assets, data, networks, supply chains, and device architectures across geographies and scale on a single platform. Sectrio today runs the largest IoT and OT focused threat intelligence gathering facility in the world.

Request Demo

