White Paper

Regaining Control of the Mobile Workforce

May 2007 - Trellia Networks Inc.

Trellia
Securing Mobility

Table of Contents

Executive Summary 1
Mobility Today 2
Mobility Drivers 3
Mobility Risks 3
Regaining Control 5
Enabling the Secure Mobile Workforce 7
Summary 7
Appendix A 8

Executive Summary

The enterprise workforce is increasingly mobile. This new work dynamic is creating pressures on IT departments to deliver on mobile worker expectations of continuous connectivity while outside of the facilities under IT control. These same departments are faced with the challenge of enforcing IT security policies on mobile devices while maintaining IT support costs at bay.

This paper explores the benefits and risks associated with an increasingly mobile workforce as they pertain to the CIO, IT Manager and other IT professional. Solutions are proposed that leverage mobility benefits while minimizing associated risks. We hope the information in this paper encourages companies to develop strategies that normalize IT policies for mobile devices to the same extent to which fixed IT infrastructure is managed today.

Mobility Today

The modern enterprise workforce is mobile. A study conducted by IDC estimates that by 2009, approximately 27 percent of the worldwide workforce will be mobile. In the United States, that number is expected to surpass 70 percent . Whether or not IT professionals are favourable to the use of mobile devices and wireless network connectivity by their workforce, the reality is that enterprise workers have embraced the convenience of connecting to the Internet in every place imaginable, from the local coffee shop, to the airport waiting lounge and even while on the road driving to a client meeting. Yet 44% of enterprises surveyed in an Aberdeen Group study indicate they have no formal wireless mobility program in place and 10% indicate there is no group responsible for managing wireless mobility within their enterprise . This has created a situation where many employees deploy their own or connect to third party wireless networks without the knowledge of IT departments, exposing enterprise data to risk and often leading to spiralling support and wireless connectivity costs . Although 56% of enterprises do have wireless mobility programs in place, which helps mitigate the costs of ad-hoc worker wireless connectivity, according to research by J. Gold Associates, less than 10%, have deployed mobile security solutions, even though such technologies have been shown to effectively minimize data risk . In light of these findings, one can conclude that:

>> **Enterprise workers are increasingly mobile**

>> **IT lacks control over mobile worker connectivity**

>> **Mobile workers expose their enterprise data to risk**

Trellia specializes in the development of enterprise mobility solutions. Its vision is to enable a world where the **mobile workforce is always securely and seamlessly connected**.

Over the past several years, Trellia has developed innovative software solutions that empower IT departments to control mobile devices in a centralized fashion, while also providing the mobile worker seamless mobile experience.

Mobility Drivers

While IT professionals have been assessing the security risk of implementing a Wi-Fi infrastructure within their organization's facilities, sales representatives, technicians and management have been activating their integrated Wi-Fi radios or have purchased 3G cards (and soon 4G) to surf the Internet via broadband cellular networks. The drivers for this behaviour are straightforward. The increased productivity enabled by wireless connectivity by converting wasted travel time into hard working time is priceless to the modern worker. According to Research In Motion, equipping workers with mobility capabilities leads to many benefits, including :

>> **Better business decisions**
>> **Increased productivity**
>> **Improved communication**

Mobility Risks

Security

Worker mobility can result in significant benefits, as listed above, however IT professionals need to be aware of the inherent risks associated with mobility. Mobile workers connect to third party wired or wireless networks to perform their jobs on the go, and increasingly such workers are moving beyond e-mail and basic internet surfing to accessing business critical systems such as ERPs and CRMs using notebooks or smartphones. Sensitive corporate data is accessed, viewed and modified on devices and over networks that are out of IT's control. According to J. Gold Associates, "… data escaping the company boundaries and thus exposing customer records, financial information, personnel files, etc., are not only damaging to company reputations, but can lead to real financial loss through lawsuits, regulatory fines, customer retention failures, loss of good will, etc." . By accepting a reality where mobile workers connect to any network they desire (e.g. manager on business trip connects to an unsecured public Wi-Fi to access CRM), IT departments are allowing situations where mobile workers expose sensitive data to external parties. Evidently, IT must control and monitor the network connectivity of their mobile workforce in order to minimize the risk of data loss.

Trellia's Nomad Mobility Platform™ is an **intelligent mobility solution** that enables secure and seamless connectivity for the mobile workforce. Nomad's powerful policy management capabilities empower IT managers to regain control over mobile devices, while Nomad's intelligent connectivity engine provides mobile workers with seamless access to LAN, WLAN and cellular networks.

The Nomad Enterprise Server™ (NES) is the server-side application of the Nomad Mobility Platform. Designed for the enterprise IT professional, the NES enables remote configuration of mobile devices. From **enforcing VPN** when the mobile worker connects to public networks, to **restricting users to secure wireless network** connectivity, the NES makes it possible to secure mobile workers as if they were connected to the enterprise LAN

Support

Beyond the risk of exposing sensitive corporate data, the mobile worker also places a significant strain on IT budgets and support resources. According to Gartner Research, enterprises that do not have an established mobile worker strategy can spend between 10% and 20% more than organizations that do . These costs will undoubtedly increase further as new wireless technologies are made available and adopted. In the US, WiMax is already generating significant interest today, where over 50% of surveyed end-users are extremely or very interested in WiMax services according to an In-Stat survey . If these figures are foretelling indicators of adoption rates, IT departments are likely to be faced with a tidal wave of support calls as workers desire to connect their laptops and smartphones to various wireless technologies, from Wi-Fi to broadband cellular networks such as 3G/EDGE/HSDPA, 3G/EV-DO and 4G/WiMax.

Connectivity

IT support costs are not the only financial hit facing enterprises with a mobile workforce. Indeed, according to research by the Aberdeen Group, enterprises can spend up to ten (10) times more managing wireless and mobility services for their workforce than wireline. This exorbitant cost multiplier is primarily due to the unmanaged and decentralized nature of wireless connectivity in the mobile workforce. In a multi-network environment, the mobile worker is primarily concerned with establishing connectivity. The cost of connecting to one network over another is rarely an active preoccupation. As such, workers will maintain high-cost connectivity (e.g. 3G network) even when a pre-paid Wi-Fi network is within reach.

The sum of support and connectivity costs and the rapid expansion of ad-hoc mobility amongst the enterprise workforce are leading to a situation where according to J. Gold Associates "company IT organizations will be unable to cope with the new mobile reality unless they rethink their existing management and security strategy." As such, enterprise IT professionals need to develop strategies that will allow them to counter the risks of workforce mobility, notably:

- >> **Exposure of sensitive corporate data**
- >> **Escalating IT support costs**
- >> **Uncontrolled connectivity costs**

Besides providing seamless mobility to the mobile worker and peace of mind to the IT manager, the Nomad Mobility Platform™ provides enterprises with significant and measurable cost savings. The complexity of today's wireless connectivity results in numerous IT support calls from mobile workers who are frustrated by the inability to connect or maintain reliable connectivity. By providing **zero-click seamless roaming** to the mobile worker, Nomad **virtually eliminates support requests** for wireless connectivity and as a result frees valuable IT resources.

With the availability of wireless data connectivity over cellular networks, a mobile workforce can generate significant connectivity expenses. To minimize these, the Nomad Mobility Platform offers extensive connectivity criteria to maximize connectivity on low-cost networks and provide access to high-cost networks only when needed. As a result, the implementation of Nomad leads to an **immediate reduction in data transfer costs**.

Regaining Control

The challenge facing the IT professional is to gain control over the mobile workforce as if these workers were confined to their desks within the organization's facilities. Avoiding the issue of mobility and wireless connectivity is clearly not an option as users will mobilize themselves, which has been demonstrated as a dangerous and costly approach. Therefore, this paper proposes enterprise IT departments:

>> **Enforce IT security policies on all connectivity**
>> **Centrally configure and manage every mobile device**
>> **Automate all connectivity choices**

Developing a comprehensive mobility management strategy is an essential first step to achieving the above objectives. Once a desired state is clearly defined and typical user profiles are developed, communication and education campaigns developed for workers can server as a first step to implementation. However, IT departments cannot merely rely on users to comply with mobility best practices due to the inherent complexities of these technologies. Indeed, according to Trellia research, over 80% of enterprise mobile users do not know what a WEP key is. Wi-Fi is the wireless technology that mobile workers are the most familiar with, yet even the most basic security technologies are not well understood. According to J. Gold Associates, any mobility management solution must enable policy-based management, provide security capabilities and require little or no user involvement. Within this context, technologies such as intelligent mobility solutions, can serve as a powerful tool to regain control over the mobile workforce.

Enforcing IT security policies on all connectivity

IT security policies for mobile connectivity will vary from one organization to another. However, any mobility solution managing connectivity should provide IT departments with the ability to monitor, restrict and/or enforce connectivity in respect to network choice and security policy. Capabilities should include:

>> **Connectivity restrictions based on network security assessment**
>> **VPN enforcement over unsecured networks as defined by IT**
>> **Internet routing via proxy**

Trellia's Nomad Enterprise Server™ enables the **centralized distribution of IT policies to mobile devices** over the Internet. This powerful capability allows the IT professional to modify a single user's network access rights while he or she is travelling across the globe, or implement a new business logic rule for network switching on all of the enterprise's mobile devices to instantaneously reduce wireless connectivity costs.

Policy-based rules can be applied for security, throughput, location, cost, preference or other criteria.

Centrally configure and manage every mobile device

Over 85% of knowledge workers will purchase a smart device within the next 2-3 years. The power inherent in these new smart devices provides the possibility of performing increasingly complex tasks, which inevitably generates greater support requirements. Mobile devices should be treated no differently than fixed IT assets. As such, to manage mobile worker support costs, any mobility solution should provide IT departments with the ability to pre-configure devices and continuously update these devices once they are in the field. Capabilities should include:

>> **Ability to pre-configure devices before deployment**
>> **Over the air (OTA) continuous updates as policies evolve**
>> **Device configuration restrictions for users**

Automate all connectivity choices

Mobile workers should connect to wireless networks in a seamless and worry free fashion as they connect to the corporate LAN today. As such, any mobility solution should intelligently automate the connectivity process by selecting the appropriate network and manage connectivity dynamically based on pre-established business and IT policies. Capabilities should include:

>> **Automatic network selection based on IT and business policies**
>> **Application and session persistency as connectivity is switched**
>> **Switching based on Internet access capability**

Trellia's Nomad Mobility Client™ eliminates the complexity of choosing which network technology to connect to, Wi-Fi to 3G to 4G, as well as which specific sites to connect to. In many locations today, a mobile worker may have access to numerous Wi-Fi access points, a LAN and two or three cellular networks.

Nomad uses predefined connectivity settings determined by the IT manager, Internet sensing, as well as built-in heuristic algorithms to intelligently determine which network to connect to.

Enabling the Secure Mobile Workforce

For several years, research and development teams at Trellia have focused their efforts on the development of solutions that mobilize an enterprise workforce securely, while being transparent to the end-user. The Nomad Mobility Platform™, through unique capabilities such as VPN enforcement, zero-click seamless roaming, and application persistency, manages connectivity and roaming across wireline and wireless networks. Nomad can represent a powerful tool for enterprise IT departments by enabling the enforcement of stringent security guidelines and IT policies onto mobile devices.

Summary

Mobility in the modern workforce is an inevitable phenomenon that offers the potential of improved productivity, communication and decision making. Without a centralized IT management policy, these benefits can be reduced or completely negated through increased risk to sensitive corporate data as well as escalating IT support and connectivity costs. Intelligent mobility solution such as Trellia's Nomad Mobility Platform™ serve as essential tools for IT departments to implement mobility policies throughout an organization in a cost effective manner, leveraging the promised potential of unfettered worker mobility.

Appendix A

To illustrate some of the possibilities offered by enabling a secure mobile workforce, the following three scenarios highlight problems encountered with unmanaged mobility and the solutions rendered by an intelligent mobility solution.

Mobile Worker Jeopardizing Corporate Data Example

Picture a financial institution that provides its employees with a laptop with an integrated Wi-Fi chip. Concerned with the potential exposure of sensitive customer data through Wi-Fi connectivity, the laptop's wireless chip is disabled in the laptop's bios. A customer relationship manager at the financial institution is frustrated with the inability to connect to the enterprise database while on the road visiting clients. To circumvent the IT policy, the manager purchases a Wi-Fi card. While on the road, he connects to any available open Wi-Fi network in order to access his customer files. The IT department is oblivious to this situation, and as a result is unaware of the security hole introduced by their co-worker.

By using an intelligent mobility solution such as Trellia's Nomad Mobility Platform, all laptops and smart phones within the financial institution can be pre-configured to restrict the addition of unauthorized network devices such as a Wi-Fi card. The IT department can also use such as solution to allow access to wireless networks, but only if the network is secured. Upon connection to a wireless network, the IT department can also enforce VPN to be active and redirect Internet traffic through the enterprise Proxy.

Mobile Worker Leading to Escalating Support Costs

Consider a national real-estate firm with thousands of agents spread throughout the country. Agents are provided with laptops, but many have also purchased smart phones. In order to connect to the firm's online listing service while at a client location, many agents have attempted to use their smart phone as a modem to their laptops. Most are not able to connect, and the firm's IT staff have become swamped attempting to guide the agents through the procedure.

By using an intelligent mobility solution such as Trellia's Nomad Mobility Platform, all mobile devices, including agent's smart phones can be pre-configured or sent a configuration package over the air and then periodically updated, providing central control to the IT department, enabling them to configure connectivity for their agents.

Mobile Worker Escalating Connectivity Costs

Consider an industrial manufacturer that has a team of technicians that service the company's products across the globe. These technicians are often in remote areas and require connectivity to the enterprise's servers to run model testing before initiating repairs or replacement on the manufacturer's products. To enable technicians to access applications in remote areas, the IT department provides 3G cellular broadband connectivity cards for the technician laptops. As a result, the manufacturer's technicians increase their productivity by reducing the time needed to support the company's products. However, these technicians begin to use the 3G connectivity at all times, even when they are in areas where Wi-Fi is readily available. Worse, when technicians are at the office, they often inadvertently stay connected via 3G cellular network even when physically connected to the LAN as the carrier provided connectivity management software automatically establishes 3G connectivity whenever the card is plugged into the a technician's laptop. As a result, the company's wireless connectivity costs skyrocket.

By using an intelligent mobility solution such as Trellia's Nomad Mobility Platform, all connectivity by laptops and smartphones is automatically managed based on predefined security and business criteria. As a result, each available network is assessed based on numerous factors, including cost. Connectivity to a 3G network would only occur if LAN and Wi-Fi connectivity was unavailable.

References

i Worldwide Mobile Work Population 2005-2009. Drake, Stephen D., et al; IDC #34124, Volume 1, October 2005.

ii The Real Cost of Enterprise Wireless Mobility. Aberdeen Goup, January, 2007

iii Employees driving Wi-Fi adoption, Thomson, Iain. April, 2005

iv 10 Steps to Mobile Security, Gold, Jack. November, 2006

v Redefining the Mobile Workforce. Research In Motion, May 2006

vi Compliance in the Mobile Enterprise, Gold, Jack. April, 2006

vii 10 Steps to Mobile Security, Gold, Jack. November, 2006

viii Overviewing the Three Vectors of Mobile Worker Segmentation. Leif-Olof, Wallin., et al; Gartner #G00143165, November 2006

ix End-Users Prefer WiMAX!. In-Stat # IN0703519WBB, March, 2007

x The Real Cost of Enterprise Wireless Mobility. Aberdeen Goup, January, 2007

xi Compliance in the Mobile Enterprise, Gold, Jack. April, 2006

xii Compliance in the Mobile Enterprise, Gold, Jack. April, 2006

xiii 10 Steps to Mobile Security, Gold, Jack. November, 2006

This document is provided “as is” and Trellia Networks Inc. (“Trellia”) assume no responsibility for any typographical, technical, or other inaccuracies in this document. TRELLIA reserves the right to periodically change information that is contained in this document; however, TRELLIA makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. TRELLIA MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER TRELLIA NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF TRELLIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and/or third-party web sites (collectively the “Third-Party Information”). TRELLIA does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by TRELLIA of the Third-Party Information or the third party in any way. Installation and use of Third-Party Information with TRELLIA’s products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, TRELLIA expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with TRELLIA’s products and services is provided “as is.” TRELLIA makes no representation, warranty, or guarantee whatsoever in relation to the Third-Party Information and TRELLIA assumes no liability whatsoever in relation to the Third-Party Information even if TRELLIA has been advised of the possibility of such damages or can anticipate such damages.