

CASE STUDY:

Carnegie Mellon University

securityMETRICS®

Carnegie Mellon University

BACKGROUND

As a global research university, Carnegie Mellon University (CMU) is a birthplace of innovation, pioneering solutions for the world. Welcoming students from over 100 countries, CMU takes protecting their sensitive data seriously. Changes to the Payment Card Industry Data Security Standard brought new challenges and requirements, so CMU's PCI DSS Compliance Project Team found a security and compliance expert to lead compliance efforts and remediate data security risks.

“SECURITYMETRICS' DEEP UNDERSTANDING OF THE PCI DSS REQUIREMENTS COMBINED WITH THEIR ABILITY TO APPLY THE STANDARDS TO OUR SPECIFIC LANDSCAPE BUILT CREDIBILITY WITH OUR CAMPUS STAKEHOLDERS AND ALLOWED US TO CONFIDENTLY REPORT OUR COMPLIANCE.”

– CARNEGIE MELLON UNIVERSITY PCI DSS COMPLIANCE PROJECT TEAM

CHALLENGES YOU FACED WITH PCI COMPLIANCE

- Defining cardholder data environment (CDE) scope was difficult because we work in a decentralized environment. Correctly identifying which people and systems impact the CDE was very important.
- Our homegrown ecommerce system required us to report compliance at an SAQ D level. We wanted to be certain that we interpreted the applicable requirements correctly.

RESOLVING CHALLENGES WITH SECURITYMETRICS' HELP

- Because the Gap Assessor was a Qualified Security Assessor (QSA) who regularly performs PCI DSS audits, he had working knowledge and experience with testing the requirements. He worked with us to understand PCI requirements and the security concerns they address.
- Our assessor had real world IT understanding, allowing him to translate the requirements into our environment. He worked with us on all remediation efforts to ensure we were meeting the requirements.
- His understanding of both the IT/PCI DSS requirements, as well as his QSA experience with other university clients gave him credibility with both the IT staff and the business partners around campus.

GOALS ACHIEVED WORKING WITH SECURITYMETRICS

- Completed a thorough Gap Analysis, made a plan to remediate risks, and received advisement from our assessor.
- Gained confidence we are complying with PCI DSS and have implemented requirements correctly.
- Found a knowledgeable security and compliance partner to increase our overall security posture.