



we solve IT™

presents

# Endpoint Trends

When it comes to managing enterprise technology, endpoints are perhaps the most challenging components that IT departments must grapple with. Mobile endpoints add an additional level of complexity and risk to the equation. Yet, given the productivity and flexibility that mobile endpoints offer, IT managers need

to find the best way to manage and secure these devices.

In this eGuide, *Computerworld*, *Network World*, and *InfoWorld* look at some of the latest trends in mobile endpoint management and protection. Read on to learn how to safely and effectively enable mobile endpoints in your organization.



in partnership with



news analysis

## Mobile Management On the Rise, But Many Companies Still At Risk

Basic device management is being sold as loss leader

2

opinion

## CEOs Don't Care About Mobile, IoT or Wearables, Says Report

You've got some more explaining to do if you want a boss to embrace mobile, IoT or wearables as a strategy. A report says many CEOs don't think they're 'very important.'

5

column

## 5 Mobile Management Questions You Should Stop Asking

Android, the iPhone, and the iPad are well established in business, so it's time to stop thinking about them as new issues

7

# Mobile Management On the Rise, But Many Companies Still At Risk

## Basic device management is being sold as loss leader

**BY MATT HAMBLÉN, COMPUTERWORLD** | There's a lot of confusion, disruption and even turbulence in the market for enterprise mobility management (EMM) software, which is used to manage smartphones and tablets and the data and apps running on them.

The EMM market is growing robustly eight years after the emergence of the first iPhone, with fewer than half of all U.S. workplace devices under management, according to a recent survey by analyst firm J. Gold Associates.

There are still dozens of small EMM vendors along with about 10 large ones, even after several consolidations in recent years. Among them were VMware's purchase of AirWatch in 2014, IBM's buying FiberLink and Citrix' acquisition of Zenprise in 2013.

About 40 million mobile devices are under EMM management in the U.S., and that number is expected to grow to 62 million in 2017, according to Gold Associates research.

Choosing a vendor and software management products is increasingly complex for IT managers, who must deal with the crush of smartphone and tablet users at work while still protecting the company's sensitive data.

"EMM vendors are not all that different and are all trying to do the same thing, basically," said Jack Gold, principal analyst at J. Gold Associates, in a telephone interview. His firm did a

Web-based survey of 300 businesses based in the U.S. in April, asking questions about their use of EMM. (Gold is an occasional columnist to *Computerworld*.)

"Our survey found that EMM brand loyalty isn't that high, and that companies are willing to switch EMM vendors pretty readily," Gold said. "Often, these companies picked a vendor because they needed something done in a hurry. Maybe it was because somebody on staff got an iPhone and there was a decision to give iPhones to other workers. The IT guy might have a week to do something to protect data and he's only going to buy 50 licenses."

Quite often, the software price isn't an issue, so an IT manager might pick a vendor based on whether the vendor is well known. "It's usually something like, 'I've heard of AirWatch or another company; let me call them,'" Gold said.

While the procurement of EMM is often haphazard, it behooves buyers to think more strategically, Gold said. Buyers should consider how EMM fits into a larger corporate role of managing the sensitive data that runs in many places, including on devices used by workers in the field and at work. They should not concern themselves only about managing the devices or the apps running on them.

The latest trend in new EMM products is to manage the data

***Buyers should consider how EMM fits into a larger corporate role of managing the sensitive data that runs in many places, including on devices used by workers in the field and at work.***

on the devices, not just the apps or the devices themselves, Gold said. The EMM software will encrypt the data, which might be a part of an Oracle database or just a single file.

An IT manager can set policies for which data is allowed to be seen by the end user of a smartphone or tablet, and can even say whether the data can be forwarded or edited. "It could be customer data or even a medical file," Gold said. "It's better to protect the data because it's very hard to protect devices and the many apps out there."

Losing a smartphone could cost a company \$200, but a hospital losing sensitive data like an X-ray of an important patient could result in a \$10 million lawsuit, Gold noted.

The EMM survey "indicates that the market will continue to be turbulent and one where vendor loyalty will be a mixed bag at best," Gold wrote in his latest technology brief.

## Gartner's Magic Quadrant

Research firm Gartner has evaluated EMM vendors for several years and recently issued its latest "Magic Quadrant" report for 12 of them.

The report listed five companies as "leaders" in EMM—AirWatch by VMware, MobileIron, IBM, Citrix and Good Technology. Those companies were followed by SAP as a "challenger" and Soti, Microsoft and Sophos as "visionaries." The remaining three—BlackBerry, Landesk and Globo—were listed as Gartner's "niche player" quadrant.

BlackBerry, which released its latest Enterprise Service 12 (BES12) last November, "should meet many organizations' requirements for cross-platform management," Gartner noted in its report. "BES 12 is a good fit for organizations that plan to support BlackBerry devices for the foreseeable future and are satisfied with a capable EMM product for non-BlackBerry devices."

Despite such language, BlackBerry Chief Operating Officer Marty Bear took offense in a blog with Gartner's ranking of BlackBerry's EMM capabilities. "We were a little disappointed by the limitations of the influential annual vendor survey," he noted.

Bear criticized Gartner for gathering its information on EMM vendors in early 2015, which ignored moves by BlackBerry in the past three months to release BES 12 Cloud and to acquire mobile content management provider WatchDox. Gartner also didn't mention BlackBerry's Android for Work support.

"BlackBerry deserves to be considered a leader in EMM today," Beard concluded.

Beard's reaction to the Gartner report underscores how quickly the EMM industry is changing and how the products it provides have evolved. It makes it hard for IT managers to keep up, much less the analysts that study the software.

## Is EMM a good investment?

Given the turbulence and changeability in the EMM market, it's fair to ask if EMM software is even a good investment.

Gold said EMM can be a good investment depending on how a company assesses its level of risk from workers using smartphones and tablets with access to sensitive data.

"The real issue with EMM is what's your risk?" Gold said. "For a lot of companies, EMM is really insurance. If you lose data and you're an Exxon Mobile or a Bank of America, what does that cost you? A lot. That's the real issue."

The cost of EMM software may not be the most important consideration for a company, depending on the level of risk. Gold noted that prices for basic mobile device management software (part of EMM) are falling. "They're almost giving that stuff away," he said, sometimes for as little as \$1 a month per user.

Gold defined basic MDM software as allowing a company's IT department to keep a full central inventory of smartphones and tablets by model and OS and all the apps running on them. MDM will often include a kill switch ability if a phone is lost and possibly application management that prevents certain apps from being used on devices. There might even be the ability to turn off a camera on a smartphone, if management doesn't want users to be able to take photos in some settings.

"With MDM at \$1 per user per month, it's like a loss leader," Gold said. "It's like going into McDonald's and buying coffee for \$1 when they figure you'll also buy a doughnut for \$3."

With EMM vendors, the "doughnut" is part of the upsell of a "smorgasbord" of software used for higher management functions, Gold said. Such products manage apps or provide "app wrapping," which refers to taking an app and wrapping security capabilities around it, Gold said. A newer management software, sometimes called "file sync and share," is part of a general category for managing data on devices.

Prices for the up-sell software can vary widely and can usually be negotiated. Meanwhile, Gold said that the EMM cost per user for management features is going down. However, when customers buy a suite of products and add more components and new capabilities, Gold said companies can expect to see their EMM costs rise by 15% to 20% over the next three years.

### What's scariest of all

While the overall use of EMM by U.S. companies is on the rise, Gold's survey found that less than half of all devices deployed at companies are under EMM management.

"What is scary is that companies, even the big ones, have so many devices in use that are not even under management," Gold said. "It's well below 50% that are being monitored, managed or secured. Maybe if your business is delivering pizza, that's not a big deal. Otherwise..."

Gold believes there will be growing recognition of the value of EMM, but not an explosion. "The level of use will probably still be in the 50% to 60% range [of devices under management] in three years," he said. "It will vary by industry."

While that growth might sound like good news for EMM vendors eager to sell more products, Gold's report was less positive.

"Clearly, companies are planning to increase the number of devices that will be included in EMM solutions they are implementing," Gold wrote. "But this may not directly equate to increased sales for EMM vendors. Many companies overbought licenses initially and are now clearing their internal inventory and applying those licenses to their devices."

Gold's conclusion signals more turbulence to come.



## Listennow

*free podcast*

## Increase Field Service Productivity

 **listen to the  
podcast**

# CEOs Don't Care About Mobile, IoT or Wearables, Says Report

You've got some more explaining to do if you want a boss to embrace mobile, IoT or wearables as a strategy. A report says many CEOs don't think they're 'very important.'

**BY PATRICK NELSON, NETWORK WORLD** | CEOs' priorities are different from the rest of us when it comes to tech.

For one thing, half of U.S. CEOs worry more about new industry entrants from the technology sector disrupting their businesses, than adopting devices as a strategy, according to a recent survey from analysts PricewaterhouseCoopers, or PWC.

## Strategic importance

CEOs aren't getting over-excited about devices. Investment is being made, but more CEOs thought cybersecurity was strategically more important to them than mobile, IoT and wearables, the survey found.

Mobile gets barely half of CEOs' attention. Only 55 percent of those polled reckoned mobile tech for engagement with customers is strategically "very important" to their enterprise.

## IoT

Even less impressive was the IoT, or Internet of Things' numbers. Not many thought of it as being "very important" with only 29

percent going there.

Wearables had an even more dismal showing in the survey. Just eight percent thought it was "very important."

However, overall CEOs are "embracing digital technology." It isn't going away, in other words. Seventy percent of U.S. CEOs see changes coming in the "core technologies used for production or service provision."

## Tools

CEOs are using tech as tools. Technology creates operational efficiencies; data mining and analysis helps the company; decision-making is better with tech; and customer experience and innovation capacity are all seeing investments. This is according to the 2015 US CEO Survey from PWC.

CEOs are embracing big data. Strategic decision-making and risk-taking decisions are improved through the use of technology tools, the respondents said. More than half of the CEOs asked now use such tools.

**Mobile gets barely half of CEOs' attention. Only 55 percent reckoned mobile tech for engagement with customers is strategically "very important" to their enterprise.**

## Wary of new market entrants

But CEOs are worried about threats to business growth. Much of that threat comes from disruption and technology.

CEOs know that they need to keep a wary eye out for direct and indirect competitors, in particular disruptive ones, who emerge onto the scene with technology-based alternatives to their incumbent business models.

These new tech-oriented market entrants worry CEOs. Sixty-three percent of CEOs in the U.S. are concerned about the threat and its potential effect on the individual enterprise's growth.

## Disruption

So much so that businesses are actively looking for new industries to do business in, and are looking for ways to disrupt their own businesses. For example, drugstores are branching into healthcare.

"U.S. CEOs are widening their use of alliances to secure new technology and speed up innovation," the report says.

## Consumer-facing tech

Technology is important in customer experience. Eighty-five percent of U.S. CEOs think its importance is on par with operational efficiency gains (84 percent); data and data analytics investments (89 percent).

"The thing that's been driving us has been digital and technology," said J. Patrick Doyle, president and CEO of Domino's Pizza, in the report. "It's driving loyalty and frequency," he said.

## Tech overall

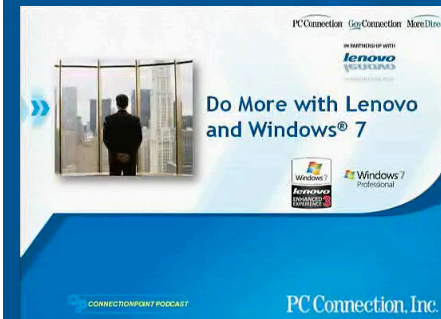
But tech overall is becoming more important to CEOs. "Technologies and the opportunities they represent are migrating to the core of the business where once they may have been treated as 'bolt on,'" the report says.

# Listennow

free podcast

## Enhance Your PC Refresh

 listen to the podcast



PCConnection GoConnection MacDirect

IN PARTNERSHIP WITH

**lenovo**  
SOLUTIONS

» Do More with Lenovo and Windows® 7

Windows 7  
Lenovo Business Solution

Windows 7  
Professional

CONNECTIONPOINT PODCAST

PCConnection, Inc.



# 5 Mobile Management Questions You Should Stop Asking

Android, the iPhone, and the iPad are well established in business, so it's time to stop thinking about them as new issues

**BY GALEN GRUMAN, INFOWORLD** | It's conference season, and enterprise mobility remains a big draw. But I'm surprised by how, for several years now, the IT issues at these conferences haven't changed.

Never mind that the iPhone and Android are eight years old, and the iPad is five years old, all common in today's enterprises—they're the same questions over and over again, with the same mix of vendor FUD and good advice from expert panelists like Benjamin Robbins, Steve Damadeo, Brian Katz, Bob Egan, Maribel Lopez, and me. The core questions have been settled for some time, yet they keep getting asked.

In the interest of getting enterprises to move from the past to the present, so they can then focus on the future, here are the mobility questions you can stop asking. Instead, adopt them as the known best practices.

## 1. Do I do BYOD or COPE?

Many organizations remain obsessed with the question of supporting bring-your-own devices (BYOD) versus issuing corporate devices to which employees can add at least some personal apps

and data (COPE, or corporate owned, personally enabled).

The answer is yes. Issue devices to employees for whom a smartphone or tablet is part of their required technology portfolio and pay the data charges. With employees for whom the use of personal devices enhances their business performance but is not strictly required, let them bring their own devices—meaning devices that conform to your security requirements and employees consent to your managing.

The truth is too many execs see BYOD as a way to make employees pay for business technology, so they contorted themselves to make BYOD the standard. At the same time, too many IT organizations freaked out about “alien” devices they could not control up the wazoo. Both reactions come from bad motivations, not from issues of business value.

It may be that your industry has a reason to favor BYOD over COPE, or vice versa, usually for proving your level of compliance on various regulations or for reasons of asset management. A law firm is more likely to insist that its lawyers use only corporate-owned devices to leave no doubt as to the ownership and source of control, whereas a publisher or university is likely to

***The truth is too many execs see BYOD as a way to make employees pay for business technology, so they contorted themselves to make BYOD the standard.***

be more flexible about device ownership given the more porous nature of what many staff members do.

There are edge cases that might require a draconian approach: A government agency might forbid both BYOD and COPE, so as not to get bad press around employees wasting time on the job, instead issuing highly limited devices for work-only use.

This is not a technical issue but a risk-management one, with the risk being not so much about data security (your management policies should handle that issue regardless of BYOD or COPE) but about reputational risk and legal comfort.

## 2. Do I need EAS, MDM, MAM, or EMM?

This is the question vendors want you to ask, so you start thinking of the issue not in terms of policy but in terms of products: What do I need to protect, and which users does that affect in what circumstances? That will let you know which security and management products you need, as well as which favor employees.

Here's the framework of how the various options address your actual needs:

**EXCHANGE ACTIVESYNC (EAS)** is the baseline security method that every company should use at a minimum. Its policies enforce the use of encryption and passwords, and it allows you to remotely lock or wipe a device that is lost or stolen. iOS 6 and later, Android 3 and later, Windows Phone 8 and later, and BlackBerry 10 support the core policies. Support varies from mobile OS to mobile OS for more discrete EAS policies, such as disabling the camera.

**MOBILE DEVICE MANAGEMENT (MDM)** has evolved over the years, so the top providers—such as Citrix Systems, Good

Technology, MobileIron, IBM, and VMware—have long ago moved beyond managing only the device and now provide ways to manage apps and, in some cases, content. If you have legitimate needs to control which apps users can have, to manage VPN settings, to impose standard configurations, and to disable features like copy and paste or cloud access, these tools have you covered.

Be aware that their specific capabilities beyond the core differ, so you should do a deep assessment of candidates to find the best fit. All the major providers support the core APIs provided by Apple's iOS and Google's Android, and an increasing number are supporting those in Windows Phone. Some also support Apple's APIs for Macs (they're based on the iOS APIs).

Where they differ is in the edge areas, like support for Apple's content-management APIs, and in new technologies, like Google's new Android for Work containers.

Many support additional content controls for apps that use the MDM vendors' proprietary APIs, but that approach ties you to specific apps and MDM servers. It's a big investment that can also limit your ability to get strong value from mobile usage.

**MOBILE APPLICATION MANAGEMENT (MAM)** used to be a separate category of management tools to manage access to apps and their content. It's been subsumed into MDM tools from the major providers. Unless you have an MDM tool that doesn't offer the app management controls you need, a separate MAM tool doesn't make a lot of sense today.

**ENTERPRISE MOBILITY MANAGEMENT (EMM)** is a marketing term, nothing more. I call it "expensive mobility management" because the term arose from vendors seeking to



free podcast

## Mobile Device Management

 listen to the podcast



convince IT pros they needed more than “simple” MDM, by offering a large portfolio of bells and whistles that are largely unnecessary but appeal to IT’s control instincts.

Focus on your needs, not the label.

### 3. Should I set up an internal app store?

The short answer is probably not. Yes, having an internal Web page that links to recommended iOS and Android apps from their respective app stores is a good idea. If you want to call that your app store, fine.

But running your own actual app store through an independent third-party tool is overkill. After all, you manage app distribution with the business app store that Apple provides to companies via its Volume Purchase Program (VPP), which lets you buy app licenses in bulk and manage their distribution, as well as distribute your homegrown apps. Google offers a similar capability for its Play Store, called private channel. Why reinvent the wheel?

If your goal is to configure devices used by employees (regardless of who owns them) so that specific apps are installed, updated, and managed for users in specific workgroups, you can do so via your MDM server, which use the Apple and Google APIs, respectively, to the VPP and Google Play private channel. This capability is available in the better MDM tools.

MDM tools also let you blacklist or whitelist specific apps, so you can prevent users from installing known bad apps from the public Apple and Google app stores.

### 4. How do I keep mobile devices from leaking my corporate data?

This question is based on a pervasive but very false premise: that smartphones and tablets are a major vector for data leak-

age. They are not, as you can easily see by checking the public breach report databases. Stolen laptops and misplaced USB drives are the major vectors, while mobile devices almost never show up as a breach vector.

If you fear data leakage and believe the best approach to combating it is to target the device, then you should ban Windows PCs, remove their Internet connections, or at least bind them with encryption, app management, and content management tools. PCs are where that sensitive data is, and (shock!) PCs are the devices most targeted by hackers and data thieves.

Very few organizations apply the kinds of controls to PCs that they want to apply to mobile devices, which has to make you ask if those controls are truly necessary. Also, if they are, why aren’t they on your PCs, too?

However you answer that question, it takes very little to enforce encryption and password usage—the key protections for lost or stolen mobile devices—on smartphones and tablets. Set it up in EAS or MDM policies, and you’ve all but eliminated the data loss risk from mobile devices.

But what about leakage through iCloud, OneDrive, Dropbox, Box, or Google Drive, not to mention personal email? Well, if you think that only mobile devices use these services, you’re naive. Mobile devices are one conduit among many, and clogging one pipe doesn’t stem the unwanted flow of information—it simply moves it to another pipe.

The right approach is to manage data access at the source, not the endpoint. Think access permissions first; if a person can’t be trusted on a smartphone, he or she can’t be trusted on a PC, either.

The good news about mobile: There’s real thinking going on about managing data, so mobile is pioneering safer data practices that, if we’re lucky, will find their way into PCs, too.

## 5. How should I protect against viruses?

Don't use Windows PCs. That may sound flippant, but that's the truth if you're really concerned about malware like viruses.

Even more so than OS X, iOS is highly immune to malware, so the number of exploits has been very small.

Android is not immune, given its Windows-like file architecture, so researchers keep finding malware targeting it (mainly from fake and adware apps in the Google Play Store and, outside the West, from non-Google app stores). Yet it appears that very little malware actually is running in the Android wilds, so the true threat—versus the potential threat—is highly exaggerated in IT and vendor discussions.

The minuscule usage of Windows Phone means that malware hasn't targeted that platform. Ditto for BlackBerry.

There's a theme: Vendors prey on your Windows malware experiences to suggest that everything is as threatened as the

PC. It's not. Malware should be a concern on Android, but no reason for panic.

The real issue for IT is whether Android antimalware apps actually protect you—and the answer is they are more an alerting mechanism rather than a remediation mechanism. It's better to disable access from devices that have sideloading/rooting enabled and to focus on data access rights of Android users, to control what could be at risk to malware.

### Move on to the question that really matters

The truth is that mobile devices are safer to use than PCs (just as cloud services are probably safer than your data center), so figure to how to make PCs as secure as mobile devices and how to protect data wherever it may happen to be.

Then ask the question that really matters: How do you get the most value from the use of mobile technology in your business?



# Listennow

*free podcast*

## Valley Agricultural Upgrades



**listen to the  
podcast**