Incredibly, it wasn’t that long ago that CIOs and CISOs were saying “no” to most mobile devices – or at least trying to. But those objections proved movable, as mobility proved irresistible.

Of course, it’s one thing to give everybody a smartphone. Whether you really want those phones to have unlimited access to corporate applications is another matter. Devices get borrowed, lost, and stolen; tracking phones and tablets, providing support, keeping mobile applications patched, ensuring reliable and secure connectivity – it’s a lot to manage.

Mobile Device Management technology emerged as a first attempt to address those issues. As the name suggests, MDM started life as a device-centered approach. As limitations to that approach became more obvious, an alternative developed, taking an application-centered tack, dubbed Mobile Application Management.

Going back to the original problem – CIOs just want to ensure the right level of access and the right level of management, all at the right cost – it seems inevitable that the two options would merge and converge, rather than remaining an either/or proposition.

But the devil is still in the details. Vetting, choosing, and implementing the right software or service, and matching it with the necessary processes and controls, requires attention to those details. It’s hard work and vital to ensuring that employees can do their jobs on the go.

In this eBook, enterprise users and mobility experts provide practical guidance on the convergence of MDM and MAM, and how these technologies play into the broad challenge of getting maximum benefit from mobile computing.
The mobile device market is moving ahead at warp speed as a host of new technologies and capabilities keep appearing, having their day and then disappearing. One key recent trend has been the convergence of mobile device management (MDM) systems with mobile applications management (MAM) capabilities by enterprises.

One factor in the evolution is that MDM providers are incorporating MAM systems into their services because they both need to work together, explains Vikrant Gandhi, mobile and wireless principal analyst with Frost & Sullivan. “You need dedicated resources to continuously monitor apps,” he says. To do this requires major interplay between devices, applications and cloud/wireless infrastructures.

CONTROL ISSUES
Security remains a key consideration for mobile devices and the enterprise networks they access. Companies still need for layered defenses, as in any IT system, Gandhi says. These needs are creating a growing ecosystem, with access control technology vendors and single sign-on applications vendors working with MDM vendors. The ultimate result of this collaboration is the provision of a single MDM/MAM service to enterprise customers, he says.

One factor of the speed and evolution of the marketplace is that MAM as a capability did not come to most enterprise’s attention until 2013, notes Colin Gibbs, a mobile consultant and strategist at GigaOm Research. A key reason that organizations are turning to combined MDM/MAM systems is greater control. Despite its popularity, bring-your-own device (BYOD) programs won’t achieve much lasting uptake in corporate enterprises unless controls improve, he believes.

Security is a driving force for MDM/MAM convergence and in recent years it has haunted MDM systems for better or worse, says Gordon Van Huizen, research director at Gartner. “MDM gets a lot of the attention but it only solves part of the problem,” he explains, adding that traditional MDM services don’t to a very good job of protecting and managing applications on user’s private devices.

BALANCING CONTROLS WITH ACCESS
The other side of the coin is that in company BYOD or issued-device programs, poorly designed MDM efforts can be so draconian as to create usability and performance issues.

GORDON VAN HUIZEN, RESEARCH DIRECTOR AT GARTNER

As companies struggle to balance these requirements, large developers and vendors such as IBM, Apple and Google are either working on capabilities or considering jumping into the marketplace. Both Apple and Google are gatekeepers in the converged MDM/MAM space, says Jules White, assistant professor of computer science as Vanderbilt University. He adds that this high degree of control is creating tensions to open things up, especially to the applications development community. For example, White notes that Samsung and other device manufacturers are trying to increase their devices’ overall capabilities to compete with Google and Apple, but they haven’t gotten much traction with enterprise customers.
Public and private organizations are getting mobile device management (MDM) capabilities pinned down to meet their needs. But some key concerns remain, such as security, usability and other options, such as containers and device migration.

MDM users and vendors have a history of thinking about the capability in a very end-point centric manner, explains Gordon Van Huizen, research director at Gartner. “The idea is that if you control the device, you’re safe,” he says. But mobility, even secure enterprise mobility, is more about usability and access to applications, rather than being about devices alone. Van Huizen sees MDM systems evolving into more of an asset management solution with overt security fading away as it becomes more integrated at the applications and content level.

Van Huizen sees MDM systems evolving into more of an asset management solution with overt security fading away as it becomes more integrated at the applications and content level.

One organization looking at mobile devices and the various security issues attached to them is the U.S. Army. For five years, the service’s Connecting Soldiers to Digital Applications (CSDA) initiative has been experimenting with providing troops with smart phones and tablet computers on base and on the battlefield.

Lessons learned from the program are influencing how the Army and the Defense Department select and acquire mobile devices and issue them to military personnel. A key part of the CSDA program is data transportability: Any information on a soldier’s device has to be able to move to any other new device. To do this successfully – and in potentially very large numbers – when applied across the Army and DOD, the program had to go beyond simple mobile device management, explains Michael McCarthy, director of operation and program manager at the Army’s Training and Doctrine Command (TRADOC) Brigade.
Applications are the other side of the mobile device/software coin. Managing applications on devices and making sure they don’t contain malware or viruses are a major concern for enterprise level users. But the software space is dynamic and constantly changing, which means that organizations must decide how they will acquire applications—by purchasing them commercially, writing their own, or using some combination of the two approaches.

Although the evolving applications environment is complex, one of its advantages is that it is relatively easy for organizations seeking to upgrade to MAM or similar capabilities to do so, says Vikrant Gandhi, mobile and wireless principal analyst at Frost & Sullivan. “The reality of the market is that it’s not difficult to catch up,” he says.

SERVICES, CONTAINERS, AND OTHER APPROACHES
There is a growing niche for third party firms such to work with MDM providers to provide vetted methods to use applications, Gandhi says. The convergence of MAM and mobile content management is another trend that has appeared in the last 18 months, he shared. This convergence is enhancing content and making it easier to access. Security concerns for applications remain however. To meet this need, some firms are providing “application reputation” services that create databases of applications vetted for their security and ease of use, Gandhi says.

Applications developers are also making software containers that can automatically examine code for issues and automatically rewrite it if they detect a flaw, says Jules White, assistant professor of computer science at Vanderbilt University. This approach makes applications more secure and allows them to work in a way that MDM system have more control over, he adds. The containerization approach is useful for large enterprise users because it allows them to drop in apps and use them without having to rewrite the code themselves, he says.

On the federal side, especially in the Department of Defense, the government has spent the last several years working on a series of pilot programs that are now on the verge of major deployments.

AUTOMATING COMPLIANCE CHECKS
This being the federal government, besides security, an important measure is compliance with Section 508 of the Workforce Rehabilitation Act that requires all government developed electronic information to be accessible to disabled users. If the application meets DHS guidelines, it is published, Capella said. If not, developers can make changes based on the dashboard’s recommendations and restart the cycle. “It gives you everything from coding best practices all the way to security, [section} 508 and other compliance checks,” he said.

Enterprise users running internal app stores or menus are grateful to have a variety of build-or-buy options for vetting applications. With AT&T Mobile Enterprise Management, it’s never been easier to keep your business moving forward. Together, we can design and execute your mobile solution, from strategy to design to testing, to delivery. And it can be platform-agnostic, to fit your needs and goals. Today’s leading companies are choosing AT&T to make their mobile. Learn more about our Mobile Enterprise Management solutions at att.com/enterprise.
With many emerging options, some large enterprises are starting to get their MDM and MAM capabilities pinned down. But while that is a major part of the equation, CIOs and CISOs need to consider the details of how their mobile systems interact with the network, with business processes and workflows, and to be ready for the inevitable surprises that crop up, analysts say. For example, if a company is setting up a BYOD program, it may need to plan for unexpected events with user devices, says Jules White, assistant professor of computer science at Vanderbilt University. Among the many things that will have to be considered and worked out are security applications and user support aspects. Who does an employee call if they have an issue with their device: a help desk, the device provider, or the wireless carrier? And which issues might the help desk need to escalate to those outside parties?

Hidden costs and risks MDM offerings also becoming more complex, which may make it impractical for some smaller organizations to deploy and manage them, White says. One potential solution, however, is that wireless carriers are starting to offer MDM-like capabilities. White predicts that it may soon be possible for a company to sign up for a carrier-provided MDM service.

Security remains an ongoing concern for organizations because of the constant possibility that previously undetected flaws in application software might open the enterprise up to new threats, observes Vikrant Gandhi, mobile and wireless principal analyst at Frost & Sullivan. For example, BYOD policies present a variety of challenges, even with good security in place. Many smart phones have some sort of email access capability, which in some cases can get around security procedures by inadvertently accessing company email. While BYOD allows more personnel to join in a company mobility plan, firms need to consider the associated security and mitigation costs of such a policy before implementing it, he says. But even with the best security and policies in place, for both BYOD and organization-issued employee devices, unforeseen issues can pop up. Gandhi notes that a case that recently arose with iPhone’s Siri voice activated software, which turned out to be able to skirt access controls and reach programs such as company/work email via voice command. “Nobody had thought of that,” he says.

Staying in sync As applications and their management tools become a more central part of how enterprises approach mobile device deployments and management, it becomes a question of where to best store those apps. While there is a place for applications resident on a device, virtualization and cloud storage look attractive for a number of reasons such as accessing value added services from vendors, says Gordon Van Huizen, research director at Gartner. This approach may lead the rise of synchronization services for applications that allow them to run virtually while their devices are turned off or otherwise offline, he says. Virtualization also may create an operational triangle of applications, cloud services and mobile devices providing enterprise services, Van Huizen says. However, he adds that most enterprises are not yet in a position to work out such service arrangements.
Convergence in Action: Federal Programs Test Mobility at Scale

BY HENRY KENYON

Although merged MDM and MAM services and networks are showing up in the commercial sector, industry analysts say they are at their most mature and extensive in the public sector. The size and breadth of the federal government means that mobile device deployments across entire agencies and departments can be massive, complex affairs.

Depending on the agency, security is an overriding necessity for mobile devices in government service. Although there are some analogs in the finance and health care industries, where confidential information must be protected, analysts note a lack of such efforts on the enterprise side. “I’m a little surprised it hasn’t happened already,” Van Huizen observes.

CONFIDENTIALITY REQUIRED

On the federal side, especially in the Department of Defense, the government has spent the last several years working on a series of pilot programs that are now on the verge of major deployments. One of the military’s capstone mobile efforts is the DOD Mobile Capability. Managed by the Defense Information Systems Agency (DISA), which is responsible for managing all of the DOD’s communications and IT systems, the program’s goal is to support both classified and unclassified mobile device communications.

At the end of January, DISA will begin deploying version 1.0 of its unclassified mobile services with the goal of supporting up to 100,000 users by the end of the fiscal year, agency officials said. Launched in early 2013, the program currently supports 1,800 unclassified mobile devices such as Apple and Samsung tablet computers and smart phones and 80,000 BlackBerry devices.

STAGED ROLLOUTS

The program’s initial capabilities include an MDM system, a mobile applications store, an approved devices list, supported cellular access and DOD public key infrastructure (PKI) support. Release 1.0 also includes the transition of approved applications and related enterprise mobility services such as DOD enterprise email, the DOD global address list, service desk support and services such as Defense Connect Online, DISA officials said.

The long term goal for the program is to connect up to 600,000 military and civilian DOD personnel with mobile devices that will be used anywhere from offices to the battlefield, explained Robert Carey, the department’s principal deputy chief information officer at an industry event in June 2013.

Besides the DISA program, there are a variety of other mobile device efforts under way in the DOD. The U.S. Army has been actively working on issuing mobile devices to its personnel. In January, Army recruiting command began issuing 10,000 smartphones and tablets to its staff, said Michael McCarthy, director of operations and program manager at the Army’s Brigade Modernization Command.

McCarthy notes that the Army mobility program borrowed many data management techniques used by the health care industry for security and access to telemedicine services.

The program continues to steadily expand. In 2013, some 25,000 smart phones and tablets were issued to soldiers and McCarthy says he expects the number to grow to 35,000 or more this year. "If the budget can support expanding beyond that number I would look at it going up as high as 50,000," he says.

A DESKTOP IN YOUR HAND

Instead the Army replicated a desktop-computer type environment for its mobile devices. This consisted of a protected environment that took measured security steps to protect data at rest, when it is transmitted and when it is processed, McCarthy says.

The program took a similar approach to applications development. Instead of controlling everything, which was “a bridge too far,” it created an online software marketplace where troops could access vetted apps for Android and Apple devices, McCarthy says. The site gives troops the flexibility to select the apps they need to perform their specific jobs, he adds.

Like any large enterprise with security needs, the CSDA program has experimented with ways to keep data safe. This is relatively easy for troops on base, as information can be stored and accessed in a secure DOD cloud. McCarthy notes that the Army mobility program borrowed many data management techniques used by the health care industry for security and access to telemedicine services.

McCarthy notes that the Army mobility program borrowed many data management techniques used by the health care industry for security and access to telemedicine services.
Simplify Your Mobility Strategy with AT&T Mobile Management Solutions

Mobile Security Challenges are evolving. Make sure your Mobile Management Strategy does as well.

**Unique mobile threats grew by** 261% **the last two quarters of 2012 alone**

**IT decision makers were asked:**
What challenges, if any, does your firm face when developing and managing smartphone/tablet applications and devices?²

56% Securing the apps and data

54% Providing device security

40% Managing devices that are used for both personal and corporate apps

**A Holistic Mobile Security Strategy should address:**¹

Device stops threats before they attack

Content protect data

Applications secure apps and maintain functionality

**With so many mobility vendors today, one solution provider can help:**¹

1. Limit the supplier assessment time.
2. Build a holistic mobility strategy.
3. Build and manage mobilization activities.

**AT&T Mobile Management Solutions:**

MDM Mobile Device Management

MAD Mobile Application Development

MAM Mobile Application Management

MWM Mobile Workspace Management

✓ Span the lifecycle of mobility needs allowing you to meet multiple demands with a single provider

✓ Offer increased security, mobile agility, productivity and efficiency

✓ Device and carrier agnostic

For more information, visit att.com/mem.

¹ Source: ABI Research, Transforming Your Organization with Mobility, Making Smart Choices, April 13, 2013
² Forrsight Mobility Survey, Q2 2013, Forrester Research, Inc.