



# SECTRIO HUB

The Sectrio Hub ("Hub") acts as the heart of the Sectrio deployment. The Hub is the central point for Edgetech Appliances and Remote Collectors and presents the user interface for Sectrio. The Hub gives an intuitive and easy to use interface, it also acts as the centralized brain where all Edgetech Appliances securely send data to be analyzed.

## Challenges



Gaining a unified view of threats, alerts logs and device data



Detecting threats in real-time



Enabling cybersecurity teams to operate with actionable information and insights



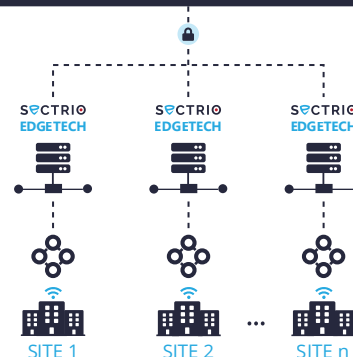
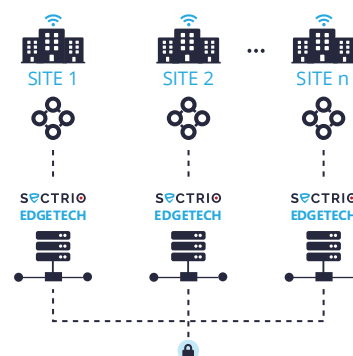
Centralizing threat response measures

All custom interfaces between Sectrio and other systems such as SIEMs, SOARs, email systems, etc. are typically done on the Hub. The Hub uses metadata from the Edgetech to perform AI-ML detection using its Sectrio's anomaly engine to detect threats.

## Benefits

Alerts, metadata, logs and device data traverse from Edgetechs and Collectors to the Hub. The Hub sends threat intelligence to the Edgetechs and configuration information from user changes. The Hub to Edgetech traffic can be disabled if the deployment has to be in unidirectional networks (OT networks) and updates can be manually applied periodically.

The Hub is available in multiple form factors; installable, containerized, virtual machines, hardware, and hosted



The Hub Connects regularly to the update center for Threat Intelligence changes. The three Sectrio modules namely Vulnerability Management, Threat Management and Micro-segmentation are also displayed within the Hub.

versions. Hosted cloud versions are available in three locations India, London, and Denver. The Hub is also supported on most public cloud providers as images that can be spun up as a form factor that the customer chooses and is compatible with their cloud deployment. The Hub has no dependency on any cloud native technology and hence can be run on any public cloud environment.

All images of Hubs are hardened, however if the customer chooses an installable version, the customer must harden the machine where the Hub is installed.

Hubs are sized and licensed based on the network interface they support. There are four listed sizes Hubs that support 1 Gbps, 10 Gbps, 100 Gbps and 1 Tbps. The higher sizes are exclusively designed for Telcos and for enterprise the 1 Gbps and 10 Gbps should suffice. The number of nodes supported is dependent on many factors such as the throughput of the devices and number of network appliances connected to the Hub, etc. For example, the Hub will support many more low power sensors as compared to 4K CCTV cameras. The number of devices below is therefore just indicative; however, the sizing does guarantee to support the network throughput it is sized and licensed for.

Network Throughput	1Gbps	10 Gbps	100 Gbps	1 Tbps
Max Supported Nodes	5000	50000	500000	5000000
CPU (2 threads)	16	48	124	396
RAM (GB)	64	192 GB	576 GB	1.7 TB
Storage (SSD)	5 TB	15 TB	45 TB	150 TB
Data Retention	30 Days	30 Days	30 Days	30 Days
Concurrent Users	20	50	100	200
Max Collectors supported	10	25	50	100
Edgetech Appliances	10	25	50	100
Container	Docker	Docker	NA	NA
Virtualization	ESXI 6.0+, KVM	ESXI 6.0+, KVM	ESXI 6.0+	NA
OS Supported	CentOS 7.6, RHEL 7.6	CentOS 7.6, RHEL 7.6	RHEL 7.6	RHEL 7.6
Compatible Hardware	R-SMALL	R-MEDIUM	R-LARGE	NA

## 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. To learn more visit: [www.sectrio.com](http://www.sectrio.com)

 Global Offices:  
India, Americas,  
Europe, Asia Pacific  
Middle East & Africa.

 @sectrio

 Sectrio