EDTECH™ FOCUS ON HIGHER EDUCATION

Brought to you by:

CDW·G

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

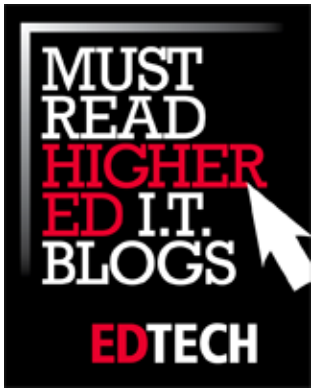
Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe



View caption

Annie O'Neill
Mobile Security

How to Save Money, Time and Sanity with Mobile Device Management Software

By adopting mobile device management software, colleges and universities ensure security, set policies and save time.

Karen D. Schwartz

posted July 31, 2012 | Appears in the Summer 2012 issue of *EdTech Magazine*.

Related Articles

Three Tips to Secure Telework

Campus Technology 2012: Colleges Support Learning on the Move

How to Repel Notebook Thieves

4 IT Security Tips for BYOD

5 Backup Pointers for Mobile Devices

Editors Picks

Three Easy Steps to BYOD
5 Tips for Optimizing Load Balancers
Why Computer Labs Are Still Essential On Campus

Some people seem to live on their smartphones. Such is the case at the University of Pittsburgh, where many of its employees rely heavily on the devices to access information, connect with other staffers and manage their calendars.

Richard McIver, senior systems administrator for the university's Financial Information Systems (FIS) group, says that when Pitt transitioned away from BlackBerrys for about 200 of its staff, ensuring security became a greater concern.

"As we moved to iOS, we knew we needed a good way to secure it," says McIver. "We wanted to ensure that all devices used by the staff would have policies for passwords and full device encryption, and we needed the ability to remotely wipe the device if it were lost or stolen."

McIver says FIS began using the AirWatch mobile device management (MDM) software in January 2011. For all smartphones and tablets, the IT department logs in via the web to access the cloud-based AirWatch management portal, adds a username and ID, and enrolls the device with AirWatch MDM. That process applies the department's policies to the device.

In addition to security, the MDM software adds a Microsoft Exchange account and an app catalog with recommendations from the IT staff. Eventually, McIver says FIS may permit staffers to use Android devices. AirWatch MDM can manage those as well, he says, by installing a client agent on each device.

Growing in Popularity

Installing MDM software on mobile devices has become a popular way of managing and pushing policies, applications and configurations, as well as keeping track of devices and ensuring security. Popular solutions include those from BoxTone, MobileIron, AirWatch, Fiberlink, Sophos, Absolute Software and Sybase Afaria.

"With MDM, as soon as you install an agent on the device, you have a lot more granular control," says Mark Tauschek, lead research analyst at Info-Tech Research Group. "You can do selective wipes — wiping only enterprise apps, or only e-mail, calendar and contacts. It almost always makes sense to use MDM."

At Stark State College in North Canton, Ohio, MDM quickly became a requirement when the college began furnishing its faculty and staff with new tablets and smartphones about two years ago. It didn't take long for the IT department to realize that without some automated way to monitor the devices, it would lose track of them.

"We realized that it was taking a lot of time to deploy each device," says Geoff Starnes, network systems and security manager. "And once they were deployed, we knew we might not see them for a long time, so we needed a way to manage them remotely, push apps to the devices, track them and, if necessary, remotely wipe the contents."

45 Minutes
The amount of time an organization can save per mobile device by implementing MDM, based on managing 1,000 devices over five years.

SOURCE: MobileIron Lifecycle Cost Savings Calculator

About a year ago Stark State began installing an MDM solution from MobileIron on all college-owned tablets and smartphones. Before the devices are distributed, the MobileIron software is installed using a template that configures the units, including the service set identifier (SSID) for the wireless network. Starnes says deploying a unit now takes about two minutes, compared with 20 to 25 minutes without MDM.

The college's 15,000 students use their own mobile devices, which makes it virtually impossible for the college to control them. To maintain security, the IT department has created two wireless SSIDs: one for wireless devices the college owns and another for external mobile devices.

At National American University, a for-profit university with several U.S. locations and online programs, staff use a variety of mobile devices. About 40 percent choose to use their own smartphones and tablets, while the rest opt for a university-issued device. In both cases, the devices are secured with BoxTone's MDM software.

"We have a lot of sensitive data and have to deal with Sarbanes–Oxley issues since we are a publicly traded company," says Cody Reynolds, a network analyst. "We needed something that could wipe sensitive data if an employee quits, is fired or loses the device, and we needed full device encryption."

The university began using BoxTone about a year ago and has found it invaluable. Although previously IT admins could remotely wipe mobile devices with Microsoft ActiveSync mobile software, doing so required wiping the entire contents of the device. With BoxTone, they can keep the university's information in a secure container that can be wiped if needed, leaving personal data intact. The MDM software also provides "data at rest" encryption, which gives the IT department peace of mind if a unit is lost because it can be set to automatically wipe the device. What's more, it's easy for IT administrators to provision devices, and easy for staff to use, freeing up the IT staff for other tasks.

The New Breed of Mobile Security

There's an entire range of products emerging beyond MDM software that helps IT staffs manage and secure mobile devices.

Products such as Enterasys' OneFabric Edge for Mobility and BYOD, Aruba Networks' ClearPass and Cisco Systems' Identity Service Engine let network administrators fingerprint devices and users, and apply the appropriate network access policies automatically. "These solutions can apply policy in an automated fashion, so when a student or employee connects to the wireless network with a personal device, it will know who they are, what device they are connecting with and where they are," explains Mark Tauschek, lead research analyst at Info-Tech Research Group. "It can apply rules and policies and control access for specific categories of users, as long as they are connected to the network."

Mobile application management (MAM) is another emerging product. Unlike MDM, which focuses on securing

and managing mobile devices, MAM concentrates on securing and managing the applications that those devices access. Examples include Symantec's Nukona and IBM's Worklight.

Tauschek says that securing mobile devices should become easier as providers add mobile device, network and application management, along with traditional systems management, networking and security features. McAfee, Microsoft (with Systems Center 2012), LANDesk, Symantec and Sophos are among those offering MDM and system management capabilities.

Higher Ed Scope
For more stories on colleges in Ohio | Pennsylvania | South Carolina
About the Author
Karen D. Schwartz
Karen D. Schwartz is a freelance technology writer based in the Washington, D.C., area.

…more

Security

What Colleges Can Learn from Mat Honan's "Epic Hacking"

Simple security measures can prevent digital catastrophes.

Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2

Get control of your organization's data security policies.

…more

Storage

Colleges Use Storage Virtualization to Support Distance Learning

As colleges expand online learning, storage takes center stage — and virtualization makes…

5 Strategies for Deploying Deduplication Effectively

Deduplication can save space, time and money, but it must be done correctly.

…more

Networking

Increase in Devices Causing Bandwidth Trouble on Campus [Infographic]

How can IT departments keep up?

Dark Fiber Delivers for Columbia College Chicago

An upgraded network at the noted arts and film college gives students and faculty the…

…more

Mobile

Call Me, Maybe? The College Student's Affair with Smartphones [Infographic]

How are students using their high-tech smartphones?

3 Ideas to Make the Most of Mobile Apps on Campus

Students already have the devices, so how can schools embrace the trend?

…more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management