

SAIC Manages Threat of Open Device Ports with DeviceLock®

A top information technology and systems integration contractor to government, healthcare and business, Science Applications International Corporation (SAIC) has built its multi-billion dollar business on making IT decisions that are both smart and safe. As claimed on its website, SAIC “maintains a laser focus on the security implications of all decisions.” SAIC takes on high-profile projects that set a standard for security in a given domain. For example, the Department of Homeland Security (DHS) has enlisted SAIC to design its IT foundation. And SAIC is also involved in bringing state-of-the-art security to the healthcare domain through its work with the University of California, San Diego School of Medicine, on a project known as PCASSO for patient-centered access to secure systems online.

SAIC is no less focused on data security when it comes to its internal IT networks. The IT staff at one location recognized that floppy disk and CD-ROM devices open to normal user access could pose a security hole, and they took steps to lock them down. The team considered locking down the ports in the BIOS; however, it seemed a drastic approach to solving a simple problem. They wanted users to be able to access the devices on their workstations when necessary and appropriate. Adjusting permissions on each PC individually would be a time-consuming process, especially given that they were making decisions for systems operated by 300 employees across their location. Eventually, they opted to install DeviceLock® due to its comparative ease of implementation and the fact that a system administrator would be able to adjust open/locked settings of PC devices from a central location. Installation was easy and they’ve been satisfied with the solution.

www.saic.com

Based on survey questionnaire filled out by Paul Maingault, SAIC.