Mobile operations management

Build a strong infrastructure for business mobility

Table of Contents

Executive summary .................................................. 2
The mobile reality: flexibility with no downtime ............... 2
The mobile imperative: integrate or get left behind .......... 2
Operations are diversifying with mobility ....................... 3
Consolidate operations to fully adopt mobility ............... 3
Device management ............................................... 4
Network availability management ............................... 4
Applications management ....................................... 5
Mobile security options ......................................... 6
Virtual private network (VPN) .................................. 6
Network access control (NAC) ................................ 6
Encryption .......................................................... 6
Intrusion detection and prevention ............................ 6
Data leakage prevention (DLP) ................................. 6
Beyond the box: mobility know-how ......................... 7
Glossary .......................................................... 7
Product spotlight .................................................. 8
Executive summary

Mobility gives a business more choices about how its workforce utilizes time, where employees perform their work, how it meets customer and partner needs, and what information it can make available. All of these choices, however, must be managed properly. Networks must be cultivated to enable mobility, while devices must be acquired that power it. Applications must be chosen that integrate mobility with business processes, while security strategies must be devised that protect the business data transmitted among all of these components. As mobility becomes a fact of doing business today, companies must consider how they will consolidate the management of all of these choices in time to stay ahead of the curve of “ubiquitous mobility” (in which wireless users experience a seamless transition as they travel from network to network, public or private, urban or remote).

“As this trend continues, more enterprises will take on mobility as a core IT initiative in 2008, spreading the benefits of a mobile work style to a larger portion of users than ever before.”

— Forrester Research, Topic Overview, Enterprise Mobility, July 2007

The mobile reality: flexibility with no downtime

With mobile solutions, the realities of time and distance shift in your favor. Downtime is uptime. Employees have the flexibility to turn the minutes spent waiting for a flight into the minutes spent closing a deal. Location limitations become nonissues. Businesses gain access to pools of talent in cities far flung from their own, as well as the ability to respond quickly to their customers’ needs even when key employees are absent from the office. This flexibility and fluid uptime become assets that can create a competitive edge. Employees are able to manage their days in favor of both the business and their personal lives, making companies more responsive to customers, and employees more likely to stay and cultivate the business.

The mobile imperative: integrate or get left behind

It is no surprise that analysts are heralding business mobility as an imperative. The days of surprising your customers with quick responses from the field or beating your competition with a secret weapon of mobile flexibility are coming to an end. Mobile solutions are a fact of doing business today. In fact, the time of ubiquitous mobility is nearly upon us. “This level of services, infrastructure and device maturity will become attainable in the 2012 to 2013 time frame,” predicts Forrester Research. (Forrester Research, Mobile Evolution: Moving Toward an All-Wireless Enterprise, September 2007.)

The time to recognize mobility in your operations with the same level of integration as any other business-critical capability is now. And that will require a centralizing of mobility-specific operations with the rest of your IT and business processes, and perhaps even a specialized role to facilitate it.
Operations are diversifying with mobility

As businesses go mobile, the needs and capabilities of their IT operations change. Enabling mobility in any enterprise will require that careful attention be paid to four main areas:

- Devices
- Networking
- Applications
- Security

These areas are not foreign by any means to the IT department, but mobility complicates their management. As tech-savvy consumers, your users have expectations of IT performance and — specifically — network accessibility that are at an all-time high. Applications that make handhelds function as mini-PCs, changing business processes forever, hit the market with growing speed. The devices themselves are getting cheaper and more business-friendly, while the malware that preys upon them becomes decidedly less so. And with the increasing number of business transactions — whether simple, such as communications (e-mail, instant messaging [IM], voicemail), or sophisticated, such as inventory inquiries, order status and customer financials — the damage that can be done by security breaches associated with mobile solutions that function outside the firewall cannot be overstated.

Consolidate operations to fully adopt mobility

Managing mobility as a mission-critical capability will require you to evaluate your processes, budgets and roles to combine efforts and operate more efficiently. To get the most out of mobile solutions onsite, internal network configurations will have to be optimized for wireless devices such as notebooks and smartphones. You’ll need to decide how these devices will gain productive access to the network from outside the firewall on public networks. Carrier plans need to be chosen and monitored well. Devices must be chosen and managed according to business need and network functionalities. And the mobile workforce must be educated on policies specific to device usage, data handling and network access in order to maintain a strong security profile.

As you heed mobility’s effects on your IT and business operations and decisions, you’ll probably find that a mobility operations manager role begins to take shape, straddling both worlds. Set expectations with executives about this possibility, so you do not meet with resistance when the need to have a central role that bridges the gap between conventional and mobile IT processes becomes evident.

“But to streamline mobility decisions and maintain the edge mobility investments provide, it’s critical that companies take into account the multiple elements they must manage. Forming a mobile operations role is the right path toward managing this complexity.”

— Forrester Research, The Business Mobility Imperative, June 2008
Five tips for getting the most out of your mobile carriers

1. **Know your service needs.** Understand the kinds of devices in your employees’ hands and what services best match the capabilities of those devices.

2. **Know your service usage.** Account for which services — voice only, voice plus data, short message service (SMS), Internet, e-mail — and how many minutes each user or department consumes monthly so you can optimize your plan accordingly.

3. **Make them earn your business.** Don’t hesitate to negotiate for more minutes, free services or discounts.

4. **Regularly reassess your carriers’ coverage areas.** See if you can consolidate carriers across regions as coverage areas grow. (Be careful: consolidating down to only one carrier can decrease your coverage and your negotiation leverage.)

5. **Remember to provide for international travel.** Services abroad can be costly. If you have frequent travel overseas, make sure you have a plan that includes appropriate coverage.

---

**Device management**

Where mobile operations are concerned, the device needs of a business fall into two primary categories: procurement and enablement.

Deciding whether to restrict devices to being company-owned or to allow personal devices is the first issue you should get a handle on when acquiring (or allowing) mobile devices on the network. There is no simple or right answer. Your approach to this will depend on your users, network capabilities, business needs and budget. With company-owned devices, your company has final say about every aspect of a device it owns, which can be of great benefit. However, if you’ve got a healthy population of prosumers who bring their own devices to the table, and you’d like to leverage that resource, remember that there are solutions such as desktop virtualization and measures such as virtual private network (VPN), network access control (NAC), data leakage prevention (DLP) and encryption that go a long way toward securing your data on employee-owned or third-party devices.

The second thing to consider for device manageability is enablement. Just as software helps to simplify the management of conventional clients, software is also available that simplifies the management of an enterprise’s multitude of mobile devices. So, regardless of the mixture of company-owned, employee-owned or third-party devices, there are suites available that make the monitoring and remediation of your mobile devices easier and more effective.

**Network availability management**

Internally, you must ensure that your network infrastructure is optimized to support mobility to your company’s greatest advantage. For example, as you march toward ubiquitous mobility, you’ll need to evaluate when you go from 802.11a/b/g standards to 802.11n, or when you let go completely of wired networking. You must also strike a balance between ensuring network security and making the network a guest-friendly place for clients, partners and even field reps who spend frequent time onsite.

Externally, there are two main things to consider: 1) how effective your devices are in gaining secure, productive access to external networks, and 2) whether or not you’re getting the best mobile services possible from your carriers. These are related but separate issues to manage, as the capabilities you require of your devices directly affect the kinds of services you can take advantage of and vice-versa. You’ll also need to consider when you invest in devices with up-and-coming capabilities, such as worldwide interoperability for microwave access (WiMAX).
Applications management

When managing applications for your mobile solutions, you’ll have to consider a variety of them. There are the device management applications, as discussed earlier. Then there are applications that expand the capabilities of mobile devices to behave like mini-PCs, such as e-mail or Internet browser applications, or common desktop word processing and visual programs. Finally, there are applications, such as customer relationship management (CRM) or sales and inventory management, that extend role-based or job-specific functionality from desktops to handhelds. It is this latter group of applications that will have the most profound effect in allowing mobile capabilities to influence business processes at your company.

Some analysts predict that applications will play the most significant role in steering mobile technology’s adoption and impact on productivity. After conducting a survey of 535 network and telecommunications decision makers in North America and Europe, Forrester estimated that “companies have enabled roughly 10% to 20% of their employees to use applications. It also says that leading firms are extending line-of-business applications to handhelds, with more than 24% of the firms interviewed using mobile CRM and 22% using field service.” (Forrester Research, Topic Overview: Enterprise Mobility, July 2007.)

When devising a mobile operations strategy enabled by applications, it is essential that you have someone who can account for the capabilities of the mobile devices in use by the company. This goes back to the need for a mobile operations manager or similar role. IT may identify the perfect application for the job, but could inadvertently miss how many employees perform that role on mobile solutions. If the application isn’t compatible with the predominant type of device, or with the delivery of service to the devices, it is an application purchase that will never realize its intended return on investment.

“Leading companies are thinking beyond just mobilizing applications — they’re optimizing business processes, which often span multiple applications.”

— Forrester Research, Key Device Trends That Will Shape Enterprise Mobility in 2008, February 2008
Mobile security options

Because mobile devices reside outside the company firewall and beyond the reach of corporate security policies, they are often hotbeds of unauthorized activity. Users can inadvertently pass viruses, spyware and other malware to the company network through the VPN. It still matters that a network has a formidable configuration of layered security, but when a notebook is lost or stolen, your network data and any data stored on the notebook’s hard drive is up for grabs. You’ve got to have a way to protect that data regardless of its location or place of breach. Here’s a quick rundown of some security options available to you to help address these concerns.

**VPN**

Many organizations use Internet Protocol Security (IPSec) VPNs, but the fact that IPSec works at the network layer can mean greater exposure of the entire network to malware found on remote machines. The newer Secure Sockets Layer (SSL) VPN technology works at the transport layer of the Transport Control Protocol/Internet Protocol (TCP/IP) stack and is session-oriented, offering more precision in granting access — even down to a specific application, file or window of time. More vendors are offering all-in-one appliances that package not only VPN working on both layers, but also firewall, intrusion prevention and network antivirus.

**NAC**

NAC gives the network the ability to grant access to a device based on preset criteria, then monitor it throughout its connective cycle. If the device behaves in a way that’s out of line with policies, the device is quarantined, given an opportunity to remediate and then disconnected if it remains noncompliant.

**Encryption**

A data-level form of protection, encryption is centrally managed and updated. It works by jumbling data according to a complex algorithm that machines are able to unlock once they’ve been authenticated. Everything from a single file to the entire hard disk can be encrypted.

**Intrusion detection and prevention**

Intrusion detection and prevention systems focus on identifying incidents, logging information about them, taking action to stop intrusions and reporting incidents to administrators for further review. These systems work well to stop unusual IPs and to block worms, botnets and other malware. They add an additional layer of security between the firewall and antivirus software.

**DLP**

Secure your data, regardless of where it is in relation to the network, with DLP technology. DLP solutions tag data based on a set of criteria such as location of data, application type, file type, keywords and common data strings. These tags alert IT when the data is being used in a certain manner. DLP can prevent the data from being copied, e-mailed, sent via IM, printed, saved to a different device, changed to a different file type or otherwise altered.
Beyond the box: mobility know-how

When you look for consultants outside of your organization to help you centralize mobility operations, plan wisely and make the right investments for your remote access security, look no further than CDW. We evaluate your current applications and network and help you develop an appropriate strategy for your business mobility. Our dedicated team of mobile wireless specialists brings its deep knowledge of a broad number of mobile and wireless solutions to assist you with activating of new devices, adding to existing carrier contracts and guiding you through a vast array of wireless notebook options.

With a dedicated account manager as our single point of contact, your team of certified professionals becomes a seamless extension of your own IT staff. You get specialized software and hardware expertise that might otherwise involve expensive consultation or dedicated employees. We assess, plan, implement and support, beginning with free consultations from our mobile wireless specialists. Then we work behind the scenes to review the best options for the job and present you with those options. After your purchase, our work is just beginning. Your solutions are configured in state-of-the-art ISO 9001:2000-certified configuration facilities. Whether you need onsite assistance or postsales support products, we and our service partners deliver support that’s second to none. Our vendor-neutral approach means that you get to choose the best products for you, period, from the deepest selection of hardware and software available.

Glossary

Data leakage prevention (DLP): Technology that tags data according to its location, application type, file type, keywords and common data strings, alerting IT when tagged data is being used in a certain manner. This makes it possible to prevent the data from being copied, e-mailed, sent by IM, printed, saved to a different device, changed to a different file type or otherwise altered.

Network access control (NAC): Network security that includes health assessments for devices connecting to the network as well as automated threat mitigation and remediation. Infrastructure-based NAC incorporates NAC capabilities into routers, firewalls, software and other aspects of your network, so that turning on your network automatically means turning on NAC. Appliance-based NAC integrates multiple network security functions into a single device. Endpoint software-based NAC relies on individual firewalls, protection for wireless devices and USB sticks, and content filtering to block threats at the point of contact. Most full NAC solutions integrate appliances and endpoint approaches.

Personal digital assistant (PDA): Small, handheld computers. Examples include Palm organizers and BlackBerries.

Smartphone: Phones enabled by a software platform to do more than connect phone calls. They have screens to display a wider variety of data than simple cell phones, including but not limited to such applications and functions as e-mail, web browsers, contact database and audio/visual technology. A smartphone is a type of PDA, but a PDA is not necessarily a smartphone.

Ubiquitous mobility: A generally accepted concept of the future state of mobility in which users and devices will be able to connect seamlessly from network to network, uninterrupted, regardless of urban or rural locations.

Virtual private network (VPN): Provides secure, private connections to remote workers and branch offices. VPN strengthens security through dual password authentication, security tokens and encrypted tunnels created over public IP lines.

Worldwide interoperability for microwave access (WiMAX): A telecommunications interoperability standard for IEEE 802.16 networks.
Product spotlight

Our deep selection of products like these ensures that you can focus on your mobility needs while we focus on meeting them.

BLACKBERRY® T SUPPORT
Provides comprehensive technical support and software maintenance services for your Blackberry® solution
Technical Support Services (TSupport) is an annual subscription program that provides software maintenance and technical support services for your Blackberry solution.

TX1 support
Per Server Fee
CDW 900300
Per CAL Fee
CDW 900301

TX2 support
Per Server Fee
CDW 855038
Per CAL Fee
CDW 873226
Additional levels of support, for those who require the highest server and device availability, can also be acquired at CDW. Please contact your Mobile Wireless Specialist for details.

BLACKBERRY ENTERPRISE SERVER™
Robust, scalable, all-in-one wireless solution
• On-the-go access to e-mail, personal information management, voice and web
• Allows you to connect and collaborate with all the tools and applications necessary for you to make important decisions quickly
• Integration with third-party online research tools
• Advanced security features to protect the integrity and confidentiality of client data and your firm’s information
Enterprise Server Edition for Microsoft Exchange
One server, 20 users
CDW 950822

BLACKBERRY 8800 SERIES
Integrated Wi-Fi® for increased in-building coverage and fast data connections
• Quad-band GSM/GPRS/EDGE provides global roaming capability
• Integrated Wi-Fi networking — connect to a Wi-Fi network for additional data coverage and ultra-fast data connections at work or home
• Built-in Global Positioning System
• Work and personal e-mail pushed to your Blackberry
Call your CDW account manager for more information on specific EDCs.

BLACKBERRY CURVE™ 8300 SERIES
Stay connected with the BlackBerry Curve
• Quad-band GSM/GPRS/EDGE provides global roaming capability
• Built-in Global Positioning System
• Bluetooth® 2.0 with stereo headset support, speakerphone and voice-activated dialing
• Access up to 10 e-mail accounts
• Review Word, Excel® and PDF documents
Call your CDW account manager for more information on specific EDCs.

Contact your CDW account manager today to see how CDW can help you design and purchase the right mobility solutions for you, or visit CDW.com/mobileoperations

The terms and conditions of product sales are limited to those contained on CDW’s website at CDW.com; notice of objection to and rejection of any additional or different terms in any other form delivered by customer is hereby given; CDW®, CDW®G® and The Right Technology. Right Away.® are registered trademarks of CDW Corporation; all other trademarks and registered trademarks are the sole property of their respective owners.