Bring Your Own Device (BYOD)—Key Trends and Considerations

Introduction and Research Overview

Introduction and Overview

This Frost & Sullivan insight presents an overview of the key trends in the U.S. bring your own device (BYOD) market. This insight will highlight the key success factors for BYOD vendors in the United States, and provide strategic recommendations for organizations that want to implement a BYOD solution.

Enterprise Mobility—Managing BYOD

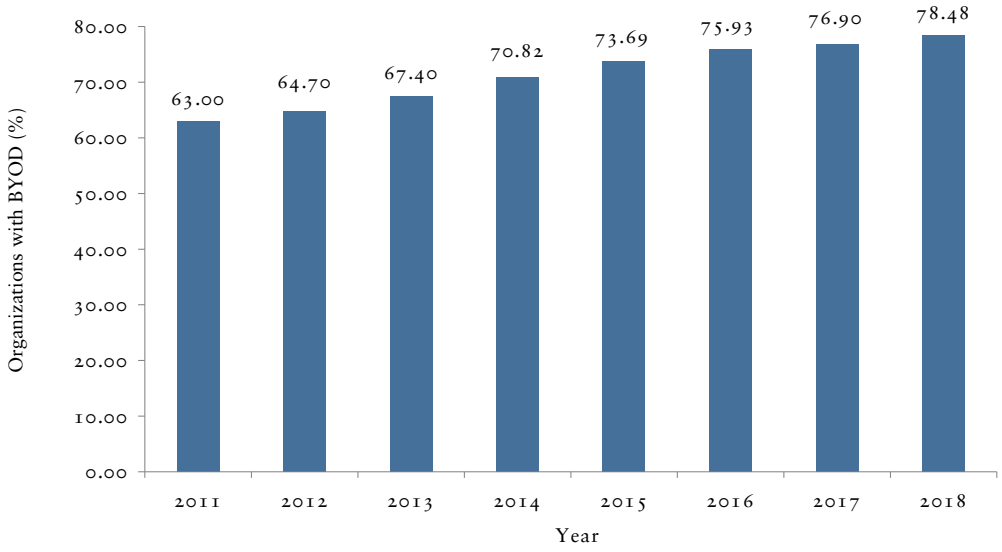
BYOD—Need; Importance; and Approaches

BYOD refers to the practice of allowing employees to use personally-owned mobile devices for accessing enterprise IT resources and data. The proliferation of BYOD points to a future in which enterprise information technology (IT) departments (also referred to as "enterprise IT" or simply as "IT" in this document) will have to manage a mix of corporate-owned and employee-owned mobile devices. More specifically, enterprise IT will be required to manage the workspace on devices and personal computers (PCs), rather than the entire device or PC. As the ecosystem becomes increasingly complex, it will get incredibly difficult for IT departments to manage all these deployments with traditional technologies, policies, and processes. For example, on a personal device that accesses privileged corporate data and applications, the organization will generally have less control over security. However, mandating restrictive IT policies for personal devices (such as lock, wipe, and geo-fencing) can lead to employee dissatisfaction and reduced productivity. Such policies can, in fact, also make it harder to attract and retain talent. Thus, it is prudent to implement solutions that can efficiently manage the trend of BYOD in a controlled, secure, and scalable manner. Providing corporate access to a broad base of employees on their personal devices can be more economical for a company, as the employee (and not the organization) generally pays for the device and data plan. Moreover, restricting access, without a workable alternative to corporate mobile users, creates new risks including competitive disadvantage, employee dissatisfaction, and work inefficiencies. Clearly, BYOD has become a catalyst to encourage IT to prioritize an employee's s efficiency without compromising security, which requires a new way of thinking about enterprise mobility.

Exhibit 1 shows the percent of organizations with BYOD activity in the United States from 2011 to 2018.

EXHIBIT 1

BYOD—Key Trends and Considerations: Percent of Organizations with BYOD Activity, United States, 2011-2018

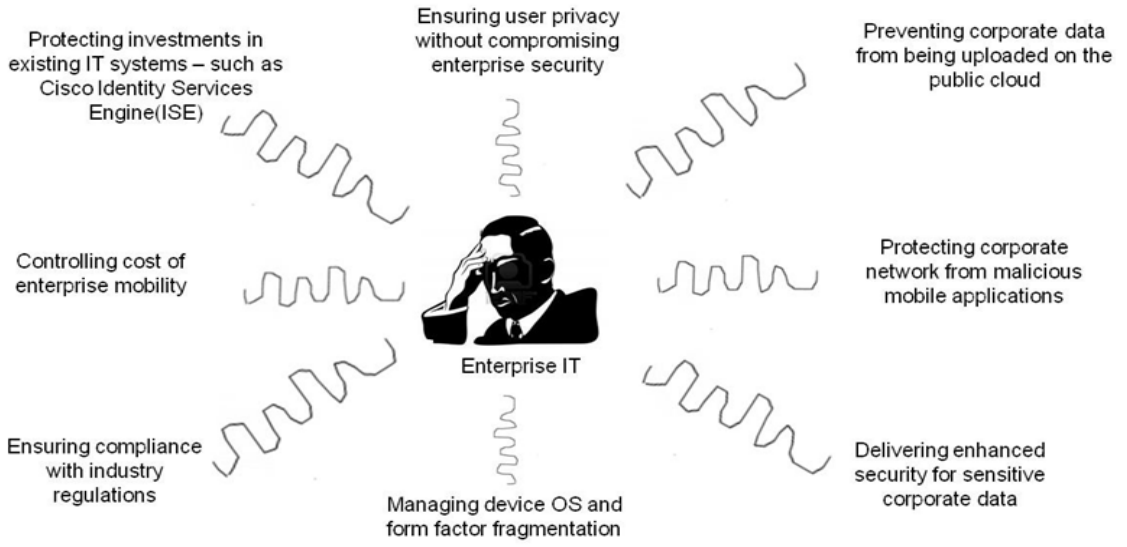


Note: All figures are rounded; the base year is 2012. Source: Frost & Sullivan

Exhibit 2 shows the top enterprise IT challenges for enterprise mobility management in the United States in 2013.

EXHIBIT 2

BYOD—Key Trends and Considerations: Top Enterprise IT Challenges for Enterprise Mobility Management, United States, 2013



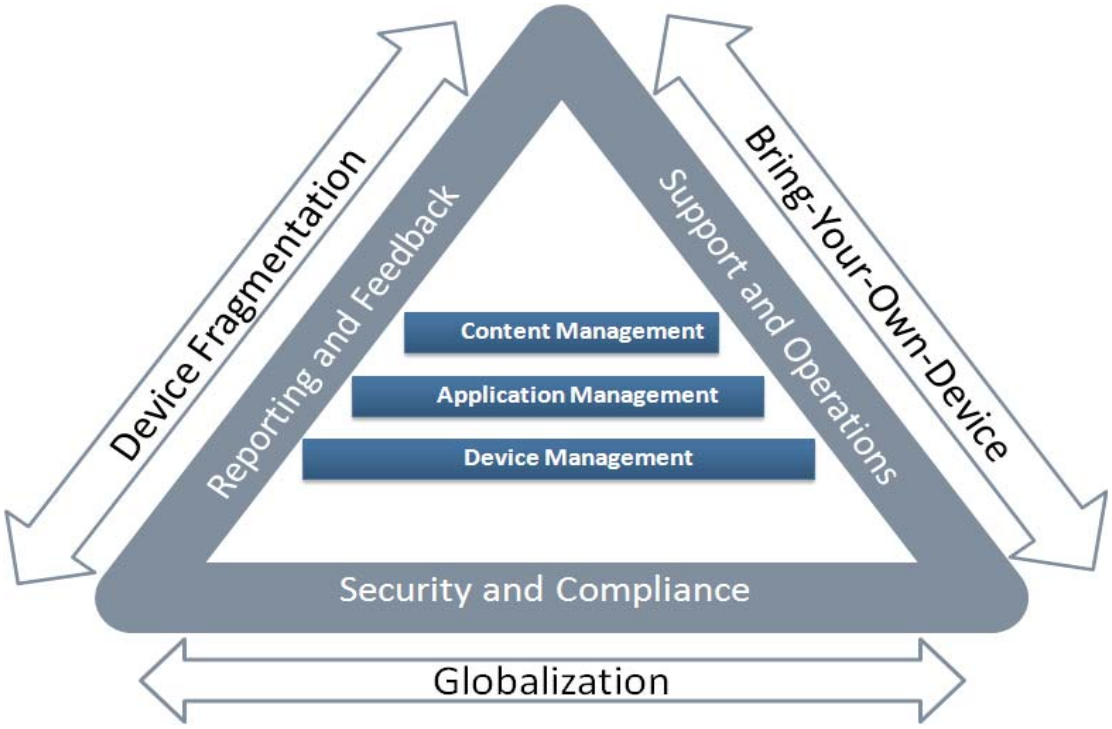
Source: Frost & Sullivan

It is extremely likely that more personal (or personally liable) mobile devices will access enterprise IT resources than corporate owned (or corporate liable) devices within the next few years in the United States. However, BYOD is just one component of the broad enterprise mobility equation. According to Frost & Sullivan, enterprise mobility management is about enabling, securing, monitoring, and supporting enterprise mobile users, devices, content and applications, while considering relevant parameters such as device fragmentation, globalization, and BYOD.

Exhibit 3 shows the key elements of enterprise mobility management in the United States in 2013.

EXHIBIT 3

BYOD—Key Trends and Considerations: Key Elements of Enterprise Mobility Management, United States, 2013



Source: Frost & Sullivan

Confusing Options

Extending the corporate IT environment to mobile devices helps improve worker productivity, improve supply chain operations, ensure faster and more efficient business operations, and facilitates real-time collaboration with customers, partners and suppliers. Frost & Sullivan firmly believes that organizations leveraging mobility to manage the shift to a "virtual enterprise" framework will see increased efficiencies and operational advantages in their respective industry verticals. Yet, determining the right solution to manage all aspects of enterprise mobility can be a challenge. Enterprise IT is expected to: 1) give access to corporate IT resources to authorized users on personal mobile devices; 2) ensure that corporate network, data, and applications are secure and are not misused or shared inappropriately; and 3) respect the users' privacy. There are various device-level and network-level technologies that can be used to manage BYOD programs, including:

- Mobile device management (MDM)—for centralized management and role-based administration of mobile devices in the enterprise.
- Container-based solutions—to deliver greater control over secure email and data communication in an organization.
- Type 1 and type 2 hypervisors—leverage virtual machines to provide secure enterprise domains on mobile devices.
- Wireless Access Point (WAP)—simple mechanism to offer controlled (or limited) access to network resources.
- Network access control (NAC)—primarily network-based solutions to define and implement policy-based access to enterprise I.T. resources.
- Dual persona—separation of mobile devices into personal and secure enterprise modes.
- Custom mobile applications—custom or customized third-party applications to enable secure communication and collaboration with remote workers on their mobile devices.

Organizations need to be totally clear on the end goal of their mobile business strategy; they need to clearly define the business objectives and impact of mobility before taking a closer look at specific BYOD management products. A thorough analysis of product capabilities, product deployment and support options, and total cost of ownership can help business organizations identify the right set of solutions that best meet their requirements. Evolving security, operational, and legal considerations also make it important to constantly evaluate how best to implement mobility in the enterprise. Solutions that don't infringe on employees' privacy yet can ensure that corporate applications (and corporate data) are secure and protected are more likely to be accepted by the corporate workforce.

Role and Importance of Containers

Effective BYOD implementations enable corporate IT to create, secure, manage, and monitor a virtual corporate "persona" on personal mobile devices. A protected corporate workspace—also loosely referred to as a "container"—allows access to enterprise IT resources from within this secure mode. Appropriate corporate policies are defined to control what the user can or cannot do within the container. Additionally, containers can be designed to not allow any potential malware that might exist on the personal side of the device to make way into the corporate persona (residing inside the container) on the same device. Most containers include a secure email application (or application interface), and may also include other mobile productivity tools such as a secure browser, and document viewer and editor.

Leading providers of device containers also provide software development kits (SDKs), and "wrapper" codes to allow organizations to use in-house as well as commonly available third-party mobile applications for various organizational communication and collaboration requirements. In certain cases, a wrapper might prove to be a better approach than a SDK, since it can be difficult for software vendors to re-compile their apps with SDKs. On the other hand, certain types of wrappers may not be approved for use in certain environments (such as Apple's iOS), which makes the SDK approach the only option. Even though there could be some limitations in terms of granularity of information that could be obtained via certain lightweight wrapper implementations (such as lack of insight into aspects as telecom usage, data usage, and how often are users using certain menu options), all leading BYOD solution vendors consider wrappers as an effective long-term strategy for increasing their market reach.

It should be noted that the term "container" is very broad and used quite loosely in the industry. Containers are means to an end, "end" being to provide proper features to manage BYOD—including authorization, authentication, configuration, encryption, tunneling, DLP controls, analytics, and selective wipe.

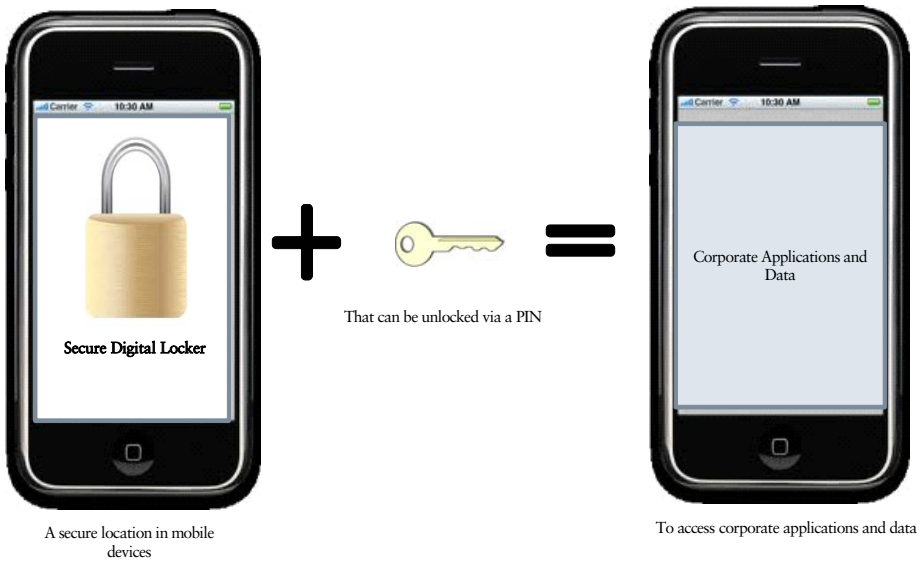
Types of Containers

Containers can be monolithic, which means all enterprise applications are wrapped inside a protective application (the container). There can also be multiple app-level connected containers that exist on a mobile device where each application is secured and each can share data and policy only with other secure apps. While there are pros and cons of a "captive" (every enterprise app is in a single container) versus an "integrated" (multiple separate app experience on the device) user experiences for BYOD, it will ultimately come down to the preference of the users. What is clear, however, is that containers have become critical to managing a successful BYOD program. This is more evident in regulated industries such as Healthcare and Financial Services, as well as for senior-level executive across multiple industry segments. "Securing the Mobile Experience with Containers", a strategic analysis by Michael Suby of Stratecast (a division of Frost & Sullivan), presents additional details on the types, importance, and future of mobile containers.

Exhibit 4 shows a simplistic representation of a container on a mobile device in the United States in 2013.

EXHIBIT 4

BYOD—Key Trends and Considerations: A Simplistic Representation of a Container on a Mobile Device, United States, 2013



Source: Frost & Sullivan

The Web vs. the App Debate

Advancement in web technologies can have serious implications for enterprise mobility and BYOD programs. It is generally simpler to maintain, upgrade, and distribute simple web apps. Web apps can be wrapped within a native app container as well (which then appear as native apps to the user for all practical purposes). A well-designed web app that has no local storage can help protect against the threat of mobile malware or a lost/stolen device with data left on it. However, from a user experience perspective, a native app might be a better option. Any long-term corporate BYOD policy has to consider the possible emergence of mobile web-driven enterprise mobility service architecture, and provide solutions to enable the enterprise IT to manage the user and the device behavior in a HTML 5 (or other) web technologies driven information flow. Every IT department needs to be prepared for a mixed application environment consisting of native, web, and hybrid applications. This is where having appropriate network-level control (versus having only device-level protection) to ensure that all network traffic is monitored and managed in a secure manner could prove to be valuable.

Security Concerns—Enterprise Data Protection

Employees feel more empowered with their smartphones and Tablets and are likely to find ways to make mobile work for them, including using third-party apps and cloud services to get their work done. Well-intentioned employee behavior (such as forwarding email or storing a document in the cloud), malware, lost devices, and compromised devices can all pose significant risks to enterprise security. Simple technologies such as copy-paste or even speech-to-text programs could result in inappropriate data usage. Today's connected workforce believes in the "everything is public unless stated otherwise" paradigm, while traditional corporate IT has worked along the lines of the "everything is private unless stated otherwise" rule. Protection of data in transmission, and protection of data that is stored on personal (or on corporate-owned) mobile devices are both extremely important for organizations. Proper BYOD tools, along with employee training programs should be used to help enterprise IT guide, educate, and help their mobile workforce. This can help to reduce the "wild west" of applications and cloud services that can exist in an organization that chooses to ignore the trend of BYOD.

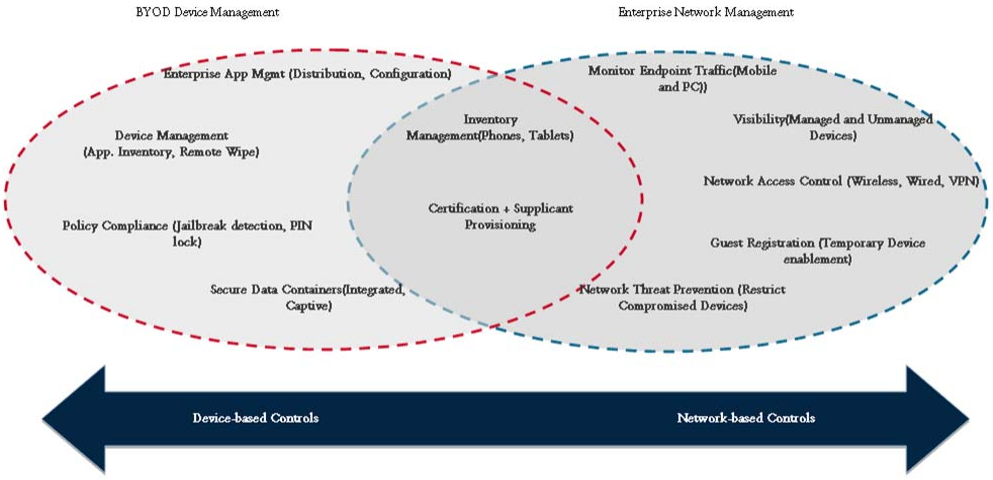
Security Concerns—Enterprise Network Protection

Implementing policy-based access to network resources is critical for corporate network security. The real issues of data loss could very well be server-targeted, since that is where the "big data" really resides. It could be argued that with MDM (or BYOD) implementations, there is a reasonable degree of security that is ensured on the mobile devices, or at the very minimum, the corporate side of the mobile device. However, malicious programs can still reside on the unprotected mobile device, and make their way into the enterprise environment. Similarly, devices that don't have the latest software or firmware versions may try to access the corporate IT environment, and should be first updated before access is provided. Finally, there is always the risk of unmanaged and unprotected personally-liable device attempting to access corporate IT resources. As any experienced security professional knows, a tiered security architecture that focuses on protecting both the device as well as the network side of a corporate IT network is an extremely effective approach for network security. Network-side incident prevention and remediation solutions don't face the constraints of a limited power supply (as is the case with device-side protection tools) and can—at a very minimum—protect the network (and the data that resides in the network). Frost & Sullivan firmly believes that adopting a device-centric as well as a network-centric view of security for BYOD is critical to deliver complete peace of mind to enterprise IT.

Exhibit 5 shows the role and importance of device-based and network-based security controls for enterprise mobility management in the United States in 2013.

EXHIBIT 5

BYOD—Key Trends and Considerations: Role and Importance of Device-based and Network-based Security Controls for Enterprise Mobility management, United States, 2013



Source: ForeScout Technologies Inc., Frost & Sullivan

Traditionally, IT security managers have installed network security, PC security, and data security solutions. The migration away from corporate-owned PCs to personally-owned endpoint devices does not remove the obligation to protect all three entities—the network, the device, and the data.

Legal Implications

Some top legal concerns with BYOD include:

- Ownership for intellectual property (IP) created on personal devices—does the employee own the IP, or does the organization own the IP?
- Ensuring user (and data) privacy—to what extent should the usage patterns be monitored?
- Loss of IP from personal mobile device—loss of company data, loss of customer data, and loss of IP created on personal devices: who is liable—employee or the organization?
- Defining appropriate processes for incident response and device remediation—can the organization take control of the personal mobile device to ensure compliance?
- Liability for possible device software (or hardware) issues when personal devices are used for corporate work—will that amount of snooping on personal mobile devices?
- Potential liability for lost personal data (such as photos, contacts, documents)—when an organizations ends up fully wiping a BYOD device.

Organizations have to ensure that their acceptable use policy (AUP) are well defined and are clearly understood by corporate users that want to use their personal devices in a corporate environment. Simply extending the existing AUP for corporate-owned mobile devices to personal devices is clearly not a very practical approach.

So what should the Corporate IT do?

BYOD—Important Considerations for Enterprises

The following are some important considerations for organizations that want to embrace a BYOD program.

- Mobility is an ally, a key business enabler, a strategic tool for competitive differentiation, and the future of enterprise communication. This point cannot be stressed enough. Organizations should, at the very minimum, deploy a pilot program to evaluate how to leverage the potential of BYOD. This can also help to understand the risks involved in BYOD, which, in turn, can help develop an effective BYOD policy. Forward thinking organizations will treat mobile as a core IT service and consider that mobility will span all aspects of IT infrastructure, technology processes, and service levels. Yet, in the short and the mid-term, IT should leverage the established IT infrastructure as much as possible to protect existing investments into the incumbent systems and platforms.

- BYOD, company-liable devices, cloud-based storage, and custom-built and third-party native and web apps are the key drivers of the current revolution in enterprise computing. In the long-term, it is not unreasonable to expect tablet-only, smartphone-only, or BYOD-only organizations in the United States. However, the mobile environment presents some unique challenges that go beyond just the technical aspects of BYOD. As discussed earlier, there are other implications of BYOD (such as legal, and human-resources related) that have to be considered when implementing a BYOD program. An effective BYOD policy can only be developed when different departments within the organization—including finance and accounting, legal, HR, and operations—collaborate to design the correct BYOD framework.

- The importance of proper training to users cannot be overstated. Successful organizations will have trained users on what is/is not safe to do on their mobile devices, and what the rules are. Also as part of BYOD policy, IT doesn't need to say "yes" to everything. It can create tiered policies based on job grades, OS types, apps, and other parameters. For example, an organization may choose to provide core business apps on the iOS platform, which limit BYOD access to only specific smartphone and tablet models.

- Corporate IT needs to take a long-term view of their mobility strategy. For example, organizations need to know how the traditional authentication and identity management approaches will evolve. New devices quickly make their way into the corporate environment in just a few days after their commercial release. BYOD vendors have to ensure that they are ready to help their customers manage any new mobility platform that comes into the corporate environment. Implementing readily-available BYOD (and MDM) platforms offered by well-qualified vendors that have the necessary resources to invest in product innovation is the right approach for any organization.

- Organizations may still struggle to ensure up-to-date device protection for BYOD devices. Focusing only on device-level protection may not be sufficient to provide complete protection against every possible security threat in BYOD. However, organizations usually always have a 100 percent control over their networks and should implement a dynamic policy-based control system that can enforce which mobile endpoints can connect to which IT resources. Cost considerations, type of access control desired by the organization, and extent of data protection mandated by law are some other factors that will eventually decide the security and compliance approach for organizations.

- BYOD will lead to increased request for device configuration and support. IT should ensure that users are able to use the existing helpdesk systems that support other connected endpoints (such as PCs) and enterprise apps. They also have to plan for the cost of increased requests, and should look to establish a tiered support model comprising of user self-service systems, as well as corporate helpdesk technologies and processes that require active participation of IT personnel.

- Even though BYOD means that organizations don't pay for devices, apps, or data, there are other costs that may be incurred for enabling BYOD services. These may include investments in infrastructure technologies that may need additional licensing, such as NAC, Identity Management, and VPN, as well as labor and support costs for these implementations. There is no "free lunch" with BYOD. A true ROI measurement for BYOD has to consider increase in employee productivity, increased revenues, impact of employee satisfaction, and potential for employee retention, as well as direct and indirect cost of BYOD implementation and management.

- Organizations should consider addressing the requirement of regulatory compliance in specific verticals. For example, in the healthcare vertical, the Health Insurance Portability and Accountability Act (HIPPA) compliance related to rules for protection of individually identifiable health information are applicable for encryption and protection of patient information on mobile devices. As organizations look to embrace a BYOD strategy, they need to ensure that the solutions they choose can deliver on various compliance-related requirements, particularly related to data encryption, remote data wipe, and possibly the need to ensure that business data is automatically wiped from personal devices after it has been disconnected from the network for a certain period of time.

- Lastly, organizations have to ensure that they don't simply end up making it difficult to access corporate IT resources for their employees. Properly designed identify federation solutions can help here, so can other related next-generation devices technologies including automated device authentication, biometrics, audio-visual recognition, location-based services, and other behavioral and contextual elements.

Enterprise Considerations for Selecting the Right Vendor – The Non-technical Side

Specialized MDM vendors, mobile operators, traditional device security services providers, identity management providers, niche container-based solution providers, and organizations with a hypervisor-based solution offer BYOD solutions. Technical capabilities alone may not be sufficient to help identify the "best" solution for BYOD. The following strategic parameters should also be considered at when evaluating MDM/BYOD vendors.

- Platform extensibility, modularity, and roadmap- BYOD enables employees to select their preferred device and infers that the organization will have the ability to support it. As enterprise requirements change and companies expand, their MDM solution should grow with them. At first, an enterprise may only be looking for base features such as remote lock and clear passcode. As the enterprise grows, application and content security may become more important. Also, enterprises should look for vendors that rapidly support devices as they are released.

- Security strategy—it is important to work with MDM/BYOD vendors that can provide security across multiple data types—email, email attachments, apps, content, web, etc.—for data at-rest and data in-motion. Security credentials—such as Federal Information Security Management Act of 2002(FISMA) compliance, Federal Risk and Authorization Management Program (FedRAMP) certification, Cloud Security Alliance (CSA) certification, and Service Organization Control (SOC) reports—are important to consider particularly for cloud-based BYOD solution providers. As discussed earlier, it is important to also evaluate different network monitoring, network protection, and policy implementation tools that could work in conjunction with BYOD platforms.

- Approach to identify management—in a BYOD environment, identify really determines the types of services delivered. Delivering single sign on (SSO) services for enterprise web and native applications on the smaller screen mobile devices is important to deliver a good user experience on the small-screen mobile device. Enterprise may or may not have a public key infrastructure (PKI). BYOD vendors should be able to work in either case, and provide an embedded certificate authority and ongoing engineering investment (and therefore a roadmap) around identity.

- Customer support capabilities—MDM vendors' investment in customer support systems is indicative of the vendors' long-term commitment to the enterprise mobility market. Any technical issues should be resolved immediately. This can also be specified in appropriate service-level agreements (SLAs) offered by BYOD vendors. It's also important to remember that customer support isn't just about the system itself. Training materials, knowledge portals and self service portals are integral pieces of customer support services as well.

- Pricing strategy- low cost solutions may not be the best, especially when the stakes are high in BYOD. Low prices can help BYOD vendors win new deals, however; vendors must have the ability to invest in scaling and enhancing the capabilities of their implementations. It is therefore prudent to consider vendors with a significant customer base, breadth of MDM capabilities, and large employee base dedicated to supporting BYOD. These types of characteristics validate the vendor's BYOD expertise.

- Preserving the user experience—the user experience should ideally never change with the security implementation in place. For example, the on-device client should not consume too many processing resources and slow down the device. Users should not be forced to remember multiple passwords for different services that they want to access and use on their mobile devices. The intuitive user interface should ideally be maintained for enterprise mobility deployments, which will actually help make the workforce more productive.

- Simplicity and platform flexibility—a well-designed solution should be easy to use for IT administrators as well as the end users. The platform also needs to be able to support varying use cases across business teams. For example, a MDM platform with true multi-tenancy allows executives to have different security settings and policies as compared to field employees.

- In-house versus licensed technology—MDM/BYOD vendors can license core portions of their product (such as application wrapping) from other vendors. In certain cases, the success of MDM/BYOD solution providers could depend upon the ability of technology providers to continue to innovate (since the technology itself needs to be upgraded frequently), which may not happen if the technology provider gets acquired or goes out of business. However, rarely does a MDM/BYOD vendor have enough resources to build everything AND be the best at everything. This is particularly true in enterprise security, where it could be better to rely on proven security experts to provide thoroughly tested and effective implementations.

- Ensure that the organization is always in control—the enterprise mobility strategy should ideally never be dictated (or limited) by the capabilities (or limitations) of the BYOD platform. The organization should have full control over the default system behavior and should be able to define and control how it manages its BYOD implementation. For example, while a BYOD solution provider may offer several options to address the issue of jail broken devices—including blocking and/or removing all or specific applications or profile types, and forcing a full device wipe or device check-in, it should be up to the organization whether it wants to remove specific resources or do a full device wipe.

A Few Other Key Success Factors for BYOD Vendors

Platform Architecture

Frost & Sullivan expects the enterprise segment to increasingly make long-term "strategic" decisions about the role of mobility in their IT programs. This will define the types of solutions, support, and customization capabilities that customers expect. Platform architecture, enterprise app strategy, and enterprise infrastructure strategy are the three important sets of capabilities for BYOD vendors.

Important elements include the following:

- Ability to integrate with existing enterprise IT applications and systems—including email programs, collaboration tools (such as Microsoft SharePoint), and certificate authority. The solution must also integrate with Active Directory (for policy) and potentially other identity and access management systems.
- Ability to scale vertically and horizontally—ability to support new seats from within the same application, and ability to support new corporate applications and services if required.
- Platform extensibility—ability to develop new platform capabilities. This is also critical to help support transformational business processes that help to make employees more efficient in their work. A cloud-based solution with the right security capabilities can help address some of these challenges.

Enterprise App Strategy

BYOD vendors have to provide appropriate tools to allow organizations to leverage in-house as well as third-party enterprise communication applications within their networks. BYOD vendors' enterprise app strategy should consider the following:

- Facilitating a collaborative enterprise app ecosystem—providing appropriate SDKs or wrapper solutions to third-party application providers to help them leverage BYOD platform services. BYOD vendors can consider strategic partnerships with leading enterprise application providers—starting with productivity and collaboration apps and extending to other application types in future—to offer a complete package of applications.
- Application distribution service—effective and scalable application distribution and application configuration capabilities are critical to ensure that all types of BYOD devices can be provisioned and managed easily. Change management for updates, and auto-selective-wipe for apps when user leaves or device is lost/stolen are also important features.
- Application security strategy—effective security for data at rest, and data in transmission is extremely important for the long-term success of corporate BYOD programs. Enterprises are increasingly demanding application-level data security versus having to broadly implement device-wide VPN control on devices.

Enterprise Infrastructure Strategy

Important capabilities include:

- Facilitating a collaborative IT infrastructure ecosystem—BYOD vendors can enhance the effectiveness and value of their implementations by working with established third-party solution providers in areas such as identity management, NAC, VPN providers, firewall provider, and others.
- Implement a short-term, as well as a long-term plan for infrastructure services—in the short term, identity, certificate management, VPN, and NAC capabilities are likely to be in high demand. In the long term, services such as Security Information and Event Management (SIEM), and data analytics will also see good traction (although Frost & Sullivan has observed strong enterprise interest for mobile SIEM and data analytics solutions).
- Adopt an open approach—realize that BYOD vendors will see custom demand for integrating with certain "preferred" vendors of enterprise IT solutions. The ability to implement key third-party infrastructure services as demanded by enterprise customers is important too. However, this cannot be done for each and every enterprise. BYOD vendors need to make judicious decisions on where they want to focus on and if a particular deal is large enough to provide customized integration services.

Conclusions

Many leading BYOD (and MDM) vendors offer no-commitment trial programs that can help enterprise IT evaluate the benefits of BYOD. Enterprises should always insist on a live evaluation of the product. While it is important to look at technical capabilities, that alone may not be sufficient to help select the optimum solution. Thus, various legal, operational, and economical aspects should also be evaluated to help design a successful BYOD strategy. At no point should the user experience be compromised, especially on personal mobile devices that are owned and paid for by individual users. Only then will the organization be able to fully realize the benefits of BYOD.