Managing mobile devices: IT's version of Whack-A-Mole

As enterprises try to reign in mobile devices, new ones pop up on the network and additional software is installed to manage the chaos. Has MDM gotten out of hand? Evan Schuman reports.

It is Christmas Day at 2 a.m. and a new mobile device just connected to your network. Your servers are configured to send a text message to alert you when new devices connect, so you immediately know that something has happened. But you have no policy that requires that new devices be configured with mobile device management (MDM) software before they are allowed to connect so you don't know if this is an employee playing with their new smart phone or an actual attack. Do you get up and troubleshoot the alert or go back to sleep? This scenario plays out all day every day for security professionals and it is only getting worse.

With mobile and cloud growth soaring and new requirements such as the European Union's General Data Protection Regulation (GDPR) forcing CISOs to better control access to data, regardless of the physical location of the data or company, mobile device management (MDM) has never been more essential. In some cases, however, it is too popular, with some enterprises housing a dozen or more MDMs, which itself creates new security holes.

Having too many MDMs is only one of the implementation problems that cause anxiety for mobile security experts. Other concerns include wearables being ignored, a lack of consistency and implementation processes that simply make life more complicated than is needed for CISOs, and the practical problems with a bring-your-own-device (BYOD) environment, which itself will force changes to IT's favorite after-the-fact defense of a mobile remote wipe. And then there are questions about whether CISOs are focusing too much on devices and ignoring the more crucial data and applications. Sometimes CEOs like to weigh in on MDM policies, which is rarely a good thing.

Rob Smith, a London-based research director for Gartner, argues that the biggest concern he has about how Fortune 1000 CISOs uses MDM is that they think through their needs insufficiently, preferring to purchase whatever top-rated software they can find and hope it does the job.

"The number one thing they are getting wrong is buying products without knowing what they are using it for, without knowing their use case," Smith says. "They buy one product and expect it to do everything."

Smith counsels CISOs to focus on four areas before exploring MDM options:

- Who is the user and what is their role?
- What is the device and who owns it?
- What kinds of apps and data do they need to access?
- Where in the world are they located?

Different regions have different rules

OUR EXPERTS: MDM

Avery Chipka, CSO, Circle Technology Collective International

Ajay Gupta, program chair for computer networks and cybersecurity, University of Maryland; CEO of HSR Inc.

Andrew Hewitt, analyst, Forrester Research

Stephanie Lawrence, research analyst, ABI

Peter Meuser, independent IT consultant, iTlab Consulting

Rob Smith, research director, Gartner

John Sprunger, senior technical architect, West Monroe Partners.

$8B

The global MDM market size is expected to grow from $2.81 billion in 2018 to $7.86 billion by 2023

– Reportlinker

about data protection, Smith says, above and beyond GDPR. "Data for England and Wales can only be stored in England and Wales," Smith says, adding that even the much-beloved mobile remote wipe might have to be rethought.

Rob Smith, research director, Gartner

The issue with mobile remote wipe is the question of device and data ownership in a BYOD situation. A common kneejerk response to a missing device that is suspected of being stolen is to wipe everything right away. Sort of a "destroy first, ask questions later" approach. But does IT have the right to wipe clean all of that personal information? "Even if IT thinks they have the right because of [an employee agreeing to such wipes due to a form with] a click through, click throughs never hold up in court. [IT] needs a physical release form," Smith says.

Even physical release forms might not always do the trick, as European courts often insist on a knowing agreement that is non-coerced. Insisting that an employee sign such a form to get access to essential databases might not be considered a true choice in the eyes of the court.

On remote wipe, Forrester Research Analyst Andrew Hewitt adds that companies need to partition off corporate content and use MDMs that support full-device as well as selective wipe, allowing them, in theory, to obliterate only corporate content. That should avoid the legal complications of destroying employee personal data.

But Gartner's Smith also says that he is very concerned with how many MDMs enterprises have these days. In Gartner surveys of the Fortune 500, Smith says they found that "29 percent had three or more and one guy had 10 different products in production. How do you get to three — forget 10?"

He says there are quite a few reasons a company can accumulate more than 10 MDMs. First, there are inherited software licenses from acquisitions. Second, companies will purchase different MDMs for different operating systems (getting an Apple-specific MDM, for example, is common) along with some for different geographies and different kinds of apps. CISOs seem to be burdening their MDM strategies with an embarrassment of niches. Smith argues that any number of MDMs greater than three is a problem.

Forrester's Hewitt says that he sees most companies with about four to five MDMs and he also says he would strongly prefer an enterprise to use no more than three. "I don't think they really need [more than three]. The technology has advanced quite a bit," Hewitt says. "The best enterprises are doing this with one and maybe two MDMs."

Avery Chipka, the chief security officer at the Circle Technology Collective International in Rutland, Vt., is willing to tolerate clients having far more MDMs, although he does have a ceiling. "I start having concerns when the number is above 10. When it's more than 15, something needs to be done about it," Chipka says. He stressed that having so many MDMs can cause confusion and make it far more difficult to track users.

Sometimes an employee will have "one profile as an executive, another for creative, [and] another if they are doing sales. An individual can only serve so many roles. Does each person really need a separate account for every email account?" Chipka asks. "During an acquisition, MDM profiles are one of the first things IT should be looking at. How many people didn't make it through the acquisition?" he asks, adding that removing those accounts should be a priority. This is even more important given that some of those who are let go might be quite unhappy about it.

Forrester's Hewitt sees the plethora of

73%

Percentage of survey respondents who cite the evolving nature of cyber threat as a major security challenge for their business

– Hiscox Cyber Readiness Report

MDMs as its own risk. "It is a security hole because they don't have a coordinated way to look at that employee so they can get that one view of an employee," Hewitt says.

Ajay Gupta is the program chair for computer networks and cybersecurity at the University of Maryland and he sees a different security hole from an overabundance of MDMs: Attackers leveraging the fact that many MDMs don't communicate with each other. "It is possible in that situation that a device could sneak in," he says. This can happen because each MDM knows that it is not alone. Therefore, it might not necessarily block an unrecognized mobile device, as it can legitimately assume that it is authorized via a different MDM.

Ajay Gupta, program chair for computer networks and cybersecurity, University of Maryland; CEO of HSR Inc.

Each MDM "has to respect them all. They can't reject because it's not recognized because the apps don't talk with each other," notes Gupta, who also serves as president and CEO of HSR Inc., a non-profit data security organization in the healthcare industry. "The default is usually to allow access. This is the problem with centralization versus decentralization. This is why standardizing on a smaller subset of vendor tools is just a good idea."

Chipka says that companies can have multiple MDMs but it must address how they are to coordinate, assuming they can. "Which one takes priority? What happens when you have two platforms and one says allow and one says deny? Each platform has a different way of handling it. For some, 'deny' is the overwhelming factor."

Another MDM concern from Gartner's Smith is internet of things (IoT). "You put a monitor in a conference room and it happens to be running Android firmware. That's the kind of device that will completely bypass IT. There are so many proprietary solutions, which is a big part of the IoT problem," Smith says. "That conference room TV running Android should have [a] mobile threat defense. Then you're stuck with a coffee maker. IT has to be involved because devices often have external communications, a built-in radio. It could be sending data without your knowledge."

Part of the IT MDM problem, Smith says, is a lack of training and, as always, budget. "IT is trailing whenever you bring in new technologies. Every IT staff is overworked, but that time [and budget] has to be allocated. [Corporate] is not budgeting to keep up with new technology. They're not accurately predicting the operational expenses that will be required. Mobile is chaos, a perpetual rate of change. Don't be surprised when Apple puts out an iOS update that breaks the system or Google makes a change how data is stored on the cloud. You have to ride the chaos."

Gupta has a suggestion for perhaps using the MDM BYOD problem to shake loose a few more IT dollars. He argues that "this whole mobile management bring your own device" trend is solely "to escape the costs of buying devices. CIOs should ask for that [savings] numbers and use that [for example] $15 million to move into the IT budget," Gupta says. "Otherwise, the CIO should tell management to post an invitation to every hacker in the world to come into our network because that's what we're doing by opening up your network to devices that you don't own and that you don't know."

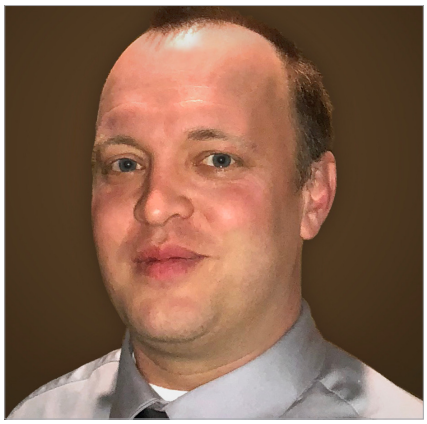
> "Mobile is chaos, a perpetual rate of change."
>
> – Rob Smith, research director, Gartner

92%

Percentage of cyber security experts in cybersecurity that have a budgeting process integrated into all security projects and activities versus only 40% of novices

– Hiscox Cyber Readiness Report

Gupta says another major MDM problem is the lack of CISO follow-through. "They buy the [MDM] product with a set of expectations that are sometimes unreasonable" and then "no one does training for its actual capability. Maybe you should hire the [MDM vendor] to send their engineers to your facility for a week of training. Real engineers, not sales engineers. If you care about security, you may have to spend the [training] money."



Avery Chipka, CSO, Circle Technology Collective International

Chipka points to the ability to identify and track unrecognized mobile devices as a key hole in some MDM systems. He describes one offering that paired MDM tracking with digital security cameras. "Security cameras, when paired with access points and known devices, can be used to identify and record unknown devices' presence in a building, allowing for the security cameras to intelligently track those signals that it is not able to identify. This is just one of many cutting edge impacts that MDM can have on our future," Chipka says.

> "Maybe you should hire the [MDM vendor] to send their engineers to your facility for a week of training."
>
> *– Ajay Gupta, program chair for computer networks and cybersecurity, University of Maryland; CEO of HSR Inc.*

Another concern Chipka has is that some systems default to allowing the user to delete their own profile. Although this would make some access from the phone more difficult, it also gets around legitimate security restrictions that IT wants to impose.

"A good portion of end-users know how to configure their own email. I've seen profiles deleted because the person was trying to get around the restrictions we put in place. Most [IT and security staff] don't bother to prevent removal of the profile devices." Chipka argues that they need to prohibit any changes that are not done using the administrative panel.

On the flip side, Chipka also complains that IT sometimes will impose too many MDM restrictions, thinking that "because the setting option is there, I have to use it. Just because you can do something doesn't necessarily mean you should." As an example of overreach, he points to some MDM systems that control which screen saver the user can select.

Forrester's Hewitt agrees that some CISOs overreach when making setting selections through MDM. Many are "building way too heavy-handed policies on MDM profiles," he says, specifying "annoying security practices such as 'every three months, we are going to change your 6-digit phone password.'"

ABI Research Analyst Stephanie Lawrence says one of her top MDM concerns involves wearables. "Businesses often overlook wearables and forget to add wearables to their EMM (enterprise mobility management)/ MDM plans, particularly as the devices are added after the EMM/MDM is in place, so it is important that these devices are more strongly considered," Lawrence says.

Today, many wearables have no authentication capabilities, such as the ability to key in a PIN/password or to perform biometric authentication. That should limit those devices from being able to get into a network on their own, analysts warn. But as wearable devices get a larger market share and as their capabilities expand, they almost certainly will ultimately be able to access restricted networks. By that time, it will be too late to go back and generate profiles for all such

$5.3B

Dollar loss due to business email compromises

– FBI

devices retroactively. Therefore, it is not a bad idea to start adding wearable devices today.

Forrester's Hewitt sees another MDM problem being an excessive focus on the hardware at the cost of paying too little attention to apps and data, which is more likely where the bigger dangers lurk. "A lot of enterprises believe that MDM is the only thing they need to use for mobile security. They focus way too much on the device side," Hewitt says. "Let's say a [registered] phone is jailbroken. There nothing that is protecting them from [a cyber thief] getting that data out."

Stephanie Lawrence, research analyst, ABI

Hewitt also says that he is seeing fewer companies using mobile VPNs due to the VPN's well-earned reputation of slowing down devices. Using cloud security gateways and "traffic inspection are doing [security] in a much faster way" than a traditional VPN could, he says.

A concern of some MDM specialists is a lack of simplicity with deployments. "One of the biggest mistakes we're seeing in MDM deployments is that they are overcomplicated.

> "Businesses often overlook wearables and forget to add wearables to their EMM (enterprise mobility management)/ MDM plans"
>
> – *Stephanie Lawrence, research analyst, ABI*

Many organizations are rolling out mobile app management or containerization when only mobile device management and monitoring is needed," says John Sprunger, a senior technical architect with consulting firm West Monroe Partners.

"Another mistake is overbearing deployments," he continues. "Tech leaders need to ensure that security policies are aligned based on data sensitivity and apps used, not using separate policies for BYOD versus corporate devices. Half-hearted deployments are another issue, as some organizations enforce device enrollment but don't fully implement or enforce security policies or don't enforce device enrollment at all, thus allowing a bypass of security policies."

Peter Meuser is a Munich-based independent IT consultant at iTlab Consulting who also expresses frustration at companies having too many MDMs. Meuser offered tips for determining if your company has too many MDMs.

"You know that you have to reduce the number of MDM instances in your enterprise if you have to carry multiple mobile devices because you do not have the necessary access to all corporate assets from your single device," he says. "Only one MDM can be the master of your device and control access to backend services. You do not want to build multiple channels into the same datacenter just to support multiple MDMs. Avoid data silos."

Other indications that a company has too many MDMs, according to Meuser, include, "your operations and support teams are not able to develop the necessary deep skills to drive your mobile workforce at the edge of innovation because they spent most of their time trying to organize external vendor support they depend on for all these different MDM solutions. These days, qualified MDM engineers are a rare species. Or you are doing the same thing with different tools?"

Why should you manage thousands of iOS devices with multiple MDMs, Meuser asks rhetorically. Choose the best one for your situation and then unify across all subsidiaries. But remember, not every MDM is the right

59%

Percentage of phishing emails that deliver ransomware

– Osterman Research

product for every use case. For example, he says, there is a story about Microsoft integrating Jamf, a management application for Apple products, with Microsoft's own Intune for macOS management. Apparently, he notes, Microsoft had no other third-party macOS MDM product to integrate into Intune so that was the company's only option. Ultimately, Meuser says, JAMF dropped its Android support to focus only on Apple's operating system.

There are other examples where niche MDM products gained a foothold because of their specialized capabilities, he notes.

Peter Meuser, independent IT consultant, iTlab Consulting

Meuser's also suggests that you need to reduce your number of MDMs when "all of your bigger subsidiaries run their own MDM system because the products are not able to carry the combined load or does not offer the necessary separated administration."

Meuser also complains of CEO involvement, which can undermine MDM goals. "Stories like this often begin with: 'Why can't I have these Office apps on my corporate iPad? Even my son is able to install them on my private device. Why is our IT not able to do this and why is security blocking all innovations?'

"It's not all about installing just a small app but introducing a whole service to the IT infrastructure," Meuser says. "The mobile device is what your boss sees, MDM is the middleware to connect the device to the backend services. If the backend services are not well implemented and integrated, MDM can't fix what's broken."

If the middleware is not implemented to meet the IT department's security requirements, it could create security vulnerabilities in the network, and it is exactly these vulnerabilities in the apps the potential attackers see. Just because an Office application can be installed on an iPad, for example, that does not mean that it should be.

"I also see CISOs still relying on security policies that are not built for the mobility age. They go back in times where firewalls, virus scanner and smart cards ruled corporate security," he continues. "These times are gone with cloud services and corporate devices that are also enabled for personal use. Enforcing outdated security policies for MDM not only impacts user experience, but also lowers security in many cases," Meuser says.

"Products will not be integrated as they are designed and the resulting solution gets so complex that operations is challenged to maintain the system and keep it updated. Times are over where an IT system is introduced and not changed for years. Progress in mobile development and security threads requires an agile management of all components," he notes.

Ultimately, the choice of which and how many MDM systems is as much a personnel management consideration as it is a technical consideration. If companies make managing personal devices too cumbersome and intrusive on employees, the company's security team might not have the user buy-in to be secure. As Forrester's Hewitt notes, "There's a limit to how many employees are going to get MDM enrolled. Some would rather not have access on mobile, rather than go through" too many security hurdles. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

90%

Percentage of cyberattacks that start with a successful phishing campaign

– 2017 Verizon Data Breach Investigation Report