

Cloud security and monitoring services

G-Cloud 15

Contents

Cloud security and monitoring services	3
Service overview	4
Features and benefits	5
Features	5
Benefits	5
Case study	5
Background	5
The Challenge	6
Our Approach	7
The Outcome	7
Evidence of Success	8
Business continuity and disaster recovery plans	8
Onboarding and offboarding	8
Onboarding	8
Offboarding	9
Ways of working	9
Training	10
Quality assurance and performance testing	10
Security services	11
Ongoing support	11
SLA Incident Response	12
Hosting managed services	12
Service constraints	13
Ordering and invoicing	13
Pricing	13
Industry standards	13
Contact details	14

Cloud security and monitoring services

CDS provides the full range of services needed to define, build, assure and deploy secure cloud platforms, creating robust cloud computing architectures on which applications can run, providing end-users with the ability to leverage the power of cloud resources.

Our expert cloud architecture capability provides services including:

- Cloud security and monitoring services
- Cloudflare
- Cyber and information assurance consultancy
- Data architecture, analysis, and consultancy
- Secure by design technical consultancy
- Secure infrastructure and monitoring design
- Splunk.

We work with client stakeholders to capture and prioritise business requirements and constraints, hosting needs, service levels and maintenance implications. Our cloud architects implement secure-by-design infrastructures with risk-proportionate controls, to support reliable, scalable cloud provision that ultimately delivers improved services to end-users whilst minimising administrative and labour overhead for our customers.

CDS has both wide and deep experience of enabling organisations to move to the cloud, with a proven methodology that includes discovery and consultancy as well as implementation and migration. This methodology starts with discovery and requirements gathering, using business analysis to understand the role of legacy systems and technologies that need to remain on-premise, vs applications that are natively cloud-based.

We then make recommendations for the appropriate cloud hosting provider and architectures, with a formal integration and implementation plan that ensures a seamless and timely migration with an extremely high level of availability.

In addition, as a partner to Cloudflare, CDS' work in cloud hosting and migration is secure by design. Cloudflare now handles 10% of the world's internet traffic, with 10 trillion requests flowing across the platform from 2.5 billion users.

CDS is experienced in architecting, managing, and implementing scalable cloud services on a range of platforms.

- UK Policing Single Online Home on Microsoft Azure: a secure, high-availability, scalable platform, active-active across two data centres, leveraging Terraform, PowerShell and Chef

- Social Work England on Microsoft Azure, including microservices-based using Azure AD, Storage Queues, Functions, Logic-Apps, Redis Cache and MySQL Service, solution to migrate and transform large volumes of data
- Rail Delivery Group: content management and delivery solution on Amazon Web Services (AWS) for National Rail Enquiries, capable of handling daily peaks of up to 10 million users.

Service overview

CDS' leading cloud architects and security professionals provide a range of bespoke cloud architecture, security and monitoring services designed to support customers in every aspect of their cloud journey, from early adoption through to management of complex enterprise-level cloud and multi-cloud architecture that harness the power of hyperautomation.

Our qualified security professionals can support strategy and design services right through to full assessment of current cloud deployments to ensure alignment with industry best practice, identify security risks, introduce continuous improvement models, support compliance, assist with architecture and security improvements and undertake security testing.

Should your project require data consolidation and migration, CDS data migration and planning services support customers with assessment to understand dependencies, migratory needs, and cloud architecture requirements with an ability to support customers further with dedicated resource assistance or end to end implementation services.

Features and benefits

Features

- Strategy, design and audit of complex cloud security architectures
- Development of security policies, procedures and architecture documentation
- Security audit, risk assessment, gap analysis and comprehensive security testing
- Audit of security architecture design in line with NCSC & HMG standards
- DevSecOps support and advisory services
- Advice on cloud security information and event management (SIEM) solutions
- Azure WAF, Azure ExpressRoute, Azure DDoS, Microsoft Defender, Azure AD MFA
- AWS WAF, AWS Advanced Shield, AWS Inspector, AWS GuardDuty
- Zero trust access leveraging Cloudflare
- ISO27001 certified.

Benefits

- Experience of security, privacy, compliance and cloud provider best practice
- Experience of secure cloud architectures across public and private sectors
- Experience in design of high availability services
- Service design considerations for scale, agility and security
- Assurance on deployed services and data protection
- Compliant enterprise security posture
- Adherence to Cloud Security Standards
- Proactive management and monitoring
- Embedded business continuity and contingency planning
- Security cleared staff to SC and NPPV2 levels.

Case study

The Digital Public Contact (DPC) programme, commissioned by The Mayor's Office for Policing and Crime (MOPAC) and The Metropolitan Police Service (MPS) engaged CDS to deliver the most significant transformation in UK policing since the introduction of the 999-emergency number in 1976. Their ambition was to deliver a single digital platform through which every UK police force can provide nationally consistent, locally branded services – brought together in one seamless 'digital police station'.

Background

At the heart of this transformation is **Single Online Home (SOH)** – the national digital policing platform - delivered by CDS. SOH enables secure, scalable communication between citizens and police forces in a secure, modern cloud environment, forming a cornerstone of the UK's national policing strategy.

The platform allows regional police forces to retire legacy websites, content management systems and infrastructure, replacing them with a unified, GDS-aligned service built on consistent functionality and architecture. It acts as a single, trusted digital ‘front door’ through which the public can engage with the police online.

SOH supports a wide range of services, from reporting all categories of crime – including domestic abuse, rape and sexual assault, spiking, theft, burglary and assault – to non-crime services such as reporting missing persons, applying for firearm licences, and submitting road traffic incident reports. It also facilitates access to vital safeguarding services, including Clare’s Law and Sarah’s Law disclosure requests.

By streamlining these interactions, SOH reduces administrative burden, improves operational efficiency, and allows police call centres to focus on genuine emergencies. Today, the platform provides access to policing services for more than 90% of citizens in England and Wales – over 53 million people.

CDS is the prime contractor for SOH, delivering the web platform, hosting police data on SQL server, and providing data administration, configuration, security, monitoring and integration - supporting 41 of the 43 Home Office police forces across England and Wales.

The Challenge

In 2021–2022, SOH was subjected to relentless and escalating cyber-attacks. At their peak, the platform faced 120 million malicious requests in just five minutes – more than 20 times the normal traffic of around six million requests.

These attacks had serious consequences: platform stability and availability were compromised, and public confidence was eroded. Many citizens, no longer trusting the online service, reverted to traditional channels such as 101, placing further strain on police resources.

The existing DDoS mitigation solution was also failing under pressure – both technically and commercially. The vendor’s volume-based pricing model meant that every attack surge triggered huge, unplanned cost spikes, blowing through budgets and introducing unacceptable financial risk.

With 53 million citizens relying on SOH and a mandated 99.99% uptime, failure was simply not an option. A completely new approach was required – one that could withstand an evolving threat landscape, deliver predictable costs, and provide rock-solid reliability.

With 41 independent forces, each with its own IT teams, governance processes, security requirements, operational constraints, decision-making structures, we needed to establish a flexible yet consistent configuration approach.

This included managing DNS, traffic routing, and firewall policies across multiple domains to ensure seamless performance and alignment with national standards.

Given the sensitivity of policing data, strict compliance with UK data protection and security standards was mandatory. At the same time, CDS had to ensure that Cloudflare configurations had to be designed to deliver the agility and scalability needed for the national platform, ensuring future growth.

Our Approach

When 120 million attack requests can arrive in just five minutes, the stakes are high – and choosing the right protection is critical. Our Cloud Engineering team undertook a comprehensive evaluation of five leading DDoS protection solutions. Each was rigorously assessed against defined threat scenarios, cost models, feature sets, and technology roadmaps.

Cloudflare emerged as the clear choice. It demonstrated superior threat detection, offered predictable fixed-cost pricing, scalability and provided a robust innovation roadmap aligned with future requirements. The client agreed with our recommendation.

To validate this decision, CDS built a full-scale testing environment designed to replicate every real-world scenario:

Complete security stack: Zero Trust, Web Application Firewall (WAF), DDoS protection, VPN replacement.

Rigorous testing: Internal performance tests, client-led load, spike and soak testing, plus full penetration testing.

Real-world validation: Pre-production URLs mirroring live SOH conditions.

The proof-of-concept delivered outstanding results: performance, resilience, and security all showed significant improvements. The client's own acceptance testing confirmed that Cloudflare was the right solution.

Our deep knowledge of Cloudflare services enabled the design of secure, high-performance configurations for DNS, traffic routing, and application security across multiple domains.

Every deployment was aligned with UK policing standards and data protection requirements, ensuring confidence in the platform's resilience and compliance.

The Outcome

CDS successfully delivered the migration project in just five months, seamlessly moving the entire SOH platform – 26 domains (at the time of migration) serving over 53 million citizens – to the new solution with zero service interruptions.

By using a structured, repeatable approach, CDS enabled new forces to be onboarded quickly with minimal disruption. This reduced time to service and allowed the programme to scale at pace.

Deployments were aligned with national policing standards, ensuring robust protection of sensitive services while maintaining high availability.

The approach created a foundation that can be extended to additional forces or adapted to new requirements, ensuring long term value and sustainability.

The result: a platform that is more secure, more resilient, more predictable in cost and fully equipped to support the critical public services millions of people rely on every day.

Evidence of Success

Since deploying Cloudflare's WAF solution, SOH has achieved **100% uptime over three years** – even while defending against an average of **50 million malicious requests every month**. The move to Cloudflare has transformed operations, enabling our Cloud Engineering teams to shift from constant firefighting to proactive innovation.

Cloudflare continues to deliver measurable value across several key areas:

- **Improved platform stability and uptime** – The enhanced availability and performance of the platform have built public confidence and driven sustained adoption of online reporting. As a result, more citizens are choosing to engage through digital channels rather than resource-intensive and more costly phone calls – exactly as intended.
- **Greater cost predictability** – Cloudflare's pricing model has eliminated the volatile cost spikes caused by attack surges. This has allowed the programme and police forces to plan and manage budgets with far greater confidence and control.
- **Enhanced security intelligence** – Cloudflare's detailed threat analytics provide deep visibility into attacker behaviour, allowing the team to understand what adversaries are attempting and when. This insight turns every blocked attempt into a learning opportunity – enabling us to adapt, evolve and stay ahead of emerging threats.

“Since migrating, we have experienced 100% service uptime – which is critical when hosting a national platform providing essential services to the UK public. This is how a successful digital project should be run.” **Mohammad Asif, Head of Service.**

Business continuity and disaster recovery plans

CDS is committed to minimising and managing its exposure to disruption to the business and the services provided to our customers. This encompasses robust systems and processes necessary to maintain continuity of service and operations.

CDS maintains a comprehensive Business Continuity and Disaster Recovery (BCDR) plan, certified to **ISO 23001**, that defines clear roles, responsibilities, processes, and procedures for assessing and responding to disruptions to ensure continuity during disruptions. **Our plan is tested annually with lessons learned incorporated into plan improvements.**

Our Business Continuity Management System (BCMS) is underpinned by regular business impact assessments and threat and risk analyses, and annual tests to ensure all contingencies remain effective, current, and fit for purpose.

Onboarding and offboarding

Onboarding

CDS provides a tailored onboarding pathway, based on clients' individual requirements.

Onboarding is a collaborative process, through which we fully understand our clients' short-, medium- and long-term goals, and plan our service accordingly, to deliver best value and appropriate resourcing, governance, communication and planning.

Our multi-disciplinary agile teams will work with project stakeholders to understand the client and project needs and requirements.

We will define and capture ways of working, including definitions of 'ready' and 'done', and identify acceptance criteria for each sprint, underpinned by modern test practices and OKRs.

Offboarding

Upon starting the engagement, CDS will provide an exit plan for client approval. This will cover matters such as knowledge transfer and documentation, roll-off schedules, data and asset transfer, intellectual property and removal of access / permissions and return of devices / equipment.

Ownership of data contained in any solution belongs to and rests with the client; as the service is decommissioned, raw data will be transferred to the client. CDS is certified to ISO 27001 for data security and will always adhere to these standards – including data removal and destruction.

Ways of working

At CDS we apply agile principles across our projects, primarily using the SCRUM Agile methodology. We operate multi-disciplinary squads that combine domain expertise with technical excellence, delivering value early and iteratively through two-week sprints. Our approach is underpinned by the following core practices:

- **Daily standups:** A team call for 15 minutes each morning to track progress, surface blockers and ensure sprint goals are achieved.
- **Sprint planning:** Held at the start of each sprint to prioritise the work, align on objectives and ensure the team is fully prepared.
- **Sprint review:** At the end of the sprint, the team demonstrate to all stakeholders the deliverables achieved and present the sprint goal for the next sprint.
- **Sprint retrospective:** For each sprint the team will review what went well, identify areas of improvement and embed lessons learned to drive continuous improvement.

Additionally, we have an Agile mindset and culture at CDS, in which we apply:

- **User-centred design and customer-focus:** Through collaboration and partnership working we deliver outcomes that meet user needs.
- **Adaptability and flexibility:** Short feedback loops enable us to respond quickly to change, with teams empowered to pivot as required.

- **Continuous learning:** Retrospectives encourage open, honest feedback to continually improve ways of working and delivery effectiveness.
- **Partnership and teamwork:** We create a one-team culture with our clients and their supplier partners, working collectively towards shared project goals.

Training

As well as continual ‘on the job’ knowledge transfer to upskill client teams, CDS can provide formal, comprehensive training for administrators and users prior to handover and go live designed to support successful change management, ensure smooth implementation and embed solutions that are integral to business operations. Our training also builds internal technical capability, empowering teams to become self-sufficient and reduce the long-term cost of change.

In most cases, we adopt a ‘train-the-trainer’ model, delivered through a blend of on-site and remote sessions. This is supported by comprehensive training materials and easy-to-follow digital end-user guides, written for non-technical audiences and compliant with WCAG 2.2 accessibility guidelines

Quality assurance and performance testing

CDS applies rigorous testing as part of our Quality Assurance process (ISO9001) to ensure we maintain quality across our deliverables and that outcomes are fit for purpose and fulfil functional and performance requirements.

Our testing capability is led by ISTQB (International Software Testing Qualifications Board) qualified testing experts with all the skills and expertise to quality assure AI, technology & cloud services.

We use a flexible, agile testing approach utilising tools and techniques tailored to each client’s context to ensure solutions meet business objectives and success criteria.

We adopt an automation-first approach, embedding high-quality automated checks into robust CI/CD pipelines to ensure quality is treated as a first-class citizen throughout the deployment process.

Our testing services include:

- Test strategy
- Test planning
- Automated test frameworks
- Testing, defect management and reporting
- Support of customer UAT
- Security (perimeter/application) testing / DevSecOps
- Performance and stress testing.

Security services

CDS holds certifications to international standards - Cyber Essentials Plus and ISO27001 Information Security, encompassing physical security, personnel security, storage, electronic data handling and secure destruction.

We embed 'secure-by-design' principles in our standard service design approach, aligned with security best practises and in addition we provide expert security consultancy.

CDS works closely with National Cyber Security Centre CHECK-accredited providers to conduct IT Health Checks (ITHC)/penetration testing in line with best practice.

CDS staff are BPSS cleared as a minimum. We can deploy SC, NPPV cleared teams and staff with DV clearance, if required.

Ongoing support

Our service model is designed to provide comprehensive, proactive support that operates to **ISO20000:2018 Service Management and ITIL best practices**, covering the full-service management lifecycle.

We deliver a fully managed service that encompasses application support, platform maintenance, incident management, problem management, change management, supplier management, and out-of-hours support for major incidents. This approach ensures that business-critical systems remain operational and performant whilst maximising customer value through continuous service improvement.

All CDS Service Delivery team are ITIL-certified.

We offer three service levels (Bronze, Silver and Gold) each providing:

- Online Service Desk Portal available 24x7 for logging and tracking incidents and requests.
- Telephone support via a dedicated helpline available from 9am to 5pm Monday – Friday (excluding English Bank Holidays).
- Highly skilled service desk team who manage and resolve incidents and requests in accordance with the agreed SLA.
- Ongoing maintenance including application of security patches.
- Structured change management to ensure updates are properly assessed, approved and implemented.
- Monthly performance report to provide visibility of service levels and operational metrics.

Support and maintenance contracts stipulate a minimum level of support provision per month, appropriate to the size and complexity of the service, aligned to the preferred service support tier. Additional time is chargeable at the day rates listed on the rate card.

SLA Incident Response

Service	Bronze	Silver	Gold
Incident response			
P1 - To be called in	15 minutes	15 minutes	15 minutes
P2	1 hour	1 hour	1 hour
P3	1 hour	1 hour	1 hour
P4	4 hours	4 hours	1 hour
P5	1 working day	1 working day	1 hour
P6	1 working day	1 working day	1 hour
Target incident resolution - core hours			
P1	8 hours	6 hours	4 hours
P2	15 hours	11 hours	8 hours
P3	5 working days	3 working days	1 working day
P4	7 working days	5 working days	3 working days
P5	N/A	14 working days	10 working days
P6	N/A	N/A	N/A
Major Incident Report	N/A	10 working days	5 working days

Hosting managed services

CDS provides a range of consultancy and management services for design, implementation and management of application infrastructure, including:

- Technical architecture and implementation
- Infrastructure management and maintenance including:
 - Critical security patches
 - OS (operating system) patches: testing and deployment

- Application and platform availability
- Anti-virus & Malware updates
- Obsolescence management
- Proactive monitoring and alerting of Infrastructure & solution performance and function.

Service constraints

Attainable service levels will be dependent upon the service performance of cloud suppliers within the service chain. Maintenance windows may apply, and clients should refer to the SLA for the specific service in use.

Ordering and invoicing

We recommend contacting CDS before placing an order via G Cloud 15, to confirm and agree scope, scale, SLAs, KPIs, outcomes, etc. We will be pleased to support clients to define statements of work that reflect their requirements.

Invoices are issued monthly in arrears, with payment terms of 30 days.

Pricing

Timescales and costs vary, depending on several factors; we recommend a preliminary review to provide a firm cost.

Please refer to our pricing document and rate card.

Industry standards

CDS delivers all its services to internationally recognised standards. CDS is accredited to the following standards:

- ISO 9001 Quality Management System.
- ISO 27001 Information Security Management.
- ISO 20000 IT Service Management and IASME certified.
- ISO 14001 Environmental Management.
- BSI 1008 Electronic Information.
- ISO 22301 Security and Resilience (Business Continuity).
- ISO 45001 Health and Safety Management.
- ISO 10008 Evidential Weight and Legal Admissibility of Electronic Information.
- ISO 50001 Energy Management Standard.
- Cyber Essentials Plus.
- IASME certified.
- ITIL compliant service desk.
- PlanetMark Sustainability.

We comply with the Data Protection Act 2018 and UK GDPR regulations.

Contact details

Matt Johnson,
Head of Public Sector
CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH
Email: bidteam@cds.co.uk
Telephone: 07939 866831
Website: www.cds.co.uk