WHITEPAPER

ACCELERATING PRODUCTIVITY WITH SECURE ENTERPRISE INSTANT MESSAGING

Mobile IM for Security Sensitive Organizations

BlackBerry®

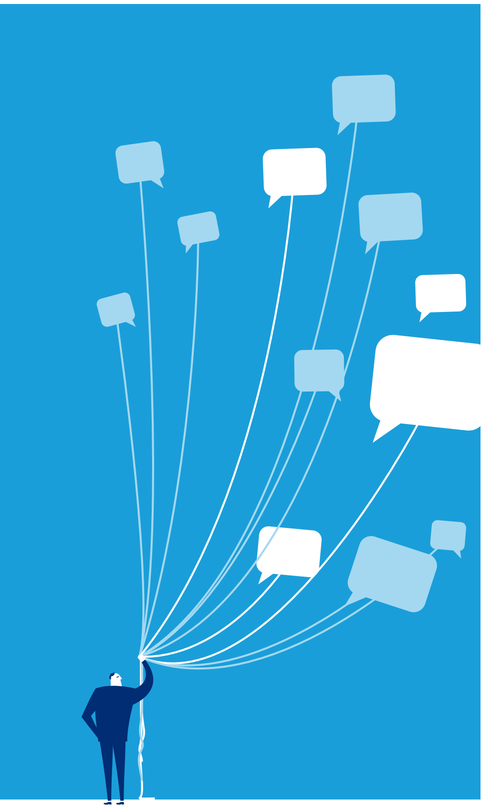
ACCELERATING PRODUCTIVITY WITH SECURE ENTERPRISE INSTANT MESSAGING

Contents

Instant messaging is an efficient real-time collaboration and communications tool that enables organizations of all sizes to increase end-user productivity by accelerating and enhancing interactions among workers, partners and suppliers. Due to a lack of sufficiently secure and compliance-capable IM solutions, many regulated businesses and other organizations operating in high-security environments have been unable to take full advantage of these business-transforming benefits. The recent availability of enterprise-grade and risk-restricting mobile IM solutions, however, is opening up opportunities for productivity advancements at even the most security conscious organizations.

But not all solutions are equal. In what security experts are calling the “post-Snowden” era, a flurry of purportedly hyper-secure messaging applications have been rushed to market. Targeted primarily at consumers, these applications need to be measured against solutions from suppliers with well-established pedigrees in messaging, security and enterprise mobility. The bottom line objective for organization in highly-secure industries, such as government, financial services and healthcare, is to adopt secure mobile IM solutions that deliver the optimal mix of functionality, ease-of-use, risk mitigation and regulatory compliance.

Introduction



Instant messaging's enterprise journey has been long and winding.

Though business workers were able to exchange near-instantaneous electronic messages as early as the 1980s, it wasn't until the end of the next decade that IM found significant enterprise traction. That's when end-users started installing public IM services, most prominently AOL Instant Messenger, MSN Messenger and Yahoo! Messenger, on their work PCs.

In late 2013, the market research firm The Radicati Group estimated that out of the nearly 3 billion worldwide IM user accounts, 379 million were being used for work. That figure is projected to rise to 449 million in 2017, according to the research firm, which also projects that in 2014 enterprise workers will send about 28 billion IMs every day.

The most obvious communications and collaboration advantage of IM over email and other messaging types is the ability to work in real time. By combining the immediacy of a face-to-face conversation with an electronic messaging medium, end users are able to significantly accelerate business decisions among co-workers, partners and customers. As IM evolved to include presence information, enriching work-related communications with valuable contextual information – participant availability and location, for example – its contribution to business productivity increased significantly.

IM reached another productivity plateau through its steady integration into enterprise Unified Communications & Collaboration (UCC) packages, which also include email, presence, voice and video conferencing applications. UCC software, which enables enterprise workers to conduct all popular forms of communications and collaborations from a single application and common user interface, generates between $5 billion and $10 billion annually, according to market size figures from multiple sources.

The latest leg of IM's journey through the enterprise is being influenced by the rising prominence of mobility in the workplace. As end users turn to smartphones, tablets and other mobile end points to drive personal productivity even higher, enterprise IM adoption has taken a slight detour. Mobile IM has yet to be fully embraced in the enterprise for several reasons.

For starters, many employees are accustomed to using SMS technology to conduct messaging sessions from mobile devices. While common text messaging lacks many of the bells and whistles of modern IM, including presence information and the ability to escalate to a voice or video session, SMS's universal reach makes it appealing to a large percentage of employees. Most mobile IM services are closed, requiring sender and recipient to use the same service and, sometimes, mobile device platform. An SMS message is assured of reaching nearly anyone with an active mobile telephone number.

△ Back to the Contents

From a usability standpoint, enterprise workers have been slow to embrace the “mobilized” versions of enterprise IM apps designed for the desktop. More comfortable with an interface engineered for a mobile environment, enterprise end users, who also prefer to use a single IM app for both work and personal communications, often adopt consumer mobile IM services. Not coincidently, the popularity of consumer mobile IM services, such as WhatsApp, Facebook Messenger and BBM™ have skyrocketed in recent years. With a few exceptions, consumer IM services offer only rudimentary protection of IM content.

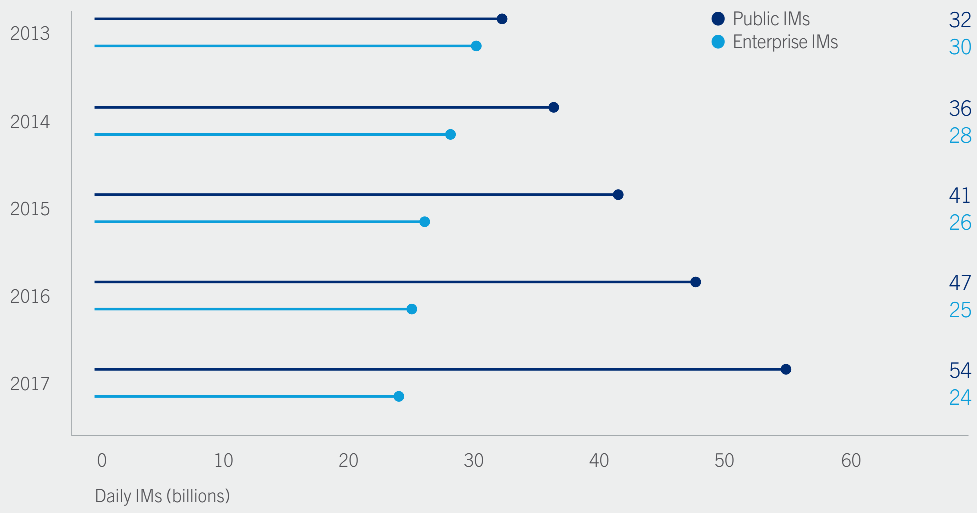
The list of potential security risks associated with commercial IM services – as well as some enterprise-level applications -- is a long one. The big issue is that most of these services require IM traffic, including messages containing potentially sensitive corporate content, to travel over a public network outside the oversight of corporate IT. IM is vulnerable to the same Internet-borne maladies as email, including malware, spam and viruses, as well as spoofing, identity theft and eavesdropping. Cyber thieves and attackers can also use Mobile IM to prop open backdoors to behind-the-firewall servers.

This situation has left many enterprises with little choice but to discourage or prohibit end users from conducting mobile IM sessions. In fact, many businesses within regulated industries, including financial services, healthcare, education and government, prohibit mobile IM due to security and noncompliance concerns as few mobile IM services support IM logging or auditing. Other public and private entities with high-security concern are also reluctant to embrace mobile IM and have been collectively holding their breaths in anticipation of an IM-related security breach.

Billions a Day

While IM traffic in general is expected to soar over the next few years, The Radicatti Group research firm projects that IM traffic from enterprise-level services will fall off as employees migrate to consumer-oriented messaging platforms.

Enterprise and Public IM Traffic, 2013-2016



Source: “Instant Messaging Market: 2013-2017,” The Radicati Group, September 2013

△ Back to the Contents

Adding to the corporate clampdown on mobile IM among regulated and security conscious enterprises are revelations over the past 18 months of what now appears to be rampant occurrences of cyber surveillance operations and industrial espionage. In an era in which competitors or foreign governments could be snooping through inter or intra-company communications, trolling for intellectual property or backdoors into corporate servers, security conscious organizations are thinking twice about utilizing mobile IM.

As a result, many regulated businesses and other organizations operating in high-security environments are unable to take full advantage of the business-transforming benefits of mobile IM.

The good news for these businesses is that relief is on the way. In what security observers have described as the “Post-Snowden” era, a reference to National Security Agency (NSA) whistleblower Edward J. Snowden, a spate of suppliers have released or are rushing to market purportedly secure mobile IM applications and services.

The bad news is that these services differ significantly in the quality of experience their suppliers bring from the messaging, mobility and security segments of the market, the sophistication of security they offer and, consequently, their ability to protect organizations against data leakages and regulatory compliance violations.

The remainder of this report provides an overview of high-risk security and compliance vulnerabilities associated with mobile IM and how they might be mitigated by a new breed of secure mobile IM applications and services. It also provides advice on identifying secure mobile IM solutions optimized to enable even the most security conscious organization to fully realize the productivity accelerating potential of enterprise instant messaging.

Enterprise IM Risks

Enterprise IT must apply the same vigilance to protecting the integrity of instant messaging as other forms of corporate communications. Just like email or Web browsing, IM is a fertile environment for malware, worms, viruses and other forms of cyber mischief and malice. But the two IM-related security and liability risks generating the worse cases of indigestion for CIOs in regulated industries and at businesses with stringent security demands are concerns over data leakage and running afoul of regulatory compliance requirements.

Data Leakage

Data leakage can be segmented into two major categories, accidental and malicious. According to a 2013 report from a division of Ernst & Young Global Limited, more than 20 percent of mobile devices will be lost during their lifetimes. While an IM history is probably not the richest source of competitive information stored on a mobile device, instant messages are frequently unencrypted and, consequently, easily accessible to third parties. Another source of accidental data leakage is the unintentional dissemination of corporate information contained in IM chats through public channels.

It's the malicious forms of IM-related data leakage, though, that represent the largest potential threat to the competitive standing and reputation of an organization. In the case of a government agency or any organization responsible for protecting the privacy of individuals, such as a healthcare provider, data leakage could also result in severe legal and financial penalties. Penalties for unlawful disclosure of patient information have exceeded $1 million.

While any organization doing business on the Internet or through commercial telecommunications carriers has long been sensitive to the threat of cybersecurity breaches, it's only been in the past couple of years that enterprises have been alerted to sophisticated and widespread spying and industrial espionage operations being conducted by government surveillance agencies and other entities.

These activities became public knowledge in 2013, after several media outlets published details of extensive surveillance operations – both domestic and foreign – conducted by the United States National Security Agency (NSA). The leaked documents, provide by former NSA contractor Edward J. Snowden, also revealed that several telecommunications and Internet companies had cooperated with the data collection operations, despite public denials.

Cyber surveillance operations are not exclusive to the US. The monitoring of corporate and personal communications is a common practice of most modern nations, which consider electronic surveillance to be a component of national defense initiatives. In May 2014, the United States Justice Department charged five members of the Chinese military with industrial espionage, alleging that the individuals were responsible for hacking into the networks of large American corporations. An article in the May 25, 2014, edition of *The New York Times* reported that a classified document from the US government accused the Chinese military of attacking more than 3,000 American companies with the intent of capturing intellectual property.

Regulatory Compliance

Potential penalties related to regulatory compliance violations have also pushed many security-conscious businesses and organizations into severely limiting or prohibiting IM within their enterprises. Government agencies, financial services firms, healthcare providers or any organization doing business in regulated environments must navigate a thicket of compliance requirements, which grows denser by the day.

Nearly every behavior or business activity, including all electronic correspondences, must now conform to a prescribed set of policies and procedures, which often vary from country to country or across legislative jurisdictions, such as federal, state and local. While dealing with this labyrinth of regulations and requirements has never been easy, the task became considerably more complex nearly a decade ago, when organizations started moving many of their business practices to the Internet.

The rapid adoption of enterprise mobility over the past few years has unleashed yet another torrent of new regulations related to the governance of electronic communication. Few, if any, industry segments have escaped the recent onslaught of compliance requirements:

- The Sarbanes-Oxley Act and the Dodd-Frank Wall Street Reform and Consumer Protection Act have added to the compliance complexity of the financial services industries in the past few years.
- The Third Basel Accord is a frequently updated set of compliance rules for international banking.
- The healthcare industry-aimed HITECH Act, issued in 2011, added another set of regulations to the already onerous Healthcare Information Portability and Accountability Act (HIPAA).
- For any company doing business in Europe, data protection and privacy practices must now comply with regulations set down by the European Union’s Directive on the Protection of Personal Information act.

A major shortcoming of most IM services is a lack of support for logging or auditing. The inability to track business-related IM exchanges or ensure that content embedded into instant messages meets privacy and other legal requirements has prevented many regulated industries from adopting an IM service.

The Road to Secure Mobile Enterprise IM

Early forms of electronic message exchanges, mostly conducted among university researchers, predate the Internet by decades. But the first real commercial chat services started showing up in the early 1980s. CompuServe’s CB Simulator, available in 1980, capitalized on the citizens band radio craze that was rampant in the US at that time. The mid-to-late 1990s witnessed the Golden Age of IM, as ICQ (I Seek You), AOL and Yahoo! services were launched, turning millions of teenagers into turbo typists and flooding the vernacular with an onslaught of acronyms.

It was around this time that IM made its debut in the enterprise market. The predilection of employees to chat electronically with colleagues, partners and even customers evolved into a full-blown habit when corporate operating system giant Microsoft introduced Microsoft Messenger in 1999 – and eventually Lync. The 2000 introduction of Jabber introduced the concept of IM federation and the 2003 launch of Skype leveraged broadband Internet access to spice up the real-time flavor of IM with voice and, eventually, video.

Though it seems like SMS has been around forever, it wasn’t until the late 1990s that mobile phone users started texting in mass – initiating the first real form of mobile messaging. As Smartphones gained prominence as work productivity tools in the late 2000s, mobile device platform manufactures, including BlackBerry, offered proprietary IM services utilizing the mobile data channel, giving enterprise workers a bells-and-whistles alternative to SMS. Just around the corner was the debut of WhatsApp, a consumer mobile IM app.

The end of the first decade of 2000 marks the initiation of efforts by desktop IM providers to move their clients to mobile environments. The fruits of those labors have been slow to be embraced by a large percentage of the mobilized workforce, which prefers the usability and universality of consumer IM products. The inherent vulnerability of consumer IM services prompted many security conscious organizations to severely limit or prohibit mobile IM. These concerns where validated in 2013 when evidence of government surveillance of electronic communications was publically revealed, fueling the development of multiple secure mobile IM apps and services.

1980	CompuServe CB Simulator
1996	ICQ
1997	AOL Aim
1998*	Mass adoption of SMS
1999*	Enterprise IM catches on
2000	Jabber
2003	Skype
2006	BBM
2008*	Other Mobile IM Services
2009	WhatsApp is Born
2011*	Desktop IMs go Mobile
2014	BBM Protected

*Circa

Enterprise IM Risk Mitigation

The most effective means of mitigating risks related to mobile enterprise IM, of course, is to simply block usage through mobile application management (MAM) and mobile device management (MDM) policies. A draconian approach, though, is bound to negatively impact both end user satisfaction and workforce productivity. IM is utilized by a high percentage of employees for personal communications. Outlawing all forms of IM would force workers to carry a personal mobile device to conduct those conversations, increasing the opportunity for work-related information to leak outside the company. A more severe consequence of IM prohibition, though, is the inability to reap the productivity benefits of real-time electronic communications, which accelerate and enhance interactions among workers, partners and customers.

To reap those benefits through the sanctioning of IM exchanges over mobile devices, organizations need to take three primary actions to reduce the risks associated with data leakage and regulatory compliance: isolate, encrypt and log.

Isolate

The first step to delivering secure enterprise mobile IM is to ensure that all IM messages are confined to a trusted domain. All components of an IM exchange, including authentication, presence awareness and message routing, should not be administered by a third-party that is vulnerable to security breaches or may be cooperating with state-sponsored data collection operations. To ensure the highest level of security, the IM service provider should also be isolated from administering security keys.

Encrypt

End-to-end encryption is at the heart of a highly secure mobile IM solution. All potentially sensitive IMs must be encrypted during every step of the sender-to-recipient journey. In addition to in-transit encryption, IM-related content must be protected at rest – while residing on mobile end points. As discussed later in this document, the layers and sophistication of cryptography implementation are major factors in determining the efficacy of a hyper-secure IM service and in a comparison of competing solutions.

Log & Audit

Though logging and auditing of IM exchanges are core requirements of regulatory organizations and other businesses that could be required to satisfy eDiscovery requests, these functions are not typically integrated into IM services. Most enterprises employ standalone software solutions or Enterprise Mobility Management (EMM) platforms to log voice, email and IM messages. It's imperative, then, that regulated businesses and others adopt a compatible combination of mobility management and secure mobile IM service. CIOs also have to be conscious of mobile platform selection, as some mobile OSs do not currently expose the APIs necessary to support IM auditing.

△ Back to the Contents

Selecting a Secure Enterprise Mobile IM Solution

The market for secure IM solutions has transitioned from famine to feast in the past year. A climate of unease brought on by the fear that all communications are susceptible to snooping and doubling as backdoors into corporate servers has generated a flurry of development activity in the secure mobile IM market. The participants in this fledgling market segment range from well-established companies from the messaging, security and mobility industries to two-person startups operating on shoestring budgets. At least two of these startups, taking a cue from Snapchat, offer a "self-destruct" function, which resonates from a security perspective but falls flat in terms of satisfying regulatory requirements.

IM Usage Policy

You don't need to be a former CEO of a major retailer to understand that nothing is 100 percent secure.

End users need boundaries and even the most secure mobile IM solution should be accompanied by a clear and simple user policy that spells out rules of behavior for all segments of the workforce.

Many common IM vulnerabilities, including malware and viruses, can be eradicated through end user education. For example, employees should be reminded in writing to exercise caution when opening an IM attachment or Web link, even when it appears to come from a trusted source.

Human error can defeat nearly any security measure. Police officers in Sweden narrowly avoided legal hot water after mistakenly including a civilian in a work-related chat session. The incident, recounted in several published reports from February 2014, involved multiple officers using a popular consumer messaging application to chat about and share images related to an ongoing investigation. Though the sensitive information was apparently not distributed beyond the university professor who was inadvertently included in the group chat, accidental leakages of this sort, especially by government agencies, could result in lawsuits, as well as inflict severe damage to the agency's reputation.

The irony of secure mobile IM is that it may now be the most protected and reliable communications channel in the enterprise – precisely because message routing is overseen by the organization. Given the documented incidences of government surveillance and industrial espionage related to the collection of email and texts, businesses with an effective secure mobile IM solution may designate it as the communications channel of choice for highly sensitive content and communications.

None of that will matter, of course, if end users are unaware of usage policies.

The competitive landscape for secure mobile IM is dense, complicating the challenge of busy CIOs to find a solution with the optimal mix of functionality, ease of use, risk mitigation and regulatory compliance capabilities. CIOs and other IT decision makers can accelerate the secure mobile IM selection process by limiting their search to solutions that possess the following characteristics:

Engaging Interface

Mobile end users do not suffer from a lack of options. Any mobile app that does not deliver an optimal user experience – or impedes productivity to the slightest degree – will be rejected by employees in favor of an "unapproved" alternative. While risk mitigation is paramount in the adoption of a secure mobile IM service, the most secure solutions will be non-starters if they lack an engaging, easy-to-use interface that enables workers, for example, to smoothly navigate between modes of communications: or seamlessly send IMs to recipients inside or outside the organization. IM is about getting things done in a hurry. If it takes a series of awkward gestures for an end user to attach a file or escalate an IM session to a video session, employees will move in mass to an alternative.

Built for Mobile

Though the enterprise mobile app movement is still in a nascent stage, businesses have already learned that processes built for a desktop environment rarely translate to a mobile environment. IM apps are no exceptions. IM apps built from the ground up for mobile make the best use of the limited real estate of mobile displays and the on-the-go mentality of mobile users. As already mentioned, usability is imperative. A desktop IM app migrated to mobile is almost assured of bringing with it functions and features that end users will find unsuitable for an anytime, anyplace environment.

△ Back to the Contents

Enhanced Security Model

Security is all about layers – overlapping layers. Look for a mobile IM that employs multiple layers of encryption to deliver new levels of enterprise-grade security to protect the content of IMs while in transit and at rest. Only a company with years of experience in cryptography will be able to create the novel techniques for exchanging signing keys and other security measures that regulated business will require to ensure the needed integrity and confidentiality of their corporate communications. CIOs should also restrict their secure mobile IM options to services that comply with the most demanding encryption standards. Solutions that lack a FIPS 140-2 validated cryptographic library or fail to meet NIST Suite B cryptography guidelines, for example, should be disqualified from consideration.

Complete Control

The only way to ensure that a technology partner or service provider is not complying – voluntarily or involuntarily – with government or private surveillance operations is to select a secure mobile IM supplier that relinquishes the ability to decrypt the information in encrypted IM exchanges. If any entity other than your organization possesses the capabilities to intercept or read secure messages, the solution is flawed. Find a partner, for example, that employs out-of-band mechanisms to ensure the secrecy of key exchanges and places encryption keys exclusively under the control of your organization.

Established Pedigree

The enterprise mobility market is governed by few standards. There are no common blueprints for IM applications. Unable to leverage industry best practices – applied to functionality, implementation or legality – startup solution providers are essentially learning on the job. Trial-and-error is a poor model for any electronic service, but a particularly dangerous one when it comes to security. Organizations with elevated security requirements need to partner with suppliers with deep and well-regarded pedigrees in the messaging, security and enterprise mobility markets. Secure mobile IM solution providers not backed by a research & development arm with thousands of patents in messaging, mobility and security are a risky bet, at best.

EMM Integration

The optimal secure mobile IM solution is one that is tightly integrated with a comprehensive multi-platform EMM solution. The benefits of IM and EMM integration are substantial from expense, complexity and compliance perspectives. On the cost side, a single-vendor solution could eliminate the purchase of the additional hardware required to host a standalone IM solution, as well as the expense of training IT on a separate management console. EMM integration also reduces the complexity of implementing a secure IM service to a simple policy change. Compatibility between EMM and IM means that the voice and email logging and auditing capabilities of the EMM platform can be extended to include IM.

Universal & Transparent

Industry research indicates that employees prefer to use a single IM solution for both work and personal communications. An IM app that enjoys both widespread consumer and enterprise penetration – and allows users to chat with employees and acquaintances from a single interface -- will find the most favor with end users. It's also imperative that the app is able to transition between security levels and usage scenarios automatically – without the intervention of the end user. As an example, the IM service should be able to automatically detect – and elevate the encryption level – when the sender is conducting an IM session that requires the highest levels of security and confidentiality.

Conclusion

The combination of mobility and instant messaging is a productivity powerhouse. The insertion of real-time communications into an anytime, anyplace setting has the potential to turbocharge the business-decision process, ushering in new levels of productivity and innovation. But many organizations, especially those operating in regulated or high-risk environments, have severely curtailed or prohibited the use of IM services due to security or regulatory noncompliance concerns.

While revelations of rampant cyber surveillance and industrial espionage have heightened the security concerns of enterprises, they have also spurred a surge in the development of IM applications and services that purport to provide a hyper-secure layer of protection. As these products reach the market, CIOs at regulated businesses, including government agencies, financial services, education and healthcare firms, must sift through a crowded landscape of secure mobile IM solutions that vary widely in their ability to provide an optimal mix of security, regulatory compliance and end user satisfaction.

To find the best fit for their businesses, CIOs and other IT decision makers should only consider secure IM services that were designed for mobile end points, offer an optimum user experience, apply an enhanced security model, simultaneously support work and personal communications and are backed by suppliers with solid pedigrees in security, messaging and enterprise mobility.

The BlackBerry Difference

BlackBerry's BBM Protected is a secure enterprise IM service that enables employees to take advantage of the speed, reliability and privacy of BBM for faster communications, collaboration and decision making while providing security conscious organizations enhanced enterprise-grade security over corporate data.

BBM Protected is the only secure mobile instant messaging app that uses a FIPS 140-2 validated cryptographic library. For regulated business and highly security conscious organizations, BBM Protected offers an enhanced security model for BBM messages sent between BlackBerry smartphones. BBM Protected protects corporate data in transit by adding an additional layer of encryption to BBM and follows the BES model by assigning control of encryption keys to your organization.

BBM Protected enables employees to use the same app to securely message colleagues inside the company for work as they do to chat and share with family and friends outside the company. To meet increasingly onerous compliance requirements, enterprises can use the logging capabilities of BES10 or leverage messaging and call tracking and auditing software from BlackBerry partner GWAVA, or another member of BlackBerry's extensive enterprise application partner ecosystem. All the added security offered by BBM Protected happens in the background. When a BBM Protected user sends a message, if the recipient is also a BBM Protected user then their conversation is automatically subject to the added level of encryption.

The ideal business tool, BBM Protected enhances communication, collaboration and sharing between employees with the speed, confidence and privacy loved by over 85 million BBM users worldwide. For more information about BBM Protected visit: BlackBerry.com/bbmprotected

BlackBerry®

△ Back to the Contents