

Thomas Jefferson University



Philadelphia's Thomas Jefferson University (TJU) is an academic health center comprised of six colleges and schools, including Jefferson Medical College. TJU offers undergraduate, graduate, post graduate and first professional courses and degrees to over 3,500 students focused on earning healthcare-related degrees. Of TJU's over 2,000 medical school faculty, many also practice within the physician practice group (ranging from family and community medicine to complicated surgery) and have admitting privileges to the affiliated teaching hospital.

CHALLENGE

TJU needed an encryption solution that would:

- › Encrypt data across a variety of desktops and laptops, on both Windows and Mac OS
- › Deploy quickly and transparently
- › Help comply with regulatory requirements
- › Encrypt student data within files sent electronically out the university
- › Integrate with their existing systems management tools
- › Provide a single management interface

BUSINESS PROBLEM

In response to Health Information Technology for Economic and Clinical Health (HITECH) Act mandates, as well as requirements to protect student data under the Family Education Rights and Privacy Act (FERPA), the university sought an encryption solution that would provide safe harbor from public disclosure if any sensitive healthcare, medical research, faculty or student data were compromised. TJU focused initial data protection efforts on devices used by 1,000 faculty (including physicians, nurses and other healthcare workers) and support staff members working within the physician practice group.

"What led us quickly to CREDANT is we that had a large amount of multi-user computers. Disk encryption was not an option for us, because that would force users to share the decryption passwords," recalled David Reis, TJU's Associate Vice President for IT and Information Security Officer. "We needed a solution

that would encrypt the data, but not the disk, so we could have multiple users. CREDANT's was the best-of-breed product to address that need."

Reis' team selected CREDANT's solution not only because it encrypted at the user level but also because it provided the flexibility to remotely deploy CREDANT over their existing Altiris environment, so users did not have to surrender their computers while they were being encrypted.

SOLUTION

TJU uses CREDANT Mobile Guardian Enterprise Edition for Windows and Mac, one CREDANT Mobile Guardian Enterprise Edition Server, one CREDANT Mobile Guardian Enterprise Edition multi-domain server and CREDANT to GO.

"We had a professor who traveled to Europe to present some research, which had not yet been published, so timing was sensitive. His laptop was stolen from his car, but we took comfort in the fact that it was encrypted with CREDANT."

David Reis, Associate Vice President for IT and Information Security Officer, Thomas Jefferson University

Thomas Jefferson University



“The deployment happened so quickly, it was really gratifying. This was truly an easy deployment for something that could have been very disruptive.”

David Reis, Associate Vice President for IT and Information Security Officer, Thomas Jefferson University

RESULTS

CREDANT Mobile Guardian and CREDANT to GO enabled the university to:

- › Encrypt data at the user level across a variety of desktops and laptops, on both Windows and Mac OS
- › Support multiple user profiles on the same device
- › Experience seamless integration with existing systems management tools
- › Deploy quickly and transparently
- › Comply with regulatory requirements
- › Quickly and securely transmit electronic files

WHY CREDANT?

“The first-time success rate was even higher than we expected,” Reis said. One staff member deployed CREDANT across 700 devices on the 16-acre campus in only 3 ½ months.

End user feedback has been positive; most agree that CREDANT is not disruptive. The deployment has been so successful, now users are approaching Reis’ team to request CREDANT — something that Reis said was previously unheard of. End users like the peace of mind that their sensitive data has been protected. “It’s a testament to how well the product is working. They are talking to their peers and hearing that it is not disruptive.” Now, CREDANT encryption is part of the base deployment for any new computers issued at TJU.

Reis said he would definitely recommend CREDANT to other universities, and has, in fact, provided a reference to another CREDANT client. “I would tell any university that CREDANT really is a tool that has very low operating overhead, it is fairly non-intrusive to the end user,” he said.

Reis adds that encryption in higher education is on the rise, noting that institutions have been increasingly pressured to protect FERPA and HIPAA data, and that CREDANT meets those needs. “From a reputation standpoint, institutions are becoming more aware of how breaches can affect the standing of the university. You want to do what you can to show your appropriate stewardship of students’ information.”

Reis also notes that TJU gets frequent requests to transmit electronic files for admissions, healthcare and other purposes. Previously, administrative systems were limited in functionality for this and requests could take days to fulfill. With CREDANT to GO, Reis says, faculty and staff can quickly and securely transmit HIPAA and FERPA-protected data. Response times are greatly enhanced, and end users have peace of mind when sending files. “We have a one-time cost, and the value-add is incredible,” Reis said.

- › Minimal end-user disruption
- › Compliance with HIPAA/HITECH and FERPA
- › Fast, remote deployment
- › Flexibility to securely and quickly transmit student data as requested
- › Agile, rapid deployment across the campus

BENEFITS

CREDANT’s non-disruptive encryption, fast deployment and ease of use.