

Secure Containerisation G-Cloud 15





Table of Contents

1	Service Overview	3
1.1	High Level Design	3
2	Business Need	3
3	Our Approach.....	4
3.1	Engagement Model	4
3.2	Capgemini's Proposition	5
3.3	Benefits	6
4	Why Capgemini.....	7
5	Buyer Responsibilities	8
6	Service Management	8
7	Protection of Data	8
8	On-boarding and Off-boarding	8
9	Skills and Knowledge Transfer	8
10	Vendor Accreditations/Awards	8
11	Sub-contractors	9
12	Business Continuity and Disaster Recovery	9
13	Pricing	9
14	Ordering and Invoicing	9
15	Termination Terms	9
16	Further Information	9



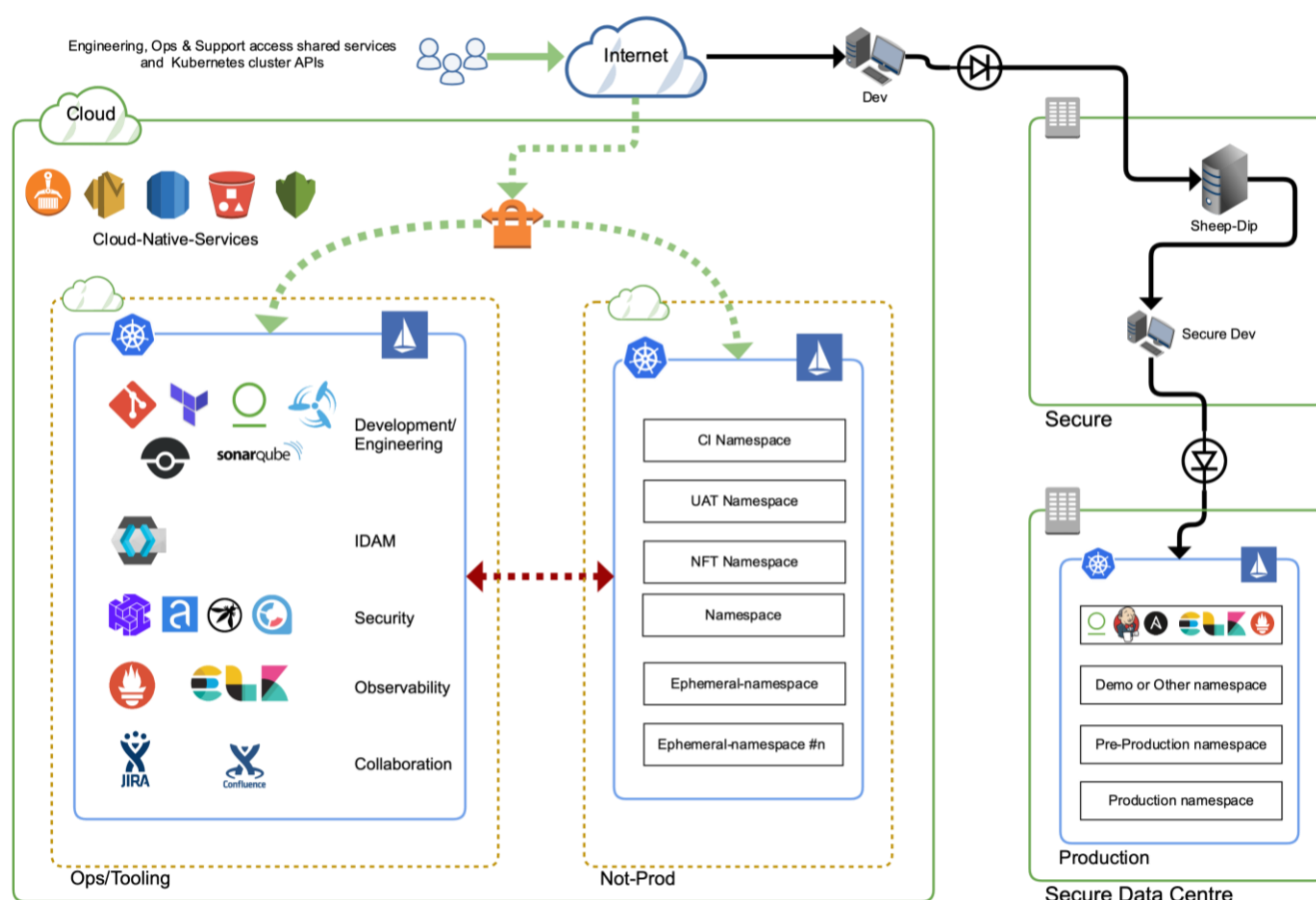
1 Service Overview

Capgemini can provide secure Kubernetes and Docker-based strategic, container-first development and hosting approaches classifiable to Official, Official-Sensitive and Secret levels. Capgemini has proven experience in designing and deploying these platforms in a UK Government context supporting high availability configurations and zero-downtime deployment for UK Critical National Infrastructure.

Capgemini's approach is cloud-agnostic, delivering identical application hosting environments to cloud, hybrid and on-premise infrastructures. Operating at scale and maximising resource utilisation through dynamic elasticity and "bin packing" allows the buyer to pay only for what is needed and used. Capgemini's approach also supports multiple agile delivery teams working independently at pace and within dependent ecosystems; this enables them to realise value quickly through continuous delivery, amplified feedback loops and metric-based decision making.

Importantly, Capgemini can implement security controls compliant to the latest National Cyber Security Centre's guidance and the Cloud Security Alliance v4 guidelines across all domains ensuring systems pass IT Health Checks and gain the UK Government's Authority To Operate (ATO).

1.1 High Level Design



This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

2 Business Need

Modern digital solutions are created using microservice architectures that enable horizontal scalability and support small incremental changes. Congruent to this design pattern, digital services are frequently delivered by multiple, disparate, delivery teams, facilitating greater flexibility, diversity, and ingenuity whilst reducing costs



through more competitive procurement. However, the early realisation of value achievable through the use of these design and operational patterns is only possible if each team develops and releases at its own cadence and independently of each other. Teams need to be able to measure the value of what they are producing and rapidly pivot based on the analysis of business metrics.

It is important to recognise that these delivery streams are part of a bigger system, and they need to collaborate with each other in order to deliver an end-to-end service. Individual teams can't break the work of other teams and hence the end-to-end service, either through incompatibility or insecurity. Such challenges are further exacerbated when end-to-end services cross security domains, from Official and Official-Sensitive to Secret, which then creates fundamental application development and hosting disparities caused by cloud, on-premise and hybrid environments.

Capgemini's Secure Containerised Application Development and Hosting Approach overcomes these challenges, and enables projects to realise the benefits of commodity cloud computing using a single technology stack across environments. This approach is widely used in UK government where many projects span security classification domains requiring secure data centre hosting on physical infrastructure.

3 Our Approach

Capgemini's Secure Container approach is based upon a standardised methodology which can be tailored according to buyers' requirements. Activities would typically be undertaken using agile principles aligned to the Government Digital Service (GDS) Manual.

The buyer's journey towards Secure Containerised Application Development and Hosting begins with Capgemini undertaking a two-week discovery by a small team (2 to 3) of experts skilled within the fields of DevOps, Software Development and Security. The team can cover the following areas:

- Agile practices
- Lean and scientific methodology adoption
- Value measurement
- Value stream analysis
- Build management
- Continuous integration
- Environment management
- Deployment capability
- Release management
- Compliance
- Testing strategy
- Data management
- Cloud Security maturity.

The discovery findings will be presented and will inform the buyer's aspirational roadmap to deliver a Secure Containerised approach.

3.1 Engagement Model

For each engagement, teams can be a mixture of people from the buyer organisation, third parties and Capgemini or they can be entirely staffed by Capgemini.



Upon selection, we will mobilise and perform project initiation activities using agile principles aligned to the Government Digital Service (GDS) Manual.

Our recommended approach is to undertake the initial discovery phase on a day rate basis to help establish a joint understanding of scope, complexity and requirements. Once this is established, a project can then be set up to deploy the core deliverables.

Where the buyer requires greater flexibility or where scope is less certain, Capgemini can supply resources on a day rate basis. These resources can be utilised to:

- Allow the service to flex as the buyer's understanding develops. This approach can be appropriate where the buyer is looking to develop its own internal capability and is looking for skills transfer until it can take on responsibility for the service.
- Augment the existing in-house capability with additional skills within a limited time-frame.

3.2 Capgemini's Proposition

Capgemini's Secure Containerisation proposition can offer:

- Advice and guidance
- Strategy definition
- Maturity assessments
- Architecture and tool selection
- Build and implementation services
- Ongoing service and support
- Development and production platforms
- Automated development and deployment pipelines
- Security hardening and accreditation
- Metrics and monitoring
- Service management
- Application deployment and release management
- Accounting.

The phases of delivering a Secure Containerised approach can include:

- Discovery
 - Baseline assessment (DevOps, Development & Security)
 - Create and present improvement roadmap.
- Design and Planning
 - Technical governance - Tech RADAR, TDA, etc.
 - Detailed design of development platform
 - Detailed design of pipelines
 - Detailed design of production platform
 - Detailed sheep-dip design
 - Develop detailed Implementation planning.
- Implementation phases



- Network/Pipeline Integration
- Shared services
- Create CI/CD pipelines for application build and deployments
- Implement development platform
- Deploy to development systems
- Create sheep dip systems
- Implement production platform
- Metrics & Monitoring
- Accounting and provisioning (cost per transaction)
- Service design and transition
- Change and release management
- Security accreditation
- Deploy to production systems.

Capgemini's Secure Containerisation is implemented using secure-by-design principles as followed for all our engineering projects. These principles encompass the Cloud Security Guidance published by CESG UK alongside other industry sources, for example the National Cyber Security Centre (NCSC), Open Web Application Security Project (OWASP) and Amazon Web Services (AWS) Well-Architected Framework guidance.

Capgemini can work with the buyer to define the key metrics and goals to be measured in the DevOps lifecycle. This can allow the DevOps team to implement monitoring and feedback loops throughout the development lifecycle, enabling them to stay aligned with the buyer's strategic vision.

3.3 Benefits

Our Secure Containerisation approach provides the following benefits:

- **Cost savings through, for example:**
 - Minimised physical data centre hosting charges
 - Maximised use of commodity cloud resources
 - Optimised resource utilisation through bin packing, autoscaling and scale-to-zero
 - Faster feedback loops
 - The rapid on-boarding of disparate delivery teams.
- **Improved Quality as a result of:**
 - CI/CD using identical environments
 - Contract based automated testing
 - Chaos engineering
 - Design for failure approach which mitigates risks and enhances service continuity.
- **Greater Flexibility including:**
 - Supporting private, public and hybrid cloud hosting
 - Adopting an Opensource first strategy to reduce lock-in to vendors and technology
 - The use of Autoscaling and self-service provisioning



- The provision of provider/hosting agnostic containers avoiding lock-in.
- Multi-cloud deployments integrated with a single identity and observability layer
- **Improved Culture, Process and Values through:**
 - Enabling the creation of loosely coupled systems empowering disparate delivery teams to release frequently and independently
 - Using rapid metrics-based feedback loops to drive decision making
 - Implementing agile and lean practices to ensure the delivery of real needs
 - Supporting DevOps transformational strategies.
- **More Efficient Operations and Service Management by:**
 - Facilitating the creation of light touch and automated ITIL processes
 - Reducing operational overheads through the standardisation of technology and pipelines.
- **Increased Security by:**
 - The implementation of National Cyber Security Centre and Cloud Security Alliance v4 guidelines
 - Establishing Multiple security controls at every level to achieve Authority To Operate Critical National Infrastructure.
- In addition, our approach features:
 - Assuming roles with least privilege and RBAC
 - Encryption at rest and in transit by default
 - Mutual authentication and Transport Layer Security (TLS) between microservices
 - Service mesh and security controls at container, POD, Namespace, Host, Cluster, Subnet, VPC and Account levels.

4 Why Capgemini

Capgemini has more than 300,000 employees in over 50 countries with 12,000 working within Capgemini UK PLC. With over 3,000 SC and 300 DV cleared engineers Capgemini has the capacity to scale and deliver for the most demanding projects within the public and private sectors.

We are leaders in Lean, Agile, and DevOps transformation, and our engineers are recognised for their contributions to the open-source community. In addition, our global internal network of DevOps specialists, dialogue with open-source communities and relationships with technology suppliers and our other ecosystem partners means we are able to constantly evolve the service to stay aligned with industry best practice.

The service is technology-agnostic. We work with open-source, proprietary and bespoke products; these include but are not limited to:

- Identity and Access Management (IDAM): Keycloak, Forgerock, OpenAm. Including integration with existing Identity providers
- Cloud Hosting: AWS, Azure, Google, Cloud Foundry, UK Cloud, Openstack, Openshift
- Database: Object, document, relational, non-relational, graph, key-val (MongoDB, Postgres, MySQL, Oracle, MS SQL, Neo4j, Redis, memcached)
- Big Data: Hadoop, Casandra, Apache Spark and Storm, Kafka, KSQL, Streams, Elasticsearch, Hortonworks – HDFS, Hbase, Solr/Lucerne, Nifi



- Development: Golang, Node.js, .Net, Jenkins, Drone, Concourse, GoCD, Artifactory, Atlassian Suite, Gerrit, Gitlab, Slack, GitHub, Hipchat, Mapreduce, JIRA/Confluence, Maven, Python, Ruby, SonarQube, Visual Studio Team Services, Ract, Angular, Vue
- Infrastructure: Serverless, Docker Containerisation, Kubernetes, Mesos, Ansible, Chef, Puppet, Terraform, Consul, Vault, Packer, PowerShell
- Cloud Native: Lambda, Service Mesh, Istio, Prometheus, StatsD, KNative, Linkerd, Envoy, Anchore, Claire.

5 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

6 Service Management

Capgemini can design, implement, and manage a Secure Container Application Development and Hosting solution across one or more delivery teams. Solutions can be specially tailored for each use case providing for full stack delivery and with focus on Site Reliability Engineering, Cloud Native or Continuous Delivery models.

7 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss. Additional requirements this may be subject to additional Charges in accordance with the SFIA Rate Card.

8 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which can be charged for in accordance with the Pricing section for this service.

9 Skills and Knowledge Transfer

Capgemini recognises skills and knowledge transfer is critical for the provision of G-Cloud services to public sector clients. Where possible, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for private and public sector clients.

Our standard Assess-Plan-Implement framework can be tailored to specific topics, skills-gaps and individuals to provide consistency and effectiveness. This approach has been used repeatedly by our teams to structure the work required to transfer skills and create new capable teams. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods, materials and deliver and evaluate success.

10 Vendor Accreditations/Awards



For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

12 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

13 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

14 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2026 Capgemini. All rights reserved.