

Virginia Commonwealth University



Virginia Commonwealth University (VCU), located on two campuses in Richmond, is known as one of the nation's leading research institutions, with 33,000 students and 17,000 staff and faculty members (including physicians at the VCU Medical Center and its five health sciences schools). The VCU Medical Center offers care in more than 200 specialty areas and is the region's only level 1 trauma center.

CHALLENGES

VCU needed a data protection solution that would:

- › Encrypt data across a variety of desktops and laptops
- › Avoid end-user disruption
- › Work with existing hardware devices
- › Prove that devices were encrypted
- › Provide reporting to prove compliance with state and federal mandates

BUSINESS PROBLEM

University officials knew that compliance with all data protection laws—and protecting the institution's prestigious reputation—was critical. As a healthcare and educational institution as well as a major employer, the university must adhere to a variety of compliance mandates for:

- › Patient information from the School of Medicine, which is regulated by the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
- › Federally funded medical research, which is regulated under the Federal Information Security Management Act (FISMA)
- › Student educational data, which is regulated by the Family Educational Rights and Privacy Act (FERPA)
- › Faculty, staff and student data, which is regulated under Commonwealth of Virginia laws

After a security audit at the School of Medicine revealed they needed a way to encrypt data on a variety of desktops and laptops, VCU Information Security Officer Dan Han faced a difficult challenge. VCU's many educators, physicians and

researchers have the autonomy to choose any type of desktop or laptop they want to use. Han and his team needed to find a data protection solution that would work across a vast variety of computer brands and platforms.

Han examined several products and found many lacking. Some did not have reporting they needed to verify that devices were encrypted. Self encrypting drive (SED) solutions required they replace existing drives, which was cost-prohibitive. And software-based FDE solutions requiring pre-boot authentication were also inadequate, since none would work across all device types.

Whatever the chosen solution, the imperative to IT was that it cause as little end-user disruption as possible.

SOLUTION

VCU's School of Medicine uses 300 CREDANT Mobile Guardian Enterprise Edition licenses (250 are specifically used for Windows and 50 are used for Mac). The entire university purchased over 2,250 licenses in total.

RESULTS

CREDANT Mobile Guardian enabled the university to:

- › Use a single encryption solution across an array of desktops and laptops
- › Deploy transparently, with no end-user disruption
- › Maintain end-user autonomy in their choice of devices
- › Avoid pre-boot login authentication for end users
- › Leverage their existing IT device investments

Virginia Commonwealth University



"I have to say CREDANT has been just fantastic, from the time they first demonstrated the software, to today. If you have a mixed environment of various devices, and can't create a huge disruption to the workforce, I would highly recommend CREDANT."

Dan Han, Information Security Officer
Virginia Commonwealth University

WHY CREDANT?

Han's team implemented a pilot program to encrypt about 30 laptops within the medical school's IT department. They did not experience a single failure. They then deployed CREDANT Mobile Guardian to 106 machines in only 2 ½ weeks and have now extended the solution to several medical school departments. Han said his teams surveyed faculty and staff about their end-user experiences and received positive reviews.

"Most people agree that the product is not disruptive, and they are happy with it," he said. Soon, VCU will deploy CREDANT Mobile Guardian to protect all end user devices (excluding students') across the university.

Han's advice to other universities is this: "If you have a mixed environment of various devices, and can't create a huge disruption to the workforce, I would highly recommend CREDANT. It doesn't create many disruptions, and it will work with almost any device. For higher education institutions, CREDANT is probably the best bet."

- No end-users disruption
- Phased deployment for a more gradual and controlled implementation
- Data protection without pre-boot authentication
- Reporting to prove that lost or stolen devices are protected

BENEFITS

CREDANT's non-disruptive, flexible technology and superior customer support were the benefits that Virginia Commonwealth University felt were right for their specific data protection requirements and unique needs.

CREDANT TECHNOLOGIES

CREDANT is the Trusted Expert in Data Protection. Founded in 2001, CREDANT enables organizations to control, manage and protect data on vulnerable laptops, desktops, PCs, Macs, smartphones and removable media devices. Protecting sensitive information on more than 7 million endpoints at over 1,000 global customers, CREDANT provides the most comprehensive mobile data protection and management platform.

For more information, visit www.credant.com.