CYBERFORT

MDR. It's not a trend, it's a revolution...

... and it's about to be cybersecurity's worst kept secret.

CYBERFORT

By 2025, 50% of organisations will be on board with Managed Detection and Response (MDR).

With numbers like that MDR isn't just a trend in cybersecurity – it's a revolution in how businesses protect themselves.

What is MDR?

Delivered and overseen remotely by specialist cybersecurity teams, MDR offers organisations cloud-based Security Operations Centre (SOC) capabilities that combine the latest analytic technologies, threat intelligence methodologies and incident response tools.

It allows businesses to leverage an external team of specialists to expand their security capacity, capability and firepower – all while maximising scalability and reducing spend.

MDR is a simple answer to today's complex challenges.
And Cyberfort MDR is the smarter way to build an enterprise-level security function.

CYBERFORT

Who is MDR for?

It's a fast-changing world out there, and organisations globally – from established sector-leaders to fast-growing start-ups – are asking big questions of their cybersecurity teams.

HOW CAN WE?

Strengthen our security posture?

Stay ahead of sophisticated, cloud-smart threats?

Simplify spend, reduce white noise and overwhelm from threat alerts, and manage the increased exposure caused by an exponential rise in remote working?

The answers don't always come easily.

Maybe you've already made some key security decisions for your organisation. Maybe you've even committed to some hires and invested in some kit. Or maybe you're struggling to find answers to some of the big questions you're being asked.

WE BUILT CYBERFORT MDR TO ANSWER THOSE QUESTIONS.

CYBERFORT

Capacity. Capability. Firepower.
Why sector-leaders and industry heavyweights are choosing MDR

Cyberfort MDR is a hard-hitting, class-leading suite of frontline cybersecurity services that protects the technology you use, manage and develop.

While an in-house centralised security unit monitoring and managing threats sounds great on paper, it's a huge challenge to run a SOC well, and often means round-the-clock hassle, spiralling costs, and resourcing and recruitment challenges.

That's why businesses are turning to MDR to bring in the firepower, the tools and the expertise they need to stay ahead in a fast-evolving threat landscape.

Monitoring:
Always on, always watching

24/7 monitoring, 365 days a year. Cyberfort MDR logs event data and contextual information, allows you to view real-time intelligence on incidents, and utilises smart software to cut the white noise from event reporting.

Proactive advanced monitoring spots and defuses potential problem areas before a threat even occurs. And it’s not just the tech that’s always watching – MDR is managed by one of the best security teams on the planet.

Revolutionary

CYBERFORT

Detection:
If it’s there, we’ll catch it.

MDR offers access to a game-changing security software suite. We partnered with sector leaders Elastic to build MDR on the world’s most powerful data analytics platform for search-powered solutions.

Cyberfort MDR looks deeper, and our class-leading multi-vector threat detection means that if it’s there, we’ll catch it – however well it thinks it’s hidden.

Response:
Faster, smarter & harder hitting

MDR uses best-in-class response tools to offer proactive, full-service rapid incident response.

Intelligent software and machine learning help identify and categorise risks, correctly target incident responses and drive your system’s improvement roadmap.

And our team is on hand to give tailored incident response support and guidance.

We’ve got you covered

CYBERFORT

Financial & operational streamlining: Do more for less

Eliminate costly SOC set-up, maintenance and upgrading requirements, and replace unwieldly, eye-wateringly expensive in-house systems with an agile, scalable cloud-based alternative.

No more system management.

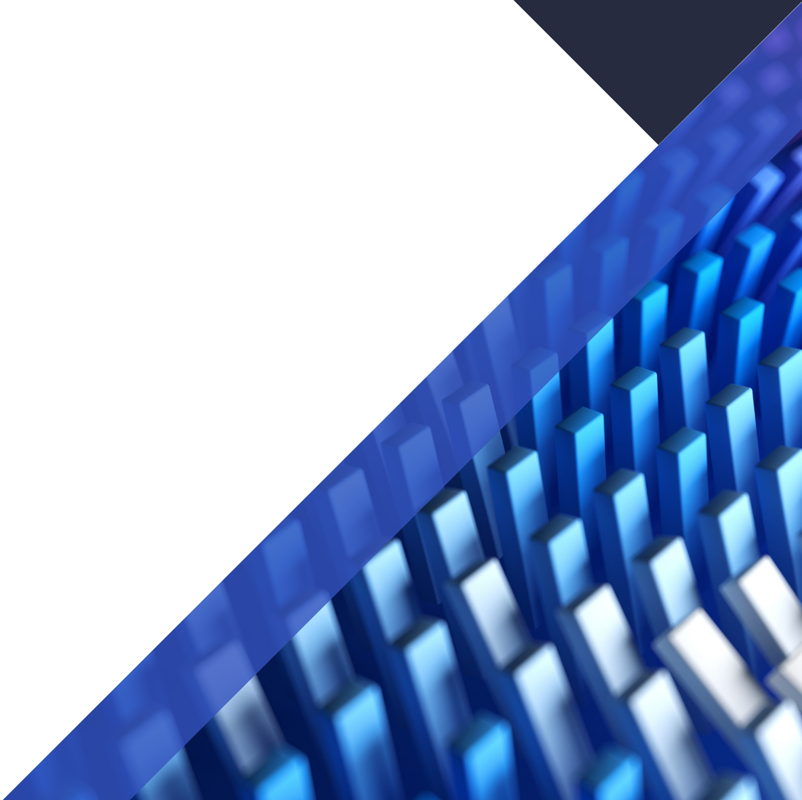
No more second-guessing strategic cybersecurity decisions.

No more alert fatigue.

MDR means automatic upgrades to the latest threat intelligence and advanced analytics, instant scalability, lower costs, streamlined service delivery and expert management. MDR means more time to get on with doing what you do best.

CYBERFORT

What about SOC?



Owning & operating a SOC

Spiralling costs, operational challenges & joining the battle for talent...

The alternative to MDR is owning and running your own SOC, with in-house systems, processes and teams. Owning and operating and SOC may sound appealing, but it has the potential to present significant, far-reaching operational and financial challenges.

At worst, attempting to establish and maintain your SOC can be a real distraction from fighting threats. Your SOC will make huge demands on your people’s time, present resourcing and management burdens, and may fail to deliver the firepower and agility that you need in today’s threat landscape.

Let’s take a closer look.

CYBERFORT

CYBERFORT

Challenges for in-house SOCs

Securing buy-in

An in-house SOC is essentially a cost centre with no financial return or revenue generating capabilities. As such, securing C-Suite buy in can be a major challenge.

While cybersecurity represents a vital business function, this resistance isn't as surprising as you might think – the cost of building and maintaining a 24/7 SOC can easily run to millions of pounds a year.

Attracting, recruiting and retaining talent

A SOC can't be run by your IT department. You need dedicated, qualified, highly skilled security analysts who can look beyond the standard preventative controls and face sophisticated and emerging threats head on.

That talent is in high demand – so it isn't easy to find, and it doesn't come cheap.

Staying flexible & scalable

In-house SOCs require ongoing upgrades to run efficiently, and to stay effective. That means constant monitoring, analysis and optimisation of systems – and that means more capital investment. Costs around upgrading can be particularly unpredictable and prone to spiralling.

Getting the stack right, maintaining the system and staying ahead is a huge challenge for SOCs.

Managing & finetuning the SOC

The right tech isn't enough – a SOC needs strong management to stay effective.

That means understanding and identifying risks, targeting incident responses and overseeing your system's improvement roadmap. It means tuning the system constantly to optimise performance. And it means understanding what the data is telling you, amidst a sea of white noise.

Strategic vision & operational ability

Pivoting strategically with an unwieldy in-house SOC can be sluggish, and your business can suffer as a result. Consider the exponential rise in remote working because of the pandemic, and the sudden need to maintain a strong organisational security posture across a dispersed team.

Whatever your business faces, your SOC will need to provide the security that will support it.

What if we've already committed to a SOC?

While stakeholders will always scrutinise the cost of security programmes, it's impossible to quantify how much you save by preventing a malware attack or phishing campaign.

Ultimately, it's essential to get the big decisions around security right – and to get the best service possible for your spend – even if that means walking away from the wrong investments after you've made them.

There's a huge and mounting body of evidence around the financial and operational benefits of MDR over a SOC. And there's a reason why 50% of organisations will have moved to MDR by 2025.

Our expert team have a wealth of experience in helping leading businesses transition from SOC to MDR. We'd love to help you make that move too.

CYBERFORT

MDR vs SOC

MDR vs SOC: A summary

System management

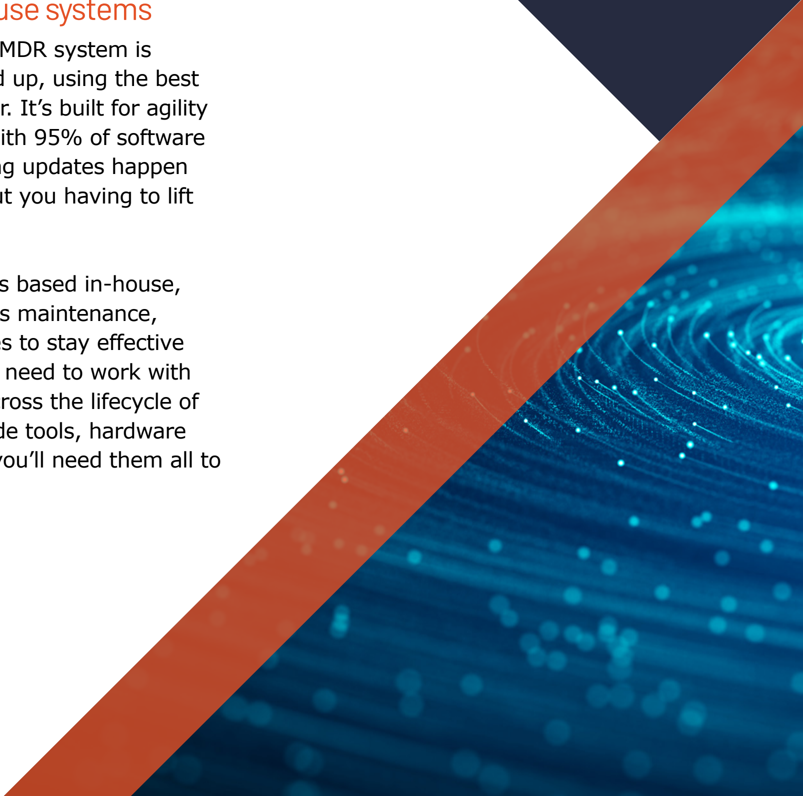
MDR – Your system is managed by Cyberfort’s world-leading team of cybersecurity experts and threat finders. We operate as an extension of your in-house team, overseeing the system’s maintenance and functionality day-to-day, and providing tailored, event-specific support or guidance wherever needed.

SOC – Your system is managed by your in-house team. That means hiring, retaining, upskilling and managing the right talent – experts who are in high demand in an employee’s market.

Remote vs in-house systems

MDR – Your remote MDR system is built from the ground up, using the best software in the sector. It’s built for agility and for integration with 95% of software and systems. Ongoing updates happen automatically, without you having to lift a finger.

SOC – Your system is based in-house, and needs continuous maintenance, patches and upgrades to stay effective and compliant. You’ll need to work with multiple providers across the lifecycle of the system to upgrade tools, hardware and software – and you’ll need them all to integrate seamlessly.



Financial commitment

MDR – With Cyberfort MDR, you'll pay for what you use. It's a simple, predictable opex model. No eye-watering set-up costs. No big board approval needed for million-pound budgets.

SOC – There is always real potential for the costs around a SOC to spiral – they often run to millions of pounds. SOC requires a huge up-front investment, and significant ongoing costs from software and hardware updates, recruitment and training of security analysts and more.

Updates and maintenance

MDR – We handle the day-to-day security management, leaving you and your team more time to get on with doing what you do best. We bring 35 years' combined experience of managing security operations and staying ahead of threats.

SOC – A SOC requires strong management to run efficiently and effectively. You'll manage that burden, and you'll need to constantly monitor and optimise your security centre to keep it up to date and to keep your technology secure.

Time commitment

MDR – We handle the day-to-day security management, and your remote system takes care of a lot of the heavy lifting automatically. You and your team have more time to get on with doing what you do best.

SOC – You'll need specialist security analysts and system managers, and they'll need the time and space to manually manage your system. That means everything from sifting through endless threat-alert white noise, to managing complex, multi-vendor system updates and patching.

Breadth of threat monitoring

MDR – 24/7, 365 days a year, your system is watching every possible breach point and every interaction, monitoring for any threat – from malware and ransomware to account privilege escalation, mass file encryption, brute-forcing… the list goes on. If it's happening, we'll see it and respond.

SOC – The range of threats your system is – or isn't – watching for, the possible breach points it is watching and how well it responds can vary massively, depending on your system's spec, maintenance and management.

CYBERFORT

MDR vs SOC: A summary

Why Cyberfort MDR?

24/7 remote threat monitoring. Intelligent detection. Rapid response.

CYBERFORT

Your new frontline

Cyberfort MDR provides your business with a new frontline – a hard-hitting, world-class cybersecurity team overseeing a best-in-class software suite that monitors your networks, proactively identifies threats, and responds fast if there ever is a breach.

Every possible breach point.

Every interaction.

All day, every day.

CYBERFORT

Do more for less

Outsourcing your detection and response functions to MDR allows you to leverage our world-class team to expand your security capacity, capability and firepower – all while maximising scalability and reducing spend.

A simple answer to complex challenges.

The smarter way to build an enterprise-level security function.

CYBERFORT

The right tools, the right team

Our class-leading tools are built on the world's best threat detection software. MDR offers cutting-edge machine learning and real-time incident reporting and response – and our expert team to oversee your remote SOC capabilities.

You get on with doing what you do best – **we've got you covered.**

CYBERFORT

Contact us now

MDR isn't just a trend in cybersecurity – it's a revolution in how businesses protect themselves.

Our team would love to talk to you about moving to Cyberfort MDR, and how we can give you the tools and support you need to stay ahead in a fast-changing world.

Ash Radar Station
Marshborough Road
Sandwich
Kent
CT13 0PL

E: info@cyberfortgroup.com
T: 01304 814800