

INDUSTRY SPOTLIGHT

Enterprise Mobility in the Telecommunications Industry

**How a Mobile VPN Creates Better Service for
Customers and Increased Productivity for Employees**



Prepared by
NetMotion Wireless

Executive Summary

Mobile-technology initiatives deliver tangible benefits in improved customer service and increased productivity for telecommunications companies. As these organizations have learned, a mobile virtual private network (VPN) is the key to achieving best practices in their deployments and realizing the full benefit.

A mobile VPN provides secure, reliable network connections for adjusters, builds acceptance to overcome common change-management issues, and allows greater span-of-control for managers and IT staff.

The Drivers Behind Mobile Initiatives

Telecommunications companies offer an increasing variety of services in a highly competitive market. Installations can be complex in a business that is becoming more and more service-driven. To meet the challenges, companies are giving their service fleets direct online access to applications.

These applications serve up customer data and technical information, provide access to and manage parts inventory, and communicate vehicle locations to make dispatch more efficient.

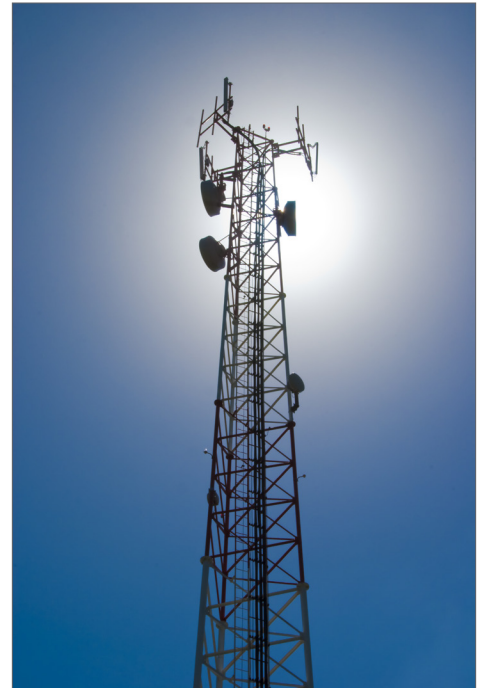
Among the larger telcos, service fleets number in the thousands to tens of thousands of employees and trucks. Minor increases in productivity such as improvements in first-call completion and fewer calls to dispatchers can have huge bottom-line impacts.

The Role of a Mobile VPN

Implementing a mobile-computing system can be a challenge because it typically involves significant organizational change and new work habits. Selecting the right VPN – an often-overlooked yet vital piece of the infrastructure – is essential to facilitating a successful rollout. A mobile VPN acts as the foundation to any mobile deployment, ensuring essential management and visibility into mobile devices and their activity, establishing security policies and enforcing them, and creating persistent connections for field workers, enhancing their productivity.

Results often seen when deploying a mobile VPN include:

- Increase in mobile worker efficiency
- Enhanced customer service
- Reduced IT support needs for mobile workers
- Greater security to the overall network
- Reduced complexity in the deployment of applications to mobile devices



A mobile virtual private network acts as the foundation to any mobile deployment, ensuring the management, security, and productivity elements necessary to ensure a successful mobile deployment.

Mobile Vs Conventional VPN

Like a conventional VPN, a mobile VPN secures enterprise data across public networks through encryption, and protects corporate networks by ensuring that only trusted users and devices gain access. However, it does much more. It is the key to delivering the full benefit of the entire mobile deployment.

NetMotion Wireless Mobility XE is expressly designed for the unique characteristics of mobile environments, where workers roam and use computing devices constantly, while expecting uninterrupted use of open applications throughout the workday. Mobility XE is the essential “glue” that ties together multiple networks including various cellular data services and Wi-Fi, aggregates disparate mobile devices, and manages them as a single virtual network and deployment.

After deploying Mobility XE, telecommunications service organizations reported their workers completed more tasks in a day, spent more time in the field, and were overall more productive.

Any application that runs over a wired network works in a wireless environment with Mobility XE. It allows field-service forces to go beyond paper systems or simple dispatch functions to directly access applications such as:

- Mobile workforce / work order management
- Scheduling / dispatch
- GIS & mapping
- Asset management
- Service diagnostics / repair
- CRM
- Order entry / delivery
- Automatic vehicle location (AVL)

Where policies allow, workers may also access:

- Standard office applications
- General internet browsing
- Corporate E-mail



Real Results: Comcast Implements Strategic Field Service Initiative

Comcast replaced a paper-and phone call-based system with hand-helds accessing applications over cellular networks. Deploying Mobility XE mobile VPN allowed the application sessions to persist despite interrupted connections for field technicians, increasing productivity and customer calls.

“The Comcast Dream Big initiative includes a customer guarantee that we’re going to keep the appointment, be on time and be there when convenient for our customers. The key to getting there was connecting technicians to our applications through a secure, reliable method. That’s the big piece of the problem that Mobility XE solves for us.”

– Greg Otto
Sr. Director of Infrastructure and Operations, Comcast

Deployment Best Practices

There are many commonalities to the challenges that telecommunications companies face in mobility field deployments. Understanding them is key to developing a successful mobile computing environment.

Lack of User Acceptance

The most common reason for failed mobile deployments is lack of user acceptance. If field tools are cumbersome or difficult to use, workers will not embrace them. And as many organizations have discovered, connectivity problems are the most common source of frustration. Workers often lose connections and need to re-log in; and when applications are running during those interruptions they often crash, requiring workers to not only log in again, but re-enter the data they lost.

Mobility XE makes the wireless experience secure and transparent. It handles logins automatically as service technicians transition between various cellular networks and access points, and keeps the applications and connections alive as they traverse those boundaries and encounter coverage gaps.

This is especially important since many telecommunications companies employ multiple cellular carriers for wireless connectivity. In fact, the most common technical reason cited by telcos for using Mobility XE is to allow workers to roam between these cellular networks and in some cases, to also use Wi-Fi hotspots.

Removing the Complexities

With Mobility XE, workers only need to log in once at the beginning of their shift and enjoy a seamless user experience. This single sign-on also supports two-factor and multi-factor authentication via RSA SecurID (used by many telecommunications service fleets) or alternatively, smart cards or device certificates. Workers freely use their devices without having to manage connections. Plus they can suspend or hibernate devices throughout the shift without having to reauthenticate or risk data loss. Data connections remain secure without hindering users.

In mobile deployments that began with conventional VPNs and were subsequently replaced with Mobility XE, this simplified user experience led to significant productivity gains. In new deployments, it delivers a positive user experience that facilitates change-management and speeds adoption of field tools.

Managing, Controlling and Securing Mobile Devices

Managing mobile devices across a dispersed workforce is a challenge, and more so in large deployments. Securing and maintaining hundreds or thousands of field-based devices, miles from the corporate data center, is much easier with Mobility XE.



Real Results:

Cox Communications Reaps a Half-Million Dollars in Yearly Savings

IT Administrators at Cox Communications use the Mobility XE Policy Management module to manage application and network access across for its 3,500 field technicians. Management through Mobility XE and Sybase iAnywhere's Afaria allows Cox to deploy and update software on the mobile devices remotely, resulting in IT savings estimated at a half million dollars a year.

“NetMotion Wireless software helps us overcome everyday wireless coverage gaps and interruptions. Their solution is helping to make our field service operation more efficient, ultimately helping us to deliver better service to our customers.”

– Al Briggs
 Director, Mobile Solution Services, Cox Communications

Control Over Device Use

Giving the IT team and field managers control over remote devices allows them to:

- Set and enforce policies to manage user and device access to networks
- Improve security and protect users from inadvertently taking action that bogs down devices or connections
- Set rules to limit access to specific applications, prohibit web browsing, or restrict access to intranets or specific sites
- Enforce restrictions based on connection speed or time-of-day
- Prioritize users by line-of-business applications, so critical traffic has the highest priority

This policy-management capability is especially useful for keeping file synchronizations and other large data transfers off of cellular networks, where they might interfere with customer-related and service applications. Workers carrying laptops, handhelds or smartphones can all have different policies, or supervisors may have policies separate from the workers they manage.

Visibility Into Usage Patterns and Problems


Monitoring performance across multiple networks is a challenge, especially when networks are outside of IT’s direct control. Mobility XE provides an Analytics module that measures and reports on device, application and network usage. Administrators can spot coverage or connection problems, find high bandwidth consumers, drill down to monitor traffic patterns, verify version details, monitor battery life and much more. In addition, proactive notifications based on adjustable thresholds can dramatically decrease help desk calls. Staff are alerted to potential device or network problems so they can be resolved before they disrupt workers or impact service quality.

For installers whose tasks often find them atop telephone poles or cellular towers, a mobile VPN can provide an added level of safety. An active device indicates that all is likely well, and the mobile device also provides a reliable communications link.

Enforce Device Security

Mobility XE’s Network Access Control capabilities verify that devices have required security precautions in place – such as patches, operating system updates, and active antivirus with current signatures – before allowing a connection.

Depending on the severity of the issue, administrators may choose from a variety of actions, ranging from simply warning the user, to requiring immediate re-mediation, to quarantining the device. This gives administrators the flexibility they need to protect the corporate network without hampering worker productivity. They can also automatically re-mediate the device, at a time and in a way that doesn’t interfere with its productive use.



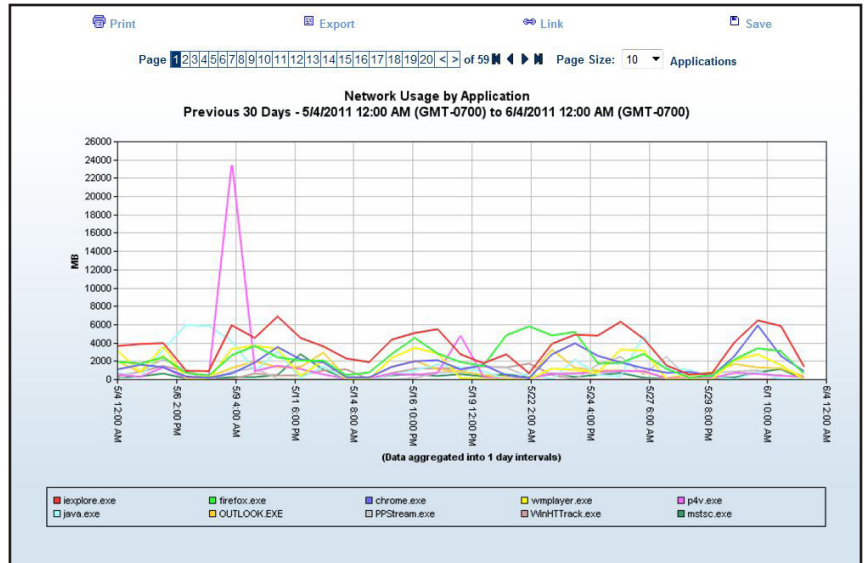
Real Results:
Windstream Realizes Field Service Productivity Gains

Windstream Communications delivers telephone, high-speed Internet and high-definition digital TV throughout largely rural areas. With Mobility XE, connections survive the inevitable gaps in cellular coverage; technicians have hassle-free, continuous application access; and they remain logged into the home network at all times. Mobility XE delivers secure, always-on, always-reliable connections to Windstream technicians – so Windstream can keep their customers connected.

Patch Management and Upgrades

Mobility XE allows devices to be managed “over the air”, through third-party systems management software, as easily as the organization manages desktops and laptops on the wired corporate network.

Application updates and patches may be pushed out while the unit is still in the field, but when users aren’t actively logged on, between shifts. This eliminates the need to dock a unit or wait for a wired connection and can provide significant labor and cost savings for IT staff.



NetMotion Wireless Mobility XE Analytics module allows managers to monitor network usage by application and by user, allowing for informed decisions about access policy and security

Conclusion

Mobile initiatives deliver clear bottom-line results for telecommunications service fleets. Deploying a VPN built for mobility such as Mobility XE is essential to realizing the full benefits of the investment and achieving best practices. These include delivering secure, reliable network connections, promoting user acceptance, and gaining management visibility and control. In this way, competitive telcos can ensure that they achieve greater productivity and deliver exceptional customer service.

Learn More

For more information about best practices in mobility deployments, please visit www.netmotionwireless.com