

# MANAGED DETECTION AND RESPONSE

Managed Detection and Response with integrated world leading threat intelligence that helps protect your endpoints and keep your organisation safe 24x7.



Six Degrees' Managed Detection and Response (MDR) service integrates world leading threat intelligence into Microsoft Azure Sentinel and Defender for Endpoint. Combined, they provide an exemplary managed endpoint protection and response service, protecting your organisation 24x7.

Our UK-based cyber security experts harness Microsoft's leading security products and threat intelligence from Recorded Future to provide intelligence-led, human operated cyber incident management, leveraging automation for swift response and containment of security incidents identified on your endpoints, with service support you can trust.



Six Degrees' Managed Detection and Response service leverages threat intelligence from Recorded Future, the world's largest threat intelligence company. The service combines persistent and pervasive intelligence collection and analytics to provide real-time visibility into the ever changing digital landscape. This intelligence complements and extends our capabilities to take proactive measures to disrupt adversaries.

When your users are distributed outside your office, your organisation's exposure to data breach increases:

- Larger attack surface as your users are accessing more public cloud-based services from beyond your corporate perimeter
- Non-managed corporate devices reduce cyber security best practices
- Increased targeting from highly motivated and increasingly sophisticated hackers bypassing traditional antivirus software

Six Degrees' Managed Detection and Response service leverages the industry-leading Microsoft Defender for Endpoint and Azure Sentinel platforms, alongside integration with Recorded Future's world leading threat intelligence platform. The service is delivered by highly trained cyber security professionals operating from our 24x7 UK onshore Security Operations Centre (SOC). We deliver cyber incident management, incident response, breach prevention, and incident analysis, all while assuring we are detecting breach attempts proactively based on the very latest cyber security intelligence and threat indicators.

- Mitigate the cyber security risks of maintaining a remote workforce
- Reduce hackers' ability to expand cyber-attacks across your infrastructure
- Minimise the risk of data breach resulting in financial, operational and reputational damage
- Maintain operational resiliency, backed up by an industry-leading fully managed service

## Managed Detection and Response

Managed Detection and Response is a fully-managed service powered by Microsoft Defender for Endpoint, a unified endpoint security platform for preventative protection, post containment investigation, and contextualised response.



24x7 real-time alert management, detection and rapid response



Comprehensive protection throughout your infrastructure – right down to the endpoint



Trended reporting to quantify the risks that have been contained



Bespoke deployment, configuration and management to maximise your protection



Industry-specific expertise that elevates your cyber security to the next level

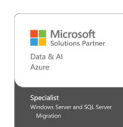
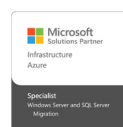
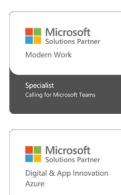
## Managed Detection and Response Features

What It Does	Why This Matters	What It Means
True 24x7 service managed by security professionals working from a UK onshore SOC.	Being able to see and respond to a cyber incident as it happens greatly reduces the potential damage it can cause.	Complete oversight and analysis so all threats are identified and remediated.
Full incident analysis with actionable remediation guidance.	Alert investigation is time consuming and requires the necessary expertise to truly understand.	Concise contextualised prioritisation of threats and relevant communications based on business asset classification.
Regular review and recommendations of security insights.	As attacks become more complex and multi-staged, it's difficult to make sense of the threats detected.	Board level security key performance indicators that allow your organisation to visualise the value generated from the service. Outcome-focused actions to improve your cyber security posture and combat against new threats.
Bridging the gap between IT operational teams and cyber security.	Provides the correct levels of insight and advice for IT operational teams to provide a secure and stable IT environment.	Ensures the correct levels of controls are in place to protect the needs of the business and assets.
Feature rich and fully integrated cyber security ecosystem.	Analysing interactions between users, devices, applications and locations ensures any hostile threat is seen and stopped.	Continuous assessment coupled with cyber security expertise gives you the who, what, how and when.
Ongoing cyber security trend analysis.	As your digital estate changes and threat actors adapt their tools and tactics, regular trend reviews provide insight into what is changing and how that can impact your environment.	Our cyber security experts will be able to advise on how attacks are changing and how your defences should adapt to provide the necessary levels of protection.

## Introducing Microsoft Defender for Endpoint

- ✔ **Cloud-powered.** No additional deployment or infrastructure. No delays or update compatibility issues. Always up-to-date.
- ✔ **Unparalleled optics.** Built into Windows 10 for deeper insights of kernel and memory level attacks. Signals and blocks are shared across Microsoft security products to apply protection and orchestrate remediation automatically.
- ✔ **Threat hunting over rich data.** Six months of historical data and real-time search to hunt across all your raw data for all monitored endpoints.
- ✔ **Automated security.** Take your security to a new level by letting automation investigate alerts and remediate threats from machines, in minutes – at scale.
- ✔ **Risk-based vulnerability management.** Reduce risk in your organisation with real time discovery, smart prioritisation, and integrated remediation of vulnerabilities and misconfigurations.
- ✔ **Flexibility through APIs.** Rich set of APIs providing flexibility to integrate with your existing security solutions and to enrich your own data with Microsoft Defender for Endpoint data.

**Our  
Credentials:**



To learn more about Managed Detection and Response visit [hub.6dg.co.uk/schedule-call-managed-detection-response](https://hub.6dg.co.uk/schedule-call-managed-detection-response)