

Cross Domain Security Zone



Contents

Overview 3

Why Vysiion? 3

Cloud characteristics delivered 4

Key characteristics of our service 5

Pricing and packaging 5

Connectivity options 7

Discount and purchase schemes 7

Trial service 8

Service Level Agreement 8

On-boarding 9

Data Migration 10

Service Management 10

Service constraints 10

Technical requirements 11

Customer responsibilities 12

Termination 12

Ordering and invoicing 13

Conclusion 13

Overview

What the service provides

Vysiion's Cross Domain Security Zone (CDSZ) is based on UKCloud's service and enables you to securely transfer data between the UKCloud Assured OFFICIAL (formerly IL2) cloud platform and the UKCloud Elevated OFFICIAL (formerly IL3) cloud platform, using National Cyber Security Centre (NCSC)-approved cross-domain security patterns.

What the service can help you achieve

- Create secure applications that are accessible to citizens, but ensure data safety
- Reduce your infrastructure and compliance costs, by leveraging UKCloud's ready-made solutions
- Ensure your solutions are aligned with information security requirements
- Meet changing requirements by controlling and adapting the service

Key service capabilities

- A secure and flexible way to transfer data between your workloads hosted on the UKCloud Assured OFFICIAL cloud platform and the UKCloud non-internet connected Elevated OFFICIAL cloud platform
- A choice of services:
 - UKCloud Guard, which is managed by UKCloud and delivered as a cloud service
 - The single-tenant Walled Garden, which enables you to deploy your own controls to support a wider range of use cases and traffic flows
- A flexible application process with a self-assessment route for customers with simple implementations; and an assurance review approach with UKCloud's experienced professionals for more complex implementations
- Independent validation (including NCSC design reviews) that CDSZ is fully aligned with the 14 NCSC Cloud Security Principles and suitable for data classified at OFFICIAL (including OFFICIAL-SENSITIVE)

Why Vysiion?

Vysiion is a strategic partner of UKCloud, Ark Data Centres and Crown Hosting Data Centres (CHDC) with offices at Spring Park, Corsham and Cody Park, Farnborough. We have:

- ISO9001 and ISO27001 accreditations for quality and information security
- Cyber Essentials PLUS certified
- Highly resilient Tier 3 data centres, on UK sovereign territory and separated by >50 miles for geographical diversity
- Security Cleared staff
- 24/7 ITIL based Service Desk

The diagram in Figure 1 illustrates the complementary capabilities available from Vysiion. These can be procured alongside this service to support an organisation's transition towards more commodity based ICT.

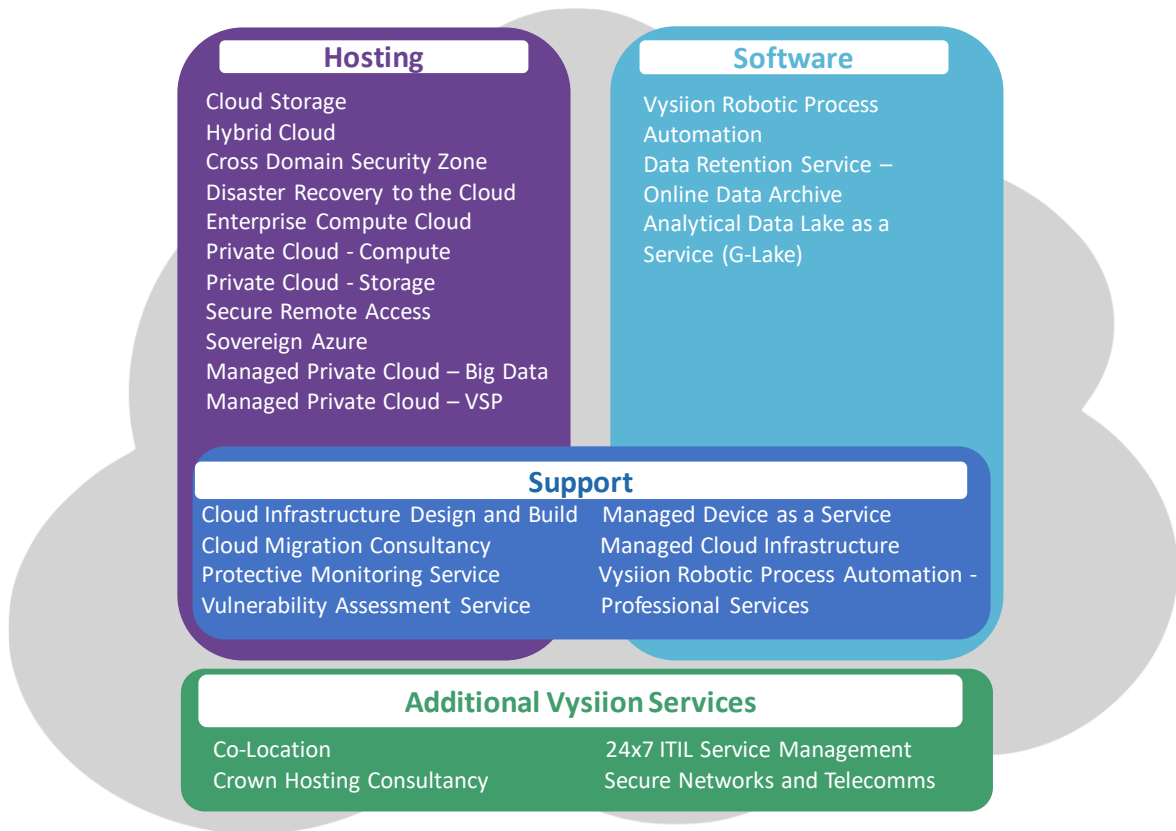


Figure 1 - Vysiion Services

Cloud characteristics delivered

- Elasticity — you can scale the UKCloud Guard and Walled Garden solutions horizontally or vertically to adjust for increased traffic flows
- Ability to make changes approved by the compliance team to your Walled Garden without involving the UKCloud support team
- Measured usage — you will be billed only for what you use as you adjust the number and size of virtual machines (VMs) your solution needs
- Broad networking — connect via DDoS-protected internet; a government community network such as PSN, N3/HSCN, Janet or RLI; or HybridConnect, using your own dedicated circuits
- Resource pooling — both the UKCloud Guard and the Walled Garden operate within the UKCloud platform with no need for customer-built solutions

Key characteristics of our service

The Cross Domain Security Zone helps you achieve the goals of the Government Digital Strategy by making government community-facing (for example, PSN) applications available to citizens and industry via the internet. It's ideal for solutions where service accessibility and data security are key underpinning principles.

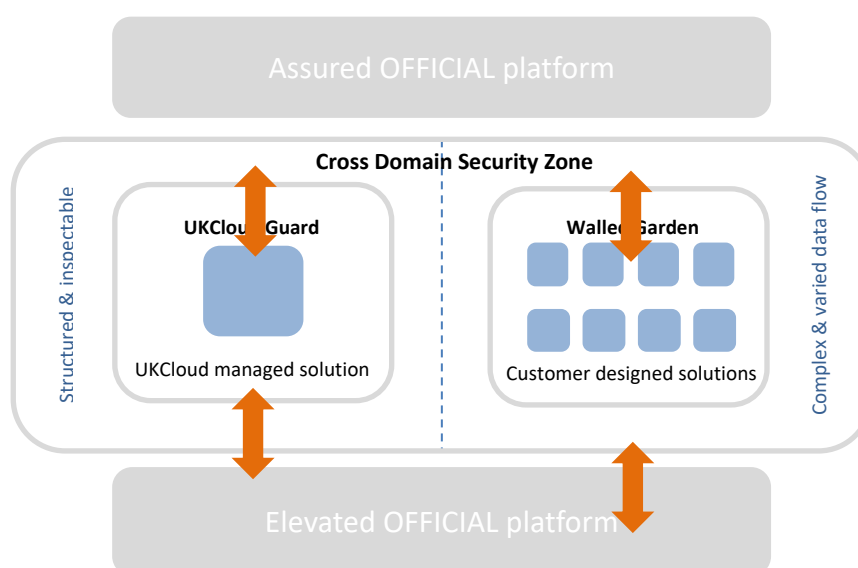
There are two service options: the UKCloud-managed UKCloud Guard, and the self-managed Walled Garden.

UKCloud Guard

The secure, scalable managed UKCloud Guard supports structured and inspectable HTTP-based data flows. This option provides an immediately available solution to support simple use cases, such as applications designed to make inspectable web services calls between the security domains.

Walled Garden

Access to the Cross Domain Security Zone enables you to design, implement and manage your own Walled Garden, using technology and application services of your choice. We provide an assurance wrap by managing firewalls between the security zones and ensuring you use appropriate risk management to understand and mitigate identified risks.



The Walled Garden is ideal for organisations that require more control and flexibility over what is passed between security domains, to support a wider range of use cases.

Pricing and packaging

UKCloud Guard

The UKCloud Guard is priced as per the table below. Once the consumption of the service reaches the next pricing tier, all usage for the month will be charged at that lower price.

		Upgrade options
Data volume	Monthly price	Dual site
Starter Pack (1TiB)	£500	£500 per month
Next 4000GiB	£0.50 per GiB	
5001GiB+	£0.10 per GiB	

Walled Garden

The self-managed Walled Garden is priced with a baseline monthly fee plus a fee per VM per hour, depending on the VM size and inclusion of Snapshot protection options, as follows:

Baseline (per DC / month)	£500
---------------------------	------

VM (per hour)				
	2GHz vCPU	RAM (GiB)	POWER	
Tiny	1	2	£0.12	+
Small	2	4	£0.15	
Medium	4	8	£0.26	
Medium High Memory	4	16	£0.40	
Large	8	16	£0.50	
Large High Memory	8	32	£0.75	
Tier 1 Apps Small	8	48	£1.05	
Tier 1 Apps Medium	8	64	£1.39	
Tier 1 Apps Large	8	96	£1.85	
Tier 1 Apps Extra Large	12	128	£2.30	

VM Protection ^[2]	
14-day snapshot	28-day snapshot
£0.07	£0.07
£0.12	£0.12
£0.19	£0.19
£0.25	£0.25
£0.35	£0.35
£0.60	£0.60
£0.85	£0.85
£1.05	£1.05
£1.55	£1.55
£1.60	£1.60

Block Storage (per GiB/per month) ^{[6] [7]}	
Tier 1	£0.25
Tier 2 ^[4]	£0.10

+

Block Storage Protection (per GiB/per month)	
£0.20	£0.30
£0.10	£0.20

Licensing										
VM Size	Microsoft Windows Server OS		Microsoft SQL Standard ^[2]		Microsoft SQL Enterprise ^[2]		Microsoft RDS		Red Hat Enterprise Linux	Bring Your Own Subscriptions
	£ / hour / VM	Academic £ / hour / VM	£ / hour / VM	Academic £ / hour / VM	£ / month / VM	Academic £ / month / VM	SAL Licence per month	Academic SAL Licence per month	Subscribe through UKCloud £ / hour / VM	
Micro, Tiny VM	£0.012	£0.002	£0.310	£0.054	£825.00	£195	£4.19	£0.44	£0.04	No charge
Small VM	£0.023	£0.003								
Medium VM	£0.046	£0.007								
Medium High Memory	£0.046	£0.007								
Large VM, Large High Memory, Tier 1Apps	£0.135	£0.020	£0.580	£0.15	£1650.00	£390			£0.09	

Service description G-Cloud 10: Cross Domain Security Zone

^[1] You must choose the same protection option for both VMs and storage.

^[2] SQL Enterprise is bought on a monthly basis: you must report the quantity of SQL Standard and Enterprise licences that you need each month to UKCloud.

^[3] 60GiB of Tier 2 storage is included in the pricing for all VMs while they are powered on. For VMs in powered-off state, consumed storage will be charged at the prevailing rate.

For all services above, billing is per unit or part thereof.

Connectivity options

UKCloud provides one of the best connected cloud platforms for the UK public sector and offers a range of flexible connectivity options that enable access to its secure platform by virtually any government user community or system. The variety of government, public and private networks is shown in the following diagram:

Connection Type	DDoS protected internet	PSN assured	PSN protected	N3	HSCN	Janet	RLI	Hybrid Connect	Crown Connect	Cloud Connect
Metered Usage	FREE	FREE	£250	£250	£220	FREE	N/A	N/A	N/A	N/A
Unmetered Usage	FREE	£2,500	£3,500	£3,500	£3,000	FREE	N/A	N/A	From £200	From £200
Set-up Fee	N/A	N/A	N/A	N/A	N/A	N/A	£2,000	From £2,000	£1,000	£1,000

PSN Protected: Encrypted higher-security Public Services Network. Connected to legacy IL3 networks including GSI, PNN, CJX, GSE, GSX and others.

HybridConnect: Supports a variety of flexible private connectivity options. Enables connection to Crown Hosting (CHDC) and other third-party facilities.

RLI: A high-security network for defence and industry partners. Connection to RLI is subject to extensive vetting and approval from the MoD.

CloudConnect: Enables customers to establish connectivity to UKCloud-approved public cloud providers through peering exchanges or via

PSN Assured: The general-purpose unencrypted Public Services Network. Connected to most central, local and devolved government organisations.

N3/HSCN: : The NHS National Network and its replacement, the Health and Social Care Network. This enables you to connect to all health and social care organisations nationwide.

Janet: The UK's research and education network. Connected to all education organisations and research councils.

Discount and purchase schemes

There are two discount or purchase schemes — see below. You can find full details of each one in our pricing guide.

Option 1: Commitment discount

Commit to spending a specific minimum amount each month for a minimum of 12 months and receive a discount based on the total spend committed.

Option 2: Cloud Credits

Purchase Cloud Credits upfront and redeem them against UKCloud services over a maximum two-year period. This enables you to effectively commit your CAPEX or budget spend in advance, with monthly usage deducted from the balance until depleted.

Trial service

Owing to complex assurance requirements, a trial service is not available.

Service Level Agreement

We understand that UK public sector organisations need a dependable service that demonstrates value to stakeholders, which is why we offer one of the best SLAs on G-Cloud.

What's more, we back our SLA with Service Credits. If we fall short of our agreement, we'll compensate you with Service Credits so that you can be confident that we have a financial incentive to deliver on our promises.

The table below outlines the SLA and Service Credit details. For more in-depth information, see the terms and conditions.

Service level agreement	99.90%
Portal level agreement	99.90%
Availability calculation	Availability is calculated based on the number of hours in the billing month (for example, 744 hours for months with 31 days), excluding any planned and emergency maintenance.
Measurement of SLA	Unavailability applies to the UKCloud Guard or the underlying Cross Domain Security Zone infrastructure due to a fault recognised at the IaaS layer, data centre facilities, physical firewalls or routers.
Key exclusions	The following are examples of what is not covered by the SLA: The fault is within the customer's control (such as VM configuration, customer networks, application logic) Faults within external connectivity providers (for example DDoS-protected internet, PSN, JANET or N3/HSCN) and components co-located at UKCloud.
Service Credit*	10% of monthly spend on the Cross Domain Security Zone. 1% of monthly spend per 1% below service level target or part thereof for the UKCloud API and Portal.

* You will not be eligible to receive a Service Credit if your account has any undisputed payments outstanding beyond their due date or you are in violation of UKCloud's Terms and Conditions including the UKCloud System Interconnect Security Policy (SISP).

On-boarding

Setting up a new customer within the UKCloud Portal will typically be completed within eight hours from acceptance of order.

Customers will have two options when purchasing a CDSZ service.

- A light-touch design review/self-assessment route for customers with simple implementations, or those who are experienced at designing secure solutions.
- An assurance-wrap style approach with UKCloud's experienced professionals for more complex implementations or those customers who would like support and guidance when developing their solutions.

Both options require the same submission documentation to enable UKCloud to provision the service.

When you apply for a CDSZ service, you must provide the following documents to show that you have identified and mitigated for any risks:

- Details of your proposed implementation that covers the intended design in the CDSZ, the Assured and Elevated VDCs you are connecting to and data flows.
- Evidence of acceptance of risk from the data owning organisation.
- An explicit statement that the solution has been reviewed by a named UKCloud Cloud Architect or that you do not require a review.
- If you're connecting to a PSN Protected enabled VDC, proof of PSN compliance

Validation of inclusion of appropriate documentation for a self-assessment service request will happen in 4 hours.

Deployment time following validation is 5 days. This includes the setup and configuration of customer specific firewall requirements.

UKCloud will create the customer's Primary Administrator account and send the customer a Welcome Pack which includes the URL for the UKCloud Portal for access to the Knowledge Centre and service management function.

Once enabled, the customer's Primary Administrator can create additional administrator users and configure the Cross Domain Security Zone virtual data centre (such as virtual networks, virtual firewalls, virtual machines, OS provisioning and application configuration) as required.

Resources to support the assurance wrap approach activity will be assigned within 10 days of order acceptance.

Due to the variable nature of this service, full onboarding of the customer organisation including enrolment of all users and end-user devices will take an indeterminate amount of time.

If you choose an assurance wrap review for your proposed implementation, the UKCloud compliance team and Cloud Architects will work with you to help identify risks on your platform. This includes:

- Review of design and data flow with a Cloud Architect.

Service description G-Cloud 10: Cross Domain Security Zone

- Advice and guidance for how to design secure solutions
- Conversation between UKCloud SIRO and customer SIRO or nominated representative covering risk management and mitigation
- Review of ITHC scope and summary with a Cloud Architect

UKCloud takes no ownership or responsibility for the implementation or running of components specific to the customer's own solution or ownership for any risks to the data.

UKCloud reserves the right to charge SFIA day rate charges for time spent on customer projects if you disengage with the assurance wrap review process before completion.

Vysiion will provide a number of videos, help guides, manuals and FAQs to help train and instruct users so that they are up and running quickly and easily. These are also available within the Knowledge Centre, accessed via the portal.

In addition, you will be assigned a Service Delivery Manager (SDM) to provide any assistance required during the first 90 days of the service.

Data Migration

For service migration, UKCloud allows existing data to be migrated to and from the Walled Garden virtual data centre.

Vysiion can also help facilitate a bulk migration to the platform using offline data ingest and extraction — please ask Vysiion for details.

Service Management

If the customer requires it, Vysiion can assign an experienced, ITIL qualified SDM. The SDM will provide additional assistance with reporting, incident escalation and continual service improvement, following Vysiion's ITIL aligned service management framework and established processes.

Vysiion will allocate an Account Manager (AM) to provide you with an assigned point of contact. The AM will provide additional assistance with reporting and incident escalation, at all times following UKCloud's ISO20000-certified ITIL-based process framework.

For organisations that require a managed service, we can provide value-added services such as consultancy, training, support and on-going custom managed services.

Service constraints

The UKCloud Cross Domain Security Zone can be used only for connectivity between UKCloud services such as Enterprise Compute Cloud and Hadoop in the Cloud.

The constraints below will be applied as standard to the UKCloud guard. For customers purchasing the walled garden, UKCloud strongly advises that those using this service apply the following constraints to protect their own applications and data:

- Configuration and management of application services in both the low- and high-security domains must be hardened, with regular security patches applied
- Application services must use appropriate anti-malware software which is regularly updated

Service description G-Cloud 10: Cross Domain Security Zone

- Only specified traffic types will be allowed via a UKCloud-managed whitelist
- The data owning organisation must understand and accept the residual risks associated with this solution

UK Cloud will adhere to the following in terms of maintenance windows:

‘Planned Maintenance’ means any pre-planned maintenance to any of the infrastructure relating to the service. Planned Maintenance activity may result in periods of degradation or loss of availability depending on the nature of the activity required. In such cases, UKCloud shall provide affected customers with at least fourteen (14) days' advance notice of the Planned Maintenance.

If during Planned Maintenance there is a loss of availability outside the scope described in the planned maintenance notification to the service, an SLA event will be triggered, but excluded from Service Credits.

‘Emergency Maintenance’ means any urgent maintenance required to prevent or mitigate against any event compromising the infrastructure relating to the service. Whenever possible, UKCloud shall: a) provide affected customers with at least six (6) hours' advance notice and b) carry out the emergency maintenance between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday or between the hours of 08:00 and 20:00 (UK local time) on Saturday, Sunday and bank holidays unless there is an identified and demonstrable immediate risk to customer environment(s). Emergency Maintenance may result in periods of degradation or loss of availability depending on the nature of the activity required.

If during Emergency Maintenance there is a loss of availability to the service, an SLA event will be triggered. This time will be excluded from the availability calculation but will be included in monthly service reporting related to the service.

Technical requirements

Customers must ensure that systems in both security domains meet the requirements of this service:

- Recommended use of a CPA-approved data-at-rest encryption solution
- Recommended use of anti-malware software (regularly updated) to reduce risk of malicious code execution on the servers
- Recommended use of an enterprise audit and monitoring service by the customer organisation to ensure security events are centrally logged and reviewed
- Recommended implementation of an Incident Response plan by the customer organisation to respond to security incidents such as loss of data confidentiality

Customers will require appropriate network connectivity such as DDoS-protected internet access or accredited connectivity such as a government secure network to the UKCloud platforms. Connectivity via the DDoS-protected internet, a government secure network (PSN, JANET or N3/HSCN) or private leased line is available but may incur additional charges if the hosting of CPE routers is required — see the pricing section for more details. Where they are required, customers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

Customer responsibilities

The control and management of access and responsibilities for end users including appropriate connectivity, security and accreditation if required. If access is required over Government Secure Networks such as N3/HSCN, JANET, RLI or PSN (including legacy networks), the customer is responsible for adhering to the Code of Connection (CoCo) and for providing evidence of their CoCo to UKCloud upon request. UKCloud is unable to provide access to secure networks where such evidence had not been [provided by the customer].

Satisfying their customer and internal assurance teams that suitable technology controls in both the low-side and high-side domains (such as Protective Monitoring, anti-malware and security patches) will be implemented and maintained.

We recommend ensuring a suitably scoped IT Security Health Check against the application using the Cross Domain Security Zone is performed.

We recommend keeping evidence that suitable and ongoing assurance process and governance regime are implemented and maintained to ensure that risks are regularly reviewed and controls are regularly audited for effectiveness.

Providing access requirements between the Cross Domain Security Zone and customer solutions (firewall ports).

Managing security incidents related to the use of this service (for example, data breach).

The customer is also responsible for ensuring only lawful data that supports the UK public sector is stored and processed by applications on this environment, and that they fully comply with the UKCloud Security Operating Procedures (SyOPs) and other information assurance requirements as specified in the UKCloud System Interconnect and Security Policy (SISP) and associated accreditation documentation sets.

Termination

Terms

The Guard option is subject to a minimum term of one month.

The Walled Garden option is subject to a minimum term of one month.

Customers are required to provide notice of termination of not less than 30 working days.

Customers using Global Load Balancing or Application-tuned DDoS protection service options have a minimum term of 12 months for these specific services.

At the point of termination, customers must ensure that they have extracted any required data from the Walled Garden virtual data centre as UKCloud will ensure all customer data, accounts and access will be permanently deleted. These will not be able to be subsequently recovered or restored.

Costs

An Early Exit charge will be payable if the UKCloud Guard contract is terminated within the minimum term. The Early Exit charge will be equal to the cost of three months' service less payments already made.

There are no termination costs for the Walled Garden. Customers are responsible for extracting their own data from the Enterprise Compute Cloud service if required.

Customers are responsible for extracting their own data from the platform if required.

UKCloud may make an additional charge for transferring data out of the service.

Offboarding

Prior to terminating the contract, the customer is able to transfer all their data out of the solution (for example using the UKCloud API to retrieve data).

When the organisation terminates its agreement with UKCloud, UKCloud ensures all of the organisation's data is deleted.

Ordering and invoicing

The service can be ordered via the G-Cloud Framework and must be supported by a valid purchase order.

The client can engage with Vysiion either by:

Email to cloudsales@vysiion.co.uk

Telephone: 01249 446500 and ask to speak to the G-Cloud sales team.

Following detailed discussions about your requirement Vysiion will assist you to develop the G-Cloud Call-Off order to meet your requirements.

Billing for the service is monthly in arrears based on either the amount of traffic sent through the UKCloud Guard or the consumption of resource during the month for the Walled Garden.

Vysiion will issue invoices as follows:

- At point of order for up-front fees and service options
- Annually in advance for pre-payment fees
- Monthly in arrears for monthly fees

We are able to use a range of electronic purchase and payment systems.

Conclusion

Vysiion has a full complement of cloud services to take you on a journey from initial idea through to the transformation of your IT through cloud.

Whatever your goals, Vysiion will work with you to get to your destination.