



# MANAGED DETECTION AND RESPONSE (MDR)



**ENDIDA**  
NEXT GENERATION CYBER DEFENCE

## WHAT IS MANAGED DETECTION AND RESPONSE?

Endida provides a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response. The main benefit of MDR is that it helps rapidly identify and limit the impact of threats without the need for additional staffing.

**70%**

Of cyber attacks target small to mid-sized businesses.

*Source: National Cybersecurity alliance*

**788**

Average number of weekly cyber attacks in the UK in 2022

*Source: Checkpoint*

**£100k**

Average cost of a cyber attack for UK business.

*Source: National Cybersecurity alliance*

**83%**

Of UK business feel they are not fully prepared for a cyber attack

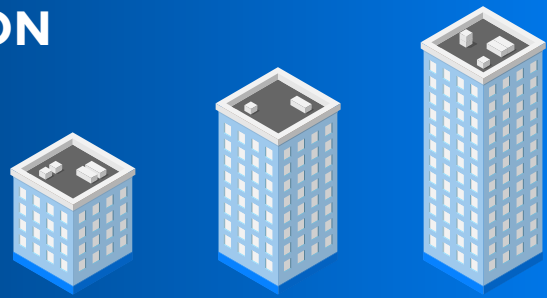
*Source: Gartner report*

**GET IN TOUCH TO FIND OUT HOW WE CAN  
HELP YOU TODAY**

[endida.com](https://endida.com) | 0238 2180 428 | [info@endida.com](mailto:info@endida.com)



# WHAT SIZE OF ORGANISATION IS A MANAGED DETECTION AND RESPONSE SERVICE MOST SUITABLE FOR?



An MDR service can be suitable for businesses of all sizes. However Endida recognises that different sizes of organisations will have different needs so have tailored our services to fit your specific needs.

Mid-sized to large organisations are likely to already have their own IT or CS teams however may still be challenged with a lack of capacity or capability due to the complexity of their IT environments and a large number of endpoints.

Smaller organisations may not have the same level of complexity but may also find that building their own in-house cybersecurity capability is very costly and complicated, and therefore it is far more cost effective to enlist outside help.

Statistics have shown that both small and large organisation are equally likely to be a target for hackers.

## WHAT CHALLENGES DOES MDR SOLVE?

- ✓ Shortage of internal resources and expertise
- ✓ Keeping up with increasingly sophisticated cyber threats
- ✓ Faster incident response to prevent damage and downtime caused by cyber attacks
- ✓ Overwhelming volumes of incident data leading to alert fatigue
- ✓ Lack of visibility of your network and endpoints
- ✓ Enables advanced threat identification and threat hunting

### HOW IT WORKS

#### ADDING PROACTIVE DEFENCES

Stopping threats before they get into your network

#### INCIDENT INVESTIGATION

Thoroughly digging into any suspicious behaviour or files

#### ALERT INVESTIGATION

Ensure a security alert is fully investigated in minutes and is not a false positive

#### REMEDIATION

Fixing any vulnerabilities and issues as they happen

#### PROACTIVE THREAT HUNTING

As it says on the tin! Going hunting for

## GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

