6 Steps to Migrate from BlackBerry to a Secure, Multi-OS Environment

airwatch®

We Simplify Enterprise Mobility™

6 Steps to a Successful Migration

BlackBerry's uncertain future has highlighted a fundamental challenge that all IT professionals must eventually face: becoming integrators, rather than people who roll out and manage a single technology for everyone in their organization.

Migrating away from BlackBerry to meet user demand for iOS and Android devices is not a new trend. An August 2013 Gartner survey showed that only 9 percent of users at organizations expect to be using BlackBerry by 2016, compared to twenty four percent of users today. The following month, BlackBerry's financial losses started making headlines, and what IT professionals suspected they would need to change in the next few years quickly became a priority.

In September, BlackBerry reported Q2 losses of nearly $1 billion and announced plans to lay off 40 percent of its workforce. Then, the company announced plans to go private. BlackBerry received a tentative purchase offer from Fairfax Financial Holdings for $4.7 billion – a fraction of the company's former $83 billion value.

Days later, Gartner published a report: "BlackBerry Announcements Require Enterprises to Take Action." Migrating away from BlackBerry is no longer an option, according to the firm. In an email interview with CIO.com, Gartner analyst Bill Menezes said, "Gartner recommends that our [BlackBerry enterprise] clients take no more than six months to consider and implement alternatives to BlackBerry. We're emphasizing that all clients should immediately ensure they have backup mobile data management plans and are at least testing alternative devices to BlackBerry."

For most businesses, transitioning to a multi-OS environment is inevitable. IT departments that were once comfortably BlackBerry-only shops are facing pressure from users to support multiple device types, and in some cases, scrambling to plug security leaks where users have found ways to access corporate email and documents from other personal devices.

Companies should begin mapping out how to implement a multi-OS strategy as soon as possible. The following migration guide is designed to aid planning for business leaders and IT professionals who are considering transitioning corporate users from BlackBerry to a secure, multi-OS environment with AirWatch. Create a migration strategy that will guide a smooth transition for users with a minimal burden on IT, follow these 6 steps.

1 Determine whether a cutover or a gradual migration makes more sense for your organization.

Determining Factors

Timeline

Budget

User Demand

To determine whether migrating all at once or in phases makes the most sense, decision-makers should consider their timeline first. Does the organization have contractual obligations on existing BlackBerry devices that would prevent a cutover migration? Is the cost to maintain the BES infrastructure an issue, or will the budget allow a gradual transition?

It is also important to consider how much demand there is within the organization for other device types. Consider surveying employees to find out how many would keep their BlackBerry devices if given the choice to use something else. When given the opportunity to switch, nearly 90 percent of employees at an AirWatch customer organization chose iOS or Android over BlackBerry. The company offered corporate-owned devices and went with the platform that was most popular among employees. A cutover migration, which involves employees handing in old devices and receiving new devices within a short period of time, makes the most sense in situations where organizations are migrating away from BES management and from BlackBerry devices entirely and are ready to make an immediate overhaul on their mobility strategy.

A gradual migration, however, can give executives and the IT team time to consider which platforms will be most appropriate for their specific use cases. Because AirWatch integrates with BES, IT administrators can use the existing BES infrastructure and centralize management of every device in the corporate environment.

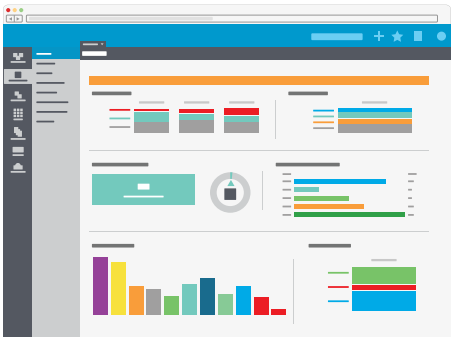
Sheffield Hallam University in South Yorkshire, England, gradually migrated away from BlackBerry devices and BES management. The gradual process gave IT administrators a way to immediately begin more granular management of various device types in AirWatch's central console, as well as begin mapping out a bring your own device (BYOD) plan, without disrupting current BES users. The corporate-issued devices had already reached a tipping point. "When iPhone brought out 3GS, which made data encryptable, the vice chancellor wanted an iPhone. And of course, if the VC gets one, everybody wants one. Soon, we reached a critical mass to where we were a more than fifty percent iPhone environment."

But the true impetus for migration at Sheffield Hallam was IT's awareness of increasing back-door access to university networks. "Unless we actually lock down the exchange server, there was no way to stop people, other than to give them a better alternative than what they're doing right now," said David Wragg, who works in IS&T and is the project manager for the migration at Sheffield Hallam University. "That and tempt them with the extra goodies we will allow them to have with AirWatch – apps that we'd be deploying by the VPP that they might not want to buy themselves, for instance."

In the future, Wragg plans to leverage AirWatch app wrapping and the AirWatch SDK to enable students to create their own apps. "There are a number of courses the students take on app development and app design," Wragg said. "If they create apps that are useful, we will be able to roll them out to certain groups or to the whole university. We can deploy them using AirWatch rather than relying on the Apple store or Google store approving them."

Wragg recommends that organizations that are still using BlackBerry start the migration process now. "Try and do it as soon as you possibly can, because it's been a slow death by a thousand cuts for BlackBerry over the last eighteen months. I would have done it quicker if I could have."

2 Integrate BES into AirWatch for reporting during the transition.



After completing the initial evaluation and deciding on a cutover or a gradual migration, the first step is to integrate BES into the AirWatch platform. AirWatch supports BES, so with a few simple steps, administrators can integrate BES management into the AirWatch console. Administrators can then monitor their entire BlackBerry fleet using real-time dashboards with graphical displays, and drill down into specific device details, including GPS location, installed applications, roaming status and more.

Seeing BlackBerry devices alongside other platforms in the same console can help administrators hone in on problem areas and potential threats.

One AirWatch customer was able to systematically transfer users to their new devices (employees were issued Windows phones, Android phones and iPhones). Users were then prompted to enroll, and their devices were automatically configured. This process ensures the user is enabled and the device is secure. If a user does not enroll, administrators can see that in the console and go directly to that user to resolve any issues. The ability to hone in on problems helps ensure a positive user experience.

After the new device is enrolled, an administrator can simply deactivate the BlackBerry from the BES system. AirWatch will automatically remove that device from the view and from the panel, so the device no longer appears in the console. Then, once all users are migrated off BES, an administrator can decommission the BES server and know all devices are enrolled in AirWatch and under management.

3 Ensure a consistent security experience.

After all devices are under AirWatch management and the BES system has been decommissioned, administrators can integrate AirWatch® Browser, AirWatch® Secure Content Locker™, AirWatch® Inbox and AirWatch® App Wrapping for a security experience consistent to BlackBerry, but that can be applied across device types.

AirWatch Browser is a secure browsing alternative to native browsers with customizable settings. AirWatch Browser allows administrators to define and enforce secure mobile browsing policies from the AirWatch console. Administrators can disable native browsers and public browser applications; authenticate users before granting access; make real-time adjustments; and define use policies for cookie acceptance, copy/paste and printing, and capturing browsing history. Administrators can also require downloaded content to open in Secure Content Locker. With AirWatch Browser, administrators can offer seamless access to intranet sites without requiring device-level VPN.

Secure Content Locker protects sensitive content in a corporate container and secures distribution and mobile access. Administrators can provide end users anytime, anywhere access to the latest versions of important content, and an intuitive user experience that can be branded to provide a consistent look across enterprise resources.

Users are authenticated using existing corporate credentials and must accept a customizable Terms of Use agreement before gaining access to Secure Content Locker. All data and content is encrypted in-transit and at-rest with AES 256-bit, FIPS 140-2 compliant encryption. Administrators can prevent data loss with geofencing, disabling printing capabilities and limiting access for third-party applications. Device status is continuously monitored, and access can be disabled and content can be wiped if a device is compromised.

AirWatch® Mobile Email Management delivers comprehensive security for corporate email infrastructure, regardless of email client. Administrators can control which mobile devices access email, prevent data loss, encrypt sensitive data and enforce advanced compliance policies. AirWatch supports native email clients, containers, enterprise services and cloud-based clients. In addition, administrators can leverage

AirWatch Inbox, a secure, sandboxed email client that provides a native user experience with additional usability enhancements. To keep data secure, administrators limit access to only AirWatch provisioned EAS and POP email accounts and silently configure and update email profiles over the air.

Administrators can also configure email profiles, settings, certificates, SSL security and email compliance policies and create custom whitelists and blacklists based on email client, device model and operating system. If a device is detected as compromised, unenrolled or non-compliant, administrators can prevent access to email to protect sensitive information. Administrators can block attachments based on document file type and require that approved attachments open in Secure Content Locker. Attachments are encrypted using AES 256-bit encryption and administrators can prevent copy/paste of data from an attachment to another application. If a device is detected as compromised, attachments are wiped from the device.

AirWatch® Mobile Application Management provides administrators with sophisticated app development workflow, security and management. With AirWatch, administrators can containerize applications, secure data and enforce compliance policies on Android and Apple iOS devices. AirWatch provides the tools to enable organizations to develop, secure, deploy and manage critical business applications.

For organizations looking to build custom internal applications, AirWatch offers a software development kit (SDK). AirWatch® Software Development Kit enables organizations to take advantage of the advanced AirWatch security features and embed them into custom business applications. In organizations that have already developed internal apps, administrators can leverage AirWatch App Wrapping to add AirWatch security features to existing internal applications without code change.

4 Enable choice and a positive user experience.

Research shows that employees are most productive when they are using the devices they prefer. Because it supports Apple, Android and Windows devices, as well as Symbian and BlackBerry, AirWatch allows organizations to enable choice and a positive user experience. AirWatch offered same-day support for the latest operating system updates for iOS, Android and Windows.

Enabling employees with the devices they prefer was key for another AirWatch customer, whose mobility team recently migrated 1,500 BlackBerry users to iOS devices under AirWatch management. The company has already seen the positive effects. Associates have devices they want to use, with more options at the application level. The mobility teem has watched usage climb steadily ever since.

AirWatch features comprehensive management capabilities for Apple, Android and Windows.

Apple: AirWatch provides complete mobility management solutions for iPhone, iPod touch and iPad enterprise deployments. Operating system versions supported include iOS 4, 5, 6 and the new iOS 7. The new

release from Apple introduces revolutionary security and management capabilities. With AirWatch, administrators can take advantage of the latest mobile innovations and enterprise mobility management capabilities available for Apple iOS. Open in management and per app VPN, both configurable in the admin console, give administrators greater control over which apps can access corporate content and networks. Single sign on will simplify the user experience, and additional query, restriction and configuration settings enhance analytics, usage limitations and device setup.

Android: AirWatch provides complete enterprise mobility management solutions for Android enterprise deployments. AirWatch supports all devices with native Android operating systems, including versions 2.2 (Froyo), 2.3.X (Gingerbread), 3.X (Honeycomb), 4.0 (Ice Cream Sandwich), and 4.1 and 4.2 (Jelly Bean). HTC, Kindle Fire, Lenovo, Motorola and Samsung smartphones, tablets and ruggedized devices are all supported.

Windows: AirWatch provides complete mobility management solutions for Windows Phone enterprise deployments. AirWatch supports Windows Phone 7+ (Mango) and Windows Phone 8 (Apollo) operating systems and all devices running Windows 7+ or 8, including Nokia 820, Nokia 920, HTC 8X and HTC 8S. AirWatch also provides comprehensive management for Windows PC and RT laptops, notebooks and tablets. With AirWatch, administrators can secure all devices enrolled in your enterprise, including smartphones, tablets and laptops, and implement consistent corporate policies across your entire deployment from the admin console.

AirWatch offered same-day support for Windows 8.1, which introduces new security and device management capabilities for Windows PC and RT. With AirWatch, administrators can take advantage of the latest enterprise mobility management capabilities available with Windows 8.1. Clientless enrollment with customizable branding and multi-factor user authentication gives your users a simple and secure experience. Advanced security features, including device encryption, email encryption, VPN, certificates and passcode policies, can be centrally managed from the admin console. Administrators can also disable data when roaming, configure webclips and enable Wi-Fi, all over the air.

5 Host physical or virtual trade-in events where users can setup new smartphones.

To ensure a smooth transition for users, some organizations have hosted trade-in events at local offices, ordered devices ahead of time, and invited representatives of device manufacturers and service carriers on-site for support. Organizations can also get cash back by partnering with a third-party re-use or recycle provider that accepts traded in BlackBerry devices and accessories. Several carriers and third parties offer such programs.

One company recently hosted a successful trade-in event at each local office, where administrators set up a room and scheduled time on each employee's calendar for them to come in. Administrators had previously sent out order forms and allowed employees to choose their new devices and ordered them. At the event, AirWatch, the device vendor and the service carrier each had tables with instruction pamphlets and FAQs. Employees came in, handed in their BlackBerries and got their new devices. If there were any issues, representatives were on hand to troubleshoot. For companies with employees who do not report to a local office, another approach is to host the event during the company Christmas party or a sales meeting.

Another company approached the trade-in from the perspective of user enablement and self-service. The IT team created a website on the company's intranet that mapped out the BlackBerry-to-iPhone conversion.

6 Avoid a major burden on IT during the transition.

The AirWatch self-service portal empowers employees to enroll and manage their own devices. From the portal, employees can enroll additional devices, view detailed device information and perform remote actions. Users can see installed profiles and applications, view GPS location (if enabled), query the device, and clear passcodes. Users can also make requests for apps, profiles and technical support through the portal. These capabilities significantly reduce IT helpdesk burden.

At Sheffield Hallam University, IT administrators are planning to send self-service enrollment information out to all students, faculty and staff via QR codes in an email to make it easy for users to enroll both corporate-issued and BYOD devices.

For IT administrators, AirWatch's user interface is simple, intuitive and responsive, enabling IT administrators to get things done with less effort and time. All devices enrolled in AirWatch Mobile Device Management, regardless of device type, platform or ownership type, are managed on a central, web-based console. An administrator can see all devices in his or her environment in a single, unified view, or filter the view according to parameters such as device type, ownership type or user role.

Additional Resources

For additional information, please visit **www.air-watch.com**.

To get started with a free trial of AirWatch, visit **www.air-watch.com/free-trial**.

AirWatch Global Headquarters

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch

AirWatch is the largest Enterprise Mobility Management provider in the world with over 1,600 employees globally. More than 9,000 companies trust AirWatch to secure and manage their mobile enterprise. With market-leading solutions for mobile security, device, email, application, content and browsing management, we simplify enterprise mobility.