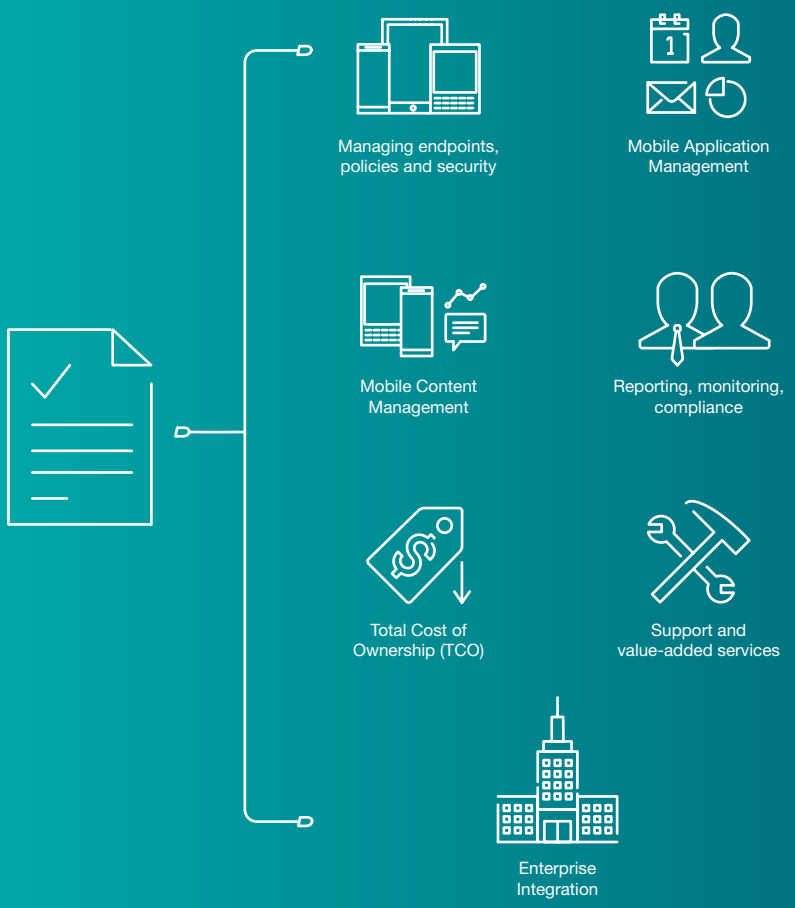
BlackBerry

White Paper

A UEM Checklist for CIOs

How to Choose a Unified Endpoint Management Solution

A UEM Checklist for CIOs



As you decide on a Unified Endpoint Management (UEM) solution, there are dozens, if not hundreds, of factors to weigh. Comparing features across three or four shortlisted solutions can become incredibly time-consuming.

As a starting point, consider the issues in the following list. It's derived from third-party research and best practices. While not exhaustive, it covers the critical areas you'll need to think through as you arrive at a decision.

Thinking about all the key factors will help you arrive at a solution that best fits your business.

Managing Devices, Policies and Security

When it comes to endpoint management and security, does the solution you're considering:

- ☐ Support the endpoints your employees want and need?
- ☐ Allow you to easily manage multiple devices per user?
- ☐ Control which applications are installed and provide protection against non-approved applications?
- ☐ Monitor/control access to web services and app stores?
- ☐ Detect policy violations (such as using data while roaming) and initiate action if required – e.g. disabling access?
- ☐ Restrict or prohibit access to your servers in case of policy violations?
- ☐ Allow IT to set user profiles for activation, SSO and proxy settings? Limit the number and type of devices?
- ☐ Set policy and controls based on device ownership model?
- ☐ Provide a streamlined deployment experience across multiple servers and domains?
- ☐ Enable advanced auditing of users and administrators?
- ☐ Provide remote log collection for advanced troubleshooting?
- ☐ Offer an enhanced custom enterprise app store?
- ☐ Allow automated enforcement of compliance policies?
- ☐ Provide a self-service portal for end-user device management tasks?

Managing Devices, Policies and Security

When it comes to endpoint management and security, does the solution you're considering:

- ☐ Control how endpoints connect to your corporate network (corporate Wi-Fi®, VPN, etc.)?
- ☐ Consolidate traffic through a single outbound port?
- ☐ Manage and deploy certificates?
- ☐ Allow users to connect securely to access resources behind your firewall?
- ☐ Provide Data Leak Prevention (DLP) by ensuring work content can't be exported to personal apps?
- ☐ Allow remote wipe – with the ability to choose what to wipe (corporate-only vs. total device wipe)?
- ☐ Let you enforce password use (so that you can control the complexity and rotation)?
- ☐ Let you specify how long a device can be inactive before it automatically locks?
- ☐ Enable certificate-based authentication?
- ☐ Allow you to monitor/enforce what's in use – e.g. operating systems and versions, installed applications, latest patches and critical updates?
- ☐ Detect jailbreaking and rooting on iOS®, Android™ and Windows® Phone devices?
- ☐ Control, automatically, what happens next when devices are found to be non-compliant?
- ☐ Give you control over how corporate apps are managed on personal devices (and vice versa, if required)?

Managing Devices, Policies and Security

You also need the details on the solution's:

- ☐ Third-party security approvals and certifications – e.g. Federal Information Processing Standard [FIPS] 140-2
- ☐ Interaction with your corporate firewall and antivirus software
- ☐ VPN requirements and capabilities
- ☐ Message archiving capabilities, for compliance, audit trails and reporting
- ☐ Containerization approach (there are five main strategies – which one best suits your security requirements?)
- ☐ Ability to provide out-of-the-box access to corporate email, GAL, PIM, Intranet and apps
- ☐ Ability to securely deploy and manage custom and/or third-party apps

Zooming out to look at the bigger security picture, you'll want to determine whether the solution will:

- ☐ Safely enable all the ownership model scenarios you may need it to – e.g. BYOD, COPE, CYOD (Choose Your Own Device)
- ☐ Support all the user segments/groups in your organization (versus a one-size-fits-all security approach)
- ☐ Allow your organization to comply with any and all regulations or government legislation (if applicable)
- ☐ Allow you to manage your entire UEM environment through a single, unified console

Mobile Application Management

Organizations that see the strategic, long-term value in mobility know that the real advantages are in apps.

On the subject of apps and data containerization, does the solution:

- ☐ Containerize each corporate app to encrypt app data?
- ☐ Provide validated app-level encryption (e.g. FIPS)?
- ☐ Require authentication to access containerized apps and encrypted data?
- ☐ Restrict personal apps from accessing containerized data?
- ☐ Allow selective wipe of apps and data?
- ☐ Enable users to define the configuration of the springboard for app launching, for an optimal user experience?
- ☐ Offer an SDK for integrating security capabilities directly into code? Are reference implementations available?
- ☐ Provide support for native apps, hybrid apps and web apps? Does it provide secure network connectivity, including:
  - ☐ A scalable access model?
  - ☐ Strong encryption over the air (OTA)?
  - ☐ No impact on your firewall (no open inbound ports through which devices authenticate or request direct access)?
  - ☐ No requirement to upgrade your existing network or VPN infrastructure?

When it comes to app-specific policies, does it allow you to centrally manage the following?

- ☐ Password/authentication policies?
- ☐ Restrict/allow Open in and Copy/Paste between applications?
- ☐ Jailbreak/root detection check on app access?
- ☐ Compliance policies for device and app configuration/versions?
- ☐ Automated actions based on compliance status?
- ☐ Allow/deny offline access?
- ☐ Dynamic policies changeable from central console?
- ☐ Lock and wipe of app container?

Mobile Application Management

Does the solution support convenient app distribution, by enabling:

- ☐ Role-based access to relevant apps?
- ☐ A unified view of commercial and in-house developed apps?
- ☐ App reviews and recommendations?
- ☐ Entitlement based on group membership?
- ☐ Access for non-employees in the extended enterprise?
- ☐ Are users able to access corporate apps through single sign-on (SSO)?
  - ☐ Can a single login enable across approved app containers?
  - ☐ Are administrators able to define which apps can be part of SSO authentication?
  - ☐ Can authentication permit SSO across multiple apps in multi-app workflows?

Additional app management considerations:

- ☐ Does the service interaction model allow you to connect apps?
- ☐ Does it enable secured communication between apps and other apps or shared services?
- ☐ Does the solution allow tracking and reporting on app entitlements and apps downloaded? Tracking and reporting on actual app usage? Can you compare apps side-by-side?
- ☐ Does it support high availability and fault-tolerant configurations?
- ☐ Does it offer enterprise directory integration?
- ☐ Does the platform provide built-in ISV support with app security verification?
- ☐ Are integrated ISV apps available on public app stores?

Mobile Content Management

Now more than ever, Mobile Content Management (MCM) is critical to everyday business. With critical files leaving your repositories all the time, can the solution help your IT team maintain control and trackability?

Does the solution allow:

- ☐ Secure connectivity and access to shared network drives behind the firewall and to Microsoft SharePoint repositories?
- ☐ Segregation of all work content from personal apps and data?
- ☐ Secure browsing of intranet and other content behind the firewall?
- ☐ Automatic encryption of email attachments that employees can open and modify on-the-go?
- ☐ Setting of content download restrictions? (e.g. for roaming)

Does it enable end users to:

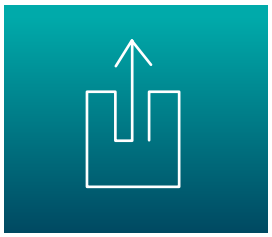
- ☐ Manage files and workspaces with consumer-like usability?
- ☐ Work from anywhere with files always in sync?
- ☐ Access, synchronize, share and control files on all platforms: web, mobile (iOS, Android™, BlackBerry® 10), and desktop (Windows®, Mac®)?
- ☐ Access, create, annotate (highlight, comment, draw, erase), edit, search (folders, files and content), stream and share files through integrated mobile applications?
- ☐ Share files with anyone (internal and external), anywhere, on any device, without losing visibility or control.
- ☐ Share extremely large files with colleagues, partners and third parties easily?
- ☐ Control the ability to access, view, edit, copy, print, download and forward files?
- ☐ Apply custom, administrative watermarks or use the spotlight feature to deter screenshots and increase accountability?
- ☐ Track, revoke, wipe or expire file access at any time - even after the document has been downloaded or shared?

Mobile Content Management

To satisfy IT and security requirements, does it provide:

- ☐ Data protection, keeping sensitive data encrypted and controlled by default, reducing the risk of a breach or loss of intellectual property?
- ☐ Enterprise-level security, including mobile passcode, jailbreak detection, remote document control, full tracking, always-on AES-256 encryption (in transit, at rest, and in use) and advanced key management?
- ☐ Visibility into how users are accessing sensitive data and what they do with it, maintaining an audit trail?
- ☐ Flexible deployment options: cloud, on-premises or a hybrid?
- ☐ Seamless integration with enterprise systems, including Outlook®, SharePoint®, Salesforce.com®, custom web portals, proprietary applications and other content repositories?

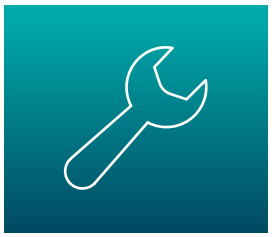
Scalability



Some solutions make it much easier than others to roll out and sustain enterprise-sized deployments.

- ☐ How many endpoints can be added per domain?
- ☐ Does the solution include high-availability and disaster-recovery options?
- ☐ Does the vendor provide published scalability benchmarks?

Implementation



Is the solution flexible enough to meet your needs? For example:

- ☐ Does it come in both on-premises and cloud (SaaS) versions?
- ☐ How hard will it be to get up and running? What support can you access if you need or want help at the deployment stage – or even earlier, as you plan your migration?
- ☐ Are the licensing options appropriate for your needs?
- ☐ Does it come from a vendor you know and trust?

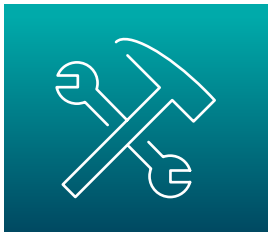
Total Cost of Ownership (TCO)

Along with ROI, it's one of the items at the top of every CIO's list of priorities when it comes to UEM.

Does the solution:

- ☐ Allow you to leverage your existing investment in mobility technology?
- ☐ Allow the scalability you may need?
- ☐ Provide proven technical support to ensure maximum uptime and fast-issue resolution? (see more on support below)
- ☐ Fit with your IT help-desk strategies and capabilities?

Support and Value-Added Services



Does the solution:

- ☐ Include full end-to-end support (rather than limited help-desk support only)?
- ☐ Offer users a self-service portal, to lighten the load on IT and your help desk while empowering employees?
- ☐ Provide support for all the endpoints under management, as well as the solution itself?
- ☐ Flex to fit with your unique needs?
- ☐ Integrate with existing and/or new enterprise services you have or may require in the near future?
- ☐ Have global reach to support any and all relevant languages, locations and remote workers?
- ☐ Come with flexible options to support your migration planning, implementation, and post-install ramp up?

Enterprise Integration

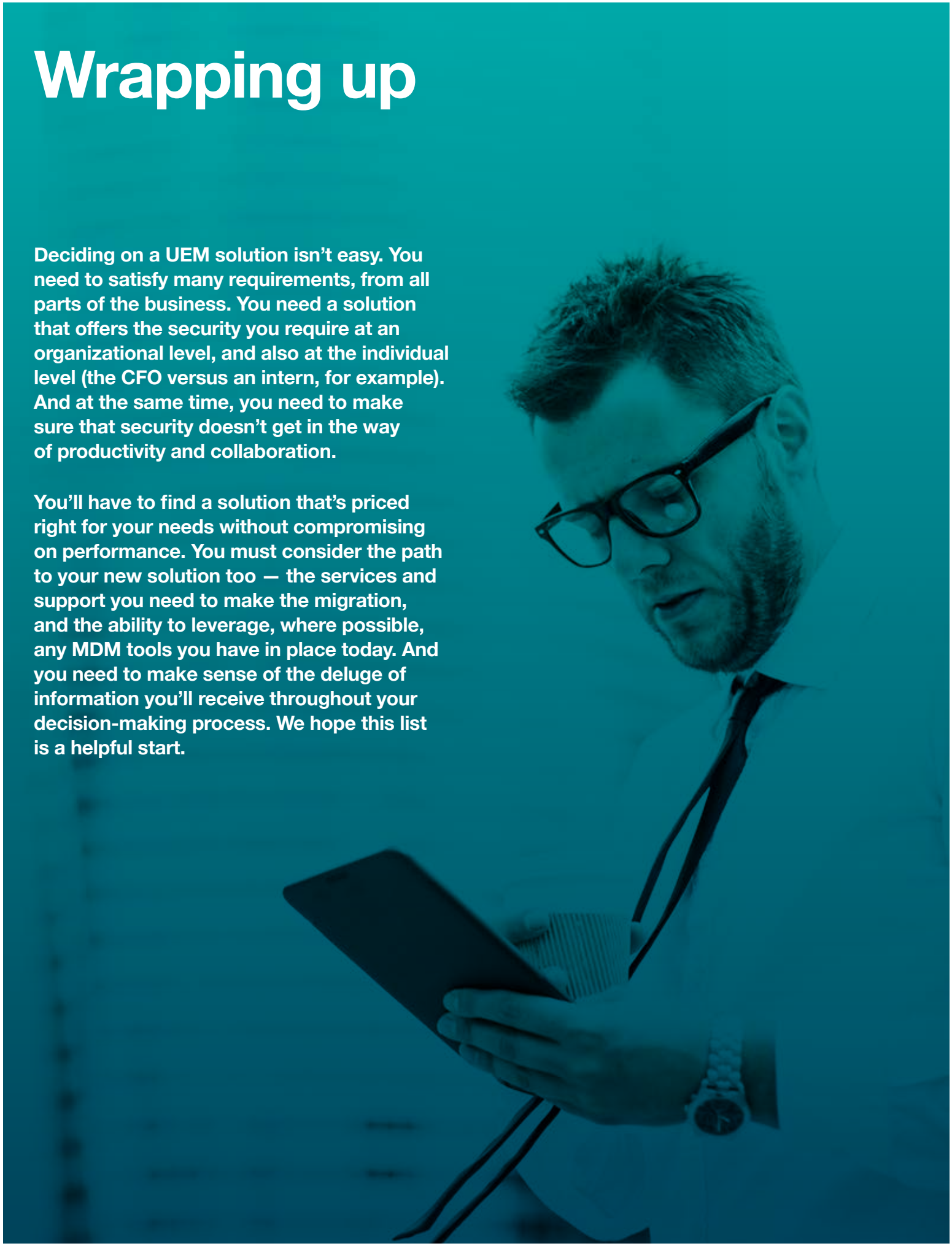
Does the solution provide:

- ☐ System health diagnostics?
- ☐ End-to-end secure integration of third-party mobile solutions?
- ☐ Mobile device auditing and archiving integration?

Wrapping up

Deciding on a UEM solution isn't easy. You need to satisfy many requirements, from all parts of the business. You need a solution that offers the security you require at an organizational level, and also at the individual level (the CFO versus an intern, for example). And at the same time, you need to make sure that security doesn't get in the way of productivity and collaboration.

You'll have to find a solution that's priced right for your needs without compromising on performance. You must consider the path to your new solution too — the services and support you need to make the migration, and the ability to leverage, where possible, any MDM tools you have in place today. And you need to make sense of the deluge of information you'll receive throughout your decision-making process. We hope this list is a helpful start.



BlackBerry Unified Endpoint Manager (UEM)

BlackBerry UEM delivers complete, unified endpoint management and policy control for your diverse and growing fleet of devices and apps. With its single management console and trusted end-to-end security model, BlackBerry UEM is designed to help you increase the productivity of your mobile workforce while ensuring the full protection of your business data.

BlackBerry® UEM, part of the BlackBerry® Enterprise Mobility Suite, allows you to securely manage your key devices (including iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry®) and support all device ownership models.

BlackBerry Dynamics, managed by BlackBerry UEM, extends access to best-in-class secure mobile app development and containerization, enabling multi-OS support for a wide range of collaboration, line of business (LOB), third-party and custom-built secure apps.

BlackBerry UEM can be deployed on premises or in the cloud, depending on your business needs and preferences.

BlackBerry Enterprise Mobility Suite

BlackBerry
Enterprise Mobility Suite

Wherever you are on your mobile journey, the BlackBerry Enterprise Mobility Suite has a solution to protect your organization's data and boost your workforce productivity. Whether you're just starting to say yes to mobile devices or mobilizing critical business content, the BlackBerry Enterprise Mobility Suite offers a range of editions including designed to meet your evolving needs.

The BlackBerry Enterprise Mobility Suite delivers secure, consistent management policies and controls across operating systems and device ownership models. No matter which edition you choose, your enterprise data will be safeguarded by the industry leader in mobile security, trusted by organizations with the highest security requirements. Your employees can easily access a broad range of apps and intranet resources, wherever and whenever, while your organization maintains full control of its data.

To learn more, visit www.blackberry.com/enterprise