Cyberfort
Expert-led. Security Driven.

Managed Extended Detection & Response (MXDR)

SERVICE OVERVIEW

Defend your organisations networks, systems and people 24x7x365, with an MXDR service aligned to your organisations unique risks

Introduction

Cyberfort Managed Extended Detection and Response (Managed XDR) delivers an uplift in customers cyber defences, visibility and awareness. The platform integrates our cyber expertise with a suite of security products that can actively and efficiently detect, analyse, and respond to threats.

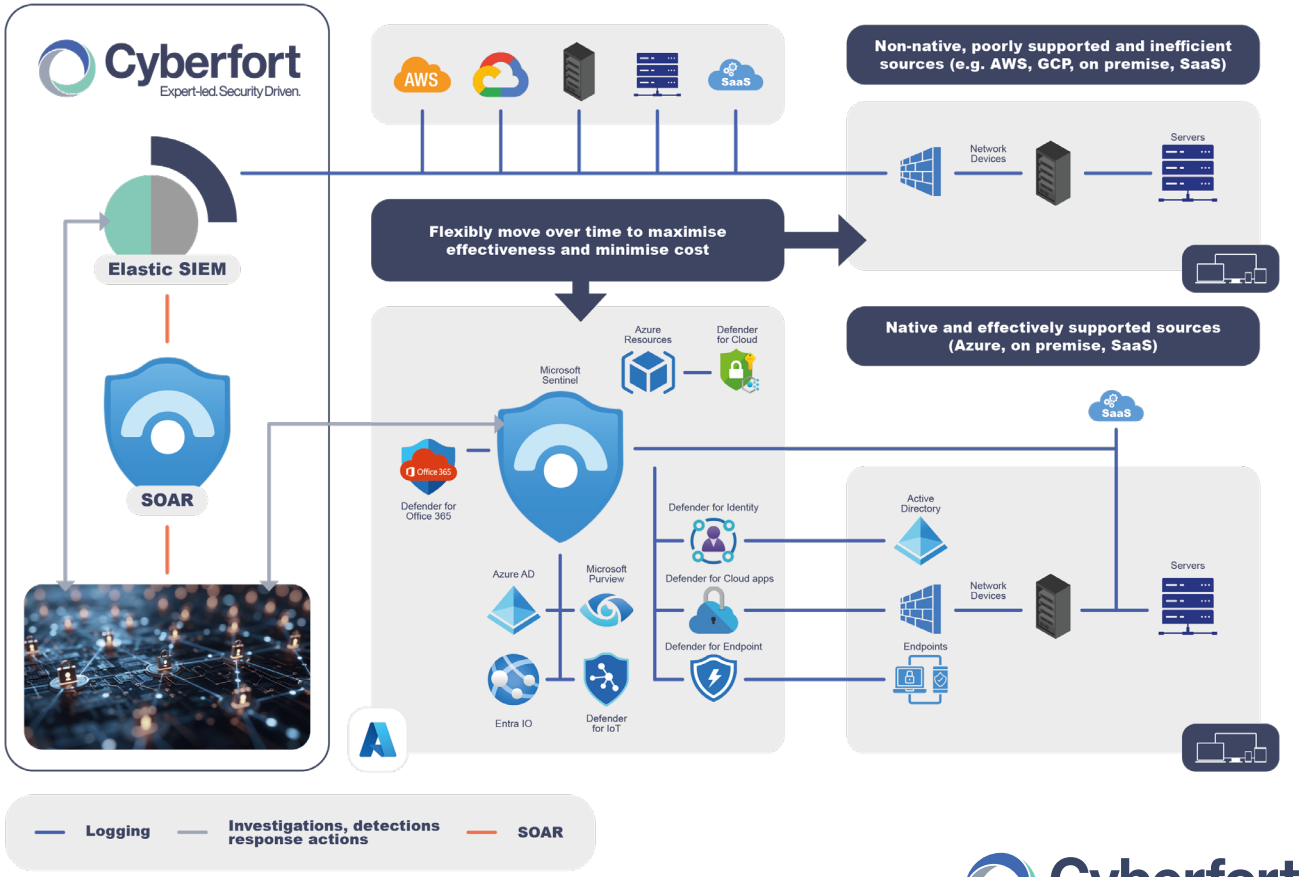
Cyberfort Managed XDR provides organisations with a strategic advantage over attackers which enables cyber security leaders to focus on core business activities while our experts concentrate on defending against cyber-attacks. By consolidating security operations into a single, expertly managed solution, our customers can not only improve their security posture but also enjoy operational efficiencies, cost savings, and reduce the burden of compliance and regulatory requirements. As cyber threats continue to evolve in complexity and severity, the adoption of managed XDR services is becoming an imperative component of a modern business's cyber security strategy.

> ***Your active responses contained a ransomware attack at 11pm on a Friday night, the impact was one machine on Monday morning, instead of our whole business.***

MXDR Service Overview

Cyberfort work with cyber security leaders to maximise their organisation's security defences. Leveraging both your internal and external visibility and controls to increase your awareness, visibility, and risk mitigation. Our MXDR Service delivers a 24/7/365 monitoring service with a team of analysts and engineers who can detect, investigate, notify, and respond to incidents and potential threats. Our service enables improved compliance and reporting, accelerating your security maturity, defending your business and delivering actionable insights into the maturity, exposure, risks and required mitigations.

How MXDR works at Cyberfort



Cyberfort
Expert-led. Security Driven.

Our MXDR Solution includes the following features to meet your organisations cyber security requirements

By using the latest technology and industry best practices the MXDR service provides enterprise level threat detection and response

Work globally with customers to deliver monitoring, analytics and streamlined incident response aligned to your business risks through SOAR workflows and SIEM deployments and leverage pattern matching and/ or AI monitoring capabilities

Provide a series of dashboards and access levels to ensure that the appropriate data views, investigations, responses, governance and required cyber situational awareness visibilities are available to the correct individuals within customers.

Agreed SLA's and KPI's with customers which enable cyber security teams to define business outcomes and clearly demonstrate the improvements in their risk posture.

Develop the necessary parsing rules to ingest clean data into the SIEM to provide actionable insights.

Identify and report on data sources that contain PII and could be in breach of GDPR and/or other internal data privacy and data protection regulations.

Work collaboratively with customers and the portfolio companies to identify mission critical data sources. We then use this knowledge to monitor, defend and prioritise your key assets.

Provide enhanced reporting allowing for streamlined management decision making, including KPI's evidencing continuous improvement and highlight any challenged and associated remediation mechanisms quickly.

Monitor, detect and respond to the latest vulnerabilities and evolving threats providing a co-ordinated response to all attacks, from random attacks to persistent well-funded organised attackers.

Utilising our expert analysts to enable rapid response times, reducing the attack surface. Providing enterprise level threat detection and response using the latest technology and industry best practices the MXDR industry

Cyberfort
Expert-led. Security Driven.

Cyberfort's Security Operations Centre comprises the following capabilities to enable the delivery of unified, modular integrated services

Security Information and Event Management (SIEM)

Provide threat detection, compliance and security incident management through collection and analysis (both near real time and historical) of security events.

Threat Intelligence

Threat Intelligence is used to enrich event data providing context against current known threats to aid threat detection and event management.

Experienced Analysts

Our highly skilled analysts will investigate all alerts to reduce false positive alarms so you can focus on your job.

Immediate Notifications

We'll alert you as soon as an incident is detected and verified.

Continual Monitoring

Continual monitoring of your estate with log and event collection and analysis to detect new indicators of compromise as they occur.

Storage Requirements

Configurable rolling storage to meet customer's needs, including compliance requirements.

Management Reporting

We will provide regular reports with key findings highlighting your cyber security posture.

Incident Management

Security incident management to identify, record, analyse and manage security threats or incidents. Our team will manage these incidents to closure working with your teams to deliver peace of mind.

Use Cases

Design, deliver and fine tune use cases to encapsulate detection and responses against specific threats.

Machine Learning (ML)

Machine learning enables threat analytics to automatically identify malicious activities.

Peace of Mind

We'll watch your estate while you run your business, allowing you to sleep soundly at night.

Endpoint Detect and Response (EDR)

Next Generation EDR agents deployed on your assets to protect and monitor for malicious activity (if required).

Compliance Monitoring

For compliance or regulatory requirement, where Security Monitoring is required, we are more than a tick box for you.

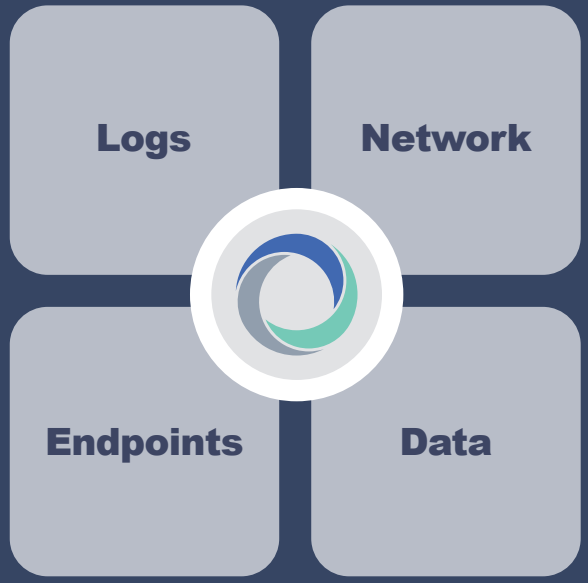
Dashboards

We will configure customised dashboards delivering a real-time view of vulnerabilities and threats.

Benefits & Outcomes

In an era where businesses of all sizes and sectors are challenged to improve efficiency, cost saving and productivity, distractions are something that must be avoided. While cyber-attacks continue to increase in volume and complexity, if they are not managed correctly they can become another distraction to your core business activities. All businesses require robust security defences to defend their assets. Cyberfort Managed XDR delivers a comprehensive security solution that extends beyond your traditional defences, delivering holistic visibility and active defence of endpoint, log, network, and data.

We develop a deep understanding of your business and its critical operations, focusing on your defences - integrating your existing security products, identifying and filling gaps with our innovative technologies, and applying our expertise and industry intelligence. We deliver a cohesive solution managed by seasoned experts, that continues to iterate and adapt as your organisation evolves.



Cyberfort
Expert-led. Security Driven.

Customer benefits of Cyberfort's MXDR

Cyberfort
Expert-led. Security Driven.

Operational Risk Reduction

24/7 Monitoring, analytics and Response

Continuous defences by security experts ensures that threats are identified and responded to at all times.

Advanced Threat Detection

With Cyberfort managed XDR, security teams benefit from a higher level of threat intelligence, leveraging global insight and your business context together with advanced analytics to identify complex, multi-vector threats earlier.

Increased detections

We combine known bad detections (fast and efficient), machine learning and AI (new, emerging, and iterating attacks) behavioural and anomaly (unknown and insider) with threat hunting (technique or indicator driven) to provide maximum coverage of threats as early as possible.

Streamlined Incident Response

Our integration of response capabilities within Cyberfort's managed XDR facilitates quicker and more coordinated incident response actions, mitigating the impact (and cost) of breaches.

Enhanced Security Posture

Managed XDR provides a holistic view of an organisation's security landscape, enabling the detection of threats across endpoints, networks, and cloud services.

> ***Cyberfort Managed XDR solution included industry leading EDR, meaning we didn't renew our standalone tooling, saving us over £100k of license renewals.***

Efficiencies and Cost Savings

Reduction of technical debt

By integrating multiple security functions into one solution, customers often reduce the overheads associated with managing disparate tooling. Where solutions are duplicated, or due for replacement, our Managed XDR solution will provide empirical data and expert input to deploy effective appropriate visibility and response.

Highly scalable human/AI collaborations

We utilise advanced automations, machine learning and AI to deliver an uplift in efficiency. Strict automation processes (when our analysts undertake a manual task 5 times, we automate it) combine with utilising machines to process and correlate vast amounts of data, meaning our human experts work at the grey area of "maybe" where their strengths are maximised.

False Positives are used for context but aren't raised to customers

Our expert analysts are complemented by sophisticated correlation algorithms decreasing the noise from false positives. We don't waste your time, while we collect information to enable detections from multiple low noise signals, we act on threats where appropriate and tell you quickly and efficiently about genuine threats, working with you to maximise the speed and efficiency of mitigations.

Access to Security Expertise

Access to 130+ cyber security professionals with extensive experience in managing complex threats provides insight and awareness into security strategy, planning and ensures maximum ROI from security investments.

Cyberfort aligns our Managed XDR service to your business processes

Traditional managed services operate the same service for all customers, we're different, we align to each business, and its risks without requiring expensive and time-consuming changes to your business operations and processes.

Reduced burden of regulation, compliance, statistics, and evidence

> ***We love your dashboards, our BI is always up to date, the compliance and exec reporting now takes us less than 20 minutes a month – and when we have a question, the team is always there on the end of the phone.***

Increased Business Performance

Increased customer confidence

For end users of your services or solutions, how you defend their personal data, financial transactions and any access to their system or environment is paramount – we provide empirical, continuous evidence of these defences.

Extended supply chain choices

With Cyberfort's managed XDR solution defending your entire business, organisations can potentially broaden their choice of available supply chain partners. While cyber posture and risk is important when choosing a supplier, often smaller suppliers can be more agile and cost effective, Cyberfort's MXDR mitigates cyber risk wherever it originates.

Productivity and focus

Our customers want to focus their resources on their core business goals, understanding and responding to cyber security where additional organisational governance or context is required. By using Cyberfort MXDR, your organisations staff are no longer distracted from achieving core business goals, or required to recruit and retain expensive and rare cyber experts as Cyberfort embeds this knowledge into your business.

Regulatory Compliance

Cyberfort Managed XDR solution enables compliance and the evidence of compliance with industry regulations by providing comprehensive logging, reporting, and data protection features.

Why Cyberfort are well-positioned to help you achieve your cyber security objectives

At Cyberfort we are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant. With over 20+ years' experience of designing, delivering and improving cyber security services for a range of customers, we believe we have the experience, knowledge, and tools to help cyber security leaders move forward with their defensive cyber security strategies. So why do customers choose us to deliver cyber security services for them?

Outcomes-driven

In the face of growing complexity, we make finding a cyber security provider easy. Our 20+ years experience in the cyber security industry combined with accreditations from major industry bodies including NCSC ensures we provide the outcomes and value you seek in a trusted cyber security partner.

Quality-delivery

We bring together a powerful combination of technology, domain experience, partnerships and industry knowledge to deliver real business and technology outcomes for our customers. Our focus on quality means we consistently work to help our customers realise their strategic cyber security goals.

Value-focused

Our 5 core values of Teamwork, Curiosity, Ownership, Agility and Innovation guide our behaviours in helping our customers overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

Cyberfort

Expert-led. Security Driven.

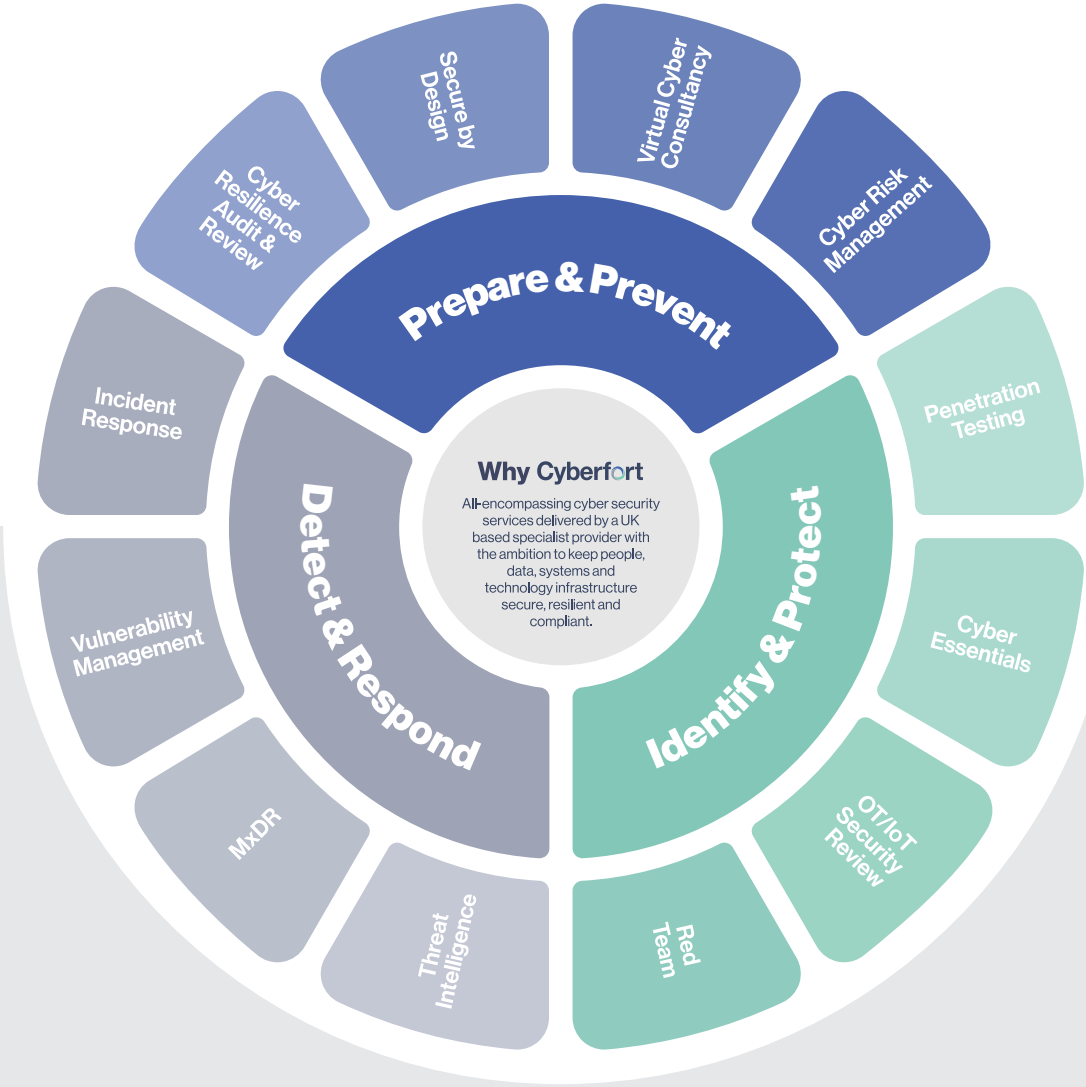
Discover more about Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks and proactive Detection and Response to security incidents through our 24/7 security operations centre.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort
Expert-led. Security Driven.



For more information on our Cyber Security services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you