WHITEPAPER

PREVENT DATA LEAKAGE AND KEEP BUSINESS USERS HAPPY

Finding the right mobile device containerization solution for your business

BlackBerry

iOS

FINDING THE RIGHT MOBILE DEVICE CONTAINERIZATION SOLUTION FOR YOUR BUSINESS

Contents

Mobile device containerization has emerged as a mandatory means of preventing sensitive information from being attacked or leaked outside the business or organization, as well as a tool for providing business users with the ability to effectively and securely utilize a single mobile device for both work and personal communications and computing activities. IT administrators are also eying the data segregation capabilities of containerization as a way to rein in security and management chaos created by the Bring Your Own Device (BYOD) movement. All of these factors, along with rising pressure on IT departments to expand and accelerate workforce mobilization within their businesses and organizations, are fueling urgency around mobile device containerization adoption.

Mobile device containerization technologies, however, come in multiple shapes and sizes, each presenting subtle or sometimes-significant variations in the way they manage and secure on-device work spaces, which can dramatically impact the effectiveness of an overall Enterprise Mobility Management (EMM) architecture. The guiding principle for IT departments looking to exploit the benefits of mobile device containerization is to select solutions that simultaneously provide effective risk management, further business productivity and preserve a consistent and attractive user experience.

Introduction

of all U.S. enterprises cite malware as a top mobile security threat

A 2013 IDC survey on mobile security

Corporations and organizations of all sizes are being infiltrated by an increasing number and variety of employee-owned mobile devices, as the BYOD movement continues to gain momentum. Predictions from analysts and industry pundits vary, but nearly all enterprise mobility experts estimate that a majority of businesses worldwide already support some flavor of BYOD policy — with BYOD acceptance projected to increase over the next few years. Accordingly, vulnerability to data leakage and malware attacks due to the co-mingling of corporate and personal data on mobile devices, both corporate-issued and employee-owned, will create an even greater security threat than currently exists. And things are only going to get worse, as businesses and organizations expand and accelerate efforts to mobilize their workforces by extending mobile access to sensitive corporate information to a greater number of users and by making more and more of their core business processes accessible to mobile devices.

Simple productivity applications, such as email, calendar and file sharing, currently make up the majority of work-oriented applications running on employee smartphones and tablets. But as business units continue to realize productivity advances through the empowerment of workers with anytime, any-location computing and communications capabilities, pressure will mount on IT departments to extend mobile access to core enterprise applications, such as CRM, ERP and sales-force automation, as well as data assets unique to industry segments, such as healthcare and financial services. The combination of more mobile workers, more mobile devices and the mobilization of more business-critical work-flow, applications and data has created significant urgency for IT departments to adopt new security technologies that segregate work and personal information without hampering productivity or compromising the user experience.

Containerization, by any other name...

Application wrappers, containers, hypervisors, sandboxes, work spaces – oh, my. As is the case with most technologies, containerization defies a consensus definition – or nomenclature. Vendors, analysts and technologists differ significantly in how they classify mobile technologies that allow for the partitioning of devices into virtual spaces or containers. Some sources, for example view application wrapping and containerization as closely related, with app wrapping defined as a component of the containerization process. Others go out of their way to classify the two approaches to mobile security as separated by degrees of granularity, with app wrapping functioning at the individual application level and containerization referring to a work space that could house multiple applications. And still other sources draw categorical distinctions between hypervisors and containers, with both types of solutions falling under the general category of dual persona technology.

With so much name-swapping going on, it's sometimes difficult to get a handle on containerization without a program. The best approach is to not get hung up on labeling. A container, by any name, is defined by function: protecting corporate-owned information from leaking outside the business or being compromised or stolen through a mobile device-enabled backdoor. What's vital to making an informed decision about this critical security component is understanding how a container -- application wrapper, hypervisor, sandbox, etc. -- accomplishes that function.

△ Back to the Contents

Mobile device containerization provides a potentially efficient solution for one of the thorniest issues facing IT departments worldwide: vulnerability to attacks on sensitive business data or the leakage of that information through mobile devices that are used by employees for both work and personal computing and communications activities. Mobile device containers are designed to manage the risks associated with intermingling work and personal information on mobile devices, which may not have been designed with security in mind. By deploying technology that enables IT administrators to segment a mobile device into virtual compartments, which can be managed and secured independently, businesses can essentially encase work-related data in a protective envelope, where it is no longer as susceptible to leaking into users' personal spaces or being infiltrated through malware.

Leakage Threats

While slippery is an adjective oft associated with eels, at-large criminals and other elusive creatures, the descriptor is also applicable to corporate data, which has a way of wiggling its way outside the oversight of IT. Mobile devices, especially those that contain a mixture of work-related and personal data, offer one of the best escape routes for sensitive information, as well as an access path into the corporate network for malware attacks and other intrusions.

In many instances, sensitive work data exits a mobile device, either accidentally or intentionally, through an unprotected communications channel, such as social networking applications, web browsing, webmail, instant messaging or other untrusted personal applications. An external storage device, such as a USB memory stick or microSD data storage card, is another potential path for corporate data leakage or intentional exfiltration.

Without some sort of partition that provides a leak-resistant boundary between work data and personal data directly connected to these consumer-oriented channels, information is susceptible to exiting the network through seemingly innocuous mechanisms, such as file attachment or transfer or a simple cut and paste operation. On the malicious side, work-related data or information on the device or corporate network can be accessed by a rogue application the user may have downloaded from the Internet or even a commercial application store.

The following examples represent typical data leakage scenarios:

- Bob is away from the office when he receives an email on his tablet containing an attached spreadsheet with sensitive corporate information. To edit the attachment, Bob forwards the message to an Internet-based email account and copies the attachment to his home PC. Alternatively, Bob copies the work file to a USB device and then transfers to his PC.

- Bob is on the road and is on a tight deadline to deliver a file containing customer data to a contractor. Instead of sending the document through a secure channel, Bob instead delivers the file using P2P file transfer.

- Alice is frustrated over the marketing team-imposed procedural hurdles she needs to clear to promote a soon-to-be-released product. To circumvent these roadblocks, Alice uploads an unapproved product picture to a Web site that is accessible to the company's competitors.

- A budding epicurean, Alice downloads a restaurant guide application to a tablet she uses at work. The application, which is actually malware, scans her corporate intranet via the smartphone VPN for sensitive servers to identify in an attack. It's also reading Alice's corporate email, in search of key words that identify messages with potentially sensitive information, which can be flagged and emailed to an overseas server.

- Disenchanted with company leadership, Bob and Alice submit their resignations in preparation of starting up a competitive business. Before leaving corporate headquarters, Bob downloads critical intellectual property from a Sharepoint server, storing it on a removable Flash drive.

Properly deployed, mobile device containerization offers benefits in addition to data leakage prevention. For starters, containerization technology is a pivotal enabler of a shift in enterprise mobility management from device focused to data and application focused. Containerization brings a new dimension to enterprise management, allowing IT to focus on protecting and managing applications and content. Mobile device containerization could also assist IT administrators in overcoming the objections of end users to submitting their personal devices to IT oversight. End-user tendency to shy away from IT creates a breeding ground for data leakage, as unmanaged employee-owned smartphones, tablets and even laptops end up loaded with corporate data and applications that sit next to consumer-based social networking, messaging, file sharing and other Internet-based data leakage channels.

△ Back to the Contents

IT departments are also enthusiastic about container technology as a mechanism for avoiding the violation of liability and compliance rules, which tend to vary from country to country. An unattractive byproduct of BYOD adoption is the increased possibility that a well-meaning IT manager will end up in legal hot water after deleting or corrupting personal data on an employee-owned device. Technology that allows IT to manage only work-related data may also mean fewer irate trouble calls – possibly from the CEO – and the avoidance of getting scratched by still-thorny privacy issues associated with BYOD.

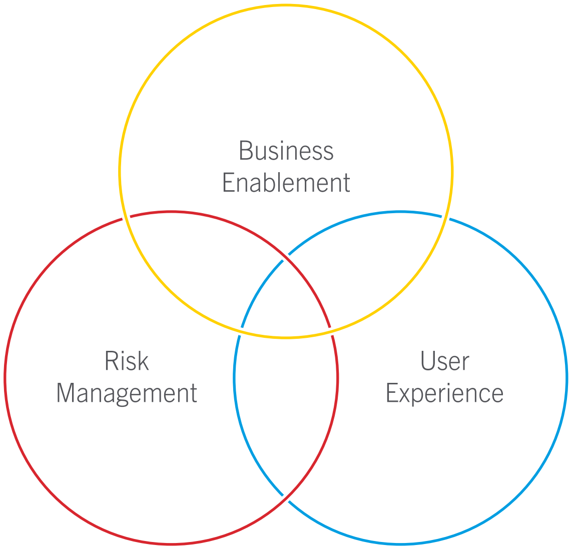
The bottom-line benefit of containerization, however, is its ability to assist IT administrators in accomplishing a fundamental business goal: enabling workers to safely and securely conduct business from any location or any device without imposing usability obstacles. But there are multiple approaches to mobile device containerization and great care should be exercised in the selection of a containerization approach and vendor. All utilize different technologies and methodologies and each approach must be evaluated on its ability to harmonize three distinct and sometimes opposing objectives of enterprise mobility – business enablement, risk management and user experience.

Meeting Enterprise Mobility Objectives

An effective containerization strategy, as is the case with all elements of an EMM solution, will satisfy the requirements of multiple corporate constituencies: management, the IT department and end users. Each of these groups is driven by different objectives and values – business enablement, risk management and user experience, respectively. The right approach to containerization is the one that best satisfies each of these objectives, with little or no compromise in productivity, security or user satisfaction.

Business Enablement

Business enablement is the value driver for mobility in the enterprise. A beneficial byproduct of the consumerization of IT, which helped to put mobile devices into the hands of large numbers of workers, was the realization by enterprises and organizations that business-user productivity surges when employees are empowered to do their jobs outside of traditional business settings. With utility-based applications, such as email, calendar and file sharing and synchronization driving the first wave of productivity improvements, business units are now pushing for the mobilization of core business processes. Protecting increasingly sensitive behind-the-firewall assets from attacks or leakage outside the organization through mobile devices is a front-line objective of mobile device containerization. Protecting that exposed data, however, must be done in a cost-effective manner. Other important attributes of a business-advancing container approach are the ability to scale to meet expected growth, as well as flexible and comprehensive management capabilities.



The optimal container approach best balances business enablement, risk management and user experience

Risk Management

Protecting the enterprise is the core objective of containerization, as well as a potential roadblock in the delivery path of a high-quality user experience. Accordingly, mobile device containerization must impose resilient and flexible security without impinging upon usability or workflow. Container technology must construct a wall around vital enterprise assets, including intellectual property (IP) and regulated data, such as customer/patient information, but one that is easily surmounted by authorized users and capable of supporting the native look and feel of the device. Intellectual property is the biggest strategic asset at risk for most businesses. Though losses associated with the theft of IP are difficult to quantify, the competitive impact can be calamitous. The security objectives of containerization also include ensuring regulatory compliance and protecting the privacy of employees. An additional objective is preventing work data from leaking through personal channels by way of cut and paste functions, file transfer or email forwarding.

User Experience

Providing an optimal user experience is the lynchpin of any containerization strategy. A container solution offering ironclad security, impressive total cost of ownership (TCO) credentials and mobile access to core business processes and productivity tools will be an abject failure if it also imposes too many restrictions and usability hurdles to capture employee buy in. With so many application and device options available from the consumer realm, employees will not accept solutions that do not meet their needs or impinge upon their ability to perform their jobs. It's imperative that mobile device containers support a variety of devices and deliver a work space environment capable of hosting applications that are easy to use without diminishing performance or productivity.

IT departments deploying containerization technology should strive for the following user experience milestones:

- Support for a variety of device types
- Consistent and native "look and feel" across work and personal spaces
- Efficient user interface designed for multitasking and productivity
- Uncompromised personal space experience
- Complete privacy and unfettered use of personal space

The least-favorable container approaches will impose significant trade-offs between these enterprise mobility values and objectives. An optimal approach, on the other hand, will score high marks across all three objectives.

△ Back to the Contents

Approaches to Containerization

While all containerization technologies share the same objective – securing corporate applications and data on mobile devices – they vary significantly in the way they achieve that objective. What follows is a sampling of four current approaches to mobile device containerization.

Virtual

There are two container types that fall into the virtualization category: Mobile Virtual Desktop Infrastructure (VDI) and Mobile OS Virtualization.

Mobile VDI is essentially a mobile version of traditional server-hosted desktop virtualization, also known as a "thin client," which has a long history in the enterprise. This virtual container approach protects data chiefly by executing applications and storing content in a behind-the-firewall centralized location, rather than the device. Mobile VDI containers also come in a hybrid model, where content is stored both offline and online.

Mobile OS virtualization containers, implemented using hypervisors, create virtual machines that can be managed essentially as separate operating systems. These containers come in two flavors, Type 1 and Type 2. Type 1 containers run at the device, or hardware layer, and are embedded into the smartphone or tablet. Type 2 containers run on top of the OS and are inherently less secure than Type 1, but not as difficult to deploy.

Mobile VDI-based containers present several challenges when measured against the three enterprise objectives – business enablement, risk management and usability. This approach's best attribute is security, as all or nearly all corporate data resides on a server located in the cloud or in the corporate network. Still, a thin client running on top of a compromised OS is vulnerable to screen scraping, particularly if there are no security assurances for the integrity of the host operating system. Mobile VDI-based containers score low marks for business enablement and usability, primarily due to their dependence on a persistent, high-bandwidth mobile connection, which still presents a problem in many work environments. This approach also suffers from limited feature sets and potentially high application development costs.

Mobile OS virtualization containers, similarly to VDI-based approaches, provide a secure environment by thoroughly isolating corporate data into dedicated workspaces. The hypervisor technology, however, is far from optimal on the usability front. Usability issues related to this container type include sluggish performance, short battery life and the requirement for users to switch between completely independent device environments. The need to constantly switch between separate work and personal calendars to manage appointments, for example, can be a cumbersome process for many users. Furthermore, the most worrisome aspect of OS virtualization is the high cost of ownership due to the inherent complexity of virtualization technology, which is not well suited for resource-constrained mobile devices.

Application-Specific

Application-specific containers are distinguished by the requirement to custom-develop applications for the workspace and are also known as bolt-on Software Development Kit (SDK) containers. This container approach requires utilization of APIs in the applications to protect against the data leak issues already discussed.

One of the first entries in the containerization space, application-specific containers have largely fallen out of favor. This brand of containerization suffers from across-the-board shortcomings connected with the requirement to custom build applications for secure environments. Ironically, from a security perspective, bolt-on SDKs can actually create new exposures to attacks. In addition to introducing application development costs, application-specific containers have not been widely embraced by developers, who cite complexity and a lack of features as drawbacks. Moreover, application-specific containers impose a non-native user experience that leads to employee dissatisfaction.

Container Check List

Since knowledge is power, familiarity with the following facts will put IT managers in the strongest position to adopt a containerization strategy that best meets their needs:

More than MDM: A mobile device management solution will not solve work-to-personal data leak issues. MDMs can only manage the publically available APIs of mobile device platforms and iOS and nearly all Android OS versions do not currently offer integrated containers.

Beyond email: While corporate email and calendars were the early killer apps for mobile devices, the modern mobilized workforce is looking to move up the app stack. Going forward, the mobilization of strategic business processes will be a key objective of most businesses. Consequently, IT departments must adopt a container that is cost effective, easy to use and provides a feature-rich environment for app developers.

Users know usability: What the IT team thinks of a container's user experience often differs from feedback received from the field. IT managers need to test any container solution with a sampling of business users to get a realistic sense of the technology's ability to protect corporate data without undermining the end-user experience.

TCO tunnel vision: While total cost of ownership is an obviously important selection criterion, it shouldn't be the overriding factor in settling on a mobile device containerization solution. If it does not drive corporate productivity or employee acceptance, even a solution pulled out of the bargain bin will come with huge opportunity costs in the long term.

Means of production: It's all about employee productivity. Make sure any container solution ships with a stable (or integrated suite) of productivity tools and applications that can deliver near-native look and feel capabilities.

Integrated solution: Any containerization approach needs to be part of a comprehensive EMM solution and support multiple device OS platforms. Avoid solutions that require a third-party management tool or are limited to a single platform or a few device types.

Application-Neutral

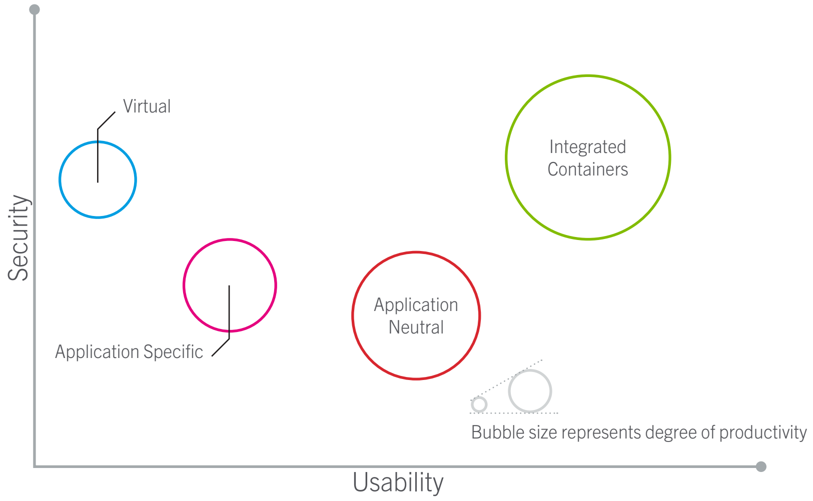
Application-neutral containers utilize application wrapping, a process that involves securing an application by encasing it with security capabilities that reside outside the platform's native application code and that can be manipulated by a management application. Application-neutral containers do not require recoding of the application and the application wrapping process can be accomplished in a short period of time.

With the introduction of application-neutral containers, IT departments gained access to data leakage prevention solutions capable of bringing harmony to the enterprise's simultaneous need for security, usability and productivity. The wrapping of an application's binary is an effective means of plugging up potential data leakage channels and segregating work and personal spaces on the device. Application development is also streamlined, as enterprise developers can leverage native SDKs. In terms of usability, an application-neutral approach provides a native-like look and feel to applications, as well as a consistent user experience across work and personal spaces.

△ Back to the Contents

Integrated Containers

Resting at the top of the mobile device containerization food chain is the integrated container, which is characterized by deep integration into the mobile device OS. This approach provides excellent security, significantly reducing vulnerabilities associated with containerization types that are not embedded into the OS. An integrated container also simultaneously offers greater security, flexibility and user transparency. The holistic design strategy associated with embedded containers optimizes security and productivity by utilizing bundled business productivity tools and apps, which increase work-flow efficiencies. In addition, integrated containers excel in the areas of security and usability due to the container supplier's intimate knowledge of the underlying OS, which can be leveraged throughout the design process.



A comparison showing the relative positioning of containerization technologies using security, usability and productivity evaluation criteria

Conclusion

Enterprises and organizations worldwide are seizing upon the productivity benefits associated with workforce mobilization. As businesses expand and accelerate these efforts, including the mobilization of core business processes, vulnerability to data leakage and attacks on corporate information assets intensifies. The co-mingling of work-related and personal data on mobile devices, both employee-owned and corporate-issued, is creating gaping security holes.

To plug those holes, many enterprises are deploying or evaluating mobile device containerization solutions. Containers, however, come in multiple shapes and sizes and IT administrators must select containerization solutions that best meet their particular requirements. For most businesses and organizations, the optimal mobile device containerization approach is the one best able to advance productivity and reduce security risks, without compromising user experience.

BlackBerry, a global leader in mobile communications, provides containerization solutions that deliver exceptional risk management and usability for devices running BlackBerry, iOS and Android operating systems. All BlackBerry container solutions can be administered from a single management console.

BlackBerry®

△ Back to the Contents