What does the MiWorkspace team do “under the hood” when your computer migrates?

**Encrypt Mac Notebooks**
Using Apple FileVault, the contents of your hard drive are encrypted in real time keeping your data private in the case of laptop loss or theft. MiWorkspace manages the recovery keys for instances where you need to get data off your computer and no one has a working password.

**Install Managed Software Center**
This U-M version of the Apple App Store manages updates to your computer. It regularly sees what version of software you have vs. what is available.
If it notices that you have outdated software, it will let you know. You then have the opportunity to install or defer the update.

**Install a Tool that Pushes Low Level Policy Settings**
This tool manages about 15 settings on your machine. It includes requiring a password to wake-up; shutting off the Apple software update; adding “Welcome to MiWorkspace” text to log-in screen; and preregistering the U-M licensed MS Office.

**Install Virus Scanning Software**
MiWorkspace uses System Center Endpoint Protection (SCEP) instead of Sophos.
It runs and updates automatically and might push out a patch; if it finds something, you’ll get an alert or quarantine (most of the time they are Windows viruses that are deleted.)

**Join Computers to Active Directory (AD)**
One password (UMICH) lets you log into your computer. MiWorkspace uses AD only for user names and passwords specific to accessing storage and printing.