NetMotion Wireless Mobility XE™— the Industry's Leading Mobile VPN

Mobile VPN—the Fulcrum of a Successful Mobile Deployment

The benefits of mobility are compelling—increased worker productivity, lower operational costs, and improved customer service and support. A successful mobile deployment empowers mobile workers with the resources they need to be effective—resulting in faster business transactions, improved customer service, and ultimately, happier customers and increased revenue.

At the fulcrum of a successful mobile deployment is a **Mobile Virtual Private Network (Mobile VPN)**— providing mobile, wireless workers with secure, reliable, remote access to network resources and information from virtually anywhere. Only a Mobile VPN is designed to deal with the unique challenges associated with mobile computing such as wireless security, performance and roaming.

Improve Security, Productivity and Management

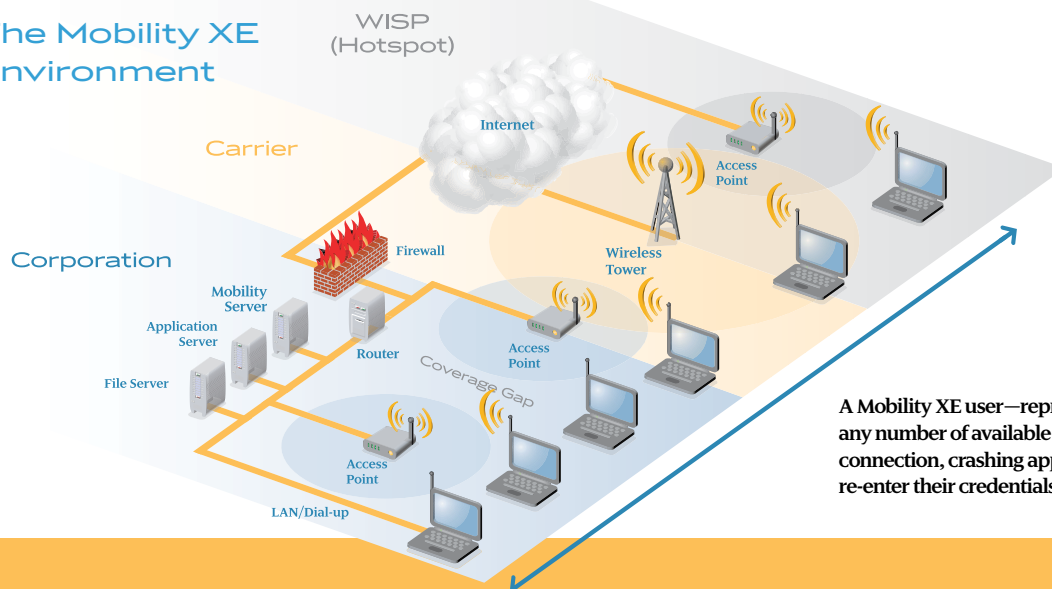> "From our vantage point, NetMotion Wireless is the clear leader in the space at this point in time."
> **- Tony Rizzo, Director, Mobile Research with The 451 Group**

The best-in-class Mobile VPN is **Mobility XE**—NetMotion Wireless' flagship solution built from the ground up for mobile and wireless environments. Unlike legacy SSL and IPSec VPNs that do not perform well in wireless environments, Mobility XE is a Mobile VPN designed to deal with wireless security, coverage gaps, roaming, performance and handheld device support.

Easy to Deploy, Software-only Solution

Mobility XE is an easy-to-deploy client/server software solution that helps minimize costs and complexity. Remarkably easy to install, Mobility XE deploys in hours, not days, without custom software development or expensive application rewrites. Its use is transparent to end users—no configuration or training required. Mobility XE server software can be installed on a server behind the firewall or in the DMZ, and lightweight client software is installed on each device—any combination of laptops, tablets, pocket PCs and smartphones.

The Mobility XE Environment

WISP (Hotspot)

Carrier

Internet

Access Point

Wireless Tower

Corporation

Firewall

Mobility Server

Application Server

Router

Access Point

File Server

Coverage Gap

Access Point

LAN/Dial-up

A Mobility XE user—represented by a laptop icon—can traverse among any number of available IP-based networks without dropping the connection, crashing applications, losing data or requiring the user to re-enter their credentials.

Proven in the World's Most Challenging Mobile Environments

Mobility XE is used in some of the most mission-critical, highly regulated and technically challenging environments in a wide range of industries including telecom, utilities, healthcare, transportation, government, manufacturing and public safety. Over 1,200 customers have maximized the productivity, security and management of their worldwide mobile workforces with Mobility XE.

Field Force Automation

Atlanta Gas and Light
Continental Airlines
Cox Communications
Kansas City Power & Light
Philadelphia Gas Workss

Medical Records and Reporting

Lee Memorial Health System
Mayo Clinic
St. Joseph's Hospital
St. Luke's Episcopal Health System
Visiting Nurse Service of New York

Sales Force Automation

Beckman Coulter
Diamond Partners
Optident (United Kingdom)
Unilever
U.S. Foodservice, Inc.

Dispatch

Los Angeles County Sheriff
Miami-Dade Police Dept.
Orange County Sheriff
Orlando Police and Fire Dept.
Vancouver Police Dept..

Flexible Control over Productivity and Security with Mobility XE Policy Management and Mobile Network Access Control
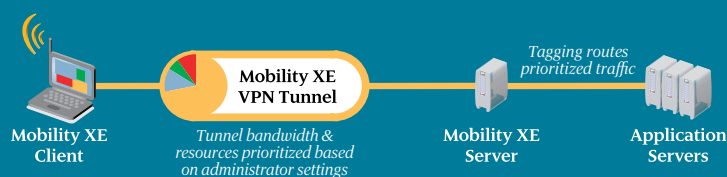
Policy Management Module

An optional **Policy Management Module** lets administrators create custom policies to manage access to network resources. Conditions and actions can be combined to help control WWAN costs, bandwidth usage and user experience according to your organization's security policies. Basic block, allow, disconnect or pass-through actions can be assigned to parameters such as network interface speed, network name, IP address, date and time, OS version and application name. Policies are centrally maintained in the Mobility XE™ server and automatically pushed out to mobile devices in the field. Policy enforcement is transparent to the user and can be modified for an individual, work group or entire organization.

Practical Policy Management scenarios include:
- Limit access to network resources based on the time of day or network in use
- Automatically synchronize data when a high-bandwidth connection becomes available
- Block bandwidth-intensive applications such as Web surfing or antivirus updates over low-bandwidth networks
- Prevent unauthorized applications from consuming network resources
- Automate hotspot authentication

Mobility XE Policy Management integrates best-in-class **Quality of Service (QoS)** using traffic classification and traffic shaping for even greater control over the speed and quality of mission critical transmissions. Administrators can allocate more or less of the available bandwidth to specific applications. Traffic shaping can significantly improve performance on low-bandwidth networks, like wireless WANs, and is especially important when latency and jitter sensitive, real-time applications such as VoIP and streaming video are being used. Without QoS, all VPN traffic is treated equally and the most sensitive applications are vulnerable to delay.

Mobility XE **Client**

Mobility XE VPN Tunnel

Tunnel bandwidth & resources prioritized based on administrator settings

Tagging routes prioritized traffic

Mobility XE Server

Application Servers

Mobility XE Policy Management integrates QoS based on traffic classification and traffic shaping to prioritize applications so the most critical ones take precedence for the fastest, smoothest transmission.

Packet loss recovery (PLR) improves the quality and performance of real-time application transmissions such as VoIP, video, web conferencing and instant messaging, by automatically replacing lost or missing packets without having to re-transmit them. As a result, Mobility XE can maintain much higher transmission quality than traditional IPSec or SSL VPNs, even on wireless networks.

Mobile Network Access Control Module

IT administrators who support highly mobile field forces need security solutions that protect their networks without impacting the productivity of the mobile professionals they serve. Mobility XE's **Mobile Network Access Control (NAC) Module** allows devices to connect to the enterprise network only after meeting specified security policies, but gives administrators greater control and flexibility over how and when to administer remediation policies.

Mobile NAC typically deploys in minutes without any need to reconfigure network infrastructure. A NAC wizard makes it easy to configure and enforce access security policies. Administrators can check compliance for required software including antivirus, antispyware, firewall, operating system version, Windows™ Update status, registry keys, and other applications. Unlike automatic security policies that force users to perform time-consuming, non-critical software updates before allowing access, Mobile NAC integrates with Policy Management, giving administrators flexibility and control over the response to a device that does not meet security guidelines. Based on severity and even the speed of their connection, administrators may choose from simple warnings, to triggering customizable remediation policies that can limit application access, launch websites, or even initiate software downloads, to disconnecting or quarantining the device. When rules are updated, they are automatically pushed down to client devices, and devices are automatically rescanned at regular intervals to ensure ongoing compliance.

> "With Policy Management, we can easily monitor and manage our mobile workers, including what applications and wireless networks they connect to. Policy Management is an invaluable tool for us."
>
> **– George Vinson, Director of IT with Strack, Inc.**

Mobility XE™ security and functionality are tightly integrated to provide secure, seamless operation as users traverse multiple networks, and the best possible performance over wireless networks. Mobility XE allows enterprise application servers to identify each client with the same, unchanging virtual IP address—even as clients transition to a new network and are assigned a new IP address. Typical IP addresses assigned by various networks make it almost impossible to identify a client as it moves in and out of network coverage areas.

> "We just loved the whole idea of NetMotion Mobility and the simplicity of implementation ... it was logically the best choice."
> **- Neriah Roberts, Network Engineer with Continental Airlines**

Maximize Productivity with Single Sign-On Authentication

Unlike other VPNs that require a separate login step and force users to re-login every time they lose connectivity, Mobility XE can provide single sign-on authentication with standard Windows® login credentials. This feature saves mobile workers valuable time as they traverse networks and coverage areas, and provides a transparent user experience with no additional steps to learn or passwords to remember. Single sign-on authentication combined with VPN enforcement also helps prevent users from circumventing the VPN security.

Protect Networks and Data with Standards-based Security

Mobility XE is certified with RSA SecurID two-factor authentication and supports NTML and RADIUS authentication protocols to protect networks from unauthorized access. Mobility XE secures network access and all data transmissions

> "Integrating standards-based security that includes RSA SecurID two-factor authentication and AES encryption into Mobility XE gives us greater confidence that our network and data will remain secure."
> **– John Marshall, Senior Vice President - Delivery with Kansas City Power & Light**

through the VPN tunnel—to and from mobile devices in the field. Using **FIPS 140-2 validated AES encryption**, the industry's highest security standard, Mobility XE provides the security advantages of an IPSec VPN without its configuration, client provisioning and management burdens. And because mobile device loss or theft can compromise information on the device and the network, Mobility XE allows network administrators to quickly and easily quarantine lost or stolen devices. And administrators can easily restore network access when the device is recovered.

Ensure Critical Applications are Always Available

No other VPN can match Mobility XE's **Application Session Persistence**—its ability to sustain application sessions even through suspend-and-resume cycles and loss of connectivity. Other VPNs in these situations lose application sessions— causing data loss and corruption, and forcing users to re-login and restart applications. If a user loses connectivity while an application is transmitting data, Mobility XE suspends the transmission—for days if necessary. As soon as connectivity is re-established, Mobility XE resumes transmitting the data at the exact point the application was interrupted.

> "We needed to establish an architecture which met the full variety of demands across our global business operations. NetMotion Mobility XE is the only product which met all our requirements for the project including secure and persistent application connectivity for a variety of PDA devices."
> **- Richard Oxenham, Mobile Solutions Specialist with Unilever**

Roam Seamlessly Across Networks

Mobility XE does not require re-authentication when a user roams to a new network. This **InterNetwork Roaming™** capability allows users to securely and reliably traverse any combination of wired and wireless IP-based networks. There is no need to re-segment networks, implement VLANs or deploy additional hardware to enable mobile workers to roam freely. This feature works in conjunction with Mobility XE's single sign-on and network session persistence so that users do not have to repeat the login process when they roam, suspend and resume, or go in and out of network range[1].

[1] Within wireless service coverage area only. Availability and coverage depends upon carrier and/or network capabilities.

roductivity and Management

Run Existing Applications Without Modification

With Mobility XE™, any application—even home grown ones—that works in your current wired environment will run over wireless without modification, expensive development or upgrades. Since most applications were written for use over a single, high-speed, wired connection, many

> "...Server and client deployment were a breeze, and the management interface was the best we tested."
> – **Network Computing**

legacy VPNs require additional configuration for applications to work properly in wireless environments. And without modification, applications often crash, resulting in lost data, repeat logins and huge drains on worker productivity. Even the leading SSL VPN solutions continue to suffer from application compatibility issues.

Optimize Performance Over Wireless Networks

Mobility XE's **Wireless WAN Optimizations** automatically reduce network consumption and improves throughput and application responsiveness, particularly over bandwidth-constrained or wireless networks. Other VPNs typically degrade performance, especially over wireless networks, often by as much as 50%. Mobility XE uses link optimizations to reduce the number of retransmitted packets, excess control information and other network "chatter," and dramatically improves throughput by compressing data and images. **Best-Bandwidth Routing™** technology ensures the fastest, most efficient, available network connection is used. For example, Mobility XE automatically roams to a WLAN connection the moment it becomes available—resulting in greater productivity, improved efficiency and reduced WAN expenses.

Support a Broad Range of Mobile Devices

Mobility XE delivers the same robust features and security across device types—for the same protection and seamless work experience on laptops, handhelds and smartphones. Other VPNs provide only a subset of features as you move between platforms and devices. Mobility XE offers support for all current Microsoft® desktop and handheld client platforms, **including Windows Mobile® devices.**

Manage Thousands of Connections from a Central Console

No other VPN provides the spectrum of flexibility, visibility and control afforded by the **Mobility XE Management Console**. The centralized, web-based interface gives administrators a complete system-wide view, from overall metrics down to device connections, worker behavior and application use. Detailed activity logs preserve a historical view of user activity. From the management console, administrators can quarantine devices that are misused, lost or stolen.

The "Client Status" tab shows device connectivity status, number of quarantined devices and even battery life. From this screen, administrators can search for information on a specific user or device, such as open applications, device operating system and interface or port in use.

Scale Easily to Meet the Needs of Your Growing Mobile Workforce

Mobility XE is ideal for organizations of all sizes. Deployments scale quickly and easily to adapt to growing mobile workforces. Each Mobility XE server supports up to 1,500 concurrent sessions. Multiple Mobility XE servers

> "Enterprises need a solution that not only meets their needs now, but will evolve with them. Mobility XE from NetMotion Wireless does just that."
> – **Enderle Group**

can be "pooled" to support up to 15,000 concurrent sessions or 35,000 registered devices, and to provide load-balancing, failover and redundancy. Even the largest Mobility XE deployments are easily managed through a single, centralized management console.

About
NetMotion Wireless

NetMotion Wireless is a software company that enables organizations to maximize the productivity of their mobile workforces. The company's flagship solution, Mobility XE, allows mobile workers to maintain and optimize mobile data connections as they move in and out of wireless coverage areas and roam between networks. Mobility XE mobile VPN software resolves today's key mobile deployment challenges including coverage gaps and interruptions; inter-network roaming; performance issues and network security. Over 1,200 organizations worldwide rely on NetMotion everyday. NetMotion has been named one of the country's 50 fastest growing wireless companies and has earned over 25 industry awards for its outstanding technology.

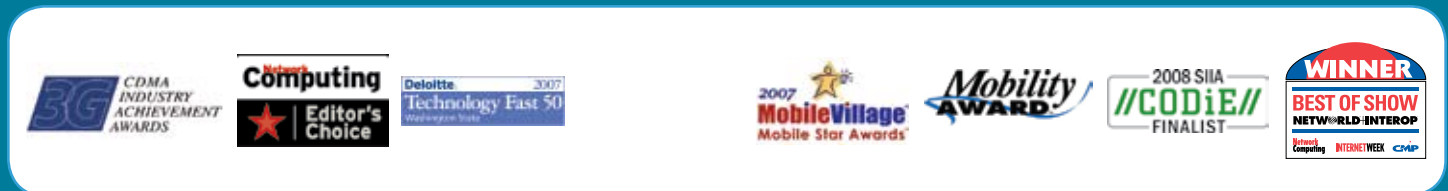## For more information about NetMotion Mobility XE contact:

NetMotion Wireless
NORTH AMERICA
701 N 34th Street, Suite 250
Seattle, WA 98103
United States
TEL 206.691.5555
FAX 206.691.5501
www.netmotionwireless.com

NetMotion Wireless
INTERNATIONAL
4 Mandelbrote Drive
Oxford, OX4 4XG
United Kingdom
TEL +44 (0) 1865 714814
FAX +44 (0) 2076 919487

DuraTech USA Inc.

6765 Westminster Ave   #314   Westminster, CA 92683
Email: sales@DuraTechUSA.com
www.DuraTechUSA.com
Phone: (714) 898-2171
Fax: 866-704-9132
Toll Free: 866-761-9555

Certifications and Awards

RSA SECURED®

FIPS VALIDATED 140-2
FIPS 140-2 Inside*

Designed for
Windows Mobile®

palm
Designed for
Palm Products
Treo® 750 smartphone
Mobility XE™
v.7.1

3G CDMA INDUSTRY ACHIEVEMENT AWARDS

Network **Computing** Editor's Choice

Deloitte 2007 Technology Fast 50 Washington State

2007 MobileVillage Mobile Star Awards®

Mobility AWARD

2008 SIIA //CODiE// FINALIST

WINNER BEST OF SHOW NETWORLD·INTEROP
Network Computing   INTERNETWEEK   CMP