

Reliance acsn

Introduction and overview



1 Introduction

Reliance acsn is a specialist cyber security company providing managed security services and 'on demand' professional advice and support – enabling our customers to comprehensively defend their people, property and data against cyber security threats. We do this not only by blocking attacks, but by delivering a greater understanding of who and what the threats are targeting, and where they are going next. Our solutions predict the attackers next move and our expert resources work with customers to respond appropriately enabling business led decisions with a clear understanding of risk versus benefit.

Our independence and singular focus on the issue of cyber security means we provide our customers with a number of key benefits:

-  **Access to exceptional security expertise:** Whether through our managed security services or as part of our on demand professional services, as a specialist cyber security company, we attract some of the best talent in the industry. Drawing on expertise with experience gained in secure government and national security, defence, the financial services sector, telecoms, retail and other commercial organisations, we have highly skilled security experts who are knowledgeable about the challenges our customers face and have a proven track record of solving them.
-  **Solutions designed specifically to meet our customers' needs:** We are vendor agnostic. We design solutions for our customers that are right for them. We combine 'Gartner top right' commercial products with in-house developed capabilities to create unique technical solutions that are engineered with integrity and that specifically address customers challenges directly.
-  **Customer service excellence:** We only do one thing and that's provide security services. We've adopted rigorous processes and procedures to ensure repeatability, efficiency and quality in everything we do. However, most importantly, it is by fusing this rigour with one of the industry's most highly qualified corps of security experts, who are dedicated to delivering outstanding customer service, that we consistently and reliably deliver for our customers. Our personalised service means that the most common feedback we get from our customers is that 'we feel like part of their in-house team'.

We build long term relationships with our customers, supporting them throughout their cyber resilience maturity journey. Our solutions deliver a continuous uplift in cyber capability, provide in-depth visibility of activity on networks, and support regulatory compliance to a variety of standards. Our customers often ask us to engage to manage complex multi-supplier relationships where good information security is essential, or to provide expertise and oversight to ensure that business critical systems are continuously available.

We deliver managed services to over 80 customers from our UK base. We hold a number of industry certifications including ISO 27001 and cyber essentials plus, and our people hold certifications and accreditations from a wide variety of independent organisations such as Crest.

2 Managed Services

Reliance acsn provides ongoing managed security services to our customers ensuring they have an appropriate and effective security posture. We are often contracted directly by our customers and also work with large system integrators and VAR partners. We flexibly and agilely fill gaps where partners don't offer or operate solutions, or where existing partner solutions don't fit the customers' requirements or budgets.

Every organisation's security challenges are different. Devices and technology from multiple vendors; security teams with varying skill-sets; risk landscapes that change markedly from one sector to the next, and even amongst organisations within them. Reliance acsn solves these challenges through a number of key capabilities:

- **Proven, long-standing industry experience:** For many years, blue-chip clients have entrusted the management of their security services to us, across a broad range of sectors including government, Critical National Infrastructure (CNI), defence, legal, finance and retail.
- **Extensive expertise on tap:** Reliance acsn has one of the most capable teams of accredited security experts for a pure play security service provider, including analysts, consultants, testers, developers and more.
- **Technology agnostic:** Reliance acsn gives our customers independent advice. We utilise multiple technologies, with different configurations and architectures, ensuring that our customers get the most effective, efficient and appropriate solutions.
- **Flexible service offerings:** Many years of experience has enabled us to develop a range of flexible managed security services that can be tailored and customised to support customers individual and specific needs.

Reliance acsn operates our managed security services from our own resilient, geographically dispersed datacentres. All datacentres, SOC's and analysts are exclusively located within the UK. Reliance acsn delivers full redundancy by utilising a hyper converged next generation architecture. Our datacentres are based on Nutanix and provide resilience, redundancy and business continuity of all of our services to our customers. These datacentres meet stringent SLA requirements for availability of service from our high risk and highly regulated customers.

The outcome of all of our services is to ensure our customers can focus on their core business activities, taking full advantage of digital developments, confident that they are prepared and defended appropriately. We provide 24x 7 UK operated services across:

- 🔗 **Managed Detection and Response (MDR):** Continuous security monitoring, analysis and response to whatever is happening on our customers networks
- 🔗 **Managed Security Services (MSS):** A managed service provided to ensure all information assets are appropriately monitored, maintained, configured and secure
- 🔗 **Endpoint Management and Defence:** The identification, management and security of all end points across our customers' IT estate
- 🔗 **Privileged Access Management (PAM):** Granular control over all privileged accounts

2.1 Managed Detection and Response

Our key offering is our Managed Detection and Response (MDR) service, delivering pervasive monitoring analysis and response that factors in risk identification and prioritisation, effective and appropriate security controls, and is tailored to each customer's individual risk appetite and threat landscape. We break the service down into Monitor, Analyse and Respond:

- Monitor
 - ☞ Breadth - our monitoring draws on extensive threat intelligence (commercially sourced, partner and sector sourced and individually targeted intelligence that includes our unique darknet monitoring solution) combined with data collection that covers the entirety of a customer's business giving us excellent situational awareness
 - ☞ Depth – we utilise multiple vectors (such as logs, forensic host and network monitoring) and we correlate across these sources enabling us to build the complete picture.
- Analyse
 - ☞ Using advanced technologies such as machine learning, we collate information across all of our sources and identify anomalies
 - ☞ Utilising world class analysts we bring both the human oversight of incidents and proactive threat hunting to add experience and intuition
 - ☞ Our priority is to build a deep understanding of, and integration with, our customers so that we can contextualise threats directly to business priorities and goals
- Respond
 - ☞ Business value output – we've pioneered active response, managing and mitigating threats to clients before they are even aware of them. Where this isn't possible or appropriate, we deliver clear, real world actionable advice and intelligence, enabling business stakeholders to take informed business led decisions.
 - ☞ Reduced risk and exposure – by detecting and handling threats earlier, we reduce cost, complexity and exposure for our customers.
 - ☞ Our priority is to map SLAs and KPIs to your key risks and assets, providing maximum protection where it's needed most to reduced cost exposure.

We deliver the above in partnership with our customers, upskilling teams and resources through coherent multi-level communications. This creates a culture of security as 'business as usual' and develops senior stakeholder awareness and engagement.

2.2 Managed Security Services

We manage and operate some of the UK's highest risk and most complex security networks, and the devices within them. We ensure the devices, and hence the services utilised by clients are monitored 24x7, optimised, functioning correctly, up to date and defended from threats. We provide security services on over 2,500 security devices across the globe, with in excess of 100 different security solutions from more than 40 vendors under management.

At Reliance acsn, we're committed to client security that is both effective and appropriate:

- We manage a broad range and type of devices, meaning that we address the whole security landscape holistically.
- We sweat clients existing security assets harder through optimisation, smart advice and configuration.
- We focus your security investments on return on investment, never replacing systems 'for the sake of it' or to match 'our preferred standards'. Our laser focus on security value means your budgets go further.
- We manage solutions on-premise, in datacentres, in the cloud and at all stages of transitions between them, our clients appreciate our expertise, knowledge and flexibility that enables security to support the right directions for their business.

Whether it's a complex multi-national network for the finance sector, high risk government clients at risk from nation state, dispersed operations for key members of the international defence supply chain, or simple firewall environments that helps our NHS to operate, we apply the same level of expertise and rigour to our managed services.

Reliance acsn provides assurance to our clients that they will be able to operate, safe in the knowledge that our experts are identifying, managing and mitigating security risks.

2.3 Endpoint Management and Defence

Endpoints continue to increase in risk as clients adopt more flexible and remote working, and as users become more embedded into their devices. Reliance acsn delivers our 24x7 world class endpoint management and defence service, providing our clients unrivalled speed, visibility and scale together with an unparalleled number of services from a single managed service provider.

The service is module based, and Reliance acsn provides an overview of the current landscape at the start of service. This enables us to help our clients to identify which components deliver most value and structure an effective and appropriate service. Critically this can flex at any point and on-demand, meaning that at times of enhanced risks or critical business/compliance support requirements additional modules can simply be added.

The core platform provides visibility of the estate, through dedicated, virtualised, on-premise, remote and cloud-based hosts giving Reliance acsn experts the ability to interrogate and analyse hosts, whilst

also giving full integration with client core systems such as SIEM / SOC and infrastructure data sources.

Our approach delivers the following benefits:

- Reduce the attack surface: modules for patching, vulnerability management, software deployment and management all reduce the available attack surface that an attacker can utilise
- Increased visibility, awareness and understanding: asset management, discovery and integrity monitoring support better visibility, comprehension and evidencing of the current landscape
- Advanced detection, analytics and response: threat and incident response, together with trend analysis support the discovery and utilisation of advanced threat detection and response

Wrapping multiple vendor solutions into an integrated approach enables us to deliver services that are effective and appropriate for all of our clients, whether large or small and irrespective of market sector.

2.4 Privileged Access Management

Our Privileged Access Management solution provides our customers have granular control over all of their privileged accounts, ensuring that they have 24x7x365 real time visibility of how these accounts are being used and critically the power to revoke their use at the first sign of suspicious activity. Our service includes:

- Session monitoring and recording: We monitor the most sensitive accounts on our customers IT environment and record every user action, enabling forensic playback of account activity from both past and recent times, at any time
- Full audit trail of every activity across all privileged accounts: Who did what, where, and when – which provides an invaluable full chain of custody at all times and helps to meet compliance requirements
- Threat analytics: We provide valuable evidence that threats have been responsibly analysed to establish and combat the risks they present
- Compliant password enforcement: Fully managed on behalf of our customers

3 On Demand Services

Complementing our managed services described above, Reliance acsn has a focussed portfolio of security led on-demand services. These solutions enable us to help clients understand their existing assets, and work with them to evolve their cyber security awareness and defence. We provide:

-  **Penetration testing:** Reliance acsn delivers Crest certified testing, evaluating and assuring the reliability of client's key systems, infrastructures and platforms. Reliance acsn incorporates traditional and next generation penetration testing with red teaming and threat mapping to enable connected testing and defences.
-  **Advisory Services:** We assist our clients to help them assess their current security posture, review existing policies and procedures, develop plans for improvement, provide easy to follow next steps and support implementations that enable real change and improvement.
-  **Incident Response:** We support our clients in both a proactive and a reactive capacity when either planning for or dealing with a live breach. In a reactive situation we use state of the art tooling to provide our experts with 'eyes on' across the full infrastructure of the organisation and manage the incident remotely to avoid time delay in enabling 'boots on the ground'.
-  **Security Engineering:** We deliver expertise in design, architecture and engineering supporting our clients in major engineering projects, technology optimisation and refresh and configuration, documentation, and review engagements.
-  **Cloud Security Services:** Reliance acsn enables our clients to leverage the benefits from cloud adoption including cost, speed and an unparalleled ability to scale whilst ensuring it is secure.

3.1 Penetration testing

Reliance acsn penetration testing brings customers additional value through a next generation approach. This addresses the complex and constantly evolving nature of customer networks, the continuous flow of vendor vulnerabilities, and the threats both inside and outside of the organisation.

From simple packaged solutions through to more complex dynamic penetration testing, we help our customers to identify and prioritise where security resources should be focused to achieve minimum risk with maximum return on investment.

Our testing covers a broad range of devices, architectures and connectivity including external, internal, mobile, web application and wireless, and our testing methodologies across all these attack surfaces are also constantly updated to reflect the latest guidelines from the testing community, including ISO, ISACA, OSSTMM, OWASP and CLAS.

Our testers are industry certified (including Crest) and are passionate about both their expertise and how it maps into the real world for our customers. In one recent example, we worked with a long standing customer to identify and remediate a number of sub domain takeover vulnerabilities – within four hours of this threat being identified and mitigated it was published to the wider community and added as a focus area for upcoming tests, resulting in additional detections, remediations and defence.

Our Penetration testing services include

- External Testing
- Code Review
- Build Review
- Web Application Testing
- Web Services Testing
- Wireless Network Testing
- Physical Access Testing
- Internal Testing
- Firewall Ruleset Review
- Cloud Penetration Testing
- Attack Surface Review
- Open Source Intelligence
- Red Teaming
- Social Engineering

3.2 Advisory Services

Reliance acsn Advisory Services assist our clients to assess their current security posture, review existing policies and procedures, develop plans for improvement, provide easy to follow next steps and support implementations that enable real change and improvement. Reliance acsn believes in a holistic approach, taking into consideration all the access points, hardware, software, people, processes and technologies in an organization to gain full understanding and awareness of security posture.

This end-to-end approach allows an organisation to mitigate immediate risks by priority, develop a robust security strategy and ensure that the roadmap is aligned to improve overall security posture, and that these improvements are driven by an organisations' business priorities and goals.

Reliance acsn offers a number of different services that review and assess the high-level processes and policies currently in place and then enable drill down into specific areas for in depth assessment and advise, including:

- Security Posture Assessment
- Threat Modelling
- Identity Access Assessment
- Privileged Access Assessment
- Security Awareness Training (all staff levels)
- Data Security Assessment
- Critical Application Assessment
- Supply Chain Review
- Endpoint Security Review
- Firewall Reviews
- IDS/IPS Configuration Reviews
- Data Classification and Governance Review
- PCI DSS Review
- Policy and procedures review
- QSA Services
- Disaster Recovery Assessment
- GDPR Advice Services

3.3 Incident Response

Proactive Services:

As cyber threats evolve along with the leading thinking on how to effectively defend against them Reliance acsn are being asked more frequently to help them plan and prepare for a breach. To do this comprehensively we developed a range of proactive services to help with specific elements of incident preparedness:

- Threat Modelling – this is used to inform the playbook reviews
- Playbook review – these assess the effectiveness of the playbooks against the output of the threat modelling to ensure all identified high risk scenarios are covered within the playbooks
- Crisis Management Exercises – these are then leveraged to put your playbooks through their paces in as close to a ‘live fire’ exercise as possible. These can be tailored to both exec and operational level teams.
- Deploy Tooling – as a part of our retainer service we will support you in preparing for rapid deployment (or deployment ahead of breach) of our state-of-the-art tooling for managing breaches.

Reactive Services:

When you have a live breach in your organisation you want to be able to quickly engage a trusted partner with the skills, expertise, experience and tooling to help you mitigate the breach and remove the threat actor from your environment. Reliance acsn have experts in live incident response, investigations and forensics required to achieve this and use state of the art tooling to give our experts ‘eyes on’ across your infrastructure allowing remediation and clean-up activities where required. These services include:

- Retainer based fee structure – have expertise on hand to support you when required without having to arrange proposals and purchase orders.
- Pre-packaged or pre-deployed tooling to support you in a live breach scenario
- Access to appropriate forensics and specialist support where needed based on the type of attack and the type of technology impacted

3.4 Security Engineering

Our Clients often bring us complex security engineering projects requiring the integration of many disparate hardware and software components, they also regularly bring us smaller installations, configurations and upgrades – because our security engineers are experts who excel in the security

environment, and apply the same level of rigour and detail to every engagement, whether large or small.

Working on security designs, architectures and networks globally, Reliance acsn security engineering adopts our core principles of expertise, effective and appropriate solutions, a vendor agnostic approach and a focus on security return on investment for clients.

Some of the key services we provide are:

- Security Architecture
- Security Design Review
- Security Device Deployment
- Security project delivery and management
- Security Device Optimisation
- Integration of Monitoring, tools and systems
- Security Device Configuration Reviews
- Security Device Health checks
- Security “bake off” Assessments
- Back up, business continuity and disaster recovery systems, planning, implementation and testing
- Security device upgrades, refreshes
- Security documentation

3.5 Cloud Security Services

Reliance acsn enables our clients to leverage the benefits from cloud adoption including cost, speed and an unparalleled ability to scale. With almost all clients having some form of cloud engagement, (ranging from SaaS services (such as office365) to cloud native delivery of complex platforms and infrastructures) Reliance acsn supporting customers with a strong defensive cloud security posture is critical. We work holistically with traditional environments, enabling clients the flexibility to transform to and from traditional, hybrid and cloud environments to maximise the business outcome.

Whilst there is a new set of challenges to consider with cloud, these environments also bring the opportunity for security benefit. Reliance acsn helps customers adapt to and leverage the environment, evolving security controls and policies to complement and enhance traditional defences.

Reliance acsn works with clients at all stages of cloud maturity, delivering effective and appropriate security solutions, expertise and configuration. Our services deliver value to clients by enabling them to adopt these benefits, safe in the knowledge that independent, vendor agnostic, expert security design, governance and assurance has been applied to their environment.

Reliance acsn has built considerable expertise in a broad range of cloud services and platforms, including Azure, AWS, G-Cloud and a number of proprietary platforms and systems across a range of PaaS, IaaS and SaaS deployments. We work with a broad range of cloud vendor, 3rd party and in house developed tooling to achieve and evidence best practise and maximise available security ROI.

Our cloud services include:

- Cloud Security Design and Architecture
- Cloud Security Posture Assessment
- Cloud Transformation planning
- Cloud identity management (CIDAM)
- Cloud Privileged Identity Management
- Cloud Application / Platform testing
- Cloud Data Governance
- Cloud incident analysis and response
- Cloud tenancy hardening
- SaaS best practise hardening and optimisation
- Cloud security tooling design, configuration, optimisation and deployment
- CASB and cloud application management
- Cloud SOC/SIEM integration

4 About Reliance acsn

Reliance acsn has 70 staff and a turnover of approximately £6m. We deliver managed services to over 80 customers around the globe from two locations in the UK and are an independent, UK owned pure play security provider that is services led and vendor agnostic.

Reliance acsn delivers services to some of the highest profile, and high-risk customers in the UK, including in government, the financial service sector, the legal sector and retail. We hold a number of industry certifications including ISO 27001 and cyber essentials plus, and our people hold certifications and accreditations from a wide variety of security vendors and independent organisations such as Crest.

Our greatest strength is our technology independence and our commitment to service excellence which our customers attest to. This comes from our high-quality people and the vision we have developed together. A further strength is our private ownership. Brian Kingham (our chairman and sole investor) is building a business based on long-term trust. This commitment to longevity, passion, culture and service quality resonate with customers who value this vision when selecting long term security partners.