

FEDTECH™

TECHNOLOGY INSIGHTS FOR LEADERS IN FEDERAL GOVERNMENT



CASE STUDIES

TACTICAL ADVICE

RESOURCES

Infrastructure Optimization

Security

Storage

Networking

Mobile & Wireless

Hardware & Software

Management

CURRENT ISSUE



Subscribe





Management of Change

Click for full coverage

FEDTECH **Solutions Report**

5 Next-Level Data Consolidation Tips

Follow these five data management tips for a successful consolidation project.

As featured on



SIGN UP FOR

FedTECH

E-NEWSLETTERS

Follow FedTech

RSS Feed

Connect With CDW

LinkedIn YouTube Spiceworks

6.7k

ADVERTISEMENT

Home » Management

[< previous](#)

[next >](#)



Agencies Use MDM Tools to Secure Mobile Devices

A new crop of application and device management solutions protects federal data while helping enforce policies.

Karen D. Schwartz

posted July 19, 2012

Like 0 Tweet 5

Share Spice



Editors Picks



How Adopting Shared Services Boosts Efficiency
Software for Monitoring and Management
Next-Generation Tech Gets Agencies Ready for Enterprise
ADVERTISEMENT

Since last November, NASA employees and contractors have been able to access and download applications they need for work on a mobile device of their choice from a NASA-developed app store.

Although the agency doesn't yet have a formal bring your own device (BYOD) policy, the IT staff is doing what it can to ensure the security of the apps and mobile environments through a set of tools that function as a mobile application management (MAM) system.

"We know the BYOD policy is coming, but we didn't want to wait, so we took a MAM approach to mobile apps," says Erna Beverly, an enterprise applications service executive at NASA. "For us, the solution to mobile management is to secure and manage the application and data as opposed to the mobile device."

While the MAM system's primary goal is to secure applications and data, it has several functions in common with a traditional mobile device management (MDM) tool. For example, the system allows NASA to provide access to apps for specific groups of users based on their roles or needs.

The space agency plans to incorporate Public Key Infrastructure (PKI) certificate-based authentication as an additional security measure, probably sometime within the next year. Through the use of pulse analytics and administration, Beverly says administrators also can determine what type of device is being used and where.

Once NASA's mobility strategy is fleshed out and the BYOD policy is implemented, Beverly expects the agency to move to a full-fledged MDM system to gain more control over the hardware, such as the ability to remotely wipe devices.

Remote Control

Installing MDM software on mobile devices has become a common way of managing and pushing policies, applications and configurations, as well as keeping track of devices and ensuring security. Popular solutions include those from *AirWatch*, *Absolute Software*, *BoxTone*, *Fiberlink*, *MobileIron*, *Sophos* 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 the National Nuclear Security Administration (NNSA), implementing MDM is table stakes. For several years, the NNSA has used some type of solution to manage the mobile devices of 20 to 30 percent of its geographically dispersed workforce. Pending an upcoming BYOD policy, that number could easily double within the next few years.

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 Mobile Device Lifecycle Cost Savings Calculator

For Anil Karmel, the nuclear-security agency’s management and operations chief technology officer, the ultimate goal is to expand the scope of MDM beyond device management to data management. “We want to be able to secure the data based on user-centric approaches,” he explains.

If a worker needs access to general internal data, for example, the policy applied to that device would be relatively open with some minor controls. But the policy would dynamically change based on the security level of the data requested: When that user requests access to more restricted information, additional controls would be deployed. Once the data no longer resides on the device, the basic policy would be put back into place.

Getting to that point requires the agency to fully understand the type of data it processes, where that data needs to be processed and the controls that should be applied to each type of data. With that information determined, the next step is to build a system on top of a commercial MDM solution that would enable policies to be changed dynamically. Karmel is determined to achieve this goal sometime within the next few years.

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 Services 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 someone 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.

0 comments

0 Stars 



Discussion 

Community 



No one has commented yet.

Infrastructure Optimization

Pull the Plug on Excessive Data Center Costs

IT managers find that they can take advantage of new technologies and techniques to...

Windows Server 2012's Cloud Connection

Microsoft's newest server solution can help agencies migrate their IT infrastructure...

more »

Security

FedBytes: Is Communication the Best Defense Against Cyberthreats?

Hardware, software and tech news from across the government and around the country.

How Agencies Keep Mobile Data Safe

Encryption technology protects data on notebooks and other mobile devices.

more »

Storage

Which Disaster Recovery Site Strategy Is Right for You?

Be sure to factor in the agency's objectives and continuity needs before making an...

NAS Creates Lots of Storage in a Small Space

Network-attached storage devices can fulfill the needs of both large and small...

more »

Networking

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

How to Make a Smooth Switch to IPv6

Determine agency needs and existing environments before jumping into the new...

[more »](#)

Mobile & Wireless

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

3 Ways the Military Is Using Mobile Applications

How technology is powering the Army, Air Force and Veterans Affairs.

[more »](#)

Hardware & Software

Maximizing Windows 8 Security Features

Three core enhancements can improve security.

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 »](#)

Infrastructure Optimization

Security

Storage

Networking

Mobile & Wireless

Hardware & Software

Management

Copyright © 2012 CDW LLC | 230 N. Milwaukee Avenue, Vernon Hills, IL 60061