Trusted CI Success Story
UC Berkeley

UC Berkeley was looking for experts in higher ed cybersecurity and found Trusted CI

The Research IT team at the University of California at Berkeley knew the time had come to develop a more secure computing platform for its researchers, especially the ones who work with large and highly complex data, like genomes, and sensitive data, from fields like public health. COVID-19 research has added an extra layer of urgency to protecting university research from bad actors.

"We had been building the case to provide better security for our researchers for two or three years. We were working closely with the university's Information Security Office and outside security consultants," said Chris Hoffman, associate director of Research IT at UC Berkeley. "But what we were lacking was the scientific and cyberinfrastructure experience from higher education institutions who could help us balance out and review the recommendations from the consulting firms."

When funding for the Secure Research Data and Compute (SRDC) platform came through in October of 2019, UC Berkeley was able to tap into the expertise of multiple universities involved in Trusted CI, the National Science Foundation (NSF) Cybersecurity Center of Excellence. Trusted CI partners include Indiana University, the University of Illinois, the University of Wisconsin-Madison, the Pittsburgh Supercomputing Center, and the Lawrence Berkeley National Laboratory.

"Trusted CI had people who had gone through the process of implementing robust and highly secure scientific infrastructure at their campuses," emphasized Hoffman. "They gave us the perspective and experience in higher ed that we needed, especially as we worked to build confidence with university officials and faculty researchers on our campuses. We needed them to realize they could trust us with their research and data."

Trusted CI technology recommendations to improve the SRDC platform included design, storage set-up, firewall configurations, security plans, and architecture.

Trusted CI also helped UC Berkeley develop policies, procedures, and best practices in regard to health information and data privacy. "With sensitive data, there's a lot of regulations and rules that govern what you can do, such as FERPA, HIPAA, and Europe's GDPR, which has even tighter controls. We also work with companies who have intellectual property that needs to be protected in order to partner with them," explained Hoffman.

For high performance computing service providers that support NSF-sponsored research, pursuing compliance also diverts resources. External help can reduce the impact, especially for providers tackling compliance for the first time.

UC Berkeley Sather Gate

"We met weekly with the Trusted CI team online and we became part of a network and a community. We knew we were doing the right thing and working with the right people. We worked with experts from multiple institutions, so we felt comfortable that we were making the right decisions," Hoffman added.

When it was time to deliver the 21-page Trusted CI report to university officials in March, the normally in-person presentation had to be delivered online due to the 2020 pandemic. "The presentation went great and helped us build trust with faculty and researchers. They understand that UC Berkeley is not alone in developing secure cyber technology, policy and procedures," Hoffman said.