THE CIO'S GUIDE

To Enterprise Mobility Management

Whitepaper

SERIOUS MOBILITY FOR SERIOUS BUSINESS

BlackBerry | ENTERPRISE

How IT leaders are using this guide

CIOs make tough decisions every day. To make the right ones, you have to trust your sources and be confident that you're prioritizing the right issues.

Enterprise Mobility Management (EMM) is top of mind for most CIOs today, not just because of BYOD and COPE (Corporate Owned, Personally Enabled), but also because of the clear opportunity that mobility presents to boost productivity, customer engagement, job satisfaction and more.

But realizing these opportunities requires an EMM strategy – and forming an EMM strategy is complicated. As Computing magazine summarizes it, "the playing board is prone to wild fluctuations in a game where some pieces can suddenly take on unexpected new powers, with others disappearing altogether."[1]

Getting to the right answers means scratching well below the surface

This guide is designed to help CIOs decide which issues to focus on, which tough questions to ask, and ultimately, how to make the right choice for EMM. It's based on real-world research, includes input from Fortune 500 companies and has been vetted by mobility analysts and experts.

Forming an Enterprise Mobility Management strategy: Key factors

An Enterprise Mobility Management strategy lists and describes your company's key requirements and positions on a wide range of mobility issues. The goal is to align mobile IT priorities with short-term and long-term business goals. It should be a formal document created by IT, HR, and Legal, but must include input from all stakeholders.

If your organization doesn't have an EMM strategy today, there's no reason to postpone it. Think of it as a living document. The discussions you have while you build it will allow you to make the critical decisions you need to get an effective long-term EMM solution in place.

Your Enterprise Mobility Management strategy answers important basic questions such as:

- Who pays for hardware, software, and wireless services?
- Are BYOD and COPE devices supported, and if so, how? And for which business units, roles or individuals?
- Which employees get what type of mobile device, e.g. laptop, smartphone, tablet?
- How much security is required, for which user types, and how will it be enforced?
- What data, applications and functions are allowed on which enterprise devices?
- Who supports the mobile device users and manages the devices?
- How will you handle LCM (Lifecycle Management) when it's time to upgrade devices and apps?

But this is only the beginning. There are several categories to weigh, across management, security and implementation.

The list on the following pages is detailed, though not exhaustive. If your stakeholders can form clear opinions on these issues, you'll be on your way to an Enterprise Mobility Management strategy. And with that strategy in place, finding the right EMM solution (and optimizing it from there) will be much, much easier.

The issues can be broadly grouped as follows: Management, Security, Everything Else. Let's take a closer look.

Management

Device and platform support

Whether your devices are corporate-owned, BYOD, COPE, or a mix, chances are you're already dealing with multiple platforms, operating systems and device types. So you've got to make sure your EMM solution can manage those devices in all the ways you need and want it to.

Consider not only the platforms you support today, but those you may support in the future. Most MDM solutions now support iOS, Android™, Windows® Phone and BlackBerry®.

But to be sure your solution will support the devices of tomorrow, think about the track record of the providers: Are they well established, or a VC-funded newcomer? Do they have a history of innovation and anticipating enterprise needs? Do they have a clearly defined vision and roadmap for the future?

Administration features for MDM

Marco Gocht, CEO of the mobility innovation leaders ISEC7, says that the enterprise customers his company works with today have, on average, 3.2 MDM solutions in place already, though they might not think of it that way. "They often have BlackBerry® Enterprise Servers, another solution to manage software deployments, and then a third-party MDM solution to manage their iOS devices. Now, they're looking to consolidate all of this into one platform to cut operating costs and lighten the administrative burden on IT and support staff," he explains.

From a day-to-day management perspective, the platform you choose should allow IT administrators to manage everything from one unified console. And given that IT has enough on its plate without the challenges of learning an entirely new management paradigm, familiarity and interface usability are critical factors. That's true whether you're seeking to replace several MDM platforms with one, or looking for your first EMM solution. Determine how important it may be to manage user accounts, assign user groups, administrative roles, email profiles, software configurations, and IT policies to user accounts – all from the same dashboard. A "single pane of glass" is what some EMM solutions offer, and when that promise is delivered on, the savings in time and money can be significant.

Since mobile workers spend so much of their time away from the office, controlling MDM over-the-air (OTA) is practically an entry-level requirement by now. OTA for mobile devices is also important since they tend to be replaced more often than laptops and desktops – an average of 18 months as opposed to three years.

Find out how the EMM solutions on your shortlist facilitate device lifecycle management (LCM). Does the solution make the switchover process simple for end users? Some force users to essentially start from scratch when they transition to their new smartphone or tablet. But other EMM solutions ensure that when a user gets started with their new device, the data and apps they need are ported over (pre-provisioned). The same goes for their personal data – with some EMM solutions, users have to move their videos, music, photos and personal apps over to their new devices themselves; others make this process easier. Since employee satisfaction and productivity are such important drivers in mobility today, these factors matter.

And although OTA has become the norm in EMM, you still need to pay careful attention to the specifics. Important OTA features include (among others): setup and configuration management, backup/restore, remote lock and wipe, mobile application deployment and management.

- Remote setup and configuration of mobile devices allows IT staff to configure new devices quickly and easily without resorting to a USB cable and tethering the configuration information onto the device. Remote configuration from a central solution enables IT staff to manage a number of different parameters.
- Backup and restore are essential OTA features for dealing with lost, stolen or damaged mobile devices. Automatic backup and restore of mobile device settings, data, and applications is also valuable for new and replacement devices (especially given the 18 month lifecycle of many enterprise smartphones). These OTA features can also be used to synchronize important files between a mobile worker's desktop computer and their mobile device.
- Remote locking/wiping prevents access to any sensitive data on the device, but can also prevent unauthorized access to the corporate network. Mobile workers should be trained to report a lost or stolen mobile device as soon as possible, because even a brief delay can have serious implications for the company. If the mobile device is returned, the OTA restore and remote configuration features of an EMM solution can quickly re-configure the device to its natural operating state. Advanced EMM solutions can also enable selective remote wipe for some devices, which is useful in scenarios where a BYOD device is temporarily misplaced (this way, the user's personal content can be left untouched, even while the corporate data is completely removed).

Mobile Application Management (MAM)

What apps are your employees using today? How are those distributed, managed and secured? How important is it that IT can control apps from one place? How will you keep untrusted apps from accessing your network? What is your organization's attitude to BYOA (bring your own app) – where employees use third-party apps for work situations? For example, is it okay to have an employee uploading receipts and expense details to an expense app they happen to like? Does HR or Finance have reservations about it?

Enterprises today are striving to mobilize the desktop – in other words, to provide users with all the tools they need to do their jobs from virtually anywhere, anytime. So they're working to make familiar desktop tools and applications available and easy to use while mobile. That's why your approach to apps is critical. The more custom and third-party apps you mobilize, the more productivity gains you stand to realize – and the more security risks you need to be prepared to tackle.

For many enterprises, in a BYOD scenario, it's important to be able to allow users to access and download business, productivity and personal apps, as well as games, videos, movies and music. But the apps employees download to their devices may come from untrusted sources and expose your organization to security risks. You want control over what these apps can access. At the same time, you want the ability to push required or recommended apps out to BYOD users and manage their use.

Many MDM providers offer some version of a corporate app storefront or catalog for enterprise users. But when you think about how many apps you're likely to enable over the next few months and years, for how many users, across how many platforms and devices, you need to know the details – because mobile application creation, deployment, management and security all become top priorities.

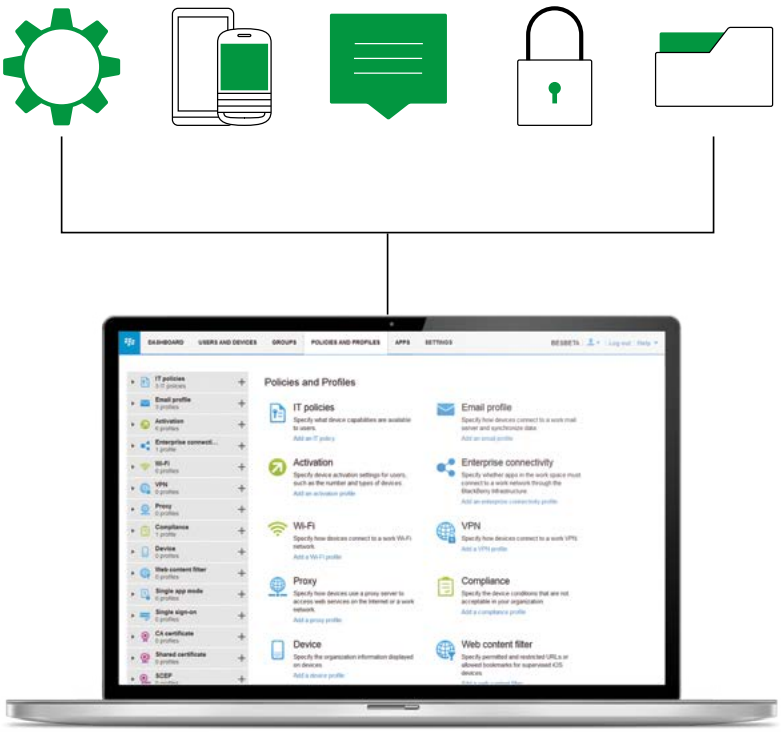
Leading EMM solutions can provide application security, so that work apps are kept secure and separate from personal apps and data, and user authentication is required to access these secure apps.

Some EMM solutions have inherent limitations when it comes to app management. Specifically, they may require that your custom apps be re-developed (re-coded) using the EMM vendor's own SDK (software development kit) to apply encryption and other security capabilities. And when an app is updated to a new version, that code may need to be re-written and re-deployed yet again.

Best-in-class EMM solutions make it easy to containerize and add new security capabilities to existing custom apps without having to re-code the app. And they make it easy to refresh apps in other ways, again without making more work for IT, developers or end users.

Reporting and Monitoring

What are your reporting requirements? And what will they become as your organization grows? For IT administrators, an EMM solution needs to provide a quick, clear look at the entire mobile fleet. Reporting capabilities give IT a detailed view of what's going on, so they can identify issues and get them resolved quickly. To consider: Will your IT administrators want immediate access to a unified dashboard of key metrics across their entire mobile deployment? Is it important that they can drill down into more detail on any area they choose so they can take immediate action or export data for further analysis? If your industry is one that needs to meet strict regulations, then reporting, auditing and monitoring capabilities are not just beneficial – they may be legally required.



Cloud vs. On-premises

Many EMM solutions now offer both cloud (AKA Software as a Service or SaaS) and on-premises versions. There are advantages to each. Both approaches are legitimate and the answer depends on your organization's specific scenarios. Among the factors that may play into your decision:

- Deployment time: Cloud-based solutions can often be up and running very quickly.
- Feature requirements: Some cloud solutions offer fewer features – particularly if they're geared toward businesses at the smaller end of the scale.
- Maintenance: Cloud-based solutions can lighten the load on IT when it comes to updates and upgrades, which is especially helpful for businesses with limited technical resources in-house.
- Access and control: An on-premises solution sits server-side in your datacenter. Some IT organizations believe this provides a greater amount of control over data and tighter integration with other systems.
- Compliance: For financial institutions, healthcare, and government organizations, regulations may dictate that an MDM/EMM solution must be on-premises. For example, if you're a US-based organization with international users, the USA Patriot Act will affect how and where you can store customer data.

Security and Privacy

Company information stored on a mobile device must be just as secure as information stored behind the firewall on the corporate network. Unauthorized access to corporate data can cause bad press and embarrassment, or equally likely, financial loss or litigation.

To mitigate this risk, IT staff should have the ability to control all aspects of mobile device security. This includes the ability to mandate passwords for mobile device users, encrypt data stores and erase data from mobile devices remotely. Most enterprises also want an EMM solution that can auto-detect non-compliant usage, apps and devices and then take automatic pre-defined actions. And for iOS and Android devices, detect 'jailbreaking' or 'rooting' and prevent malware from reaching the network.

Data Leak Prevention (DLP)

With the consumerization of IT comes the co-mingling of personal and work use cases – and pure consumer devices offer no integrated protection against sensitive enterprise data leaking through personal channels. As enterprises mobilize business processes, more and more sensitive data passes through and resides on mobile devices.

Meanwhile, risk-inherent personal use-cases continue to grow, spanning:

- Social networking
- Personal email
- Untrusted personal apps
- Instant Messaging, SMS/MMS, other P2P messaging
- Web browsing
- MicroSD storage
- USB connectivity

Data loss/leak prevention is about detecting potential data breaches and eliminating them. EMM solutions may do this in several ways. But fundamentally, they must protect sensitive information, while data is in-motion (that is, transmitting or sharing data on the network), and while data is at-rest (data storage). Data leakage can be intentional, but often it's simply a mistake – such as a user who copies and pastes sensitive details into an insecure channel. The best EMM solution will make it virtually impossible for data leakage to happen, either way.

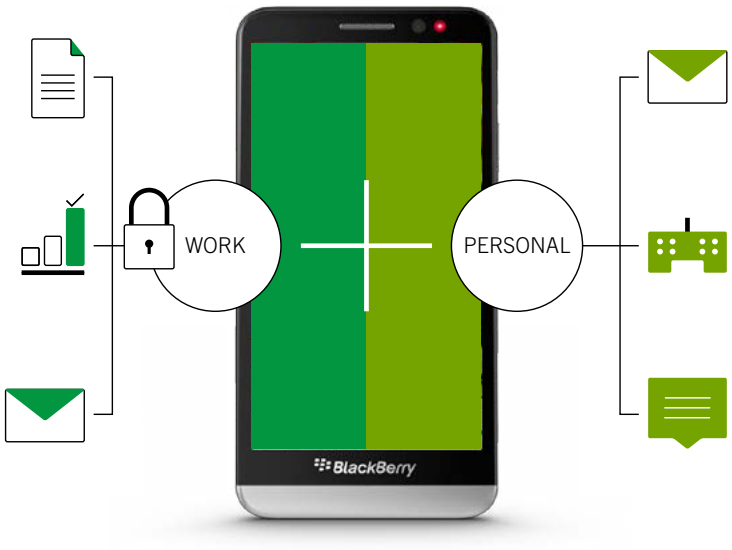
Containerization/Sandboxing

Containerization, sandboxing, workspaces – if you've explored EMM, you recognize these buzzwords. Each vendor has a slightly different take on what these terms mean, but fundamentally, it's about securely separating enterprise data and apps – keeping work and play from co-mingling and creating security issues for your business. Containerization is, in part, a DLP strategy.

It's also about creating a better experience for users. For example, with appropriate containerization in a BYOD scenario, IT doesn't have to wipe an employee's personal photos, videos, music and apps when that employee leaves the company. Some approaches to containerization can create headaches for users too – forcing them to sign in every time they send an email, to use one example. So how your solution handles it matters.

Authentication

Mobile device authentication and mandatory passwords are the easiest, most effective MDM policies to enforce. When a mobile device is lost or stolen, the device should not be usable by anyone other than the owner, and the data on the device needs to remain secure. IT staff should force mobile devices to adhere to a defined password policy. All mobile devices (or at least the work portion) should have an inactivity lock and be protected by a strong power-on password that's refreshed every three to six months. EMM solutions should provide a complete set of password functions to secure mobile devices.



Establish a separate container for work apps, data and content across iOS, Android and BlackBerry devices – all managed through BES12

Virus and other malware protection

There's no question that mobile applications can increase the productivity of mobile workers; however, which applications are installed on a mobile device and how they're sourced and deployed is a serious concern for the enterprise. It's easy for viruses, trojans, worms and other malware to be unknowingly loaded onto many wireless devices. Malware threatens information confidentiality, endangers system passwords and increases the risk of data compromise. Your EMM strategy needs to address your enterprise's risk factors (and attitudes toward those risks) so that you can choose a solution that addresses them appropriately.

IT policies and controls

How many user profiles exist in your organization? How many user-cases? What's the range of security scenarios you need to address? And what's likely to change over the next several months and even years? Effective mobile IT controls give administrators the peace of mind that comes from maintaining the precise control they need, appropriate to every situation and user.

Your EMM strategy document should assess how many security profiles you need to account for, from interns all the way up to the CFO. And your EMM solution should allow you to tailor policies and controls with the granularity you need. Today, you likely don't need 500+ settings – a complete EMM solution will inherently account for many of the issues automatically through features like DLP and containerization.

Everything Else

Pricing and Total Cost of Ownership (TCO)

Consider all the costs associated with deploying an end-to-end EMM solution. According to a detailed TCO study by Strategy Analytics, optimizing or upgrading an existing setup can be more cost-effective than changing the setup completely.[2]

Strategy Analytics also points out that enterprises need to consider the hidden costs associated with BYOD. BYOD may appear to be a quick and easy way to drive greater productivity and efficiency as well as reduce costs, but the cost of managing it can actually be more expensive than you might expect. Consider the costs of not only making changes and supporting multiple platforms, but also hidden costs and time constraints involved in training. And, of course, support.

To get to a real picture of TCO in EMM, you need to consider direct and indirect costs. Failure rates and downtime costs (including any productivity loss, lost revenue streams, plus opportunity cost) are important factors that are often left out of the equation. What level of reliability does your enterprise require? Will your solution provide it?

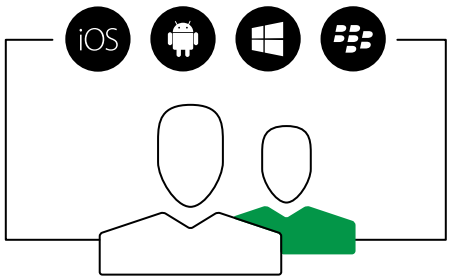
Moving to any new EMM solution will involve buying licenses, whether those are subscription or perpetual. Some vendors make it possible to leverage your existing investments, in both licenses and even in end-of-life devices. Find out what's available – you may be able to save your organization thousands.

Migration and implementation

Migrating to any new platform requires a commitment of time and resources. But the process doesn't have to be stressful. Choosing the right approach is critical – you want to be up and running with as few interruptions to your end users as possible.

Your EMM strategy needs to account for this process. What resources do you need and where will these come from? Marco Gocht of ISEC7 explains: "Typical enterprise customers have thousands of devices operating on different continents, from multiple offices around the world. You need to have a transition plan for the migration phase, a schedule for these migrations and a training plan for both IT and end users."

Speed is another key aspect. If you're migrating hundreds or thousands of devices, does your EMM provider offer services to make this happen in an automated fashion? Each manual migration can take 30 minutes or more.



Technical support

You rely on your mobile platform – to speed up decision making, boost revenue and profit, facilitate workflow, and keep users, teams, customers and suppliers connected. It's business critical. So when you're choosing your EMM solution, ensuring that the vendor offers the support capabilities and options you need makes smart business sense. Otherwise, you're jeopardizing the gains that your EMM investment is meant to achieve in the first place.

Training and end user features

After your Enterprise Mobility Management strategy is developed, employees must be educated. All company employees should be trained on and have access to the latest version of the document on the company intranet. Your strategy must also account for time to train IT on the new EMM solution. What training support will you need and how will you access it, and at what cost? The easier your EMM solution is for IT and for end users to interact with (both for initial provisioning and ongoing management), the less time you'll need for training – so be sure to find out what each potential vendor has done to streamline and simplify processes for these two key stakeholder groups.

The company

The MDM world is full of venture-cap funded startups that popped up to meet a burgeoning need. As the market matures, many of those startups are folding or being bought up by larger players. What do you need to know about the vendor? And do you believe their solution is built to last, even if they merge with another company? You may have internal procurement requirements around the vendor's structure, policies on the environment and accessibility, diversity and inclusiveness, market share and so on – be sure to get those on the table early so you can quickly rule out vendors that don't comply.

An EMM strategy: Worth the effort

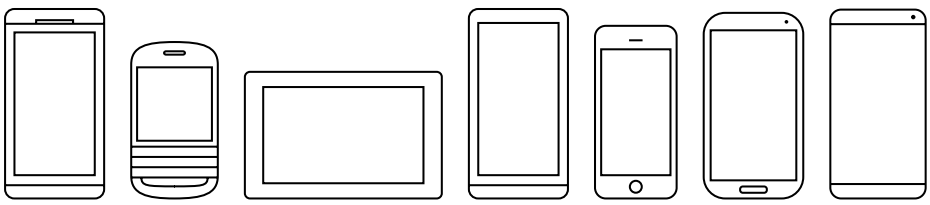
Enterprises that develop an Enterprise Mobility Management strategy and follow up with an EMM solution can expect significant benefits. An EMM solution improves mobile security, reduces risk, and makes it easier for IT administrators to manage the growing number of mobile users.

This document covers many of the key factors to consider as you form or re-form your EMM strategy – but there are many more, and those will depend on the specifics of your organization. And although the process can be time-consuming and sometimes even political, working out the answers before you decide on your solution will save time, reduce costs and prevent headaches every step of the way.

Best-in-Class Enterprise Mobility Management

BES12 is the command and control center for the secured enterprise and the core of the BlackBerry cross-platform Enterprise Mobility Management (EMM) portfolio. BES12 helps you manage enterprise mobility across iOS, Android, Windows Phone, Samsung KNOX and BlackBerry devices. Built on BlackBerry's trusted, global network, BES12 makes managing enterprise mobility efficient and secure.

While there are a number of startup companies that make bold claims, BlackBerry has more software engineers and the most resources dedicated to developing the most innovative solutions to address this complex challenge.



Why should you explore BES12? If you've taken the time to read through this guide, you know that the issues at play in any EMM decision are complex. For each of the topics and questions covered here, we have an answer we'd love to share with you. To touch on a few:

Comprehensive EMM

BES12 gives you control over the availability and usage of devices, apps, activities and critical data. Comprehensive and cross-platform MAM, MDM and MCM make BES12 the only command and control center for your secured enterprise that you'll ever need.

End-To-End Security

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 mission-critical data both on-device and in-transit. All mobile management traffic passes through a single port behind your firewall, 3101, via our world-renowned NOC, to ensure user privacy and data security. With secured work spaces on iOS, Android and BlackBerry devices, your data traffic is also routed through a consolidated port, protecting your most important asset – your business data. BES12 is built on proven security you can trust.

Enterprise Mobility Ecosystem

BES12 is the 'central nervous system' of a powerful ecosystem that brings together mobile devices, apps, cloud services, and carrier services. Extend your EMM capabilities with integrated BlackBerry Enterprise Communication & Collaboration and Identity & Access solutions. With BES12, consolidate and manage your business workflows within one of the most secure and extensible mobility ecosystems on the planet.

Unified UX for Administration

Manage all endpoints through one, consolidated, easy-to-use console. Manage devices, apps and data, by person or by group, more efficiently than ever. Monitoring and easy-to-use dashboards are more streamlined and customizable than ever.

Modern Architecture

Scalable up to 25K devices per server and 150K devices per domain, BES12 can be deployed on-premise, in the cloud or as a hybrid of both. Options are available 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).

Client-Side Lockdown

Secure work spaces managed by BES12 allow 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 enhances that security through encryption, certificates and containerization. You are in complete control of all the corporate assets being used on your employees' mobile devices.

Trusted Network

BlackBerry is renowned for its secure global network. Encrypted end-to-end, BlackBerry secure connectivity offers BES12 customers always on, always connected control over managed devices and consolidates all traffic through a single port for ease-of-administration and tight control of mission-critical traffic and data.

Hardened For Regulated Industries

BES12 supports all tiers of device ownership and deployment models from BYOD to COPE: but for critical, regulated industries, such as financial services, healthcare, and government, BlackBerry offers a COBO (corporate owned, business only) model. Combining BES12 and BlackBerry devices guarantees one of the most secure, end-to-end, mobility solutions on the market today.

World Class Global Support

You can rely on the industry-leading support that is 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 even greater user satisfaction.

To find out more and to sign up for a free 30-day BES12 trial, head to **blackberry.com/enterprise**[6]

[1] Available at **http://www.computing.co.uk/ctg/news/2274017/making-enterprise-mobility-strategy-like-playing-chess-on-acid**

[2] Available at **http://ca.blackberry.com/content/dam/blackberry/pdf/whitepaper/northAmerica/english/StrategyAnalyticsReport.pdf**

[3] 30-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.

BlackBerry®