InformationWeek
:: reports

Reports.InformationWeek.com February 2012

Next

Mobile Malware: Is Prevention Possible?

Fact is, today "proactive" translates to "real-time reactive" via auto remote wipe, sharply defined mobile policies and enforcement, and segregation of personal and corporate data. We know malware is going to happen. Here's how IT can limit damage.

By Paul Williams

Report ID: S4340212

TABLE OF CONTENTS

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com,* editor-at-large **Andrew Conry-Murray** at *acmurray@techweb.com,* and research managing editor **Heather Vallis** at *hvallis@techweb.com.* Find all of our reports at *reports.informationweek.com*.

Paul Williams
InformationWeek Reports

Paul Williams brings a wide range of experiences to his writing. He has worked extensively in technology, as both a software engineer and a technical writer. His technology experience includes being lead developer on one of the first data warehouse implementations in the insurance industry and doing embedded software engineering on medical devices, as well as a wide range of Web, mobile and desktop application development, with a focus on data modeling and design. His band, Quarkspace, has long been considered one of the top American space rock bands.

Paul recently leveraged more than 20 years of software engineering, musical and writing experience to form a nimble organization, Makes Words Work LLC, to serve the communication and technology needs of its clients.

EXECUTIVE SUMMARY

While reports of malware infection seem more pronounced on the open Android platform, malware can affect end users no matter the mobile operating system in use; as *InformationWeek*'s Jonathan Feldman discussed recently, there are some cracks in Apple's walled garden, too. And we're poised to see a more splintered ecosystem, according to our January *InformationWeek* Research In Motion Survey of 536 business technology professionals, all of whom are involved with evaluating, procuring or managing smartphones or creating mobility policies. While currently the platform breakdown heavily favors the more secure and manageable RIM BlackBerry, that's set to change. Within 24 months, respondents expect a relatively level field among Android, Apple and BlackBerry (see Figures 1 and 2).

Form factor is another wild card. Almost 80% of the 323 respondents to our latest *InformationWeek* Mobile Device Management and Security Survey, all of whom are involved with determining mobile/wireless strategy or evaluating, recommending or purchasing mobile devices, say tablets will grow in importance, even as laptops and smartphones hold pretty steady. That means how we battle malware has to evolve as well, moving beyond just desktop antivirus.

Battle Lines Are Drawn

While mobile malware is able to propagate through phone-to-phone transfer, or even by a user accessing an infected network, the majority of attacks stem from someone downloading an infected app. This creates problems for network administrators, who are often more attuned to desktop virus protection, where they must defend against vulnerabilities and exploits that install malware without the user knowing. Mobile malware effects run the gamut from attackers stealing sensitive data to making expensive phone calls to foreign locales, but the key for attackers is to convince your users to download and install the malware.

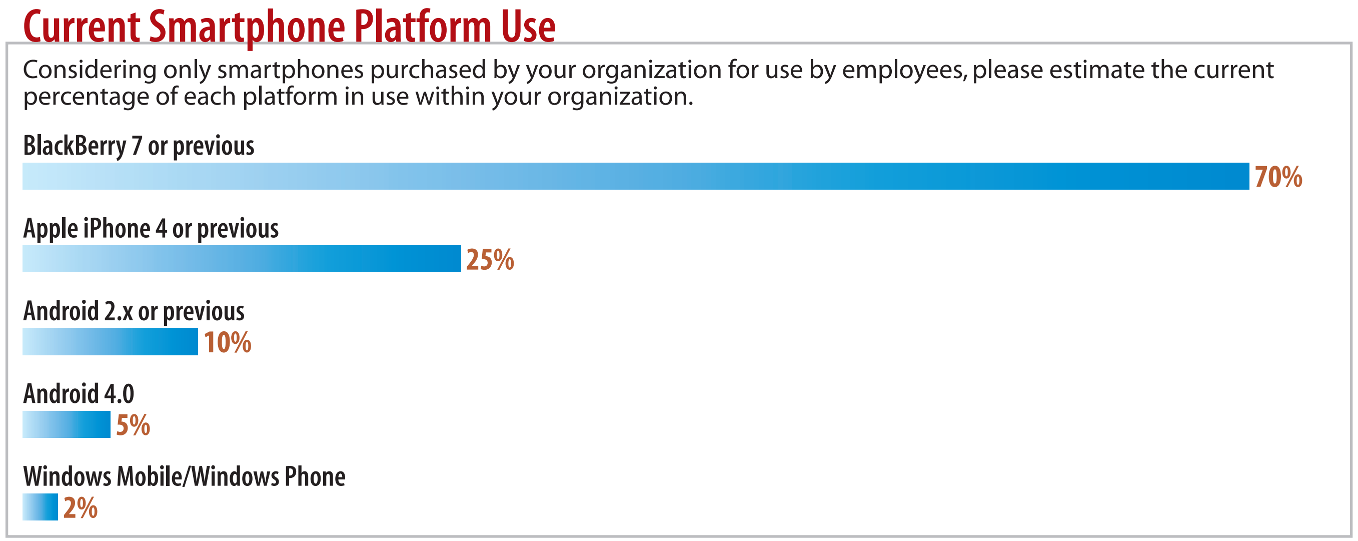
Current mobile device management, or MDM, systems include a measure of mobile malware protection; we recently did a roundup of these tools. While some aspects of malware prevention in the mobile age mimic our struggles on the desktop, innovations have enhanced enterprise IT's ability to react to infections and protect valuable corporate data in near real time, no matter where breaches occur.

To illustrate the three key principles of a real-time reactive strategy—technology like remote wipe augmented by well-defined mobile policies and enforcement and segregation of personal and corporate data—we'll discuss three leading MDM systems, from MobileIron and antivirus veterans Symantec and McAfee. We'll also look at policy highlights and ways to segregate data, to complete the picture.

Technology: MDM vs. Mobile AV

To illustrate the technologies available for battling malware, we'll look at McAfee VirusScan Mobile and Enterprise Mobility Manage-

Figure 1


Current Smartphone Platform Use

Considering only smartphones purchased by your organization for use by employees, please estimate the current percentage of each platform in use within your organization.

Note: Median percentages

R4330212/2

Data: *InformationWeek* Research In Motion Survey of 536 business technology professionals, January 2012

FAST FACT

25%

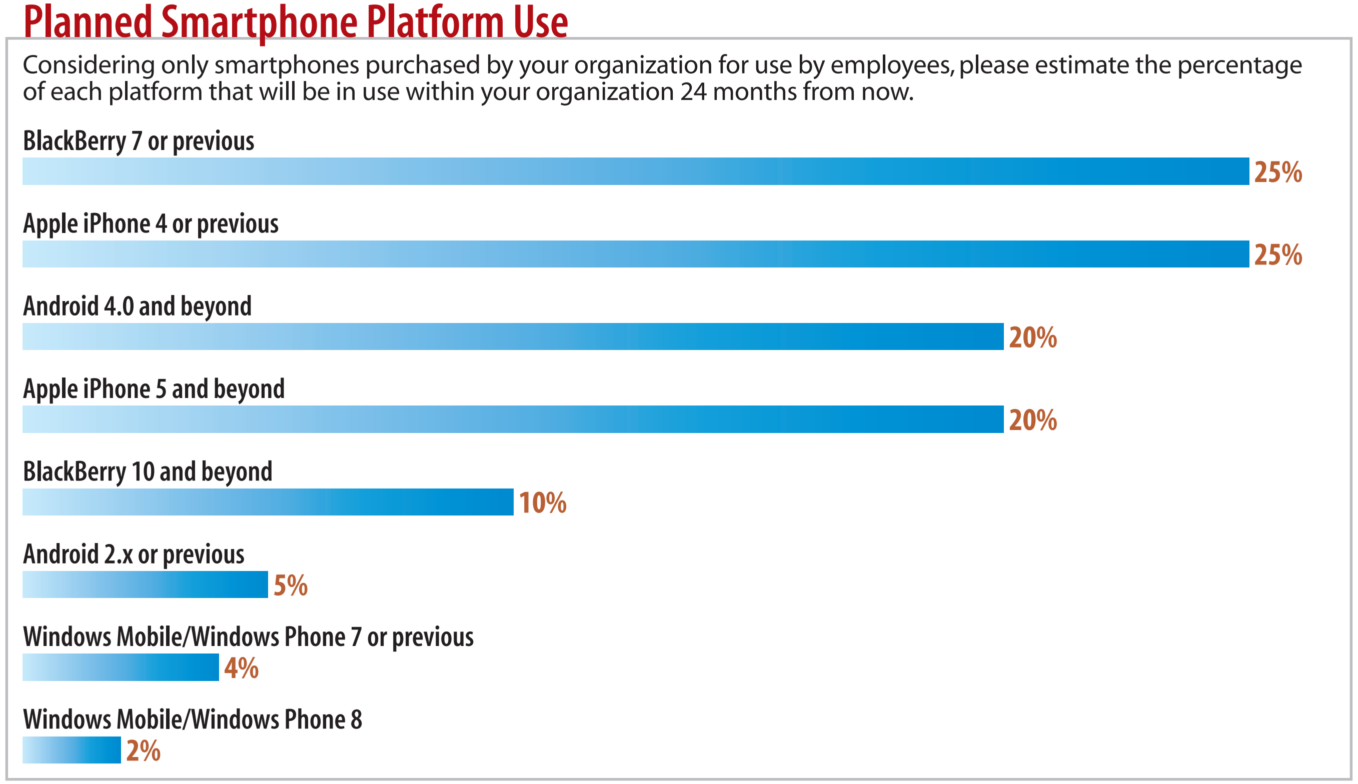
of respondents to our Research In Motion Survey expect employees to use BlackBerry 7 or earlier versions in the next two years, the same percentage as iPhone 4 or earlier versions.

ment, MobileIron's Advanced Mobile Device Management system and Symantec's Mobile Management; these products are representative of what's on the market today. (We dig deeper into the MDM space in our recent Buyer's Guide.)

Key things to look for are broad platform support and an ability to differentiate between corporate and personal data. MobileIron's Advanced Mobile Device Management system encompasses most major mobile platforms and device types, including smartphones and tablets. Sandboxing of all mobile device data is the centerpiece of the MobileIron Virtual Smartphone Platform, an architecture that allows remote management of an organization's mobile infrastructure, including both corporate- and employee-owned devices. Once installed, MobileIron provides separate sandboxes so that the data doesn't commingle.

Figure 2

Planned Smartphone Platform Use


Considering only smartphones purchased by your organization for use by employees, please estimate the percentage of each platform that will be in use within your organization 24 months from now.

Note: Median percentages
Data: *InformationWeek* Research In Motion Survey of 536 business technology professionals, January 2012

R4330212/3

The Advanced Mobile Device Management module of MobileIron's platform contains a host of real-time features, but vital to the topic of mobile malware protection are the app management functions, which include a secure app store, so companies can compile an approved app inventory accessible by IT staff and employees.

Protection against rogue apps using MobileIron involves administrative management of an approved app list in the form of traditional whitelisting and blacklisting capabili-

Previous Next

Table of Contents

ties. Should a user download an app marked unsafe by IT, a set of rules is enforced; these normally involve informing both the user and the administrator of the policy breach via SMS and email. MobileIron can also detect when an application attempts to root or jailbreak a phone and notify IT that such an attempt occurred. Additional enforcement steps can include locking the infected device and quarantining sensitive corporate data; administrators control these policy rules using the MobileIron App Control tool. MobileIron's overall strengths reside in its management infrastructure, which allows administrators to define role-based policy rules.

As usual in security, technology isn't the whole answer, and no one system offers complete protection.

Symantec Mobile Management is the flagship MDM product for the antivirus industry veteran. SMM supports nearly all current mobile device platforms, including iOS and Android. The product provides a similar level of mobile policy enforcement as MobileIron's MDM, as well as standard MDM features such as the segregation of corporate and personal data and a remote-wipe capability.

Like the other MDM products, SMM uses security certificates to control mobile access to corporate resources, like email, Wi-Fi networks and VPNs. Devices found to be out of policy compliance lose connection privileges. An enterprise app store is also provided for deployment of internal apps and to support a framework for public app recommendation. SMM's Mobile Content Library performs a similar function for corporate documents, videos and podcasts.

Symantec also offers the Endpoint Protection Mobile Edition mobile malware prevention system, which combines antivirus technology with a firewall and functionality to prevent SMS spam. It integrates with Symantec's Mobile Management; however, it's available only for the older Windows Mobile and Symbian platforms. The company says a version with support for iOS and Android is under development but did not provide a timeframe for that version's release. IT teams need to consider the current lack of support for iOS and Android if they want mobile malware prevention dependent on in-memory device agents.

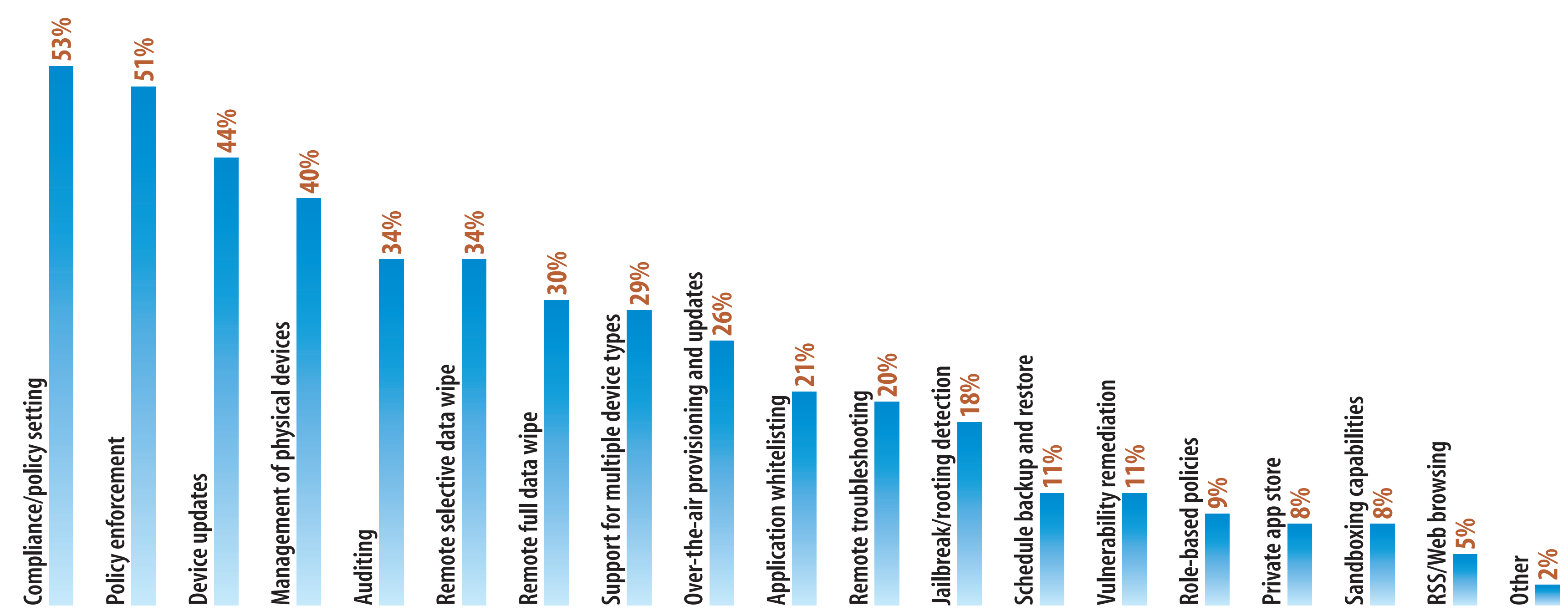
McAfee's VirusScan Mobile provides endpoint security for a range of mobile devices, including all versions of Android (up through Honeycomb), Windows Mobile, Symbian and BlackBerry. While native support for iOS and Windows Phone is not included with VirusScan Mobile, a software development kit is available for enterprises looking to support devices running those and other mobile and embedded operating systems. Obviously, those extra development costs need to be factored in. Running as a process on the mobile device, VirusScan Mobile promises real-time malware detection in less than 200 milliseconds. McAfee says removal of infected files happens automatically while alerts are sent to IT staff. In addition to spotting nefarious app downloads, VirusScan Mobile scans for malware, including Trojans, dialers, worms and viruses, contained in email, text messages and file attachments.

Unfortunately, VirusScan has inconsistencies in the types of protection available, depending on the mobile operating system. For example, malware-infected emails aren't handled on Android devices; only BlackBerry, Windows Mobile and Symbian smartphones enjoy that level of protection. BlackBerry users, however, remain vulnerable to infections through messaging. In addition to incident reporting and the deletion of malware, Windows Mobile and Symbian users get the benefit of quarantining and the attempted repair of any detected infections.

Figure 3

MDM Features of Interest

Whether or not you have a mobile device management (MDM) system for controlling tablets and smartphones, which centrally controlled features are of greatest interest to you?



Note: Five responses allowed

R3321011/27

Data: *InformationWeek* 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

While these inconsistencies will be frustrating for those struggling to put in place an enterprise-wide MDM strategy, the VirusScan Mobile SDK can be used to make up the gaps in protection—once again, at additional development cost.

VirusScan Mobile comes packaged as a separate product but requires the purchase of McAfee's enterprise MDM package, Enterprise Mobility Management. McAfee EMM is a two-tiered system, with a server layer containing the enterprise management features, while mobile device agents perform a host of data encryption, authentication and remote management functions.

McAfee EMM actually provides out-of-the-box support for iOS and Windows Phone, in addition to Android and BlackBerry, at the device-agent level. We'd prefer to see McAfee automatically include VirusScan with EMM as opposed to requiring EMM when buying VirusScan, considering that most potential enterprise customers desire full malware protection. Additionally, future versions of VirusScan need to provide support for iOS

Previous Next

Table of Contents

and Windows Phone, to eliminate the extra costs associated with engaging developers in implementing the VirusScan Mobile SDK to fully protect devices running Windows Phone and iOS.

All three of the MDM systems we profiled provide a standard level of preventative mobile malware functionality, most notably enterprise app stores and the forced segregation of personal and corporate data. In addition, the three vendors offer more reactive measures, like real-time policy-based reaction to security breaches through remote wipe or restricted access to corporate resources, such as email or VPN. Each system also features unified endpoint management across all major mobile device platforms.

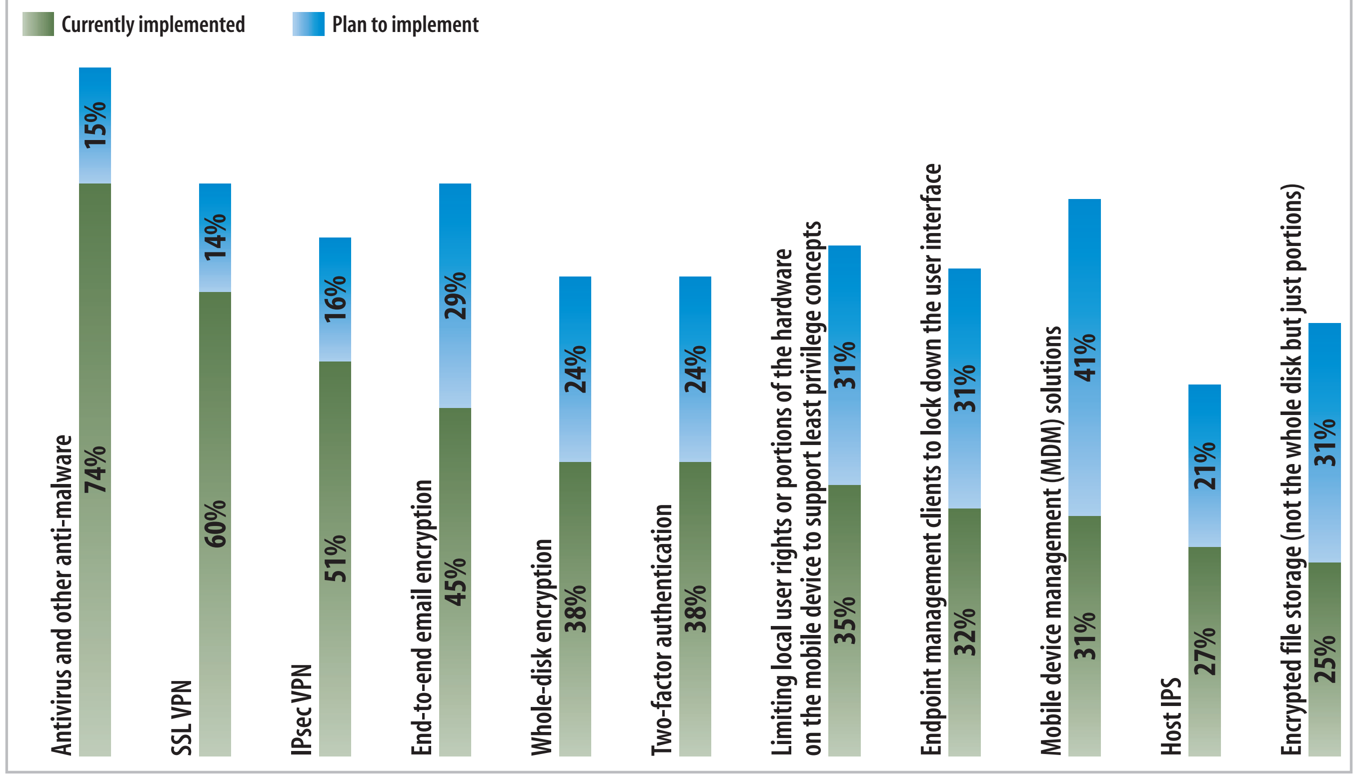
Our main concern with the mobile device management space is that most of the vendors are limited to interfacing with some devices using the API provided by the mobile operating system. All three vendors, and most of their rivals, support the same general MDM capabilities, including remote wiping and app whitelisting, so when comparing, look closely at management and integration capabilities.

McAfee's VirusScan Mobile operates more like traditional PC antivirus, by detecting malicious code and files on the device. However, we don't believe this is the biggest threat to

Figure 4

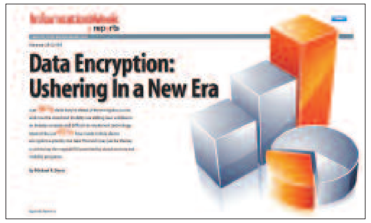
Portable Device Security Controls

What security controls have you implemented or do you plan to implement within 12 months for protecting portable devices, including laptops, netbooks, tablets and smartphones?



Data: *InformationWeek* 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/21


Data Encryption: Ushering In a New Era

Related Report: Data Encryption

Just 36% think they're ahead of the encryption curve, and now the cloud and mobility are adding new wrinkles to an already complex and difficult-to-implement technology. Meanwhile, just 47% have made mobile-device encryption a priority. Our take: This tech may just be the key to achieving the magical ROI promised by cloud services and mobility programs.

Download

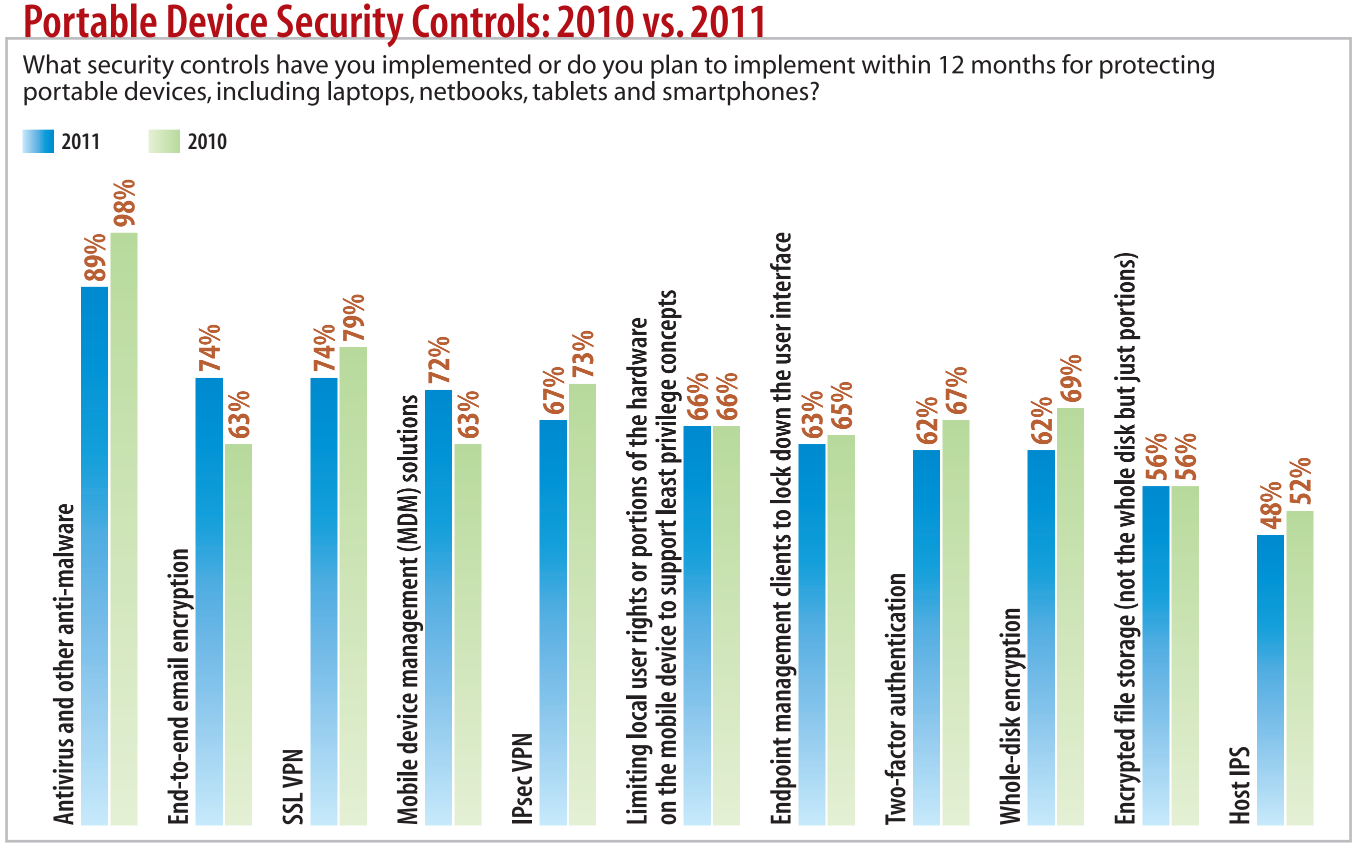
most organizations, and the additional investment in programming time to use the McAfee APIs needs to be considered.

Symantec needs to release the in-development version of Endpoint Protection Mobile Edition that adds compatibility with iOS and Android; current support for only Windows Mobile and Symbian is simply not enough for most enterprises. And, despite MobileIron's industry-leading MDM interface, the company focuses little on anti-malware functionality at the device agent level. Its strengths lie in the best-of-breed customizable workflows of the Advanced Mobile Device Management product.

It's unfortunate that VirusScan Mobile requires the purchase of McAfee's Enterprise Mobility Manager. As it stands today, the ultimate enterprise mobile malware prevention solution may in fact be the combination of VirusScan Mobile on each mobile device with MobileIron's Advanced MDM used to manage an organization's entire mobile operations.

Figure 5

Portable Device Security Controls: 2010 vs. 2011



Note: Percentages reflect a response of "currently implemented" or "plan to implement" R3321011/22
Base: 323 respondents in August 2011 and 307 in March 2010
Data: *InformationWeek* Mobile Device Management and Security Survey of business technology professionals

However, as usual in security, technology isn't the whole answer, and no one system offers complete protection. Each organization has to assess its own risk and determine what is more important—detecting a threat from an already installed application (mobile AV) or separation of corporate data from personal data (MDM). We would argue that you should choose MDM and forget mobile AV if you are an enterprise that provide access to corporate data, but use mobile AV if the majority of your end users are consumers who don't access corporate resources.

No matter what your stance, strong corporate MDM policies are as important as a technology platform choice in solving or at least mitigating the malware problem.

Policy and Enforcement

Mobile device management in this BYOD era places the onus for malware prevention directly on IT—you need clearly defined policies backed up by strong enforcement. These policies should include rules that in some cases parallel those in "normal" network management, such as requiring strong passwords or limiting the number of unsuccessful login attempts. Other must-have rules, such as requiring data encryption even when a device is powered off, are primarily relevant to the mobile domain.

Policies also need to take into account a mix of both corporate- and employee-owned devices, with a primary directive focused on the protection of corporate-owned resources and data.

Though third-party MDM tools provide a measure of automated enforcement, they still depend on well-defined rules. So no, there's no avoiding writing a policy. It's also important for IT staff to fully implement any chosen tool's policy-definition functionality and choose a system able to handle a robust set of enterprise policies.

But just as important as policy is training—in fact, that's truer now than it's ever been. An educated mobile workforce is your best line of defense against malware. This education needs to be a formalized program and could include periodic broadcast updates on the latest malware trends and news on recent nefarious apps. Simple instructions, such as not letting children play with the device and how to verify the authenticity of an app, can go a long way in reducing help desk calls and remote wipes, both time consuming and annoying for end users and IT.

We recommend that all education start with one simple phrase: "By securing your work data, we secure your personal data." Employees don't want their photos or private text messages to be stolen, and MDM technology can help prevent this personal data from getting into the wrong hands. Having your mobile security awareness focus on employees' personal lives will increase retention of the tips you provide and will get more people interested in listening in the first place.

Outside of awareness, your policies minimally must have password complexity, remote wipe and email encryption enforced. Passwords are required by all mobile devices in order for device encryption to be enabled. Let us repeat that: You must have a password on the device for encryption to work, no matter what mobile device vendor. (For more on mobility, cloud and encryption, check out our recent State of Encryption report.)

State specifically when IT reserves the right to remote wipe a personal device, but ensure that you give users the capability to fix mistakes before the device is wiped. For example, provide a grace period to remove a banned app, and allow five or six failed passcodes before a remote wipe. Setting up an easy-to-remember hotline number for lost devices will reduce the risk of a remote wipe causing the loss of data.

Segregation of Personal, Corporate Data

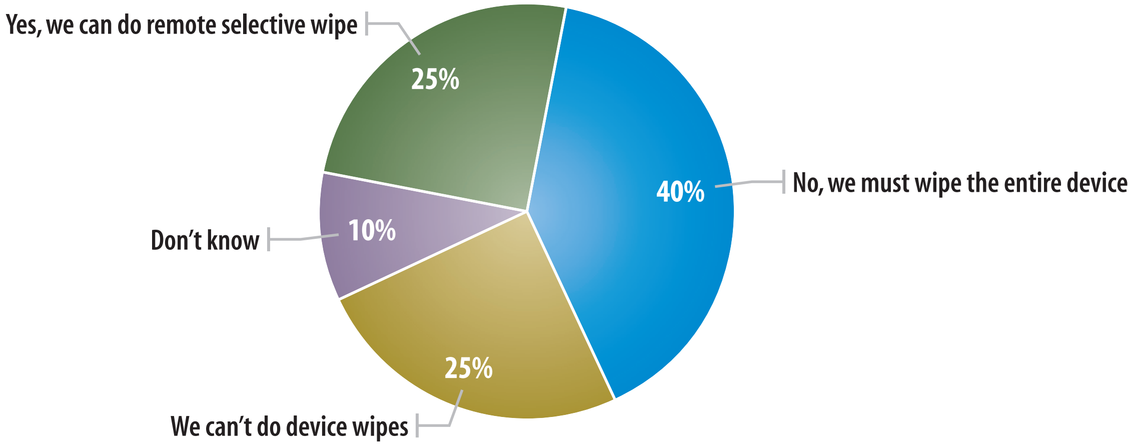
An app or agent actually deployed on the mobile device is vital for managing enterprise data encryption, access to corporate-owned network resources and potentially reacting to a malware infection by deleting local instance of corporate data, as well as restricting access to the corporate network until the infection is handled. Without the agent application, users can change the policy at will and negate any security controls IT put on the device.

As long as only authenticated devices—that is, those with an installed agent or app—are able to connect to the corporate network, IT administrators gain a measure of security knowing that corporate data remains in its own protected sandbox on the mobile device and can be deleted at a moment's notice should an infection occur.

Figure 6

Ability to Selectively Wipe Business Data From Personal Devices

If an employee uses a personal device to access business resources, do you have the ability to selectively wipe (delete) business-related data while leaving personal data intact?



Data: *InformationWeek* 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/20

While this is easy to say, implementing such an architecture may be very difficult, depending on your MDM vendor's integration with standards such as 802.1X or WPA2-Enterprise and on the networking equipment your organization has, so be advised—do research and verify through a proof of concept that the MDM system will work in your environment before cutting a check.

Technology, policy and education, and data segregation aren't just principles of a real-time reactive strategy, they're intertwined. Neglect one, and you lessen the effectiveness of the others. Put all three in place, and you empower your company to overcome the security risks presented by BYOD.

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

Research: Mobile Device Management: The only constant in mobility nowadays is change. This is changing the face of computing—and terrifying the IT managers charged with providing productivity tools while maintaining control of sensitive data.

Strategy: Tablet Security: As businesses rely increasingly on tablets for the productivity benefits they provide, IT must address the security challenges the devices present.

IT Pro Impact: Apple iPhone 4S: With preorders alone totaling over 1 million devices in 24 hours, the 4S is undoubtedly showing up on enterprise networks. Here's a rundown of new hardware and software features and the implications for IT teams charged with supporting mobility.

Informed CIO: Striking a Security/Usability Balance: At CES we saw dozens of new tablets and smartphones with unprecedented capabilities. Employees want to make full use of their shiny new devices, while IT teams want to maintain security and control. The principles of secure user access provide a strategy for CIOs to maintain equilibrium.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek 500* and the annual State of Security report; full issues; and much more.