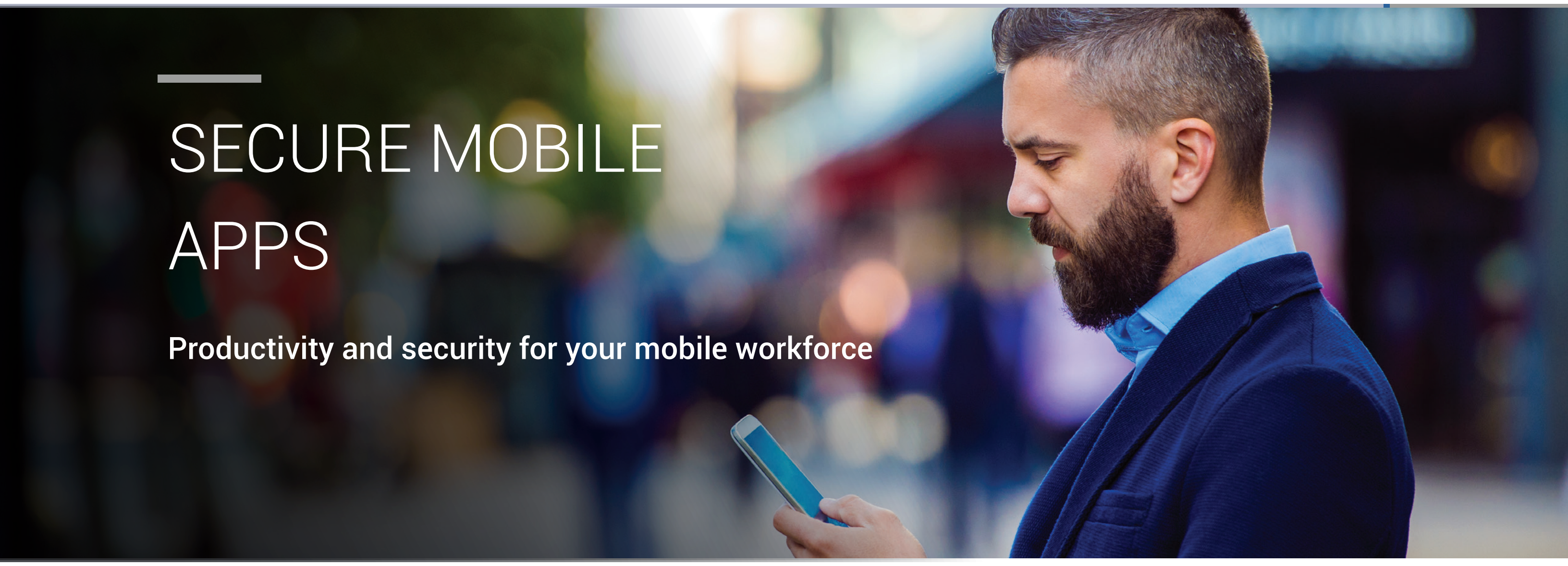
BlackBerry

Whitepaper



# SECURE MOBILE APPS

**Productivity and security for your mobile workforce**

With business travel as well as the trend toward remote work environments and distributed teams, the mobile workforce has become a common scenario at enterprise organizations. Just because an employee is out of pocket on business travel or team members don't sit in the same office, employee are still expected to work efficiently and productively. However, employees can only be as productive as their work applications allow them to be.

## Mobile Apps: An Innovative Strategy and a Security Challenge

For enterprise organizations, mobile apps are a strategic endeavor that can increase employee productivity well beyond the walls of an office, streamline processes, encourage engagement, attract customers, and boost sales.

However, off-the-shelf third-party productivity apps can present huge security gaps. For example, if a traveling employee has no alternative than to use a personal smart phone hot spot in a busy international airport to connect to a company application, there is a significant security threat.If employees choose their own productivity, collaboration, and file-sharing tools, the remote access and syncing functionality can also expose an enterprise to security breaches. Additionally, the non-standard third-party apps can hinder productivity as employees potentially use conflicting apps.

Meanwhile, the bring-your-own-device (BYOD) trend is taking root because people are more productive on their preferred devices. Since personal devices are never as secure as company-issued devices, there's yet another security risk if not managed appropriately.

Data is what fuels mobile app functionality, and that very access to sensitive company information is what puts organizations at a substantial risk of a data breach — a catastrophic event that could wreak havoc on an organization, jeopardize its image, and cost billions of dollars in restitution. Therein lies the challenge: how does an enterprise organization provide anywhere, anytime, any device mobile app functionality that keeps data secure, especially across the lifecycle of the app from development to deployment, updates to sunset.

To combat the security threat, many companies layer on the authentications, detection methods, and encryptions to prevent a data breach. And while a multi-layered security approach makes logical sense, at some point, all of the well-intended security measures prohibit the productivity that mobile apps are intended to enhance. And in addition, layered security introduces risk at each layer. As employees increasingly turn to devices, like tablets, voice-activated assistants, smart watches, and smart home technologies, cybercriminals will always be lurking in the dark web, designing sophisticated schemes to exploit security gaps.

With the high demand for mobile apps and the gains they can deliver to an enterprise organization, don't let the compliance and security risk deter your mobile app strategy. There are app development solutions that allow you to provide the productivity your end-users want with the security your company needs — using a secure foundation that combines a robust operating and management environment that app developers can trust.

### The Benefits of Mobile Apps

- Productivity on any device
- Engaged employees in any location
- Quicker response time on projects, feedback, approvals, deals
- Improved support and productivity of remote employees
- Enhanced employee satisfaction
- Lower overhead with less employees in the office
- Increased sales and profitability
- Standardized, secure functionality to reduce the need and risks of employee work-arounds

# Plan Your Mobile App Strategy

## Security Concerns are Real

When an IT team embarks on an app development project, there are many security items to consider, such as the use of third-party software components that may contain malicious code, encryption algorithms for every bit of data exchanged on the app, server-side security to prevent unauthorized access, and continuous security testing. According to a survey conducted by BlackBerry, it's no wonder that 80% of financial services organizations have only dipped their proverbial toe in the water of mobile app development with a limited deployment strategy. More than half of organizations surveyed — 57% — said they don't want to deploy a mobile app for their employees that uses sensitive data, while 23% indicated that they plan to limit the use of some mobile apps to only business-critical or executive users as a way to maintain security.[1]

**80%**
of FSI organizations are limiting the deployment of applications as a direct result of security

**57%**
holding back on apps that use sensitive data

**23%**
limiting deployments to business-critical or executive users

## The Dilemma of Mobile App Deployment

With any mobile app deployment, there's more to the story than just deciding to develop a mobile app for employees. An organization needs to consider its strategy to distribute the application: in a BYOD model or with company-issued mobile devices. There are pros and cons with either scenario — more effort but better controls with a company-issued device strategy versus less logistics but greater security concerns when employees use their own devices. More than 75% of survey respondents strongly or somewhat agree that the app deployment and management strategy across multiple devices is a top consideration.[2] With either approach, make sure security is the cornerstone of your app development and distribution roadmap.

**Trusted by Enterprises Around the World**

- Life Insurance Company in Asia
- European Trade Union
- Global Law Firms
- Governments
- Multinational Banks and Financial Services Firms

### Consequences of Late Mobile App Adoption

**Security Risks**

- **Workarounds** — well-meaning employees will find their own solutions to get their work done when the company won't invest in innovation.
- **Shadow IT** — when early-adopter employees take matters into their own hands to boost their personal productivity.

**Business Risks**

- **Productivity loss** — with employees stuck in the legacy mode of systems, processes, and tools.
- **Lost talent** — as frustrated employees leave the company in search of a more innovative workplace.
- **Reduced profitability** — when innovative competitors eclipse a laggard organization.

[1] Survey commissioned by BlackBerry and conducted by QuinStreet. 537 IT professionals were surveyed in the financial services industry in the United States, Canada, UK, Germany, France, and Switzerland between Nov. 28 and Dec. 5, 2018. The margin of error is +/- 4.5 percent at 95 percent confidence level.

[2] *In Financial Services, IT Has Little Confidence in Users Keeping Customer Data Safe*, EWeek, 2019, https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-finacial-services-study-its-time-to-recognize-user-needs-and-secure-them.pdf.

## The Competitive Advantage of Mobile Apps

As the mobility trend gains momentum, employees will increasingly demand that enterprise organizations provide apps, tools, and devices to enable them to work productively outside the office. According to the blog, "How Mobile Apps Can Boost Employee Efficiency and Productivity," on www.techjini.com, the results of a survey found that enterprise mobility makes processes 30% more efficient and employees 23% more productive.[1] The blog went on to list the reasons for enhanced workforce productivity:

- **Improved user experience** — because apps are more responsive than computer browsers and have intuitive user interfaces that automate redundant tasks.
- **Greater flexibility** — with apps that allow employees to communicate, collaborate, and access company resources so they can work and manage their time according to their needs.
- **Seamless connectivity** — to work remotely with colleagues, teams, and organizational resources resulting in better talent, ideas, opportunities, and business processes.
- **Better corporate communications** — with alerts, updates, action items, compliance checks, and other governance requirements to improve communications with employees.
- **HR functionality readily available** — since most mobile apps utilize key HR functionality, employees can accomplish HR tasks more quickly while reducing the burden on the HR department.
- **Meet specific needs for the business** — since apps can be deployed with features to address specific processes, companies can gain a competitive advantage.
- **Spark innovation** — the advanced features that make smart phones smart can trigger the development of innovative new apps.

### Employee Functionality with Secure Mobile Apps

**BlackBerry® Dynamics.** Speed up mobilization of all your core business apps, including collaboration, ISV, and custom-developed apps with a common app platform. Protect corporate and user data with industry-leading containerization. Plus, control costs with a solution that has no dependence on per-app VPNs or VDIs.

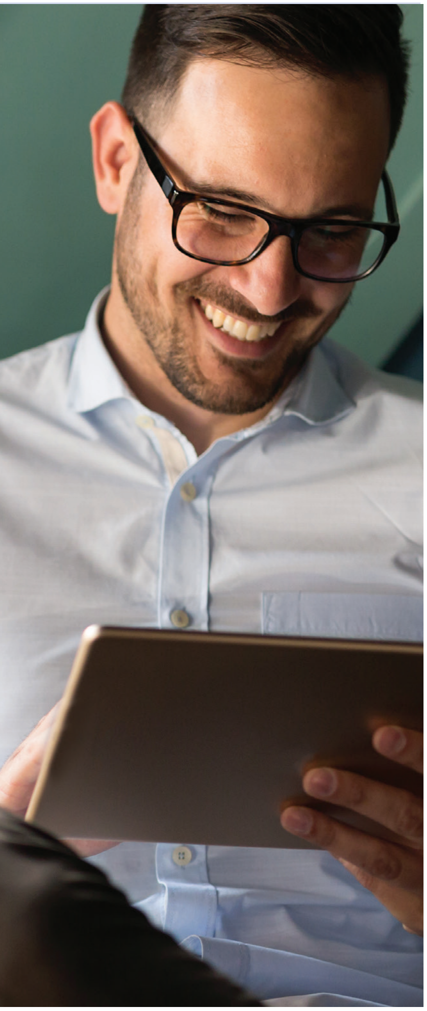
**BlackBerry® Work.** It combines enterprise email, calendaring, contacts, presence, document access and editing. It's robust, complete mobile functionality so employees aren't tethered to a desktop.

**BlackBerry® Access.** Give employees secure access to corporate networks, applications, and data in a secure browser with full containerization to protect your sensitive information.

**BlackBerry® Connect.** By integrating instant messaging and collaboration solutions, like Microsoft® Lync® or Cisco Jabber®, with your mobile apps, employees can communicate and collaborate on any device any time anywhere.

**More Apps.** A Microsoft® shop? With BlackBerry's Secure Mobile Apps, enterprises can extend Microsoft® Office, Exchange, Lync, and SharePoint® technologies to mobile devices so employees can be productive anywhere, with containerized data to protect sensitive information. To mobilize existing business applications and build in additional productivity features, choose from apps in BlackBerry's Marketplace for Enterprise Software.

[1] CITO Research. "Executive Enterprise Mobility Report." 2015, https://techorchard.com/wp-content/uploads/2015/02/2015_Executive_EnterpriseMobility_Survey.pdf.



# Introducing Secure Mobile Apps from BlackBerry

There is a better way to build cutting-edge mobile apps that offer the productivity-boosting functionality that your employees need with air-tight security. With BlackBerry's Secure Mobile Apps, users can be productive on any device in any place with access to email, web applications, an intranet, and product information management systems with robust security controls.

Most people know BlackBerry as the maker of the legendary email-friendly smartphones. For decades they have been the most secure commercial mobile devices on the market. From that legacy, BlackBerry has created a robust app development solution, called BlackBerry® Dynamics™ platform, so developers can quickly and easily build secure mobile native apps for both iOS® and Android™ devices. Here are the benefits for developers:

**Rapid Development**

The BlackBerry Dynamics platform eliminates the conflicting agendas of functionality versus security so developers can mobilize core business apps and create custom apps as quickly as possible. Whether using in-house developers, partners, or ISVs, developers can use tools from native apps, Apache Cordova™, AngularJS, and Microsoft® Xamarin® to rapidly assemble new apps using services from existing apps. Developers can also browse BlackBerry's Marketplace for Enterprise Software to find business and productivity apps, extensions, and solutions that are compatible with BlackBerry products.

**Security**

BlackBerry Dynamics offers FIPS-validated cryptography, Common Criteria EAL 4+ certification, as well as support for Android SafetyNet Attestation and Purebred-derived credentials for more robust storage, usage, and management of cryptographic keys. Developers can choose from several authentication methods, including SSO, two-factor/OTP, smart cards, and biometric authentication. Any app built on the BlackBerry Dynamics platform conforms to the same existing security baselines, and with native app deployments, developers can secure the transport layer if containerization is not required.

**Endpoint Management**

With BlackBerry® Unified Endpoint Management (UEM), enterprise organizations can extend mobile apps to IoT devices with complete endpoint management and policy control in a single visual console. Using adaptive security, AI, and spatial data, developers can build in functionality to dynamically adapt security requirements to each user's real-world usage and risk score. Your IT team can manage apps in a BYOD; company-owned, personally-enabled; and company-owned, business-only models.

### Enterprise Reliability

Apps developed on the BlackBerry Dynamics platform aren't dependent on VPNs or virtual desktop infrastructure. Instead, apps are developed on a high availability architecture using active-active redundancy to ensure uptime.

### Scalability

Offering breakthrough scalability, enterprise organizations can deploy a mobile app on as many as 25,000 devices per server and 150,000 devices per domain — on premises or in the cloud.

### App Analytics

With BlackBerry® Analytics, the IT team can track app metrics such as daily and monthly usage, duration of use, device type as well as usage by feature.

### Mobile Desktop

With BlackBerry® Launcher, developers can give users access to a single, secure mobile desktop for business applications so users can easily navigate to all of their business tools without the hassle of logging into every app.

### Familiar User Experience

With containerization, users can enjoy the same UI on any device so employees won't have to deal with the frustration of re-learning app functionality on different devices.

> "Although increased productivity is very important to us, that is not the sole reason we chose to develop our own custom applications. Doing so also allows us to explore future possibilities based on how employees respond to what we've deployed, selectively innovating where the need arises. That is one of the key reasons we chose BlackBerry — because their platform enables us to take such initiatives."
>
> *Mr. Takashi Kitano, Head of ITOCHU's Corporate IT Architecture Department and ITCCERT IT Planning Division*

## Customer Success

### BlackBerry Revolutionizes Workplace for One of Japan's Foremost Trading Companies by Deploying Customized Apps Developed on Microsoft Xamarin

Established in 1858, ITOCHU is a major trading company that represents the whole of Japan. It operates 120 locations across 63 countries worldwide and deals in imports and exports, trilateral trade, and business investment both locally and abroad.

With the goal of mobilizing its workforce, ITOCHU's IT Planning Division began transitioning its communication systems to a mobile-enabled infrastructure that included Microsoft® Exchange and Office 365®. The company planned to use a BYOD strategy, but it had to be secure, while offering easy and seamless management.

Don't let compliance and security risks deter your mobile app strategy. There are app development solutions that allow you to provide the productivity your end-users want with the security your company needs.

ITOCHU chose BlackBerry because of the simple, user-friendly interface and the advanced security features of BlackBerry UEM. In particular, features such as secure wipe (which deletes company data from a device automatically if it has not been used for a certain amount of time) were the deciding factor.

The company began developing its own custom mobile apps with BlackBerry Dynamics in 2015, and in November 2016, ITOCHU upgraded to the Application Edition of the BlackBerry Enterprise Mobility Suite to securely deploy and manage its mobile apps.

After deploying several custom apps to its employees, ITOCHU has seen excellent results across the board. Its employees are now more efficient and productive, and its mobile data is kept safe no matter where staff work. More importantly, the BlackBerry® Enterprise Mobility Suite allows the company to innovate with new custom apps and workflows.

With widespread user adoption, ITOCHU's staff really likes BlackBerry UEM's interface and BlackBerry Work, an industry-leading PIM app and secure business desktop. This positive response has been a welcomed change since employees rarely used the company's previous mobile infrastructure.

## Citi Orient Securities Improves Efficiency and Enhances Security with BlackBerry UEM and Awingu

Citi Orient Securities is a top-tier investment bank headquartered in China. The company was formed in 2012 as a joint venture between Orient Securities and Citi Global Finance Asia. In the investment banking industry, even a minor delay can mean missing out on a major investment or making an important client unhappy. The leadership team realized that mobile functionality could boost employee engagement and responsiveness. However, Citi Orient Securities needed a way to manage and secure its mobile infrastructure.

After reviewing other endpoint management offerings, the organization deployed BlackBerry UEM. Citi Orient now has a single view of its entire mobile infrastructure, coupled with the capacity to apply policy controls across devices and apps. The bank also chose to secure its mobile email with BlackBerry Work, and it deployed BlackBerry Access, a secure browser that gives employees access to a wide range of web and intranet apps.

BlackBerry helped make the company's systems more compatible with new mobile applications by integrating them with BlackBerry Dynamics, a secure application container. Employees can access web-based applications on laptops, iPads, and smartphones. This eliminates the cost associated with developing new apps, and greatly improves user enablement with easier access to new applications.

# Mobile Apps with Security and Productivity

BlackBerry's Secure Mobile Apps provides the robust development platform to build apps that can mobilize your key business applications to facilitate productivity, collaboration, and communication. Support your workforce's demand for mobile apps and maintain security to protect sensitive company data.

# Learn More

To learn more about developing and deploying apps to enable your mobile workforce with BlackBerry Secure Mobile Apps, visit www.blackberry.com/us/en/solutions/secure-mobile-apps.

# About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.