Our vision is to help you build, implement and maintain an ongoing programme to reduce cyber risk in a way that's right for your business. Our MDR service is part of a range of services that we've developed to help you succeed in an ever-changing landscape.

What is the MDR service?

MDR is our managed cyber security service that provides comprehensive intrusion detection of malware and malicious activity in your network. It proactively monitors endpoints and devices, whether they're on-premises, in the cloud or on mobile. The service looks for points of compromise on your devices and uses the agent locally to make in-flight decisions based on the detected activity – with the added value of having alerts that activate the need for human response.

How does it work?

By leveraging advanced cyber security architecture from our trusted partner network, the MDR service is designed to help organisations cope with the explosion of data today. The service is delivered in the form of an agent that goes on to mobile devices and servers – including public and private cloud environments. Centrally managed and rolled out across Windows, Mac, Linux and Android operating systems, it offers out-of-the-box threat hunting and forensic data capabilities.

KEY FACTS

- ***Comprehensive*** – integration with our SIEM service and Incident Response
- ***Reliable*** – forensic coverage on all devices and roll-back to specific points in time
- ***Seamless*** – cloud, on-premise and hybrid deployment options
- ***Rapid*** – 30-minute SLA for critical events
- ***Human*** – dedicated expertise on hand to aid critical decision making

What are the benefits?

Offers the reassurance of a human approach to cyber security

Our MDR service provides alerts as to when human involvement is necessary. Once an alert has been given, a member of our dedicated team can then begin the decision-making process to quarantine, remove and/or remediate the problem device(s) away from the network to stop any further proliferation of infection within your IT environments.

Reduces the expense of cyber security

EDR (Endpoint Detection and Response) solutions require forensic expertise before decisions are made. With today's explosion of data and an increase in the number of incidents that require attention, this can lead to increased downtime and costs associated with employing the expertise required. It's important to ensure that when flags are raised, you have the capability you need to move forward – which is what our MDR service provides.

Minimises downtime so you can rapidly return to operations

Our MDR service is integrated into our SIEM (Security Information and Event Management) service as well an Incident Response Service team. This means all teams can interact seamlessly when threats are identified to get you back to a point of operation as quickly as possible.

Integrates seamlessly with Office 365

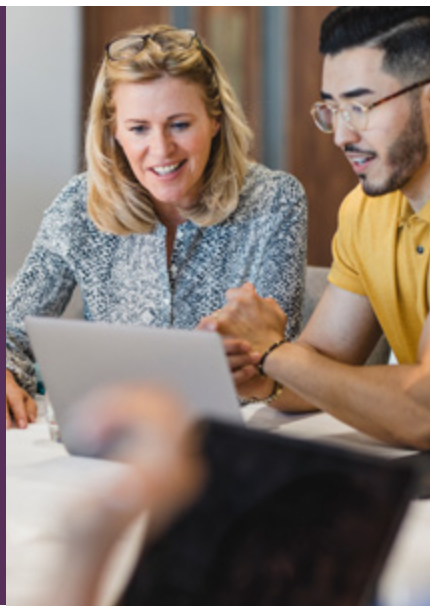
In addition to being compatible with any endpoint and any device, our MDR service fully integrates with Office 365. This means you can detect threats within that environment and make decisions based on the users that are using that software. Our service provides the reassurance that your Office 365 setup is fully protected and secure.

Leverages one of the world's largest threat and vulnerability databases

As opposed to purchasing data, we leverage our MDR Service's threat and vulnerability database, which is one of the largest in the world. With the widest visibility of when and where threats are occurring in the industry, we're able to offer threat hunting that provides proactive protection – helping you prepare for issues before they occur.

WHY SOFTCAT

- Coverage of all operating platforms – improve your threat visibility
- Around the clock support – strengthen your cyber resilience
- Forensic coverage of all endpoints – reduce the impact of incidents
- Protection for public cloud environments – ensure you're fully secure
- Support for Operational Technology (OT) – secure 'unpatchable' critical systems



Softcat