Sovereign Data Protection for Remote Working

Government and organisations in critical national industries made a dramatic leap to implement or extend remote working this year and will likely integrate aspects of this into long-term strategies. Virtual desktops are a key enabling factor for many of these organisations, and that makes it even more important that their IT infrastructures comply with Australian data security and privacy requirements.

The Australian National University (ANU) made the transition within a two-week period, implementing a virtual desktop as a service (VDaaS) solution from sovereign cloud IaaS provider AUCloud, a VMware Cloud Verified Partner. That quick response allowed the University to provide capacity for about 20,000 students to remotely access their ANU teaching labs to continue their education amidst the COVID-19 pandemic.

When stage three lockdown measures were implemented mid-semester in March 2020, ANU needed to quickly transition students, staff, and lecturers from on-campus learning to a remote platform with the same level of functionality and access to resources. In just one week, a small multidisciplinary team, comprised of staff from ANU and teams from partners AUCloud and Insitec, implemented a turnkey solution that allowed the University to move its operations online via remote access.

The ANU virtual desktop built by AUCloud enables access to over 120 applications with the same user experience as on campus whilst also maintaining visual consistency and service support to ensure curriculum continuity. AUCloud is based on VMware technology, so leveraging the VMware Horizon 7 platform for the ANU VDaaS was an obvious choice.

Horizon 7 is built on technologies that allow components of a desktop or application to be decoupled and managed independently in a centralised manner—yet reconstituted on demand to deliver a personalised user workspace. The solution provides a consistent user experience across devices and locations while keeping enterprise data compliant and securely protected and stored in a highly secure environment. End users can access their personalised virtual desktops or remote applications from organisation laptops, their home PCs, thin client devices, Macs, tablets, or smartphones.

AUCloud provides highly secure, standards-based, sovereign cloud IaaS to the Australian Government and Critical National Industry (CNI) communities. This includes Federal, State, Territory, and Local Governments and CNI organisations such as telecommunications, electricity, energy, financial services, and similar utility providers (amongst others).

Wholly owned and operated by Australians, AUCloud ensures that the data it hosts never leaves Australia. That includes customers' data, metadata, analytics, and monitoring data. As a sovereign cloud company, it is subject only to the laws of Australia and not to any extra-territorial requirements that could result in a foreign entity or government requesting access to data. AUCloud is IRAP-assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM).

AUCloud operates from geo-resilient certified sovereign Data Centres in Canberra and Sydney; both built to ASIO T4 standards for Zone 4 security. AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity, and lower costs typically associated with global cloud offerings.

AUCLOUD

vmware CLOUD VERIFIED

IDG

Learn more about AUCloud's VDaaS solutions here.