Managed Threat Detection Service – Network Sensor

Norm's Managed Threat Detection Service - Network Sensor is a module from Norm's Cyber Security as a Service (CSaaS) offering.

The Managed Threat Detection Service - Network Sensor provides cloud-based monitoring of your network traffic traversing and transiting your corporate network which is then scrutinised & analysed 24/7/365 by our Security Operations Centre (SOC).

This service module focuses on the **Technology** element of Norm's holistic trinity of cybersecurity - **People, Process and Technology**. Its purpose is simple:

* Continuous real-time security monitoring of your corporate network traffic
* Automatically alerts during an identified threat event
* Delivers total visibility of all threats and alarms that occur within your networked IT environment

The Network Sensor is a physical appliance that is hosted within your corporate network and passively monitors your corporate traffic looking for suspicious or threatening activity. The Network Sensor constantly monitors your corporate network allowing for immediate response from our SOC Team. The information collected from the monitoring process is recorded, analysed and investigated to enable a response.

Service Features

You will gain access to the following features:

- Network Sensor works through the deployment of a physical appliance or appliances at strategic (i.e. traffic intensive) points within your corporate environment. The sensor(s) continuously monitors your corporate network traffic for known threats and Indicators of Compromise (IoC).

- In-depth visibility and detection across all the organisation's corporate network(s), for all devices connected including, Laptops, Desktops, Servers, Mobile and IoT devices monitored for threat detection.

  - Detect threats across the organisation's services and infrastructure
  - Automated threat detection and correlation process
  - Significantly reduced time to detection
  - Enabling rapid incident response times

- The Network Sensor is available as two versions; Small and Medium offering an appropriate level of Threat Detection performance dependent on the size of the organisation and the volume and type of corporate traffic being monitored.

On-Boarding Process

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the installation, and introduce you to your Norm technical lead. The onboarding process will include:

- Providing you Norm's service handbook detailing our service operational processes, SLA and contacts

- Providing you with your Network Sensor Appliance and co-ordinating the installation with your IT/Network team(s) or provider(s)

- Enrolling your Network Sensor device into Norm's Threat Detection Service and SOC.

- Providing access to Norm's Visualiser platform

Once the service is fully deployed our customer experience team will provide you with access to the Norm visualiser. This visualiser will provide you with an overview of all the threats detected on your network, as well as a log of all incidents and remediation. A list of all endpoints will also be available to give you full visibility of your protected environment.

The SOC can also be available to provide technical advice and assistance on cyber-security queries or issues should this be required.

Technical Requirements

The Network Sensor is based upon Fortinet's Fortigate security appliances which supports the following:

	Small Network Sensor	Medium Network Sensor
IPS Performance	1.4Gbps	2.6Gbps
Number of WAN Port	2	2
Number of Internal Ethernet Ports	8	12
Physical Requirements (H x W x L)	38.5 x 216 x 160 mm	44 x 432 x 254mm
Form Factor	Desktop	Rack Mount, 1 RU
Power Requirements	Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz	100–240V AC, 50-60 Hz
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)
Humidity	Humidity 10–90% non-condensing	Humidity 10–90% non-condensing

The Network Sensor Appliance will passively monitor your corporate network traffic and will seamlessly operate alongside any pre-existing firewall, VPN or internet gateway solution you might have, providing a security in-depth approach.

Service Prerequisites

The customer must subscribe to Norm's Threat Detection Service to access the Network Sensor service module.

Service Availability

The service is managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Customer Experience team is available during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

Software updates and patching for Fortigate Network Sensor will be automatically managed by the Norm platform. Hardware replacement is available 24x7 with a Next Business day replacement. Hardware and Software support is available 24x7 and provided through Norm's SOC.

The Customer Experience and SOC teams will be on hand to provide technical advice and assistance for any queries or issues should this be required.

Customer Responsibilities

- The Customer will be responsible for hosting the Network Sensor appliance within their corporate environment including suitable operating environment (temperature, humidity and power as specified in the technical requirements).

- The Customer shall provide a network connection for the service monitoring port, ideally with static IP or DHCP reservation.

- The Customer shall provide a network traffic feed from the required ports/VLANs to the Network Sensor, such as a SPAN or Mirror port to obtain and monitor your corporate traffic.

- All cabling, patch panelling and associated equipment at the remote site is the responsibility of the Customer.

- The Customer is responsible for providing full site and contact details for all locations.

- The Customer shall nominate an administrator internally for the Norm Visualiser.

- The Customer shall be responsible for user administration within the Norm Visualiser.