So, what the heck is Hyperscale SECRET Cloud?

MODCloud's SECRET Cloud team are busy working the next big cloud capability, which we are calling 'Hyperscale SECRET'. However, this term is proving to be a little confusing! *So, what is Hyperscale SECRET Cloud really and what is it **not**?*

The short version is:

> *"Hyperscale SECRET Cloud is something that looks and feels like a Public Hyperscale Cloud when used but is suitably assured for workloads at SECRET."*

But this statement alone doesn't help lift the confusion, so keep reading...

Is it a Public or Private Cloud?

Neither.

It is a Community Cloud. See the **National Institute of Standards and Technology (NIST) Cloud Computing Definitions (www)** to find out more.

Public Cloud is truly 'public', meaning anyone can use it, including you. When we run workloads in true Public Cloud (e.g., Amazon Web Services (AWS), Azure, Oracle Cloud, or Google Cloud Platform), they could be running alongside any public workload or service. This includes things like Netflix and XBoxLive but also MODCloud OFFICIAL services.

Private Cloud is for a single organisation. If Hyperscale SECRET was only intended for MoD, then it would be, by definition, a Private Cloud. However, it's not; Hyperscale SECRET is for a community of customers who have a legitimate need to run SECRET workloads. This can include other government departments, agencies, or suppliers.

Will it be just like Public Cloud?

We aspire to get it as close as possible to a Public (Hyperscale) Cloud experience for customers, however there may well be some sacrifices and compromises along the way. The NIST definition describes Cloud as having Rapid Elasticity and appearing to be 'unlimited' to customers, in practice Hyperscale SECRET will be slightly less 'elastic' and 'unlimited' than true Public Cloud. However, all terms are relative and Public Hyperscale providers aren't 'unlimited' either - some occasionally run out of capacity!

The real benefit of Hyperscale Public Cloud though is the provision of services. These are the things that make Hyperscale desirable and have come to be part of the definition of Hyperscale for us because services are where the real value of Cloud lies. They enable agility in development and can include things like databases, cognitive services (artificial intelligence) and language services (e.g., translation). Most Public Hyperscale Clouds have hundreds of services; for SECRET Hyperscale we want a Cloud that is rich in services, but we accept that we might not be able to provide, and there might not be demand for all of them. We also accept that there might be a lag between a new service going live in a Public Hyperscale Cloud and a SECRET Hyperscale Cloud to make sure they are suitable for the environment.

Why not just use Public Cloud?

The **National Cyber Security Centre (NCSC) guidance** (Deployment models: Public cloud, para 5) says that it may be another 10 years before Public Hyperscale Cloud can be used for SECRET workloads. Whilst we think that might be a bit pessimistic, the guidance is clear that Public Cloud isn't yet a suitable platform for generic, utility SECRET Cloud.

Do the NCSC Cloud Security Principles apply?

Mostly.

The NCSC Cloud Security Principles are aimed primarily at Public Hyperscale Cloud and Software as a Service (SaaS), not a SECRET Community Cloud, so they meet a different context. As a set of principles though they are good practice across any cloud environment, but it's likely that in some areas there will be additional controls and principles, and in some cases, they may not make sense.

Is it 'on-premises', and does it matter?

No, 'on-premises' is a term that we avoid as much as possible in MODCloud, as it's often taken as meaning 'more secure, or 'better, when the opposite may be true.

The most secure (and energy efficient!) data centres are run by those who do so at scale as their core business, these are Hyperscale providers. If we take 'on-premises' to mean; on MoD-owned land, then much of our IT infrastructure at multiple classifications is not actually 'on-premises'. Better questions would be:

- *Do we know where it is?*
- *Do we have access rights?*
- *Can we provide suitable assurances of the security of the location?*

Is it secure?

Hyperscale SECRET Cloud is using Secure by Design (SbD) (the MoD's new approach to security assurance) from the offset. This ensures that security is built-in from the start, and tested continuously. MODCloud uses SbD for all its services and will bring experience from MODCloud OFFICIAL to Hyperscale SECRET.

We hope this helps explain a little bit more about what Hyperscale SECRET is. Watch this space for more updates on SECRET Cloud!