Maximizing mobile efficiency and productivity

Best practices and solutions for your evolving BYOD strategy

Enhancing employee mobility can pay significant dividends for organizations and their employees. With secure access to corporate resources, employees can use mobile devices and other client systems to conduct a full range of work-related projects, whether they are away from their desks, with customers, traveling or at home.

The flexibility to work from any place at any time enables employees to more efficiently manage their time, increase their productivity and be more responsive to customers, suppliers and partners, all of which can provide huge benefits for their organizations. In fact, a survey by a U.K. retailer suggested that the use of mobile devices allows employees to increase their productivity by as much as two hours each day, or up to 460 hours of work per year.[1]

Nevertheless, maximizing mobile efficiency and productivity can be challenging for many organizations. As organizations launch bring-your-own-device (BYOD) programs, IT groups must accommodate a wide variety of devices and operating systems. At the same time, IT groups must provide the right tools to support key employee job functions and meet line-of-business (LOB) requirements. Finally, IT groups must deliver efficiency and productivity for mobile users without adding substantial IT complexity — otherwise, organizations could easily negate the benefits gained through enhanced mobile productivity.

This paper examines the challenges of supporting employee BYOD initiatives, and provides several best practices that can help your organization overcome those challenges. In addition, it highlights Dell solutions that can facilitate implementation of best practices, helping you boost employee efficiency and productivity while also enhancing the efficiency of IT management.

“The use of mobile devices allows employees to increase their productivity by as much as two hours each day, or up to 460 hours of work per year.”

Source: “Smartphones and tablets add two hours to the working day,” The Telegraph, October 31, 2012.

Identifying the challenges of BYOD productivity

Support a large variety of devices, operating systems and other user requirements

Employees are more likely to be efficient and productive if they can use the devices, operating environments and apps they already know. Supporting and enabling use of those known entities is advantageous to the organization as well; organizations can reduce (or eliminate) training and see faster time to value. And of course, allowing employees to use their own personal devices as part of a BYOD program offers the additional advantage of eliminating the costs of buying, supporting and repairing devices for employees.

Nevertheless, enabling a BYOD program can lead to a proliferation of devices and operating environments. Even if IT groups do not provide direct support for a device or operating system, they will have to support the interaction of that device with the company’s network, security policies, management solutions and more.

As IT groups try to handle such a wide variety of mobile devices and operating systems, they must also combat the potential for disappointing and frustrating users. If faced with complex or seemingly restrictive corporate access policies and security measures, mobile users might begin to use unsecure ways to communicate and collaborate. Those approaches, which might include public WiFi networks, personal email or cloud-based file-sharing services, could put the organization at risk of data leakage and cyberattacks.

With BYOD programs, employees want IT groups to respect their privacy when implementing corporate IT solutions. They want to make sure their individual contacts, emails, photos and other personal data are not accessed or deleted by their company. Failing to respect the privacy of employees could potentially result in legal or regulatory violations.

Address LOB needs

Of course, maximizing efficiency and productivity by mobilizing employee access to applications and data is not just a matter of giving users what they want. The IT team must also address the needs of the LOB groups in which employees work. IT must enable access to the right resources and provide the right tools — quickly — to help users complete their jobs efficiently and support LOB goals.

Beyond supporting email, calendar and contact functions on mobile devices, IT groups need to enable the key business apps that do the real work toward meeting LOB objectives.

Find and source the right IT solutions

Supporting a BYOD program could require IT groups to implement new networking, access management, security, device management, application modernization and other solutions. Selecting solutions piecemeal increases the cost and complexity of supporting the BYOD program because these solutions might not all work together (or require time-consuming integration), and IT groups might need to interact with multiple vendors for procurement and support.

In addition to making sure new solutions work together, your IT group will want solutions (and the devices they support) to integrate with your organization's existing processes, policies and infrastructure. Re-engineering and replacing key components of your current environment, or completely reworking existing processes, can drain time and resources from new initiatives, including the BYOD initiative you are trying to support.

You need an end-to-end solution, from a single strategic partner, that can help ensure interoperability and ease integration with your existing environment while streamlining ongoing management. Your BYOD program should not increase the burden or impair the efficiency of IT.

Connect, protect and transform

The best approach to maximizing mobile efficiency and productivity while controlling IT complexity should enable your organization to connect users to the information and resources they need; protect data, applications and networks; and transform how your organization supports and manages mobile productivity.

Connect: To maximize workforce productivity, you need to securely connect users with the resources they need anytime, anywhere. Solutions must support multiple mobile device types, form factors and operating systems.

Protect: The best strategies empower users while securing the business. Solutions must provide users with secure access to the specific resources they need to do their jobs while protecting devices, data, applications and networks from threats — and ensuring end-user privacy.

Transform: To connect and protect, many organizations will need to transform their approach to enabling and supporting mobility. To free up IT resources, organizations must provide ready-to-go cloud-based and over-the-air (OTA) deployments with simplified self-service portals. Choosing comprehensive solutions can help control IT complexity and reduce costs, while selecting professional services can help streamline transformations.

Addressing challenges with best practices

Adopting several best practices can help you achieve your goals of mobile efficiency and productivity as you connect, protect and transform.

Enable mobility

Prepare for managing a wide variety of devices. Before you implement a new employee mobility or BYOD program, you need to make sure you have solutions in place that can identify and track all mobile devices accessing your network, including Apple® iOS, Mac OS, Google® Android™ and Microsoft® Windows–based phones, tablets, laptops and desktops as well as thin clients, zero clients and emerging devices. These solutions should help you streamline administrative tasks for all devices used by your employees, giving you the flexibility to support multiple mobile enablement strategies, all from a central location.

You need an end-to-end solution, from a single strategic partner, that can help ensure interoperability and ease integration with your existing environment while streamlining ongoing management.

Making it fast and easy for employees to get the tools they need accelerates the time to value and helps avoid dangerous work-arounds.

Optimize the network and the infrastructure. As you implement your BYOD program, you might need to scale the bandwidth capacity and coverage of your network for greater demand. In addition, you will need to implement secure mobile access capabilities if you haven't already done so, and make sure those capabilities are prepared for growth in the number of users and devices. More employees will use mobile devices than before, and in many cases, each employee will use multiple devices. Devices running in permanently connected mode will continuously consume network bandwidth. From your WiFi network, firewalls and secure remote access solutions to your application servers and storage, your entire IT infrastructure must be prepared to accommodate more users without sacrificing performance.

Moreover, the infrastructure must be prepared for change. You need to be sure that the strategies and solutions you choose today can accommodate future changes in device types, operating systems, mobile enablement strategies, user requirements, security threats and more.

Develop and modernize apps. Will all the required business applications run as they should, and deliver a strong user experience on all the device types, form factors and operating systems you plan to support? In some cases, you might need to develop or customize applications. In doing so, you can optimize apps for mobile use cases and take advantage of device features such as cameras or GPS capabilities. Software licensing can present another challenge as the number and types of devices expand. You need ways to understand application usage patterns so you can gain a clear picture of software licensing compliance. Correlating installed software with license agreements, and identifying unauthorized applications, is critical to protecting your organization from financial risks and possible litigation. With better visibility into application usage, you can reduce financial exposure, minimize potential security issues and maintain control over your network.

Secure data. Of course, none of these preparations will be valuable unless your data is secure. You need the ability to enable secure remote access without jeopardizing company networks and information, whether that information is residing on a mobile device's memory, in a secure "container" environment that separates enterprise applications and data from personal ones, in the corporate data center or in transit. Establishing the right level of security might require a mix of encryption, virtualization, remote wipe, network traffic inspection, authentication, device integrity checks and other solutions.

Provide the necessary tools

While bolstering the IT infrastructure, you must also be sure you can quickly provide the enterprise applications that users and LOB groups want and need to do their jobs and meet their goals. In many cases, that means providing more than just email, contacts and calendaring functions. Users will need ways to securely search, access, modify and save files in a collaborative workspace. They might need a secure browser to work with web-based applications or access enterprise — or partner — portals. And they will need to run whichever additional applications — from word processing and spreadsheet software to customer relationship management (CRM) to inventory tracking — are critical for doing their jobs.

In addition to ensuring that these applications are compatible with employee devices and operating systems, IT groups need to devise ways to deploy these tools. Providing user self-service can be an efficient, on-demand approach to delivering the right tools. Employees can download and install approved, tested apps without requiring the assistance of IT. Offering knowledge bases or a similar way to acquire assistance and information can also help improve efficiency and reduce downtime without having to involve IT staff members.

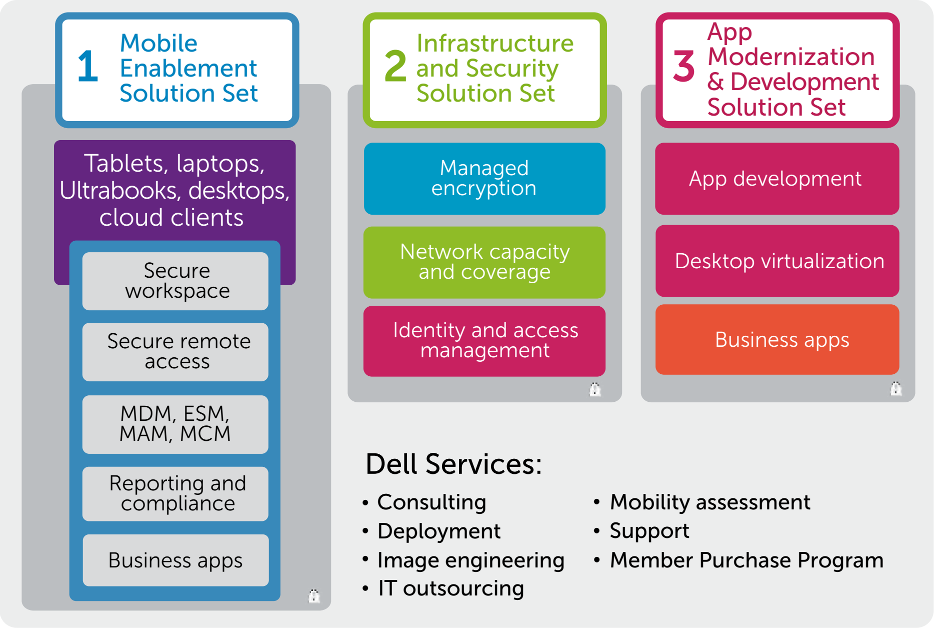
Making it fast and easy for employees to get the tools they need accelerates the time to value and helps avoid dangerous work-arounds. Employees are less likely to use unsecure public wireless networks and non-approved apps and devices if they can quickly access what they need when they need it. Simplifying deployment and installation of approved tools also helps enhance employee efficiency — employees do not need to waste valuable time trying to find and implement potentially flawed one-off solutions.

Enhance IT efficiency

Expanding support for employee mobility and implementing new BYOD programs is likely to add cost and complexity if IT administrators are asked to manually provision enterprise workspace environments, manage policies and resolve issues with a wide range of devices and operating systems. You need best practices that can help you control those costs and complexity, streamlining administrative tasks and automating processes so your IT group can stay focused on innovating and contributing to strategic projects.

Automate. Whenever possible, automate tasks. Establish repeatable processes for tasks such as onboarding new employees and their devices, and then automate those processes. You could identify access needs, assign profiles and even initiate training with human resources without IT intervention. Automating these and other processes can help enhance efficiency for users and IT while also ensuring consistency, reducing errors and freeing up IT resources.

You need best practices that can help you control IT costs and complexity so your IT group can stay focused on innovating and contributing to strategic projects.



Dell Mobility Solution Sets can help you boost mobile efficiency and productivity with capabilities to enable mobility, prepare your infrastructure and deliver business apps to a range of platforms.

Dell offers complete solution sets that can help you implement best practices and achieve your goals of improving mobile efficiency and productivity while accommodating evolving needs.

Centralize management. Select solutions that allow administrators to conduct a full array of management tasks from a centralized location and with integrated consoles. Make sure your administrators are pushing out new apps, managing devices and providing support from a single place. They will be able to respond faster to LOB and user needs — again helping to boost efficiency and productivity — while reducing administrative complexity.

Reduce the number of vendors. Avoid selecting multiple, discrete point solutions from multiple vendors. An end-to-end solution from a single strategic partner can streamline procurement, help ensure interoperability (avoiding the need for integration work) and simplify ongoing support.

Boosting efficiency and productivity with Dell Mobility Solution Sets

Dell offers complete solution sets that can help you implement best practices and achieve your goals of improving mobile efficiency and productivity while accommodating evolving needs. Enable mobility, prepare your infrastructure and security strategy, and provide the business applications that users need. These solution sets allow you to progressively add capabilities as your BYOD program expands and your requirements change. With support for heterogeneous IT environments and diverse collections of devices, these solution sets enable you to easily integrate new capabilities into your existing infrastructure (*see figure*).

Mobile Enablement Solution Set

The Mobile Enablement Solution Set provides unified, comprehensive management and security capabilities — built with industry-leading security technology — to support your choice of devices, operating systems, user types, use cases and mobile enablement strategies. A key part of this solution set, the Dell Enterprise Mobility Management (EMM) solution can help you deliver anytime, anywhere access to corporate resources, maintain tight security, and control administrative complexity by integrating management of both endpoints and enterprise workspace containers.

With this solution set, you can provide a secure enterprise workspace on all devices your employees use — from smartphones to desktops — regardless of who owns them. Employees gain the apps and services they need to collaborate and become productive. At the same time, you can retain IT control over the workspace and minimize complexity. Manage systems, devices, apps, content, access policies and encryption while providing secure remote access.

For organizations using a choose-your-own-device (CYOD) mobile enablement model, this solution set also offers a portfolio of business-approved devices such as Dell desktops, laptops, Ultrabook™ systems, tablets and cloud clients that can help deliver the performance and reliability they need while streamlining support. These devices can be made available to your employees through the Dell Member Purchase Program so you can encourage them to buy devices you prefer.

Infrastructure and Security Solution Set

The Infrastructure and Security Solution Set helps you prepare your processes, policies and infrastructure for rapidly growing resource demands while protecting enterprise data. Use this solution set to provide employees with fast, simple and secure remote access to enterprise resources so they can be productive anywhere, anytime without compromising security. Capitalize on identity and access management capabilities to control access to company systems and information, improve IT efficiency and maintain compliance.

Bolster your wireless network to improve wireless performance, support more devices in your corporate space and create distinct employee and guest wireless networks, with different access and security levels, to optimize resources. And implement centrally managed encryption solutions to help protect enterprise data residing on desktops, laptops and mobile devices as well as on external media and in public cloud storage.

Application Modernization and Development Solution Set

The Application Modernization and Development Solution Set can help you extend business applications to a wide variety of mobile devices and deliver a robust user experience, capitalizing on mobile device capabilities to improve employee efficiency and productivity.

Use this solution to develop new applications or port existing applications to smartphones, tablets, cloud clients, laptops and desktops. Dell experts can help you assess your existing application collection, design and then implement the appropriate architecture.

For enterprise customers, the Dell Mobility Center of Excellence (COE) can build an overall mobile app strategy, typically with multiple applications planned. Dell provides subject-matter expertise and guides the overall strategy and process. Because IT and business priorities often differ, the COE helps brings all parties together to form ideas, and develop and deliver solutions that meet the needs of the entire business.

This solution set can also help you create a virtual desktop infrastructure (VDI) environment so you can stream enterprise Windows applications and operating systems on personally owned or corporate-issued client systems, without the work of re-architecting an application.

Dell Services

Supplementing these solution sets, Dell offers an array of services, ranging from mobility assessment and consulting to image engineering, deployment and support. Dell Services can help you rapidly realize the value of these solution sets while tailoring capabilities to your precise needs.

Overcoming the barriers to productivity

For organizations and their employees, the benefits of enhancing mobile efficiency and productivity are clear. But achieving those benefits can be difficult. Implementing best practices can help your organization meet the needs of users and their lines of business while controlling IT complexity.

Dell Mobility Solution Sets provide the end-to-end capabilities you need to enable mobility, optimize your infrastructure and maintain high data security, and deliver the business apps that employees need to do their jobs. With these solution sets, you can address the challenges of improving mobile productivity and rapidly realize gains while laying a foundation for an evolving BYOD strategy.

> Dell offers an array of services, ranging from mobility assessment and consulting to image engineering, deployment and support.

Learn more

Dell Mobility Solutions:
dellmobilitysolutions.com

Dell Enterprise Mobility Management:
Dell.com/EMM

Dell laptops and Ultrabook systems:
Dell.com/XPS

Dell Data Protection | Encryption:
Dell.com/dataprotection

Dell SonicWALL Mobile Connect, Secure Remote Access and Next-Generation Firewall:
software.dell.com/landing/80

Dell Networking W-Series Wireless and ClearPass:
Dell.com/networking

Custom Application Development Services:
Dell.com/applicationservices

Client Mobility and BYOD Consulting:
Dell.com/learn/us/en/555/services/client-mobility-solutions-consulting

Contact a Dell expert:
https://marketing.dell.com/mobility-solutions

[1] "Smartphones and tablets add two hours to the working day," The Telegraph, October 31, 2012, http://www.telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html.

December 2013