# Business insight: Mobility

Enabling user mobility with enterprise security solutions

## The user mobility scenario

A fundamental principle for Generation Y, "work is something you do, not somewhere you are," is rapidly becoming reality for a much broader swathe of the corporate workforce. Teleworking, for instance, continues to take off as an attractive business practice, with increasing numbers of employers offering related programs to their employees in an effort to cut commuting and facilities costs while boosting morale and retention. But teleworking is really just the tip of the iceberg. With mobile technologies ranked among the top 10 technology priorities for 2011 in a survey conducted by Gartner[1], savvy business leaders have clearly caught on to the broader trend of user mobility and the many benefits it yields, including:

- Increased employee productivity
- Improved customer relationships (through increased face time)
- Greater resilience in the face of disruptive events (such as bad weather, influenza outbreaks or site-level outages)
- Lower infrastructure and operating costs

Part of this is also the realization that the "Consummerization of IT" is an unstoppable force – one that is characterized by a blending of life and work activities that also promotes mobility, along with its close companion, the proliferation of user devices.

With so many advantages, it's all too easy for business managers to overlook the fact that user mobility is also accompanied by a number of challenges, particularly in the areas of information security and privacy.

**Loss of control** – A significant expansion in the number of different device types being used is actually the first part of this problem. IT must not only support but also secure and to protect against a rapidly growing collection of user devices. Indeed, with over 50 million smartphones entering the worldwide market quarterly, it is not unrealistic that enterprises will see over 1 billion new networked mobile devices within the next three years. The second part of the problem is that these devices are increasingly user owned, or otherwise outside the control of corporate IT – a characteristic that considerably complicates related security and privacy efforts.

The proliferation of powerful smart devices also introduces a new problem for IT. As applications on the most popular mobile operating systems such as iOS and Google® Android™ become part of the infrastructure, IT must be able to guarantee critical bandwidth to critical applications, while limiting the negative impact of undesired traffic.

[1] See "mobile technologies" listing in: http://www.cmswire.com/cms/information-management/the-cloud-rises-to-top-of-2011-cio-priorities-009987.php

**Loss of identity** – Security for user mobility is further complicated by the virtual elimination of a 1-to-1 relationship between users and devices. The combination of portability and proliferation means it's no longer practical for security administrators to rely on user identity being synonymous with device identity (and vice versa).

**Greater exposure** – By definition, mobility entails user devices residing and operating beyond the confines of the corporate network and, therefore, beyond its associated defenses. Direct connections to the Internet, coupled with the loss of control discussed earlier, mean that mobile devices are not only exposed to more threats that can pass through undetected into the corporate network, but also are more susceptible to them.

## Dell SonicWALL for the mobile enterprise

Taking full advantage of the benefits of user mobility obviously depends on being able to address the related security challenges. In this regard, enterprise security solutions from Dell SonicWALL give today's organizations exactly what they need.

## Dell SonicWALL VPN solution

Dell™ SonicWALL™ is the only provider that solves the challenges of access, security and control with one integrated Clean VPN solution that combines Dell SonicWALL Clean VPN technology and Application Intelligence and Control. When a Dell SonicWALL SSL VPN solution is deployed with a Dell SonicWALL firewall, Dell SonicWALL Clean VPN scans tunneled traffic to block malware from using smartphone communications as a conduit into the network. Dell SonicWALL Application Intelligence and Control can allow increased bandwidth for critical applications, while limiting bandwidth for unimportant or unacceptable traffic.

**Dell SonicWALL Clean VPN™** delivers the critical dual protection of SSL VPN and high-performance Next-Generation Firewall necessary to secure both VPN access and traffic. The multi-layered protection of Clean VPN enables organizations to decrypt and decontaminate all authorized SSL VPN traffic before it enters the network environment.

**Dell SonicWALL Application Intelligence and Control** provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. A tightly integrated feature of Dell SonicWALL Next-Generation Firewalls, Dell SonicWALL Application Intelligence uses Dell SonicWALL Reassembly-Free Deep Packet Inspection® to identify and control applications, regardless of port or protocol.

## Bottom Line

Enterprise security solutions from Dell SonicWALL help IT departments tackle device proliferation and related security challenges, enabling today's enterprises to embrace the practice and more fully realize the corresponding benefits of having a truly mobile workforce.