Efficiency Through Mobilizing Public Service
A Primer for Government Agencies

Executive Summary

Government agencies such as law enforcement and first responders have always been early users of mobile computing technologies. The reason is simple; their duties require access to real-time information in order to complete their work safely.

As mobile computing has evolved and equipment and service costs reduced, more government agencies are realizing the productivity increases garnered by equipping workers with laptops, tablet PCs and smart handheld devices. A wide array of government organizations from child and family services to public works, field inspectors and utilities are deploying mobile computing technologies to improve public service, increase worker productivity and better harness budgetary resources more efficiently.

This paper outlines examples of mobile technologies within different government agencies and details the key components that organisations such as these considered to uncover and remove unseen hidden costs as they mobilized their workforce: Bedfordshire Police, Birmingham City Council, Bournemouth Borough Council, Cherwell District Council, Dorset County Council, Durham City Council, Derby Homes, Dwr Cymru Welsh Water, Harrow Borough Council, Leeds City Council, Airwave Solutions, London Fire Brigade, Newcastle on Tyne City Council, Newport City Council, North Wales Police, Oxfordshire County Council, Partnerships UK, Partnerships for Schools, West Oxfordshire District Council, Westminster City Council and Wolverhampton Borough Council, South East Water, South West Water and Strathclyde Partnership for Transport (SPT).

Mobile Computing for Government

Emergency Services and Law Enforcement

In many cases Police and Fire Services have been the innovators in mobile computing. Typically the first application for these deployments is computer-aided task or job management and computer-aided dispatch (CAD) which delivers complete information about a call including address information that speeds response time and enhances employee safety. Newer systems are more sophisticated and transmit more data, including maps and turn-by-turn directions. Staff also use computer applications and data networks to access criminal justice information, update incident reports, view images of missing children, or fingerprints and photos of suspects, run drivers' license and other DVLA checks, check e-mail and access departmental intranets, and stream video traffic from dashboard-mounted cameras.

Fire response pre-plans can include building maps, information on suppression systems, hydrant locations and exactly where gas and power shutoffs may be accessed. Pre-plans also detail hazardous materials on-site. Responders can then use mobile data access to confirm information about the risks presented by burning materials so they can protect themselves and the public.

Some of the newer systems link with GPS systems in each vehicle so dispatchers know exactly where each unit is throughout the operational area. This is extremely useful in rural counties, or in congested urban areas where transit time could be an issue. Often, a unit already deployed in the field could be closer to an incident than one in the nearest station. Departments have also found that mobile data access eliminates double entry during fire inspections, as notes of violations and changes that impact the pre-plans can be transmitted directly to the system and updated with a single entry, gaining efficiency.

Wireless data access can save staff time – and their lives with real-time alerts of dangerous situations.

Emergency Medical Services

Vital medical information about patients gathered on the scene and during transport to the hospital has typically been gathered on paper forms, and entered later into EMS department systems by hand. This time-consuming double entry by clinicians and paramedics doesn't just drain productivity - it can delay treatment at the hospital as hospital workers review patient records upon arrival. As a growing number of EMS departments have found, entering the clinical data directly into a laptop, tablet or handheld computer and transmitting it directly to the receiving hospital via wireless networks is a boon to patient care. It sends complete medical information while the patient is en route, so the medical centre is fully aware of the patient's condition, can prep the treatment room beforehand and shorten the time-to-treatment, thereby improving efficiency.

Public Works

Public works involves all kinds of tasks, from patching roads to clearing sewers to repairing park benches and maintaining parks and gardens. These are generally outdoor jobs, in far-flung locations, requiring different kinds of tools and equipment. Most public work organizations have frequently operated with a pen and paper approach, or a job batch store-and-forward approach synchronised once a day. Job assignments were determined at the beginning of each day with reports updated from office or home following task completion. Efficiencies through real-time coordinating and scheduling crews and equipment through the day, responding to changing priorities and directing them to various locations to maximise productive use of the working day is gained by deploying a mobile data solution. Crews can access maps, plans and schedules, and update work orders and inspection data while still at the job sites. Reports are filed faster, project status and work completed can be reviewed on-the-fly by supervisors and personnel and equipment resources deployed more effectively for increased efficiency.

Health, Safety and Environmental Inspection Departments

Health, safety and environmental department workers constitute a broad group of government employees that perform a variety of inspections and compliance monitoring for occupational safety and health regulations. On any given day inspectors may visit restaurant kitchens, food warehousing facilities or various job sites to ensure proper health and safety regulations are followed and complied with. Over the course of the day, they will complete multiple paper form reports, complete updates to existing reports and either fax or drop off completed paperwork for processing. Deploying mobile devices and real-time data access via connection to cellular data networks has dramatically impacted inspector productivity. Reports and data record updates occur on the spot with violations and remediation plans filed before the inspector leaves the premises. Electronic data entry has also eliminated the need for paper forms and repetitive data entry, thereby improving efficiency dramatically.

Social Care, Child and Adult Services

Child and Adult Services agencies are dedicated to improving the integration of services for children, youth, families and vulnerable populations— promoting their development and protecting them from violence, neglect, abuse and abandonment. The agencies typically provide a system of family support, juvenile justice, child care and child welfare services that promote the safety and well-being of children and adults. Case workers and counsellors are responsible for day-to-day visits and calls to report on adults and children in foster care, adoption, child protective services, and protective programs. With a rising number of cases that counsellors need to address on a daily basis, many agencies are embracing technology as a way to handle their increased work load. Case workers and counsellors are now equipped with mobile devices in replace to the pen and paper notes they used to keep. Doing so has reduced the administrative burden and put more information literally at their fingertips. It's also enabled workers to spend more time in the field making more visits per day, improving care and increasing their agency's overall efficiency.

Municipal Field Services

Field service efficiency is a top priority for local government. Using mobile technologies is one of the most proven ways to increase utility worker productivity and efficiency, as demonstrated by companies like South East Water, Welsh Water Dwr Cymru and South West Water. Deploying mobile devices to field workers allows customer information and job site info to be reviewed remotely in real time, speeding the time for delivery of service. Whether they are using GIS to plan a repair, scheduling or checking on a repair, or responding to a customer service request, real time mobile technologies enable local government increase field service efficiency and customer satisfaction.

The Elements of a Mobile Deployment

The terms mobile and remote are often used interchangeably. Both terms describe data access for field workers who are not in a fixed office, tethered to a wired LAN. Most field workers need constant connectivity to applications throughout the working day. Whether they are working from their vehicle, a client's home or on a remote job site; access to data allows them to stay productive regardless of location.

It is useful to think of a mobile deployment as having three elements:

Mobile Devices
Mobile devices are typically notebook or tablet computers, although other handheld devices may feature into the deployment based on job requirements. Hardware manufacturers offer ruggedized devices designed for field use. Field-tested rugged devices are typically more costly, but these units pay for themselves in lower failure rates, incidence of damage and overall support costs. Manufacturers cite instances where units continue to function despite being dropped, exposed to water, or excessive heat.

Wireless Networks
A handful of government agencies – mostly in emergency services – have deployed their own private radio networks for data access, but most organizations today rely on data networks maintained by cellular carriers. It is important to realize that reliable coverage can be an issue especially in areas with natural and man-made barriers to coverage. Carrier coverage maps based on cell towers do not account for local conditions that can block or impede transmission (e.g. hilly terrain, tunnels, buildings, etc.).
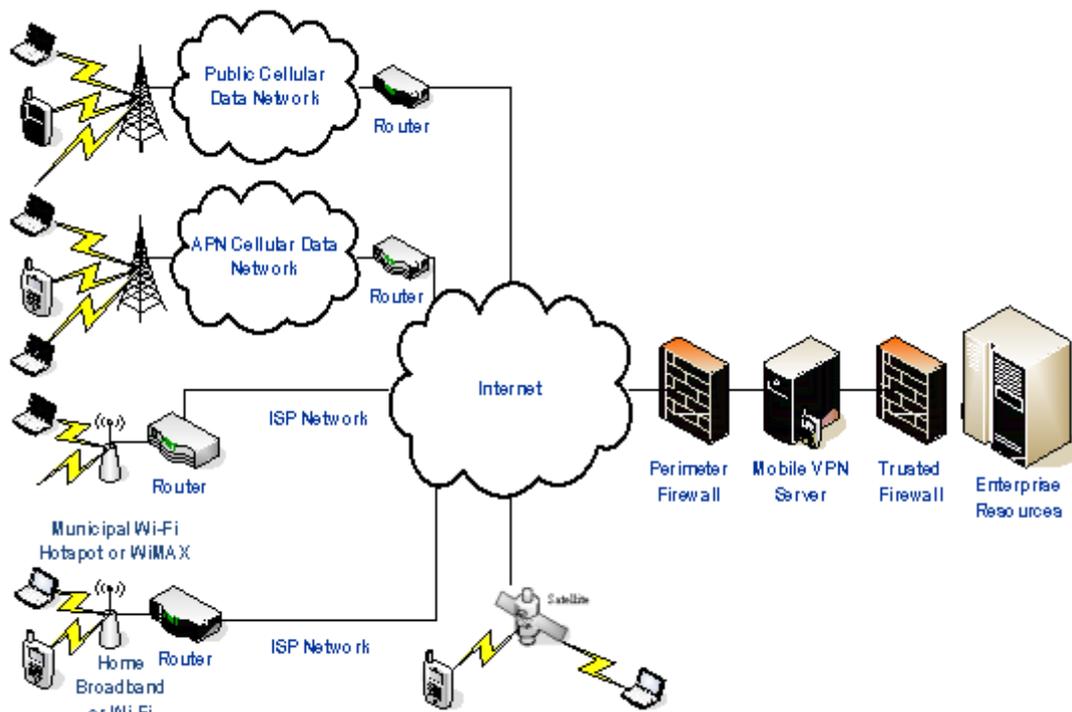
Mobile devices communicate via multiple cellular data networks or Wi-Fi hotspots in the field, to connect to departmental resources via the public Internet. A mobile VPN secures the connection end-to-end and maintains reliable connections as each device moves between the various networks.

Many organisations supplement the cellular networks by deploying their own Wi-Fi networks, with access points at strategic locations. Typical hot spot locations are car parking areas and garages, maintenance depots, libraries, fire stations, police buildings, health department stations, and other neighbourhood offices maintained by various public agencies. In some places, Shared Services agreements have enabled the deployment of locked-down hot spots in strategic locations, such as in public open spaces in metropolitan areas. This gives workers a cost effective reliable, high speed

connection, at a location where they can park vehicles to upload reports and download information. Wi-Fi connections are especially useful for data-intensive tasks that can bog down available bandwidth on a cellular network, such as updating maps and images, as well as downloading patches, software updates and antivirus signatures.

Software

For standardisation, nearly all mobile devices that are used for complex tasks and applications run versions of the Microsoft® Windows® operating system to support the most common applications. Key applications that are primarily used across government agencies include:

- CAD (Computer-Aided Dispatch) applications, which are the workhorses of public safety deployments including police, fire and paramedic services. CAD applications for law enforcement have historically been the initial focus of a governmental mobile rollout.

- RMS (Records Management Systems) for filing incident reports.

- Mapping and GIS software for route finding, task planning and vehicle / device tracking.

- General-purpose Internet applications including e-mail clients and Web browsers. These access departmental e-mail, intranets and the many applications that use a browser-based front end. Access to the broader Internet may be needed for some job functions, or available for private use as allowed by the departmental security policies.

- Client-Server database applications (so-called "fat-client" applications) that offer access to public sector databases containing confidential information; pre-filed response plans for fire departments; health records and other information.

- Scheduling, job tracking, time-tracking and other applications as necessary for the organisational mission.

Mobile devices are tools that workers use in the everyday course of doing their jobs. Like any other tool, workers simply expect them to work. They cannot be bothered to update software, tweak network settings, or deal with the minutiae of configuring devices. If a system is difficult to use, simply put, they just won't use it.

However, there is also a class of users who know too much, but not enough and need protecting from themselves. They might attempt to "adjust" or "improve" their devices and break critical settings in the process.

Remote management gives the IT department centralized control and visibility over the installed applications, application versions, configuration, security and status of every mobile device. The larger the deployment, the more essential a remote management system becomes.

A VPN handles the vulnerability issues of sensitive or privileged data sent over the public airwaves or the Internet. A mobile VPN is a special class of VPN, distinct from traditional VPNs. The most essential characteristic of a mobile VPN is that it maintains a secure tunnel through conditions that would break a conventional VPN, such as going out of coverage range or crossing from one wireless network to another.

A mobile VPN is a necessity in a remote deployment, where workers need applications and connections to be always on, always available. It can also be a logical evolutionary tool as a mobile workers' needs change from deploying one or two field applications to enabling full desktop-like functionality. Whereas a traditional VPN technology like SSL or IPSec cannot manage the vagaries of wireless network connectivity, a mobile VPN is specifically designed for these challenges.

Many organizations have attempted mobile deployments using conventional VPNs or relied on the encryption technologies built into wireless networks, and discovered the need for a mobile VPN after the fact. Once they implemented a mobile VPN, their networking and device problems disappeared and support incidence reduced while worker uptime increased.

The Unseen Challenge: Seamless Connectivity

NetMotion Mobility XE is a mobile VPN that solves the single, most vexing problem impacting mobile deployments: maintaining application and user log-in sessions. Continuous connectivity is not always present in a wireless environment. When users lose their connections, sessions drop, applications often crash, and users have to re-login to authenticate to the network.

All too often, these problems don't become evident until after an organization has deployed a system, or added applications that they would like to roll out to the field. Especially unfortunate, agencies often live with the problems, accepting increased costs from hidden inefficiencies through decreased functionality and productivity because they are unaware that implementing a mobile VPN can solve the problems, quickly and efficiently.

Common connectivity issues experienced by the sample customers mentioned above include:

Coverage Gaps

Nearly all cellular networks have local "dead zones". When workers go out of range, they lose their connections. When they have to re-login or re-enter the data they lost, at the very least it impacts productivity. In some situations an inability to connect or a lost connection can be life-threatening.

NetMotion Mobility XE is able to maintain a virtual connection to the application, even though the actual connection may be lost. It also preserves the state of the application, even in the middle of a data transmission, by holding the unsent or pending data in queue. The session simply resumes when the connection is available again.

Use of Multiple Networks

As noted previously, the majority of agencies need multiple networks to cover the entire jurisdiction. When crossing a network boundary, responders need to log in to each new network to authenticate. They may cross these boundaries dozens or hundreds of times a day. Even applications written specifically for mobile environments (many CAD applications, for instance) cannot handle crossing of network boundaries, and require users to re-authenticate.

NetMotion Mobility XE handles multiple networks by maintaining a virtual IP address for each device. As the device encounters a new network, it authenticates to the new network, transparently to the user, and receives a local IP address from the network's DHCP server. The mobile VPN maps the virtual IP address to the local IP address so that even as the local IP address changes, the deployment operates as if it were a single network.

Suspend/Resume Cycles

For devices running on battery power, suspending a device puts it in a lower-power state. For health or social services workers doing home visits, this may be required so the device makes it through the working day on a single charge. Typically, suspending cuts power to the wireless system, breaking the connection. NetMotion Mobility XE preserves the virtual connection through a suspend-and-resume event.

Application Reliability

Virtually all applications assume a permanent network connection. If the connection disappears in the middle of a network operation, the application typically can't re-establish access and crashes. Since many applications perform network operations in the background, at undefined intervals, the user doesn't even have to be actively using the application. And yet, an application failure can occur requiring re-logging in and retyping any lost data.

Special-purpose applications developed specifically for mobile deployments, such as CAD applications, are generally written with mobile environments in mind. Their store-and-forward capabilities allow them to survive through broken connections. Although store-and-forward applications present a workaround means of solving reliability issues, more agencies are opting for solutions that offer real-time access efficiencies, making a mobile VPN a better option.

In addition, general purpose applications such as Web browsers and e-mail clients, office productivity, scheduling and resource-management systems, public-health applications, general-purpose databases, mapping software, video camera software and others that are increasingly used in public agencies are prone to crash in a mobile environment, such as being used on a train. These application crashes are most often the greatest source of worker frustration in a typical mobile deployment. And solving them considered one of the most important, most welcome attributes of NetMotion Mobility XE.

Support Concerns and User Acceptance

Agencies that have deployed a mobile solution without using a mobile VPN know that sporadic coverage and crashes result in chronic reliability problems frustrate users and trigger lots of help desk calls.

Public workers are serious about their mission. Technology that makes it easier will be accepted. Technology that gets in their way won't.

NetMotion Mobility XE does its work in the background, handling logins and the complexities of roaming between networks while maintaining applications through coverage gaps. To users, it appears they are constantly connected to a single, seamless network.

Managing a Mobile Deployment

Mobile devices may be used hundreds of miles away from the data centre, on unseen networks, far out of reach of the IT department. Workers may bring their device onsite only at the beginning or end of a shift, and in some cases, not at all. This leads to management challenges far beyond those encountered with fixed machines on a wired network.

Visibility

The total value of a mobile deployment represents a major investment of taxpayer dollars and with it comes a responsibility to ensure resources are used wisely. While NetMotion Mobility XE is a fraction of the total deployment cost, it allows use of the entire system to be centrally configured, managed, and observed, NetMotion Mobility XE with its analytics capability goes a step further, furnishing reports that reveal patterns of use, how devices and networks are being employed, and how they might be used more wisely.

Control

Managing even a handful of remote devices can be a chore. In a large deployment with hundreds or thousands of devices it can be impossible without an automated solution. NetMotion Mobility XE with its central console makes it easy to quarantine devices that are misused, lost or stolen. Policy management capability allows administrators to dictate how devices and applications use the networks, to maximize productivity. And policies may be assigned to individual users or groups of users, affording flexible, streamlined control with permissions based on job function or organizational role.

These policies are stored on the central NetMotion Mobility XE VPN server, rather than on the mobile device, and pushed down automatically to the device where they are enforced. A well-defined set of policies locks down a device tightly, unseen to the end user, which prevents users from tinkering with settings that might override essential security or impair the functionality of the device.

Mobile Device Connection Management

A large mobile deployment may include hundreds or thousands of individual mobile devices. Tasks such as operating system upgrades, software rollouts, driver changes, updates and configuration changes which are simple in a small LAN environment are incredibly complex in a mobile deployment where devices are constantly on the move. The problems compound when a mobile deployment serves multiple government agencies, as the application profile for a first responder's device is radically different from that used by a health department worker. Mobile Device Connection Management includes:

- Staging of new devices or those returned from the service centre
- Standardizing software versions and configurations within and across various types of users
- Pushing out application updates, device refreshes, and security and network settings with minimal impact or interruption to the user

While system management in LAN environments is a mature industry, mobile environments pose additional challenges surrounding roaming, intermittent connectivity and variable bandwidth. A management system especially designed for a mobile environment, tightly coupled with NetMotion Mobility XE's mobile VPN that is "connection and bandwidth-aware," presents an ideal solution for large government deployments.

Monitoring
With workers far removed from IT resources, any problem with a device or network takes much longer to correct, possibly resulting in a dramatic loss of productive hours. NetMotion Mobility XE with its proactive monitoring capabilities not only detects active problems, but raises alerts when problems might be imminent. This includes problems with networks, connections or with a device itself such as a battery that might be failing.

Fault Isolation and Resolution
In a mobile deployment, access points may exist at remote locations or workers may use wireless "hotspots" in public locations, rendering entire pieces of the delivery network outside of IT control. Knowing when a problem might exist at a Wi-Fi access point, within a cellular network, or with the device itself can be problematic. NetMotion Mobility XE with its reporting and analytics capability can quickly evaluate connectivity problems across networks and isolate an individual device, network, user or time of day, detecting root causes that otherwise might take hours of technical sleuthing at the device level.

Bandwidth Management
Data access contracts with cellular carriers represent a sizable investment of public funds that must be used wisely. NetMotion Mobility XE uses application-proxy technology is able to examine the complete traffic flow and how users, devices and applications use bandwidth across each cellular network. Developing reports on these areas allows administrators to understand when:

- Total bandwidth use is approaching the contract limit and agreements need to be renegotiated
- Data-intensive applications (such as streaming media) might be wasting a public resource
- Non-essential applications are being used in the field
- Large file transfers over a cellular network could be more cost-effectively run on Wi-Fi or LAN.

Worker Productivity
NetMotion Mobility XE's application-proxy mobile VPN can also proactively ensure that individual users and devices use applications and networks properly. Policy management capabilities afford extremely effective control over user and device behaviour, with granular control by application, port and IP address over various networks. This ensures proper use of mobile devices which are not personal devices, but a public resource prevent inadvertent problems like workers who are using their devices as intended accidentally launching a process, such as initiating an anti-virus signature download or running Windows updates over a cellular data connection which can bog down their device for many minutes.

Authentication and Code of Connection (CoCo) compliance
Ensuring that users are authorized is a key concern for any network manager, but this situation is of greater concern in a mobile deployment where devices are prone to be misplaced, lost or stolen. Government agencies face increasingly stringent requirements for strong two-factor authentication, which is required to access Government Systems that need Code of Connection (CoCo) compliance

A mobile VPN ensures users are authorized by enforcing secure logins using either its own native active directory, or integration with an enterprise directory. Proactive notification capabilities alert administrators when a device has exceeded the number of allowed login attempts, indicating it may have been stolen, with centralised controls that quarantine the device so it cannot be used to access sensitive applications and data. Allowances for smart cards, RSA SecurID, digital certificates, biometric scanners and other two-factor authentication methods add the strong authentication required by GSi CoCo.

End-to-End Security
Wireless networks use the public airwaves which clearly poses security risks. And while Wi-Fi and cellular networks offer their own security technologies, some have known vulnerabilities. In addition, the

portion of the route that runs over the wired Internet remains unencrypted. A mobile VPN creates a secure end-to-end tunnel that encrypts the entire data path from the data centre to the wireless device.

In addition, NetMotion Mobility XE offers Network-Access Control (NAC) capabilities that help protect both the individual device and the corporate network against viruses and spyware. It accomplishes this by verifying that security measures are active, enabled and up-to-date, and that the device has all necessary security patches as specified by the corporate security policy. It can even remediate the device automatically, without requiring any user intervention. This protects the device and guards against lost productivity, since some malware can severely degrade device performance or burden the network with malicious traffic.

Mobile Deployment Challenges?
NetMotion Mobility XE

	Challenge	Solution
Security		
Data security	Safety of data from compromise as it traverses airwaves and the public Internet	Highest-standard FIPS 140-2 validated 128-bit to 256-bit AES encryption secures data sessions as devices traverse networks
Device health	Protection of individual devices against viruses, spyware and other malware that can expose data	Network Access Control (NAC) verifies that a device is compliant with organizational security standards before allowing a connection
Device loss or theft	Devices that are constantly in motion, and prone to being misplaced, forgotten or left unguarded	Central controls make it easy to quarantine devices that are misused, lost or stolen
Compliance	Complying with specific security standards, as required by government mandates	Support for strong authentication meets GSi Code of Connection compliance requirements
Productivity		
Intermittent connectivity	Application crashes and/or repeat logins as workers cross network boundaries, go out of range, or suspend-and-resume devices	Mobile-aware VPN handles complexities of dealing with coverage gaps and roaming between networks, so public sector workers can focus on serving the public.
Variable bandwidth	Data-intensive processes running over slower networks, bogging down device performance	Policies control device and application behaviour, and keep data-intensive processes off slower speed networks.
Multiple networks	Isolating users from complexities of managing devices on multiple networks	Devices automatically use the fastest available connection and roam seamlessly between departmental Wi-Fi hotspots and multiple cellular data networks.
Web performance	Slow performance and page refreshes when using Web applications over cellular networks	Compression and protocol optimization techniques improve throughput and application responsiveness
Management		
Bandwidth usage control	Ensuring intelligent use of a public resource, especially contracted cellular networks	Analytics capability reports on all aspects of user, device and application use - over all network types
Control and visibility	Effective, efficient management of hundreds or thousands of devices deployed in the field	Browser-based administrative console allows all aspects of the system to be centrally configured, managed and observed
User issues	Technically unsophisticated users	User-proof design is transparent, extends centralized control over configuration and minimizes trouble tickets
Troubleshooting	Fault isolation for mobile devices using multiple networks	Reports with drill-down capability uncover problems related to various data networks, time of day or other patterns of use
Monitoring	Need to continuously monitor or "babysit" the deployment	Automated notifications promote hands-off management, and pre-emptive detection of conditions of imminent failure

Efficiency Through Proven Reliability to Go: NetMotion Mobility XE Mobile VPN

NetMotion Mobility XE is an award-winning mobile VPN specifically designed to present an elegant, single solution to all of the challenges of mobile deployments. NetMotion Mobility XE:

- Keeps application sessions alive to prevent crashes as users encounter no-coverage zones, suspend and resume their devices or cross network boundaries
- Allows applications that were not written specifically with mobile deployments in mind to be used successfully in a mobile environment
- Automatically handles logins on behalf of the user, as well as the technical complexities of configuring for each connection as devices switch between networks
- Authenticates each user, through Mobility XE's own user database or integration with Windows Active Directory
- Supports strong "two-factor" authentication, and encrypts all the data transmitted
- Ensures that devices have patches that are up-to-date, as well as properly configured, active and updated antivirus and antispyware protection
- Enforces proper bandwidth use by making sure that large data transfers stay off of slower networks, and that mobile computing resources are used appropriately
- Delivers intelligence on the usage and behaviour of individuals, devices, applications and networks, to drive higher productivity, monitor use of public resources and fine-tune the deployment
- Does all of the above in way that is essentially invisible to the user, improves productivity, and is highly resistant to user missteps that might impair the functionality of the device

Mobility XE Delivers GSi Code of Connection Compliant Security for UK Local Authorities

A growing number of UK public sector bodies have selected and deployed NetMotion Mobility XE to ensure the security of their mobile computing deployments is GSi Code of Connection (CoCo) compliant.

When fully deployed, NetMotion Mobility XE delivers the following specified mandatory requirements to achieve CoCo 4.2 compliance for mobile working:

- NetMotion Mobility encrypts data while in transit using a method and encryption libraries which are FIPS140-2 certified.
- Policy Management and Network Access Control capabilities permit the portable electronic devices to be authorised, managed, configured and operated in accordance with CESG Guidance.
- Mobility's support for X.509v3 PKI user certificates and device registration methods ensures that remote connections are only permitted from authorised, official and managed devices.
- Mobility's extensive logging and reporting capabilities through our Analytics Module enables Network Managers and Security Officers to maintain detailed records of the connection and usage activity of every remote and mobile connection.
- The Mobility client installed on each device is a Transport Layer Proxy Firewall, which can be centrally configured to block or allow access to specific data streams, applications, ports, protocols etc.
- NetMotion Mobility supports strong two-factor authentication for all remote and mobile devices including Windows Mobile.

Tried and Trusted

Mobility XE installs in a couple of hours and instantly gets to work protecting the security and enhancing the end user experience for your mobile workers. It is already proving its effectiveness for around 2,000 other organisations and 500,000 end users worldwide, benefitting from the product every working day.

A selection of UK public service customers include Birmingham, Leeds, Newcastle, Newport and Westminster City Councils; Bournemouth, Harrow and Wolverhampton Borough Councils, Cherwell and West Oxfordshire District Councils, as well as Public Safety and Emergency Services such as Bedfordshire and North Wales Police forces, Airwave Solutions, and London Fire Brigade, Dwr Cymru Welsh Water, Partnerships for Schools, Partnerships UK, South East Water, South West Water and Strathclyde Partnership for Transport (SPT),.

Proven Return on Investment

Unusually for a security product NetMotion Mobility has a demonstrated and documented (by customers) return on investment period which can be measured in weeks, not months. Our product even includes the tools you need to make and report these measurements to management to demonstrate that ROI promises are being met.

Prove it for yourself at no cost
Try Before You Buy

NetMotion Mobility XE software is available on a no-cost, no-obligation 30-day evaluation license so you can gain first-hand experience of how the security and performance of your applications will be improved for working over the various Wi-Fi and cellular networks your organization uses. This also enables you to make a purchasing decision only once you have proven our product is effective in your organization's working environment. A software-only product, it installs in an hour or two on an existing Windows Server in your organisation.

For More Information or for a no cost eval

To learn more, please contact us at info@netmotionwireless.co.uk for case studies detailing various uses of the NetMotion Mobility XE mobile VPN in government, and white papers that explain how your organisation could harness NetMotion Mobility XE to improve mobile working efficiencies, including topics such as security, policy management, network access control and analytics alerts and reporting.

To request a no-cost, no-obligation, 30-day evaluation license of NetMotion Mobility XE for your project contact sales@netmotionwireless.co.uk or call on 0208 144 2332.