



Deep Dive Articles

■ STRATEGY

The BYOD Era Has Begun.....	2
Mobile Management, OS by OS.....	6
■ Table: Mobile Management and Security Capabilities Compared.....	7
■ Sidebar: What the Mobile Management Vendors Offer.....	9
Mobile Security: Safer than PCs.....	10

■ HANDS-ON

Say Yes to (Almost) Any Smartphone.....	12
■ Chart: How Each Mobile Platform's Securability Compares.....	17
BES: Express or Deluxe?.....	18



STRATEGY

The BYOD era has begun

A heterogeneous mobile device world means new thinking for IT

By Galen Gruman

IT'S TIME FOR IT TO FACE FACTS: THE GREAT CORPORATE BARRIER against employees using personal smartphones has been breached.

Despite everything you may believe about the need to control employee access and equipment, more and more companies are easing the reins on employee-owned smartphones in the corporate environment.

C-level executives are no longer alone in demanding exceptions for their iPhones. Half of the smartphones in use among U.S. and Canadian businesses are not company-issued equipment, according to a recent report from Forrester Research. In fact, some organizations are even subsidizing employees' service plans as an easy way to avoid the procurement and management headaches of an increasingly standard piece of work equipment. But should you?

Several issues beyond access and security are worth con-

sidering before you decide who should own your employees' smartphones. But take note: Smartphone use among U.S.-based information workers is expected to triple by 2013, according to Forrester. The time to establish your smartphone ownership plan is now.

the likelihood of inactive cell phones going unnoticed on the rolls. Moreover, you can eliminate the need to fight with carriers over billing or to outsource this activity to a TEM (telecom expense management) firm to ensure you're not being cheated. (To get a sense of the severity of carrier billing issues, consider this: Even after paying TEM firms to review and fix billing issues, TEM clients come out ahead, [saving real money on their telecom bills.](#))

But moving to a subsidized, employee-owned smartphone plan probably won't save you money, says Michael Voellinger, executive vice president at Telwares, a telecom services and consulting firm with a long history in the TEM business.

"It's usually a wash," says Voellinger, whose firm has seen some clients save money this way, while others ended up spending more.

Why isn't a capped per-user payment cheaper than setting up and managing a company-wide plan? Because many of the issues that come with employer-paid smartphones also apply when paid by the employee.

For example, if an employee goes overseas and incurs roaming costs, who pays? Or when an employee exceeds a data plan's limits for work purposes, how do you determine your share of this cost? As it turns out, your largest cost ends up being staff time to figure out and process these exceptions as they occur, not the specific extra charges themselves, Voellinger notes.

Moreover, if smartphone charges are treated as a reimbursable expense, it becomes difficult to quantify your telecom spend across the organization. In essence, you're burying the data, which tends to lead to unnecessary usage and, thus, higher costs.

Moving to "employee-liable" smartphones probably won't save you money. But it likely will give workers the tools that work best for them, and make them more likely to take advantage of mobile devices' connected nature.

EMPLOYEE-OWNED SMARTPHONES: A QUESTION OF MONEY

Subsidizing employees' use of their own mobile devices seems like a great way to contain cell phone costs. After all, reimbursing a flat fee for work usage of employees' phones can cap your monthly per-user costs and reduce

EMPLOYER-OWNED SMARTPHONES: A QUESTION OF MANAGEMENT

Of course, many companies that issue smartphones to employees do a poor job monitoring and keeping track of devices. This often leads to some employee usage bills of several thousand dollars on any given month, as well as "ghost" devices that continue to be paid for even after the



employee is gone.

Voellinger advises companies to consider the context of their employees' smartphone use before settling on a strategy. For example, if most employees' use of smartphones for work purposes is limited, then a subsidized, employee-owned smartphone plan can make sense, as it adds convenience at a predictable cost. This approach can also make sense for dispersed organizations, especially those spanning multiple countries, as no single carrier can meet all of their smartphone needs, thereby reducing savings typically available via group discounts and bulk purchases.

But subsidizing employees' personal smartphone use could end up costing much more than an organization-wide plan from a single carrier, Voellinger notes, especially when reliance on mobile minutes and bytes is heavy. For some businesses, cost won't be the deciding factor: Strict auditing or compliance standards may require you to keep personal and corporate systems separate.

Although Voellinger advises companies to issue and manage employee smartphones, he says some companies will nonetheless end up with personal devices in use and should factor them into their policies and systems. (Voellinger walks through many of the considerations [in his own blog](#).)

YOUR SMARTPHONE STRATEGY: OBTAINING THE RIGHT MIX

Of course, your smartphone strategy need not be black-and-white. Some companies may want to mix employee subsidies for certain users with company-provided devices for other users, Voellinger suggests. In other words, you may have several classes of users and choose a different provisioning and cost strategy for each.

Forrester analyst Ted Schadler strongly recommends dividing your information workers into several groups based on how their mobile enablement benefits the company. "Don't treat everyone the same," he says.

For example, you might segment your staff as follows:

- Those who use the most sensitive data get company-paid, company-managed smartphones
- Those who work extensively away from their desks receive subsidies for most or all of their personal smartphone charges
- Those who work away from their desks occasionally receive a partial subsidy for their personal smartphone use

■ Those who rarely work away from their desks receive no subsidy, and you may consider locking their smartphones out of your systems altogether

When considering costs, don't forget that there is more than just service plans and device costs. The complexity of supporting multiple kinds of smartphones — a mix of BlackBerrys, Android devices, and iPhones — adds a cost as well, Voellinger notes. The price for that extra support could neutralize any savings you earn focusing entirely on cell phone access charges.

Then again, that cost could be worth it, Voellinger notes, as it allows you to use the right smartphone for the job. This approach often bolsters employee productivity through increased satisfaction, given the expectations of today's employees, Voellinger says: "What makes my blood boil is that an employee gets downgraded when they walk in the door" compared with what they use at home. The employee's reaction is increasingly likely to be, "You're seriously going to hand me XP Pro and a BlackBerry Curve?"

And don't forget that company-issued and company-managed smartphones have their own support costs, not just for employee support but also for billing and asset management.

NAVIGATING THE SMARTPHONE'S DUAL- USE NATURE

One argument for allowing employees to use their own smartphones for work purposes is that carrying two devices and having two mobile phone numbers is a pain.

Sure, people have long had personal phones at home and office phones at work, but because people carry their smartphones with them most of the time, it can be an employee-friendly policy to let them use just one device for both purposes. It could be a personal device that's subsidized for work usage or a work device that allows personal usage to a certain cost limit.

People take care of personal issues on their work phones and take work calls at home, so allowing for the same mix on a cell phone isn't a stretch. Data capabilities, however, provide a new wrinkle, and the fact that employees' smartphones can store and access company information such as emails, contacts, calendars, and documents is enough to make many IT and security pros wince at the thought of dual use.

This problem is not unique to smartphones. Many



employees work at home — and [even at the office](#) — on personal computers. A December 2009 Gartner survey estimates that 10 percent of midsize businesses allow employees to use their own personal laptop at work, a figure expected to rise to 14 percent this year. Also, some users play games, check personal email, or [run iTunes](#) or Windows Media Player at work to listen to their personal music on their work computers.

“The focus is on mobile, but the problem is universal. What’s the demarcation? There is none,” says Telwares’ Voellinger. “By owning the asset [the smartphone or PC], is the prevention [of abuse or breach] any different? The risk is still the same.”

That’s why the “secret” to smartphone management is “treating employees like grown-ups and using a ‘trust and verify’ model for policy control,” Forrester’s Schadler says. “You have to stop treating it as an IT policing issue and instead treat it as a business risk management question.”

More and more companies are making this shift in their thinking, Schadler says, not just for smartphones but also for [bring-your-own PCs](#) (and Macs) and other user-facing technologies.

Yet for smartphones, the dual-use bar for managing access and data security is quite different, given that most smartphones don’t yet offer PC-level security and management capabilities.

For example, it’s fairly straightforward to require the [use of encryption](#), certificates, and other security tools on Windows PCs, no matter who owns them, thereby allowing IT to ensure that a home PC is secured the same way as a work one. (For Macs, it’s not quite as easy, but still largely possible.) But for smartphones, security and management capabilities vary greatly from device to device. BlackBerrys and Windows Mobile devices can enforce PC-level security and data management if the business has the [right policy servers in place](#). The newest iPhone operating system supports a significant number of policies, but less than on a BlackBerry or Windows Mobile device. Very few policies are enforceable on WebOS, Windows Phone 7, Google Android, and Nokia Symbian devices. Third-party tools are beginning to change that reality, but by and large it’s fair to say that you can’t control the data and access on these newer devices at the same level you can a home PC.

“You need to strike a balance between an IT-controlled management tool set such as you have built for desktop

management and employee-led management, where employees are responsible for their own devices,” says Schadler. “That balance point will vary based on your industry and culture.”

SURPRISE: YOU PROBABLY CAN’T CONTROL AS MUCH AS YOU MAY WANT

Further complicating this issue are the legal ramifications of dual-use devices.

The laws on what employers can do with employees’ personal equipment and accounts haven’t caught up to today’s mix of devices and cloud services, notes Peter Vogel, an attorney at Gardere Wynne Sewell who specializes in Internet, computer, and e-discovery issues. There are plenty of misunderstandings as to what a business can and can’t control.

Despite the legal ambiguity from conflicting court decisions and the lack of precedent in many areas, patterns have developed in cases involving home PCs and other personal technology that may influence your smartphone ownership strategy.

For example, corporate email belongs to the company, and the company has full access to it, no matter where the employee accesses it. Plus, the company can set policies for what is transmitted through corporate email.

“But email issues are complicated by employees who use Webmail services such as Gmail, AOL, and Hotmail to conduct company business. Many courts have ruled that employers lose confidentially and potentially valuable trade secrets when employees send confidential information via Webmail,” Vogel says. That reasoning could easily be applied to the use of personal smartphones.

International issues also pop up, Vogel notes: “Generally in the U.S. emails are private to employers, while in the E.U., Canada, and Japan emails are private to employees. Furthermore, in the E.U. there are data privacy laws for individuals called the [1995 Data Directive](#) that permits citizens of the E.U. to access any computer that contains data about them and change that data. The U.S. has nothing like this at all, and when there is communications between the E.U. and U.S., determining which law applies gets very complicated.”

In a 2008 case, a federal court ruled that text messages on police department-paid pagers belonged to the police officers, not the police department, because the messages



were stored by a carrier. The department wanted the messages to see which were personal so that they could calculate how much the officers owed the department for personal use. Vogel says this case was [decided on very narrow grounds](#) — the fact that the messages were stored at the carrier, which is subject to different laws than a company that stores its own records — but nonetheless raises the kind of ambiguity sure to surface as smartphones are used increasingly for both personal and corporate activities.

You might try to deal with these and other issues through employment agreements, Vogel suggests.

“Generally employees are bound to the terms of employment agreements,” he explains. “So if the employment agreement states that the employees provide their own PDAs or smartphones but the employer pays a monthly allowance, one would have to look at the terms of the employment agreement to see if the employee is entitled to privacy.”

But “generally just having a corporate policy is not enough without some affirmation of the employees to agree,” Vogel notes. “Companies run the risk that courts will conclude that even though corporate policies are in

The laws on what employers can do with employees’ personal equipment and accounts haven’t caught up to today’s mix of devices and cloud services.

place, they are either unenforced or selectively enforced. As a result, without rigid enforcement, a company cannot depend on the courts to adopt these corporate policies regarding who owns emails and text messages and who is entitled to privacy.”

Another issue: What information on these devices is discoverable in a court case?

“Every state is wrestling with this,” says Telwares’ Voellinger. “Pennsylvania, for example, assumes that the moment information goes out onto public networks, it’s discoverable.” That could cover anything delivered through the Internet, for example, which smartphones and PCs use routinely.

THE PRACTICAL ISSUES OF PERSONAL SMARTPHONE USE

Beyond the law are practical considerations: If an employee uses a personal smartphone for business purposes and then leaves the company, customers and partners can still contact that former employee — and may not know how to contact his or her replacement. If the company issues the smartphone, the phone number can be moved to another employee, Voellinger notes. But this risk is not that new nor is it smartphone-specific.

Moreover, although BlackBerrys, Windows Mobile devices, iPhones, and Palm Pres support remote-wipe capabilities, there’s a risk that an employee-owned device could still retain corporate data when the employee leaves, Voellinger says. The risk here can be largely managed by requiring employees to use smartphones that meet specific requirements, so the devices you let access your networks are ones you know you can manage as needed, no matter who owns them.

Some employees may be less apt to answer a personal smartphone after hours when it is subsidized by the employer than to answer a work smartphone issued by the employer, Voellinger says. The reason: The employee figures the subsidy just applies to work hours, especially if getting reimbursed for extra work usage is a painful process. On the other hand, if the phone is routinely used for work and business purposes, there may be no rigid work/home time boundaries in the employees’ mind.

Forrester’s Schadler also recommends that your corporate policy be thought out more than most are: “Most firms that support iPhones require their employees to sign a statement that lets the company do a remote wipe on the device and implement other policies in exchange for application support. We recommend that you extend this policy-based approach to cover [jailbreaking](#), password requirements, and use of features such as cameras and GPS for work purposes.”

In the end, who should own your smartphone? Sometimes the employee, sometimes the company, and sometimes one of each. There are good reasons for all three scenarios, even in the same company. The trick is to understand the ownership options that make the most sense in your context, not fall back to “this is how we’ve always done it.”



Galen Gruman is an InfoWorld executive editor and its [Mobile Edge](#) blogger.



STRATEGY

Mobile management, OS by OS

Enterprise-grade security and manageability aren't exclusive to BlackBerry

By Galen Gruman

ALTHOUGH MORE AND MORE BUSINESSES ARE OPENING UP TO smartphones other than the BlackBerry, it's amazing how many people still believe that the iPhone in particular doesn't have appropriate security for most enterprises. It does, and [iOS 4](#) and later for the iPad, iPhone, and iPod Touch support more security and management capabilities than all competitors except the BlackBerry and perhaps (based on what criteria matter to your business) Windows Mobile. "Businesses do seem to be comfortable with BlackBerry, certainly, and also with Windows Mobile. They are increasingly comfortable with iOS, especially with iOS 4," notes Forrester Research analyst Andrew Jaquith.

Why? Because these three mobile OSes use a mobile management server approach that lets IT set and enforce policies across the user base. In fact, Apple added that capability in iOS 4, released in summer 2010. Most management tools

While you're rethinking your mobile management strategy, go ahead and make your website mobile-friendly as well for iPhones, Androids, and more. Dori Smith explains how in the InfoWorld.com tutorial "[How to make your website mobile today.](#)"

support multiple devices; the exception is BlackBerry Enterprise Server (BES), which supports only RIM devices.

But what about the other mobile devices? Google's Android is fast gaining popularity, now selling more devices than Apple and RIM each. Then there's the new [Windows Phone 7 from Microsoft](#) and WebOS 3.0 in [Hewlett-Packard's short-lived TouchPad](#). Can they safely be brought in?

Let's go through the current versions of the seven major mobile platforms and their variants to see how securely they can be managed. The table at the end of this story highlights the capabilities of each mobile platform for the most common security and management needs.

First, a note on Exchange ActiveSync (EAS) policies, Micro-

soft's protocol for mobile security and device management: EAS is fast becoming the de facto protocol for managing mobile devices, supported to varying degrees by Apple (in iOS and Mac OS X), Google (in Android OS 3 and 4 and in corporate Gmail, and in some Android 2 devices), Hewlett-Packard/Palm (in WebOS 1.1 and later), IBM (in the latest version of Lotus Notes), Nokia (in some Symbian-based devices), Novell (in a server add-on for GroupWise), and of course Microsoft (in Windows, Windows Mobile, and Windows Phone 7). Only RIM is avoiding EAS, preferring to stick with its BES. It's also key to note that although there are 29 possible EAS policies, some of them don't apply to many mobile devices, such as disabling infrared or disallowing unsigned CAB files (Windows-specific app files).

Second, a note on storage of corporate email, calendar, and contact data: Devices that support Microsoft Exchange, IBM Lotus Notes, or Novell GroupWise wipe out the emails and address books when access to the server is revoked — or even just disabled, as in the case of iOS — using protocols such as LDAP to do so. In other words, these servers use the same mechanisms to recall such corporate data from mobile devices as they use for PCs.

RIM BLACKBERRY OS

The key to securing a BlackBerry is to use BES 5.0, which provides over-the-air management based on more than 400 security and management policies that IT can use, from password requirements to remote wiping.

RIM does offer free versions of BES for Microsoft Exchange and IBM Lotus Notes environments; it does not support Novell GroupWise as the full version does.

New to BES 5.03 is the ability to selectively wipe business data and apps from users' BlackBerrys without affecting user data (they must run BlackBerry OS 6 or 7).

Some BlackBerry models support RSA's SecurID second-factor hardware authentication tool, which is required in selected military environments.

RIM BLACKBERRY TABLET OS

RIM's strategy for securing its BlackBerry Tablet OS, used



MOBILE SECURITY AND MANAGEMENT CAPABILITIES COMPARED

Key: EAS = via Microsoft Exchange ActiveSync. BES = via BlackBerry Enterprise Server 5.x. 3PS = via third-party server. NA = information not available

Capability	Apple iOS 3.x, 4.x, 5.x	Google Android 2.x, 3.x, 4.0	HP WebOS 1.x, 2.x, 3.0	Microsoft Windows Mobile 6.x	Microsoft Windows Phone 7.x	Nokia Symbian 2.x, 3.x ¹	RIM BlackBerry 5.x, 6.0, 7.0 ⁹
On-device encryption	Yes	Yes (AOS 3,4)	No	Yes	No	Yes ²	Yes
Over-the-air data encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Complex passwords	Yes	Yes (AOS2.2 and later)	Yes	Yes	No	Yes	Yes
Enforce password policies	Yes ³	EAS ⁴ (AOS 2.2 and later)	EAS	EAS, 3PS	EAS	EAS, 3PS	BES
Support VPNs	Yes	Yes	Yes (WebOS 2.0 only)	No	No	Yes	Yes
Disable camera	Yes ³	No	No	EAS, 3PS	No	No	BES
Restrict/block app stores	Yes ³	No	No	EAS, 3PS	No	No	BES
Restrict/block wireless LANs	Yes ³	No	No	EAS, 3PS	No	No	BES
Remote lockout	Yes ³	EAS (AOS 2.2 and later), 3PS (AOS 2.2 and later)	EAS	EAS, 3PS	EAS	No	BES
Remote wipe	Yes ³	EAS (AOS 2.2 and later), 3PS (AOS 2.2 and later)	EAS	EAS, 3PS	EAS	EAS, 3PS	BES
Selective wipe of business apps and data only	3PS (iOS 4,5)	No	No	No	No	No	BES (BB OS6,7 only)
Enforce and manage policies	EAS, 3PS (iOS 4,5)	EAS (AOS 2.2 and later)	EAS	EAS, 3PS	EAS	EAS, 3PS	BES
EAS policies supported	14	9 (AOS 2.2) ⁵ , 13 (AOS 3,4) ⁵	5 (WebOS 1,2), 7 (WebOS 3)	29 ⁶	7	NA	none ⁷
Manage over the air	EAS, 3PS (iOS 4,5)	EAS (AOS 2.2 and later), 3PS	EAS	EAS, 3PS	EAS	EAS, 3PS	BES
Second-factor authentication (RSA SecurID)	No	No	No	Yes ⁸	No	No	Yes ⁸

Notes: 1. Some Nokia E-series and N-series devices only. 2. Storage cards not encrypted. 3. Via choice of Apple iPhone Configuration Utility (no over-the-air confirmation or auditing), Mac OS X 10.7 Lion Server, EAS, and 3PS. 4. Require PIN only. 5. Some third-party email client applications support additional EAS policies within those applications only. 6. Exchange Server Enterprise license required for support of all 29 EAS policies, lower-tier licenses support 15 EAS policies. 7. BES supports more than 500 policies of its own. 8. Some device models only. 9. BlackBerry Tablet OS 1.0 requires BlackBerry tethering to support all these capabilities except VPN.



in the [RIM PlayBook](#), is the same as for the BlackBerry: BES. But that's because the PlayBook must be wirelessly tethered to a BlackBerry to access corporate resources; the BES that protects the BlackBerry thus protects BlackBerry data available via the PlayBook. Note that BlackBerrys and PlayBooks not managed by BES have no security capabilities.

APPLE IOS

iOS 4 stepped up mobile management significantly by allowing auditable, assured application of EAS policies, as well as iOS-native policies, over the air. It allows for selective wiping of business data and apps, and it supports complex passwords, on-device encryption, and remote wipe.

iOS supports 14 EAS policies managed through Exchange, and it uses configuration payloads that can be emailed to users, made accessible via a Web link, or provisioned over the air through [Mac OS X 10.7 Lion Server](#). If you use a mobile device management tool from AirWatch, Boxtone, Good Technology, MobileIron, Symantec, Sybase's Afaria unit, Tangoe, Trelia, Zenprise, or others, you can audit and enforce their use, as well as provision them over the air.

iOS 5 adds a few additional policies for MDM tools to take advantage of as well: They can turn off iCloud syncing, require the use of a password to access iTunes, disable email forwarding, delete – not just render inaccessible – apps (both individually and for all corporate-provisioned apps), disable voice and data roaming, set policies for the handling of nontrusted certificates, detect and reapply user-deleted MDM configuration profiles, set Web proxies, set autologin for approved Wi-Fi access points, send crash data, and monitor battery levels

MICROSOFT WINDOWS MOBILE

Although this mobile OS was discontinued two years ago, it remains in use at many companies running legacy applications, especially in government. Windows Mobile 6.x supports all 29 EAS policies if you use an enterprise license for Microsoft System Center Mobile Device Manager, which is part of Exchange; otherwise, it supports 14 EAS policies.

A variety of mobile management tools support Windows Mobile devices as well, and some Windows Mobile devices support the SecurID authentication device.

MICROSOFT WINDOWS PHONE 7

The new Microsoft mobile OS has fewer management

and security capabilities than Windows Mobile, even though it uses the same Exchange or EAS-compatible servers as the management console. The biggest omissions are lack of support for on-device encryption and for requiring use of complex passwords, so will not work with many companies' ActiveSync policy requirements. (Microsoft says it will add such support later.)

Windows Phone 7 – including the 7.5 “Mango” release of fall 2011 – supports fewer EAS policies than Windows Mobile and iOS, for example. It does not support several policies that may matter to some enterprises: disable camera and disallow application downloads. It also doesn't support VPNs.

GOOGLE ANDROID OS

Although one of the most popular smartphone OSes, Android has been among the least secure. The Android 2.2 and earlier smartphone versions do not have on-device encryption nor do they support complex passwords, for example. “Enterprises are generally quite uncomfortable with Android right now, partly because the enterprise security road map doesn't seem to clear to them, and partly because the vast number of Android devices makes it hard to understand what will work for them and what won't,” says Forrester's Jaquith. “The lack of OS file system encryption is often cited as a concern.”

But just as rabid iPhone users forced many businesses to allow iPhones in before Apple stepped up iOS's security, enthusiastic Android users are doing the same today. “Many customers seem willing, essentially, to punt and use something like Good Technology's product to put a secure workspace on Android devices so that they can use them,” Jaquith notes. IBM's Lotus Notes Traveler app adds such a secure workspace for Notes users, as does NitroDesk's TouchDown app for Exchange users.

Over time, Android should get more secure. In fact, the tablet-oriented Android 3.0 OS does support on-device encryption and policies for complex passwords, password history, and password expiration.

The [Android 4 OS](#), released in late 2011 for some devices, brings those security capabilities to Android smartphones, as well as tablets.

And it may not be just Google that fills in that blank in the short term. For example, Android 2.2 includes only a basic VPN, but Motorola Mobility's Droid Pro includes the more robust and beefed-up AuthenTec IPSec multi-



■ WHAT THE MOBILE DEVICE MANAGEMENT VENDORS OFFER

As smartphones and tablets proliferate, and as employees make the case for device diversity, IT is faced with the challenge of managing access, usage, and security across multiple mobile devices. To address that need, many vendors have developed tools that provide a central console to manage multiple devices over the air with a common set of policies, ensuring consistent policy enforcement and providing auditing capabilities as well.

These tools use one of two approaches, and sometimes both: (1) They use policy profiles, typically based on the widely used Microsoft Exchange ActiveSync (EAS) protocol. (2) They use a client application on each supported device to provide the managed, secured workspace and additional policies. Those that support the BlackBerry work with Research In Motion's own tool, BlackBerry Enterprise Server (BES).

AirWatch supports Android, BlackBerry, iOS, and Windows Mobile. It also provides content-filtering policies, provides data-roaming policies, and allows on iOS 4 selective wiping of business data (leaving personal data intact for employee-owned devices).

Boxtone supports Android, BlackBerry, iOS, and Windows Mobile. It also provides tools for troubleshooting user devices, user self-registration, and asset tracking (including carriers used).

Good Technology's Good for Enterprise and Good for Government tools support Android, iOS, Symbian, and Windows Mobile. The tools also permit control over application installation, allow on iOS 4 selective wiping of business data (leaving personal data intact for employee-owned devices), and can be set to allow

only specific device/operating-system combinations.

McAfee's Trust Digital EMM supports Android, iOS, Symbian, Windows Mobile, and WebOS. It also provides tools for troubleshooting user devices and user self-registration.

MobileIron's MobileIron Server supports Android, BlackBerry, iOS, Symbian, Windows Mobile, and WebOS. It also permits control over application installation, allows on iOS 4 selective wiping of business data (leaving personal data intact for employee-owned devices), and provides telecom expense management capabilities.

Sybase's Afaria supports Android, BlackBerry, iOS, Symbian, and Windows Mobile. It also provides control over application installation, lets IT set up an internal "app store," and permits asset tracking of mobile devices.

Symantec's Mobile Management supports Android, BlackBerry, iOS, and Windows Mobile. It also provides application update management, asset management, and endpoint security capabilities such as antimalware.

Tangoe's MDM supports Android, BlackBerry, iOS, and Windows Mobile. It also permits control over application installation and provides telecom expense management and service monitoring capabilities.

Trellia's MDM supports BlackBerry and iOS, with Android support planned. It also provides data-usage policies.

Zenprise's Mobile Manager supports Android, BlackBerry, iOS, and Windows Mobile. It provides telecom expense management and service monitoring capabilities.

headed VPN. Likewise, the Motorola Mobility [Atrix, the Photon 4G, and its other business smartphones](#) uses adds on-device encryption and Android 3-level EAS policies despite Android 2.2's lack of native support for them.

HEWLETT-PACKARD WEBOS

Although WebOS got a lot of buzz before it was released in 2009's Palm Pre, it didn't win a significant audience. HP bought it in summer 2010, released the WebOS 2.0 update in fall 2010, and released WebOS 3.0 in summer 2011.

But WebOS remains the least secure of the major mobile OSes. WebOS 1 and later support complex passwords, WebOS 2 introduced support for VPNs, and WebOS 2.1 added support for on-device encryption. WebOS 1 through 3 support just five EAS policies: four for password management and one for remote wipe. WebOS 3 added two more. Unlike Android, there aren't client apps that can create secure workspaces to fill in the security gaps.

NOKIA SYMBIAN

Billed as the most popular smartphone OS in the world, Symbian is almost invisible in the United States. Symbian's share of global Web traffic has declined steadily, as Nokia has retired it for smartphones in favor of Windows Phone 7.

The Symbian OS comes in many varieties, with most Nokia devices not supporting business-class security or management. But the Nokia E-series and N-series devices usually support the basics, including on-device encryption, complex passwords, and remote wipe. These devices support an unknown number of EAS policies – Nokia wouldn't say how many – but the total appears to be fewer than iOS.

Disabling the built-in camera and preventing access to Wi-Fi networks are two examples of EAS policies that iOS and Windows Mobile handle (and that BES offers) that Symbian does not. Many mobile management tools support these Nokia devices.

Galen Gruman is an InfoWorld executive editor and its [Mobile Edge](#) blogger.



STRATEGY

Mobile security: Safer than PCs

Malware is not yet a serious problem, but other threats could emerge

By Galen Gruman

IN SECURITY CIRCLES, THE TALK ON MOBILE CENTERS AROUND mobile management, protecting access to and use of corporate information by smartphone users. Summer 2010's iOS 4 was a game-changer for most IT organizations, giving the Apple iPhone, iPad, and iPod Touch security capabilities equivalent to those of Windows Mobile and meeting the needs of most BlackBerry users, ending the main objection at many companies for allowing iOS devices in. (When used with BlackBerry Enterprise Server, the RIM device does remain more secure for high-requirements organizations.)

What they're not talking about are threats that reach the smartphone itself, the equivalent of the malware that ravages Windows PCs every day. There are no equivalents of Symantec's Norton Antivirus or Kaspersky Lab AntiVirus for iOS devices, and just a handful for, Android devices, and BlackBerrys. Does that put your devices at risk, or are they somehow inherently secure?

A key reason that so-called endpoint mobile security is not seen as a big deal is that mobile OSes such as iOS, Android, BlackBerry, and Chrome OS use a couple techniques not common on desktop OSes to make infection more difficult. One is sandboxing, which confines apps and their data and requires explicit permission to exchange data among them. The other is code-signing, which makes software developers register and be vetted before their apps can be installed.

"A lot of mobile devices have a very different security model," says Scott Crawford, a security analyst at the consultancy Enterprise Management Associates (EMA), and the OS makers have built in security from the get-go. "By contrast, the original Windows had very little security," creating a tempting target early on and an architecture whose vulnerabilities became widely known.

There've long been antivirus products for Windows Mobile and Nokia Symbian devices, but they're not that necessary. All smartphone platforms combined have seen fewer than 1,000 malware threats, versus hundreds of thousands for Windows PCs, notes Khoi Nguyen, group prod-

uct manager for mobile security at Symantec. In fact, the need for antimalware apps on smartphones is so low that Symantec is focusing on delivering mobile management tools instead. (It and McAfee do offer antimalware tools for Android, though, which has proven [highly susceptible to malware](#) through its unregulated app market.)

THE EMERGING THREATS, AND WHO'S SUSCEPTIBLE

But despite their more secure designs, a few threats have begun to emerge for mobile OSes, so security experts and vendors figure it's just a matter of time before the increased usage of such devices and their use of more valuable information than just emails will attract hackers. For example:

■ The [Android Market contains lots of apps that are spyware](#), Trojan horses, or other malware. One recent malware app [secretly sends SMS messages](#) to a Russian service, which charges the user very high fees for the messages. Google doesn't evaluate the apps posted there for security or other concerns, pulling malware from the Android Market only after enough users complain, and the company requires minimal information for developers to be code-signed, notes EMA's Crawford.

■ Apps don't have to be malware to be trouble, says Symantec's Nguyen. He cites an Android app whose poor coding saps lots of network access, overwhelming nearby cell towers and making it unavailable to other users. Hackers who want to do denial-of-service attacks can use such techniques intentionally.

■ A flaw in the PDF reader plug-in for mobile Safari let hackers [load a jailbreaking app onto iOS devices](#) — raising the specter of desktoplike malware on the iPhone and iPad, though Apple quickly patched the flaw.

■ One Apple developer's code-signing identity was stolen, letting the thieves submit apps to Apple under his name. Crawford says that shows the Achilles' heel of the cryptography-based code-signing approach: There's a single "root of trust" that, once breached, makes everything vulnerable, and the breach often can be done through non-technological means (phishing is the prime example).



■ Nokia has seen several episodes of Symbian vulnerabilities relating to flaws in its code-signing technology — a year ago, one hacker even found a way to disable the code-signing requirement, Nguyen recalls — and in 2005 [a major malware attack](#) caused Nokia to rework the OS's security approach.

It's situations like these — especially for the unvetted Android Market — that has Kaspersky Lab working on an Android antimalware app. But Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab Americas, isn't so sure there'll be equivalent products for iOS, BlackBerry, or Windows Phone 7 because all do more serious vetting of the apps sold through their stores — at least not in the near future. He notes that sandboxes aren't hacker-proof and may get easier to hack as more connections are made between sandboxes to allow applications to work together or share data, as users expect from their desktop experience.

There likely won't be an antimalware app for iOS devices — because Apple won't allow them, note both Schouwenberg and Crawford. (Apple declined to comment.)

As mobile devices get more popular and users access and store more valuable information than email on them, they'll begin to attract the attention of hackers now happily making lots of money by breaking into Windows PCs. "It will happen," says Ted Julian, a mobile security analyst at Yankee Group.

It's clear that if any mobile OS is likely to be the easy target for hackers, it's Android, whose architecture is most like that of the desktop PC due to its openness, says Schouwenberg. "Android is forcing other OSes to be more open, which increases risk," adds Symantec's Nguyen.

It's also harder to protect Android devices than other devices, notes Julian. The reason: There are so many Android variants in use — four versions of the OS itself, just as many UI overlays from device makers, and a variety of other customizations from both carriers and device makers — that [Google or the carriers couldn't quickly patch all the devices](#) as, say, Apple can with its iOS devices.

THE FALSE SECURITY OF APP STORES

Apple pioneered the concept of a vetted app store, and every other mobile platform maker has followed suit. It's well known that [Apple reviews apps](#) to ensure they conform to Apple's programming and even "decency" standards, and such review gives users the sense that Apple has

filtered out malicious apps, says Julian.


But that's a risky assumption for any app store, not just Apple's, Julian says. Reviewing all the apps line by line by security experts simply isn't possible given the thousands of apps that are submitted each month, and automated code analysis tools aren't yet up to snuff, he notes. Julian says that Apple, Google, Microsoft, RIM, and the rest will eventually be able to find the "obvious stuff," reducing the risk to everyone's benefit. But some malware will still get through.

Android users can make any vetting meaningless by [disabling the OS's block on unsigned apps](#), a setting easily changed in the OS's Settings app. Some users disable the block so that they can install apps not available in the Android Market, such as apps not authorized for their specific device/carrier combination. Likewise, iOS devices [jailbroken to allow unapproved apps](#) undercut any security vetting by Apple in the App Store.

Theoretically, sandboxing would limit the damage of mobile malware. And it will, everyone interviewed for this article agreed. "It's good that people are building in isolation" via sandboxes, Julian says. But it's not a perfect defense. "You can Swiss-cheese a sandbox," notes EMA's Crawford, as you add mechanisms to allow apps to communicate with each other or share data.

The app most likely to have such holes punched in it is the browser, for which plug-ins add both capabilities and entry points for hackers, as Apple discovered in the PDF-jailbreak vulnerability, says Kaspersky's Schouwenberg. "That showed the limits of sandboxes."

Crawford notes the issue "wasn't the design of the browser itself, but how it's stretched — through the extensions, helper objects, and plug-ins that open the doors where control is slight." He notes that users want such extensions, which are often developed by smaller companies and individual developers not necessarily well versed in application security, so mobile OS makers who wall off the browser are likely to get strong user pushback.

And the push to [using HTML5](#) as a pan-mobile application development platform could increase the risk of the browser as a malware vector, he says, if the HTML5 apps were to rely on local helper apps. Web apps concern Crawford the most of all the potential mobile threats because "Web security is getting too little action today," despite the constant stream of reported exploits on the desktop. 

Galen Gruman is an InfoWorld executive editor and its [Mobile Edge](#) blogger.



HANDS-ON

Say yes to (almost) any smartphone

How to welcome iPhones, Androids, and other devices beyond the BlackBerry

By Galen Gruman

RESISTANCE IS FUTILE: THE IPHONE HAS WON. TRY AS YOU MAY to maintain the great corporate barrier against employees using the latest smartphones on your network, the iPhone has or will soon enter your business and connect to your IT systems, and Google's Android devices such as the Galaxy series are not far behind. In fact, many CIOs and CSOs have already stopped resisting and are instead putting their energies to greater use: figuring out how to say yes to smartphones that are quickly becoming key business devices.

Sure, devices such as the iPhone have strong personal utility and appeal, but they are also increasingly able to meet core corporate security and management needs. The PC revolution 25 years ago blurred the distinction between "business" and "personal." Today's mobile devices are meeting IT halfway, permanently ending any pretence of a hard line. Now it's your turn to figure out how to make the most of the smartphone revolution.

This guide will help you say yes to the latest mobile devices, beginning with security capabilities, which remain a core concern for most organizations. To address this issue, I've created four classes to cover most businesses' security needs. I then explain how to ensure that each mainstream mobile device can meet those requirements, noting clearly when a particular device is ill-suited to your environment. Your obligations may vary, but you can fine-tune your smartphone strategy by starting with the closest-fitting category.

To hone your pursuits, I've focused on Apple's iPhone (including the iPod Touch and iPad), Google Android OS devices, Microsoft Windows Mobile and Windows Phone 7, business-oriented Nokia Symbian devices (such as the S60 and E71), and Research in Motion's BlackBerry. Hewlett-Packard's WebOS-based devices have been discontinued, so I've not included it here in the detailed explanations.

Given the importance of email on mobile devices, I also note considerations for the main business email platforms — IBM Lotus Domino/Notes, Microsoft Exchange, and Novell GroupWise — and explain when it might make sense to use a third-party mobile management product. Be aware that many of those products don't really add

security capabilities. Some simplify the provisioning of the devices' native security capabilities, but most are focused on monitoring and managing your cellular telecom spend, tracking the devices as assets, and giving IT basic status information for help desk support. Rather than adding yet another management tool, you may want to opt out of the smartphone-provisioning business altogether, which may solve the accounting issues these management platforms have been devised to address.

Keep in mind that mobile is a moving target. The advice that follows is based on what is available today, but vendors (hopefully) will continue to improve their products' capabilities.

WHAT SECURITY CATEGORY FITS YOUR NEEDS?

Although [scare stories about smartphone security](#) often try to hold these devices to the standards of military and financial services firms, most companies don't require those levels of security. Besides, many defense and financial services firms have already figured out how to support iPhones and iPads despite their higher security needs. Bank of America, Citigroup, Nationwide Insurance, and Standard Chartered are recent examples.

Many companies will require a blend of the four broad categories outlined below. After all, you likely support employees who are involved in sensitive negotiations, as well as those who have little to no access to vital corporate data. As such, your "say yes" strategy should reflect that internal diversity. The universal truth of mobile is that it is not one-size-fits-all.

One final note: If you're not treating employee use of personal and provisioned PCs and laptops with the same level of security requirements you're placing on mobile devices, then something's wrong. Doing so would mean a more immediate security gap to fix at the PC level.

Category 1: Routine business information. Truck drivers, sales reps, sales clerks, graphics designers, Web developers, repair and maintenance staff, personal coaches, restaurateurs — people in these professions deal with routine



information that is rarely personally or legally sensitive.

If their smartphone is lost or stolen, the resulting hassle amounts to reconstructing some data, ensuring the cell service is discontinued, and buying and re-outfitting a replacement device. There's a risk of a thief accessing your email, so you do need to immediately change passwords at the server.

Required security includes a PIN to use the device. Good, but not essential, security and management capabilities incorporate password expiration and complex-password requirements, remote wipe, in-transit SSL encryption of email and other data, and a "wipe contents after x failed attempts" policy.

Category 2: Important business information. Sales managers, veterinarians, personal assistants, management consultants, IT administrators, teachers, editors, videographers, programmers, most midlevel managers — people in these professions and positions have access to some personal and financial information that won't make or break the company but could cause economic or PR damage worth preventing. They may also have access to some internal systems via passwords that could be abused by a bad actor who gets the device.

If their smartphone is lost or stolen, the cleanup effort goes beyond the individual's information and may require changing shared passwords, informing business partners, and losing short-term competitive advantages.

Required security and management capabilities include a complex password to use the device, password expiration, remote wipe, in-transit SSL encryption of email and other data, and a "wipe contents after x failed attempts" policy. Good, but not essential, security and management capabilities include VPN and/or second-factor access to sensitive systems and data stores, and on-device encryption.

Category 3: Sensitive business information. Finance staff, auditors, bankers, medical professionals, HR staff, lawyers, regulators, product managers, researchers, division managers, lead IT admins, marketing and sales chiefs, chief executives in most firms, and all of their assistants — people in these impressions work with significantly confidential information (legal, financial, product, and personal) and usually have significant access to key internal data stores and systems.

If their smartphone is lost or stolen, there could be serious financial consequences, such as the notification costs if personally identifiable information is unprotected and the

competitive losses if details on business negotiations, staff salaries, and the like are revealed.

Required security and management capabilities include a complex password to use the device, password expiration, remote wipe, in-transit SSL encryption of email and other data, a "wipe contents after x failed attempts" policy, VPN and/or second-factor access to sensitive systems and data stores, and on-device encryption. Good, but not essential, security and management capabilities include the ability to control access to specific networks, to turn off the built-in camera, and to control application installation.

Category 4: Top-secret information. Military contractors, spies, police, senior diplomats, military personnel, congressional chairmen and their aides — people in these professions work with confidential information, the exposure of which could jeopardize individual's lives or compromise the public at large.

Required security and management capabilities include a complex password to use the device, password expiration, remote wipe, in-transit military-grade encryption of email and other data, a "military-grade wipe contents after x failed attempts" policy, VPN access to sensitive systems and data stores, physical second-factor authentication support, military-grade on-device encryption, support for S/MIME and FIPS 140 standards, and discrete "lockdown" control over accessible networks and allowable applications.

SECURING THE NEEDS OF CATEGORY 1 BUSINESSES FOR ROUTINE INFORMATION

If your business deals with routine information, it's pretty easy to embrace smartphones beyond the BlackBerry.

Apple iOS. The iOS used in the iPhone, iPad, and iPod Touch supports the PIN requirement for this category, as well as all the good-to-have options. (Note that email encryption is handled through on-device encryption, but just for the iPhone 3G S, iPhone 4, iPhone 4S, third- and fourth-generation iPod Touches, iPad, and iPad 2.) SSL encryption of messages in transit is a native capability of iOS.

Enforcing these requirements and options is the issue at hand. If you can't trust users to enable themselves, you can opt for the free [iPhone Configuration Utility](#) to set up the security policy profiles. But to ensure employees actually install the profiles, you have to manually sync them via a USB cable to your PC. If you trust your staff, you can send them the profiles or have them install the profiles from a



Web link. Another option that enables both over-the-air provisioning and enforced installation is the use of Mac OS X 10.7 Lion Server's new policy management tools.

Otherwise, you'll need a third-party mobile management tool, such as those from AirWatch, Boxtone, Good Technology, MobileIron, Symantec, Sybase's Afaia unit, Tangoe, Trelia, or Zenprise, among others. These also support over-the-air management, compliance and deployment auditing, and additional security controls that the iPhone Configuration Utility does not, and more policies than Lion Server.

If you use Microsoft Exchange 2007 or 2010, you can enforce PIN and password-expiration requirements using EAS policies. You can also issue a remote-wipe command via EAS.

Lotus Notes-based organizations can password-protect email access by combining Domino 8.5.1 or higher with the free Lotus Notes Traveler app available at the iTunes App Store. Notes Traveler also provides remote wipe of email, calendar, and contact data. But Domino/Notes can't enforce device-wide policies on the iPhone or iPad, just on Notes access, though it can remotely lock or wipe an iOS device. If such policy enforcement is critical, you might consider the profile validation, device locking, and access control capabilities provided by a third-party mobile management tool.

If you use Google's corporate Gmail, you're restricted to using EAS policies.

If you use Novell GroupWise, you can use the Data Synchronizer Mobility Pack add-on for GroupWise 8 to manage the iPhone via EAS policies. Or you can use the GW Mail iPhone app to provide a secure email client that works with GroupWise 6 and later – but GW Mail can't enforce device-wide policies, just policies within its client.

Google Android. Android devices can be set to require a PIN or custom swipe pattern before they can be accessed, and with Android 2.2 and later you can require use of a password on the device and remote-wipe it. It also supports SSL in-transit encryption, but it does not support on-device encryption. The tablet-oriented Android 3.0 *does* support encryption, as well as EAS policies for password expiration, password history, and password complexity. So does Android 4.0 for both smartphones and tablets, as well as [Motorola Mobility's line of Android 2.x smartphones](#).

So far, there are only two general options for more-secure Android usage, such as to gain encryption of stored email data on pre-3.0 devices. One is NitroDesk's TouchDown

app, which provides Exchange 2003 and 2007 access, as well as allows you to enforce EAS PIN requirements and enable EAS remote wipe. Each user would need to install this app. It's critical to note that many Android phones that claim Exchange compatibility, such as the Motorola Droid and HTC Droid Eris, do not support EAS policies natively, just unsecured Exchange synchronization. Thus, their built-in mail clients won't connect to an Exchange server that uses EAS policies. The Android 2.2 OS update brings some EAS policy support to such devices, such as password requirements.

The other option is to deploy a third-party management tool's client, such as the Good for Android app, which provides email, calendar, and contact access to both Exchange and Notes servers. The app can require a password, encrypt the messages and other data, and remotely wipe the messages and other information stored within the app. Of course, using it requires having a Good for Enterprise server in place. The same is true for similar clients from MobileIron and others.

For Lotus Notes environments, IBM has an Android version of its Lotus Notes Traveler app that lets you secure access to Notes and to data pulled in from Notes, as well as remote-wipe that data.

Microsoft Windows Mobile. Windows Mobile supports this category's PIN requirement and the good-to-have options. You can enforce most of them using Microsoft Exchange and its EAS policies; SSL encryption of messages in transit is a native capability of the Windows Mobile operating system.

If you use Lotus Notes with Domino 8.5.1 or later, you can use the free Lotus Notes Traveler app to remote-wipe Notes email, calendar, and contact data. But Domino/Notes can't enforce any device-wide policies on the iPhone, just on Notes access.

If you use Novell GroupWise 8, you can install the optional Data Synchronizer Mobility Pack to gain EAS policy access. Otherwise, you're stuck with the Mobile Server product, which uses the Nokia IntelliSync technology (discontinued in late 2008) rather than EAS to manage devices; that means each device needs to have an IntelliSync client installed, though Novell is no longer providing the client. Effectively, this limits GroupWise to older Windows Mobile (5.0 and 2003) devices.

Windows Mobile 7. Microsoft's newest mobile OS



has less support for security than Windows Mobile. In this category, it supports the PIN requirement, as well as the following good-to-have capabilities: SSL encryption of in-transit email, and remote wipe. It does not support the good-to-have on-device encryption or complex-password enforcement policy.

You can enforce the supported policies if you're using an EAS-compatible server such as Microsoft Exchange, Google's corporate Gmail, or GroupWise 8 with the optional Data Synchronizer Mobility Pack installed.

There is currently no support for Lotus Notes.

Nokia Symbian. Many Nokia devices support this category's PIN requirement, as well as the good-to-have options.

For Exchange users, Nokia supports a subset of EAS policies and management capabilities, but the company declined to say which. It appears from my research that Nokia supports fewer EAS policies than Apple's iOS 4 or 5.

For Notes users, IBM offers the Lotus Notes Traveler application to secure Notes email, calendars, and contacts, and to remote-wipe that data. If you want to manage Nokia devices, the Good for Enterprise server bundle can do the trick for some models such as the S60, if you're using Exchange or Notes/Domino.

For Novell GroupWise, you're limited to older devices that use the discontinued Nokia IntelliSync technology, which also requires you to have GroupWise Mobile Server in place.

RIM BlackBerry. The BlackBerry supports this category's PIN requirement and all the good-to-have options — if you use the BES or BES Express servers in addition to your Exchange, Notes, or GroupWise server.

The new free BES Express server software makes BlackBerry management a viable option for small businesses that use Microsoft Exchange or Lotus Notes. Without BES, the BlackBerry can have a PIN set on the device itself and can encrypt in-transit messages.

If you run Microsoft Exchange and want to use its EAS policies instead of relying on BES (such as if you support other smartphones in addition to BlackBerrys), there are third-party tools that let the BlackBerry support EAS, including AstraSync and NotifySync.

Note that the BlackBerry PlayBook tablet does not have any native security capabilities in the 1.0 version of its operating system (that may change in 2012's expected 2.0 release). But the tablet has no access to corporate data protected by BES unless you tether the PlayBook first to

a BlackBerry smartphone, in which case the tablet is just a window onto the protected smartphone's data and apps.

SECURING THE NEEDS OF CATEGORY 2 BUSINESSES FOR IMPORTANT INFORMATION

If your business deals with important information, it's a bit harder to embrace smartphones beyond the BlackBerry, but you can confidently support iOS, Windows Mobile, and Nokia Symbian.

Apple iOS. iOS supports all the requirements for this category, as well as the good-to-have options such as VPN support. The issues and capabilities for Category 2 businesses are the same as those described for Category 1 businesses.

One Category 2-specific issue to be aware is that the VPN support for Cisco networks does not let you use Cisco profile distribution files; you have to manually enter the VPN profile or use the iPhone Configuration Manager, Mac OS X Lion Server, or a third-party management tool to generate it, so there's more IT overhead in implementing VPN access.

Google Android. The Android 2.x operating system lacks the services to provide many of this category's requirements, such as on-device encryption and password expiration. OpenVPN and PPTP/IPsec VPNs are supported in the operating system but may not be available in all devices (device makers don't have to implement it). Android 3.x and 4.0 do fill in the gaps on encryption and password expiration policies.

If your concern is about protecting email, calendar, and contacts data — and you use a compatible VPN — you can probably compromise the Category 2 requirements a bit for Android users. But you can't meet them all.

Microsoft Windows Mobile. Windows Mobile supports all the requirements for this category, as well as the good-to-have options such as VPN support. The issues and capabilities for Category 2 businesses are the same as described previously for Category 1 businesses.

However, for large-scale deployments in Microsoft-based IT shops, you may want to use Microsoft System Center Mobile Device Manager 2008, which lets you add self-provisioning, such as for password resets, and handle thousands of users across multiple Active Directory controllers if they are in the same forest.

Windows Phone 7. The Microsoft OS supports most of the requirements for this category, with the notable excep-



tions of a complex-passwords policy. It supports none of this category's good-to-have options. The issues and capabilities for Category 2 businesses are the same as those described for Category 1 businesses.

Nokia Symbian. Nokia supports all the requirements for this category, as well as the good-to-have options such as VPN support. The issues and capabilities for Category 2 businesses are the same as those described for Category 1 businesses.

RIM BlackBerry. The BlackBerry supports all the requirements for this category, as well as the good-to-have options such as VPN support. The issues and capabilities for Category 2 businesses are the same as those described for Category 1 businesses.

SECURING THE NEEDS OF CATEGORY 3 BUSINESSES FOR SENSITIVE INFORMATION

This level of business – financial services, legal, HR, and health care – is where businesses have to start making support choices that could displease users.

Apple iOS. The iPhone and iPad support all the requirements for this category. The issues and capabilities for Category 3 requirements are the same as those described for Category 1 businesses.

Where iOS becomes problematic is in the good-to-have capabilities. You can disable the camera and limit Wi-Fi access to specific SSIDs via the iPhone Configuration Utility's or Lion Server's profiles or through third-party management tools.

Likewise, you can use third-party management tools to restrict users to specific apps. Using the iPhone Configuration Utility, Lion Server, or a third-party management tool, you can disable the App Store, Safari, and iTunes, but those are heavy-handed control options that will reduce the iPhone's intrinsic utility and appeal.

Google Android. The 2.x version of Android OS lacks the services to provide most of this category's requirements, so it cannot legitimately meet the needs of Category 3 businesses. Android 3.x and 4 do meet this category's basic needs, but not the nice-to-have capabilities.

Microsoft Windows Mobile. Windows Mobile supports all the requirements for this category, but you'll need Microsoft System Center Mobile Device Manager 2008, Good for Enterprise, or Mobile Iron products to handle the good-to-have option of managing which applications

users may install. Otherwise, the issues and capabilities for Category 3 businesses are the same as those described for Category 1 businesses.

Windows Phone 7. The Windows Phone 7 OS lacks the services to provide most of this category's requirements, so it cannot legitimately meet the needs of Category 3 businesses.

Nokia Symbian. Nokia supports all the requirements for this category. The issues and capabilities for Category 3 businesses are the same as those described for Category 1 businesses. For the good-to-have options, I could not find third-party management tools that provide them for Nokia's devices.

RIM BlackBerry. The BlackBerry supports all the requirements for this category – if you use the full version of BES with Notes or GroupWise, or either the free Express or the paid full version of BES for Exchange. You'll need the full BES for the good-to-have features for all three email platforms. The issues and capabilities for Category 3 businesses are the same as those described for Category 1 businesses.

SECURING THE NEEDS OF CATEGORY 4 BUSINESSES FOR TOP-SECRET INFORMATION

If your business deals with life-critical information, such as for defense work, there are only two viable smartphone options: BlackBerry and Windows Mobile.

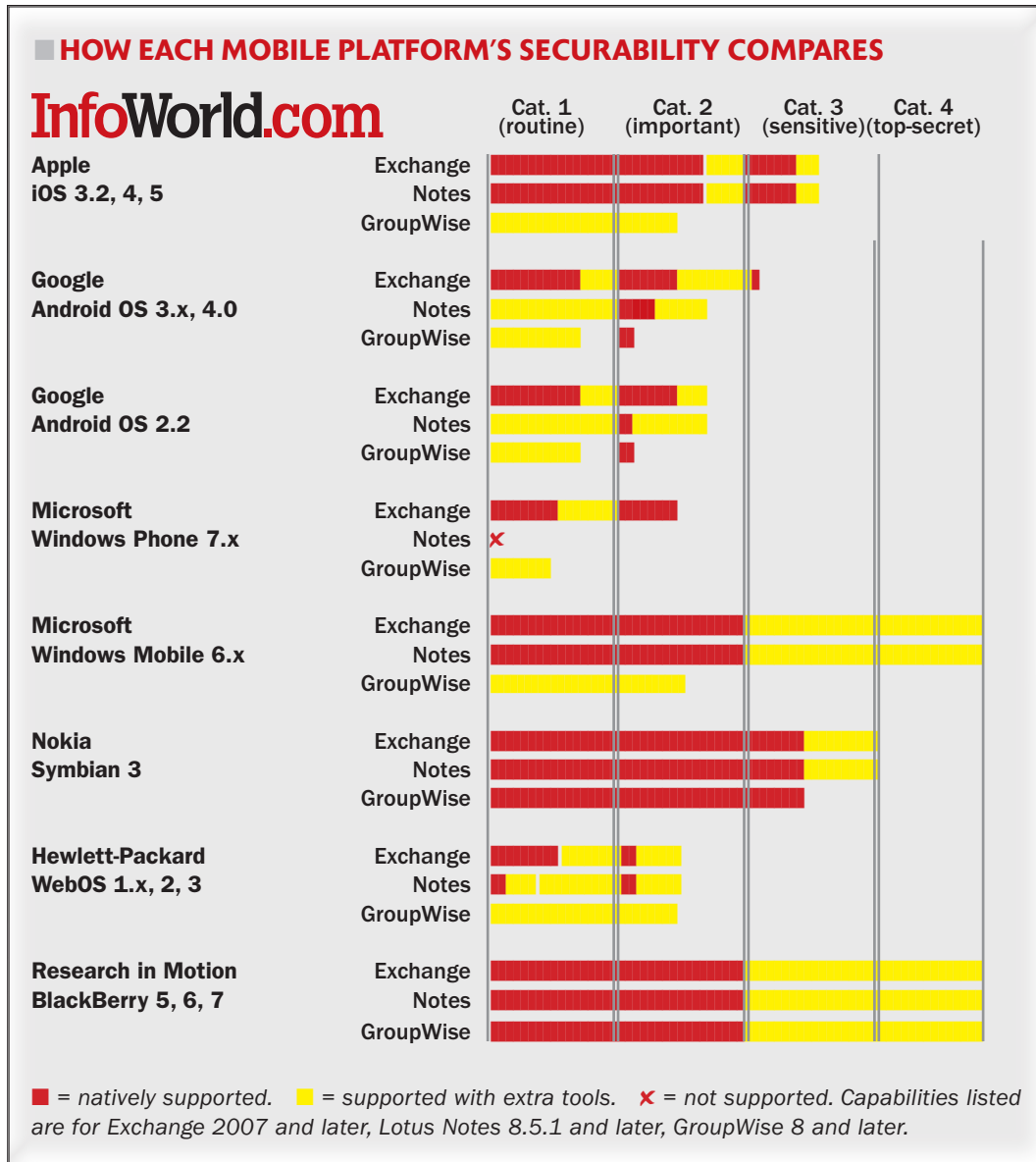
Apple iOS. iOS can't meet the military-grade encryption (FIPS) requirements (except for S/MIME support in iOS 5) or provide the level of application and network-access control necessary, nor can it support physical second-factor authentication. It can be used in military organizations, but only by those people whose level of clearance doesn't require these extraordinary security measures.

Google Android. The Android operating system lacks the services to provide most of this category's requirements, so it cannot meet the needs of Category 4 businesses.

Microsoft Windows Mobile. Natively, Windows Mobile can't meet military-grade requirements such as physical second-factor authentication support and military-grade (FIPS) encryption, but the Good for Government product adds them to meet Defense Department requirements.

Windows Phone 7. The Windows Phone 7 operating system lacks the services to provide most of this category's requirements, so it cannot legitimately meet the needs of Category 4 businesses.

Nokia Symbian. The Nokia devices can't meet the mil-



itary-grade (FIPS) encryption requirements or provide the level of application and network-access control necessary. They can be used in military organizations, but only by those people whose level of clearance doesn't require these extraordinary security measures.

RIM BlackBerry. When used with the full version of BES and the BlackBerry Smart Card Reader, [certain models of the BlackBerry](#) can meet Category 4 requirements.

THE BOTTOM LINE: YOU CAN SAY YES A LOT

By now, I hope it's clear that most businesses can say yes

to many of today's smartphones.

Although the minimal capabilities of Windows Phone 7 and Android 2.x largely limit their use to Category 1 companies, Category 2 and Category 3 businesses can support iOS and even Android 3.x and 4.0, not just the traditional BlackBerry, Windows Mobile, and Nokia Symbian devices.

So now the question is not whether your business should say yes to smartphones but what value it seeks from their broad use. That's a better question to ask and an even better one to help the business answer.

Galen Gruman is an InfoWorld executive editor and its [Mobile Edge](#) blogger.

HANDS-ON

BES: Express or deluxe?

The free BlackBerry Enterprise Server Express is good enough for most

By Mike Heck

FOR ALMOST AS LONG AS BLACKBERRY SMARTPHONES HAVE been the darlings of enterprise business users, RIM's BlackBerry Enterprise Server (BES) has been the preferred solution for managing these devices and for providing secure access to corporate email.

BlackBerry Enterprise Server has grown along the way, with the latest version 5.0.1 sporting a new, simplified Web-based administration interface and groups for easier management of roles, IT policies, and software configurations. BlackBerry Enterprise Server 5 also promises better reliability through server failover features and system health checks. That's all good news for large organizations.

There's also good news for smaller organizations. The BlackBerry Enterprise Server Express provides small and midsize businesses with many of the same security, management, and push technologies of BlackBerry Enterprise Server – but at no cost beyond their existing Microsoft Exchange or Domino servers.

From the BlackBerry user's perspective, BES and BES Express are the same. Both let users wirelessly synchronize email, calendars, and contacts, as well as access files stored on the server. The two products even play together nicely in large organizations. You could use Express to manage personal BlackBerry phones that employees purchase and bring to work, while BES handles the heavy lifting of corporate BlackBerry devices that are deployed in large numbers.

How do these two BlackBerry-only solutions stack up for companies and their IT organizations? I created a [Microsoft Small Business Server 2008](#) test environment to find out.

BLACKBERRY ADMIN

Installing BlackBerry Enterprise Server or BlackBerry Enterprise Server Express requires about three hours, including any prerequisite software.

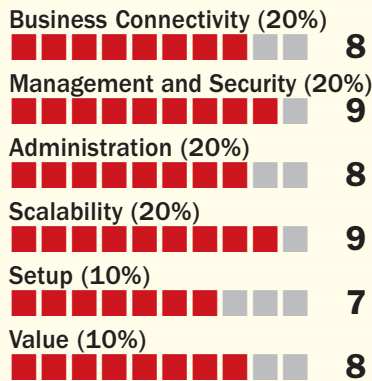
(The process is much faster for upgraders, thanks to the [BES Transporter Tool](#).) Experienced IT staff shouldn't have any problem with the step-driven setup application. Others, though, would be well advised to let a consultant do the job. I discovered several unintuitive settings related to user accounts and Active Directory, as well as configuration problems with the Web server that could easily trip you up.

The top screenshot shows the BlackBerry Administration Service web interface. It features a navigation sidebar on the left with categories like 'Quick user search', 'BlackBerry solution management', 'Devices', 'Servers and components', and 'Preferences'. The main content area is titled 'Manage users' and shows a user profile for 'David Wright'. Below the profile, there are tabs for 'User Information', 'Groups', 'Roles', 'Wi-Fi profiles', 'VPN profiles', 'VoIP profiles', and 'Software tokens'. A dropdown menu is open, showing options like 'Default', 'No Camera', 'Security', and 'Test Center'. The bottom screenshot shows the 'Advanced Settings' page for a user named 'David Wright'. It displays the 'Currently Managed PIN: 21559083' and offers three main actions: 'Back up device data', 'Restore a device', and 'Advanced'. Each action has a corresponding icon and a brief description of what it does.

The Web-based BlackBerry Administration Service (above) makes it easy to assign IT policies and software configurations to users. With the Web Desktop Manager, (below) admins can let users configure their phones, install applications, and handle backups and restores.



InfoWorld Test Center **VERY GOOD**
BlackBerry Enterprise Server 5.01 **8.3**
 Research in Motion



COST
 \$3,299 for server software and 50 client licenses; volume discounts available.

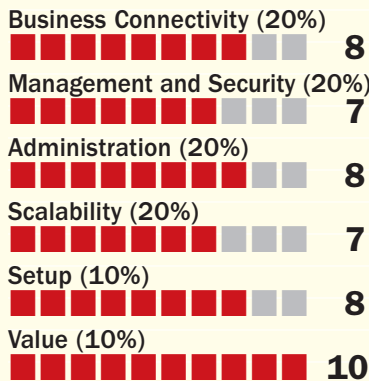
PLATFORMS
 Microsoft Exchange, IBM Lotus Domino, or Novell GroupWise; runs on Windows Server 2000 or later and Microsoft SQL Server.

BOTTOM LINE
 BlackBerry Enterprise Server 5 combines Web-based administration, over-the-air device provisioning, granular control with 450 IT policies, and a host of high-availability features required by large enterprises.

Both editions share the new BlackBerry Administration Service, a Web-based console that only works with Microsoft Internet Explorer. The GUI eliminates the desktop software that was part of BES 4.x, and it's well designed. For example, the home screen provides options for managing users and groups, creating and assigning IT policies, handling operating system upgrades on the handsets, and dealing with applications on smartphones. Administrators can also manage the server from this console.

Although previous versions of BlackBerry Enterprise Server had groups, they're more flexible in BES and BES Express 5.0.1. For instance, groups can belong to other groups (nesting or child), which helps IT managers deal with complicated corporate structures. Groups, like individual users, can be assigned to roles, IT policies, and software configurations, and they'll inherit the roles, policies, and

InfoWorld Test Center **GOOD**
BlackBerry Enterprise Server Express 5.01 **7.8**
 Research in Motion



COST
 Free.

PLATFORMS
 Exchange Server 2010, 2007, and 2003 and Windows Small Business Server 2008 or 2003, or Lotus Domino and Lotus Messaging Server.

BOTTOM LINE
 Small and medium-size businesses needing to give their BlackBerry users secure access to Microsoft Exchange or Lotus Notes email and internal documents can't go wrong with the no-cost BES Express.

configuration from their parent groups. You'll need to construct group hierarchies carefully, because there's no easy way to manage exceptions for a specific user.

Both BlackBerry Enterprise Server and BlackBerry Enterprise Server Express 5.0.1 provide new administration roles that can be used to spread out IT management tasks more efficiently. For example, you could assign one person to serve as senior help desk administrator and others to administer a particular server or group of users.

Further, both editions turn over a lot of control to users — self-service that can reduce the work for help desk staff. The Web Desktop Manager (subject to policies) allows users to activate and configure their smartphone settings, back up and restore data residing on the phone, and install applications.

BLACKBERRY ENTERPRISE SERVER VS. BLACKBERRY ENTERPRISE SERVER EXPRESS

BlackBerry Enterprise Server Express features more than 35 controls and policies, including remotely wiping a lost smartphone and enforcing password policies. I had no trouble creating policies to lock out Bluetooth, enable the still camera, and allow software loading with the device tethered to a PC. Using the tabbed interface, you pick the rule and whether the feature is enabled or disabled. Typically, both products start with most device features enabled, so you only need to create a rule when restricting a particular capability.

Most organizations will be satisfied with the basic controls in BlackBerry Enterprise Server Express, while those who need lots of fine-tuning will find it in BlackBerry Enterprise Server. Where BES Express can either allow or prohibit the use of a feature (MMS, SMS, Bluetooth, camera, media card, modem, Wi-Fi, USB/serial, internal network connections, and so on), BlackBerry Enterprise Server can control exactly how the feature is used. For example, BES lets you control whether Bluetooth can connect to BlackBerry Desk-



top, be used for device discovery or dial-up networking, exchange contacts, or transfer files. You can set a minimum encryption level for Bluetooth connections and even ensure that the LED connection light flashes whenever the BlackBerry is connected to a Bluetooth device.

The one policy area where BES Express matches BES is application control. In both editions, “listed” applications (such as the BlackBerry Java applications you choose to include in your company’s repository) can be made optional or mandatory, or they can be prohibited based on a user’s permissions. Similarly, “unlisted” applications can be allowed or blocked; if allowed, these applications can be prevented from using device storage or limited in the types of connections they can establish.


Both BlackBerry Enterprise Server and BlackBerry Enterprise Server Express automate operating system and application updates, but BES has additional tools to make the whole software management process more reliable. That’s because you can check for any software dependencies that need to be installed first. It’s even possible to trigger a software upgrade based on a device’s hardware or wireless carrier. For instance, if you have a [BlackBerry Torch](#) user on AT&T, you could specify an AT&T-specific version of BlackBerry OS 6 for the Torch to be installed. Again, that sort of precision isn’t available with Express.

In both editions, application and IT policy updates can be pushed during off-peak hours to minimize disruptions to users. While BlackBerry Enterprise Server allows devices to be activated over the air, initial provisioning is a manual process in BlackBerry Enterprise Server Express. But with the Web Desktop Manager, users can handle it by themselves.

BlackBerry Enterprise Server also has [high-availability features](#) that Express lacks. For instance, you can configure primary and standby servers for automatic and manual failover — which could keep downtime to a minimum when there’s a hardware problem or during server upgrades. (There are no additional licensing fees for servers running in standby mode.)

Working in concert with failover, BES 5.0.1 adds system health checks. For example, you can create a certain performance threshold. If that measurement is exceeded, the failover to the backup server automatically occurs.

Both flavors of BlackBerry Enterprise Server do a very good job of providing BlackBerry users with secure, wire-

less access to email and documents behind the firewall, and the Web-based interface minimizes the workload of IT administrators. For personally liable BlackBerry devices that only require access to an Exchange server and where a basic set of security policies is adequate, Express will do the trick. But when your support staff has to manage thousands of devices or when email to mobile executives absolutely positively must never stop flowing, BlackBerry Enterprise Server is the only choice. 

Mike Heck is an InfoWorld contributing editor.