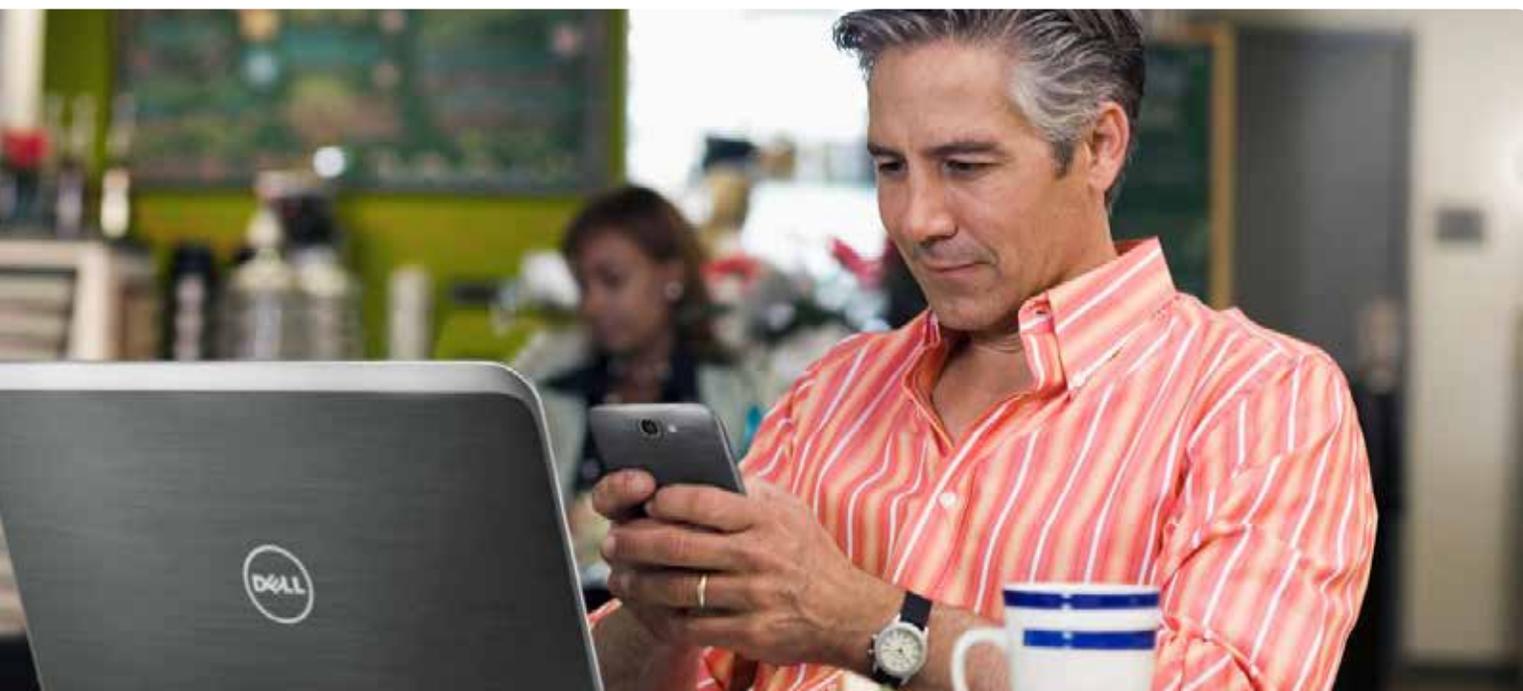# Future-proof your mobility strategy with Dell Enterprise Mobility Management

Change is the only constant in the mobile workforce landscape. Changes in mobile device technology are leading the way. Smartphone, tablet and laptop vendors are introducing multiple new models per year, in a range of form factors, while Apple, Google and Microsoft release frequent OS updates. Meanwhile, new vendors are entering the mobile marketplace, offering new devices, enterprise device management solutions and security solutions. Filtering out the noise in the marketplace is no easy task.

At the same time, users are changing the ways they work. Employees are increasingly relying on mobile devices for a wider range of work functions and expecting to access corporate information anytime, anywhere. These changes in work habits can lead to new security issues. In some cases, employees are resistant to corporate security policies and corporate control if it impedes their productivity or appears to encroach on their personal privacy — users don't want

their IT department to access personal social media posts or accidentally erase personal photos stored on a device. Organizations need ways to expand access to corporate networks and increase user adoption of corporate solutions without making the organization vulnerable to a large and growing array of threats.

The enablement strategies for promoting mobile productivity and flexibility are changing, too. Organizations that once issued corporate-owned, corporate-managed devices are beginning to implement choose-your-own-device (CYOD) programs and allowing employees themselves to enable and manage corporate-issued devices. At the same time, the bring-your-own-device (BYOD) trend is accelerating rapidly, with users demanding the use of personally owned devices for work and organizations recognizing the potential productivity and cost advantages of BYOD. The question is, if and when organizations move to an all-BYOD approach, will the IT group be ready?

> To maximize workforce productivity, you need ways to securely connect users with the resources they need anytime, anywhere.

Changes in devices, operating systems, work habits and mobile device business models can make endpoint management and security very difficult. IT groups need to continuously adjust the way they provision new devices, deploy enterprise apps, enable remote access, secure corporate information and more.

Many IT groups will simply add new mobile device management and security solutions as needed. But this piecemeal approach brings its own challenges.

Choosing multiple point solutions from multiple vendors can produce integration issues and add ongoing management and support complexity while forcing organizations to manage multiple vendor relationships. Mergers and activities among smaller vendors can make the situation worse — IT groups can be left scrambling to ensure the products they selected will continue to be supported in the future. Using a piecemeal approach, IT groups might find the point solutions they selected yesterday cannot address their organization's evolving business needs and emerging requirements.

Given the continuous changes in the mobile workforce landscape, how can your organization future-proof its mobility strategy? How can you accommodate a wide range of variables today and prepare for supporting even more devices, operating systems, work habits and mobile enablement strategies in the future?

This paper identifies best practices that can help your organization devise a flexible and scalable approach to address a large number of variables and accommodate change while maintaining security and controlling administrative complexity. It then explores the Dell Enterprise Mobility Management (EMM) solution and highlights how this solution can play a key role in helping meet current needs while enabling you to prepare for the future.

Connect, protect and transform

The best mobility or BYOD strategy 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 ways to securely connect users with the resources they need anytime, anywhere. Solutions must support multiple, evolving mobile device types, form factors and operating systems, including smartphones and tablets based on Apple iOS, Google® Android™ and Microsoft® Windows 8; laptops and desktops running Mac OS X, Windows and Linux® operating systems; cloud clients, including thin and zero clients; and emerging technology.

Protect: The best strategies free the user while securing the business. Solutions must provide users with safe access to the specific resources they need to do their jobs while also protecting devices, data, applications and networks from threats. Implementing virtual private network (VPN) technology, passwords, encryption, firewalls and policy management along with container-based security (which isolates corporate apps and information from the personal operating environment) can help organizations secure sensitive information while simultaneously ensuring employee privacy.

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

Adopt best practices

Adopting several best practices can help you address a wide array of current variables while also preparing your mobility or BYOD strategy for change.

Know your users

Before first implementing a BYOD strategy, adopting particular security approaches or choosing mobile device management solutions, you need to understand your mobile users:

- What are their job functions?
- What devices and operating systems are they using?
- How do they need to access and use data?
- What skills do you need to help them connect, collaborate and find unique ways to work?
- How do they support their line-of-business goals?

Answering these questions will help you make the right technology choices and then subsequently define the best profiles for your users. Of course, the effort to understand users cannot end when you implement a new solution. You must continue to track user needs and behaviors to improve planning and accommodate changing needs.

Define mobility/BYOD policies across the organization

Defining mobility or BYOD policies across your organization is essential for meeting the requirements and addressing the concerns of users and business units. For example, employees will want to know whether they can select any type of device, who will support the device, and how personal information will be protected if they need to turn in their device for service. The human resources group needs to know if employees will receive stipends when they purchase their own devices and whether productivity will suffer if a device needs to be repaired or replaced. The legal department will need to determine what information can be remotely wiped, whether the devices allow the organization to track the user, and how the organization can

best secure data in transit and at rest. Answering these and other questions before implementation is critical.

Implement flexible strategies and select flexible solutions

You need strategies and solutions that can adapt to changing mobile enablement strategies, devices, user requirements, security threats and more. For example, your organization might currently offer corporate-owned, personally enabled devices, but in the future, you might decide to implement a CYOD program, adopt a BYOD strategy or employ a combination of multiple strategies. At the same time, you need ways to handle the continuous introduction of new devices, form factors and operating systems. You need solutions that will enable you to provision devices, manage endpoints and containers, secure enterprise data and applications and handle other functions no matter what enablement strategies and devices you support today and tomorrow.

Choose embedded security solutions

New devices and new work habits could open new vulnerabilities for your data, applications and networks. Meanwhile, hackers will continue to introduce new types of threats. Incorporating embedded security — security that cannot be modified or worked around by users — can help ensure the strongest protection, even as devices, work habits and threats change. Embedded security solutions can help protect data, apply the right profiles and policies to users, and secure the network.

- **Data:** Implement solutions that automatically encrypt data at rest and in motion. Use data loss protection (DLP) solutions to prevent data leaks.
- **Users:** Require two-factor authentication (such as a password plus a hardware-based token) to help ensure correct identities. Adopt solutions that integrate with Microsoft® Active Directory® to match users with the right profiles and policies.

> Defining mobility or BYOD policies across your organization is essential for meeting the requirements and addressing the concerns of users and business units.

DELL

> With container solutions, workers can capitalize on a responsive, native-like experience no matter where they are.

- **Network:** Protect the network with next-generation firewall solutions that scan every packet entering and exiting the network. Enable secure remote access and require employees to connect to corporate resources through a VPN connection.

Create secure containers

As part of your security strategy, adopting container-based solutions can help prevent security problems even as devices and personal operating environments change. The container can separate enterprise data and applications from personal ones. Doing so prevents personal applications, data or threats from commingling with or capturing corporate information. This protects end-user privacy as well.

Some desktop virtualization solutions can also prevent the commingling of personal and corporate data by running applications and retaining data only in the data center. Container-based solutions can supplement a virtualized desktop approach, enabling users to also work offline without compromising security.

By enabling offline productivity, container-based solutions can help support an increasingly mobile workforce that is often forced to deal with poor internet connectivity while traveling. With container solutions, workers can capitalize on a responsive, native-like experience no matter where they are. In addition, container solutions can help organizations accommodate a wider range of device types, including smartphones and small tablets, for which virtualization solutions are often a poor fit because of the devices' smaller screen size.

Adopt solutions designed to control complexity

As your organization expands support for workforce mobility, your IT environment is likely to become more complex. Administrators will need to manage more device types, operating systems and work habits, and they will employ more security and mobile device management solutions.

Selecting solutions designed to control that complexity will be essential in addressing current requirements and preparing for the future while working within your resource limitations. Choosing end-to-end solutions with integrated management consoles can help significantly diminish management complexity; reducing the number of distinct consoles that administrators must use will save time and money. Appliance- and cloud-based solutions can help cut deployment complexity and help achieve fast time-to-value.

Stay focused on innovation

IT groups must stay focused on innovation. IT can become a strategic partner, empowering business users by providing the tools to increase productivity and efficiency. To continue to make important contributions to the business, your IT group needs to anticipate changes, investigate emerging technologies and devise ways to quickly apply new approaches to support an evolving business. Staying engaged with leading mobility solution vendors and maintaining ongoing dialogs with peers can help your IT group stay on top of trends and envision new ways to enhance mobile productivity.

Work with a single, end-to-end solution vendor

Working with multiple vendors can create a variety of challenges. First and foremost, you are likely to pay more when you purchase solutions from multiple vendors compared with acquiring the same capabilities from a single vendor. Integrating those solutions can also be difficult — and in many cases, IT administrators are forced to use multiple, distinct management consoles. IT groups also need to deal with multiple vendors for ongoing support.

Choosing a single vendor that offers end-to-end solutions can help reduce costs, ensuring integration of capabilities and management consoles while simplifying support.

DELL

Look for a vendor with an excellent support track record

Small vendors, whose limited resources could make them subject to mergers and acquisitions, might not be able to provide the long-term support and the reliable, consistent road map you need to prepare your strategy for continued change. Choose a vendor that has staying power in the industry and a long track record of delivering excellent support.

Gain flexible, end-to-end management with Dell Enterprise Mobility Management (EMM)

Dell EMM enables you to implement best practices that can help you prepare your mobility strategy for change. Designed to support a wide range of devices, operating systems, worker needs/profiles and mobile enablement strategies, Dell EMM is a comprehensive mobile enablement solution from a single strategic partner. Dell knows IT — Dell has been empowering customers to build successful environments since 1984. The Dell EMM solution is built with proven, industry-leading security technology, so it delivers a higher level of security than typical mobile device management solutions.

With Dell EMM, you can implement the security and management capabilities for your precise requirements, whether you need to support corporate-issued devices or a BYOD program, mobile devices or desktops, endpoints or containers (*see figure*).

Dell EMM offers secure mobile enablement for a full array of corporate-issued and BYO devices, including smartphones (iOS, Android), tablets (iOS, Android, Windows), laptops and desktops (Windows, Mac, Linux), thin clients and zero clients. This comprehensive solution provides the following capabilities for all of these endpoints:

- Mobile device management (MDM)
- Mobile application management (MAM)
- Mobile content management (MCM)
- Endpoint systems management (ESM)
- Secure access to corporate resources
- An integrated management console
- End-user self-service
- Real-time, consolidated reporting and alerts
- Automatic backups of end-user data

> Dell EMM enables you to implement best practices that can help you prepare your mobility strategy for change.

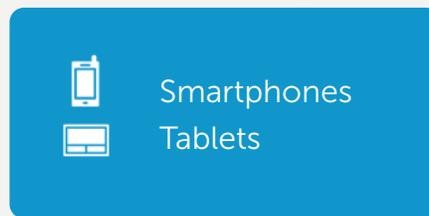## Dell EMM: Comprehensive mobile enablement

Endpoint management
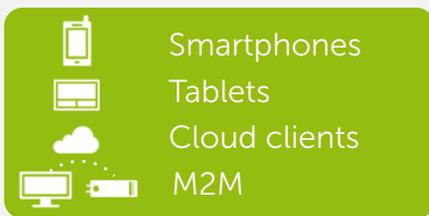
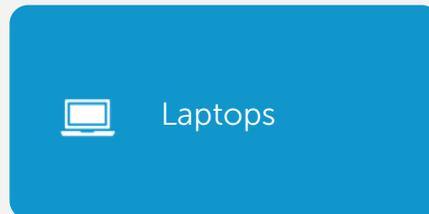Smartphones
Tablets
Cloud clients
M2M

Laptops
Desktops

Container management

Smartphones
Tablets

Laptops

Dell EMM is a comprehensive solution with management and security capabilities to manage a variety of endpoints and containers.

BYOD

Dell believes that you cannot support corporate-issued and personally owned devices the same way — personal devices must be treated differently. To enable all the capabilities listed above for BYO devices, Dell EMM enables you to manage a secure enterprise workspace on the device instead of managing the device itself. Dell EMM provides a container for personally owned smartphones, tablets and laptops. The container — which includes managed encryption, policy management and DLP — separates enterprise data and apps from personal ones, and simplifies integration with your existing IT infrastructure and processes. The container benefits users as well — they can access all the corporate resources they need simply by downloading a non-invasive app. Users can then be assured that the company is not accessing or potentially deleting any personal information.

For BYOD smartphones and tablets, Dell EMM provides:

* Built-in secure remote access with DLP
* A single, secure corporate mobile app for productivity and collaboration, which provides:
   – Email
   – Calendar
   – Contacts
   – Secure mobile browser
   – Secure local file explorer

While smartphone and tablet operating systems allow for fewer changes from IT, laptop and desktop operating systems might require IT deployment of a full corporate image/operating system. As a result, for BYOD laptops and desktops, Dell EMM offers a secure corporate Microsoft Windows image (on Mac OS, Windows and Linux). With Dell EMM, your IT group can achieve easy integration with existing IT infrastructure and processes.

The unified Dell EMM solution is different from those offered by other point solution vendors. With Dell as your strategic partner, you gain:

* **Breadth and choice of management:** You can manage everything from smartphones and containers to cloud clients and desktops — regardless of who owns the endpoint — and you can choose how you manage each endpoint, whether by user identity or use case.
* **Integration of proven technologies:** Dell has industry-leading IP in management and security, and we are integrating these elements into our solution. Dell EMM is not a "new" solution — it has proven strength.
* **Industry-leading security:** This built-in feature lets you control multiple functions from your management console, including setting up configurations, policies, DLP, secure remote access, encryption and passwords.
   Professional services: Dell offers image engineering to help you create and manage the image deployed to personal devices, while Client Mobility and BYOD Consulting help you analyze customer needs and define the road map for mobility technologies. With EMM migration, you can move from your current management service to EMM, and a Center of Excellence helps you become a mobility expert, which can enhance the partnership with your line-of-business owners and end users.

Best practices

Dell EMM can help address several best practices to help you prepare your endpoint enablement strategy for change. It offers:

* **Comprehensive management:** Comprehensive mobile enablement capabilities help streamline a full range of administrative functions while also helping you understand which devices employees are using and how they are using them.

- **Flexibility:** Dell EMM provides the flexibility to support a wide range of current technologies plus technologies you might not yet have implemented, such as thin or zero clients. Dell EMM also enables you to deploy and support the business apps and services you need.
- **Embedded security:** Embedded security features, such as secure remote access and encryption, as well as containerization capabilities, help keep corporate information, applications and networks secure.
- **Controlled complexity:** Integrated management consoles help control the complexity that can come with expanding mobility or BYOD programs, plus user self-service that helps offload tasks from IT. Integrated capabilities mean that you can add components seamlessly without having to conduct your own time-consuming integration work.
- **Innovation:** Dell EMM helps facilitate IT innovation by supporting a diverse array of devices plus emerging technologies. With Dell EMM, IT groups can deliver a responsive, modern experience for a growing range of use cases and enablement strategies.
- **Single vendor:** Dell EMM is an end-to-end solution from a single strategic partner — one that has staying power in the industry and a track record of excellent support. Working with a single vendor helps ensure integration of capabilities and management consoles, streamlines deployment and simplifies support.

Prepare for change

As mobile technologies, work habits and enablement strategies continue to evolve, you need ways to accommodate existing requirements, prepare your strategy for change and protect your investments. Employing best practices can set you on the right course for addressing current needs and planning for the future.

Dell EMM provides the tools you need to employ those best practices. With this comprehensive solution from a single strategic partner, you can support an evolving mobile enablement strategy that enables secure anytime, anywhere access to information from a wide variety of devices while controlling administrative complexity.

Learn more

Dell Mobility Solutions:
dellmobilitysolutions.com

Dell Enterprise Mobility Management:
Dell.com/EMM

Comprehensive mobile enablement capabilities help streamline a full range of administrative functions while also helping you understand which devices employees are using and how they are using them.

November 2013