Managed Endpoint Detection and Response *

What is it?

Our Managed Endpoint Detection and Response (EDR) service specifically protects endpoint devices regardless of where your users are working from. It can be in place, protecting hundreds of employee devices, **within days.**

The **norm.** Managed EDR Service is a standalone module of its core Cyber Security as a Service (CSaaS) product, which is built upon FireEye's industry-leading Endpoint Detection and Response software platform.

Why now?

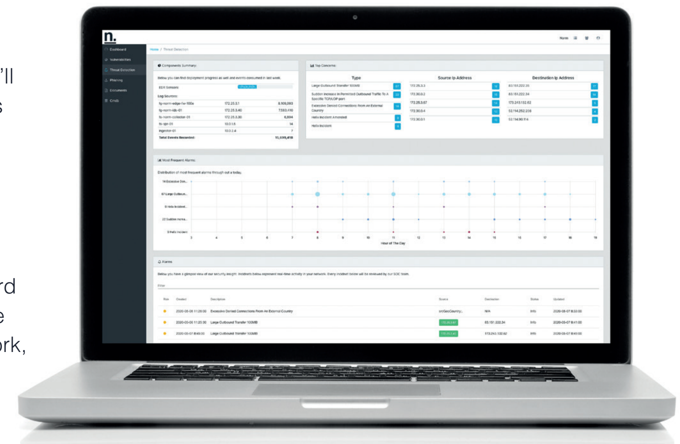
An increasingly dispersed workforce has exponentially expanded the cyber risk to UK businesses from untrained or poorly trained employees, unprotected home networks and mobile hotspots, untested collaboration software and a dramatic increase in cloud-based working.

All of these things combined mean that the attack surface has grown at a rapid rate, requiring advanced cyber security protection.

What's included?

Endpoint Detection and Response (EDR) // EDR uses software agents to constantly monitor all devices and other endpoints across your entire network. If they detect suspicious or threatening activity they then respond to the threat in a single integrated workflow:

* Automated Isolation: If a threat from your playbook is identified, the agent on the device will respond immediately according to the agreed protocol
* Manual Incident Handling: If the threat identified is not in your playbook we'll contact your nominated representative within 15 minutes to discuss options and request a decision



Managed and monitored from the UK

Our 24/7/365 Security Operations Team will manage and monitor the service for you, as well as providing technical advice and assistance on cyber security issues if needed.

Near-real time visibility

The **norm.** Visualiser Dashboard gives you an overview of all the threats detected on your network, including a log of all incidents and remediation steps.

Want more detail?

For a full service description of the **norm.** Managed Endpoint Detection and Response <<ClickHere>>.
To register interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

***Reassuringly dull cyber security**

norm.

In a nutshell…

The **norm.** Managed Threat Detection Service – Endpoint Sensor is built upon FireEye's Endpoint Detection and Response (EDR) software platform.

The service is supported and backed by our 24/7/365 Security Operations Centre (SOC) and provides constant protective and preventative monitoring of your Endpoint devices.

EDR software detects suspicious or threatening activity on endpoints (laptops, desktops and servers) irrespective of their physical or logical location; in the office, at home, on the road or in the cloud.

The service not only enables the constant monitoring of all your endpoints but also allows for immediate, effective response and neutralisation of an incident before it becomes a full breach.

How does it work?

Endpoint Detection and Response tools work by continuously monitoring activity on endpoints, with the aim of identifying suspicious or threatening behaviour in real time.

Information is recorded and analysed for internal or external attacks. EDR can identify specific behaviours to alert organisations 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 the **norm.** UK based Security Operations Centre (SOC), 24hrs a day, every day of the year.

FAQs…

We have existing technologies in place, such as anti-virus, firewall and mail filtering – aren't we already covered?

Not completely. Traditional IT security products rely on signatures and rules that have been created to identify known threats and vulnerabilities. The **norm.** managed EDR service complements your existing security solutions by looking for unknown threats. With so many users now working remotely, the attack surface has grown, meaning greater risk of exposure to unknown threats.

What about networking monitoring tools, don't they provide similar protection?

To a certain extent, but the issue of identifying unknown threats – such as zero day attacks – remains. Our managed EDR service uses a threat intelligence database to help identify and mitigate previously unseen threats. Threat intelligence combines a number of sources – such as open source, social media and the deep and dark web – to proactively identify the latest cyber-attacks.

We use remote access technology to control access to applications and services, will that protect us?

Technologies like VPNs, RDP and Citrix are great for allowing users to access online resources remotely, but they don't provide adequate protection against cyber security attacks. For example with Citrix, the applications and systems still rely on keyboard inputs and mouse movements from a device. Tools like VPNs and RDP can also be easily circumvented if passwords are compromised.

Couldn't we go out and buy our own EDR solution?

You could, but the **norm.** managed EDR service uses a number of threat intelligence databases to provide the highest levels of protection while minimising false positives. In addition, the cost of buying and managing the solution would be significantly more. Our service also gives you access to our 24/7/365 Security Operations Centre, staffed by a team of highly skilled cyber security engineers.

What customer resources are required to manage this?

The **norm.** managed EDR service requires minimum intervention from the customer. We monitor endpoint devices for potential threats on your behalf, and where previously agreed will isolate the device. Where we don't have a protocol in place, we'll contact your nominated representative to agree next steps.

How long does it take to set up?

The **norm.** managed EDR service can be up and running in a matter of days, ensuring your users and your business are protected as quickly and comprehensively as possible.

How does this service support core business operations?

Businesses are adapting to a new normal – working and technology practices have changed and will continue to do so. A highly dispersed workforce means an expanded attack surface, and regardless of where your employees are located, unprotected endpoints or devices are vulnerable to a cyber security breach. A breach can effectively cripple your business - both financially and in terms of brand reputation.

norm.