A Good Way to Contain iOS Vulnerabilities

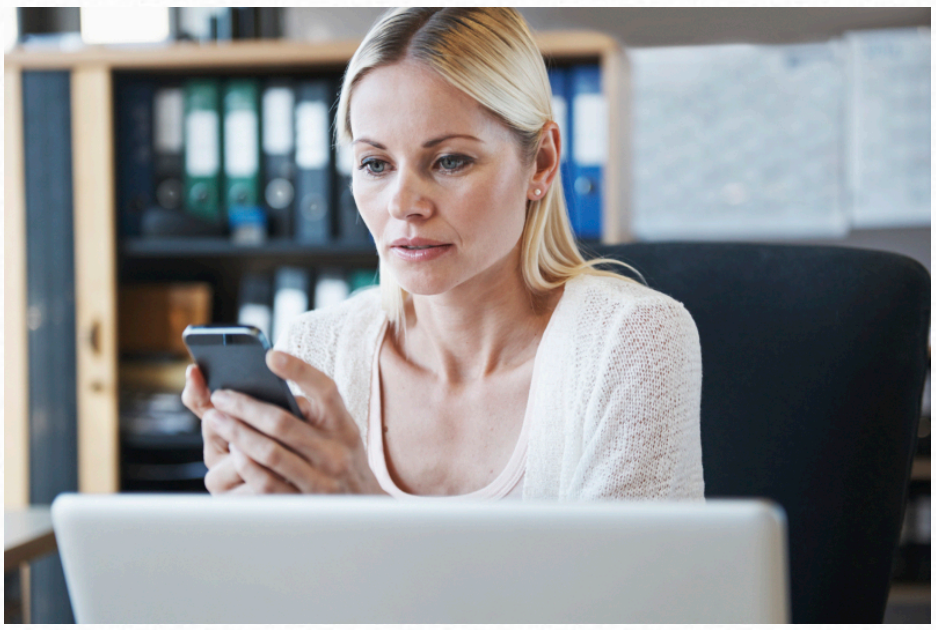
BlackBerry Dynamics

03.18.16 / Alex Manea
0 Comments

A couple of weeks ago at the RSA security conference, I had the chance to speak with hundreds of customers and partners about how BlackBerry continues to evolve and advance its mobile security portfolio. Many were excited to try out the new PRIV smartphone and see how we developed the most secure Android device, while others wanted to learn more about the things that we do to protect iOS, Windows Phone and other Android devices. Coincidentally, the same day that I got back to the office, researchers reported a new set of vulnerabilities that can be used to bypass lock screens on iPhones and iPads running iOS 9. While Apple has denied the claim, our internal testing shows that it may have some validity. This is not the first time that such vulnerabilities have been discovered and will probably not be the last. So what's the best way to manage these risks, and how can BlackBerry help?

Containing the Threat

Corporate IT administrators would love to deploy end-to-end secure mobile devices across their entire environment, but in many cases this is simply not feasible. With the BYOD movement in full swing, some employees demand the ability to use their choice of smartphone and/or tablet. Mobile devices are among the most personal items that we own, and many of us are committed to a particular brand, be it BlackBerry, Android, iOS or Windows Phone. Despite all of this, IT administrators have a duty to protect corporate data from hackers, phishing scams, malware and a multitude of other threats. If you ever have doubts about how common or expensive large-scale data breaches have become, all you have to do is read the latest news.



The best way to protect corporate data in a multi-platform environment is to deploy a secure container. By effectively separating corporate data from personal applications and encrypting the data, IT administrators can protect corporate assets from device-level vulnerabilities. Some containers also provide their own encryption, adding an extra layer of security for devices where full-disk encryption is disabled or in cases where it might be compromised. Containers let users download apps to their heart's content and let IT sleep at night knowing that they cannot access the confidential corporate emails stored on the device.

Since the launch of BES10 back in 2013, BlackBerry has supported cross-platform Enterprise Mobility Management for iOS, Android and BlackBerry devices. In 2014 we launched BES12, now known as BlackBerry UEM (Unified Endpoint Manager), adding support for Windows Phone as well as

our legacy OS. In 2015, we launched the first ever BlackBerry Powered by Android, combining BlackBerry's hardware root of trust with the flexibility of Android for Work. And now with the BlackBerry Dynamics platform (formerly known as Good Dynamics), we're able to provide Mobile App Containerization, Mobile Device Management and Mobile Content Management across every major mobile device platform.

In talking to customers about BlackBerry Dynamics, one of the things we hear over and over is how much they love the consistent UX across multiple platforms. The common look and feel evokes a feeling of comfort and safety for users, knowing that their personal data and apps are isolated and inaccessible to their employer. And while usable security is unfortunately not as common as it needs to be, it is undeniably critical in order for users to accept and embrace solutions such as mobile data containers.

Defense in Depth

We recently discussed the importance of multi-factor authentication and the many ways that BlackBerry supports it. A secure container is fundamentally another factor of authentication and another layer of security, keeping the enterprise data safe even if the device passcode and/or encryption are compromised. Customers who use BlackBerry Dynamics can rest assured that their data is protected from all of the alleged iOS 9 vulnerabilities reported last week.

Over the past few years, BlackBerry has evolved from a company focused on building smartphones to the undisputed industry leader in cross-platform mobile security. In the past year alone, we've acquired WatchDox (now known as BlackBerry Workspaces), AtHoc, Good Technology and Encription, adding even more solutions to our already extensive security portfolio. The simple reality today is that even if you don't use a BlackBerry smartphone, there's a good chance that your mobile privacy and security are protected by BlackBerry.

You can learn more about how BlackBerry Dynamics delivers mobile productivity with certified security by viewing our archived webcast, Introducing BlackBerry Enterprise Mobility Suite. Be sure to also read The CIO's Guide to Enterprise Mobility and check out the official BlackBerry Enterprise Mobility Suite product page for webinars, demos and more.

Finally, if you're interested in learning more about how you can maximize your ROI in the current EMM landscape, sign up for our upcoming webinar, ***Making Sense of the EMM Alphabet Soup – a detailed look at MDM, MAM & MCM*** *on Tuesday, April 19, 2016 at 11:00 AM EDT.*