You Can Manage Mobile Applications Without MDM. Here's How (and When You Want To)

Mobile Security

08.02.17 / Chris Hazelton
0 Comments

What do employee personal devices (BYOD) and those owned by third-party contractors have in common? Simple – they often fall outside of traditional Mobile Device Management (MDM) based strategies. This can make it difficult to provide the people who use their own devices with the same access to corporate applications and data as those with MDM-overseen devices. To secure and enable unmanaged devices (those without MDM) you need to take a different approach – an app management approach.

App management is where BlackBerry excels – as evidenced by the fact that Gartner granted BlackBerry the top score in the Unmanaged Device (non-MDM) Support use case in Gartner's 2017 Critical Capabilities for Enterprise Mobility Management Report.

Why Unmanaged Device Support Matters

Traditionally, the power of EMM comes from installing MDM agent software or a separate enterprise user identity (profile) on an employee's device. This works well enough for corporate-owned, internally-managed devices. Third-party workers and BYOD each throw their own wrenches into the gears, however.

An external consultant may already have MDM installed on their smartphone or tablet – and you can't have two MDM software agents running at the same time. An employee who brings in their own device may take issue with the fact that standard MDM allows their employer to take inventory of apps unrelated to their job and view details such as the employee's location.

In both cases, your company needs to manage its applications and data without installing MDM software on these devices. You need to deliver rich collaboration to these workers, no matter who they are or who owns their devices. BlackBerry provides exactly that.

The Power of Mobile Application Management

Thanks to BlackBerry Dynamics, our mobile application development and management platform, you don't need to install MDM to secure and control enterprise mobile apps and content. Instead, you can manage data and access through applications and software containers. This approach to security is known as Mobile Application Management, and it's an area where BlackBerry tops the competition. This becomes even more important as companies deploy their own internally built custom apps.

According to Gartner, it's also functionality that's critical for IT departments:

"Mobile application management (MAM) continues to be the most important feature of EMM, with 79% of respondents reporting that the ability to deploy applications was the reason for buying an EMM," reads the Critical Capabilities report. "As use cases have expanded, so too has the number of mobile applications per device, with 97% of respondents using their EMM tools to deliver at least one app in-house or commercially."

How BlackBerry Leads the Pack for Unmanaged Device Support

BlackBerry Dynamics, offers application security at every level, protecting both applications and inter-app communication with containerization that's independent from the device. BlackBerry Dynamics' security has achieved Common Criteria EAL4+ certification – the highest internationally-recognized certification level under the Common Criteria program. This applies to all apps protected by Dynamics, including BlackBerry Work, 80+ ISV apps, and 4,000+ custom apps developed through the BlackBerry Dynamics SDK. Besides iOS and Android devices, BlackBerry can also bring this security to Windows 10 and macOS computers, allowing companies to secure connections to cloud resources without requiring a VPN or costly VDI deployments.

Additionally, BlackBerry UEM – a single-screen endpoint, content, and application management platform developed as an evolution of our BES MDM solution – works with BlackBerry Dynamics to provide MDM-less control of compliance and data loss prevention policies. With Dynamics and UEM, apps can be deployed and wiped with ease, allowing for efficient onboarding and offboarding of any users and devices, inside and outside an organization.

UEM also allows your organization to manage and deploy Office 365 apps alongside third-party apps, custom apps, and BlackBerry apps. This is a feature few other vendors currently offer. Again, it achieves this without requiring the installation of MDM software agents or profiles on end-user devices.

Lastly, with BlackBerry Workspaces, you can add yet another layer of security, taking direct control of your files – no matter where those files reside.

Secure, Manage, and Connect Your Apps and Workers through BlackBerry

MDM still has an important role in enterprise, but it isn't suitable for every use case. It can't give third-party workers secure access to the corporate resources they need to do their job, and its use on personal devices can raise several privacy concerns.

That's where BlackBerry comes in. Via solutions such as BlackBerry Work, BlackBerry Workspaces, and BlackBerry Dynamics, we excel at ensuring contractors and employees will always have access to rich collaboration and secure productivity. And we ensure that your business remains in control of its apps and data, no matter what devices they're on.

Support for unmanaged devices is not the only category in which BlackBerry received the top score from Gartner. BlackBerry is also a Leader in Gartner's EMM Magic Quadrant, and has the top scores in six out of six use cases in Gartner's *2016* Critical Capabilities for High-Security Mobility Management. *Be sure to also check out the blog on how we manage and secure devices and endpoints for enterprises in regulated industries, an area where we continue to excel.*

About Chris Hazelton

Chris Hazelton is Director, Product Marketing for Enterprise Software at BlackBerry. A former analyst at IDC and 451 Research, Chris has been working in management and security for enterprise endpoints for over 10 years.