The purpose of any computer, whether a smartphone or a supercomputer, is to run software. Mobile devices and their stand-alone operating systems have brought a renewed focus to applications. Today, organizations need to think through their app choices. For an end-to-end mobility solution, IT management must choose the apps that will be part of the enterprise bundle as well as those that will be used only by specific users or groups of users. That’s why apps fall into two general categories:

- **Enterprisewide:** These apps are used universally: email, office productivity tools, web browsers, social media interfaces and collaboration tools such as SharePoint or Salesforce.com. Also, the organization may include utilities such as security, calendaring, contact lists and photo libraries.
- **Mission-specific:** These apps, commercial or custom-developed, serve a subset of users for a particular function, such as engineering or finance.

The choice of which apps to put on which devices depends mainly on the type of work to be done on each device. Office workers may need the full bundle so they can read (and perhaps edit) documents. Mobile workers, who might also have a cubicle and office somewhere, often can make do with the mission-specific apps in addition to the communication and collaboration programs. Field workers, in addition to their mission-specific apps, will likely need the collaboration apps and utilities.

The IT team can simplify administration and provisioning by creating a single enterprise image containing everything except the mission-specific apps. Each user would then choose from the app repository, with access based on role.

The need to develop custom apps for internal use has been decreasing rapidly as the major software makers continue to develop mobile versions of even complex software packages. For public-facing apps, not having mobile versions creates a distinct competitive
disadvantage for corporations and can reflect poorly on government and other public-serving organizations. For internal custom apps, not having a mobile version can limit the utility (and therefore the ROI) of a mobility solution. But a mobile app should not be developed as a separate entity from the web app being replicated for customers’ or constituents mobile devices. Instead, an organization should use an impending mobile rollout to modernize applications so they are endpoint-agnostic and optimized for the unpredictable performance of public networks outside of the organization’s control.

**Application Stores**

Self-service has spread to so many spheres, it’s almost hard to recall life before people booked their own travel or paid their water bills online. In enterprise life, workers routinely encounter self-service apps for human resources, financial and health benefits. And because nearly everyone is accustomed to downloading apps from popular online stores, many organizations are deploying branded app stores so that workers can self-provision their mobile devices.

Some MDM solution providers include app store modules, or an organization can use stand-alone tools to construct a store. The app store itself can work via the web on desktop and notebook systems or wirelessly on mobile devices. Users can download apps to their PCs and then add them to mobile devices when they next sync, or they can load them directly onto mobile devices wirelessly.

An enterprise app store should include a wide range of whitelisted companion apps that may also exist at consumer app stores. That will provide a convenience to users and help them avoid rogue apps, and it will ensure that the IT shop can log the apps on each worker’s device.

But distinct differences exist between public and private app stores. An organization’s store must keep track of software licenses, and it must limit downloading of some apps only to authorized users.

Managing licenses is critical so that the IT department can avoid underlicensing, which can expose the organization to payments and punitive fines from a license audit. A best practice, therefore, is for the security or financial staff to conduct periodic audits of the in-house app store to ensure compliance with all licensing agreements.

How does an organization decide whether to establish a public-facing app store? Countless retail, transportation, nonprofit and educational organizations >

**MOBILE APP MANAGEMENT FUNCTIONS**

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>WHAT IT DOES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrapping</td>
<td>Secures third-party or in-house apps by wrapping them in individual logical containers that prevent data exfiltration or interaction with blacklisted or even other whitelisted apps</td>
</tr>
<tr>
<td>Delivery</td>
<td>Automates configuration, maintenance and updating, and maintains role-based app bundles for different types of workers who provision their own devices – in effect, orchestrating the pushing of apps to users once they log in and authenticate their devices</td>
</tr>
<tr>
<td>Store and remote management</td>
<td>Changes controls, removes and adds apps to the online library, and removes apps remotely from devices if the user has changed roles</td>
</tr>
<tr>
<td>Authentication and reporting</td>
<td>Controls downloads and users’ individual app collections by authenticating users and devices, and generates reports on downloads and usage</td>
</tr>
</tbody>
</table>

**DEVICE PROVISIONING FROM CDW**

CDW can deliver devices with provisioning tailored to each worker. Users simply take the device from its box, do an initial login to enroll and download their identity certificates — and they are ready to go.
offer mobile apps from their websites, but far fewer make them available at places such as the Apple App Store or the Android Market. The decision depends on a combination of how many apps the organization offers and whether revenue from commercial apps will be enough to justify the infrastructure to support the store.

Mobile Application Management

An app store or download web page is only one component in an organization’s mobile app management strategy. MAM is emerging as a separate category of software alongside MDM, although the major MDM vendors currently include MAM capabilities in their offerings. But MAM is gaining prominence as mobile use continues to grow, because organizations have begun to realize that app management is distinct from (even if highly similar to) device management.

Full-featured MAM solutions let an organization build an app store and equip it with device enrollment and certificate-issuing functions. The MAM also serves as the repository for app-use policies and as a mechanism for the IT department to maintain whitelists and blacklists.

Mobile apps have their own lifecycles, distinct from the devices they run on. MDM focuses on devices and their access to enterprise data; MAM focuses on internally developed apps being valuable intellectual property. Because each instance of a third-party app potentially represents a license, each download must be logged and registered with the organization’s software asset management system.

In addition to securing and pushing apps to devices, most MAM programs also have a reach-back function to report on app usage, to fetch updates and apply them to apps, and to maintain configurations. MAM solutions also deliver analytics about whether and how individual workers use given apps.

Security and Apps

Safe mobility calls for a layered approach to security. To secure apps, the IT team first must make sure the devices themselves are handled securely.

An organization needs, at minimum, to take four actions should a device fall out of security compliance. The MDM solution should warn the administrator, send a message to the user with the action that must be taken, block the user’s access to email or other enterprise apps until the situation is remedied, and if necessary, remove the organization’s apps and data.

Plus, the IT department should have policies in place that enforce the use of strong passwords and device encryption.

Still, a number of threats can place apps at risk. All mobile apps to some degree — but especially Android apps because of the multiple manufacturers of Android hardware — are susceptible to malware threats.

App infections may come in via mobile web browsers or links in phishing email and texts. They may come from apps downloaded from unauthorized sites. Occasionally, malware comes in by way of bugs exploited in the software controlling the baseband cellular communications processor on a device.

Mitigating these threats requires containerizing organizational apps or creating logical sandboxes on user devices and preventing cell-wall crossover of personal data. Security best practices should also take into account the always-present threat of lost or stolen devices. Remote wiping of enterprise apps and data should be a first — and not last — resort.

HOW TO MANAGE MULTIPLE EMAIL ACCOUNTS

Most users have at least two email accounts, one for work and one for personal messaging. But many people have more than two. The security challenge becomes how to separate the organization’s email, with its confidential attachments, from someone’s Gmail or Internet service provider accounts.

Best practices for protecting enterprise email and its associated data include requiring device encryption before letting users access work email.

Here are three other steps to take:

1. Set the MAM program to prevent attachments from being opened in unauthorized apps or by apps outside the container or sandbox. Also establish the reverse condition: No personal email or attachments may be opened in secured, organizational apps.

2. Disable the ability to copy and paste among email accounts and to forward messages out of the enterprise account or into it from personal accounts.

3. Extend these restrictions to photos, links, files and attachments in workers’ personal social media accounts.
ABOUT THE CONTRIBUTORS

JASON BROWN is the Technical Field Mobility Solution Architect for CDW, helping inform customers about the ever-changing mobility landscape. He works closely with a team of internal and field solution architects, assessing customer needs in all aspects of the mobility workplace. With over 18 years of technical experience, he brings a wealth of knowledge to the team, researching mobility updates from CDW vendor partners and helping provide successful solutions for education, healthcare, government and small, medium and large enterprise environments.

STEPHANIE SULT is a Mobility Solution Architect with CDW, specializing in the healthcare industry. In her role, Sult develops and implements comprehensive enterprise mobility solutions for CDW's healthcare customers. She specializes in enterprise mobile management, mobile device management, carrier activation services, telecom expense management and mobility IT help desk services. Sult holds a bachelor's degree in business administration from Saint Mary's College (Ind.) and currently resides in Chicago.

LOOK INSIDE FOR MORE INFORMATION ON:

- Building out a holistic mobile strategy
- Purchasing the right devices for workers' job needs
- Fine-tuning MDM to better meet organizational needs
- Getting a handle on app management