

Security

Granular control for meeting exacting security requirements

Using NetMotion's mobile performance management, IT administrators can create a highly flexible and programmable secure mobile strategy. A secure tunnel protects the data sent between a device and enterprise resources, protecting applications running over public networks regardless of location. The secure tunnel exercises strong authentication and encryption to ensure that data communications are protected on insecure public networks. Administrators can configure options from the per-app level to device-wide, ensuring customizable and secure access to enterprise data. Most important, IT can tightly restrict access without making security burdensome for mobile workers.



Granular security and flexibility

When workers use public networks, requirements for security enforcement are very different compared to a corporate-controlled environment. Highly granular security controls enforced through policies allow IT to secure connections for specific applications or data flows, or for all applications and connections on the device. Security enforcement can also be controlled by physical location using geo-fencing capabilities.



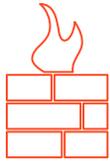
Advanced security for highly sensitive and regulated industries

Whether driven by regulatory requirements or the nature of the applications and data accessed by the mobile user, some industries require advanced security. Examples include multi-factor authentication beyond simple user/password logins, or stringent standards for encryption strength. NetMotion software has supported these requirements for years, for the most security-conscious industries and organizations.



Safeguarding corporate resources against unsecured devices

Unsecured devices allowed to access corporate resources are a threat. Security through mobile performance management is able to verify that certain security procedures such as an active firewall and updated antivirus are in place before allowing a device to access corporate networks, servers and data.



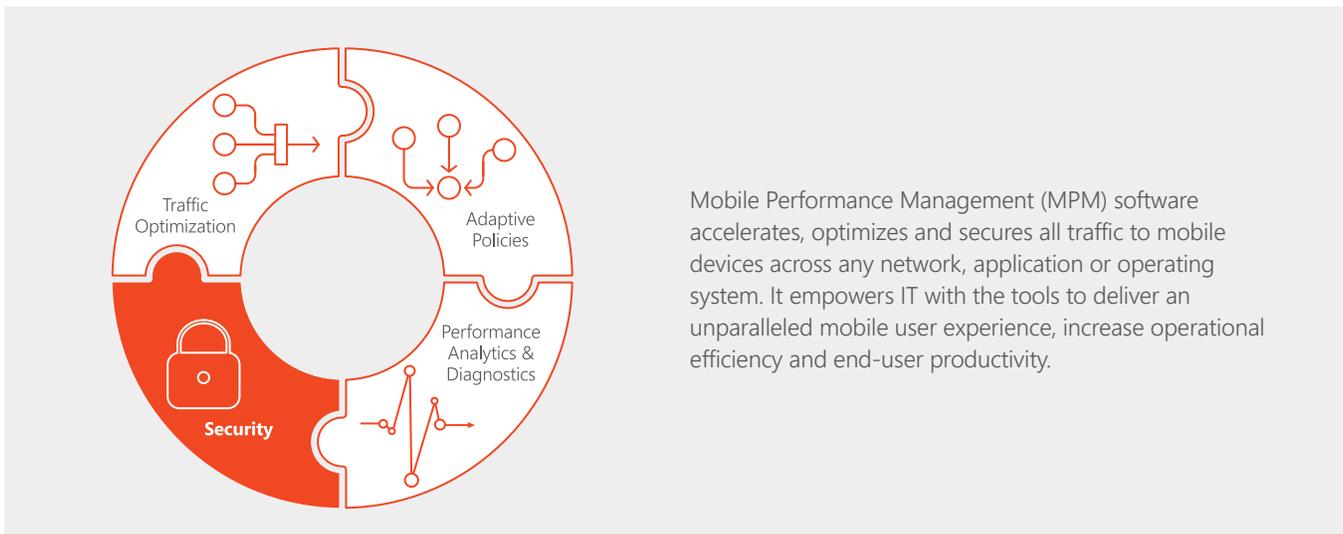
Device protections against undesirable traffic

A firewall on each device prevents unwanted or malicious traffic from entering, based on policies specified by IT to protect the user, the device and corporate resources. Centralized control allows IT to push the firewall configurations out to each device in the field, from a single console.



Integration with IT security tools

Mobile performance management software supports integration with popular security tools that identify and allow security personnel to remediate threats.



Mobile Performance Management (MPM) software accelerates, optimizes and secures all traffic to mobile devices across any network, application or operating system. It empowers IT with the tools to deliver an unparalleled mobile user experience, increase operational efficiency and end-user productivity.

Security through a highly flexible and programmable VPN purpose-built for mobility

When users roam from one network to another, security requirements change. NetMotion implements a secure tunnel that extends from the device to the control server inside the corporate data center or in the cloud, and maintains this tunnel regardless of the number of networks traversed. Since enterprise data transits the carrier's infrastructure and the Internet, strong authentication and encryption are required to protect and secure systems and data. Network access control techniques are also required to ensure that mobile devices are in compliance before granting them access to corporate assets behind the firewall.

Per-app, per-flow, or system-wide mVPN

Security through mobile performance management is enforced via a highly flexible and programmable VPN. It supports split tunneling on a per-app, per-flow basis, or device-wide lockdown requiring all traffic to route through the VPN to reach the enterprise network.

Advanced authentication & encryption

Advanced authentication & encryption meets the exacting requirements of sensitive industries. NetMotion supports two-factor authentication using RSA SecurID; x.509v3 certificates and PKI stored on the device or in a smartcard; or biometric device authentication. Encryption can be configured globally, on a user group, or per-user basis.

FIPS & Common Criteria certifications

NetMotion applies encryption using AES encryption modules at 128-, 192- or 256-bit cipher strengths that are FIPS 140-2 validated to meet the U.S. government's standard for securing non-classified information. In addition, NetMotion is certified at Common Criteria Evaluation Assurance Level 4 (EAL4+) augmented with flaw remediation, an international set of guidelines used extensively throughout Europe and by the U.S. federal government.

Network Access Control

Network Access Control (NAC) detects the security status of the client and allows IT to define security-related criteria and actions that control client access to the corporate network. For example, in order for a client on Windows to connect, it must have a certain antivirus product installed and auto-update enabled.

Distributed Firewall

Granular control over application access by IP addresses, ports or other parameters, centrally maintained as policies at the server and distributed for enforcement by devices in the field, creates a distributed firewall spanning all enterprise devices.

SIEM

Log export allows IT to use SIEM tools to analyze NetMotion logs, for integration with the enterprise's overall security strategy.

Geo-fencing

Geo-fencing enforces location-based security, alone or in conjunction with other parameters such as port number, IP address or application in use. This, for example, allows access to corporate resources only while the user is within bounds of a headquarters building, corporate campus or other authorized facilities.

Sign-on continuity

Workers only need to use one set of login credentials, at the start of each shift, and NetMotion handles all subsequent logins as they roam across various networks. This is not only a convenience to the worker, but also makes multi-factor authentication more practical to implement and the enterprise more secure because the secure tunnel persists throughout the entire shift.