G-Cloud 15
Service Definition

Aspire RealProtect Managed Cloud Security Services

Aspire Technology Solutions

Table of Contents

Introduction

Company Overview

Aspire Technology Solutions is an award-winning IT Managed Service Provider and Internet Service Provider. We deliver leading technology solutions across cloud, connectivity, telephony, technical support, cyber security, and professional services to help our customers drive real organisational benefits.

Our mission is to deliver technology like no other; we are dedicated to putting technology to work to help our customers innovate, become more efficient and grow quicker.

We have an extensive customer base across the UK including SMEs, public sector, and not-for-profit organisations as well as large enterprises and blue-chip organisations with a global presence. We provide services across multiple sectors, to a vastly diverse portfolio of organisations, which means our experience is well-rounded and our expertise is constantly tested to the highest levels.

We help our customers accelerate their ambitions through inspirational technology and to achieve this, we have a passion for delivering a sensational data-driven customer experience. To make sure we're on track, we measure our performance using the Net Promoter Score (NPS) global measure. In the past 12 months our score has averages +82 which is deemed 'world-class'.

At Aspire, we design and deliver innovative IT solutions that drive organisations forward. In a world that's changing faster than ever, we expect our customers to expect more from their technology.

Value Proposition

As a managed security service provider with extensive experience in providing both cyber and information security services, we understand the security challenges and requirements facing organisations. We believe that we are an extremely suitable IT security service partner who can provide the managed security services you require today, but we are also dedicated to working with you to provide the IT service flexibility to develop the way your services will be delivered in the future.

Our value is demonstrated through the technology journey on which we take our customers. At Aspire, our mission is to deliver technology like no other; we are dedicated to putting technology to work to help our customers innovate, become more efficient and grow quicker. Through our dedicated account management, we will form a deep understanding of your organisation, your challenges, and your opportunities. We then use our vast experience of technology and industry trends to develop a roadmap aligned to your organisational strategy to ensure that all services provide real value.

We will work hard to build a robust and mutually beneficial relationship with you, supporting your network, infrastructure, applications, and systems to maximise opportunities for growth. We are well-versed in providing innovative IT security solutions that work. We have designed a service that we know will enhance your cyber security and drive significant value, while minimising risk and striving to reduce cost wherever possible. As part of our commitment to you, we will assess your security technology spend, identifying and reducing any excessive areas and we will look to deliver improvements using these cost savings.

We believe Aspire have a unique proposition with our data-driven 24/7 dedicated Security Operations Centre (SOC), as well as our separate Network Operation Centre (NOC) helpdesk support offering. Our service delivery methodology, closely modelled on ITIL has been 10 years in the making; this incremental improvement with careful customer feedback at every stage along the way has led us to our current position with record positive feedback and over 99% SLA being met for over 12 consecutive months.

Our level of commitment to customer service is best illustrated by our high customer retention and fantastic Net Promotor Score (+83 which is deemed world class), we would be delighted to introduce you to customers who will verify our claims and explain in their own words, the value we add to their organisation.

Aspire are committed to delivering success to your organisation. With all of the above, we hope to make evident our dedication to working with you as your preferred technology partner.

What This Service Provides

Service Packages

Aspire RealProtect is our flagship managed security service- available in 2 different packages, our Managed Detection & Response (MDR) package and our Complete package. Our MDR package offers essential threat detection and response, ideal foundational 24/7 endpoint security monitoring. Our RealProtect Complete package offers elite level protection with comprehensive coverage across your endpoints, Microsoft 365 and perimeter firewalls.

The below table highlights the features and tooling available in both packages.

RealProtect Features	MDR	COMPLETE
24/7/365 In-House Security Operations Centre	✓	✓
Proactive Threat Hunting for Advanced Threats	✓	✓
EDR Tooling Powered by MS Defender or CrowdStrike	✓	✓
Incident Response (IR) Containment & Eradication	✓	✓
Aspire XIR Containment, Eradication & Extended Recovery	✗	✓
Sentinel Powered Managed SIEM & SOAR	✗	✓
Industry Leading Threat Intelligence	✗	✓
XDR/SIEM Integration For Microsoft 365 & Defender Suite	✗	✓
Detections for Firewalls & SaaS Services/Applications	✗	✓
RealProtect ASM Attack Surface Monitoring	✗	✓
Monthly Actionable Reporting	✗	✓

We also provide additional security services that can be included as part of your RealProtect contract:

- Penetration Testing (via. Punk Security)
- Phishing Simulations and Training (powered by uSecure)
- ISO27001 & Cyber Essentials

Overview of the G-Cloud Service

All Aspire RealProtect services are provided to the customer for as long as the contract remains in place, in accordance with Aspire's terms of conditions and Aspire's acceptable use, security and access policies and procedures.

As part of the service, during the initial onboarding stage, Aspire will agree with the customer, all nominated key contact stakeholders or parties where required, i.e., internal IT departments, or external MSP providers. This key contact list will then by treated as the default primary contact in the event of a security incident.

RealProtect: Managed Detection & Response

The table below details the key components of the RealProtect: Managed Detection & Response service.

Service Component	Description
Implementation & Onboarding	We will manage your organisation's onboarding including the deployment of Endpoint Detection & Response (EDR) tools required for the service on endpoints within your environment.
Maintenance	We will provide maintenance and updates of the tooling deployed as part of the RealProtect service.
Aspire SOC	We will provide 24/7/365 monitoring of endpoints, within scope, via our in-house Security Operations Centre, additionally we will respond to threats.
Threat Hunting	We will perform proactive measures to enable prevent opportunities for incidents to arise via. threat hunting using manual and machine-assisted techniques.
Incident Reporting & Recommendations	We will provide written reports of detections and incidents where threat actor activity is confirmed. Additionally, we will provide security recommendations following confirmed security incidents.
Incident Response	We provide Incident Response for an uncapped number of incidents across analysis, eradication, and containment workstreams. If the client fails to act on remediation actions or recommendations and is breached as a result, the subsequent IR work may be chargeable.
RealProtect Customer Portal	We will provide you access to the Aspire RealProtect Customer portal. As part of the RealProtect portal you will have access to the following: • The ability to raise a ticket for a security incident. • The ability to raise a ticket for a security request. • The ability to book an appointment with analysts from the Aspire SOC to raise any queries about the service. • The ability to view and respond to all security tickets in real-time.
Communication	We will establish direct communication channels to the SOC through email or via telephone in-line with our response action matrix detailed in the SLA section.

Billing	This service is a usage-based service, you will be billed against the total number of endpoints covered by the EDR tooling. It is the responsibility of the customer to ensure all endpoints are covered.
Information Security Compliance	The client is responsible for adhering to and maintaining information security compliance (such as ISO27001), including all necessary controls and policies, although Aspire will assist where possible; however, additional work may be chargeable.

RealProtect: Complete Managed Security

The table below details the key components of the RealProtect: Complete service.

Service Component	Description
Implementation & Onboarding	We will manage your organisation's onboarding including the deployment of Aspire's Extended Detection & Response (XDR) tools required for the service on endpoints within your environment.
Maintenance	We will provide maintenance and updates of tooling provided as part of the RealProtect service.
Aspire SOC	We will provide 24/7/365 monitoring of endpoints, within scope, via. our in-house Security Operations Centre, additionally we will respond to threats.
Threat Hunting	We will perform proactive measures to enable prevent opportunities for incidents to arise via. threat hunting using manual and machine-assisted techniques.
Incident Reporting & Recommendations	We will provide written reports of detections and incidents where threat actor activity is confirmed. Additionally, we will provide security recommendations following confirmed security incidents.
Incident Response	We provide Incident Response for an uncapped number of incidents across analysis, eradication, and containment workstreams. If the client fails to act on remediation actions or recommendations and is breached as a result, the subsequent IR work may be chargeable.
RealProtect Customer Portal	We will provide you access to the Aspire RealProtect Customer portal. As part of the RealProtect portal you will have access to the following: • The ability to raise a ticket for a security incident. • The ability to raise a ticket for a security request. • The ability to book an appointment with analysts from the Aspire SOC to raise any queries about the service. • The ability to view and respond to all security tickets in real-time.
Threat Intelligence	We utilise industry-leading threat intelligence from providers such as CrowdStrike & Microsoft, as well as open-source intelligence feeds, to identify, assess, and mitigate emerging cyber threats.
Gap Analysis & Security Hardening	We will provide an assessment of your current security posture to identify weaknesses & gaps in your defences. We will then provide recommendations and configuration changes to improve your security posture. For customers with a RealCare contract, we will implement these recommendations and configuration changes for you.
XDR & Managed SIEM	We will manage your organisation's Microsoft Sentinel instance and XDR platforms, including log collection, correlation, threat detection, and response.
Firewall Detections	We will monitor firewall logs for malicious detections.

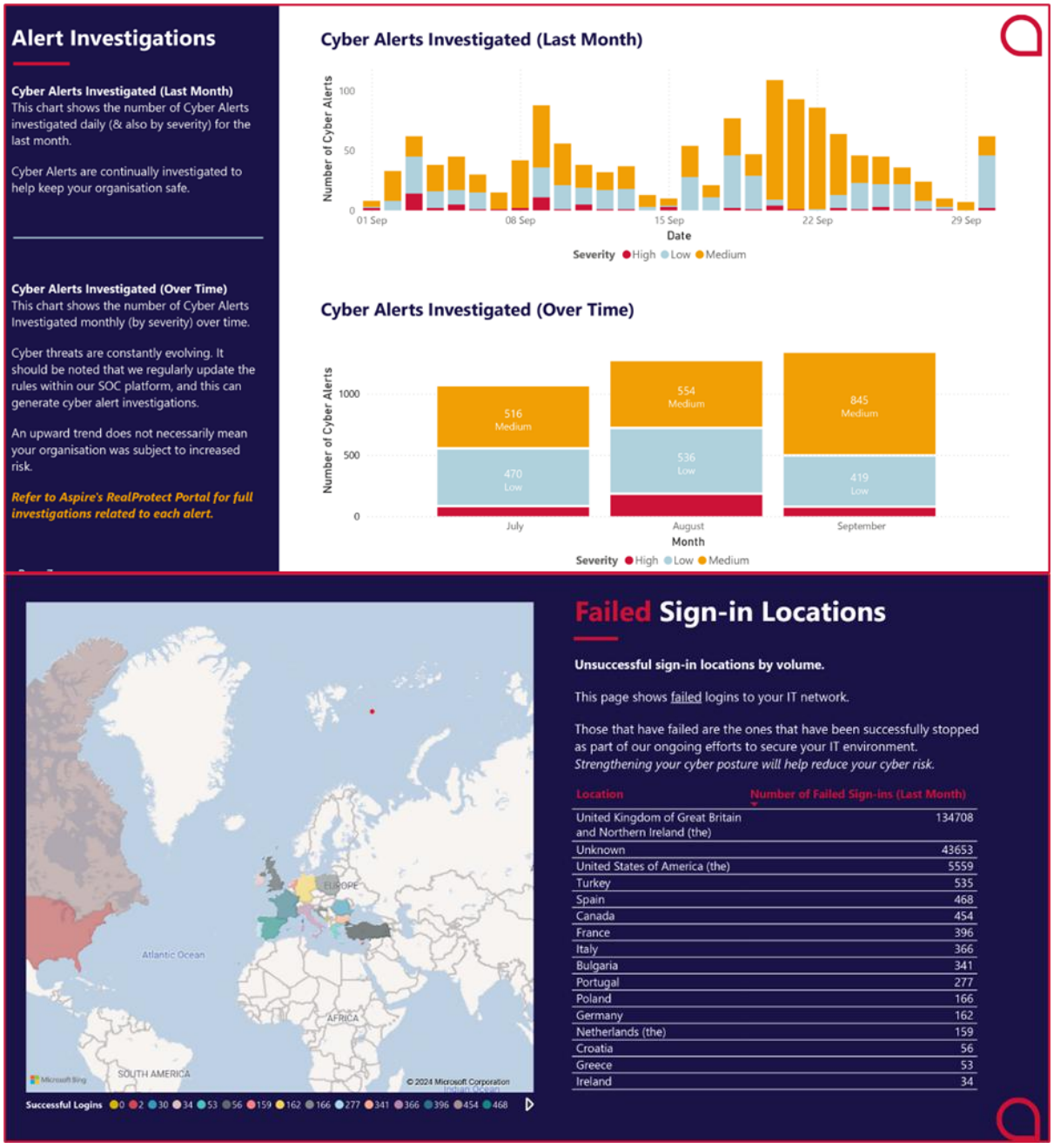
SOAR (Security Orchestration, Automation and Response)	Where possible, we will develop and manage automated security workflows and playbooks, to aid investigations and incident response.
RealProtect ASM	RealProtect ASM (Attack Surface Management, powered by Cybasm), provides you with continual attack surface monitoring for your organisation's external systems: • Monitors for leaked credentials. • Scans for DNS, websites & SSL issues. • Spots lookalike domains.
Monthly Reports	We will provide an executive monthly report, which details key service metrics as well as recommendations on your security posture.
Communication	We will establish direct communication channels to the SOC through email or via telephone in-line with our response action matrix detailed in the SLA section.
Billing	This service is a usage-based service, you will be billed against the total number of endpoints covered by the XDR/EDR tooling; SIEM ingestion is included within the cost of the service. It is the responsibility of the customer to ensure all endpoints are covered.
Information Security Compliance	The client is responsible for adhering to and maintaining information security compliance (such as ISO27001), including all necessary controls and policies, although Aspire will assist where possible; however, additional work may be chargeable.

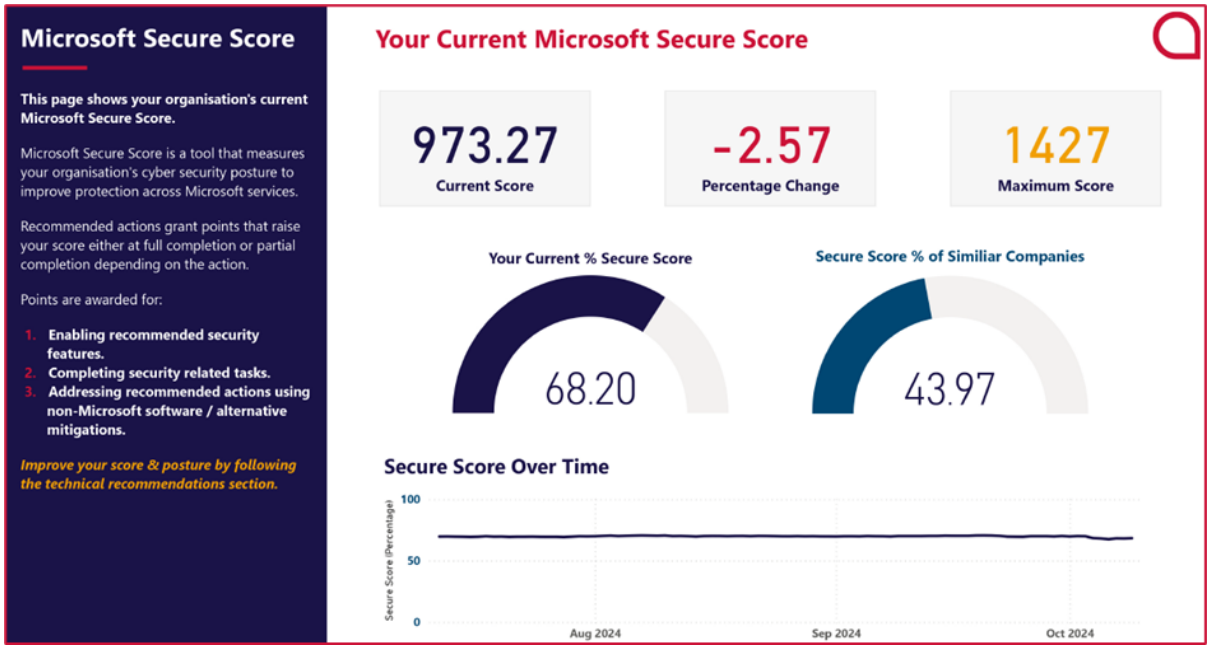
Where appropriate, we can deploy a virtual on-premises collector to ingest the following:

- Firewalls & VPN Syslog
- Advanced Server Logs
- SaaS Services & Applications
- Vulnerability Detections

Monthly Reporting (Complete)

As part of our RealProtect Complete service, Aspire will provide a comprehensive monthly SOC report, detailing recent alerts, most at-risk users, and recommendations to enhance overall security. The report also includes information on user access, such as successful and failed sign-ins, along with login locations, to help identify changing access trends, unusual usage patterns, and accounts accessing higher-than-average amounts of data.





The Monthly SOC report is a PDF board-level report which is provide as part of Service reviews by your Service Account Manager, this report includes trends and recommendations from the Aspire SOC, as well as reporting on the threats detected over the last month.

The Monthly SOC report provides insight in the following:

- Incident Summary – Exec summary, observed device counts
- Service Overview – time to triage, MTTR, 90-day trends
- Actionable Insights – At risk users, sign-ins/locations
- Local admins, users with admin access
- Downloads to untrusted devices, files shared externally
- Exchange admin activities and changes
- Login locations, machine types, OS versions
- Posture score, benchmarks with similar organisations
- Security recommendations: apps, devices, data and identity.
- Summary of security incidents. (Incident Report is also provided in the event of a security incident.)

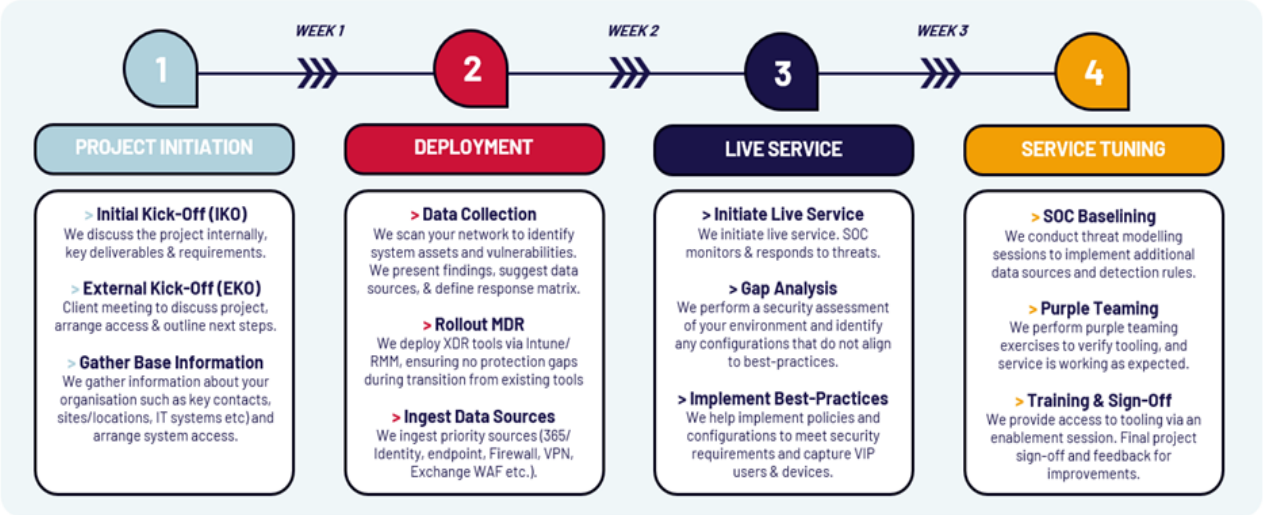
Service Initiation

Service Onboarding

The following is typically what will be included within the scope of the implementation project for our RealProtect service:

- Endpoint, Server & Device Control deployment
- Endpoint Prevention Policy configuration
- SIEM configuration and data ingestion

Our onboarding process typically takes between 2-3 weeks and is illustrated below:



Service Offboarding

We understand that the time may come where our RealProtect services are no longer suitable for your organisation. If you need to migrate away from Aspire, we will work closely with you and any 3rd parties to ensure that all tools and software deployed as part of the service are smoothly and seamlessly removed.

Service off-boarding can be initiated by formally liaising with your dedicated Service Deliver Manager and is included as part of the RealProtect service at no additional charge.

Service Description

Service Summary

RealProtect is Aspire's Managed Security product which delivers the following organisational and security outcomes:

- Next Gen antivirus and extended detection & response tools for endpoints (with Complete)
- Managed Detection & Response
- Pro-active incident detection, response and containment
- 24x7x365 service delivered from our entirely UK based SOC
- Proactive threat hunting with integrated threat intelligence
- Monthly executive reports and actionable insights (with Complete)
- Fully managed SIEM (With Complete)

Data Protection

Aspire is ISO9001 and ISO27001 accredited, as well as holding Cyber Essentials Plus. Aspire gathers and process personal information in accordance with our private notice and general terms and conditions. The RealProtect services full comply with the EU General Data Protection Regulation 2016/679 (GDPR) and national laws implementing GDPR and any legislation that replaces it in whole, or in part and any other legislation relating to the protection of personal data.

The customer will be liable for all the customer data that the customer creates from its use with Aspire RealProtect services. The customer represents and warrants that the customer owns all customer data created within the RealProtect service and that the customer has permission from the rightful owner for its use.

Aspire disclaims all liability relating to any customer data within the Aspire RealProtect Service, and for all liability relating to unauthorised use (by other users) of customer data.

Service Methodology & Mitre ATT&CK

Our RealProtect services follow a mature security methodology which enables us to effectively identify top threats to your organisation and adapt our services to your security posture.

As part of this methodology, the processes, and tools we use are based on the MITRE ATT&CK framework. In addition, the XDR tools that are deployed as part of our RealProtect services prevent breaches using a combination of prevention, detections, and contextual telemetry techniques, giving the Aspire SOC full-spectrum visibility whilst eliminating alert fatigue.

In the latest MITRE Engenuity ATT&CK evaluation program, our XDR tools that Aspire use as part of RealProtect achieved the following:

- 100% detection coverage across the intrusion stages by providing actionable alerts on each of the 20 steps of the evaluation and all MITRE ATT&CK tactics
- Prevented simulated intrusions against both threat actors at multiple steps across the MITRE ATT&CK framework
- Analysed relevant indicators of compromise and telemetry, pulling together weak signals to detect highly sophisticated and stealthy adversary tradecraft
- Prioritised and visualised the detected attacks with rich contexts such as ATT&CK tactics and techniques treat actor intelligence, devices, and users
- Produced results that were presented as actionable security incidents enriched with deep contextual telemetry – reducing discrete security alerts by 90% and dramatically speeding time-to-respond in a manner that no other supplier could match
- Provided comprehensive detection by design with visibility into attack behaviours from multiple vantage points, virtually eliminating adversary's ability to remain undetected.

Tools and Technology

Aspire's RealProtect MDR and Complete services are delivered through a single lightweight agent, which provides comprehensive endpoint security and visibility for all your workloads, including workstations, servers, cloud workloads, containers, and mobile devices.

With RealProtect, security tools are managed via the Aspire SOC, utilising EDR (If RealProtect MDR or Complete package) and Aspire's SIEM (Managed SIEM or Complete Packages) utilising industry leading cloud-based management platforms. These platforms can provide integration with 3rd party tools and products to give more context and visibility into attacker's behaviours and potentially malicious threats.

With endpoint security at its core, the EDR tools included with RealProtect combine endpoint protection leveraging cloud-scale AI and deep link analytics to deliver best-in-class XDR, next-gen AV and device control.

Depending on your current Microsoft Licensing, we can utilise Microsoft's EDR and SIEM capabilities via Defender for Endpoint & Sentinel, to provide our RealProtect Complete service, utilising your current Microsoft investment.

In this model, tooling and licencing is to be provided by the customer, with Aspire providing management, support and 24/7/365 detection & response via our Security Operations Centre.

Threat Intelligence

Aspire RealProtect services enables access to leading global Threat Intelligence systems, which provide the highest quality threat intelligence in the industry. This enables the Aspire SOC to not only track technical indicators, profile adversaries and closely monitor their campaigns, but also keep well informed about the cybersecurity implications of geopolitical changes.

Our EDRs all-source methodology examines every aspect of an adversary's profile, motivations, intentions and TTPs (Tactics, Techniques and Procedures), providing a full understanding of what the adversary is doing, why they're doing It and how we can stop them.

Some of the elements covered in our EDR's threat intelligence monitoring and analysis include:

- Tactics, Techniques and Procedures (TTPs)
- Indicators of Compromise
- Targeted Vertical and Geographies
- Detection/Prevention Logic
- Adversary Profiles and Goals

By examining all aspects of the treat landscape, from all available sources, the Threat Intelligence systems that Aspire utilise as part of the RealProtect service provide the full-picture perspective that our customers need to prevent and mitigate breaches.

Supporting Teams

Aspire RealProtect services are directly supporting by the following teams:

Product & Solutions:	With our dedicated Product and Pre-sales teams, we can guarantee you a key point of contact for pre-sales and information points, as well as future RealProtect product developments and updates.
Projects Team:	The Aspire Projects team is responsible for managing the on-boarding process for new customers. This includes collaborating and orchestrating with the supporting teams to ensure that your transition to Aspire services is seamless and pain-free.
Aspire Security Operations Centre (SOC):	Our in-house UK-based Cyber Security Operations Centre (SOC) consists of highly skilled Cyber Security Analysts. Our SOC runs 24/7/365 and delivers all of the cyber security services included with our RealProtect offering.
Aspire Service Desk:	If you have an active RealCARE contract, on your instruction our SOC will directly liaise with our Service Desk & Network Operation Centre (NOC). Providing a single point of contact for all support calls.
Customer Experience:	Our customer experience team are here to ensure everything runs smoothly and gives you a point of contact to provide us with valuable insight that will improve your tie with us.

Aspire Security Operations Centre (SOC)

All Aspire RealProtect services are delivered by our Security Operations Centre (SOC) based in our Gateshead HQ.

Our Security Operations Centre (SOC) is a dedicated team of cyber security specialists, who are ready to support your organisation. They can monitor and manage of your security infrastructure and fully manage any incidents that might occur.

Their main functions include:

> Monitoring and Detection
> Incident Response and Threat Hunting
> Threat Intelligence
> Detection Engineering

Incident Response and Containment

NIST Led Capability

In the event that a security alert is detected, the Aspire SOC will notify you of the threat and act as your incident coordinator, performing all actions and procedures to ensure that the security incident is contained.

NIST 'SP 800-6T' is the industry leading incident handling standard we utilise as part of our RealProtect services. Covering the full NIST incident Handling standard, we're able to detect incidents and handle them through to recovery and lessons learnt.

Preparation

As a Security Operations team, we adopt many methods to always assure that we're in a high state of readiness.

- Purple teaming exercises including breach & attack simulation
- Regulatory industry leading training (BTL1, SANS Institute, CompTIA, Cisco and more)
- Threat insights and research.

As part of your onboarding, we also collect key information to produce an incident readiness score and a roadmap to incident handling success, covering main areas such as:

- Key contact information
- Port and services list
- Network information and diagrams
- 3rd party suppliers
- Any other relevant information

Detection & Analysis

Aspire's SOC team consists of analysts with expertise in different key areas of the cyber domain i.e., Security Engineering, Threat Intelligence, Ransomware/BEC recovery.

We have partnered with leading vendors as our XDR and SIEM providers of choice, both 'top- right' Gartner magic quadrant products. These two products give us unprecedented insight into hosts, network devices and context otherwise unavailable.

All our detections and investigations are aligned to the industry leading MITRE ATT&CK Framework.

In-house, we have a geo-resilient 24x7 Digital Forensics platform, hosted across our very own ISO27001 accredited, private datacentres. This platform enables many key capabilities such as threat research, traditional digital forensics investigations, malware analysis and network forensics.

We're able to ingest gigabytes of data from remote locations within seconds, we have also crafted automation and orchestration technologies to enable us to parse and interpret data that might expose threat actor activity immediately, giving us valuable minutes back to getting your organisation back to 100% operations.

Detection of incidents is a reactive mindset, at Aspire we embed proactive methodologies and practices into our service offering to enable preventative opportunities for an incident arising, such as:

- Proactive threat hunting & research

- Malware research
- Development of SIEM rules to detect the latest threats

Containment, Eradication, and Recovery

Our incident response capability has been built with key principles in mind:

- Limiting further impact to the confidentiality, integrity and availability of your organisational and customer data
- Preventing further damage to your organisation as a result of a cyber security incident
- Limiting the impact of reputational damage to your organisation

We determine a containment strategy based on your organisation and your requirements, considering the following:

- Need for evidence preservation
- Service availability (Network connectivity, services provided to external parties and customers)
- Effectiveness of the strategy itself (partial or full containment)
- Time and resources required from both us and you
- Duration of the solution (Emergency work around to be removed within 4 hours, temporary workaround to be removed within two weeks, or permanent)

Utilising our EXDR, if any suspicious activity is detected, we're able to remotely quarantine your devices with immediate effect. We have a proven methodology in-house which is based on intent. We investigate anything suspicious and eradicate anything with malicious intent. As a team, we work to transparent and swift SLA's, ensuring that nobody in your organisation is out of play for longer than a few minutes.

We have a team experienced with ransomware and Corporate Email Compromise recovery, should any infrastructure require further isolation and 'deep cleaning/recovery', we also have experts on hand to develop a recovery strategy that works within your organisation's requirements and budget.

Incident co-ordination is critical, our incidents are handled in an agile working fashion. We use Kanban boards to track and report granular progress on key items leading to your organisation's recovery. Our incident response playbooks are also developed with an Agile mindset, allowing actions to be embedded into the Kanban workflow.
As part of our co-ordination offering, we have designated experts within the SOC tasked to engage with industry partners such as law firms, law enforcement, other incident response teams and other businesses in the field. From the beginning of an incident, you, as a customer will be informed of the co-ordination strategy, information sharing agreements and we will gather your reporting requirements.

Extended Incident Response (xIR)

As part of your RealProtect contract, we include Extended Incident Response alongside the unlimited Containment, Eradication and Recovery of cyber incidents.

Aspire XIR goes beyond traditional incident response, we provide extended recovery-delivering end-to-end remediation through specialists across security, IT, cloud, and communications. Our cloud recovery platform also enables rapid restoration with minimal downtime.

XIR Team

The following are the relevant teams who are engaged during incident and post incident recovery and remediation.

IR & SOC – Our IR team and Security Operation Centre are on hand to perform digital forensics and assist in the investigation.

Cloud & Business Continuity – Assist in cloud backup restoration and ensure data integrity after an incident.

Infrastructure – Support by taking containment remediation actions like disabling compromised accounts, servers and endpoints.

Networks – Contain & mitigates threats by blocking malicious IPs, domains or specific network traffic before reconfiguring network infrastructure post-incident.

Post-Incident Activity

Lessons Learnt

Our lessons learnt sessions are delivered by the expert assigned to customer engagement, ensuring a familiar face that has also dealt with the incident from the first stages. Lessons learnt are delivered in an agile fashion, reviewing the actions timeline, noting positive and negative outcomes, as well as a review of the implemented containment/eradication/recovery strategies based on tailored metrics.

Collected Incident Data

Aligned to the NIST standard, we perform both an objective and subjective assessment of every incident, no matter the size or criticality. We base our objective assessments on:

- Determining if the incident caused damage before detection
- Determining if the root cause was identified
- Determining if the incident is a recurrence of a previous incident
- Calculating the estimated monetary damage from the incident (Information and critical corporate processes negatively impacted)
- Identifying which measures, if any, could have prevented the incident
- A review of incident metrics gathered throughout the incident lifecycle

A subjective assessment is performed based on both our team's self-assessment procedure and gathering any feedback from you as the customer.

Reporting and Recommendations

At the end of the process, in line with your reporting requirements, we produce a final report of a chosen format and delivery.

We aim to describe all steps taken by the threat as well as actions taken by us as a collective (Aspire and you as the customer), provide insights into the risks that could be mitigated, as well as recommendations to mitigate on a tactical and strategic level.

As your cyber security partner, we're able to deliver a scope and implementation project for mitigations.

Service Availability

Measure	Definition	Value
Service Hours	The hours during which the service and Service Level Agreement is provided	24/7/365

Alert SLAs

Priority Level	Definition	Response Time*	Triage Time*
P1 - Critical	An alert where the activity is known to only be linked with malicious behaviour. Examples include the execution of known malicious software and tools such as Winpeas, Cobalt Strike and Mimikatz.	15 mins	30 mins
P2 - High	An alert where the activity is likely to be linked with malicious behaviour. Examples include matches on logs against IP addresses (or other indicators of compromise) with a bad reputation or the use of legitimate applications that are often used for malicious activities such as PowerShell.	30 mins	60 mins
P3 - Medium	An alert where the activity is typically followed by or leads to malicious behaviour. Examples include alerts such as successful non-UK logins followed by the creation of mailbox rules.	60 mins	120 mins
P4 - Low (& MACs)	An alert where the activity is evidence of a potential risk to the business. Examples include the use of legitimate remote access tools, which pose a potential risk but don't warrant immediate response.	4 Hrs	8 Hrs

Incident SLAs

Priority Level	Action Response Time

P1	30mins
P2	60mins
P3	120mins
P4/P5	240mins

We aim to initially contain all incidents within 15 minutes.

Immediate Response Actions

Once an incident is classified, the following actions are taken based on its priority:

Incident Priority	Response Actions
P1	• Immediate notification to the primary point of contact (POC) via telephone. • Email communications to all relevant stakeholders. • Establish a communication bridge using Teams or WhatsApp. • Create an action/decision log and a case tracker. • Initial containment of threat.
P2	• Immediate notification to the primary POC via telephone. • Email communications to all relevant stakeholders. • Establish a communication bridge. • Create an action/decision log and a case tracker. • Initial containment of threat.
P3	• Notify the primary POC via telephone. • Email communications to all relevant stakeholders. • Create an action/decision log and a case tracker. • Initial containment of threat.
P4	• Email communications to all relevant stakeholders. • Actions and decision tracker in the cyber incident ticket. • Initial containment of threat.
P5	• Email communications to all relevant stakeholders. • Actions a decision tracker in the cyber incident ticket. • Initial containment of threat.

Third Party Software

The customer may not and is not licensed to install or use software or technology in any way that would infringe any Third-Party Software Supplier's intellectual property, technology, or licencing usage rights.

Third Parties

Aspire shall not be liable in respect of any contract, agreement, or relationship that the customer may have with any third party. If a dispute arises between the customer and a third party involving RealProtect, Aspire shall provide, at the customer's expense, the customer with reasonable information and assistance to the extent that such is not averse to Aspire's interests to the Customer in the resolution of such dispute.

Additional/Alternative Services

Incident Response Retainer (IRR)

Aspire's Incident Response Retainer (IRR) service is a proactive service that helps organisations prepare for and respond to security incidents. This service provides access to a team of experienced incident responders who will aid with incident response planning and preparation.

Aspire's incident response retainer service is a valuable investment for organisations that want to be prepared for security incidents and minimise the impact of any incidents that do occur. By providing access to experienced incident responders, readiness assessments and planning services, this service can help organisations respond more quickly and effectively to security incidents, ultimately enabling organisations to maintain business continuity, as well as meet regulatory and compliance requirements.

Benefits of Aspire's Incident Response Retainer service include:

- Proactive assessment services.
- Access to a 24/7 incident response hotline.
- Initial response within 15minutes.
- Flexible and modular workstreams.
- Discounted workstream rates should an incident occur.

The following table outlines Aspire IRR's service inclusions.

Preparation	Incident Response Workstreams		XIR*
	Assess	Respond	
IR Plan Review/Development	Compromise Assessment	Containment & Eradication	Extended Incident Recovery
Gap Analysis & Recommendations	Cloud Security Assessment	Digital Forensics Investigation	Recovery Environment in ACS
Tabletop Exercises	Active Directory Security Assessment	Recovery	Physical DR Site
			Access to XIR Team

Aspire's Incident Response Retainer is available in 3 packages (tiers 1-3). The below table outlines the differences between each package.

	Tier 3	Tier 2	Tier 1
Availability	Available 24/7/365.	Available 24/7/365.	Available 24/7/365.
Remote Support SLA	Initial Incident Response within 15minutes.	Initial Incident Response within 15minutes.	Initial Incident response within 15minutes.
Hours Included	120 hours (excluding onboarding)	80 hours (excluding onboarding)	40 hours (excluding onboarding)
Unused Hours	50% of unused hours can be used on consultancy or engineer services.	50% of unused hours can be used on consultancy or engineer services.	50% of unused hours can be used on consultancy or engineer services.

Penetration Testing

Aspire have partnered with Punk Security to deliver CREST-accredited penetration testing. These tests are designed to improve your organisations cybersecurity posture by identifying and addressing vulnerabilities and weaknesses in your infrastructure before malicious actors can exploit them. In an era where digital threats evolve rapidly, proactive security measures are crucial to safeguarding sensitive data, maintaining regulatory compliance, and preserving business continuity.

By leveraging best-in-class tools and utilising industry frameworks, we ensure the highest quality and precision in our Penetration Testing Services. Moreover, our approach aligns with the Penetration Testing Execution Standard (PTES) framework, a globally recognised and respected set of guidelines. Following the PTES framework allows us to conduct ethical hacking in a systematic and organised manner, covering every aspect of your cyber-landscape.

Features/Advantages of Aspire Penetration Testing Services:

- Identify and address vulnerabilities early.
- Access security controls such as firewalls.
- Quantify risks based on potential impact and exploitation.
- Compliance validation.
- Protect your organisations reputation through successful penetration tests.
- Mitigate costly security breaches via. continuous guidance, advice and improvements.

Branches of Aspire's Penetration Testing Services

- External Penetration Testing
- Internal Penetration Testing
- Web Application Penetration Testing
- Active Directory Audit
- CI/CD Maturity
- Cloud Security Assessment
- DevSecOps Auditing
- Kubernetes Security Assessment
- Microsoft365 Entra Configuration Audit

Our Experience

Case Studies

J. Barbour & Sons Ltd is a British luxury and lifestyle brand founded by John Barbour in 1894, that designs, manufactures and markets waxed cotton outerwear, ready-to-wear, clothing, footwear and accessories. Founded in South Shields, England, as an importer of oil cloth, J. Barbour and Sons Ltd has become well known for its iconic waxed cotton jackets.

Barbour engaged with Aspire to provide planning, setup and migration, testing, training and ongoing support for a suite of cloud-based Managed Security Services including anti-virus, anti-ransomware, security exploitation protection and zero trust cloud security services.

As part of this project, Aspire was required to plan and fully setup the antivirus, anti-ransomware and security exploitation protection security services including providing the professional services to undertake quality assurance testing and training on the new cloud services as well as ongoing support.

Aspire also implemented a cloud backup and disaster recovery solution for Barbour that encompassed some 70 virtual machines and over 35TB's of data. We migrated Barbour away from traditional tape-based backups and onto our cloud-based backup and Disaster Recovery as a Service. Data is backed up and replicated and stored in our private cloud.

Aspire provided the licenses and initial planning for Barbour's Zero Trust cloud security service rollout. The setup covered 1,400 global devices in total. The solution provides device security that enables a "work from anywhere" environment without the risks associated when devices aren't connected to the Barbour network.

Triage provides skills and workplace training, as well as employability services that help people secure a job, progress in the workplace and build meaningful careers. Delivering from locations across Scotland and North East England, Triage works with local, regional and national stakeholders to deliver government-led initiatives in the skills and employability sector. We work in partnership with public, private and community organisations to deliver these employment, education and training programmes that respond to social and economic growth agendas.

Triage was in search of a partner who could provide third-party support and guidance in managing their security needs. The goal was to instill comfort and confidence in their end users, staff, and stakeholders, assuring them that Triage had taken the necessary measures to minimise the risks posed by cyber security threats. Various issues arose from a previous supplier including project delivery delays, pricing challenges, and a breakdown in communication due to a lack of proactive and meaningful engagement.

Their objective was to find a company that could offer reliable support and unwavering commitment to protecting their business.

Aspire was enlisted to offer 3rd-line IT support and to provide a comprehensive managed security service, which included enhanced vulnerability scanning. This service is managed through Aspire's 24/7 fully managed Security Operations Centre (SOC), utilising top-of-the-line MDR/EDR and SIEM tools. The onsite 24/7 team at Aspire not only reacts, responds, and contains threats but also proactively undertakes numerous tasks to prevent potential threats from materialising into actual risks.

The decision to choose Aspire was driven by our ability to offer comprehensive national coverage, expertise, resources, and state-of-the-art technology. Aspire not only met the immediate requirements but also demonstrated the capability to guide the customer on a long-term journey of growth and success. With Aspire's services and support, Triage effectively reassured its stakeholders that they had implemented appropriate measures to minimise business risk stemming from cyber threats.

Our Customers

Over 1,700 public and private sector customers are delivering citizen services and growing their organisations with us.

Contact Details

At Aspire, our mission is to deliver technology like no other. We have been helping customers to innovate, become more efficient and grow quicker through technology since 2006. Let us help you, too.

Talk to Sales
Interested in our products and solutions but not yet a customer? We'd love to hear from you. Here's how you can reach us.

- Email our Sales Team: hello@aspirets.com
- Call Us: 0330 124 2700
- Visit our website: www.aspirets.com