Warning! May contain dull*

norm.

*Reassuringly dull cyber security

Managed Threat Detection & Response (EDR) Service

Norm's Managed Threat Detection & Response (EDR) service is comprised of a standalone module from Norm's Cyber Security as a Service (CSaaS) offering.

Norm's Managed Threat Detection & Response service is built upon FireEye's Endpoint Detection and Response (EDR) software platform which is integrated onto Norm's SoC and managed service. The service proactively looks for malicious behaviour on your devices (laptops, desktops and servers) and stops it before it can harm through spreading within your environment, gaining access/control to your data, applications or devices.

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 monitoring of your devices looking for unknown threat and malicious behaviour
- Automatically alerts and isolate devices during an identified threat event
- See the Results with near real-time reporting

EDR software detects suspicious or threatening activity on endpoints (laptops, desktops and servers). EDR constantly monitors endpoints allowing for immediate response. The information collected from the monitoring process is recorded to be analysed and investigated to enable response.

EDR complements other security solutions looking for known threats such as AV, UTM, email spam solution etc, which searches for known threats through "signatures". EDR instead looks for unknown threats and malicious behaviour that doesn't have a defined signature (aka Day Zero attacks) offering additional protection for your devices, data and users.

Service Features

You will also gain access to Norm's managed service offering the following features:

- EDR works through continuous monitoring of the endpoint using Indicators of Compromise (IoC). The automated nature of EDR security allows.
  - Streamlined threat detection process
  - Instant threat detection
  - Investigation, reporting and response enablement

- In-depth visibility and detection across all the organisation's endpoints, with all devices covered for threat detection.
  - Detect threats across the organization
  - Centralised Visualiser
  - Rapid incident response times

- Real-time respond to threats. Many endpoint threats can bypass traditional and advanced security in the time it takes for a human to respond to the activity. With EDR, clients will benefit from:
  - Automated detection process
  - Significantly reduced time to detection
  - Ability to respond within minutes

How the Managed Threat Detection & Response service works

Endpoint Detection and Response tools work by continuously monitoring activity on endpoints, to identify suspicious or threatening behaviour in real-time. Information is recorded and analysed for internal or external attacks. EDR can identify specific behaviours to alert organizations to potential threats before the attackers can cause harm. Once a threat has been detected, EDR can isolate and deflect attacks from internal and external sources, protecting endpoint devices from risks. The end-to-end analysis is supported by a range of innovative technologies, including machine learning and behavioural analysis.

The EDR platform is then managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year.

Once a threat is identified there are two primary paths the incident can follow: -

Automated Isolation

If a threat from your playbook is identified, the agent on the device will respond accordingly as soon as the threat is identified; this may include isolating that device. When a device is isolated a custom message is displayed requesting that the user does not power off the device and contacts your IT team or outsourced ICT provider.

Manual Incident Handling

If the threat identified is not in your playbook a member of our SOC will contact your nominated representative(s) within 15 minutes to discuss your options and ask for a decision.

After isolating any threat, a member of our SOC will co-ordinate with your organisation to mitigate any effects caused by an incident.

On-Boarding Process

Onboarding with the service will be managed through Norm's customer experience team who will arrange a Welcome call to provide a service introduction and onboarding assistance including:

- Providing EDR agent software for your devices operating system(s)
- Assistance with EDR agent rollout phase
- Enrolling your EDR device agents into Norm's 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 on hand to provide technical advice and assistance on cyber-security issues should this be required.

Technical Requirements

The EDR agent from FireEye supports the following OS environments and technical resources:

FireEye EDR Agent

FireEye Endpoint Agent	
Host Resources	1GHz CPU, 2GB RAM, 300MB Storage
Access Requirements	Local Host
Outbound Access on Port 443	hexXXXXXX-hx-agent-1.hex03.helix.apps.fireeye.com, 3.126.32.26 & 35.157.100.155
Image Size	23MB

Supported Operating Systems and Environments	
Windows	XP SP3, 2003SP2, Vista SP1 and up, 2008, Win7, 2012, 8, 8.3, 10, Server 2016
MacOS	OS X 10.9+
Linux	Red Hat Enterprise Linux 6.8+, 7.2 + CentOS 6.9+, 7.4+

Norm will provide your technical team with the three specific installation packages (Windows, MacOS and Linux) via the Norm Visualiser. Upon receipt of these packages, your technical team can push the software to the end devices using whatever software distribution mechanism they prefer (i.e. Windows GPO, Intune, Jamf, etc.)

The EDR client will work seamlessly with any pre-existing Anti-Virus/Anti-Malware solution you might have on the end devices, providing a security in-depth approach.

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 operate Monday to Friday 9 am to 5:30 pm.

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

Customer Responsibilities

- You will need to provide information on your device estate including;
  - Type of devices,
  - Number of each device
  - Device operating system
- Customer will be responsible for deploying EDR agent software to endpoint devices. Typically, agent deployment would be managed by the customer's corporate software rollout software such as GPO.