



Whitepaper

August 2008

Wireless Push Email for the Smaller Business: A Comparison

A J.Gold Associates White Paper

“Microsoft’s newest version of Exchange provides push email capability as a standard feature. However, its limited security and management capabilities require that companies add-on to the out-of-the-box functionality to meet minimum requirements for safely handling sensitive company data..... For many companies, it may be easier and more cost effective to forgo MSCMDM and add a third party solution that is optimized for the needs of safely and securely handing wireless push email in an easily deployed environment and scaled for small businesses... We believe BlackBerry Professional Software provides a compelling alternative...”





Contents

Introduction 2

The Need for Mobility 3

Exchange: Going Mobile May Not Always Be Easy 3

Some Limitations 4

Is Free Good Enough? 4

The Alternatives: Comparing Two Push Email Solutions 5

Microsoft Exchange with MSCMDM 5

BlackBerry Professional Software 5

Comparing Installation Requirements 5

 Figure 1: Microsoft Direct Push with MSCMDM vs BlackBerry Professional Software 6

What Does Complexity Cost? 6

Simplification and Legacy Compatibility 7

Comparing Functionality 7

 Figure 2: Functional Comparison 7

Conclusions 8

Appendix 9

Appendix 1: Limitations in Microsoft’s Solution 9

Appendix 2: Security and Management Enhancements 9

Appendix 3: MSCMDM Requirements 10

 Figure 3: Microsoft MSCMDM Minimal Configuration 10

Appendix 4: Utilizing BPS 10

 Figure 4: BlackBerry Professional Software 10





Wireless Push Email for the Smaller Business

Introduction

Many small firms are exploring ways to provide push email capability to wireless devices carried by their highly mobile workforces. Indeed, workers such as medical professionals, legal professionals, real estate agents, insurance agents, banking and financial representatives, builders, maintenance workers, accountants, and sales people all spend significant amounts of time away from their desk while traveling to customers or working from remote locations. Many of these professionals work in small groups or organizations consisting of a few, or at most a few dozen workers. Despite their relatively smaller size, the sophistication of today's business environment requires that these workers are enabled with many of the same technology solutions that larger enterprises have been utilizing for some time.

One of the key functions required by virtually any mobile worker in a large or small business is wireless email pushed to their mobile device from their organizational email system. Many mobile workers spend in excess of 50% of their working hours away from their offices and must stay in touch with the company to remain efficient and effective in their work. Email has achieved mission-critical status in nearly all businesses and as such, forms the backbone of many business communications and collaboration systems (e.g., scheduling, alerting, problem resolution, workflow, work dispatching, and customer management). A number of email solutions exist, from publicly available free solutions (e.g., Gmail, Yahoo mail, Hotmail, AOL), to local ISP hosted solutions (e.g., Comcast, Verizon, Cox), to dedicated feature-rich and robust email systems designed for business users (e.g., Microsoft Exchange, Lotus Notes). Most professional users require more functionality than is typically available with web-based and/or ISP hosted public email systems. They require additional services like scheduling, data management and storage, contacts, etc., and which must be provided in a totally secure environment that does not jeopardize sensitive customer and/or company information. For this reason, many serious business users, even in smaller organizations of 5-10 professionals, are selecting and deploying more robust and commercially available Personal Information Management (PIM) and Email systems.

This whitepaper will explore the requirements and use of mobile extensions to email and PIM systems in companies that have selected the popular Microsoft Exchange environment as their email solution. The analysis will be targeted at the small office environment (e.g., under 25 users), but will assume that such groups are just as engaged in mission critical and sensitive business as much bigger organizations deploying large scale enterprise class systems. It will explore various capabilities available with such a system, from included-for-free functionality to third party add-ons, and provide guidance on specific capabilities that must be included if the overall experience is to be easily manageable, secure (especially for regulated industries like legal, medical and financial), and fully capable of meeting user needs. Finally, it will compare two solutions available to small businesses: Microsoft's Exchange Direct Push with Microsoft System Center Mobile Device Manager, and Research in Motion's BlackBerry Professional Software.



Wireless Push Email for the Smaller Business

The Need for Mobility

There is no doubt that businesses of all sizes are going mobile. Indeed, in many small organizations, mobility is not an option but a business imperative. Real Estate, Legal, Financial Services, Accounting, Health professionals, Construction, and many other service companies all have significant field workers who spend much of their time delivering their services directly at the customer site, and who often spend the majority of their working day away from their office. To remain productive, most now rely on mobile email and application support as a way to remain current with the information flow that runs their business. Indeed, we estimate that those mobile workers who have a way of remaining in touch throughout the day can achieve at least 15% more productivity than their mobile peers who do not utilize effective mobile communication and collaboration systems. In many cases, workers have been reported to increase their productivity by as much as 20%-50%. Further, because businesses can more intelligently communicate, collaborate and schedule their work force, customer satisfaction can improve considerably.

The majority of small businesses are now utilizing fairly sophisticated solutions to meet their mobile communications needs. While some deploy their own communications suite on their own servers, many utilize a hosted service from a specialty provider. Reacting to this growth in small business email deployments, Microsoft now has specifically targeted solutions (e.g., Small Business Server, which includes the Exchange application) for those companies that need sophisticated solutions and technologies comparable to enterprise systems but who desire a simplified approach to installation and management and who do not have an IT staff to manage and maintain their system. Consequently, we expect to see a substantial increase in the number of small businesses who deploy their own communications capability through a relatively low cost server/software combination. Indeed small companies can have their own system installed for well under \$3K, depending on the number of users.

The following sections of this paper will focus on the small business use of Microsoft Exchange as a communications tool for the mobile workforce. It will highlight how Exchange can be configured to provide push email to wireless devices, but will also highlight some of its limitations around security, manageability and complexity of installation, and identify a complimentary add-on for smaller businesses to overcome many of these limitations.

Exchange: Going Mobile May Not Always Be Easy

Microsoft has provided Exchange email and PIM solutions to businesses for many years, but it is only with recent versions (since Exchange 2003) that it has provided the ability to directly push email to wireless devices without utilizing third party add-ons. Enabling Exchange 2003 for push email requires that users have at least Service Pack 2 installed. Users of newer versions of Exchange (Exchange 2007) no longer need this add-on as the functionality of Direct Push Email is a standard feature. However, there remain some significant restrictions, which in the final analysis, could necessitate an upgrade of existing email systems, and could severely restrict the kinds of devices a company can purchase, and the level of security available to maintain information safety.



Wireless Push Email for the Smaller Business

Some Limitations

There are still a substantial number of pre-Exchange 2003 deployments in place, particularly among smaller businesses who may have deployed several years ago and who do not upgrade systems often. To obtain the push email available within newer versions, companies would have to purchase and install the latest versions of Exchange. Buying a small business version of Exchange (as part of Small Business Server 2003) is not a major expense in and of itself (as little as \$599 for a 5 user Standard Edition, \$1299 for the Premium Edition, plus \$1929 for an additional 20 Client Access Licenses (CALs), however Microsoft has announced substantially increased pricing for the SBS 2008 edition). However, the increased level of sophistication of the newer Exchange services would require a fair amount of work to deploy (e.g., knowledge of Active Directory).

Another limitation of Exchange push email is the restriction on supported mobile device types. The Direct Push email functionality of Exchange only works with devices that are powered by Microsoft's Windows Mobile 5.0 Operating System (OS) with Messaging and Security Feature Pack (MSFP) installed or the Windows Mobile 6.x OS. Older versions of Windows Mobile devices and devices that can not be firmware-upgraded are unable to utilize this capability. Although its share is growing, Microsoft Windows Mobile powered devices have a relatively small share of the installed mobile smart phone device market. Indeed, BlackBerry and Symbian powered smart devices both outsell Windows Mobile devices.

One of the key enablers of Exchange's Direct Push email functionality is Microsoft's ActiveSync technology, and Microsoft points to ActiveSync licensing as a way for other vendor's operating systems to become Direct Push compatible. There are some vendors who have licensed ActiveSync (e.g., Palm, Nokia, Apple) for their non-Windows Mobile powered devices, but the number of device models they have released to date with this capability is minimal. Further, although Microsoft openly licenses ActiveSync, there are no specific capabilities that Microsoft requires licensees to include in their implementation on their device. This could lead to vendors deciding not to deploy file encryption, remote wipe or some other functionality available on Microsoft Windows Mobile OS devices. These functions are critical to maintaining the high level of security needed for mobile devices to prevent sensitive company data from being lost, stolen or otherwise exposed.

Is Free Good Enough?

Many companies searching for a push email solution are tempted by the notion that Microsoft Exchange offers this capability essentially for free as part of the kernel application. However, as outlined above, there are some significant restrictions for many small businesses looking to this solution. They must have a very recent version of Exchange, which also requires an implementation of Active Directory. This may require an upgrade of a legacy system, which is not without cost. They must also commit to using the latest Windows Mobile powered devices, and to do so may require the replacement of existing smart phone



Wireless Push Email for the Smaller Business

devices in the organization. While this is not a massive cost in today's subsidized marketplace, the cost per user may nevertheless reach \$300-\$500 or more when total cost of deployment is tallied (e.g., device cost, deployment to end user, training, end user learning curve, applications replacement).

Importantly for many companies, the Microsoft solution lacks some key attributes that should be included in any business-class system, and therefore add-on products are required to overcome these limitations (see Appendix 1). We believe any company large or small that is concerned about maintaining its data in a safe and secure environment must provide for proactive security and management of their deployed devices (see Appendix 2) which is not available in the standard Exchange server.

The Alternatives: Comparing Two Push Email Solutions

Microsoft Exchange with MSCMDM

We believe that Microsoft System Center Mobile Device Manager (MSCMDM) should be a required component for any organization wanting to deploy a Microsoft-only solution for a secure environment (e.g., file encryption, device wipe, VPN, device management). But providing MSCMDM requires a significant effort on the part of the organization. It requires the latest versions of Exchange (2007), Active Directory and Windows Mobile devices (WM 6.1), and has been optimized for larger, highly scalable Exchange enterprise environments. As a result, it requires that several software components and servers be added to the IT infrastructure (see Appendix 3). This may pose a burden to smaller installations where minimum cost and simplicity are key concerns. However, if companies want to achieve acceptable security and manageability for their push email application, they will need to go beyond the out-of-the-box solution available with Exchange and install MSCMDM.

BlackBerry Professional Software

BlackBerry Professional Software (BPS) is a functionally limited version of the BlackBerry Enterprise Server (BES) software, and is targeted at smaller companies. Although it has some limitations (e.g., no MDS runtime application support, maximum of 30 users), it retains much of the BES functionality and inherent management and security mechanisms, supports all BlackBerry devices and devices enabled with BlackBerry Connect, supports Java and browser-based applications, and supports legacy versions of Exchange. Upgrading to full BES to expand beyond the 30 user limit only requires the purchase of an upgrade key.

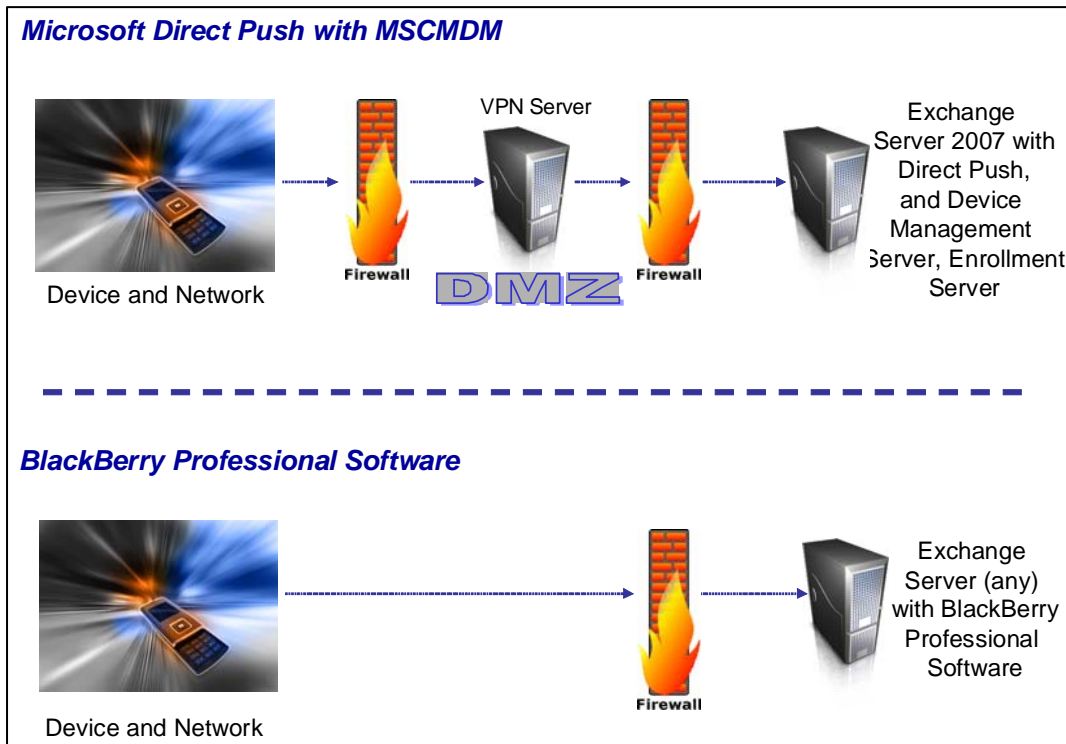
Comparing Installation Requirements

Figure 1 compares two scenarios for achieving a more secure and manageable solution than an out-of-the-box Exchange installation. The first is an all-Microsoft solution that includes Exchange Server 2007 supplemented by MSCMDM. The second is Research In Motion's small business version of its BlackBerry Enterprise Server, known as BlackBerry Professional Software (BPS).



Wireless Push Email for the Smaller Business

Figure 1: Microsoft Direct Push with MSCMDM vs BlackBerry Professional Software



What Does Complexity Cost?

To run effectively, Exchange plus MSCMDM requires several components be installed, and that these components include a VPN that must run on a server within a DMZ. Microsoft also prefers that the Device Management Server and Enrollment Server run on independent server hardware from the Exchange Server. This is advantageous in larger installations where scalability is a priority. However, for smaller installations where additional servers are a burden, these components may be combined on the Exchange Server provided it has sufficient computing resources. Therefore, the Exchange plus MSCMDM solution requires that at least one additional server be added to the network (in the DMZ), and preferably another behind the firewall for best performance.

Adding one additional server to the organization, at a cost of approximately \$1000 for the hardware, as well as the addition of the MSCMDM software components (yet to be priced by Microsoft), and the additional Total Cost of Ownership (TCO) of the server (approximately \$2500-\$3500 per server year) can create a significant cost burden for smaller organizations. Further, set up and maintenance of MSCMDM requires an IT-level manager who can cope with the complexities of policies, directories, etc. Therefore, the cost of wireless push email, even though available as a standard component of Exchange, does not come without additional costs unless the deploying organization does not care about maximizing security



Wireless Push Email for the Smaller Business

of data contained on the mobile devices and forgoes deployment of MSCMDM. We believe that virtually all organizations deploying push email through Exchange must add the MSCMDM component as a needed boost to the relatively weak security of the out-of-the-box Exchange push email and Windows Mobile device solution.

Simplification and Legacy Compatibility

BPS provides for a simpler installation and cost structure by not requiring any additional servers to be installed. It runs on the same server as Exchange, and has the additional benefit of operating with earlier versions of Exchange Server for those companies who have not upgraded their legacy systems. It is managed from a web-based interface, and allows granular control of many of the management, policy and security requirements needed by business users. It therefore requires minimal IT resources and expertise to install and maintain. Further it eliminates the additional TCO associated with adding servers and creating a DMZ.

Comparing Functionality

Figure 2 compares three possible scenarios for deploying wireless push email in a smaller business. Scenario one includes Microsoft Direct Push technology deployed to Windows Mobile 5.0 or newer devices from Exchange 2003 or newer servers. Scenario 2 deploys Direct Push but enhances the security and manageability to what we consider minimally acceptable levels with the addition of MSCMDM working in conjunction with Exchange 2007 and Windows Mobile 6.x devices. The third scenario deploys BlackBerry Professional Software connected to either legacy or current email systems and BlackBerry devices.

Figure 2: Functional Comparison

| | Microsoft Direct Push with Windows Mobile 5/6 | Microsoft Direct Push plus MSCMDM | BlackBerry Professional Software |
|---|--|---------------------------------------|---|
| Email Platforms Supported | Exchange 2003 SP2, 2007 | Exchange 2007 | Legacy Support for Exchange, Lotus Notes |
| Device Platforms Supported | Windows Mobile 5/6 plus ActiveSync Enabled Devices | Windows Mobile 6.x | BlackBerry, plus BlackBerry Connect Devices |
| Additional Servers Required | None | At least one in minimal config. | None |
| Policy and Device Mgmt | Limited - Varies by Exchange version | Extended | Extensive |
| IT Interface Environment | Exchange | Stand alone mgmt console | Stand alone mgmt console |
| DMZ Required | No | Yes | No |
| Device Data Security | Weak | Somewhat Better | Strong |
| Relative TCO | Low | High | Medium |
| Relative Overall Regulatory Compliance | Low | Medium | High |
| Upgradeability | Requires Additional SW and Server Components | Requires Additional Server Components | Path to BlackBerry Enterprise Server |

We believe that on balance, BPS may be a better choice for those smaller companies who want to maximize security and management while limiting complexity. At a minimum, the Microsoft solution requires the addition of a physical server within a DMZ and software



Wireless Push Email for the Smaller Business

added to the existing server, while BPS requires only software added to the existing server. The BPS solution is therefore less complex, and likely to be less costly to deploy and maintain long term. Further, the BlackBerry solution has a superior security model for those companies that must maintain the highest levels of data integrity and prevention of loss. Both solutions require proprietary devices to enable all of their features, and therefore this requirement balances out for both deployments. However, BlackBerry devices may be more available from carriers than Windows Mobile devices, making them easier to obtain.

Conclusions

Microsoft's newest version of Exchange provides push email capability as a standard feature. However, its limited security and management capabilities require that companies must supplement the out-of-the-box functionality to meet minimum requirements for safely handling sensitive company data. In addition, those companies that require support for older versions of Windows Mobile devices or those that have earlier versions of Exchange server installed (prior to Exchange 2003) must utilize a third party solution to enable wireless push email. Finally, even those companies that deploy the latest version of Exchange and standardize on the newest versions of Windows Mobile devices face the need to add MSCMDM to enhance security and manageability to acceptable levels, which requires deploying at least one additional server and related software.

We believe that for many companies, it may be easier and more cost effective to forgo MSCMDM and add a third party solution that is optimized for the needs of safely and securely handing wireless push email in an easily deployed environment and scaled for small businesses. We believe BlackBerry Professional Software provides a compelling alternative by being easier to deploy, less costly to run, and providing a higher level of security and manageability than the MSCMDM solution, as well as supporting legacy Exchange server installations still prevalent in many smaller businesses.



Appendix

Appendix 1: Limitations in Microsoft's Solution

Windows Mobile powered devices do not support full file encryption of on-board data unless supplemented with third party add-in software, leaving sensitive information exposed to possible hackers or bad user practice. This is a particularly critical flaw as new devices have increasingly capable data storage facilities (up to 4GB or more) and many users may download and store significant amounts of customer-sensitive or proprietary information.

The Direct Push solution does include the ability to do a total wipe of all data on the device in case the device is lost or stolen by sending it an over-the-air (OTA) remote wipe command. This is critical in companies who need to protect their data, but does not prevent data loss during the period before the loss is discovered and the command is activated.

There is no OTA remote management of the device provided (e.g., application loading, turning off functions that are unwanted, remote monitoring). Many companies find certain types of applications on their devices security risks (e.g., cameras), and wish to turn them off to prevent security breaches, as well as monitoring and enforcing all of the appropriate security settings (e.g., password, antivirus, firewalls, VPN, Bluetooth).

Appendix 2: Security and Management Enhancements

We believe that the inherent security and management features within a base-level Exchange environment are inadequate for businesses where keeping sensitive information (e.g., customer records, financial information, health data, legal filings) safe and secure is imperative. To enhance security and management of devices and overcome some of the deficits mentioned above, Microsoft will shortly (2H 08) release its Microsoft System Center Mobile Device Manager (MSCMDM). This technology provides important enhancements to the mobile environment for Windows Mobile powered devices, but will only work with the newest Windows Mobile 6.1 devices, and will not work with any other OS-powered devices. This is problematic in many organizations where a mixture of phones from various manufacturers is a fact of life and where an exclusively Microsoft environment is not the norm, or where older Windows Mobile devices are in use.

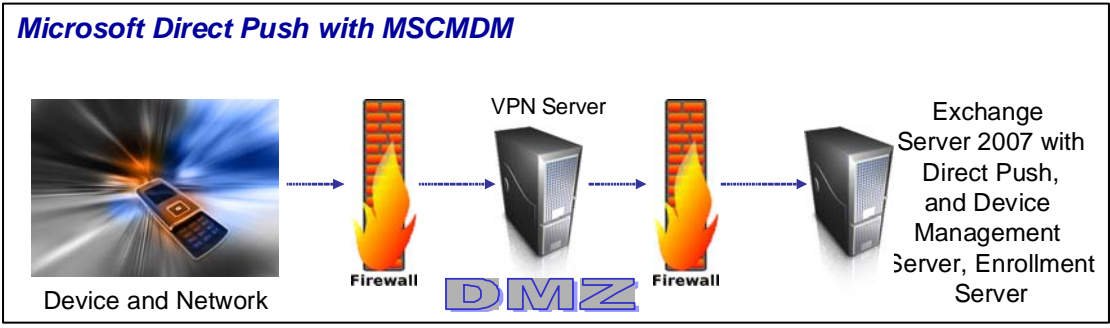
Despite its name, MSCMDM is not a fully integrated component of Microsoft Systems Center (MSC), but a stand alone environment with an independent console. While Microsoft will integrate MSCMDM into MSC console in a future version, in the interim a unique and independent capability will remain. While this may not be an issue for companies who have not yet deployed MSC, many will do so in the future to enhance management of their PC and Server inventories. Having two independent environments for management provides an increase in complexity that many companies would not find desirable. This is particularly burdensome to small companies that often do not have IT staff to cope with the complexity of heterogeneous systems.



Appendix 3: MSCMDM Requirements

MSCMDM requires a physical server be located in the “DMZ” to act as a VPN gateway. It is connected to the Internet/mobile network on one side and to the corporate firewall server on the other. This VPN gateway talks directly to the device and to key components of the MSCMDM behind the firewall, the Device Management Server (DMS) and the Enrollment Server (ES). Although in larger installations, Microsoft recommends that each of these be independent physical servers, in smaller organizations DMS and ES can be combined on a single physical server, and could potentially be the same physical server running Exchange (if scalability is not an issue). Therefore, to run MSCMDM requires at least the addition of one physical server (VPN), and the creation of a DMZ. A minimal configuration most likely to occur in small installations is illustrated in Figure 3 below.

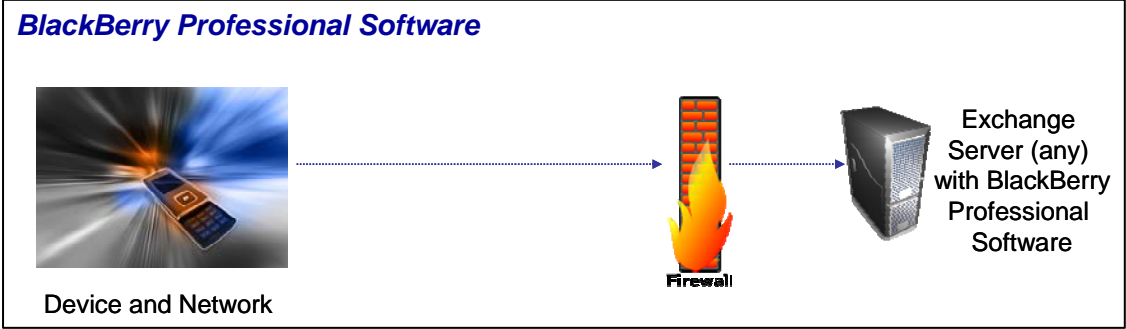
Figure 3: Microsoft MSCMDM Minimal Configuration



Appendix 4: Utilizing BPS

For those companies with older versions of Exchange, and/or mobile devices without the ActiveSync Direct Push capability, the only way to obtain push email for their Exchange installation is through a third party add-on. This adds cost and a level of complexity beyond the out-of-the-box Exchange solution available from Microsoft. We believe that to date, few smaller companies have standardized on an all-Microsoft solution (e.g., newest version of Exchange, newest version of Windows Mobile powered devices). Further, the Microsoft out-of-the-box experience may not be an optimum solution for many companies, making a third party solution the best choice even for the smaller installation. Therefore, BPS may be a better alternative for many smaller companies, providing enhanced security and management while limiting the level of complexity (see figure 4).

Figure 4: BlackBerry Professional Software



About the author

Jack E. Gold is Founder and Principal Analyst at J.Gold Associates. Mr. Gold has over 35 years in the computer and electronics industries, including work in imaging, multimedia, technical computing, consumer electronics, software development and manufacturing systems. He is a leading authority on mobile, wireless and pervasive computing, advising clients on business analysis, strategic planning, architecture, product evaluation/selection and enterprise application strategies. Before founding J. Gold Associates, he spent 12 years with META Group as a Vice President in Technology Research Services. He also held positions in technical and marketing management at Digital Equipment Corp. and Xerox. Mr. Gold has a BS in Electrical Engineering from Rochester Institute of Technology and an MBA from Clark University.

About J.Gold Associates

Founded by an internationally recognized expert and industry veteran with over 35 years of experience in engineering, product marketing, market research and analysis, and technology advisory services, J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com