CASE STUDY

SecureCloud+

SecureCloud+ accelerates secure remote working to RLI connected Collaborative Working Environment powered by UKCloudX

About SecureCloud+

SecureCloud+ is a trusted provider of secure communication and collaboration services for Defence and Government. Users are given access to their networks, resources and applications using secure solutions delivered as an end-to-end managed service.

The Company is already delivering multi-year contracts to public sector customers for managed service at all tiers of the government's IT security classification system, including TOP SECRET.

SecureCloud+ is constantly seeking to leverage advances in technology such as data visualisation, artificial intelligence and machine learning to deliver modern ways of working whilst still exploiting the investment in legacy systems. The Company's expertise in developing these technologically advanced solutions, managing complex projects and protecting secure networks has led to an enviable record for delivering on time and within budget.

The Challenge

Government and Public Sector Departments were required to maintain business continuity whilst working within the Government IT Security Classification Policy and to enable access to shared office systems, all while working from home.

The 'normal' is for users to work from secure, centralised facilities. Due to these circumstances, an accredited end-to-end managed service was required so users could securely access data from various devices whilst working from home. Business continuity needed to be maintained to support the fundamentals of the economy and to ensure an eventual orderly transition back to normality.

As several Government and public sector departments shift towards remote working, there was not enough secure IT in place to manage the demand for remote users. Thus, users run the risk of not being able to work at all or taking unbounded security risks whilst communicating.

Secure and scalable data hosting is important

The service required scalability to handle changes in the number of users or required functionality. It must also allow these users that already have access to Government issued secured IT to share information with other users who may only have access to their own enterprise or personal IT systems. Documents and shared files were required to be accessible by authorised users within a secure hosting environment.

Critically, the service's data must be held within an accredited, managed hosting environment that conforms with the security compliance and regulations of the classification of data (e.g. OFFICIAL-SENSITIVE).

UKCloud Products and Solutions:

UKCloud's mature and proven Cross Domain Security Zone helps users achieve the goals of the Government Digital Strategy. UKCloudX have unparalleled heritage working with the National Cyber Security Centre and maintains the people, process, premises and technology controls that enabled our platform to be one of the few to have achieved Pan Government Accreditation to IL3 (IL4 by aggregation) and to connect MoD networks such as the RLI.

CASE STUDY

The Solution

SecureCloud+'s Managed Mobile Information Service (MMIS) enables users to access data and share office automation systems from a registered personal IT device, and jointly collaborate with users who have a Government secured IT device.

UKCloudX provided the underpinning elastic cloud compute and storage technology, connectivity to RLI, the cross domain security zone and the government grade crown campus delivered through secure and compliant processes. UKCloudX's domain expertise in Defence reduced the risk, accelerated the time to value and delivered an affordable solution for SecureCloud+.

The MMIS end-to-end secure managed service from SecureCloud+ has already provided a communication and collaboration environment for Government personnel across several locations to create, store and share content securely, delivering efficiency gains and cost reduction.

"Users can access the secure hosted environment from their own device at work or at home"

The service is elastic and can be scaled up or down as demand changes, due to UKCloudX's flexible compute and storage billed on consumption on a pay-as-you-go model which provides value for money for the end user.

MMIS is accredited by the MOD at OFFICIAL-SENSITIVE, and allows users to create, store, and collaborate on documents on their personal devices, while continuing to meet national security and critical infrastructure priorities. Extra security is provided through two-factor authentication.

SecureCloud+ built the service to operate remotely, and therefore requires no face to face personal interaction, which is essential for maintaining compliance with the UK Government's mandate to work from home where possible during the current COVID-19 crisis.

Rob Gittins
COO of SecureCloud+

"We required a cloud hosting partner who would quickly provide us with a secure data environment for UK Government employees to collaborate — UKCloudX provided unparalleled choice, assurance, connectivity and support which enabled us to tailor a solution that best suited our requirements."

Sovereignty and assurance are critical

"UKCloudX assured the security of our service's data with their UK government grade datacentres, and unique connectivity solutions."

A shared understanding of the public sector

"We value our relationship with UKCloudX, based on our shared mission to help the public sector make transformation happen."

Results Achieved

- Users working for Government departments can access the secure hosted environment from their own device at work or at home
- Accredited by MOD at OFFICIAL SENSITIVE, enabling secure connectivity
- Users can create, store and collaborate on documents up to OFFICIAL-SENSITIVE using their personal devices
- Business continuity, ensuring the support to our National Security
- Compliance with UK Government's mandate to work from home where possible in the event of a national crisis
- Elastic and can be scaled down as the demand reduces, delivering value for money
- No face to face contact required due to remote configuration capabilities