CDW PEOPLE WHO GET IT

MOBILE SECURITY

A mix of well-thought-out policies and up-to-date technologies are needed to protect critical data.

Executive Summary

Mobile devices (notebooks, smartphones and tablets) represent the new norm for staff and managers in all kinds of enterprises. It's become increasingly common to walk into a meeting and find at least one participant with a notebook, two mobile phones (for work and home) and a tablet.

And likely all of these devices would have Wi-Fi and 3G or 4G data service. Organizations are changing — some rapidly, some slowly — to accommodate new ways of working as bandwidth, computing and accessibility evolve.

For network and security managers, these devices represent the worrisome prospect of organizational data flying around — unsecured — in easy-to-lose and easy-to-compromise packages.

Mobile devices are small and valuable, making them favorite targets of thieves. But, in fact, the content on the devices is likely more valuable than the device itself. So security awareness needs to extend to the content itself.

Keyboards are hard to use or nonexistent on phones and tablets, often causing users to auto-save their passwords for e-mail and virtual private network (VPN) access — passwords that can open up organizational resources to anyone who picks up the device. For these reasons, the security techniques that work for desktops are not enough for mobile devices.

TWEET THIS!

Table of Contents

Building mobile security means taking on five key areas of security:

- Mobile-device policy and management
- Data in motion
- Data at rest
- Malware protection
- Authentication solutions

By deploying solutions and setting policies in each of these areas, network and security managers can support the goals of their organization, empower staff to work wherever they are, and reduce the risks associated with mobile devices.

Device Management and Policies

Any approach to mobile security must start with establishing a mobile-device policy. Without a policy, network and security teams will be adrift from both a technical and administrative point of view. Policies are a critical first step, for three reasons:

- **Policies set limits.** Without a policy, the organization falls into an "anything goes" mode, which can result in security problems and internal staff conflict.
- **Policies create efficiency.** Although many IT managers find that setting policies is a tedious process, the result is greater efficiency. A stable organizational context for mobile devices, when it properly involves IT support, removes the inefficiencies of "self-service IT."
- **Policies support compliance.** In an environment where nearly every organization fits into some compliance or audit regime, policies for mobile devices and mobile security are part of the process of getting and staying compliant.

These policies should cover four areas: device selection, deployment, use and recovery.

Device Selection

This policy section defines which devices are allowed on the organization's network and which can store sensitive organizational data. It also answers the most important and difficult question: Who owns the device? The word *owns* here should be taken loosely, because discerning the physical owner of the device — that is, who paid for it — is not nearly as important, from a security point of view, as understanding who *controls* the device.

Generally, the amount of access and information thatthe IT group grants to a device should be proportional to the amount of control the organization has over it. An uncontrolled device, one owned and managed by the employee, represents a huge security risk if improperly configured.

On the other hand, a device completely managed and configured by the organization is nearly as secure as a desktop at headquarters, and thus can be granted greater access to sensitive information. The issue of control, and the relationship between different levels of control, risk and access, must be front and center at the beginning of any mobile-device policy.

There's been a great deal of talk in the information security community for some time regarding "bring-your-own-device," or BYOD, initiatives. The thinking goes: If a staffer pays $750 for a tablet device that increases information access and improves productivity, then somehow the organization should find a way to allow that device onto its networks.

But it's not as easy as it might seem. The BYOD issue comes back to ownership. If an organization can control and manage the device — regardless of who paid for it — then the risks associated with BYOD can be reduced significantly.

The mass adoption of powerful smartphones and tablets, especially by executives, is having a healthy effect on ossified IT security policies and procedures. When the CEO shows up in the office with a tablet and says, "Make this work," the IT team is forced to focus on the clear benefits of mobile devices and find creative solutions to provide secure mobility.

The Changing Device Environment

As the enterprise sets and runs the mobile-device security policy, keep in mind that it is not a static document, but must change as the device environment changes. Here are some things to consider.

1. Device trends change quickly, so make the certification program for mobile devices inexpensive and fast. Decide whether or not the organization is going to add a new device, or delete an old one, as quickly as possible.
2. Be careful about variation among devices running the same operating system. Not every Android, Symbian or even BlackBerry device is the same. Define the minimum characteristics of a device to be supported, rather than just naming a device or an operating system.
3. Stay in constant communication with users. If the enterprise has embraced BYOD and isn't going to support a popular device, let people know as soon as possible because it may influence their purchase decisions.

The trend toward supporting BYOD within organizations is reducing interest in the "walled garden" approach to mobile security (or what Gartner calls the "heavyweight approach"). In this model, the IT group adds redundant applications to mobile devices (such as a second e-mail client) in the name of security. But because this fails to deliver the experience that end users imagined when they bought their new smartphones or tablets, it's unpopular with BYOD adopters.

Still, device selection cannot be a free-for-all, and every device that accesses enterprise resources must fall under a policy.

Device Deployment

Provisioning mobile devices, deploying them to end users and managing configurations can be accomplished using software and services that the organization controls. However, there may be limitations based on the diversity of management platforms.

Obviously, tools that work well for managing Windows notebooks, such as Microsoft's Group Policy Objects and a variety of patch management and configuration products, won't work for notebooks running anything other than Windows.

The sheer diversity of options, including two popular notebook operating systems (Windows and Mac OS X) and five major smartphone or tablet platforms (Microsoft Windows, Apple iOS, Nokia's Symbian, Research In Motion's BlackBerry and Google's Android), is one reason that it's important to define a device selection policy.

The device deployment section of a mobile security policy should acknowledge that different devices might have different capabilities when connecting to the enterprise network, and that these capabilities may be driven by the deployment and configuration platforms selected by the organization.

For example, an organization that has selected the BlackBerry as its preferred smartphone will gain significant configuration control and mobile-device management through the platform itself. So devices may be granted greater access to organizational applications because the tools to reduce risk are built into the BlackBerry product line.

But when a worker shows up with an Apple iPhone or an Android tablet, RIM's tools don't apply. In this scenario, these devices may be granted a much more restricted view of the organization's network and applications.

Saying "yes" to every type of mobile device may be desirable. However, the real answer should be "yes, but ..."

This is because of each device's unique security capabilities and risk controls. Not every device can or should be given the same access. This issue has to be covered in the device deployment policy.

Such policies evolve as a natural consequence of the organization's usage requirements for mobile devices. When developing deployment policies and procedures, IT managers need to clearly define the expected use cases for mobile devices. This will help determine the deployment requirements.

For instance, if a device will be used only for e-mail and other common shared productivity applications such as calendars and contacts, then it needs the least amount of access to enterprise networks and should be deployed with a corresponding level of security. However, if a device needs to access business-critical information, retrieved using a custom app written for mobile devices, then a greater level of network access (and security) must be written into the deployment requirements for that device.

While device deployment policies will vary based on the organizational use case, the elements in the sidebar "Common Elements of Deployment Policy" are usually included in every deployment policy and can directly affect the selection of applications for mobile-device management.

Common Elements of a Device Deployment Policy

Element	Typical Requirements
Device configuration	The policy covers operating system and patch versions, installed applications (often whitelisted or blacklisted) and application usage, data and voice communications expense controls, and backup and restore schedules.
Device security	The policy covers endpoint protection tools such as antimalware and personal firewall, device locking, password complexity and change frequency, remote wipe, and VPN configuration.
Data security	The policy covers encryption and archiving of stored data, along with encryption of over-the-network communications.
Device administration	The policy covers inventory management of devices, provisioning and configuring, and device performance monitoring.

Device Use

This section needs to cover what is and is not permitted for devices that access corporate data. For organizations that have embraced BYOD, this can be touchy because they are, in effect, telling staff members what they can and cannot do with their personal devices. However, experience has shown that most workers care about security and will make an effort to comply with usage policies if they receive proper training.

An important part of the use section is the organization's acceptable-use policy (AUP), which outlines the boundaries of what is permitted in very clear and unambiguous language. Anyone with a mobile device that can connect to organizational resources, even to something as simple as a mail server, must read and sign the AUP before they are allowed to connect.

Another key part is training and education. Mobile-device users must not only sign an AUP, but also understand and follow the device use policies. Training won't make every user 100 percent compliant with an organization's mobile-security stance. But we know that an untrained user is far less likely to maintain organizational security. Training helps to explain the policies and convince mobile-device users that the policies benefit everyone.

Common Elements of an Acceptable-Use Policy

Element	Typical Requirements
Core security	All devices must have personal firewalls and antimalware tools, configured by the IT department.
Inventory and configuration	All devices must be registered and configured by the IT department.
Secure usage	Devices must have auto-lock, encryption and strong passwords. Users may not "jail break" their devices or install unapproved software.
Loss avoidance	Devices may not be loaned or shared. Users must be responsible for devices (and any other computer- or cloud-based data storage service that synchronizes with the device). Lost devices must be reported immediately and wiped if possible.
Data protection	Encryption and authentication configurations are set by the IT department and may not be changed. Passwords must be protected and can't be stored.
Device retirement	Devices must be fully wiped by the IT department before being retired or sold.
Help desk	The organization should spell out support policies, as well as policies for disconnecting devices in the event of noncompliance.

Device Recovery

Finally, the mobile-security policy must address recovery. It will need to address at least these four questions:

- Who is responsible if a device is lost, and what needs to happen?
- How will devices be upgraded and maintained? (And what happens to unmaintained devices?)
- Who determines when a device should be replaced?
- What happens to devices when they reach end of life?

The answers to these questions will also affect the organization's AUP. Mobile devices can represent a significant capital and maintenance expense, especially when product lines and pricing make them attractive to staff at every level of the organization.

Because mobile devices take a lot more abuse than desktops, they need to be replaced more frequently. A policy that spells out when a device should be replaced will guide users expectations and limit confusion.

Mobile-Device Management Tools

Mobile-device management (MDM) tools offer a dizzying array of options, which make picking the right tool a daunting task. Once an organization's mobile-security policy is written and the requirements are in place, a dozen products may fit the bill for handling mobile-device management tasks.

The first step is to narrow the field by deciding on a delivery method: either through cloud-based software as a service (SaaS) or an on-premise solution. Smaller organizations may lean toward SaaS as a cost-effective approach. When an on-premise solution is appropriate, MDM vendors can deliver preloaded appliances as well as applications that can be loaded on normal enterprise servers.

With on-premise solutions, large organizations may want to add scalability and high availability to their evaluation criteria. Several MDM vendors have included these features in their products to help support the growing population of mobile users.

Next, narrow the choice of MDM solutions by considering the range of devices they cover. There is no one product that can handle all mobile devices, plus Windows and Mac notebooks and desktops, so most organizations will need more than one MDM solution.

From this point, the evaluation of MDM products should be driven by an organization's device deployment policies, particularly as they relate to data security and device configuration, security, and administration. Using a checklist to tick off the following questions (and having a good deployment policy in hand) will help zero in on an MDM solution:

- Can the MDM tool detect and enforce device configuration policies, such as operating system and patch versions, and apply application whitelists and blacklists?
- Can the MDM tool help in installing, upgrading and removing applications?
- Can the MDM tool assist in backing up and restoring devices?
- Can the MDM tool detect and enforce communication expense controls, such as disabling roaming or data usage?
- Can the MDM tool detect and enforce device security policies, such as the configuration of endpoint protection, device lock and password rules?
- Can the MDM tool configure corporate applications such as e-mail, VPN and hotspot usage?
- Can the MDM tool configure communications applications, whitelist or blacklist service set identifiers (SSIDs) and insecure Wi-Fi configurations, and block noncompliant channels such as Bluetooth?
- Can the MDM tool block access or send alerts when a device is noncompliant?
- Can the MDM tool manage remote wipe, either partial or full, if needed?
- Can the MDM tool enforce data security policies, including local encryption of enterprise data and encryption of all network communications?
- Can policies and configurations be updated over the air? Can device synchronization occur over the air?

MDM tools vary in their enrollment, management and configuration capabilities. For example, some products operate entirely by wireless and encourage a self-service approach to device enrollment. Others require the IT group to manually install and configure their software agents on mobile devices. Organizations with large deployments will want to focus on tools that minimize human touch and leverage the self-interest and expertise of mobile-device users.

MDM tools can also assist in administrative tasks, such as device inventory and help-desk support. Plus, most offer alerting and reporting to help manage devices and keep IT staff apprised of problems.

Because mobile devices often have other management tools built in, integration between MDM solutions and existing device management functionality is important.

For instance, in an organization that already uses RIM BlackBerry server tools — some of which have strong MDM features that support only BlackBerry devices — it might be preferable to have a single MDM console that can talk to the BlackBerry Enterprise Server in the background,

The Evolving MDM Market

The demand for iPhones, iPads and Android devices in the enterprise has jump-started the mobile-device management (MDM) product space, resulting in more than two dozen vendors competing for available MDM dollars. About half of these products are available as software as a service (SaaS), an attractive option for small businesses that don't want to invest in an on-premise appliance or software solution.

Finding the right MDM tool can be difficult because there are overlapping security product categories that provide these capabilities. For example, Microsoft Exchange ActiveSync includes many MDM features, but it doesn't cover endpoint security.

On the other hand, network access control vendors have products that are good at maintaining compliance with device security policies, but they don't do anything to help configure devices. Meanwhile, endpoint security and endpoint encryption vendors offer management tools, but they're aimed at controlling the configuration of their own products and don't cover the entire mobile device.

Still, the MDM market is quickly becoming a stand-alone business, separate from endpoint protection products (although both McAfee and Symantec compete with solid offerings). Within this growing market, the unique requirements of devices running Android, iOS, BlackBerry, Symbian and Windows Mobile/Windows Phone mean device management tools fall into a phones-and-tablets category on one hand, and a desktops-and-notebooks category on another.

Even though tablets and notebooks are beginning to merge in their capabilities, and the same issues of security are present on all platforms, IT managers usually must find separate products to cover the two categories of devices.

Remote Wipe: Understand the Subtleties

Remote wipe of mobile devices (as it applies to smartphones and tablets) is considered an ideal way to handle device loss or theft. As long as the device is turned on and is within range of a communications channel, a remote command sent by the device owner or IT staff can erase all data, whether the device is encrypted or not.

But what sounds like a great idea can backfire, because not all devices that are considered lost are actually lost – they might turn up minutes, days or weeks later.

If the missing device has only enterprise data on it, then remote wipe seems safe because all the data can be downloaded again onto a new device. The problem arises when a device is acquired for both work and personal use.

If the device user has a substantial amount of irreplaceable personal data, such as photographs, he or she may hesitate to report a lost device in the hope that it may turn up. Thus organizations and device users have conflicting interests: the IT team wants to wipe devices immediately when they're lost, and owners want to delay wiping as long as possible, hoping their device will eventually turn up.

Two techniques can help resolve this conflict. The first is a well-enforced backup system that's dictated by policy. If the owner is confident that all personal data is recoverable, he or she will be more willing to wipe the device. Even if the organization has no requirement to back up information on a mobile device, a solid backup policy may be needed to reduce the risk of lost devices.

The second technique is called a "partial wipe," supported by some devices and some MDM tools. A partial wipe lets the IT group erase only certain types of data from the device, such as VPN settings, stored e-mail and SMS messages, and the organization's phonebooks.

A partial wipe may seem like a good idea, but it could raise more questions than it answers, specifically the question of what is sensitive data and what is not. A partial-wipe policy would need to trigger other policy choices; the easiest solution for IT managers is backing up devices to allow for full device wipes, rather than hoping to catch everything important by wiping part of a lost device.

keep policies consistent, and remove the requirement for double-configuration.

As with every manufacturer, RIM's tools don't extend beyond BlackBerry devices in any significant way (though a trend is building, with RIM and other manufacturers planning expansions of their MDM tools beyond proprietary devices). But endpoint protection and mobile-device encryption vendors don't hesitate to extend their footprint and product functionality. In some cases, the growth of endpoint protection and encryption consoles to cover more mobile-device features may save organizations the need to buy a separate MDM tool.

Keeping Data Safe with Encryption

Mobile devices are meant to be taken out of the office and on the road, where some are bound to be stolen or misplaced. The rates of loss are staggering – 10,000 cell phones lost each month in Chicago taxi cabs, 50,000 notebooks lost each month in major U.S. airports – which means the odds are pretty good that someone in the organization is going to lose something important. So encryption is a must-have for any mobile device that might hold enterprise data.

Although individual applications can encrypt and protect data on hard drives, best practices call for the operating system itself to enforce encryption. This avoids the possibility of an application glitch resulting in failed protection measures and gives IT staff the ability to control encryption across an entire device.

Unfortunately, individual devices have different encryption styles and characteristics. Notebooks running recent versions of Windows and Mac OS X can easily take advantage of whole-device encryption. However, not all smartphones and tablets have the same capabilities.

Generally, recent versions of Android and Apple iOS include whole-device encryption. In Apple's case with iOS (in version 4.0 and above), the encryption is enforced by the hardware and is running all the time. So enabling encryption is just a matter of flipping a few preference bits.

For Android devices (in version 4.0, although some devices running 3.0 also have built-in encryption), manufacturers' settings vary, but most devices come with their encryption turned off. Turning it on may require a wait of an hour or more, depending on how much data is on the internal drive.

Windows Mobile 7 does not include whole-device encryption, even though Windows 7 for desktops and notebooks does. BlackBerry devices, thanks to RIM's corporate focus, have had full-device encryption for many years.

Given the variation in support for full-device encryption, third parties have stepped up to offer consistent encryption tools and policy enforcement across a range of devices. Organizations trying to support multiple devices as part of their mobility policy should investigate these tools to simplify the problem of managing encryption and enforcing a consistent level of encryption across all devices.

Because mobile devices are used in a variety of public spaces, encryption of data in transit (to or from mobile devices) is critical. No Wi-Fi hotspots should be considered completely safe, and the mobile phone network is not that much safer. The IT team should ensure that all data is encrypted in transit by requiring a VPN connection for any communication back to the organization's own networks.

The one exception to a "VPN always" policy is e-mail. Because major e-mail protocols (IMAP and SMTP, or Microsoft Exchange's RPC-over-HTTPS) can all be encrypted, it's safe to let encrypted e-mail travel outside of a VPN connection. And because e-mail is one of the most-used applications on mobile devices, it makes sense to optimize e-mail's path to improve the end-user experience.

However, users should be trained to recognize suspicious activity. For example, they should know what a Secure Sockets Layer man-in-the-middle attack looks like and also know never to click on dialog boxes about untrusted or otherwise unusual digital certificates.

Authentication and Access Controls

Much of mobile security's focus is keeping devices and data safe. But the mobile endpoint isn't the only system that needs to be protected. When networks are opened so that mobile devices can connect (even using a VPN), they need appropriate controls to make sure only authorized staff members have access.

The Trusted Computing Group, an industry standards organization, has designed vendor-neutral architectures to help link mobile devices, authenticated users and network access controls. These product standards are often aimed at LAN users, but they are also ideal for mobile clients, where access control, authentication and endpoint protection enforcement all come together.

The most common form of authentication is the password. Although passwords are familiar technology, they aren't very good at authenticating remote users. Passwords are easily shared and stolen. When combined with other authentication methods or access control restrictions, passwords may do the trick. But in remote-access situations, they represent a high level of risk.

Two common authentication methods that offer higher security than passwords alone are multifactor authentication and digital certificates.

Although multifactor authentication vendors like to parse words over details of security, their products are more similar than unique. The idea behind multifactor authentication is that a user is authenticated by more than one thing (their password), such as a physical device or particular mobile phone. More factors equal more security – up to a point.

The most familiar of these authentication systems is based on small hardware (or software) tokens that display a code when activated. The code, combined with a secret personal identification number known only to the token owner, can be used as a password only once, and typically only for a brief period of time.

If the token is lost, the displayed code is useless without the PIN, username and other access information. Spying on

Caveats Come with Encryption

Although encryption is an important feature of mobile-device security, it's not a universal protection for lost devices. Casual attackers may not be able to extract data. But a device stolen by a determined, knowledgeable thief with a particular information goal may be able to exploit weaknesses in the encryption itself or recover the PIN for unlocking the device.

The built-in encryption tools of mobile devices are most likely to have known workarounds. This doesn't mean that third-party encryption tools are more secure than built-in encryption; simply that, because they are not as widely available, third-party tools haven't suffered the same level of sustained attacks.

Even if device encryption were hacker-proof, the unlock code for a device remains a weak link. Often as short as four numbers, these codes can be stolen easily by "shoulder surfers," nullifying the effect of strong device encryption. And making unlock codes longer can prove difficult: While notebook users might not mind typing longer passwords, mobile phone and tablet users may balk at requiring long or complex unlock codes.

One of the most common misconceptions among security professionals is that password complexity is important to avoid attacks. In fact, long passwords that use nothing more than letters are much more resistant to brute-force attacks than short passwords that use special characters.

Because it's difficult to use special characters on mobile devices that don't have keyboards, IT staff should take advantage of the natural power of longer passwords and drop requirements for special characters. This will reduce the risk of brute-force attacks and stolen short passwords, and it will increase end-user satisfaction by making passwords easier to type on mobile devices.

Encryption dramatically reduces the risk of a device being lost or stolen, but any risk-assessment exercise must consider unlikely scenarios where all precautions fail to adequately protect on-device data.

mobile users won't do any good because a stolen password can't be used a second time. Multifactor authentication systems are usually licensed per user. Both on-premise and cloud-based solutions are available.

In the world of mobile phones and tablets, using multifactor authentication for VPN tunnels reduces the risk that a lost device will compromise the organization's network. It may even be advisable to use multifactor authentication for e-mail when especially sensitive information is being shared.

Digital certificates represent a step up from multifactor authentication. The science behind digital certificates is complex, but the essence is that you prove who you are by proving you possess a very long string of bits (2,048 bits is not uncommon), which make up your secret key. Authentication can occur completely in the open, but an eavesdropper still won't be able to steal the secret key.

Another benefit of digital certificates is that they offer bidirectional authentication. In both multifactor authentication and normal user name/password authentication, the end user is authenticated, but the server they're connecting to is not.

This means that a man-in-the-middle attack could be used to steal credentials. With digital certificates, both the network VPN server and the mobile device user are authenticated, eliminating the possibility of a man-in-the-middle attack.

The problem with digital certificates is that software and hardware support for them is spotty. Although many government agencies have required digital certificates for more than a decade, commercial acceptance has lagged.

Companies that use Microsoft Windows and Active Directory get digital certificates for free — Microsoft includes the capability to use certificates for authentication in all recent versions of Windows. VPN clients, such as Cisco AnyConnect, can also use Microsoft digital certificates for authentication.

Organizations concerned about mobile security should look into network access control products that combine stronger authentication, access control enforcement and endpoint compliance checking. Taken together, these security functions help significantly reduce the risk presented by mobile-device users.

BoxTone

BoxTone's Enterprise Mobility Management (EMM) platform delivers centralized, automated control of all mobile devices and tablets including iPhone, iPad, Android and BlackBerry, as well as the apps that run on them. Built to CIO and CISO specifications, BoxTone aligns mobility management with core IT services, extending existing resources and processes to fully secure, manage and govern mobility on par with all other critical IT systems.

CDW.com

TREND MICRO Securing Your Journey to the Cloud

With the growing popularity of high-end mobile devices, many employees are opting to use their consumer-grade personal devices, such as PCs, tablets and smartphones, in the workplace. Trend Micro suggests you embrace consumerization and securely manage your workforce without limits. Mobile Security is a fully integrated mobile-device management and security solution within a security framework that spans physical and virtual, PC and non-PC devices. It protects data by enforcing the use of passwords, encrypting data and remotely wiping data from lost or stolen devices.

CDW.com/trendmicro

KASPERSKY lab

Kaspersky Lab has the right formula for securing your virtual systems. Virtual machines aren't exempt from the dangers of cybercrime, malware and targeted attacks. Kaspersky delivers a new breed of protection for your virtual environment, keeping it secure and allowing the administrator to manage it effectively.

CDW.com/kaspersky

TWEET THIS!

CDW® PEOPLE WHO GET IT™