BEST PRACTICES IN BYOD

How Smart Enterprises Are Making It Work

Whitepaper

SERIOUS MOBILITY FOR SERIOUS BUSINESS

BlackBerry | ENTERPRISE

Best Practices in BYOD: How Smart Enterprises are Making it Work

In a recent report, research firm Ovum concludes that:

"It is clear that when it comes to planning and implementing a mobility strategy, there is no one-size-fits-all policy that suits all organizations – or even all roles within a particular organization. Ovum thinks that we will see the majority of firms adopt a mix of BYOD, CYOD [choose your own device], COPE [corporate owned, personal enabled] and COBO [corporate owned, business only] strategies, applying different rules to different teams and employees depending on their particular requirements, security profile, risk profile and the kind of apps and the type of data that they need access to. Having an EMM solution capable of supporting all scenarios simultaneously would therefore be advantageous to organizations implementing mixed corporate and personally owned device deployments."[2]

While most organizations continue to experiment with how much BYOD to allow, in which pockets of the enterprise, many others are going all in. According to a recent Gartner survey, we'll see half of enterprises move exclusively to BYOD in 2017. Currently, "almost 40% of organizations worldwide are actively encouraging 'bring your own' (BYO), while about 20% are actively discouraging it."[1]

Today, employees are tech savvy and want more of a say about the tools that they use to get their work done. But BYOD creates a number of challenges when it comes to enterprise mobility, and it's essential that organizations know how to go about finding – and managing – the Enterprise Mobility Management (EMM) platform that meets their needs today and will continue to in the future. Because BYOD will undoubtedly expand to include other technologies, devices, and mobile endpoints.

Keep these best practices in mind as you choose the solution that's right for your organization. They'll help ensure that your mobile operations run smoothly today and down the road.

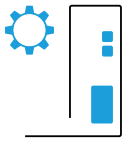
1. Set measurable goals

What goals are you trying to achieve with a mobile workforce? Understanding what your company is trying to accomplish, and measuring that success, is important to keep your BYOD implementation under control and in scope. It's not always easy to keep BYOD costs down or to measure hidden costs, like how much time employees spend managing their own devices, as well as potential security risks. As Gartner notes: "Cost reduction is not universally achievable with BYOD. A roughly equal number of organizations say they are spending more money as a result of BYO as those that are spending less."[3] However, employee productivity and new business opportunities that come from mobility are measurable. Communicate your mobility goals clearly to management and define the metrics you'll use to measure the success of your BYOD investment.

2. Define usage and cost policies

When employees are using their smartphones for work and personal use, costs can get complicated. Reimbursing adds a layer of administrative complexity. There's also the question of ownership of the work phone number, which, if not clearly spelled out, can complicate things even more. Set clear usage and cost policies around corporate phone numbers and how much your company is willing to cover in monthly costs. Defining these policies will help keep your costs on-track and manageable over time.

"Cost reduction is not universally achievable with BYOD. A roughly equal number of organizations say they are spending more money as a result of BYO as those that are spending less."



3. Choose a solution that can flex with your requirements

Every business unit is unique: the needs and concerns of one don't apply to the other. So ongoing communication with those units about their individual requirements is important. BYOD policies should be continually evolving, and they require the input of cross-functional teams such as HR, legal, IT, and business units themselves. To handle BYOD well and extract value, your infrastructure should scale to accommodate the number of users you need to manage today and any increases you anticipate. Rather than a complex, multiple server environment, most IT departments look for lean deployments, with as many devices per server and per domain as possible. You need an intelligent EMM solution that can handle high volumes of users and data traffic, and is easily customizable to individual security requirements, no matter how many users you need to manage.

4. Ensure you can effectively manage the tools employees want to use

One of the perceived benefits of BYOD is that employees can access the latest and greatest productivity apps on devices they prefer. But of course, this depends on your ability to securely manage those tools. File sharing and sync capabilities, as well as the containerization of work data and apps, are essential elements of an effective EMM solution. Find the productivity apps that your employees love to use and make them enterprise-ready by wrapping them in iron-clad security. This will encourage employee uptake and usage retention of apps approved by your company.

5. Expect the best, but plan for the worst

You can compromise on some things but not when it comes to the security and management of apps and devices. Invest in an infrastructure that is tried and true for your own peace of mind. Security and management of a rapidly expanding BYOD portfolio is complex. According to Gartner, "over three-fourths of organizations cite security issues as the biggest concern, and with good reason: 23% of U.S.-based employees say they have experienced some compromise on their personal device in the past year. . .the biggest risks for tablets and smartphones lie in data loss and theft, rather than malware."[4] To decrease some of this risk, provide a list of recommended or supported devices to employees that meet your security expectations and those of regulators. Ensure that your EMM solution can leverage existing device security, then wrap it in extra enterprise security; and that it offers high-availability for disaster recovery.

6. Get the right support

Support is an essential element of any Enterprise Mobility Management (EMM) strategy. In the emerging EMM market, where different flavors of support are being offered by a variety of vendors with vastly different levels of expertise, integrating the right support into your EMM solution will maximize your mobility uptime, help to preserve business continuity, and strengthen customer faith in your ability to deliver on your promises. With BYOD, it's more important than ever for your support partner to effectively cover your entire mobile environment, across all platforms. And it's critical to select a strategic partner who will be there to support you before your deployment, while it's underway, and long afterward. You must ensure that your support aligns closely with the demands and expectations of your user base and that the support helps, not hinders, the pursuit of company objectives.

7. Future-proof your EMM solution

BYOD is just the beginning. In the near future, BYOD will expand from smartphones and tablets to other technologies, such as wearables. An EMM solution you choose today should have the fundamentals in place to provide secure and efficient management of all endpoints – not just smartphones and tablets. Per Gartner: "In the next several years, this suite of capabilities will rapidly converge into a more consistent approach for all endpoint devices via unified endpoint management (UEM)...This trend implies that over time, all devices will be managed more like smartphones than like traditional PCs."[5] Your infrastructure should be able to adapt to the BYOD landscape of the future.

Gartner's stance on BYOD today[6]

Impacts

- BYOD creates new opportunities for CIOs and the business by increasing the number of mobile-application users in the workforce.
- BYOD drives employee satisfaction, productivity and new applications.
- BYOD requires IT and business units to invest in ongoing policy creation, enterprise mobility management, security and infrastructure expansion.
- BYOD increases risks for CIOs and CISOs and changes expectations for workforce enablement.

Recommendations

- Examine opportunities for new applications that assume personally owned devices in the workplace at all levels.
- Pursue platform-agnostic management tools and application platforms.
- Establish clear goals and policies for your BYO program. Periodically benchmark stipends, reimbursements and allowances.

Built for BYOD

BES12 is a cross-platform EMM solution by BlackBerry®. With a long-standing reputation as the most trusted mobility solution in the marketplace, BlackBerry remains the strongest brand overall, used by a third of the Enterprise market.

BES12 offers a comprehensive EMM solution that gives you control over devices, apps, activities, and critical data across all endpoints, regardless of platform. IT can manage all endpoints through one, consolidated, easy-to-use console. BES12's new attribute-driven, endpoint-permissions model lets you manage devices, apps and data, by-person or by-group efficiently. Monitoring and easy-to-use dashboards are more streamlined and customizable than ever.

BlackBerry security is trusted by thousands of enterprises around the world. Using encryption, containerization, app-wrapping and BlackBerry's secure global infrastructure, BES12 locks down critical data both on-device and in-transit. Secure work spaces managed by BES12 allows cross-platform (iOS, Android™ or BlackBerry) ownership models, from BYOD to company-owned, keeping private data private and work data secure. BES12 takes advantage of client-side security specific to a mobile endpoint and extends that security through encryption, certificates and containerization. You are in complete control of all the corporate assets being used on your employees' mobile devices. Combine BES12 with BlackBerry devices and you have one of the most secure, end-to-end, mobility solutions on the market today for regulated industries – guaranteed.

The modern architecture of BES12 can be deployed on-premise as well as through private clouds (hybrid and public clouds coming soon). With options to configure High Availability and Disaster Recovery, BES12 is designed to reduce complexity, optimize pooled resources, ensure maximum uptime and help you achieve the lowest Total Cost of Ownership (TCO).

You can rely on industry-leading BlackBerry® Technical Support Services that are included with all BES12 annual subscriptions to help evolve your EMM strategy and to manage your complex and demanding requirements. Tailor your EMM solution with additional relationship-based and technical services for an unparalleled customer experience.

To find out more and to sign up for a free 60-day BES12 trial, head to **blackberry.com/enterprise**[7]

[1] Gartner, Bring Your Own Device: The Results and the Future, May 2014, 2

[2] "Beyond BYOD: How businesses might COPE with mobility": Available at **http://blackberryresourcecenter.virtualevents365.com/bbrc/resources/content/e8d72e44-1eda-48b6-977b-a6a47f11f817/Beyond%20BYOD%20BlackberryOvum.pdf**

[3] Gartner, Bring Your Own Device: The Results and the Future, May 2014, 7

[4] Gartner, Bring Your Own Device: The Results and the Future, May 2014, 12

[5] Gartner, Bring Your Own Device: The Results and the Future, May 2014, 11

[6] Gartner, Bring Your Own Device: The Results and the Future, May 2014

[7] 60-day Free Trial Offer: Limited time offer; subject to change. Limit 1 per customer. Trial starts upon activation and is limited to 50 Gold BlackBerry subscriptions and 50 Secure Work Space for iOS and Android subscriptions. Following trial, customer must purchase subscriptions to continue use of product. Not available in all countries. Subscriptions can be purchased direct or from authorized resellers. When a system is upgraded to production, the trial subscriptions will no longer be available. This Offer is void where prohibited and is subject to modification, extension or early termination at BlackBerry's sole discretion