THE DOZEN CHALLENGES
to successful mobile deployments
eBook

NETMOTION®
WIRELESS

THE DOZEN CHALLENGES
to successful mobile deployments
eBook

IT SERVICE DELIVERY

#1 Automate Patch Management and Upgrades

#2 Keep Trouble Tickets in Check

#3 Achieve Reliable Operation Without Burdening IT

ORGANIZATIONAL SECURITY

#4 Enforce Security Without Hampering Workers

#5 Protect Against Stolen Devices or Unauthorized Access

#6 Gain Control over Workers, Devices and Networks

USER EXPERIENCE

#7 Foster User Acceptance and Manage Change

#8 Make Wireless Network Use Seamless

#9 Deliver Seamless Access to More Applications

BUSINESS OPERATIONS

#10 Gain Visibility Into Corporate Asset Use

#11 Keep Wireless Access Charges in Check

#12 Be Ready to Scale

INTRODUCTION

As wireless network capacity expands and mobile devices become more powerful, enterprises are able to bring full application access directly to mobile workers in the field.

Those workers roam across multiple networks, use multiple connection types and encounter coverage gaps, all while **EXPECTING THE SAME RELIABLE, CONTINUOUSLY AVAILABLE ACCESS TO NETWORK RESOURCES THAT THEY EXPERIENCE IN THE OFFICE**.

But the difference between wired and wireless environments presents a set of challenges. **KNOWLEDGE OF THEM UP-FRONT WILL ASSIST IT DEPARTMENTS AS THEY PLAN THEIR MOBILE DEPLOYMENTS**.

What follows are **the top 12 challenges** that organizations may face as they expand their mobile workforce and systems to support them, and the solutions to help overcome them.

AUTOMATE PATCH MANAGEMENT AND UPGRADES

Managing a large mobile deployment on a device-by-device basis can be an administrative nightmare. Ideally the same systems management suites used on the internal wired network can be extended to the mobile environment, allowing those devices to be managed "over the air."

Patches and upgrades can be applied after-hours, or at other times when users aren't actively using or logged onto their devices, to avoid impacting productivity.

"BANDWIDTH-AWARE" CAPABILITY ENSURES THAT SYSTEMS MANAGEMENT PROCEEDS NOT JUST AT AN APPROPRIATE TIME, BUT OVER A CONNECTION WITH APPROPRIATE SPEED.

Depending on use patterns and the various connections available, that optimal connection might be over a cellular network after-hours; while a device is in range of a corporate Wi-Fi connection in a parking garage; connected via home Wi-Fi; or mounted in a docking station.

CHALLENGE #2

KEEP TROUBLE TICKETS IN CHECK

A mobile environment adds new variables to the application-delivery equation including intermittent connectivity, access over third-party networks, and a need for more complex security and authentication schemes.

A solution that manages the complexities of connections on the worker’s behalf, effectively taking connection problems out of the equation, has been shown to greatly reduce the number of help desk calls. **THIS NOT ONLY LOWERS SUPPORT COSTS BUT ELIMINATES THE LOST PRODUCTIVITY THAT THOSE SUPPORT CALLS REPRESENT**.

CHALLENGE #3

ACHIEVE RELIABLE OPERATION WITHOUT BURDENING IT

Just as the wireless infrastructure should be “hands-off” for the user, it should be “hands-off” for IT as well. Active load-balancing and automated failover built into a solution allow a “set-and-forget” operation.

A proactive alerting capability allows the IT department to manage by-exception and receive automatic notification of problems or potential problems, without having to constantly monitor the deployment.

OFTENTIMES, THEY CAN INTERVENE BEFORE ISSUES IMPACT WORKERS AND TRIGGER TROUBLE TICKETS.

CHALLENGE #4

ORGANIZATIONAL SECURITY

ENFORCE SECURITY WITHOUT HAMPERING WORKERS

Protecting data and devices from unauthorized access is important, but can require a balancing act. Authentication needs to be straightforward and a lost connection shouldn't require workers to have to perform repeat logins.

Devices need verification that security precautions are active to avoid introducing malware that would place the enterprise and its user community at risk. Data streams need to be encrypted to protect corporate information and, in some cases, to meet regulatory requirements.

An ideal solution accounts for all of these security concerns, in a way that doesn't burden the user into having to take extra steps, and protects assets in a way that is as hands-off as possible.

CHALLENGE #5

PROTECT AGAINST STOLEN DEVICES OR UNAUTHORIZED ACCESS

A mobile device configured to access internal applications and data that is lost or stolen can be a huge security risk. The ability to immediately quarantine a device that has been reported lost, or to recognize that a device is being used by an unauthorized person (through too many wrong password attempts) protects the corporate network.

DIGITAL CERTIFICATES MAY ALSO BE USED TO VERIFY THAT ONLY DEVICES THAT HAVE BEEN PREAPPROVED MAY CONNECT TO CORPORATE RESOURCES; this prevents a user from using corporate credentials to connect via an unsecure home machine or other personal device.

A common practice is to automatically place any newly distributed device into immediate quarantine on the first connection, so the administrator can verify the device's configuration and user identity before allowing full access.

CHALLENGE #6

ADMINISTRATORS NEED CONTROL OVER

WHO is using a device, through authentication that integrates with corporate directories for easier management.

WHAT devices may connect, and the users who are authorized to use them.

HOW AND WHERE specific applications are being accessed and over which networks.

GAIN CONTROL OVER WORKERS, DEVICES AND NETWORKS

Mobile assets are constantly on the go and this presents challenges that don't exist with fixed assets tethered to a wired network.

The ideal solution incorporates **FLEXIBLE POLICY CONTROL**. Devices and users may be given a degree of freedom to access the Internet and use other applications. Or they may be tightly locked down so that only specific applications are allowed access, with enforcement via controls that cannot be bypassed.

CHALLENGE #7

USER EXPERIENCE

FOSTER USER ACCEPTANCE AND MANAGE CHANGE

Mobile workers are like any other worker – their focus is on doing their jobs. If technology gets in the way or is too cumbersome to use, the entire mobile deployment may fail.

Furthermore, the users themselves may introduce problems of their own making. Putting too many options in their hands might allow them to accidentally cripple their devices, open security holes, or bog down the access networks.

THE BEST SOLUTION IS ONE THAT REQUIRES MINIMAL USER INTERVENTION AND MAKES THE UNDERLYING TECHNOLOGY AS TRANSPARENT AS POSSIBLE.

CHALLENGE #8

MAKE WIRELESS NETWORK USE SEAMLESS

Most mobile deployments require multiple cellular networks, often augmented with Wi-Fi access points, to provide reliable coverage throughout the organization’s entire service area. Mobile workers shouldn’t have to log in to separate networks, worry about making configuration changes, or deal with the other intricacies and complexities of mobile access.

IDEALLY THE MOBILE ENVIRONMENT MIMICS THE IN-OFFICE WIRED EXPERIENCE.

- Furnishes a single sign-on
- Allows the worker to access multiple networks as though it were a single network
- Does it all within a single persistent session so workers only have to log in once
- Pushes down any necessary configuration changes without user intervention

THIS USER-TRANSPARENT EXPERIENCE IS ALSO EASIEST FOR THE IT DEPARTMENT TO SUPPORT.

Share this eBook

CHALLENGE #9

DELIVER SEAMLESS ACCESS TO MORE APPLICATIONS

The number of applications and types used by mobile workers is growing, beyond scheduling and dispatch. More and more, customer and task-specific applications are being deployed that are an integral part of doing the in-field job.

These applications are rarely if ever designed with mobile access in mind, where connections break without warning (for instance, when a user goes out of range) which in turn makes the applications prone to crash.

APPLICATIONS CAN INCLUDE:

CRM, **work-order management**, **GIS and mapping**, **parts inventory databases** and many more. **Voice-Over-IP**, **camera software** and **video software** enable new capabilities for communicating from the field.

The easiest way to manage the problem is with **A SOLUTION THAT ALLOWS ANY SOFTWARE USED IN A LAN ENVIRONMENT TO BE USED IN A MOBILE ENVIRONMENT**. It is also useful to prioritize application traffic that is critical or time-sensitive over less-critical traffic.

CHALLENGE #10

BUSINESS OPERATIONS

GAIN VISIBILITY INTO CORPORATE ASSET USE

Investments in wireless technology including devices, networks and the supporting infrastructure are like any other business investment and it is important to know they are performing and delivering properly. **AN IDEAL SOLUTION WILL DELIVER VISIBILITY ON THREE LEVELS:**

Real-time Visibility: Real-time visibility lets administrator immediately see which devices are causing problems and take immediate action.

Proactive Alerting: This critical capability notifies administrators that devices or users are in need of attention, so that IT personnel don't have to spend time watching for problems, but can focus instead on fixing them.

Reporting and Analytics: This capability allows administrators and managers to see the big picture of service delivery, know when assets are being underutilized, and plan for the future.

CHALLENGE #11

KEEP WIRELESS ACCESS CHARGES IN CHECK

As cellular carriers replace unlimited-use data plans with usage-based rates, enterprises face a new cost-control challenge.

ANALYTICS CAPABILITY, which monitors network use for appropriateness, helps administrators keeps unnecessary tasks off of cellular networks.

USER-TRANSPARENT CONNECTION MANAGEMENT switches automatically to free or lower-cost Wi-Fi where it is available.

COMPRESSION AND LINK OPTIMIZATION can significantly reduce bandwidth consumption while improving performance.

CHALLENGE #12

BE READY TO SCALE

For organizations that have overcome the preceding eleven challenges of a mobile environment, the twelfth is scaling the mobile environment.

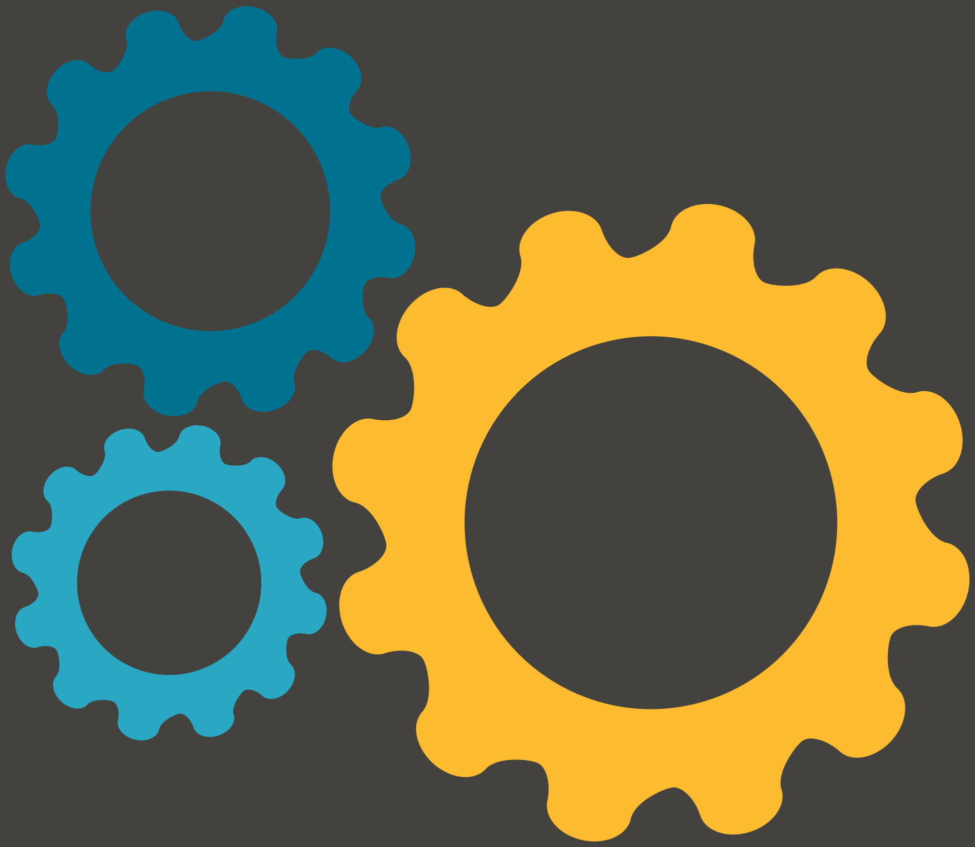
SUCCESSFUL ORGANIZATIONS HAVE OFTEN EXTENDED THEIR ORIGINAL MOBILE DEPLOYMENTS TO NEW USERS, including additional classes of mobile workers and even executives, sales personnel and other “road warriors”.

While some of these users might be served by an SSL-VPN or IPsec VPN, they can be more effectively served by a solution that handles **THE SPECIFIC DEMANDS OF A FULLY MOBILE WORKFORCE**.

CONCLUSION

Managing an enterprise mobility employment can be complex.

The more the wireless environment can operate and be managed like a wired environment, **THE MORE LIKELY IT IS THAT AN ENTERPRISE MOBILITY INITIATIVE WILL BE SUCCESSFUL.**



To learn about mobile deployment {~ to receive a more detailed version of this eBook, visit NetMotionWireless.com.

Or contact us at:
1.866.262.7626
info@netmotionwireless.com

ABOUT NETMOTION WIRELESS

NetMotion Wireless develops software to manage and secure wireless data deployment for organizations with mobile field workers. Our products address the unique challenges introduced by the use of wireless, enabling customers to maximize the return on investments in workforce automation. More than 2,000 of the world's most respected organizations across multiple industries including utilities, healthcare, telecommunications, public safety, government, insurance, manufacturing, and many others use NetMotion Wireless products.

NETMOTION® WIRELESS