BlackBerry

White Paper

The CIO's Guide to UEM

10 Critical Decision Points

How to Use this Guide

Based on real-world research input from Fortune 500 companies, and insights from mobility analysts and experts, this guide is designed to help CIOs reimagine their strategy for a new era of mobility.

Mobility is reaching an inflection point in enterprise. Not long ago, many organizations looked at it as an isolated project through which IT could enable email on mobile devices. Now, most see it as a strategic initiative for mobilizing business apps that can impact a range of outcomes. With this shift, smart enterprises are moving away from tactical point solutions for mobile device management, looking instead for a secure, comprehensive, unified and future-proof mobile-app platform.

Enterprise applications, many of them cloud based, are now at the heart of mobile productivity, because mobile workers require access to information anytime, anywhere and from any device. Traditional security perimeters are shifting as sensitive documents are regularly shared outside the walls of the enterprise. Data may now reside on and move between mobile devices; desktops and laptops; public, private, and even personal clouds.

These changes offer a clear opportunity to boost productivity and job satisfaction, improve customer engagement, and increase organizational efficiency. But in order to take advantage of these benefits, enterprises must be ready to overcome the challenges mobilization brings with it.

Acronyms change quickly in mobility, and while yesterday's focus was on MDM, and then EMM, enterprises today are seeking solutions for Unified Endpoint Management, or UEM, which encompasses management, security and identity across mobile devices as well as desktops, laptops and other endpoints. As organizations prepare for a growing range of end user and Internet of Things requirements, it's critical that they can maintain visibility and control across their endpoint environments from a unified platform.

Enterprises that develop a mobile strategy and implement the right solution can expect significant benefits, as can those that update their existing strategy to keep pace with the evolving enterprise mobility landscape. The right solution improves productivity, security, and privacy, while making it easier for IT administrators to manage the growing number of roles, apps, operating systems and device types.

While this document covers many of the key factors to consider as you form or re-form your mobility strategy, there are many more which depend on the unique qualities of your organization. Though the process can be time-consuming and occasionally political, working out the answers before you decide on a new solution will save time, reduce costs, and prevent headaches every step of the way.

Mobility is a journey, and to begin, it's useful to understand where your organization falls on the mobile maturity curve. This will help ensure that the solution you choose meets your needs today, tomorrow and well into the future.

Why You Need a Mobile Strategy

A mobile strategy is a plan that lists and describes your company's key requirements and positions on a wide range of mobility issues. The purpose is to gather input from all stakeholders to create a strategy that supports the goals of the business without compromising on security or privacy. Without a mobile strategy, making the right decision on a long-term solution can be next to impossible. Here are some of the key questions enterprises are asking, depending on their stage in the mobile maturity curve.

1. What kinds of mobile apps do we need to roll out to leverage mobility and improve productivity in our organization?

2. How confident are we when it comes to the security of business data — including that of our customers/clients — in an increasingly mobile and cloud-oriented environment?

3. Are we able to accurately forecast IT expenses around mobility? Do we have a solution that can meet our needs today and tomorrow?

4. How confident are we when it comes to the security of not only our business data, but also the application credentials and user configurations that may be stored on mobile devices?

5. How do we help app owners, app developers, and IT to work together to respect a common security baseline?

6. How do we ensure different development teams are able to apply the same security capabilities across all app types?

7. How will we address continued growth in users, devices and data as mobile becomes a bigger part of the business?

8. How easy is it to meet our compliance or security requirements?

9. What advantages could we gain by reducing the number of vendors and solutions in our mobility environment?

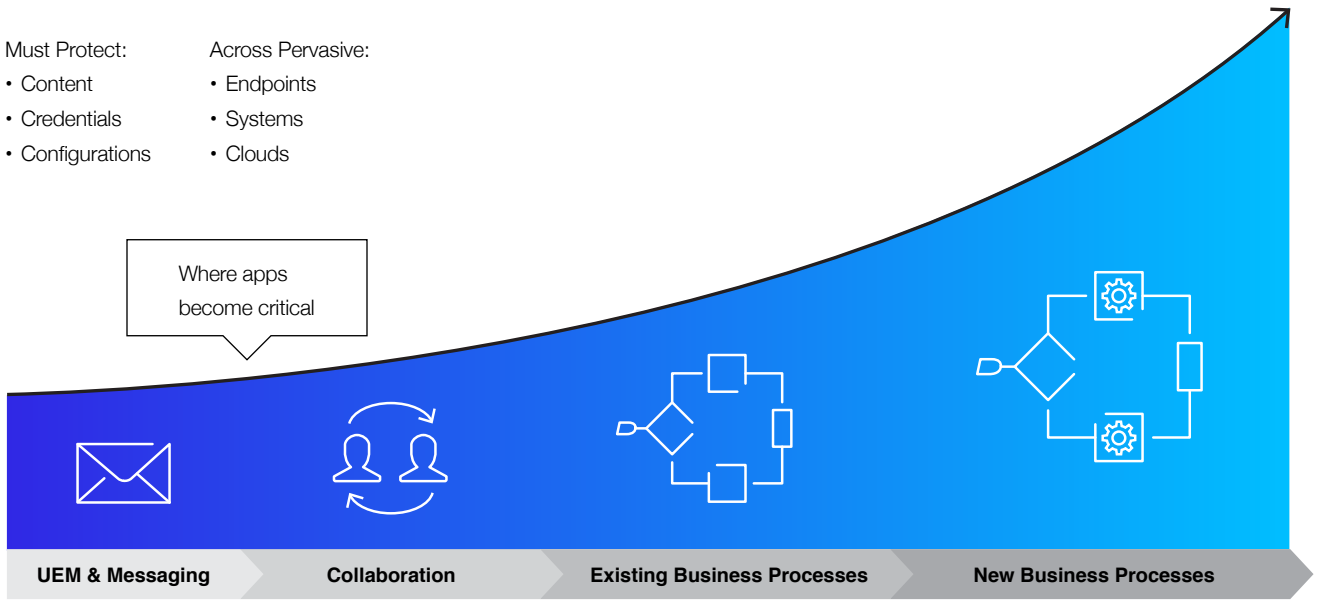
10. How successfully are we addressing our employees' trust and privacy issues?

The Mobile Maturity Curve

There are four general stages to the mobile maturity curve. As your business accelerates along the curve, your mobile approach will become gradually more transformative as you adopt new strategies, incorporate new tools, modify existing business processes, and eventually create entirely new business models.

At the same time, security requirements increase as more and more corporate applications become mobilized.

The Mobility Maturity Curve, Visualized



Basic Mobility

Basic endpoint management and email are often the first investments organizations make. Doing so can generate quick productivity gains with limited investment, particularly when coupled with a BYOD initiative. However, managing a diverse mobile fleet can open the organization to new threats.

Challenges in this stage

- Starting to secure basic corporate data (email, attachments) on mobile devices
- Understanding how devices are being used
- Establishing technical expertise in-house

Signs your business is at this stage

- You've only recently implemented a device management solution. Investment in mobility is typically minimal. It's a project, not a companywide initiative
- Mobile app development is not yet on your radar
- You understand that mobility is critical to your business objectives, but aren't sure where to start

Mobile Collaboration

Once an organization's users start getting mobile email and attachments, they naturally want to do more, and the productivity opportunities that mobility offers become harder to ignore. So, once your business has made a start with mobility, the next step is to further enable employees through better collaboration and workflow optimization. Most MDM-only platforms lack the necessary tools to secure mobile applications and protect business data.

Challenges in this stage

- Mobilizing the key Microsoft® applications that employees rely on: Exchange, Office 365, SharePoint™, OneDrive for Business, Skype for Business, Dynamics CRM, etc.
- Implementing document workflows with security and control
- Ensuring a positive mobile-user experience
- Protecting employee privacy

Signs your business is at this stage

- Investment in mobility is still minimal to moderate
- You're mobilizing horizontal business apps related to collaboration, such as SharePoint and enterprise instant messaging (EIM)
- You're increasingly concerned about data leakage as more business apps are deployed
- Lines of Business (LOBs) are starting to ask for more role-based, specific applications to improve business outcomes

Mobilizing Existing Business Processes

By now, teams are used to working together from just about anywhere through the core collaboration and communication tools you've mobilized, and again, decision makers, particularly on the LOB side, will be encouraging IT to go further still. The next stage of the mobility curve is the large-scale mobilization of your organization's existing business processes and critical applications. Typically, it's during this stage that organizations identify gaps in their app inventory and begin looking into developing their own custom, internal mobile apps.

Challenges in this stage

- Aligning mobile apps and initiatives with existing business processes and identifying gaps to fill with custom projects
- The emergence of new forms of data, or new uses for existing data
- Incorporating mobile applications or application processing into existing infrastructure
- Continuing to adhere to corporate security policy and industry regulations, particularly with regard to customer and other regulated data

Signs your business is at this stage

- Your move to collaboration apps is well-received across your business, and users are demanding more apps to get their jobs done
- You've begun mobilizing existing business processes, or are planning your future mobile investments
- Investment in mobility is moderate
- You've started deploying applications to support priority business roles in your organization, such as sales, executives, field forces, etc.
- You're planning to start developing internal applications in the near future
- You're identifying gaps to fill with custom apps across devices, operating systems, and clouds
- You've implemented a platform that lets you manage the three Cs of secure mobility: Corporate content, user credentials, and application configurations

Emergence of New Business Processes

Finally, once you've mobilized existing business processes, the next phase is about business transformation — using mobility for competitive advantage (including cost savings, customer-experience improvements, and new revenue opportunities). This is the point at which your mobile ROI is maximized, and mobility is pervasive throughout your organization. A business typically becomes flooded by mobile applications — often hundreds of them. Mobile devices become so widespread that managing single devices and applications is highly inefficient and often inconsistent from a security standpoint. You've entered into a stage of pervasive mobile computing, whereby corporate data is now on phones, tablets, PCs, and wearables, on back-end systems, clouds, even personal clouds. Digital Rights Management capabilities (DRM) for file-level security policies are needed to provide security, discovery and containment.

Challenges in this stage

- Managing a large volume of enterprise applications across devices, operating systems and clouds
- Developing a back end to support new mobile applications, business models, and devices
- Leveraging enterprise identity stores and authentication schemes to support single sign on, even to cloud services
- Aligning mobile app development with existing business needs

Signs your business is at this stage

- Your endpoint management solution is part of a larger approach to mobile management
- You're looking for a way to manage data, documents, and roles in addition to applications and devices
- You've begun deploying custom, internal applications
- Investment in mobility is typically moderate to high
- Your organization is being disrupted by new business models and is now maximizing its return on mobility investment

Seven Top Mobility Pain Points

1. **The need for real security across corporate content, application credentials, and device configuration data, and the need to protect against data leakage.**

2. **The need to address both current and evolving business needs such as new applications while integrating UEM with key business systems and processes.**

3. **The need for a security solution that doesn't hinder employees and drive them to find workarounds.**

4. **The rise of cloud computing, and the difficulties associated with securing files across both cloud applications and mobile devices.**

5. **Inconsistent security models across applications due to different development technologies (for native apps, HTML5, hybrid development environments, etc.)**

6. **Scaling of mobile management infrastructure to respond to evolving business needs.**

7. **The difficulties associated with providing mobile tech support for an entire enterprise.**

Key Factors in Making a UEM Platform Decision

Once you're able to locate your position on the mobile maturity curve, it's easier to identify the kinds of issues you need to solve in the near term — and you can also take a longer view to make sure the solution you choose will support your goals well into the future.

The list that follows is not exhaustive, but will provide you with an overview of top factors to consider. If your stakeholders can all understand and agree on the importance of these issues, then you'll be well on your way to forming an appropriate solution shortlist.

1. Cross-platform endpoint management
2. Mobile application security and management
3. Security certifications and credentials
4. User privacy protection
5. Document control
6. Deployment model (cloud or on premises)
7. Migration and implementation
8. Technical support
9. Training and user features
10. Pricing and total cost of ownership (TCO)

1. Cross-Platform Endpoint Management

Whether the devices are bring your own (BYO) or corporate-owned, managed by your IT department or not, chances are your work environment already involves multiple mobile operating systems and device types. You need to make sure your UEM solution can manage those devices in all the ways you require, across every use case and role, including business users, remote workers, highly-sensitive users, shared devices, desktop systems and kiosks. Consider not only the platforms you use today, but those you might want to use in the future, including capabilities such as Android™ for Work, Samsung Knox Workspace, and iOS Managed Apps.

From a day-to-day management perspective, the platform you choose should allow IT administrators to manage everything — user groups, administrative roles, software configurations, email profiles, IT policies and more — from one unified console. And given that IT has enough on its plate without the challenges of learning an entirely new management paradigm, a user-friendly, intuitive interface is critical.

Among other factors to weigh in UEM, you need to understand whether the solution will:

Simplify user setup and enrollment, by allowing users to quickly self enroll over-the-air. Streamlining the enrollment process increases user satisfaction while driving down mobile support costs.

Enable rich policy controls. You need the ability to define and deploy all the right policies for your organization, spanning passwords, device encryption, camera, Wi-Fi®, VPN, and more. Should a device be lost, stolen, retired or replaced, you need the ability to wipe business data without impacting personal content or apps.

Support regulatory compliance or high-security requirements: Organizations in regulated industries, such as financial services, healthcare, law, and government, must comply with stipulations governing the security of customer, financial, and other data. For many organizations, supporting these ever-growing mobile security requirements takes up valuable time and energy. Your UEM solution must be compliance-ready by design. Check for a list of security certifications and accreditations to see how solutions address your specific needs.

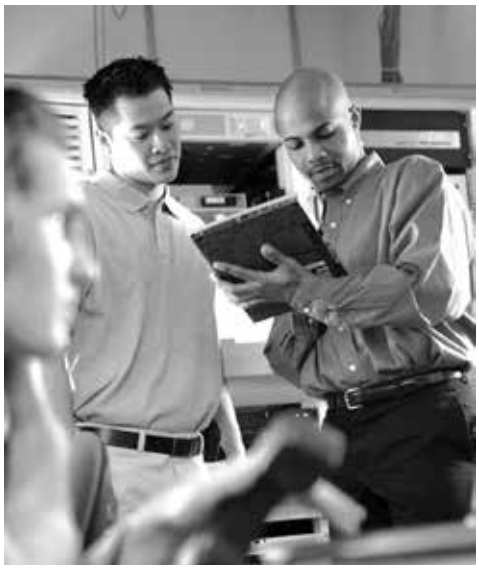
Detect jailbreak/rooting: For end users, rooting or jailbreaking a device can be tempting, as it offers more freedom to customize how their smartphone or tablet functions. At the same time, it represents a considerable security risk, as the process involves disabling an operating system's built-in security protections. This opens a device to a wide range of malware and targeted attacks. It's therefore important that your UEM solution includes a means of detecting jailbroken devices, and defeating jailbreak jammers — software used to camouflage a device's rooted status. Further, jailbreak and root detection should not be reliant on location services to trigger a test, which drains battery life and impacts user privacy.

2. Mobile Application Security and Management

Security through containerization

Containerized apps provide IT with fine control by segregating each app and its data in its own dedicated, encrypted file store. Each app container can have its own usage rules or policies, and can be protected and wiped independently. Personal apps installed by the device owner can reside safely alongside corporate-approved, third-party ISV apps or custom-built apps that interact with the intellectual property of the enterprise. Because personal apps are isolated from corporate apps, they can be restricted from accessing the data in the corporate app containers (using native services such as copy and paste, for example). Yet users can still arrange both corporate and personal apps side-by-side or in any springboard configuration they desire.

If your UEM solution provider offers appropriate Software Development Kits (SDKs), you can integrate security libraries directly into app source code before compilation. While this method of containerization requires source code access and developers to do the coding, SDKs can potentially provide productivity benefits to developers and to the enterprise. They can also enable developers to integrate new app features beyond just security capabilities, such as High Availability and Disaster Recovery services or even turnkey features to add to apps, such as user presence or printing.



At minimum, any containerizing solution should provide:

App authorization — (i.e., only allow the provisioning of an app to an authorized user's device).

App-level encryption — Using app-level encryption, independent from device-level encryption, means that even if a device passcode is compromised, the app data is still protected.

App authentication — Enable app-level password authentication with advanced options as needed, such as support for two-factor authentication.

Single sign on — Allow users to log in to one containerized app and gain access to all containerized apps, for a faster, smoother user experience.

Broad security policies — For example: strong passwords, data-loss prevention ("open in", cut/copy/paste, file content management), and compliance controls (remote lock/wipe, detect jailbroken/rooted devices, enforce OS version).

Secure access — To behind-the-firewall servers and other resources, that didn't require open inbound firewall ports or unnecessary exposure of the corporate network.

Digital Rights Management (DRM) — File-level security policies to protect corporate content as it moves across devices, systems and clouds.

Deploying and Managing Apps

With the right solution for mobile application management (MAM), IT can provide employees and business partners the application and data access their roles require, on their preferred and personally owned devices, without having to take restrictive control of those devices to meet security and regulatory requirements.

Importantly, MAM policies and technologies can limit data deletion to selective wiping of specific enterprise apps and their data, leaving the rest of the device's personal content intact. This way, mobility can be used as a true business enabler without compromising the user's whole device experience for the sake of corporate data security.

A corporate-brandable, private enterprise app store can provide a one-stop shop for distributing custom built or curated apps to employees and authorized members of the extended enterprise (e.g., contractors, ecosystem partners, etc.) — even when your IT admins don't manage the endpoint. This way, you can provide users with a consumer-like experience that's consistent across platforms, but with enterprise controls.

Some solutions also include graphical dashboards to provide a detailed view of app adoption across the enterprise. This allows you to zoom in on metrics such as registered enterprise app store users, number of apps in play, app distribution across OS platform, most popular apps and more.

Consider the Full Mobile App Lifecycle

Your EMM solution should provide a framework for security and manageability for the entire app lifecycle, reflecting:

- **App development and procurement (both third-party and in-house developed apps)**
- **App provisioning and deployment**
- **App security and policy management**
- **App usage and user feedback**
- **App decommissioning and selective data wipe**

The following features are signs that you're on the right track:

- **Single-sign-on functionality, allowing users to only authenticate once in order to gain access to content across apps**
- **Encryption of data shared between apps, and in use by apps, no matter whether on-device, behind the firewall or in the cloud**
- **Easy containerization of any application**
- **An SDK that allows developers to take advantage of advanced functionality such as app-to-app secure document sharing, or a shared services framework for easily adding common features without writing new code**

3. Security Certifications and Credentials

What sort of security certifications do your shortlisted UEM platforms have? What about the vendors? Depending on your industry, you may be required by law to seek a platform that can support your HIPAA, HITECH, GLBA, FISMA or other security requirements.

Also pay attention to which organizations, analysts, customers and industries speak favorably of each platform. Most customers claim to have great security and boast about a checklist of features — but only the organizations with third-party validation can actually back up those claims. Have they made the investment in time and resources to prove security is truly robust enough for your needs?

Mobile apps provide an open avenue for data leakage when employees send business data to personal cloud storage tools, personal email accounts and even perform device backups to personal computers. But mobile security involves more than just the protection of business data in transit or at rest on devices. Organizations also need to make sure they're securing the configuration details and user credentials that may be stored on mobile devices. Unprotected, they can create entryways that put your network and core business applications at risk. Securing the device alone doesn't prevent business data loss. You have to safeguard the three Cs of mobile security: content, credentials and configuration.

4. User-Privacy Protection

With the rise of BYOD, enterprises have become increasingly aware of sensitivities and potential liabilities in how they manage employees' personal devices and information. Employees want privacy for the same reasons organizations want security. What's theirs is theirs, and it needs to stay that way.

Further, anti-discrimination laws in some countries can make accessing a device app inventory or geo-location information potential grounds for a wrongful termination lawsuit.

One of the most important examples of privacy infringement you might face is when you fully wipe an employee's personally owned device because your business data is at risk (e.g., due to a lost/stolen device or employee departure).

You also need to be aware that requiring location services to enforce compliance (which can also drain batteries), or storing phone/location logs are potential infringements on employee privacy.

Look for a solution that will help build trust by protecting not only your sensitive business data, but also your workers' personal content, across operating systems, no matter who owns the device.

5. Document Control

File sharing — especially via mobile devices — has become an essential part of enterprise collaboration. As enterprises mobilize business processes, more and more sensitive data pass through and reside on mobile devices.

Files containing sensitive material such as intellectual property, financial data, and regulated information are therefore inherently at risk if left unsecured. This is true regardless of whether they're shared within the walls of your organization or with a third-party contractor. Consider a recent study by The Ponemon Institute[1], in which 61% of employees admitted to sending unencrypted emails, failing to delete confidential documents, or accidentally forwarding sensitive data to unauthorized recipients.

In order to prevent regulated or business-critical data from falling into the wrong hands, you need to protect your documents directly. Seek a UEM platform that offers a secure enterprise file synchronization and sharing (EFSS) solution with DRM (Digital Rights Management) capabilities to add file-level security policies, or one which integrates readily with such a tool. And in regulated industries, you'll need document tracking for auditing and compliance purposes, as well.

6. Deployment Model (Cloud or On Premises)

Many endpoint management solutions are available in both cloud (also known as Software as a Service, or SaaS) and on-premises versions. There are advantages to each model. Among the factors that may play into your decision:

Deployment time: Cloud-based solutions can often be up and running very quickly.

Maintenance: Cloud-based solutions can lighten the load on IT when it comes to updates and upgrades, which is especially helpful for businesses with limited technical resources in house.

Access and control: An on-premises solution sits server-side in your datacenter. For some IT organizations, this provides a greater amount of control over data and disaster recovery, and tighter integration with other systems.

Compliance: For some high-security or regulated organizations (branches of government or the military, for example), regulations may make implementing an on-premises solution an easier choice — although as cloud deployments (and IT perceptions about them) evolve, this too is changing.

Ideally, your UEM solution will make both deployment options available to you, with no need to compromise on security or features however you choose to go forward, even if you need different models in different locations.

7. Migration and Implementation

Migrating to any new platform requires a commitment of time and resources. But the process doesn't have to be stressful. Choosing the right approach is critical — you want to be up and running with as few interruptions to employees as possible.

Your UEM strategy needs to account for this process. What resources do you need and where will these come from? Typical enterprise customers have thousands of endpoints operating on different continents, from multiple offices around the world.

You need to have a transition plan for the migration phase, a schedule for these migrations and a training plan for both IT and end users.

8. Technical Support

You rely on your mobile platform — to speed up decision making, boost revenue and profit, facilitate workflow, and keep users, teams, customers and suppliers connected. It's business critical. So when you're choosing your UEM solution, ensuring that the vendor offers the support capabilities and options you need makes smart business sense. Find out exactly what's available, at what cost, to support your needs in planning, implementation, optimization and ongoing issue resolution. Otherwise, you're jeopardizing the gains that your UEM investment is meant to achieve in the first place.

9. Training and User Features

What training support will you need, how will you access it, and at what cost? The easier your UEM solution is for IT and for end users to interact with (both for initial provisioning and ongoing management), the less time you'll need for training — so be sure to find out what each potential vendor has done to streamline and simplify processes for these two key stakeholder groups.

10. Pricing and Total Cost of Ownership (TCO)

Migrating to a single, unified endpoint management platform will help your organization standardize infrastructure, reduce complexity and increase ROI.

Be sure your solution can offer cost-effective and flexible mobility that can scale up or down as your needs change over time. Insist on specifics when it comes to the number of devices you can add per domain. Consider payment terms, too; if the idea of eliminating a heavy upfront capital expenditure is appealing, you may prefer a subscription model for more predictable yearly operating expenses. Spreading out costs in this way can be helpful for cash flow.

Lastly, to get to a full picture of TCO, you need to consider direct and indirect costs. As you continue to move along the mobile maturity curve, reliability becomes increasingly mission critical.

Best-in-class Mobility Through the BlackBerry Enterprise Mobility Suite

BlackBerry
Enterprise Mobility Suite

With the BlackBerry Enterprise Mobility Suite®, enterprises can say yes to their users' and business leaders' demands for anytime, anywhere productivity through secure mobile apps, and benefit from consistent multi-platform policies and controls — across iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry® — no matter the device ownership model or the user groups being mobilized.

The BlackBerry® Enterprise Mobility Suite:

- Provides a turnkey solution for rolling out collaboration, line of business and custom apps, while protecting your business and your employees' privacy, by providing consistent containerization and security policies across operating systems to keep work and personal content separate.
- Provides the tools, APIs, infrastructure and software development kits (SDKs) for app development to ensure consistent security across devices and operating systems.
- Has passed rigorous third-party testing including Common Criteria security certification for app management and the underlying app security platform, making it the solution of choice for insurance, finance, legal, aerospace, defense, military and all manner of other security-conscious organizations.
- Can offer precise controls over content by embedding Digital Rights Management (DRM) protection in your files so that they stay secure and trackable at all times, even after files are downloaded and shared with third parties.
- Is flexible enough to cost-effectively address your needs as they change — so you can grow into new capabilities over time without disruption or rip-and-replace.
- Supports organizations that must meet the highest security requirements and/or achieve regulatory compliance in mobility. BlackBerry enterprise solutions support:
  - 16 of the G20 governments
  - The top 10 largest law firms
  - 5 out of 5 of the largest oil and gas businesses
  - Over half of the Fortune 100, including all of the F100 commercial banks

The BlackBerry Enterprise Mobility Suite Delivers the Right Capabilities to Support Your Mobile and Productivity Needs

Management Edition

For organizations that need device-level control and management, the Management Edition offers BlackBerry® UEM, a complete, cross-platform and highly secure unified endpoint management solution.

Enterprise Edition

For organizations that require some collaboration capabilities in addition to a UEM solution, the Enterprise Edition allows you to mobilize Microsoft® Exchange with a business class user experience, while ensuring end-to-end security and protecting corporate data.

Collaboration Edition

For organizations ready to capitalize on advanced mobile productivity, the Collaboration Edition securely mobilizes your Microsoft applications — Exchange, Office 365, Office, SharePoint, Skype for Business — and other key applications (such as CRM) through a leading-app ecosystem.

Application Edition

Organizations that are already leveraging advanced endpoint management capabilities, along with collaboration and third-party business apps, can take the next step by developing their own custom apps to enable a wider range of business processes. The Application Edition delivers a full platform for app security, development and deployment.

Content Edition

For organizations that want to add full content security to their UEM capabilities and their wide range of custom and third-party applications, the Content Edition includes BlackBerry Workspaces, the leading secure Enterprise File Synchronization and Sharing (EFSS) solution. Workspaces embeds Digital Rights Management (DRM) protection in files so content stays secure everywhere they go. Control users' ability to view, edit, copy, print, download or forward files, even after those files are downloaded or shared with third parties.

Learn more about the BlackBerry Enterprise Mobility Suite at www.blackberry.com/suite

* Current as of 10/2015

[1] Available at: https://www.complianceweek.com/sites/default/files/Ponemon-Intralinks%20File%20Sharing%20Report.pdf