

# Secure Virtual Desktop as a Service based on VMware Horizon

## The Problem

Government and Critical National Industries (CNI) communities have an urgent need to enable their entire workforce to work from remote locations. While many departments have the capability to enable some of their staff to work remotely, few have the capability to cater for larger scale adoption.

## Proposition

Based on VMware's world leading Horizon® 7, Insitec and AUCloud have deployed a sovereign remote desktop solution (Remote Government Desktop Service) designed to meet ASD's ISM controls for data classifications at Official, Official:Sensitive and Protected. The service supports concurrent users from as little as one hundred to several thousand users. Delivering the features and benefits of one of the world's leading virtual desktop solutions underpinned by Australia's leading secure, sovereign cloud IaaS providers, the AUCloud/Insitec remote desktop solution ensures customer data is never compromised.



## Features and Benefits

Key features of the Remote Government Desktop Service delivered by Insitec on AUCloud geo-resilient sovereign operated infrastructure, include:

- **VDI Desktops** based on Microsoft Windows 10
- **Streamlined deployment:** Deployment can take as little as 60 minutes, based on configuration complexity.
- **Single management pane:** Dual zone deployments can be managed from a single management console.
- **Simple upgrades:** VMware provides a simple blue-green upgrade method that allows a pain free upgrade release pathway.
- **Schedule-based power management options for VDI dedicated and floating desktops:** Schedule off an assignment of VDI desktops for weekends, holidays, and non-working hours - cost savings and enabling scheduling of higher minimum desktop counts for high-demand periods.
- **Rolling maintenance and image update:** Includes built-in orchestration to enable rolling maintenance of RD Session Hosts.
- **RD Session Hosted applications:** Supports RD Session Hosted applications and desktops with initial release.
- **Cloud and cyber monitoring:** All deployments underpinned by AUCloud's world leading cyber monitoring technology supported by Insitec's trusted services for additional security assurance.
- **User Environment Manager (Dynamic Environment Manager):** Personalisation and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment for additional flexibility.
- **Low-cost monthly billing:** Consumption-based highly competitive pricing for capacity, with no termination fees.

The Insitec/AUCloud solution provides Federal Government:

- Flexible pricing to scale from 100-1000 or more users, for rapid operationalisation
- Desktop service performance levels available to match your workforce's requirements.
- Dedicated ESXi hosts, vCenter and Security servers (VMware Unified Access Gateway) for each government customer for enhanced security.
- Desktop services via individual Internet facing URL's (unique per tenancy) enabled through dedicated VMware Horizon View Gateways for easier adoption by dispersed organisations.
- ICON or CDC data centre cross-connect for rapid integration of existing CDC Customers.
- 2 Virtual firewalls per tenancy, providing bespoke controls to meet security needs.
- Private network cross-connect via internal firewall.
- 2FA and cyber threat monitoring within a restricted community.

## Key conditions that currently apply to the solution

In order to rapidly mobilise this service for government use we have applied the following restrictions -

- VDI desktop OS is currently restricted to Windows 10 only
- The Services outlined are to support and deploy a single "Gold" image. Additional images are available upon request.
- No persistent storage is allocated to a Virtual Desktop. We assume that departments will expose their internal corporate data locations to the hosting environment through the connection methods outlined above. *No local storage with initial deployment as assumed provided through Customer environments*

## About

AUCloud is a sovereign cloud IaaS provider, exclusively focussed on meeting the needs of the Australian Government and Critical National Industry (CNI) communities and independently IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM). AUCloud is also ISO27001 certified across the whole organisation, is VMware Cloud verified and recognised as a Cisco Master Partner for Cloud and Managed Services. Through two independent geo-resilient environments based in CDC data centres in Canberra and Sydney, AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

Insitec is a growing and dynamic Canberra based business that has been supporting government for over 19 years. Insitec has proven commitment to government security standards and among many innovations, has developed PROTOS secure cloud technology, with fully embedded with ISM and PSPF security controls to support up to Official:Sensitive and PROTECTED workloads at an Infrastructure, Platform and Application Layer.