Infront's
Secure virtual Data Centre (Secure vDC)
Powered by Azure

1. SECURE VIRTUAL DATA CENTRE - POWERED BY AZURE

Secure networks, such as those found in classified government environments require adherence to strict security controls. Within the context of cloud, these controls manifest into a hub and spoke network topology.

In addition, regulatory bodies require government to have increased security and also well documented governance and processes.

These requirements can significantly delay cloud adoption and consume key resources from high value activities.

To meet these challenges Infront, the Hybrid Cloud company has developed the Secure vDC. A tailor-fit Azure landing zone built for Australian Government at both Official and PROTECTED classifications.

- Accelerate Azure adoption following Microsoft best practice
- Secure by design; Role Based Access Control (RBAC), defence in depth, hardened and battle tested
- Aligned with the Digital Transformation Agency's (DTA) Secure Cloud Strategy
- Engineered to PROTECTED; with all required documentation
- Governance, security and support for successful cloud transformation
- Reduce cloud Total Cost of Ownership (TCO) with the Shared Services Hub
- Focus on business outcomes, deliver faster and deliver with confidence

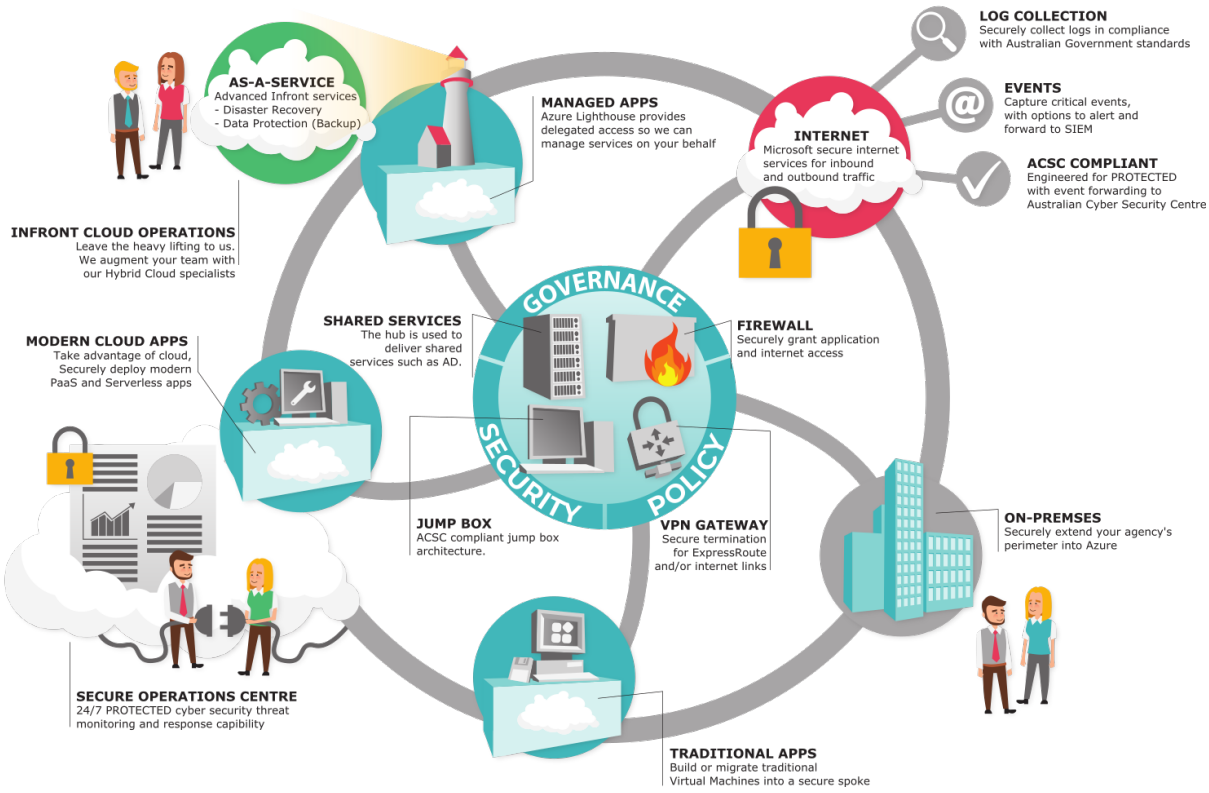

Figure 1 – Secure virtual Data Centre (vDC) – Powered by Azure

2. INTRODUCING THE SECURE VIRTUAL DATA CENTRE

The Secure virtual Data Centre (vDC) brings Infront's wealth of experience in designing and operating hybrid cloud architectures to fast track an agency's adoption of cloud services.

Built on the traditional infrastructure pattern, the Secure vDC extends on-premises data centre into Microsoft Azure while maintaining a strong security posture. Agencies retain governance while taking advantage of the flexibility and efficiencies that cloud has to offer, all engineered at PROTECTED.

Designed and built by Infront, in consultation with Microsoft; the Secure vDC applies our real-world experience to provide agencies with best practice and compliance with the Essential 8 and Australian Government Information Security Manual (ISM).

Deployment is achieved in a matter of weeks, reducing the friction and time to value of cloud adoption. The implementation includes infrastructure patterns based on best practice: defence in depth, policy guard-rails, and operational standards and the complete documentation set for both handover and Information Security Registered Assessors Program (IRAP) security assessment.

With predefined role-based access and policy driven governance, the Secure vDC is more than just a technology blueprint. Agencies are provided with the supporting frameworks, documentation and technology necessary to drive the adoption of DevOps practices.

Infront's highly skilled engineers work alongside an agency, to complete a detailed prerequisites checklist and to understand any specific requirements. This ensures a smooth transition for both greenfield and existing Azure deployments.

Ongoing support is available via our residency program, intended to both uplift and augment existing teams. Our residents work with an agency to manage their Secure vDC day-to-day operations, facilitate accelerated application migrations and provide best practice advice and assistance.

Additional advanced services are available at the click-of-a-button, built to further accelerate your cloud journey and reduce operational overheads. These services are provided by Infront together with our partner ecosystem, some of which include:

- Secure internet access with Australian Cyber Security Centre (ACSC) event logging
- Security Operations Centre (SOC) accredited to PROTECTED
- Data protection with managed Backup as-a-Service
- Disaster Recovery (DR) to or from Azure with managed DR-as-a-Service

We understand cloud while exciting; is simply the supporting foundation for applications that deliver real business outcomes for your Agency. With our Secure vDC, you have the confidence to successfully deploy and support these applications rapidly and securely.

3. FREQUENTLY ASKED QUESTIONS (FAQ)

Q. What is the Secure vDC?

A. The Secure Virtual Data Centre builds on the traditional secure data centre pattern, extending it into Azure.

Q. Why you need it?

A. The Secure vDC allows agencies to rapidly adopt the whole of government secure cloud strategy by establishing a landing zone for both new and existing workloads. This extends their on-premises capability into the cloud while maintaining best practice and compliance with the ACSC ISM.

Q. What does it let you do?

A. The Secure vDC enables agencies to take the next step on their cloud journey, establishing a landing zone with the appropriate governance.

Q. What you get?

A. You get your own Secure vDC in Microsoft's Azure with best practice-based Role Based Access Control (RBAC) and ISM compliant Azure Policy pre-established.

Q. How do you connect?

A. Agencies generally connect to the Secure vDC via Microsoft's ExpressRoute, seamlessly extending on-premises to the Secure vDC. Connections are encrypted in line with ACSC standards. A Secure Internet Gateway can also be deployed, allowing for cloud-based workloads to securely connect to the internet directly rather than being routed by on-premises equipment.

Q. What is included?

A. Pre-deployment discovery activities, deployment, and configuration of your Secure vDC and the Standard Operating Procedures (SOPs) and documentation required for an IRAP.

Q. What is excluded?

A. Physical peering devices, ICON links and cloud costs.

Q. How much will our Azure bill be?

A. The Azure cost will depend substantially on each agency's exact deployment configuration. ROI increases as more spokes leverage the shared services hub. See Azure Cost Calculator - Secure vDC for a rough order of magnitude pricing.

Q. Can I put a cap on my Azure spend?

A. Azure has basic cost management features to help track cloud spend, however, Infront recommends Buttonwood for full financial governance and cost analysis.

Q. Can you manage the solution for me?

A. Yes, Infront can provide the Secure vDC as a fully managed service.

Q. What if I need extra support after the project is complete?

A. Infront recommend our residency service to assist with handover and ongoing cloud operations.

Q. I have an existing ExpressRoute and Azure subscription, is that a problem?

A. No, **t**he Secure vDC can be deployed in parallel or as a replacement.

Q. We have our own Server SOE, can we use that in the Secure vDC?

A. Yes, while Infront puts an emphasis on minimising the use of VM based Infrastructure in favour of utilising Azure managed services, SOEs can be converted to Azure Images and uploaded.

Q. What speed ExpressRoute do I need?

A. As part of the Secure vDC project Infront will perform discovery activities that will determine, among other requirements, your bandwidth and performance requirements.

Q. How long will it take to deploy?

A. While the Secure vDC can be tailored and deployed in a relatively short period, there is a dependency on ICON or alternate networking providers outside of Infront's control. When not considering those network dependencies the Secure vDC can generally be implemented within 6 weeks.

Q. After I have deployed the Secure vDC what's next?

A. Infront can assist with a wide range of services, from advisory through to migration and application development.

Q. Can I have the Secure vDC in more than one region?

A. Absolutely. As part of the initial information gathering stage Infront engineers will work with the Agency to understand their requirements and design the best implementation for them, including multi-region Secure vDC establishment.

Q: Can this solution support PROTECTED and OFFICIAL?

A: The Secure vDC was specifically designed to meet PROTECTED and OFFICIAL Government requirements. All documentation relating to the infrastructure that is required to undergo an IRAP certification is included.

Q. What is the managed Security Operations Centre (SOC)?

A: Our partner, PCG, provides a 24/7 PROTECTED cyber security threat monitoring and response capability, managed by cyber security experts. Leading technology helps to identify and mitigate insider and external threats.

Q. Is the Secure vDC for me if I'm not a Government agency?

A. Yes, the Secure vDC is intended to be a fast track to a landing zone built in Azure, it's equally as applicable in private enterprise.

4. WHY INFRONT

Infront is a locally based system integrator with over 20 years' experience working with secure government agencies in and around Canberra. We are an international award-winning business with enviable track record in the successful delivery of next generation hybrid cloud solutions. Infront has been recognized by industry leaders such as Microsoft, Nutanix and Dell EMC for our specialist skills and commitment to customer success.

We are an acknowledged leader in hybrid cloud solutions, with a deep understanding of Microsoft Azure and Microsoft Modern Workplace; with a wealth of real-world integration and deployment experience. We have a proven track record in delivering scalable and highly resilient solutions that support some of the Australian Governments most critical, most complex and most secure application workloads.

Infront offer advisory, integration and ongoing support services; ensuring we can assist of all aspects of hybrid cloud adoption from design to build to run.

Specifically, in partnership with Microsoft we have developed accelerator service offerings built explicitly to support and to assist Government with their hybrid cloud journey including:

- Hybrid Cloud Operating Model (mitigate business risk with policy and process)
- Secure Virtual Data Centre (secure landing zone engineered to Protected)
- Infrastructure as-a-service (cloud connected on-premises infrastructure)
- Desktop as-a-service (Modern Workplace leveraging Microsoft 365 technologies)
- Disaster Recovery as-a-service (powered by Azure Site Recovery)
- Cloud Operations as-a-service (operationalise cloud with a consistent delivery model)

Gold
Microsoft Partner
Microsoft

5. CALL TO ACTION

Government agencies are keen to accelerate cloud adoption to take advantage of modern and innovative technologies.

The Digital Transformation Agency (DTA) Secure Cloud Strategy explores the key benefits for government.

- increase the speed of delivering new platforms
- allow for continuous improvement
- provide easier access to services
- reduce the effort needed for maintenance and allow agencies to focus on improving service delivery

However, existing infrastructure and audited security and regularity requirements put additional strain on already stretched ICT business units. Further, without operational procedures and governance failure of cloud projects and cloud adoption are certain.

The Secure vDC is your turnkey solution for a successful cloud transformation in Azure.

Book you Secure vDC information session today to learn more.

Canberra office

49/14 Trevillian Quay
Kingston ACT 2604

P (02) 6239 8400
F (02) 6239 8411
E salessupport@infront.net.au
W www.infront.net.au

Infront Systems Pty Ltd
ABN 72 084 698 699