SearchSecurity

TechTarget

E-Guide

MDM features vs. native mobile security

Mobile device management or MDM plays a critical role in mobile security, but should MDM security features always trump native security features of mobile devices? Lisa Phifer weighs in on how to choose the best approach for your workforce.

Contents

MDM security features vs. mobile security: Striking a balance

By Lisa Phifer

Mobile device management (MDM) products can play a big role in mobile security by provisioning and enforcing mobile native security measures embedded in smartphones and tablets.

But some MDM products blur the boundary between "governing" and "doing" by delivering integrated security measures such as secure messaging or VPN to replace the native security measures baked into each device. Which approach is a better fit for your workforce? Let's take a look at the pros and cons of each.

MDM security features: Going above and beyond

Baked-in MDM security features can complement native mobile security by protecting data at rest, data in motion, or by promoting device integrity. Some MDM-integrated capabilities date back to when mobile operating systems such as Win CE were largely devoid of native security. More recent examples of such integrated measures are the innovations to minimize bring-your-own-device (BYOD) risks. Here are some common examples:

- **Mobile content management:** Today, many mobile devices support hardware encryption, but some still do not. In addition, co-mingling of business and personal content makes it harder to reliably wipe sensitive data without negatively affecting the user. To enable safe, productive use, IT should consider pushing business documents over the air to stored in encrypted containers on the device that enable offline access while preventing data leakage. A growing number of MDM products from vendors such as AirWatch LLC and Fiberlink Communications Corp., can provision, update and, (when necessary), wipe this type of "document locker" and its contents to protect data at rest.

- **Integrated secure messaging:** Every smartphone includes email, contact and calendar apps that synchronize messages, attachments, etc. with carrier or cloud services. Devices commonly support Exchange ActiveSync (EAS)-based enterprise messaging, but supported security policies vary by device make/model. On BYODs, IT should seek to insulate business data where risk warrants by separating business and personal contacts or preventing attachments from being forwarded. To create a consistent device-independent environment, some MDM vendors, including Good Technology Inc., Denmark's Excitor A/S and Sybase Inc., incorporate secure messaging apps. These non-native apps can be used to safely access enterprise mail, contacts, calendars and tasks, while IT can easily provision and remove them via MDM.

- **Integrated VPN/firewall:** Every mobile OS includes a potpourri of native VPN clients, but the odds of finding your chosen VPN in every device without third-party client installation are slim. Moreover, unlike laptops, smartphones and tablets don't include host firewall capabilities. To eliminate gaps in VPN coverage while deflecting unwanted traffic, some MDM agents (such as those from Mobile Active Defense, Symantec Corp., and Zenprise Inc.) include their own VPN/firewall, protecting all data-in-motion without relying on native VPNs.

- **Antimalware:** Contemporary mobile operating systems take steps like application sandboxing to deter malware, but they do not include native virus scanners. Some MDM features (specifically those from McAfee Inc. and Symantec Corp.) fill this gap by building antimalware measures into MDM agents. Jailbreak and blacklisted application detection is common; a few agents also provide on-access or on-demand virus scanners.

MDM security features vs. native security: A Balancing act

Complementary security measures can be beneficial, but do you really need native *and* MDM-integrated security? When both measures are present, how can you decide which to use to implement enterprise security policies? Let's consider some of the tradeoffs.

- **Platform independence versus separation of duties:** MDM-integrated security measures level the playing field, creating a uniformly safe environment on a wide variety of consumer-grade devices. On the other hand, for integrated security measures, the fox is watching the henhouse. If you have a requirement for separation of duties, MDM should not both deliver *and* enforce security.

- **Trusted environment versus usability:** By closing gaps in native security, MDM-integrated containers and messaging apps create a trustworthy environment in which to conduct business. This secure workspace makes it easier to control, monitor and cleanly remove business data and apps. But forcing workers to interact differently with business data and apps can also create confusion and sap productivity. Assess risk by user/group and device to decide which cases warrant this extra security is worth the cost.

- **Simplicity of deployment versus best of breed:** MDM-integrated security measures tend to simplify deployment and total cost of ownership. If your workforce requires a third-party VPN/firewall or antimalware, getting these features "for free" with MDM is handy. However, if your MDM's integrated VPN or antimalware approach diverges from those used on laptops or desktops, consistency may dictate use of another vendor's third-party solution.

- **Focus versus extensibility:** MDM-integrated messaging applies compensating controls and associated policies to business assets only. IT can operate freely within that space – for example, backing up or removing containers as needed – because those assets belong to the employer, not the employee. But, unlike native security, this laser-like focus prevents easy extension to other applications.

For some workers, a hybrid approach may be preferred – for example, secure messaging for robust protection of key business assets, accompanied by native measures such as full device encryption to protect everything else. Ideally, MDM-integrated measures should not force IT's hand -- look for products that empower the enterprise to decide when and where to apply native and/or integrated security measures as appropriate to reflect business risk, device capabilities and security policies.

About the Author:

Lisa Phifer owns Core Competence Inc., a consulting firm specializing in business use of emerging Internet technologies. Lisa has been involved in the design, implementation and evaluation of internetworking, security and management products for 30 years. At Core Competence, she has advised large and small companies regarding security needs, product assessment and the use of emerging technologies and best practices.

TechTarget

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

SearchCloudSecurity

SearchMidmarketSecurity

SearchFinancialSecurity

SearchSecurityChannel