FEDTECH™ TECHNOLOGY INSIGHTS FOR LEADERS IN FEDERAL GOVERNMENT

BROUGH CDW·G

CASE STUDIES
TACTICAL ADVICE
RESOURCES
Infrastructure Optimization
Security
Storage
Networking
Mobile & Wireless
Hardware & Software
Management
CURRENT ISSUE

Subscribe

FEDTECH

Solutions Report

5 Next-Level Data Consolidation Tips

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

SIGN UP FOR

FedTECH

E-NEWSLETTERS

Follow FedTech

Follow RSS Feed

Connect With CDW

LinkedIn YouTube Spiceworks

Like 6.7k

Home » Security

‹ previous next ›

Data Loss Prevention (DLP)»

Locking Down BYOD

Agencies find ways to accommodate employees' personal devices on federal networks.

Karen D. Schwartz

posted May 18, 2012 | Appears in the Spotlight on Network Security issue of the *FedTech Magazine* e-newsletter.

Like 0 Tweet 7 Share Spice

Related Articles
Firewall Rule Management Is the Key to Network Security
Strategies for Preventing a Data Breach
Data Loss Prevention: How to Stop Inside Jobs
Bad User Experience: Another Form of Vulnerability
A Cheat Sheet on Security Monitoring
Editors Picks

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

Employees at the Federal Deposit Insurance Corp. (FDIC) have been authorized to use their own mobile devices at work for several years, and users have adopted the policy with enthusiasm. CIO Russell Pittman says every recent meeting he can remember has included several people using tablet computers.

One of the reasons that the FDIC’s “bring your own device” (BYOD) initiative has worked so well, Pittman says, is because the agency made some security-based decisions early on that set the tone and prepared the *agency’s network to deal with the risks involved*.

“We needed to ensure that the corporate data was separate from the personal data, and that the corporate data was only available to those who should have access to it,” Pittman explains.

The agency accomplished this by first putting technology in place that allows employees to access corporate data and e-mail applications on their own mobile devices but that does not let them download or save it on the devices. This is accomplished by using a secure, browser-based gateway along with a mobile virtualization platform that isolates the personal and corporate environments.

As BYOD takes off, Pittman is considering letting users store some corporate information on their personal devices. If that occurs, the organization will add a secure containerization technology that will encrypt data at rest and allow the secure container to be remotely wiped if necessary.

BYOD gives agencies valuable flexibility, but accepting users’ personal mobile devices on agency networks requires that IT shops shore up network security. Without that, IT departments can quickly lose control of who has access to data and applications and whether users’ devices are fully secure, leaving agencies vulnerable to unauthorized access to sensitive information.

For organizations that allow users to save or download data to their mobile devices, the first step is to implement a mobile-device management (MDM) solution. MDM monitors devices that are connected to the network and can remotely lock or wipe these devices.

Even if an agency doesn't let users download or save data on their personal devices, security is still a priority, says Andrew Braunberg, research director for enterprise networks and security at Current Analysis in Herndon, Va. Many solutions can bolster network security for BYOD. The goal of mobile application management (MAM) products is to make apps more manageable and secure. Some solutions accomplish this with "wrappers" that control the use of the application. Others use containerization, which creates private "sandboxes" for sensitive apps.

Hypervisors, which create virtualized platforms that ride on top of the operating system, and data loss prevention technology also help protect the network against the risks associated with personal devices.

At the U.S. Equal Employment Opportunity Commission, CIO Kimberly Hancher is in the midst of an ambitious project to let all of the organization's employees use their own devices to download and synchronize their e-mail, calendars, contacts and tasks between the network and their personal devices.

The project is partially cost-driven — Hancher has had to find ways to make significant budget cuts, including the amount she spends on agency-provided RIM BlackBerry devices — and partially an effort to remain on the cutting edge.

61%
The percentage of organizations that allow users to access network resources via personal devices.

SOURCE: SANS Mobility/BYOD Security Survey, March 2012

"As we went into the 2012 fiscal year, we had such severe budget cuts that I had to think of another way to reduce costs," she says. "I wanted to use this to spur action on BYOD. 'Bring your own device' means that employees turn in their EEOC BlackBerry and use their own device, thereby lowering the EEOC's annual operational cost of mobile-device data and voice services."

For this project to work, Hancher first had to find a way for the mobile devices and network to operate with the agency's *Novell GroupWise* e-mail system. The agency deployed a cloud-based MDM system that lets the agency set policies while providing over-the-air synchronization of e-mail and personal information management. Data is stored behind EEOC's firewall, and all data to and from devices is fully encrypted. EEOC e-mail stored on a device can be wiped if the device is lost, stolen or otherwise compromised.

The pilot started in December 2011, and a second phase is under way to fine-tune policies. Hancher hopes to have the entire program available for employee use this summer. Eventually, she says, the system also will include a "privileged interface," which will allow employees with appropriate credentials to access more information via their personal devices.

The Fine Print

Organizations that grant employees the privilege of bringing their own mobile devices into the workplace must create policies that govern which devices are acceptable, how they can be used and what applications they can access, says Cesare Garlati, vice president of mobile security at Trend Micro. Garlati suggests other important elements of a BYOD policy:

- Users must agree to install whatever security, monitoring or tracking software the organization requires.
- All devices connecting to the network must be registered with the IT department.
- Users must agree to password-protect the device.
- Use of the mobile device must impose no tangible cost to the organization.

- Use of the mobile device must not have an adverse impact on the user's performance.
- All devices must support 802.1X authentication.
- Only approved apps may reside on the device. Blacklisted apps are generally considered security or productivity risks.
- All devices must meet minimum specifications for hardware, operating systems and device management agents.

0 comments

0 Stars

Leave a message...

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