2019 Sautter Award Submission

Project title: Partnerships that scale - innovation to enterprise

Submitted by: Kristin Chu, Director, UCSF School of Medicine Technology Services, kristin.chu@ucsf.edu

Project team:
UCSF IT Security
School of Medicine, Technology Services (SOM Tech)
UCSF IT Academic Research Systems
Center for Digital Health Innovation (CDHI)
UCSF IT Infrastructure and Network
Bakar Institute for Computational Health Sciences

Synopsis:
A strong bimodal approach toward technical innovation and a commitment from cross-functional teams to solve difficult - sometimes contentious - problems was required to move UCSF quickly and securely into the AWS research cloud (ARC). The journey of ARC from many individual researchers needs to a multi-client supported pilot to an enterprise-supported service model represents not only a technical achievement but, more importantly, a bimodal orientation toward technical innovation at UCSF. This was successful through key partnerships, IT Governance, change management, and a commitment to technology innovation from UCSF leadership.

UC's system-wide agreement with AWS, signed in 2016, was a catalyst for driving an 18-month effort to create a secure, compliant cloud computing infrastructure for protected health information (PHI), which was beyond the skill and effort of most individual researchers or departments. SOM Tech worked closely with partners both in central IT (Security, Infrastructure and Network, Academic Research Systems) and individual departments with a large need for secure AWS services (CDHI and Bakar), to co-develop a pilot solution that would allow autonomous cloud-based research innovation at UCSF while aligning with larger enterprise goals and needs for secure, compliant research computing.

Description:
Over the last few years researchers at UCSF have increasingly looked to cloud providers such as Amazon Web Services (AWS) to meet computing challenges that require services not currently available in enterprise solutions. To fulfill that need, the project team followed a collaborative bimodal approach and engaged a range of expertise - from security to research systems to engineering – as we explored and experimented with secure cloud solutions for PHI while simultaneously preparing the existing business to scale cloud use safely and efficiently.

Challenge	Solution	Shared Responsibilities	
		SOM Tech	**UCSF IT**
Meet UCSF security and compliance requirements for P4 restricted data.	Build an architecture that takes advantage of AWS native and third-party services to address NIST requirements. Work collaboratively with UCSF IT Security throughout the project to continue to meet privacy and security requirements and ensure IT Security is confident in the platform's security.	Integrate IT Security and SOM Tech team members in architecture and planning from the beginning.	Integrate IT Security and SOM Tech team members in architecture and planning from the beginning. Lead enterprise monitoring solution.
Provide access to enterprise security and data resources like Big Fix, EMR, and data warehouse.	Develop new networking methods that extend the UCSF network to the cloud without exposing internal resources to additional threats.	Test departmental resources.	Lead architecture and development.
Allow researchers to work autonomously within a dedicated environment.	Architect the solution from the ground up to take advantage of AWS nesting accounts. Set enterprise account permissions at an overarching level so research accounts inherit appropriate permissions and researchers can work autonomously but with safeguards.	Pilot multiple account structures to determine which meet business requirements.	Lead the integration of the pilot into the enterprise AWS account.
Add minimal costs to the researchers/cost efficient solution.	Implement DevOps best practices to automate security monitoring and remediation, environment set up, etc. Take advantage of enterprise security tools like BigFix to standardize operations wherever possible.	Build DevOps into the pilot from the beginning.	Lead driving operations to scale through standardization of practices and commitment to ITIL practices.

The ARC project started with a proof of concept phase in the fall of 2017. Sample architectures of four solutions were reviewed with UCSF IT Security and other IT leaders. In addition to funding from the SOM Dean's Office and UCSF IT, we received support and guidance from IT Governance to move forward with our proof of concept. The team consulted with UCSF's Academic Research Systems team to ensure ARC was empowering researchers and meeting their needs. We also worked closely with security and compliance colleagues to address risk since this effort was one of the first at UCSF to support P4 restricted data in a cloud computing environment. By March 2018, in partnership with UCSF's Center for Digital Health Innovation (CDHI), the team moved one CDHI proof of concept forward to the prototyping stage.

Building on the POC's momentum, the project team requested and received funding from the Executive Vice Chancellor and Provost's Strategic Initiatives funding in March 2018 to grow the ARC platform into a multitenant environment. At the same time, we began identifying what a long-term enterprise solution would look like and how that service would integrate with UCSF's network, operational processes, and existing security tools.

In April 2018, ARC version 1.0 was approved by security and compliance groups and officially went into production.

Our first client, the Bakar Institute's Information Commons, went live in August 2018 with additional clients added through the fall and winter. The ARC platform gives UCSF researchers the ability to set up their own environments within a secure AWS platform. Under this structure, researchers can quickly and autonomously deploy complex projects with restricted data while being integrated into ARC's security and compliance cloud controls. Platform operational improvements are continuously being addressed, and the team intends to release new researcher services about 3 times per year. With over 20 users across 4 separate use cases, we've improved efficiency by automating the environment setup, security monitoring, and operational support.

The team's final, most impactful phase of work required the efforts of everyone on the project. In the spring of 2019, we took on the massive challenge of UCSF network integration. This groundbreaking work allows access to key data sources commonly used for UCSF research, including electronic medical records and data warehouses. Furthermore, the integration allows ARC to be monitored by enterprise security tools and ensures security standards are up to date without exposing the network to outside threats. UCSF IT Security continuously provides security consultation, and proposed solutions are always informed by security reviews.

The impact of the program at UCSF has been twofold. Not only has reaction from individual researchers been positive, but we have also started to transform the platform into an enterprise IT solution, putting it on the same pathway as other bimodal approaches such as the Wynton high-performance computing environment. We received nearly 40 cloud computing inquiries from UCSF researchers in the last two years, and ARC clients have reported that the ability to quickly set up their research data has allowed them to remain focused on their work instead of the intricacies of setting up a secure cloud platform on their own and perhaps incorrectly. Project funding requests have been well-received, indicating support and commitment to cloud innovation from IT and university leadership. Innovation is never an easy path, but, because of a strong commitment from every team member, ARC enables researchers to continue to meet UCSF's mission.