MOBILITY REDEFINED

As legions of employees take their work outside the office and to the far reaches of the globe, supporting the diverse needs of a highly mobile workforce has become a strategic business priority. To encompass this new world order, organizations must implement strong security technologies, intuitive remote management tools, streamlined backup solutions, and a plan for smooth product transitions.

By Jeanne Feldkamp
Daniel Bounds
Terry Myers
Tom Kolnowski

Related Categories:

Case study
Data consolidation and management
Dell Latitude laptops
Dell Precision workstations
Dell ProSupport Services
Laptops
Mobility
Remote management
Security
Systems management

Visit DELL.COM/PowerSolutions for the complete related category index.

Across industries and in organizations of all sizes, mobile technology is breaking down the borders of business as usual. Employees are taking their work with them wherever they go and expecting ubiquitous network access—from the conference room down the hall to customer and vendor sites around the world. At the same time, the rapid adoption of mobile devices (such as broadband-enabled handhelds, tablet PCs, and other portable Internet endpoints) in emerging markets such as China and India is contributing to a global explosion in network size.

Organizations are embracing these trends with enthusiasm, encouraging employees to take advantage of the flexibility inherent in mobile computing to work in their own style and on their own schedules. But all this means it is no longer enough simply to equip employees with laptops and BlackBerry devices. Mobile workers need the support of an IT department with a strong, cohesive security strategy. They must be able to access enterprise networks whenever and wherever they need to work. When they have questions, they need immediate IT support that can diagnose and fix problems without delay. And when the organization transitions to new mobile devices, they need the switch to be fast, smooth, and trouble free.

BE IN THE OFFICE—ANYWHERE

An increasing number of employees use their laptops outside their home or office. And virtually everyone is getting in on the trend: organizations of all sizes are planning to retire their desktop infrastructure in favor of laptops that are easy to manage and maintain. Laptops are being mounted in service trucks and patrol cars. Doctors are making notes and writing prescriptions using handheld PDAs instead of clipboards. Students are abandoning their binders in favor of tablet computing, while soldiers and workers in harsh environments such as oil and gas rigs are taking ruggedized laptops along so they can stay informed and productive when they are in the field.

Employee productivity depends on the mobile device's connectivity, battery life, and durability. And as mobility facilitates growing levels of collaboration, users need enhanced tools and features such as video conferencing to fully engage with coworkers and partners. As a result, workers in untraditional environments also need self-support capabilities to stem the rising tide of mobile support requests.

Part of the IT team's job is to support maximum productivity by choosing appropriate laptops and other devices to meet the individualized needs of mobile employees. But IT leaders also must support the mobile infrastructure in a way that is designed to minimize costs, simplify administration efforts, protect against mobile-specific threats, and ensure security. Key enablers of the mobile workforce include the following:

- Outstanding security and network accessibility
- Simple, intuitive systems and data management tools
- A streamlined process for backing up critical data
- Smooth transitions when changing hardware or software

Dell offers a comprehensive range of solutions to help organizations meet these requirements (for a real-world example, see the "Mobility at Merrill Lynch" sidebar in this article). Models from the new Dell™ Latitude™ laptop and Dell Precision™ mobile workstation families are designed not only to meet the evolving needs

MOBILITY AT MERRILL LYNCH

For Merrill Lynch—a leading wealth management, capital markets, and advisory organization that operates in 40 countries and manages client assets of more than US$1.6 trillion—enabling the mobile workforce is a critical factor in continuing the company's success and maintaining market leadership.

A large percentage of the personal computing devices used at the company are made by Dell—including virtually 100 percent of the laptops.

"We strive to give our employees and business partners the technology that gives them an edge over our competitors," says Joe Martella, director of client-facing infrastructure in the Architecture and Engineering Group at Merrill Lynch. "That means we need to give end users the right devices and tools to help them do business and generate revenue, wherever they are physically located."

Merrill Lynch chose Dell platforms for innovation and ease of maintenance. "We're excited about what's happening with the new E-Family Latitude laptops," says Martella. "We appreciate the quality and the innovation that Dell is putting into the platform."

According to Martella, size and weight are major considerations when it comes to working from the road. "The compact form factors are what our users are asking for," he says. "Until now, the majority of our purchasing has been in the 3.5- to 4-pound range. Our users have been demanding something smaller and lighter. The new E-Family Latitude laptops certainly will meet those requirements. We've seen preproduction units and are looking forward to evaluating them as soon as they become available.

"We're a particularly demanding organization, and Dell has been responsive to our needs," Martella continues. "It's been a great partnership."

of the mobile workforce, but also to provide the IT tools that help simplify the deployment, management, and security of mobile devices (see the "Sleek, powerful offerings support a highly mobile workforce" and "Mobile networking—simplified" sidebars in this article). In addition, these offerings reflect the Dell philosophy of commonality and long product life cycles to help keep costs in check.

SAFEGUARD SECURITY AND NETWORK ACCESS

IT support teams face a variety of security-related challenges. Laptops are particularly vulnerable to physical threats such as theft and accidental damage. Improperly secured mobile networks can allow data leaks and put proprietary enterprise knowledge in the wrong hands. Security breaches can also make organizations susceptible to notification costs, lost productivity, and potential fines that subtract directly from the bottom line. Perhaps even worse, security problems expose organizations to bad press and—most significantly—potential loss of shareholder value, customer confidence, and loyalty.

In the past, laptop security practices have not taken a balanced approach to the challenges inherent in securing mobile devices. The complexity of implementing consistent security across a range of remote devices often means that a few systems fall through the cracks—leaving gaps where the network is vulnerable to attack. Security practices and backup procedures can be confusing to end users, which puts sensitive enterprise data at risk if a laptop, smartphone, or PDA is lost or damaged. Inconsistent data management can also expose organizations to serious compliance violations.

Because complex security policies can be difficult for employees to follow, it is unrealistic to leave security in the hands of mobile employees. An effective enterprise security plan should provide for simple, automated, scalable, and comprehensive ways to protect IT investments and maintain worker productivity. Organizations must approach security from a comprehensive perspective that ranges from the desktop to the data center, following best practices to help ensure that the plan protects both physical assets and data.

The Dell strategy for mobile security is based on four imperatives:

1. **Protect systems:** Asset tags can help simplify asset management by identifying individual devices. When used in conjunction with server-side asset management tools such as Altiris® Dell Client Manager™ software, these tags can give IT organizations the ability to monitor internal system components. In addition, dedicated security locks can help prevent theft. Visual deterrent labels and company logos offer an additional layer of protection against common theft because they can prevent an easy resale.
2. **Protect data:** When physical protection fails and a mobile device is lost, stolen, or damaged, it is critical that organizations retain the ability to protect sensitive enterprise data on the system. Data protection is linked to efficient access management. If authentication is not well managed, data protection can be difficult—especially if it is not centrally controlled.

   With a central security management solution such as Wave Systems EMBASSY Trust Suite—a server-side application that

interacts with the client-side software for central management linked to the Microsoft® Active Directory® directory service—IT departments can maintain control over key client security features and link them back to Active Directory. This capability helps simplify security management and smooths the deployment process for full-disk-encryption hard drives. Hardware full disk encryption enables transparent data protection to minimize impact on end-user efficiency. Dell Remote Data Delete services also enable organizations to delete data remotely from stolen laptops, as well as trace the systems for recovery through law enforcement organizations.

3. **Prevent unauthorized access:** Security policies must strike the correct balance between providing the right people with access to the right level of information and blocking access for improper users. Organizations typically have an Active Directory implementation with systems and user references. However, attempting to enforce and strengthen rules and policies often adds unwelcome complexity for end users.

Authentication is key to enabling secure data access because it focuses on identifying the user. Authentication methods can include smart cards with PIN access, contactless cards, or unique biometric verifiers such as Federal Information Processing Standards (FIPS)–certified embedded fingerprint readers. Such technologies are available in a variety of Dell products in the new Dell Latitude laptop and Dell Precision mobile workstation families. Trusted Platform Modules also enable enhanced security (as a repository for security credentials) as well as multiple authentications to local components and applications or networks. Multi-factor authentication is the combination of these technologies into one strong authentication process, whereby any end user may be asked for more than one form of authentication.

Dell ControlPoint software offers a unified application framework that allows organizations to customize laptop security settings according to individual needs and usage styles. Dell ControlVault™ software complements these capabilities by providing a single firmware location for end-user credentials such as passwords and biometric templates, which enables Dell laptops to perform security processing and matching outside the scope of malicious applications.

4. **Prevent malicious attacks:** The Dell approach to network security focuses on antivirus deployment and security appliances, targeting three lines of defense: endpoint protection, which relies on software designed to safeguard mobile devices; network traffic monitoring, which uses appliances to watch for unusual data traffic patterns on enterprise networks; and Internet gateway appliances, which serve as filters and firewalls that selectively identify and block potentially dangerous data.

In addition, factory-installed antivirus software is standard on Dell Latitude laptops and Dell Precision mobile workstations and offers a first level of defense against malware. This software can be updated with full versions for enhanced protection or replaced by other enterprise software.

The modular Dell Solution-Based Security Framework (see Figure 1) is based on the preceding four tenets. The goals: remove complexity from mobile security by enabling integrated manageability, make the mobile infrastructure easy to deploy and maintain, and ensure that data is as safe on a laptop as it is on a desktop behind an enterprise firewall.

Hardware, software, and manageability tools—along with security appliances, storage, and services—constitute the basic building blocks of the framework. Dell technologies include encrypting hard drives and the associated manageability software, which helps streamline security by providing a comprehensive yet simple solution. Furthermore, mobile security services such as Remote Data Delete can help prevent potential leakage of valuable data if a laptop is stolen.

Security is also designed directly into many Latitude hardware and software components.[1] New Dell Latitude laptops and Dell Precision mobile workstations use a single, safe hardware location to store encryption keys, which avoids the security risk of storing credentials using software. The new laptops also use discrete processing power for credentials processing, so users do not have to access the OS or software to perform authentication.

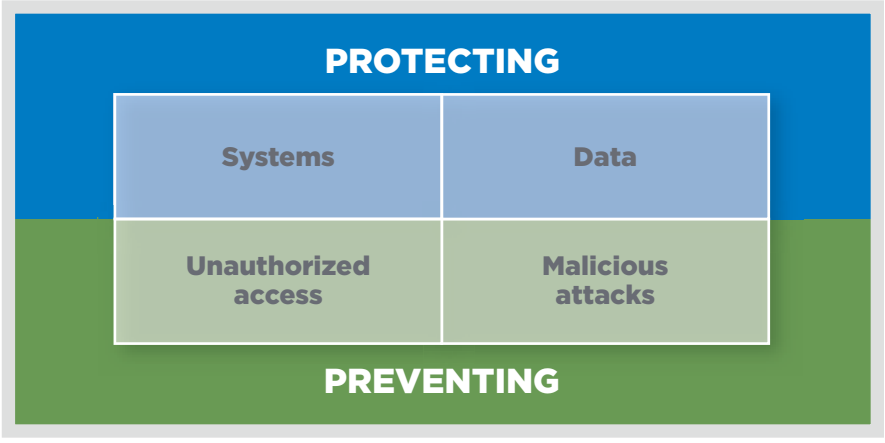

Figure 1. *Structuring a mobile security strategy from the desktop to the data center*

[1] For more information about security features, see "Freedom from Business as Usual: Introducing the New Dell Latitude," by Daniel Bounds, in *Dell Power Solutions,* August 2008, DELL.COM/Downloads/Global/Power/ps3q08-20080380-Bounds.pdf.

SLEEK, POWERFUL OFFERINGS SUPPORT A HIGHLY MOBILE WORKFORCE

The new Dell Latitude product line offers a comprehensive range of laptops to meet the diverse, individualized needs of an increasingly mobile workforce and the IT staff that supports it. At the same time, new Dell Precision mobile workstations are designed to run high-performance, graphics-intensive applications in a lightweight, durable chassis.

Anytime, anywhere computing: Dell Latitude laptops. The new Dell Latitude E4200, E4300, E5400, E5500, E6400, and E6500 laptops are designed for outstanding control and manageability, simplified security, comprehensive mobile services, rock-solid durability, and top-notch usability. For employees who travel frequently and want light, convenient devices that can last as long as they do, Latitude laptops help maximize productivity by offering up to 19 hours of battery life in select mainstream models. For those seeking a desktop replacement on the go, Latitude laptops are designed for seamless transitions between desktop and mobile work modes—supporting hot docking with small docks, stands, and peripherals across the new Latitude family. For true road warriors and power users, the ruggedized, lightweight Latitude E6400 ATG has been built and tested to meet MIL-STD 810F standards for dust, vibration, humidity, and altitude to help withstand even the most demanding field use.

Meeting diverse needs: (from left) Dell Latitude E6500, E6400 ATG, and E4300 laptops

SIMPLIFY ADMINISTRATION AND CUT COSTS

When users experienced hardware issues in the past, a member of the IT support staff could simply walk down the hall to fix the computer or handheld device on the spot. Today, mobile users are everywhere and are increasingly dependent on the technology practices provided by the IT department, which may reside in a different location. To truly enable the mobile workforce, organizations must help remote users to be as self-sufficient as possible by providing systems that perform as expected and allow people to individualize configurations without sacrificing security. In the data center, organizations need single, intuitive graphical management interfaces designed to simplify and automate routine tasks—freeing the IT staff to focus on strategic projects.

Dell offers a range of solutions, partner products, and managed service options to help organizations simplify management of their mobile infrastructure. For example, Dell Client Manager software from Altiris takes advantage of the capabilities of the Intel® Centrino® 2 processors with Intel vPro™ technology available in new Latitude laptops to provide basic hardware and software management capabilities as well as advanced client management. It also provides policy-based tools to help simplify management of remote systems by performing automated monitoring. For example, the software can check to make sure configurations for a particular employee are correct when that user logs in to the laptop. If the individual settings are incorrect, Dell Client Manager can automatically deny access, fix the settings, or schedule service.

Dell Client Manager helps reduce the need for IT support teams to arrive in person to troubleshoot or perform system maintenance and migration. Remote provisioning tools enable remote laptop configuration, helping minimize maintenance costs and user downtime. In addition, partner solutions are available for

Supporting flexible peripherals: Dell E-Flat Panel Stand integrated with Dell E-Port docking station

New Latitude laptops are designed not only to keep mobile users productive, but also to help simplify deployment and management for IT staff. Features such as Dell ControlVault, contactless smart card readers, and integrated fingerprint readers help create a secure platform that is easy to deploy, use, and manage, while a range of Dell ProSupport Services help IT staff protect valuable resources and data against theft or loss.

High-performance mobility: Dell Precision workstations. New Dell Precision M2400 and M4400 mobile workstations feature independent software vendor (ISV)–certified, workstation-class performance and enhanced graphics rendering in compact, lightweight form factors. Next-generation DisplayPort technology supports a wide variety of large external display hardware. In addition, these mobile workstations can share peripherals with Latitude laptops—helping simplify device management and support for IT departments.

Providing high-end performance in a durable, lightweight chassis: Dell Precision M4400 mobile workstation

organizations that already have management solutions in place but are looking to extend them or add new capabilities.

Dell ProSupport Mobility Services also offers solutions designed to free IT professionals from worry, helping minimize downtime and protect key enterprise data. Available most anywhere in the world, Dell ProSupport provides a globally consistent range of simple and flexible support options for mobile workers.[2] And through the Dell CompleteCare™ Accidental Damage Service,[3] Dell can repair or replace laptops that are affected by most accidental drops, liquid spills, electrical surges, extreme temperatures, or collisions.

PROTECT CRITICAL DATA

When mobile users are on the road, their backup practices can be inconsistent at best. Many mobile workers know they should be backing up their systems, but the hassle associated with the process can often sidetrack the best of intentions.

Inconsistent mobile backup processes can put enterprises at risk of losing critical data. They may even expose organizations to compliance violations if regulated data is lost. By enabling consistent, centralized backups through Dell Online Backup and Restore—which facilitates safe, secure, and automated backups of mobile systems over the Internet at redundant offsite facilities—Dell enhances data security and helps ensure that important information is centralized in enterprise data repositories.

SMOOTH TRANSITION MANAGEMENT

Even when enterprise IT executives fully understand the scope of what is required to truly enable the mobile workforce, unplanned image changes, product transitions, and other fire drills can make it difficult to focus on strategic objectives. By proactively managing product transitions, organizations can minimize costs and headaches—helping support mobile workers by making transitions as smooth as possible. Automated deployments can help organizations significantly reduce desk-side visits from technicians as well as network traffic associated with deployment.

Dell helps with transition management in several ways. For example, Dell readiness assessments, tools, and Client Migration services can help guide IT teams making the transition from the Microsoft Windows® XP Professional OS to the Microsoft Windows Vista® OS on their mobile devices. In addition, the Dell Latitude laptop and Dell Precision mobile workstation families offer dedicated hardware configuration options that are available worldwide—which means that a common image can be used in multiple countries, allowing enterprise-wide standardization that helps reduce the cost and complexity of managing hardware in a global economy.

Common peripherals—including power adapters, docking solutions, and monitor stands—are available for new Dell Latitude laptops and Dell Precision

[2] For more information on Dell ProSupport, see "Connect and Protect Workers on the Go with Dell ProSupport Mobility Services," in *Dell Power Solutions*, August 2008, DELL.COM/Downloads/Global/Power/ps3q08-20080374-Dell-ProSupport.pdf.

[3] CompleteCare service excludes theft, loss, and damage due to fire, flood or other acts of nature, or intentional damage. Customer may be required to return unit to Dell. For complete details, visit DELL.COM/ServiceContracts.

MOBILE NETWORKING—SIMPLIFIED

In a fast-moving business world, employees need constant access to the Internet and enterprise networks. However, multiple connection options and separate software clients for each network can complicate accessibility—and for many users, the amount of time required to access networks and the Internet is simply too much.

Dell ControlPoint software helps make wireless connectivity fast and easy by using information in preselected profiles to connect to different networks. A mobile broadband card, available in all Dell Latitude laptops and Dell Precision mobile workstations, supports Global Positioning System (GPS) and WiMAX to enable blazing fast Internet access once the WiMAX network infrastructure is completed.

Dell laptops support the IEEE draft 802.11n Wi-Fi® protocol with 3 × 3 antenna design in the laptop for maximum speed and throughput. Users also can utilize Bluetooth® 2.1 technology to connect to peripherals and devices such as smartphones, PDAs, mice, and keyboards. Included ultra-wideband (UWB) technology helps provide an increased range for use with wireless docking, printers, and scanners. In addition, Dell Wi-Fi Catcher™ features allow users to easily find out if a connection is available even when the system is off. Wi-Fi Catcher also has a switch that allows users to turn off antennae when not in use to help save battery life.

Dell Latitude laptops and Dell Precision mobile workstations help safeguard sensitive data by supporting various security protocols for wireless communication, including Wi-Fi Protected Access (WPA), which is designed to prevent other mobile users from capturing sensitive communications. Wave Systems EMBASSY Trust Suite helps reinforce virtual private network authentication and communication to help improve remote computing security. And for large-scale security needs, Dell offers managed client solutions or enterprise solutions such as server-based endpoint protection suites, firewall and security gateways, and detection systems.

mobile workstations, and Dell plans to continue this family commonality for years to come. As a result, transitioning from the new Dell Latitude and Dell Precision models to future releases is designed to be simpler and less costly than the transition from previous product families because it helps eliminate the requirement to purchase new docking peripherals and test or qualify new hardware.

Web-based Dell ImageWatch™ tools give IT professionals visibility into upcoming changes that could potentially impact system images. This capability helps reduce surprises, which can streamline budgeting and planning. In addition, Dell ImageDirect helps IT managers build a single image and use it on any Dell Latitude laptop or Dell Precision mobile workstation—allowing an image built on a currently shipping system to be transitioned almost immediately to a new Dell Latitude or Dell Precision system when it launches. Avoiding the need to build an individual image for each new laptop they deploy helps free organizations to develop value-added system options.

CREATE A FLEXIBLE MOBILE INFRASTRUCTURE

Given the extent to which workers around the world have adopted mobile computing, it is no surprise that enterprises in virtually every industry are redefining their policies and practices surrounding the mobile workforce. But enabling mobile computing can go well beyond just choosing which laptops to give to employees. IT support teams must develop and implement solid security plans and procedures. They must make it easy for workers to gain secure access to enterprise networks virtually anywhere, anytime. They need mobile infrastructures that facilitate simplified, centralized administration—while also making it easy for end users to back up key data. And when the time comes to upgrade to new systems, dedicated transition services can help smooth the way. New-generation Dell Latitude laptops and Dell Precision mobile workstations not only help meet the evolving needs of highly mobile workers, but also offer the requisite IT tools to help simplify deployment, management, and security of wide-ranging mobile devices.

Jeanne Feldkamp is a business and technology writer based in San Francisco. She has worked on several publications for leading high-tech corporations.

Daniel Bounds is a marketing professional for the Dell Global Relationship Marketing Group focused on commercial laptops. Daniel has previously held positions with the Dell Enterprise Product Group and Hewlett-Packard. He has a B.A. and an M.B.A. from the University of Texas at Austin.

Terry Myers is a senior product manager in the Dell Latitude product group, where he is responsible for product marketing for software and security offerings. He has a B.A. in Business and an M.B.A.

Tom Kolnowski is the editor-in-chief and publisher of *Dell Power Solutions* magazine.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Dell Latitude laptops:
DELL.COM/Latitude

Dell Precision workstations:
DELL.COM/Precision

Dell ProSupport:
DELL.COM/ProSupport

Dell ImageWatch:
DELL.COM/ImageWatch

Join the discussion on the new Dell Latitude family at the Dell TechCenter wiki:
DellTechCenter.com