

MDR for Microsoft

DATASHEET

An innovative and powerful Managed Detection and Response (MDR) service that leverages your Microsoft investment to its full potential.

Cyber-attacks continue to increase in frequency and sophistication, causing greater risk, uncertainty, and harm to organisations in industries around the world. To combat these threats most organisations have employed multiple security vendors over time. This has led to security gaps, alert fatigue, inconsistent policies and most importantly increased budgets and staffing overheads to manage these tools.

Many organisations are looking to consolidate tooling and simplify operations with the Microsoft Security suite but lack the expertise to deploy and operate Microsoft's technology. They need the help of a highly experienced, multi-disciplinary MDR service to realise the potential of their choice and deliver on their security promises. With Adarma, that's what you get.

ADARMA MDR

Built on the Microsoft XDR suite and integrated into the Adarma Threat Management Platform, our experts identify, investigate, and respond to cyber threats, mitigating risk to your business. MDR is designed to be easy and quick to adopt and give immediate access to Adarma's expertise in security operations delivering the outcome of a unified and powerful response to threat.

MDR DELIVERS OUTCOMES



Confidence in performance:

Get complete details of your high-fidelity detection and response outcomes with transparent case management, customisable incident notifications and response actions.



Fast time to value:

Easy to deploy and delivers value within 24 hours. Enjoy a fully optimised Microsoft Defender technology stack backed by The Adarma Threat Management Platform.



Access to expert staff:

Fully staffed modern security operation available 24/7 365 days a year. Get the benefit of decades of experience and tradecraft, on demand.



Instant access to advanced capabilities:

Boost your defence with immediate maturity acceleration through integrated threat intelligence, human threat hunting and elite response capabilities.



Clear outcome-based reporting:

Transparent reporting aligned to your business risk reduction objectives. Measure our performance against your metrics..



Support your business change:

Our service allows flexible coverage and scope to support business growth.



Confidence in the future:

This powerful service stays relevant to the evolution of your technology and the threats you face. Have confidence that whatever the world throws at you, together we've got this.

Supporting your Security Journey

Adarma offers two tiers of MDR to suit your changing security needs.

While our MDR Standard is comprehensive, offering the features listed above, our MDR Premium provides advanced 24/7 monitoring, investigation, and response services based in the UK, covering Server, Cloud, SharePoint, Teams, Network, and Enterprise Apps in addition to Email, Web, Endpoint and Identity.

What sets our MDR Premium apart from many other MDR services is the inclusion of Socket Analytics, our proprietary Security Information and Event Management (SIEM) solution.

Key Features

Threat coverage for things that matter.

Threat coverage for use cases across on-prem and cloud, covering:

- Identity & AD
- Documents and data
- Endpoints
- Enterprise Applications
- Network
- Cloud, IaaS, SaaS, PaaS
- Email and web

Expert threat monitoring

Continuous monitoring, triage and investigation of an unlimited number of security alerts. 24x7, 365 days a year.

Expert threat hunting

Hypothesis directed, and intelligence enabled threat hunting, Check activity, progress and results live through the portal.

Expert threat intelligence

Actionable intelligence powers our detection development, hunting, and investigations, it ensures our service stays relevant, and powerful in response to the threats you face.

Expert case investigation

Threat activity is quickly identified and validated by experts using our context-rich investigation capability. Track and interact with cases in the portal.

Adarma Threat Management Platform

Powerful integration, orchestration and automation capabilities drive increased speed and accuracy of investigation, hunting, and response actions. It delivers granular visibility and confidence in service performance.

Expert Incident Response

Rapid, effective, and proportionate response 24x7. Preauthorise, plan, interact and track response activity via the portal.

Integrated help on demand

Benefit from immediate transfer to DFIR, and access to security leadership and support on demand. Adarma can manage threat from start to finish.

We are Adarma

We are Adarma, independent leaders in detection and response services. We specialise in designing, building and managing cybersecurity operations that deliver a measurable reduction in business risk. We are on a mission to make cyber resilience a reality for organisations around the world.

Our team of passionate cyber defenders work hand in hand with you to mitigate risk and maximise the value of your cybersecurity investments. Powered by the Adarma Threat Management Platform and optimised to your individual needs, we deliver an integrated set of services that improve your security posture, including best-in-class Managed Detection and Response.

We operate with transparency and visibility across today's hybrid-SOC environments to protect your business as you transform, innovate, and grow. Adarma delivers the cybersecurity outcomes you need to make a remarkable difference.

How to Engage

For more details, discuss your needs with Adarma Client Director or email hello@adarma.com