BLACKBERRY COBO: ULTIMATE MOBILE SECURITY AND CONTROL

Corporate-Owned, Business-Only Enterprise Mobility Option for Regulated and High-Security Environments
BLACKBERRY COBO: ENTERPRISE MOBILITY OPTION FOR REGULATED AND HIGH-SECURITY ENVIRONMENTS

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>COBO at Work</td>
<td>6</td>
</tr>
<tr>
<td>BlackBerry Difference</td>
<td>8</td>
</tr>
</tbody>
</table>
Every organization has unique requirements for mobile device management, from low-security BYOD, to user-friendly COPE through to the highest level of security and control, which we call COBO. Government organizations, financial services, legal, healthcare and other regulated industries often need to employ multiple device and application management strategies across a variety of use scenarios and user risk profiles. But when security and control are of paramount concern, and IT needs to enforce business-only use, BlackBerry’s COBO option can provide optimal protection against data loss and strict compliance with regulatory requirements.

Defined and offered exclusively by BlackBerry, a true COBO option to mobility management provides peace of mind that your high-security users (often a select portions of your workforce) are equipped with mobile computing and communications capabilities that meet your corporate-only requirements for data security.

“BlackBerry is the originator and most prominent vendor offering this all-inclusive hardware and software package for COBO deployments, and remains the leader in terms of end-to-end device security and management.”

Source: Ovum, “Beyond BYOD: How Businesses Might COPE with Mobility”
Introduction

Long before there was BYOD, there was corporate liable, typically defined by an organization taking responsibility for the cost, maintenance and legal liability of devices issued to employees. Years before employees started toting their own devices into the workplace, thousands of organizations and millions of end users were sending business-only secure email, messaging, applications and even encrypted voice over corporate liable smartphones from BlackBerry.

Introduced in 1999, BlackBerry’s Corporate-Only, Business-Only option has evolved over the years but remains the only true COBO solution available. BlackBerry’s Enterprise Mobility Management (EMM) platform, BES10, is a full multi-platform solution for managing and securing BYOD and COPE deployments of iOS, Android and BlackBerry devices, including containerization options for all platforms. But government agencies, companies in regulated markets and any business that requires stringent security and control continue to turn to BlackBerry 10 smartphones and BES10 as the only end-to-end platform capable of offering an enterprise-grade COBO option.

COBO was the predominant deployment choice on the enterprise device management spectrum through the end of the previous decade, when consumer-oriented smartphones started entering the workplace and the Bring Your Own Device phenomenon emerged. The choice of device management options recently increased further with the introduction of the Corporate-Owned, Personally Enabled (COPE) approach, as well as other device policy permutations, such as Choose Your Own Device (CYOD).

The COPE approach to enterprise mobility was largely a counter to BYOD, bringing relief to IT by providing configuration flexibility between BYOD and strict corporate-owned approaches. COPE enables enterprises to adopt device management policies that allow a mix of personal and work data on the same device. For the first time, COPE handed IT the tools to effectively address risk management and user satisfaction on a single device.
Not all organizations, however, have the same requirements for enterprise mobility management. A large portion of the enterprise universe, primarily government agencies and regulated industries, including financial services, healthcare, legal, professional services, public sector and education, still requires a device management approach that restricts mobile device usage to business-only communications and computing.

For those organizations, BlackBerry offers the only true COBO option for enterprise mobility management. BlackBerry’s COBO mobile device management option delivers the ultimate security and compliance, with a granular set of commands and controls that organizations can leverage to provide an effective balance of risk management and end user productivity and satisfaction. BlackBerry is the only integrated end-to-end smartphone and EMM platform provider offering a real COBO device and application management option.

### Device Management Scorecard

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Who chooses the device?</th>
<th>Who pays for device?</th>
<th>Who pays service fees?</th>
<th>Mobility environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD</td>
<td>User</td>
<td>User</td>
<td>User may pay in full, expense all or portion, or receive a stipend</td>
<td>Minimum security and compliance oversight</td>
</tr>
<tr>
<td>COPE</td>
<td>Company or user from an approved list</td>
<td>Company</td>
<td>Company</td>
<td>Balance of user freedom and company oversight</td>
</tr>
<tr>
<td>COBO</td>
<td>Company</td>
<td>Company</td>
<td>Company</td>
<td>Business-only use</td>
</tr>
</tbody>
</table>

### Defining Ownership and Liability

The language used to describe mobile device ownership is murky. The terms corporate owned and corporate liable, for example, are often used interchangeably, with liability being synonymous with ownership of device and payment of airtime. Personal, or individual, liable devices are defined by several market research firms as smartphones or tablets used in corporate settings but purchased by an individual who is not reimbursed through a formal corporate mobile device purchasing policy. Devices defined as corporate liable are purchased by the company or organization and distributed to employees for business and sometimes personal use.

The term “liability,” however, is also often applied in a legal sense, as an indicator of financial responsibility in the event of a lost or stolen device. The implication is that whichever entity is “liable” for a mobile device is likely to be held responsible for penalties or legal fees associated with the misuse of the device or data on the device.
The principal benefit of BlackBerry’s COBO options for device management is the ability to restrict usage of smartphones to work-related computing and communications activities for organizations that require that level of control. BlackBerry COBO also empowers IT administrators to impose highly granular device, app and data management to enable government, financial services, regulated and other high-security environments to meet compliance requirements.

COBO is the optimal device management option for enterprises that require employees to carry a completely “locked-down” device, at least during specific business hours or in specific locations. COBO is also an optimized management approach for environments that require administrators to possess the ability to apply a highly specialized set of policy controls, including the activation or deactivation of a device’s camera or GPS, limiting access to a specific corporate WiFi networks or disabling Bluetooth.

BlackBerry’s 256-bit encryption of data in transit or at rest ensures that your information remains private. For compliance purposes, the BlackBerry COBO option can leverage the logging and auditing capabilities of BES10 or be pair with messaging and call tracking software from BlackBerry partner GWAVA, or another member of BlackBerry’s extensive enterprise application partner ecosystem.

A COBO approach to managing enterprise mobility is designed for government entities and regulated industries increasingly confronted with an onerous set of compliance requirements and data leakage concerns. The financial services, healthcare and public sector industries in particular have been impacted by legislation in the past couple of years that requires precise auditing of all electronic transactions, including, email, messages and voice calls. Meeting these strict compliance requirements with less conservative management approaches, particularly BYOD, is difficult – if not impossible.

But it’s not just the regulated segment of the enterprise space that requires COBO. Business units, or even individual executives, at large enterprises often require the ultra-secure control that COBO enables to protect against the theft of intellectual property, data leakage, exposure to legal liability or the violation of laws or compliance rules. Several international leaders use BlackBerry smartphones controlled by a COBO-based device management policy, often augmented with voice encryption software.
International leaders have turned to BlackBerry to protect sensitive conversations and messaging sessions in the aftermath of revelations of sophisticated cyber surveillance conducted by private organizations and government agencies. Germany Chancellor Angela Merkel utilizes a BlackBerry augmented with hardware-based encryption technology from BlackBerry partner SecuSmart to protect her official communications.

BlackBerry's COBO mobility management option provides government agencies, regulated businesses and other large organizations subject to compliance requirements with the tools to ensure mobile business practices do not run afoul of increasingly complex regulatory requirements. BlackBerry's end-to-end approach to mobile enterprise security and compliance enables your business to meet all aspects of compliance, including the encryption of data at rest and in transit, the processing and recording of all transactions and communications, as well as legislation related to privacy protection. BlackBerry also supports compliance with eDiscovery and other electronic audit requirements.

BlackBerry's COBO offering is backed by the company’s distinguished pedigree in the enterprise mobility market and industry-leading accumulation of patents, compliance certifications and other unique qualifications. BlackBerry, for example, is the only EMM provider to be awarded Full Operational Capability (FOC) designation and Authority to Operate (ATO) certification by the US Department of Defense.
Only BlackBerry provides a secure, fully integrated EMM solution. The end-to-end linkage between BES10, the BlackBerry Secure Infrastructure and BlackBerry 10 devices surrounds your entire business with the ultimate mobile security. BlackBerry also delivers a productive and feature-rich mobile experience with an integrated suite of productivity apps for your increasingly mobilized workforce.

The BlackBerry end-to-end EMM solution is also unique in its ability to support the full spectrum of use cases and risk profiles – not just COBO. An organization’s device management policy requirements may vary from business unit to business unit or country to country. Organizations must also be able to manage devices based on employee role, security risk and compliance requirements.

BlackBerry has been the worldwide recognized leader in enterprise mobile security since 1999. Nearly all of the largest government agencies and regulated industries partner with BlackBerry because they recognize that its end-to-end security solutions have reached a level of trustworthiness unrivaled in the industry.

© 2014 BlackBerry. All rights reserved. BlackBerry® and related trademarks, names and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world. All other trademarks are the property of their respective owners. iOS is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS is used under license by Apple Inc. Apple Inc does not sponsor, authorize or endorse this brochure. Android is a trademark of Google Inc. which does not sponsor, authorize or endorse this brochure.