IBM Security
Thought Leadership White Paper

Mobile data security

Protecting confidential data while keeping mobile users productive

Mobile data security: finding the balance

The terms Data Leak Prevention (DLP) and Container are beginning to dominate the mobile management conversation. Over the past few years great strides have been made in providing the tools and solutions that offer management and security for mobile devices; both for devices the enterprise owns and those that employees own.

While these solutions generally meet the need to secure the device, they have been lacking in some of the more sophisticated security aspects that are commonplace in laptop and distributed network deployments. Specifically lacking are the robust DLP controls common in laptop management solutions.

Prudence dictates that you look for ways to supplement your mobile device management (MDM) solution with additional, more robust security controls to help secure and protect sensitive data from being distributed to unauthorized third parties, either inadvertently or maliciously.

Balance your company's tolerance for risk related to securing confidential data with providing a productive, simple user experience.

Understand your goals

As you research technology, you will discover different approaches. These approaches have different strengths and weaknesses, but the first task is to understand your goals. You will need to balance your company's tolerance for risk related to securing confidential data with providing a productive, simple user experience as you develop your goals and approach profile. Be sure to consider the following:

Stopping the insider – A passcode policy and device encryption will not stop an authorized user if they are intent on copying data. Controlling this falls within the realm of DLP. Your organization may have already made significant investments in controlling the movement of confidential data beyond your hard and soft perimeters for laptops and desktops. If so, look for capabilities that extend DLP to your mobile device deployments. Your policy and goals should be consistent for all types of devices in your organization.

Stopping the outsider – The MDM vendor community has done a great job of providing tools that safeguard data on mobile devices. Enforcing a passcode and encryption, and being able to wipe the device is 90 percent of the battle. However, significant challenges still remain in being able to consistently and reliably apply and verify these controls, especially on the many variants of the Android platform. This fragmentation adds the dimension of device diversity when all your devices cannot be secured to a reasonable degree.

Broad, flexible BYOD program support – Device diversity is a huge factor in your approach and strategy. After all, Bring Your Own Device (BYOD) does not stand for *Bring Your Own IT-Approved Device* – that kind of defeats the spirit of a BYOD program. While a device certification program and process can provide some structure, a completely wide-open BYOD program will need some help on the technology front to maintain at least minimal data security.

Dual persona is the administration of two independent user environments to separate the "work" from "personal" data and experience on a mobile device.

Dual persona – This is where the debate diverges from a pure security discussion to one of functionality and desire to support a flexible BYOD program. For many organizations, there is no need or policy for robust DLP controls. They simply want to leave the user's personal data alone, but still be able to control corporate data. Once some thought is applied to your goals, dual persona may be the right solution for your organization. Essentially, dual persona is the administration of two independent user environments to separate the "work" from "personal" data and experience on a mobile device.

Other considerations – Solutions do not come without a price. Ensure your BYOD program will scale, maintain resilience, and stay within your cost boundaries. You need to factor in the user experience and make sure that you implement something that will be accepted and adopted by your users. You are living in a democracy now, not in an IT autocracy like the old days.

Choose your approach

Now that you have quantified your goals, let's look at the approaches that are available.

Container – The term "container" seems to be the most common term used to describe solutions that provide a separate work application and data area. The term "sandbox" is also often used. You may also hear "dual persona" used to describe this type of solution, but dual persona should be viewed as a goal rather than a solution (i.e., implement a container solution to achieve a dual persona).

Think of this approach as a completely separated and "sandboxed" area where certain activities occur and where the movement of data is limited to within the sandbox. Because all work activity is performed in this sandbox, the user will not be able to use the native email client, but instead will have to use the email, calendar and contacts functionality that is provided by the software inside the container. This can lead to some user dissatisfaction, but if implemented properly, can provide a seamless user experience. It is important to help your user base understand the importance the solution provides to the organization in meeting its data security goals.

Stripping – A solution that intercepts the email stream, strips out relevant content (i.e., attachments, text, etc.) and makes it available for viewing and/or manipulation in a separate application where the flow of the data can be controlled. For email, the user interacts with the native client until there is something that they need to access that has been removed (stripped) from the email stream. The removed content may be stored on the server that performed the "stripping" or on the mobile endpoint modified to open it only in a secure application.

With a stripping solution, the user experience can be disjointed. The user would receive an email with no text and no attachments – many solutions do not strip the text for this reason – and would be required to launch another application to securely access the text and attachments.

Virtualization – Specifically, what is being referred to here is the technology where a piece of software, referred to as a "hypervisor," implements a "virtual machine" in software on the mobile device (not on a remote server). In this type of solution the virtual device would be under the full control and management of the enterprise. All corporate applications and data would reside within the virtual machine on the mobile device, and the movement of data between the virtual and physical device would be tightly controlled. This is fundamentally the same as Virtual Desktop Infrastructure (VDI) for PCs and laptops, and comes with many of the same deployment and management challenges.

If your organization is focused on stopping an authorized user from propagating confidential data from a mobile device, either a container solution, virtualization, or email attachment stripping can be quite effective.

The technology holds some promise given that all functions of the device hardware and software have the potential of being virtualized and controlled, right down to the network connectivity and hardware functions. For example, the SIM could be virtualized and changed virtually when moving between networks (carriers would not like this). In reality, until mobile devices support virtualization within the hardware, similar to Intel VT and AMD-V on PCs, mass adoption is a ways off, especially on iOS.

None of the above – After the dust settles, this may be where many companies will land. If you are not in healthcare or financial services, do not have PCI or HIPAA regulatory requirements, or determined your specific mobile security needs and have implemented a sensible device and application management strategy, the additional cost and complexity placed on your users and IT may not be justified.

Select based on priorities

Now let's map it all based on your priorities.

Priority – insider threat: If your organization is focused on stopping an authorized user from propagating confidential data from a mobile device, either a container solution, virtualization, or email attachment stripping can be quite effective. They can all secure the text and the attachments, but offer fundamentally different experiences in the process, as described above. (In the case of stripping, be careful to select a product that provides both text and attachment stripping.) If there is no flexibility or tolerance for the leaking of any data from email, the container solution has some advantages by providing an improved user experience, and is somewhat less complex to configure and manage. Theoretically, virtualization would be well suited to the insider threat, but presents implementation and management challenges.

Priority – outsider threat: The outside threat is covered quite well if you take a responsible approach to the devices you allow to connect to the email system. If you use your MDM solution (assuming you have one) to restrict connections to only trusted devices that support a passcode policy, encryption and can be remotely wiped, the data that can be leaked and the related damage caused by a stolen or lost device is limited, if not zero. You can spare yourself the extra cost and complexity of DLP solutions if your priority is the outsider threat. Plugging the mobile data leak hole is generally only effective if you have the other holes plugged as well.

A container solution that provides a secure area for corporate data to reside on the unsecured device is an alternative to upgrading uncertified or unsuitable devices that users bring to the program.

Priority – BYOD program support: A prudent step in implementing a BYOD program is to have a device certification process and create a list of allowed devices that can provide a basic level of security. If you have implemented one, you will quickly realize that there is a great variance in the level of support for critical security features across the various Android variants. In a perfect world, BYOD would mean exactly that and accommodate a wide variety of devices.

A container solution that provides a secure area for corporate data to reside on the unsecured device is an alternative to upgrading uncertified or unsuitable devices that users bring to the program. Stripping solutions can offer a similar benefit, provided they support and are configured to strip and secure email text and attachments. Virtualization would not help support a broad BYOD device profile given the limited number of devices that could support running a hypervisor.

Priority – dual persona: Another compelling driver to implement a container or attachment stripping solution is not purely security related. As consumer devices proliferate in the enterprise, it is becoming unavoidable that corporate and personal data will comingle in spite of of efforts to prevent it. A move to a kinder, gentler approach in dealing with corporate data on these devices is also a key driver.

Rather than just telling users that their device will be fully wiped when it is lost, stolen or they leave the company, they can be given the choice to use a container or stripping solution. This provides the ability to confidently wipe corporate data only and not affect the personal data the user may have placed on the device. The container approach fulfills this goal most effectively and, in a carrot and stick approach, it may be the best carrot in the bunch. Users are directed to their "work" persona, and are happy to do so knowing that IT will leave their personal data alone.

The stripping approach is not as well suited to achieving a dual persona goal because there is no clean separation of work and personal data given that the native email client is still in use for personal and corporate activities.

Virtualization holds great promise here as well, but is so limited in device support that it is not a practical alternative at this point for BYOD.

Look before you leap

In summary, look before you leap. Understand your goals, understand your users and understand the available technologies and their impact on your environment and users. More importantly, get educated before the vendor pitch. As you interact with vendors and trials of their solutions, look for solutions that will adapt to the rapidly changing mobile landscape and reevaluate your goals often.

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle