NetMotion Wireless Mobility XE™

Preisgekrönte mobile Best-in-Class VPN-Lösung

Mobility XE wurde speziell für Mitarbeiter entwickelt, die häufig unterwegs und dabei auf sicheren und zuverlässigen drahtlosen Zugriff auf kritische Daten und Anwendungen angewiesen sind. Mit dieser Lösung bleiben Ihre Mitarbeiter produktiv, auch wenn sie am selben Tag an mehreren Standorten arbeiten oder zwischen verschiedenen Stockwerken und Gebäuden auf dem Firmengelände unterwegs sind, denn sie ermöglicht den Zugriff auf unterschiedliche Netzwerke, das Überbrücken von Funklöchern sowie das Ab- und Anmelden der mobilen Endgeräte.

Sicherheit

Schutz. Die branchenweit stärkste Verschlüsselung mit FIPS-Validierung (Federal Information Processing Standard) sichert Datensitzungen innerhalb des VPN-Tunnels. Vor Erteilung einer Zugriffsgenehmigung überprüft das Netzwerkzugangskontrollmodul, ob auf jedem Endgerät die neuesten Software- und Patch-Versionen installiert und sämtliche Sicherheitsvorkehrungen aktiviert sind.

Authentifizierung. Durch die Unterstützung standardbasierter Two-Factor-Authentication erhalten Behörden eine erschwingliche Möglichkeit, staatlichen Sicherheitsvorschriften Folge zu leisten. Wirtschaftsunternehmen bietet die Two-Factor-Authentication eine zusätzliche Schutzmaßnahme für gefährdete mobile Endgeräte. Mobility XE unterstützt preisgünstige Smart Cards sowie kostenfreie bzw. kostengünstige X.509v3-Benutzerzertifikate und somit die Mehrzahl der standardbasierten Infrastrukturen für die PKI-Authentifizierung, einschließlich der von Microsoft-Server-Betriebssystemen genutzten Infrastruktur, durch eine RADIUS-EAP-Schnittstelle.

Produktivität

Durchsetzung. Flexible Policies steuern das Verhalten von Geräten und Anwendungen, schränken den Anwendungszugriff ein und lassen keine Prozesse, die große Übertragungsbandbreiten benötigen, in langsameren Netzwerken zu, um eine Beeinträchtigung der Leistung zu verhindern.

Komfort. Mobile Mitarbeiter können sich ganz praktisch per SSO (Single Sign-on) einmalig authentifizieren und anschließend sämtliche Netzwerke und Access Points nutzen. Mit Mobility XE ist auch während des Aufenthalts in Funklöchern eine anhaltende Authentifizierung und die zuverlässige Funktion der Anwendungen sichergestellt.

Roaming. Mobility XE ermöglicht den nahtlosen Wechsel zwischen beliebigen IP-Netzwerken. Der Benutzer kann frei zwischen gedockten Verbindungen, Unternehmens-Wi-Fi-Netzen, Hotspots von Drittanbietern und Mobilfunk-Datennetzwerken verschiedener Anbieter wechseln. Das Gerät sucht sich dabei immer die schnellste verfügbare Verbindung.

Performance. Mobility XE verbessert den Datendurchsatz, Reaktionsgeschwindigkeit von Anwendungen und die Produktivität in Drahtlosnetzen mit limitierter Bandbreite. Es reduziert den Protokollaufwand und die Menge ausgetauschter Daten und komprimiert Informationen und Web-Grafiken, wodurch sich der Datendurchsatz maßgeblich verbessert.

Zuverlässigkeit. Kein anderes mobiles VPN hält Sessions so effektiv aufrecht und stabil wie Mobility XE. In Funklöchern werden Anwendungen einfach angehalten und nehmen die Datenübertragung erst wieder auf, wenn die Verbindung wieder hergestellt ist. Die Datenübertragung geht an der Stelle weiter, an der sie angehalten wurde, auch wenn die Verbindung tagelang unterbrochen war.

Management

Kontrolle. Mobility XE ist so konzipiert, dass Einstellungen nur einmal vorgenommen werden müssen und kaum Verwaltung für Routineprozesse anfällt. Die browserbasierte Administratorkonsole ermöglicht die zentrale Konfiguration, Verwaltung und Überwachung sämtlicher Systemaspekte – von den allgemeinen Systemparametern bis hin zu den genauen

Daten einzelner mobiler Benutzer. Die zentrale Steuerung erleichtert darüber hinaus die Sperrung unberechtigt genutzter, verlorener oder entwendeter Geräte.

Transparenz. Automatisierte Benachrichtigungen ermöglichen ein nahezu vollautomatisches Management. Ausgefeilte Analysefunktionen und umfassende Berichte geben Ihnen dabei genaue Einblicke in das Verhalten und die Anwendungsnutzung mobiler Mitarbeiter.

Kompatibilität. Alle Anwendungen, die über Ethernet verwendet werden können, funktionierten auch über eine Drahtlosverbindung zuverlässig, wenn Mobility XE installiert ist. Die Änderung von Anwendungen, teure Entwicklungsprojekte oder Upgrades auf besondere Wireless-fähige Versionen werden überflüssig. Mobility XE bietet die Anwendungskompatibilität eines IPSec-VPNs ohne die aufwändige und komplexe Anwendungsinstallation für SSL-VPNs. Mobility XE ist mit jedem IP-Netzwerk und jedem Windows-Gerät kompatibel.

Wirtschaftlichkeit. Die Installation und Einrichtung dauert in der Regel nur wenige Stunden. Der Mobility XE-Server lässt sich hinter der Unternehmens-Firewall oder innerhalb der DMZ auf einer standardmäßigen, handelsüblichen Hardware – einschließlich virtuellen Umgebungen – installieren. Die Clientsoftware kann auf jedem Windows-Gerät installiert und zentral konfiguriert werden und ist für den Endbenutzer transparent.

Skalierbarkeit. Mobility XE bewältigt mühelos den Übergang vom kleinen Versuchsprojekt zu einer umfangreichen Installation. Ein einziger Server kann bis zu 1.500 angeschlossene Geräte gleichzeitig bearbeiten. Server lassen sich zusammenschließen, um neben einer Kapazitätserweiterung auch Lastausgleich, Failover und Redundanz für Tausende von Mitarbeitern bereitzustellen. Dies ermöglicht ein hochgradig skalierbares und zuverlässiges System ohne alleinige Fehlerstellen.

Policy-Verwaltungsmodul

Zentrale, flexible Kontrolle über die mobile Produktivität und Sicherheit. Das optionale Policy-Verwaltungsmodul setzt unternehmensspezifische Sicherheits-Policies durch und gewährt selektiven Zugriff nach Benutzer, Gerät, Netzwerk oder Anwendung.

- **Kontrolle über den Zugriff auf Anwendungen und Ressourcen.** Die Policies ermöglichen eine granulare Kontrolle über den Netzwerkzugriff von Anwendungen und die zulässigen Zugriffszeiten.

- **Zuweisung von Policies**. Die Durchsetzung von Policies ist für den Benutzer transparent und kann individuell, nach Aufgabe, Arbeitsgruppe oder für die gesamte Organisation zugewiesen werden.

- **Verwaltung des Datenverkehrs nach Dienstqualität.** Durch die Klassifizierung von Datenverkehr und Regeln zur Steuerung dieses Datenverkehrs können missionskritische Anwendungen Vorrang erhalten, um ihre Verfügbarkeit unabhängig vom Netzwerktyp zu gewährleisten.

- **Einschränkung von bandbreitenintensiven Anwendungen auf Verbindungen mit hoher Kapazität.** Mit Regeln können Anwendungen, die eine hohe Verbindungsbandbreite erfordern, von langsameren Netzen ausgeschlossen werden. Außerdem können bestimmte Anwendungen proaktiv gestartet werden, wenn eine High-Speed-Verbindung verfügbar wird.

- **Unterstützung von Echtzeitanwendungen.** Neben den Funktionen zur Verwaltung des Datenverkehrs nach Dienstqualität bietet Mobility XE Funktionen zur Wiederherstellung bei Paketverlust, die für eine bessere Performance von Echtzeitanwendungen wie VoIP, Video-Streaming und Echtzeitkonferenzen sorgen, die empfindlich auf Latenzzeiten und Jitter reagieren.

- **Sichere und einfache Nutzung von WLANs und WiFi-Hotspots.** Mit Policies kann Anwendungsverkehr je nach Zugriffspunkt und Hotspot-Anbieter selektiv zugelassen oder blockiert werden.

Netzwerkzugangskontrollmodul

Durchsetzung von Sicherheits- und Compliance-Policies für mobile Geräte. Das Network Access Control-Modul (NAC) für die Kontrolle des Netzwerkzugriffs stellt sicher, dass die Geräte von Mitarbeitern einen adäquaten Sicherheitsstandard aufweisen, bevor ein Verbindungsaufbau und Zugriff auf Anwendungen und Daten gestattet wird.

- **Schnelle Implementierung.** Der NAC-Modul-Assistent erleichtert die Konfiguration und Implementierung von Sicherheits-Policies in wenigen Minuten, ohne dass die Netzwerkinfrastruktur neu konfiguriert werden muss.

- **Gewährleistet die Einhaltung von Sicherheitsvorschriften.** Beim Einsatz von NAC werden mobile Geräte gescannt, um festzustellen, ob erforderliche Software-

programme vorhanden sind, wie z. B. Viren- und Spyware-Schutz, Firewall, Betriebssystemversion, Windows™-Aktualisierung, Registrierungsschlüssel und andere Anwendungen.

- **Flexible Kontrolle über nicht-konforme Geräte.** Je nach Schweregrad können Administrator Maßnahmen definierten, von einfachen Warnmeldungen bis zur Auslösung individuell einstellbarer Verfahren, die den Zugriff einschränken, Websites aufrufen, Software-Downloads einleiten oder sogar die Verbindung trennen und das Gerät sichern können.

- **Automatische Aktualisierung und Compliance-Prüfung.** Aktualisierungsregeln werden im Push-Verfahren automatisch an Clientgeräte übertragen. Die Geräte werden in regelmäßigen Abständen automatisch neu gescannt, um die fortgesetzte Einhaltung der Vorschriften nach einem erneuten Verbindungsaufbau zu gewährleisten.

- **Einheitliche Unterstützung für mehrere Plattformen.** NAC-Policies werden von allen Windows-Clientgeräten unterstützt, einschließlich Laptops, Handgeräten und Smartphones.

Analysemodul

Proaktives Management und transparente Nutzung mobiler Endgeräte. Das Analysemodul stellt Nutzungsdetails und geschäftsrelevante Informationen zur Verfügung, die bei anderen VPNs nicht abrufbar sind. Hier erhalten Sie detaillierte statistische Daten zu Performance und Nutzung sowie wertvolle Einblicke in die Nutzung von Netzwerken und Anwendungen durch mobile Mitarbeiter, und können darüber hinaus automatische Benachrichtigungsfunktionen nutzen, die Ihnen Verwaltungsaufwand ersparen und eine bedarfsgerechte Anpassung und Kapazitätsplanung erleichtern.

- **Vom Überblick zu den Details.** Grafische Berichte zu Nutzungstrends gehen weit über einfache Aktivitätsprotokolle hinaus, wie sie von normalen VPNs bereitgestellt werden. Mithilfe von Filtern können Sie selektiv genaue Daten zu bestimmten Benutzergruppen und Zeiträumen anzeigen.

- **Machen Sie sich mit der Ressourcennutzung vertraut.** Informieren Sie sich darüber, welche Anwendungen, Geräte und Benutzer die größte Bandbreitennutzung aufweisen. Nutzen Sie Richtlinien zur Verbesserung der Produktivität und Einhaltung von Netzbetreiber-Servicevereinbarungen.

- **Erkennen Sie Funkabdeckungs- und Verbindungsprobleme.** Informieren Sie sich, bei welchen Geräten und Netzwerken Verbindungsprobleme auftreten und zu welchen Zeiten bzw. aus welchen Gründen es dazu kommt.

- **Steigern Sie die Effektivität der Helpdesk-Mitarbeiter.** Geben Sie den Helpdesk-Mitarbeitern umfangreichere Unterstützungsmöglichkeiten, indem Sie ihnen ermöglichen, die aktiven Anwendungen, die Anwendungsversionen und den Geräteakkuzustand mobiler Benutzer abzurufen. So können sie sehen, wie häufig Anwendungen ausgeführt werden, wie viel Netzwerkverkehr die Benutzer erzeugen und welche anderen Anwendungen Leistungsprobleme verursachen.

- **Erhalten Sie Warnmeldungen bei drohenden Problemen.** Nutzen Sie mehr als 30 Benachrichtigungsoptionen, zahlreiche davon mit anpassbaren Schwellenwerten, per E-Mail, SNMP oder Syslog.

- **Performance-Nachweis und proaktive Planung.** Vergewissern Sie sich, dass Benutzer die mobile Umgebung sinnvoll nutzen, und informieren Sie sich, ob mehr Bandbreite oder eine bessere Netzabdeckung erforderlich sind.